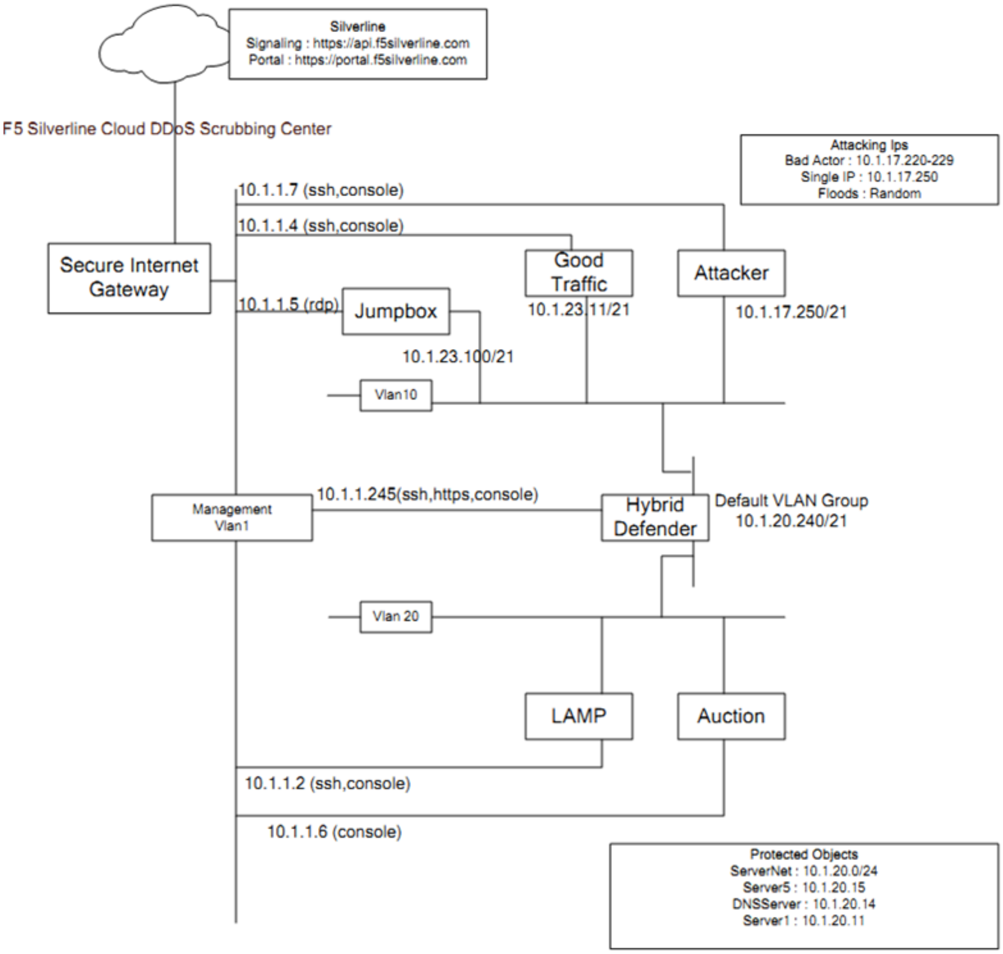
Agility 2018 Hands-on Lab Guide

Contents:

1 Getting Started

1.1 Lab Topology



1.1.1 Access and Credential Summary

You will using the Win7 jumpbox to access other systems for all labs. You will use **Putty** that has been pre-configured with appropriate keys in order to access the **DHD CLI**, **Good Client**, and the **Attacker** systems. The short cuts are on the desktop. You will be logged in as "root".

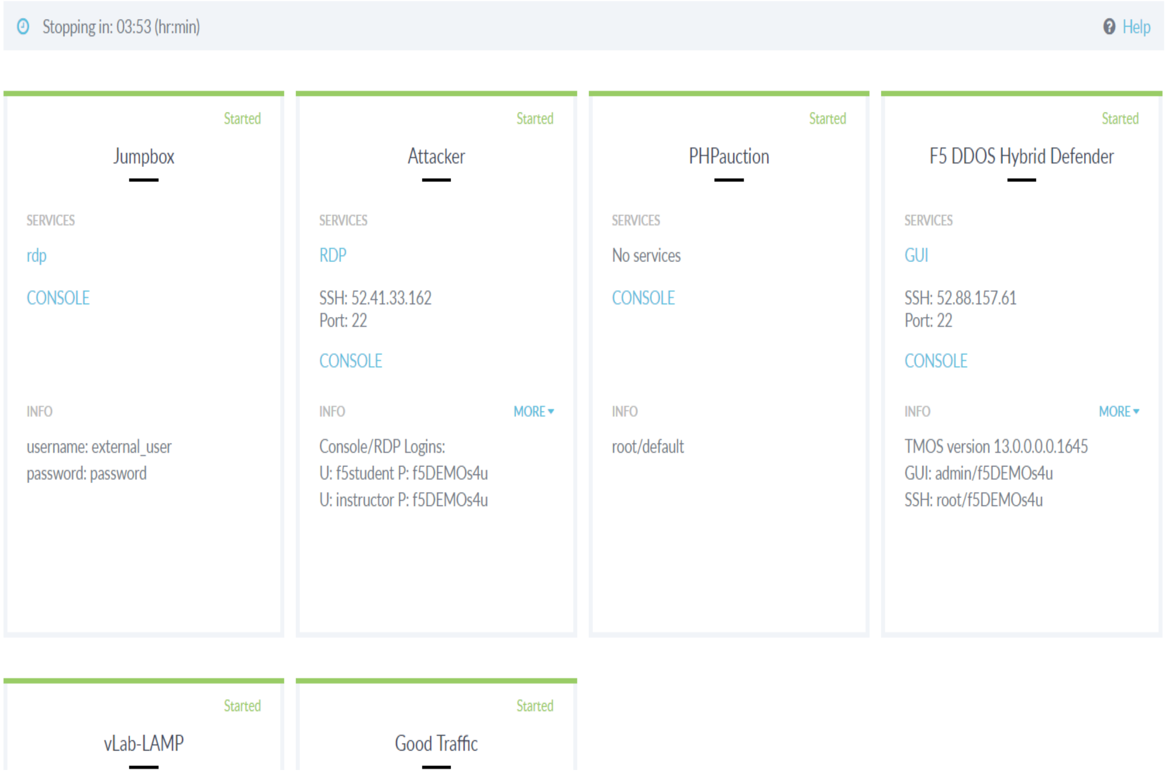
1.1.2 Lab Components

System	Username	Password
Ravello	Given at site	Given at site
Win7 Jumpbox	external_user	f5DEMOs4u
Hybrid Defender - WebUI	admin	f5DEMOs4u
Hybrid Defender - CLI	root	f5DEMOs4u
Good Client	ubuntu	Use key
Attacker	ubuntu	Use key
Auction CLI	root	default
Lamp CLI	root	default
Lamp X-Server Shell	xubuntu	<no password>

1.2 Accessing the Lab Environment

1.2.1 Task 1 – Open your RDP client and connect to your Windows Jumpbox

- A URL will be provided by your Instructor at the training site that will access the training portal.
- Click the Jumpbox RDP link.



Stopping in: 03:53 (hr:min)

Help

Started

Jumpbox

SERVICES

rdp

CONSOLE

INFO

username: external_user
password: password

Started

Attacker

SERVICES

RDP

SSH: 52.41.33.162
Port: 22

CONSOLE

INFO MORE ▾

Console/RDP Logins:
U: f5student P: f5DEMOs4u
U: instructor P: f5DEMOs4u

Started

PHPauction

SERVICES

No services

CONSOLE

INFO

root/default

Started

F5 DDOS Hybrid Defender

SERVICES

GUI

SSH: 52.88.157.61
Port: 22

CONSOLE

INFO MORE ▾

TMOS version 13.0.0.0.0.1645
GUI: admin/f5DEMOs4u
SSH: root/f5DEMOs4u

Started

vLab-LAMP

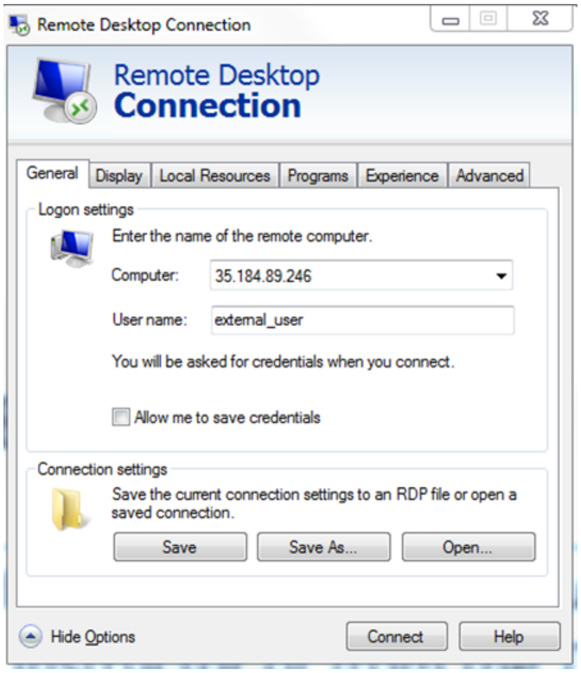
Started

Good Traffic

This will RDP to the Jumpbox where you will work all the labs from.

Note: Use the show options to provide details.

- Login to the Jumpbox
- User name: Jumpbox external_user. Password: f5DEMOs4u



Remote Desktop Connection

Remote Desktop
Connection

Logon settings

Enter the name of the remote computer.

Computer: 35.184.89.246

User name: external_user

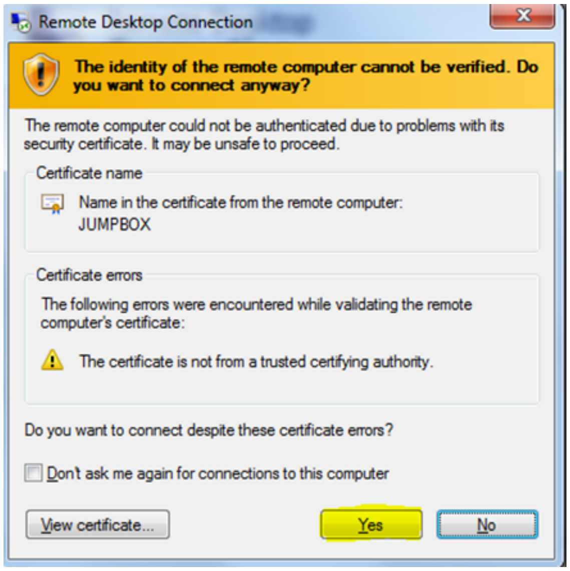
You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

- Click YES at the warning


Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
JUMPBOX

Certificate errors

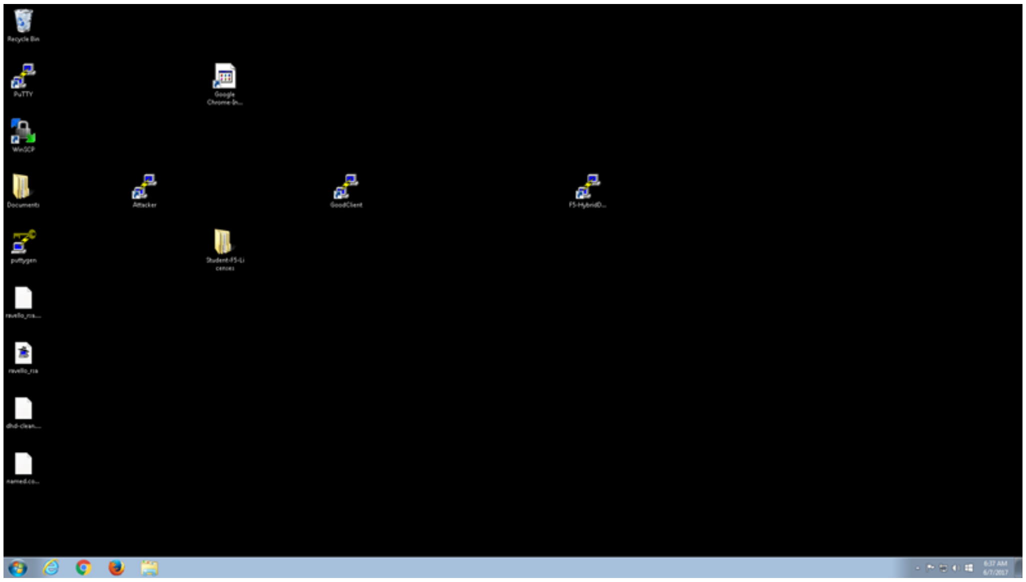
The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

Note: All Exercises/Tasks are to be completed from the Windows Jumpbox. There are various shortcuts – Chrome Incognito, Putty shortcuts, Licensing Folders on the jumpbox that you will use through the exercises.



2 Class 1: Introduction to DDoS with F5 Herculon

DDoS Hybrid Defender, a hybrid DDoS solution that offers comprehensive protection, high availability, and is easy to deploy and manage. It guards against aggressive volumetric and targeted DDoS attacks, includes hardware-assisted DDoS mitigation, and optionally, connects with Silverline, a cloud-based scrubbing service.

This class covers the following topics:

- Initial Set-up, Device Configuration and Protected Object Configuration.

2.1 DDoS Hybrid Defender Setup

In this module you will learn how to complete the initial setup of F5 Networks DDoS Hybrid Defender

2.1.1 Lab 1 – DDoS Hybrid Defender Setup

Estimated completion time: 45 minutes

Task 1 – Initial Set-up

- Open a web browser and access supplied link.(Given at Location)
- Login to the BIG-IP Configuration Utility via your preferred browser?

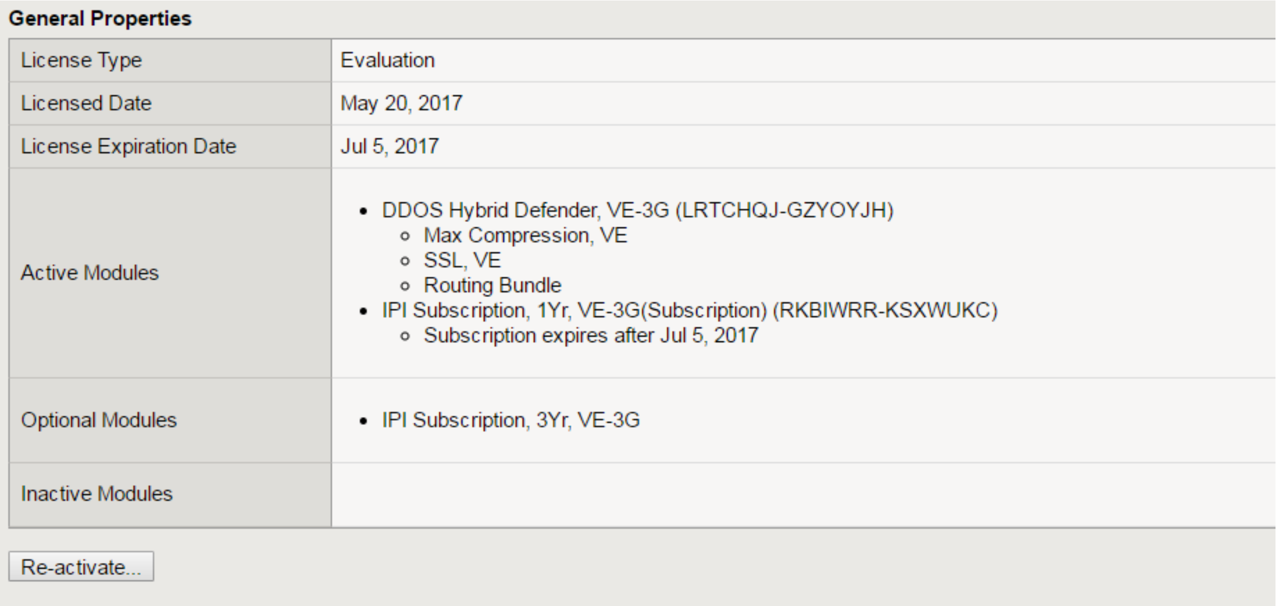
Note: When you first power up a F5 DHD device you would go through the steps of Licensing and Provisioning. We have assigned the management IP, hostname, NTP and DNS servers. You will be re-activating the license using a new license key.

- On the **System > Platform** page configure the following, and then click **Update**.

Host Name	<your name>.f5demo.com
Root Account (Password and Confirm)	f5DEMOs4u
Admin Account (Password and Confirm)	f5DEMOs4u

- This will log you out. Log back in

- On **Device Management->Devices** select the device and then click "**Change Device Name**. . . ". Update the device name to match the hostname you have chosen. Retain Current Authority
- Click **Update** to save changes
- Review and Verify the following: **System -> Configuration -> Device -> NTP** page add **pool.ntp.org** to the Time Server List, and then click **Update**.
- Review and Verify the following: **System -> Configuration -> Device ->DNS** page add 8.8.8.8 to the DNS Lookup Server List, and then click **Update**.
- Open the **System > License** page and **re-activate** the BIG-IP system using the new development license key using Manual mode. Copy and Paste License file.



General Properties

License Type	Evaluation
Licensed Date	May 20, 2017
License Expiration Date	Jul 5, 2017
Active Modules	• DDOS Hybrid Defender, VE-3G (LRTCHQJ-GZYOYJH) ○ Max Compression, VE ○ SSL, VE ○ Routing Bundle • IPI Subscription, 1Yr, VE-3G(Subscription) (RKBIWRR-KSXWUKC) ○ Subscription expires after Jul 5, 2017
Optional Modules	• IPI Subscription, 3Yr, VE-3G
Inactive Modules	

- Click **Next** and explore **Resource Provisioning** page

Note: The above task ensures that you are using a purpose built DDoS Hybrid Defender. If you are familiar with other F5 Modules/Technology that you have used in the past, you will notice that we have none of those provisioned.

- When done click **Submit**.
- Access the Jumbox via RDP. PuTTY into the Hybrid Defender. Login with `root` and restart services

```
bigstart restart
```

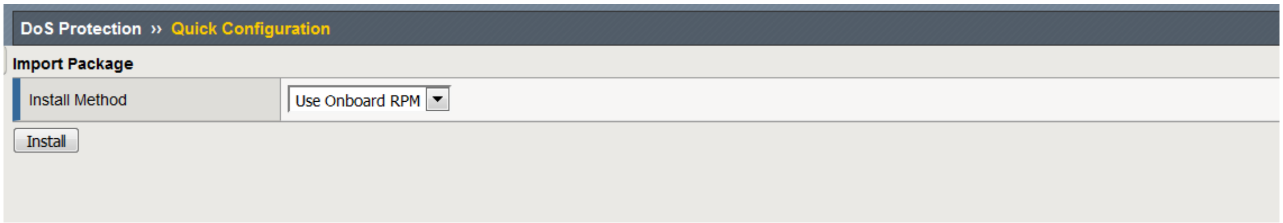
Take a break, ask questions, talk to your neighbor ..it will take several minutes to restart

Note: You MUST re-activate, even if the current license key hasn't expired. For Silverline access each BIG-IP system must use a unique license key.

Task 2 – DDoS Hybrid Defender iApp and Base Configuration

- In the BIG-IP Configuration Utility, open **DoS Protection > Quick Configuration** page.

- Select Install RPM method of Onboard
- Click **Install**

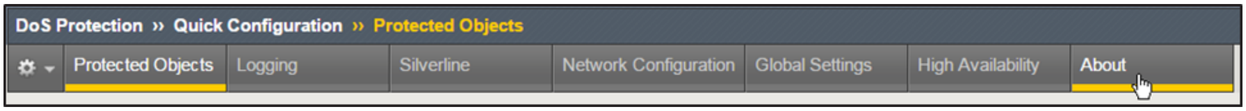


DoS Protection » Quick Configuration

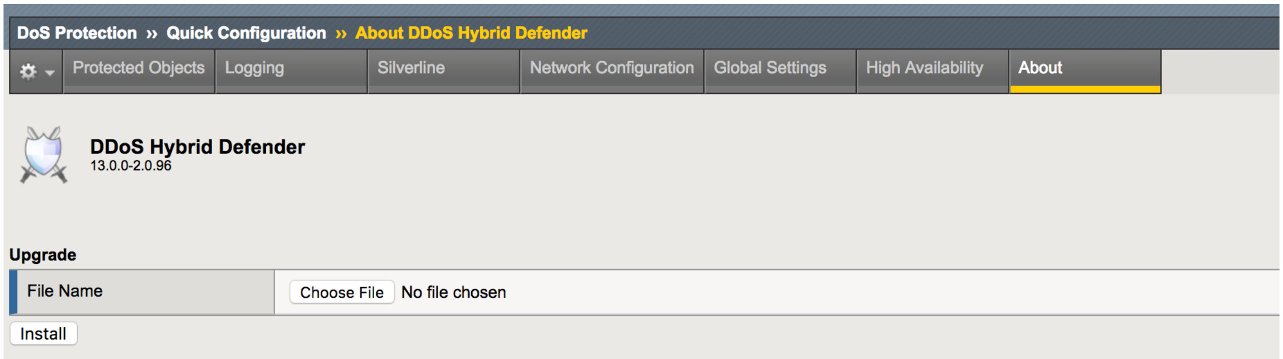
Import Package

Install Method: Use Onboard RPM

- Open the About page



- This page displays the current version of DDoS Hybrid Defender (DHD). You use this page to install and update the iApp LX version for DHD when newer versions are released.

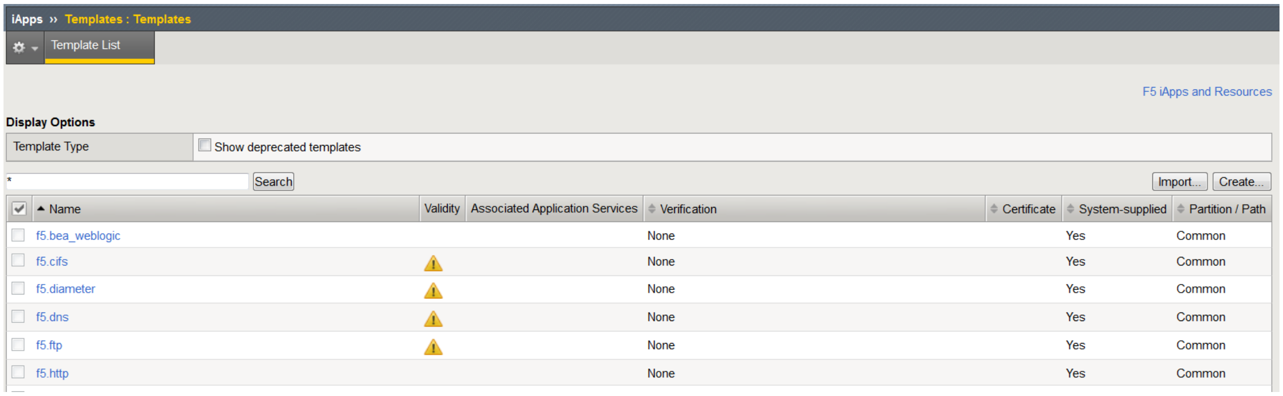


DDoS Hybrid Defender
13.0.0-2.0.96

Upgrade

File Name: Choose File No file chosen

- In the BIG-IP Configuration Utility, click **iApps**, **Templates** and **Import**, importing the two templates located on the jumpbox documents folder.

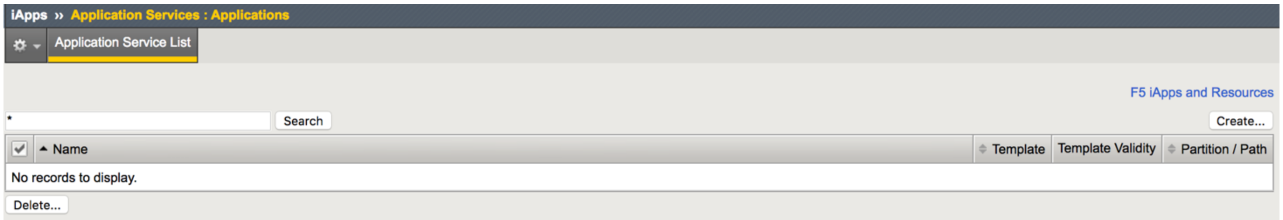


Display Options

Template Type: □ Show deprecated templates

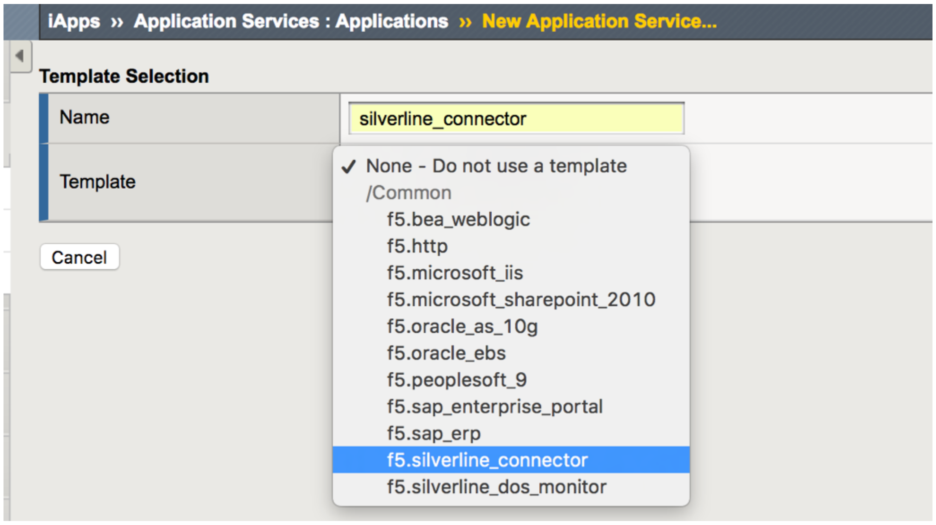
☑	Name	Validity	Associated Application Services	Verification	Certificate	System-supplied	Partition / Path
□	f5.bea_weblogic			None		Yes	Common
□	f5.cifs	⚠		None		Yes	Common
□	f5.diameter	⚠		None		Yes	Common
□	f5.dns	⚠		None		Yes	Common
□	f5.ftp	⚠		None		Yes	Common
□	f5.http			None		Yes	Common

- Use the **Browse** and **Upload** buttons. (You will do this once for each template)
- In the BIG-IP Configuration Utility, open **iApps > Application Services** and select **Create**



No records to display.

- You will be creating two services based on the two Silverline Templates:
  - F5.silverline_connector
  - F5.silverline_dos_monitor


iApps » Application Services : Applications » New Application Service...
Cancel
None - Do not use a template
/Common
f5.bea_weblogic
f5.http
f5.microsoft_iis
f5.microsoft_sharepoint_2010
f5.oracle_as_10g
f5.oracle_ebs
f5.peoplesoft_9
f5.sap_enterprise_portal
f5.sap_erp
f5.silverline_connector
f5.silverline_dos_monitor

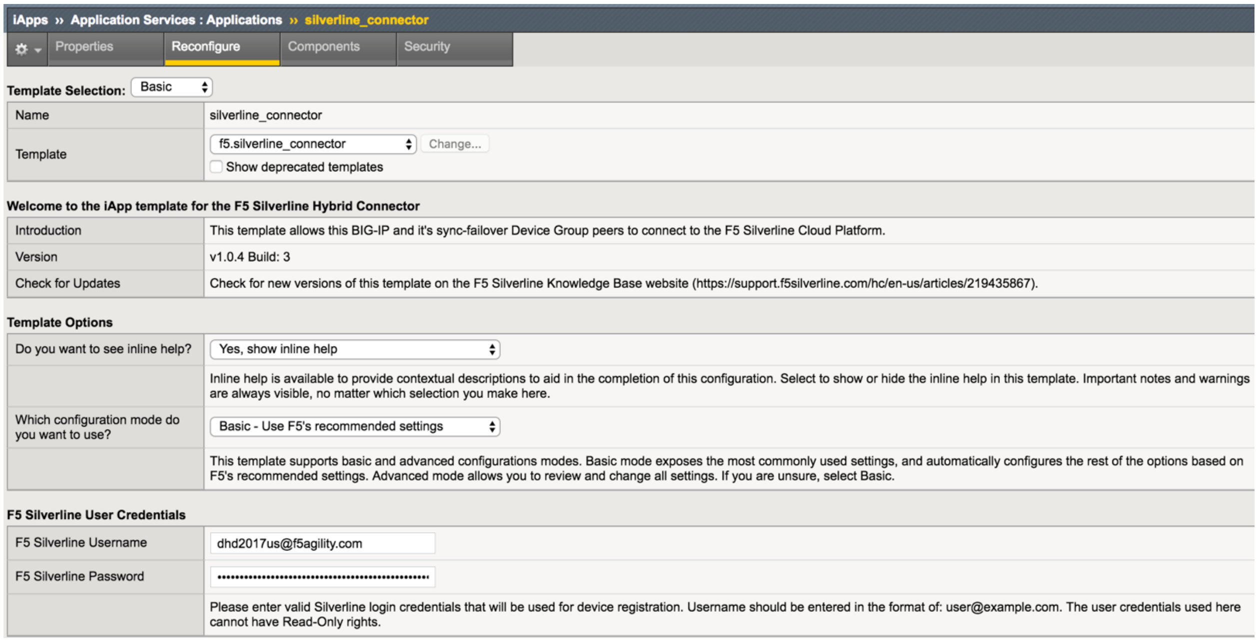
Template Selection

Name: silverline_connector

Template: f5.silverline_connector

- Use the default settings for the Silverline connector
- Use the Silverline username and password supplied

Note: This is case sensitive – make sure email address is all lowercase



iApps » Application Services : Applications » silverline_connector

Template Selection: Basic

Name	silverline_connector
Template	f5.silverline_connector Change... □ Show deprecated templates

Welcome to the iApp template for the F5 Silverline Hybrid Connector

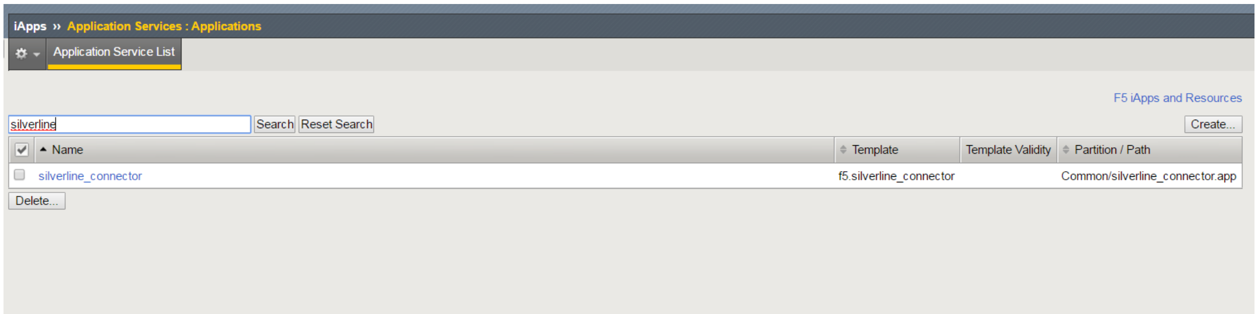
Introduction	This template allows this BIG-IP and it's sync-failover Device Group peers to connect to the F5 Silverline Cloud Platform.
Version	v1.0.4 Build: 3
Check for Updates	Check for new versions of this template on the F5 Silverline Knowledge Base website (https://support.f5silverline.com/hc/en-us/articles/219435867).

Template Options

Do you want to see inline help?	Yes, show inline help
	Inline help is available to provide contextual descriptions to aid in the completion of this configuration. Select to show or hide the inline help in this template. Important notes and warnings are always visible, no matter which selection you make here.
Which configuration mode do you want to use?	Basic - Use F5's recommended settings
	This template supports basic and advanced configurations modes. Basic mode exposes the most commonly used settings, and automatically configures the rest of the options based on F5's recommended settings. Advanced mode allows you to review and change all settings. If you are unsure, select Basic.

F5 Silverline User Credentials

F5 Silverline Username	dhd2017us@f5agility.com
F5 Silverline Password	••
	Please enter valid Silverline login credentials that will be used for device registration. Username should be entered in the format of: user@example.com. The user credentials used here cannot have Read-Only rights.

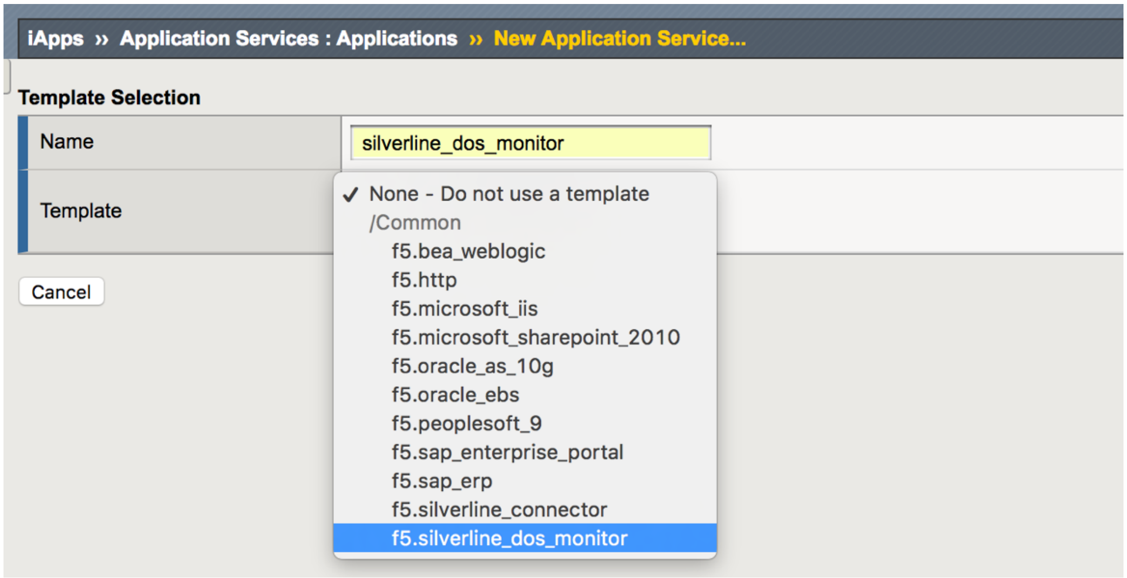


iApps » Application Services : Applications

silverline

☑	▲ Name	Template	Template Validity	Partition / Path
□	silverline_connector	f5.silverline_connector		Common/silverline_connector.app

- Create the 2nd service for the Silverline DOS Monitor (f5.silverline_dos_monitor)

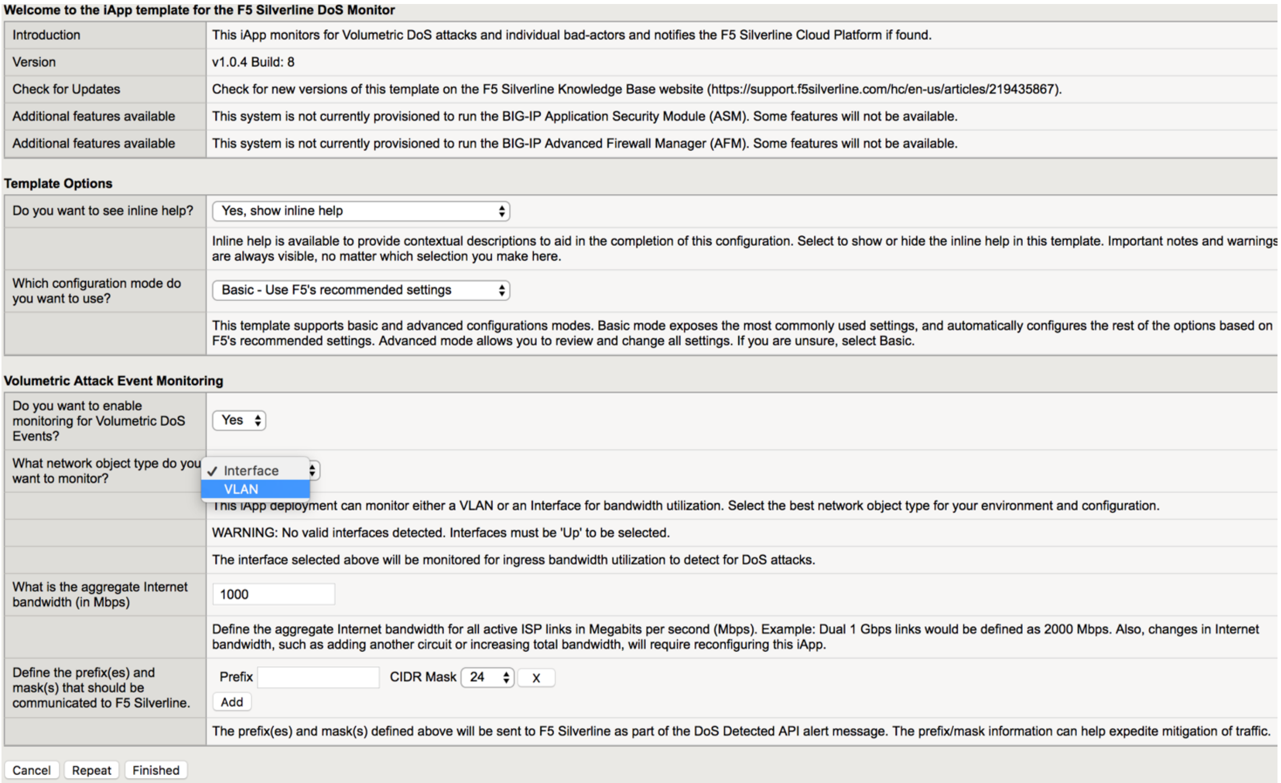


iApps » Application Services : Applications » New Application Service...

Template Selection

Name	silverline_dos_monitor
Template	✓ None - Do not use a template /Common f5.bea_weblogic f5.http f5.microsoft_iis f5.microsoft_sharepoint_2010 f5.oracle_as_10g f5.oracle_ebs f5.peoplesoft_9 f5.sap_enterprise_portal f5.sap_erp f5.silverline_connector f5.silverline_dos_monitor

- Use the default settings for the dos_connector except for Volumetric Attack Event Monitoring, switch the network object from interface to VLAN.



Welcome to the iApp template for the F5 Silverline DoS Monitor

Introduction	This iApp monitors for Volumetric DoS attacks and individual bad-actors and notifies the F5 Silverline Cloud Platform if found.
Version	v1.0.4 Build: 8
Check for Updates	Check for new versions of this template on the F5 Silverline Knowledge Base website (https://support.f5silverline.com/hc/en-us/articles/219435867).
Additional features available	This system is not currently provisioned to run the BIG-IP Application Security Module (ASM). Some features will not be available.
Additional features available	This system is not currently provisioned to run the BIG-IP Advanced Firewall Manager (AFM). Some features will not be available.

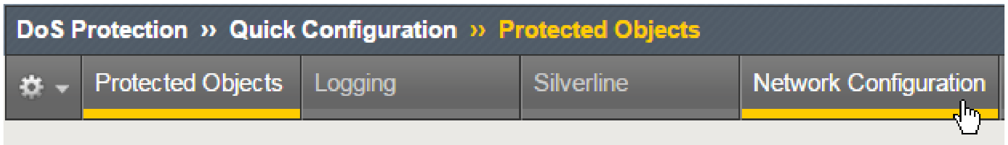
Template Options

Do you want to see inline help?	Yes, show inline help
	Inline help is available to provide contextual descriptions to aid in the completion of this configuration. Select to show or hide the inline help in this template. Important notes and warnings are always visible, no matter which selection you make here.
Which configuration mode do you want to use?	Basic - Use F5's recommended settings
	This template supports basic and advanced configurations modes. Basic mode exposes the most commonly used settings, and automatically configures the rest of the options based on F5's recommended settings. Advanced mode allows you to review and change all settings. If you are unsure, select Basic.

Volumetric Attack Event Monitoring

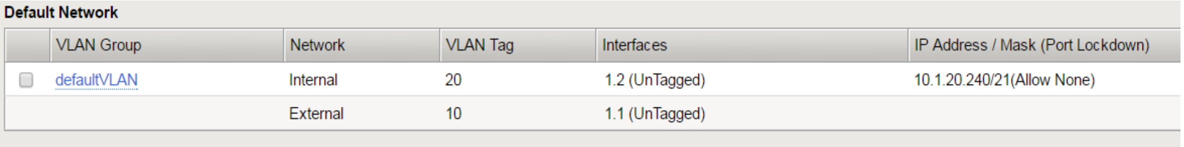
Do you want to enable monitoring for Volumetric DoS Events?	Yes
What network object type do you want to monitor?	✓ Interface VLAN
	This iApp deployment can monitor either a VLAN or an Interface for bandwidth utilization. Select the best network object type for your environment and configuration.
	WARNING: No valid interfaces detected. Interfaces must be 'Up' to be selected.
	The interface selected above will be monitored for ingress bandwidth utilization to detect for DoS attacks.
What is the aggregate Internet bandwidth (in Mbps)	1000
	Define the aggregate Internet bandwidth for all active ISP links in Megabits per second (Mbps). Example: Dual 1 Gbps links would be defined as 2000 Mbps. Also, changes in Internet bandwidth, such as adding another circuit or increasing total bandwidth, will require reconfiguring this iApp.
Define the prefix(es) and mask(s) that should be communicated to F5 Silverline.	Prefix CIDR Mask 24 X Add
	The prefix(es) and mask(s) defined above will be sent to F5 Silverline as part of the DoS Detected API alert message. The prefix/mask information can help expedite mitigation of traffic.

- Open the **DoS Protection > Quick Configuration Network Configuration** page.



- In the Default Network section click **default VLAN**.
- Configure the VLANs using following information, and then click **Done Editing**.

Internal: VLAN Tag	20
Internal: Interfaces	1.2 Untagged
Internal: IP Address / Mask	10.1.20.240/21 (Click **Add**)
External: VLAN Tag	10
External: Interfaces	1.1 Untagged (Click **Add**)



Default Network

	VLAN Group	Network	VLAN Tag	Interfaces	IP Address / Mask (Port Lockdown)
□	defaultVLAN	Internal	20	1.2 (UnTagged)	10.1.20.240/21(Allow None)
		External	10	1.1 (UnTagged)	

- At the bottom of the page click **Update** to create the default network.
- Open the **Network > VLANs > VLAN Groups** page and click **defaultVLAN**.
- A Bridged (VLAN Group) L2 configuration consistent recommended practices for most deployments was automatically created
- Open the **Network > DNS Resolvers > DNS Resolver** list page and click **Create**.

- Enter default_DNS_resolver and then click **Finished**.
- A DNS resolver is required by bot signatures to allow for proper detection of benign search engines such as Google and Bing.
- On the Jumpbox desktop, PuTTY to the BIG-IP
- Login as `root`
- Verify DNS by typing the following

  ```
  nslookup api.f5silverline.com
  ```

- Type the following to verify the correct date setting:

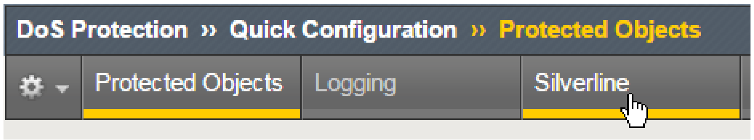
  ```
  date
  ```

- If the BIG-IP system date is not accurate, correct it using the following commands:

```
bigstart stop ntpd
ntpdate 10.1.1.254
bigstart start ntpd
```

Task 3 – Configure Silverline Signaling

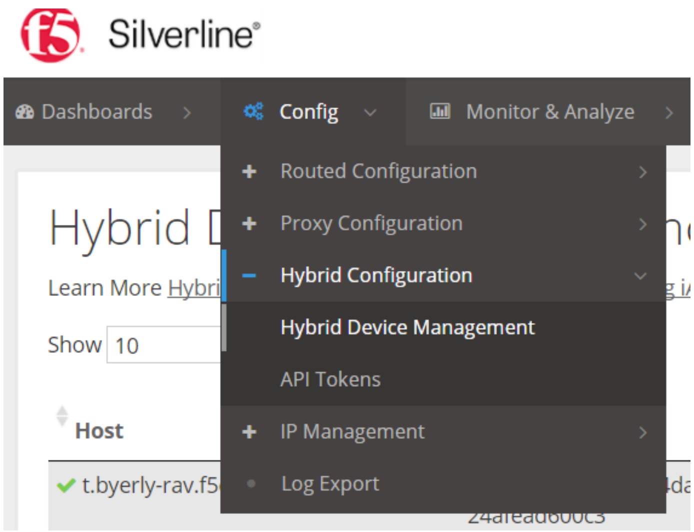
- In the BIG-IP Configuration Utility, open the **DoS Protection** > **Quick Configuration** page.
- Open the **Silverline** page.



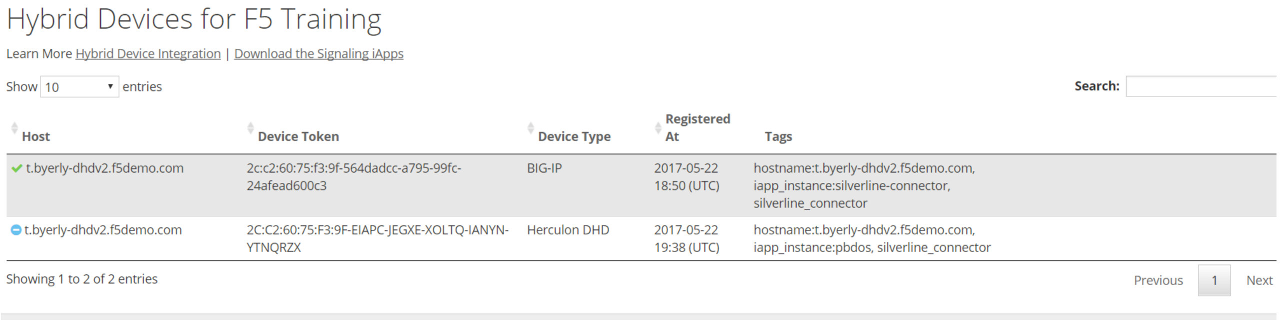
- Configure using following information, and then click **Update**.

Username	dhd2017us@f5agility.com
Password	HybridDefense!Wins!
Service Address	https://api.f5silverline.com

- Register the device with the Silverline iApp, to provide bandwidth utilization updates in **iApps->Application Services->Applications->silverline_connector**. In the iApp, select **Reconfigure** and then click **Finished**. This will cause the iApp to register under the new device name.
- Use a web browser and access https://portal.f5silverline.com.
- Log in with the above credentials
- In the Silverline browser, open the **Config->Hybrid Configuration->Hybrid Device Management** page**.**



- Locate your DHD device by searching for (<your name prefix>.f5demo.com) .
- Click the **Approve** button to approve device registration.


Hybrid Devices for F5 Training
Learn More Hybrid Device Integration | Download the Signaling iApps
Show 10 entries
Search:

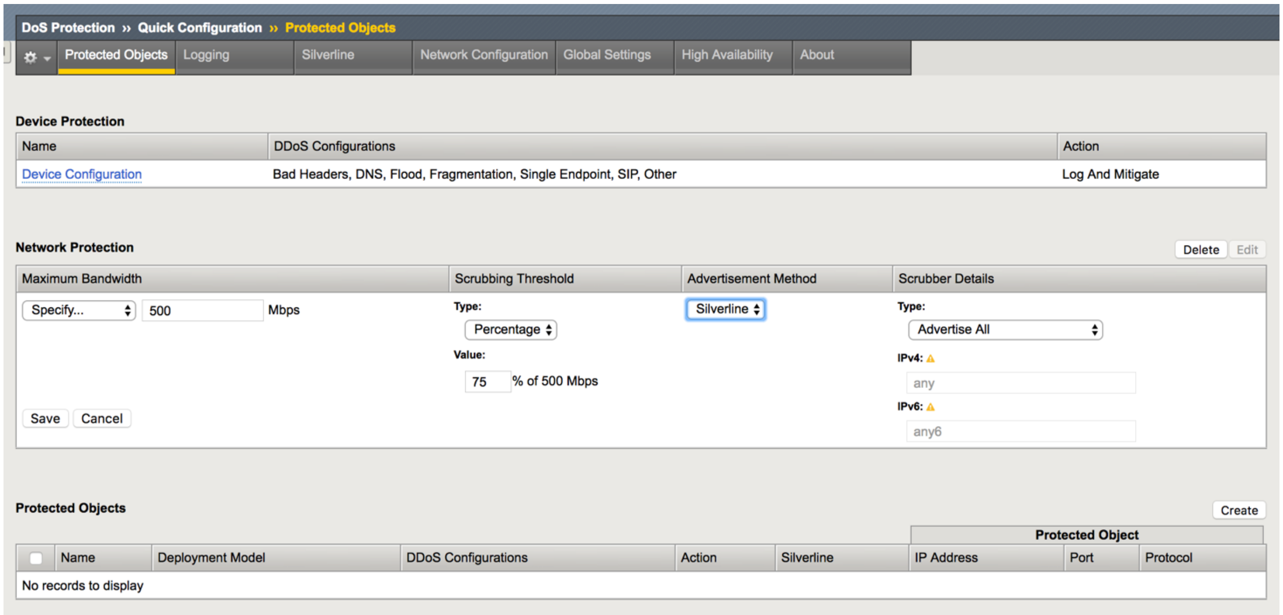
Host	Device Token	Device Type	Registered At	Tags
✓ t.byerly-dhdv2.f5demo.com	2c:c2:60:75:f3:9f-564dadcc-a795-99fc-24afead600c3	BIG-IP	2017-05-22 18:50 (UTC)	hostname:t.byerly-dhdv2.f5demo.com, iapp_instance:silverline-connector, silverline_connector
t.byerly-dhdv2.f5demo.com	2C:C2:60:75:F3:9F-EIAPC-JEGXE-XOLTQ-IANYN-YTNQRZX	Herculon DHD	2017-05-22 19:38 (UTC)	hostname:t.byerly-dhdv2.f5demo.com, iapp_instance:pbdos, silverline_connector

Note: For Silverline device registration to function properly there must be some specific considerations. The BIG-IP system must have a unique device ID, which is comprised of attributes like Base MAC and registration key. In Ravello and similar virtual environments the Hybrid Defender VE must be re-licensed uniquely each time.

Task 4 – Configure DHD Device Bandwidth Thresholds

- **In the DoS Protection > Quick Configuration page, open the Protected Objects** page.
- In the **Network Protection** section click **Create**.
- Configure using following information, and then click **Save**.

Maximum Bandwidth: Specify	500
Scrubbing Threshold: Type	Percentage
1.20Scrubbing Threshold: Value	75
Advertisement Method	Silverline
Scrubber Details: Type	Advertise All



Device Protection

Name	DDoS Configurations	Action
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other	Log And Mitigate

Network Protection

Maximum Bandwidth	Scrubbing Threshold	Advertisement Method	Scrubber Details
Specify... 500 Mbps	Type: Percentage Value: 75 % of 500 Mbps	Silverline	Type: Advertise All IPv4: any IPv6: any6

Protected Objects

						Protected Object		
□	Name	Deployment Model	DDoS Configurations	Action	Silverline	IP Address	Port	Protocol
No records to display								

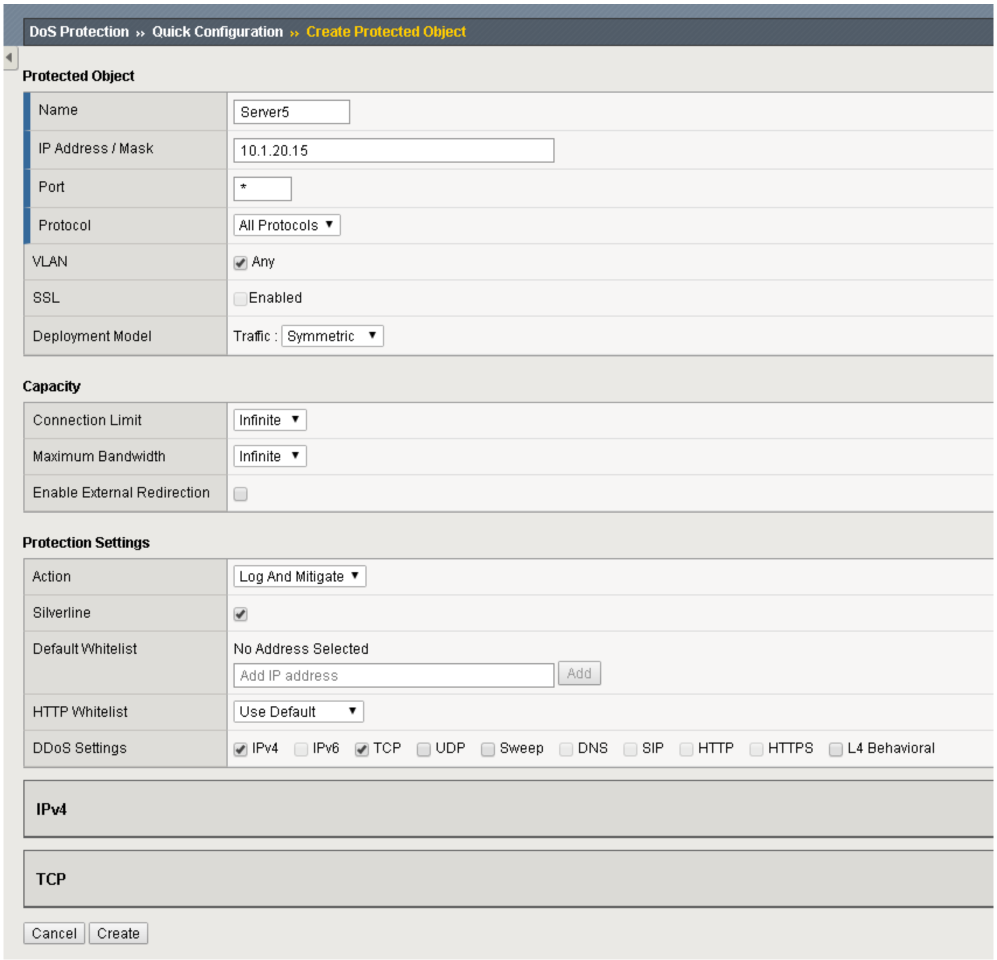
- That completes the setup for BIG-IP DDoS Hybrid Defender with Silverline integration.

2.1.2 Lab 2 – Start Baseline Traffic Generation

Task 1 – Create Protected Objects that the baseline traffic will be targeting

- In the BIG-IP Configuration Utility, open the **DoS Protection>>Quick Configuration** page and in the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	Server5
IP Address	10.1.20.15
Port	*
Protocol	All Protocols
VLAN	Any
Protection Settings: Action	Log and Mitigate
Protection Settings: Silverline	Yes (selected)
Protection Settings: DDoS Settings	IPv4, TCP,



DoS Protection » Quick Configuration » Create Protected Object

Protected Object

Name	Server5
IP Address / Mask	10.1.20.15
Port	*
Protocol	All Protocols ▾
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric ▾

Capacity

Connection Limit	Infinite ▾
Maximum Bandwidth	Infinite ▾
Enable External Redirection	□

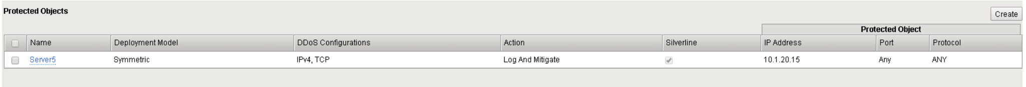
Protection Settings

Action	Log And Mitigate ▾
Silverline	☑
Default Whitelist	No Address Selected Add IP address [Add]
HTTP Whitelist	Use Default ▾
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

IPv4

TCP

- This protected object will be used for Auto-Threshold



Protected Objects

						Protected Object		
□	Name	Deployment Model	DDoS Configurations	Action	Silverline	IP Address	Port	Protocol
□	Server5	Symmetric	IPv4, TCP	Log And Mitigate	✓	10.1.20.15	Any	ANY

Task 2 – Run Scripts to start L4 traffic generation – Good Traffic

- Putty SSH (use the shortcut) to open a shell to the good client system.
- Login as user : `ubuntu`. The session is preconfigured to authenticate with a certificate.
- Start the auto-threshold baselining script with:

```
# sudo bash
# cd ~/scripts
# ./baseline_l4.sh
```

Note: Ignore the “sudo: unable to resolve host xjumpbox” when you issue the sudo bash command throughout the labs.

2.1.3 Lab 3 – Configuring Hybrid Defender DDoS protection

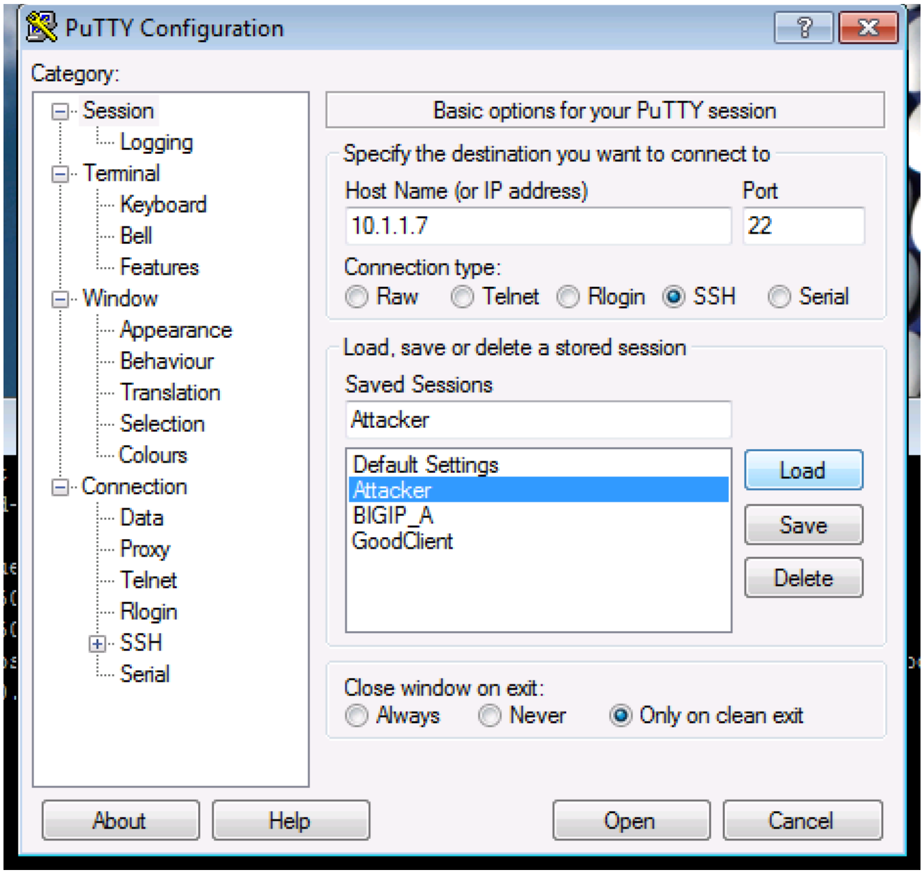
Task 1 – Disable Device-Level DHD DoS Protection

In this lab you will disable **device-level** DoS flood protection, and then issue an ICMPv4 flood and review the results.

- **PuTTY** to the BIG-IP CLI (10.1.1.245) and resize window by making it wider. Login with root/f5DEMOs4u.
- At the **config** prompt, type (or copy and paste) the following command:

  ```
  tcpdump -i 0.0
  ```

- Open a second **PuTTY** window and Load the Attacker Saved Session at **10.1.1.7** and log in as **ubuntu**. I't will use **a pre-loaded public key** as the credentials.



Specify the destination you want to connect to

Host Name (or IP address): 10.1.1.7

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Attacker

Default Settings
Attacker
BIGIP_A
GoodClient

Close window on exit: ○ Always ○ Never ● Only on clean exit

- At the **config** prompt, type (or copy and paste) the following command:

  ```
  ping 10.1.20.12
  ```

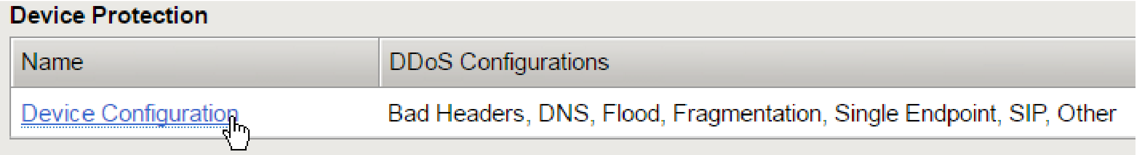
The attacker can successfully communicate with a back-end resource behind the BIG-IP DHD.

- Examine the **tcpdump** window and verify ICMP packets are flowing through the BIG-IP DHD.

Note: The listener for the ICMP packets is the VLAN group.

- Cancel the `ping` command, then verify the `tcpdump` stops receiving ICMP packets, and then press **Enter** several times to clear the recent log entries.

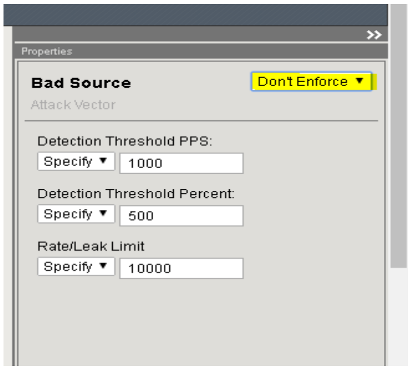
- In the Configuration Utility, in the **DoS Protection, Quick Configuration, Device Protection** section click **Device Configuration**.



Device Protection

Name	DDoS Configurations
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other

- In the **Bad Headers** row click the **+** icon, and then click **Bad Source**.
- On the right-side of the page select the drop-down to “Don’t Enforce”



Properties

Bad Source Don't Enforce ▾

Attack Vector

Detection Threshold PPS:
Specify ▾ 1000

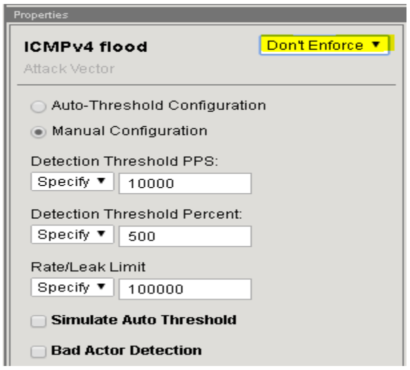
Detection Threshold Percent:
Specify ▾ 500

Rate/Leak Limit
Specify ▾ 10000

- In the **Flood** row click the **+** icon, and then click **ICMPv4 flood**.

Note: If you minimize by clicking the + icon, it will make seeing the other sections easier.

- On the right-side of the page select the drop-down to “Don’t Enforce”



Properties

ICMPv4 flood Don't Enforce ▾

Attack Vector

○ Auto-Threshold Configuration
● Manual Configuration

Detection Threshold PPS:
Specify ▾ 10000

Detection Threshold Percent:
Specify ▾ 500

Rate/Leak Limit
Specify ▾ 100000

□ **Simulate Auto Threshold**

□ **Bad Actor Detection**

  - Apply the settings above for **TCP SYN flood** and **UDP Flood**., and then click **Update**.

- On the Jumpbox in the **Attacker** PuTTY window type (or copy and paste) the following:

```
# sudo su
# cd scripts
# ls
```

Note: Ignore the “unable to resolve host Attacker message”

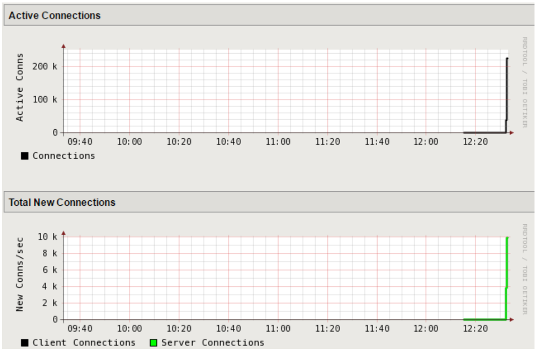
These are the different scripts we’ll be using during the exercises to simulate DoS attacks.

- Type (or copy and paste) the following commands:

```
for i in {1..10}; do ./icmpflood.sh; done
```

This script launches 1,000,000 ICMP requests and then repeats for a total of ten occurrences.

- View the `tcpdump` window and verify that ICMP attack traffic is reaching the back-end server.
- Let the attack run for about 15 seconds before moving on.
- In the Configuration Utility, open the **Statistics** > **Performance** > **Performance** page.
- View the Active Connections and Total New Connections charts.
- There is a drastic spike in active connections.



- View the Throughput (bits) and Throughput (packets) charts.

There is also a drastic spike in both bits per second and packets per second.

- Open the **Security** > **Event Logs** > **DoS** > **Network** > **Events** page.

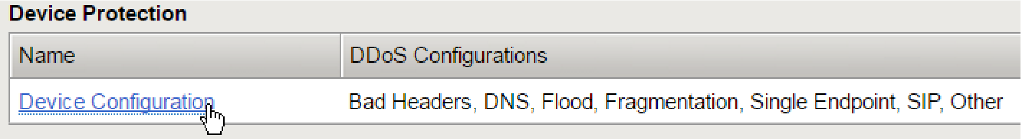
The log file is empty as we disabled device-level flood protection on BIG-IP DHD.

- On the Jumpbox Attacker shell slowly type **Ctrl + C** several times until back at the `scripts` prompt.

Task 2 – Re-enable Device-Level DHD DoS Protection

In this task you will re-configure **device-level** DoS protection, and then issue an ICMPv4 flood and review the results.

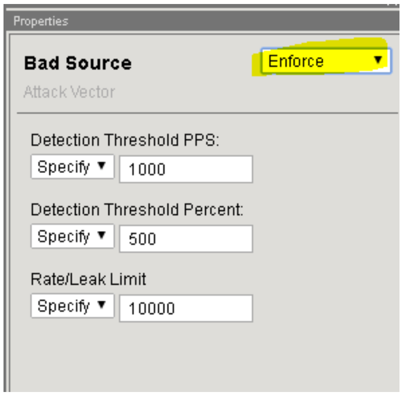
- In the Configuration Utility, in the **Device Protection** section click **Device Configuration.**



Device Protection

Name	DDoS Configurations
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other

- In the **Bad Headers** row click the + icon, and then click **Bad Source**.
- On the right-side of the page select the drop-down to "**Enforce**"



Properties

Bad Source Enforce ▼

Attack Vector

Detection Threshold PPS:

Specify ▼ 1000

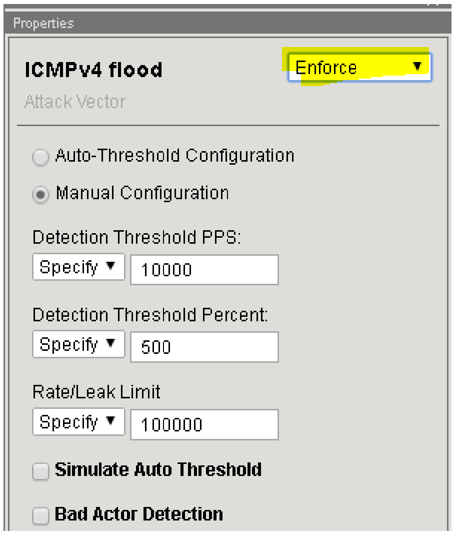
Detection Threshold Percent:

Specify ▼ 500

Rate/Leak Limit

Specify ▼ 10000

- In the **Flood** row click the + icon, and then click **ICMPv4** flood.
- On the right-side of the page select the drop-down to “**Enforce**”



Properties

ICMPv4 flood Enforce ▼

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS:

Specify ▼ 10000

Detection Threshold Percent:

Specify ▼ 500

Rate/Leak Limit

Specify ▼ 100000

□ **Simulate Auto Threshold**

□ **Bad Actor Detection**

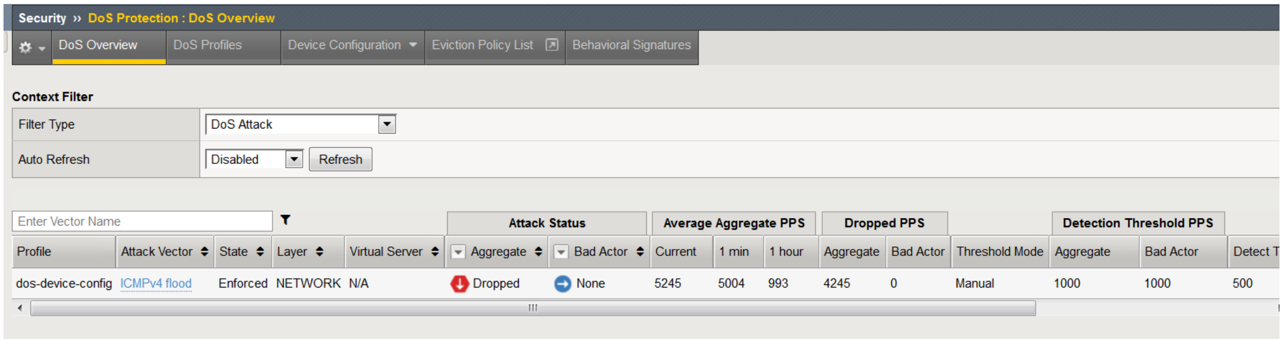
- Click **Update**.

Note: This returns the configuration back to factory supplied device level enforcement.

- On the Jumpbox in the **Attacker A** PuTTY window re-run the following command:

```
for i in {1..10}; do ./icmpflood.sh; done
```

- Let the attack run for about 15 seconds before moving on.
- In the Configuration Utility, open the **Security** > **Dos Protection** > **DoS Overview** > page
- You should see the attacks and statistics. Explore the sections



Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

Enter Vector Name

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS		
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect T
dos-device-config	ICMPv4 flood	Enforced	NETWORK	N/A	Dropped	None	5245	5004	993	4245	0	Manual	1000	1000	500

- In the Configuration Utility, open the **Security** > **Event Logs** > **DoS** > **Network** > **Events** page.

Note: You may need to refresh this page several times before the log files display.

- Sort the event by **Time** in descending order.

There are now log entries showing dropped packets.

- The DoS Source is **Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS**.
- The type is **ICMPv4 flood**.
- The action is **Drop**.
- On the Jumpbox Attacker shell slowly type **Ctrl + C** several times until back at the `scripts` prompt.

Reset the Device-Level ICMPv4 Flood Settings

- In the Configuration Utility, open the **DoS Protection** > **Quick Configuration** page and click **Device Configuration**.
- In the **Flood** row click the **+** icon, and then click **ICMPv4 flood**.
- On the right-side of the page configure using the following information, and then click **Update**.

Detection Threshold PPS	Infinite
Rate/Leak Limit	Infinite

Task 3 – Configure Protected Object-Level IPv4 Flood DHD DoS Protection

In this task you will configure object-level DoS IPv4 flood protection, and then issue an ICMPv4 flood and review the results.

- On the Protect Objects page, in the Protected Objects section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	ServerNet
IP Address	10.1.20.0/22
Port	*
Protocol	All Protocols
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	IPv4

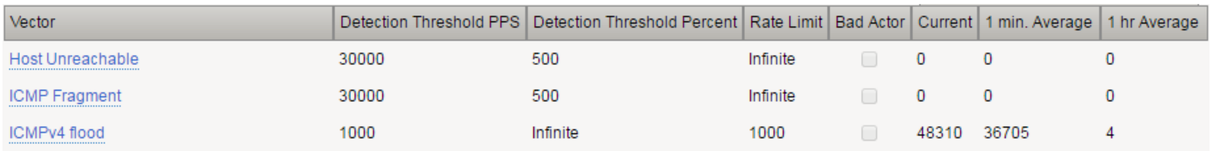
- In the **IPv4** row click the **+** icon, and then click **ICMPv4 flood**.
- On the right-side of the page configure using the following information, and then click **Create** at the bottom of the page.

Detection Threshold PPS	Specify: 1000
Detection Threshold Percent	Infinite
Rate/Leak Limit	Specify: 1000

- On the Jumpbox in the **Attacker A** PuTTY window re-run the following command:

```
for i in {1..10}; do ./icmpflood.sh; done
```

- Examine the `tcpdump` window to see if there are any ICMP packets hitting the back-end server.
- Let the attack run for about 30 seconds before moving on.
- In the Configuration Utility, click **DoS Protection > Quick Configuration** > **ServerNet**, and then in the **IPv4** row click the **+** icon.



Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
Host Unreachable	30000	500	Infinite	□	0	0	0
ICMP Fragment	30000	500	Infinite	□	0	0	0
ICMPv4 flood	1000	Infinite	1000	□	48310	36705	4

- Open the **Security > Event Logs > DoS > Network > Events** page.
- The DoS Source is **Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS**.
- The context column displays /**Common**/**ServerNet**, identifying this is protected object-level protection.
- The action is **Drop**.
- The difference between packets in per second and dropped packets is roughly 1000.
- On the Jumpbox slowly type **Ctrl + C** several times until back at the `scripts` prompt.
- In the BIG-IP PuTTY window type **Ctrl + C** to stop the tcpdump.

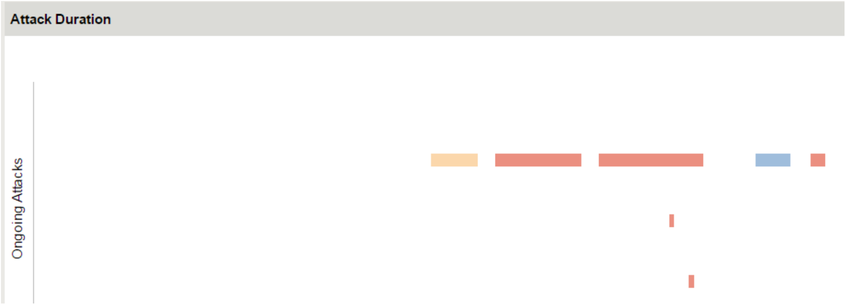
Task 4 – View the DoS Visibility Page

You can now use the new DoS Visibility page to view statistics about the DoS attacks you submitted during this exercise.

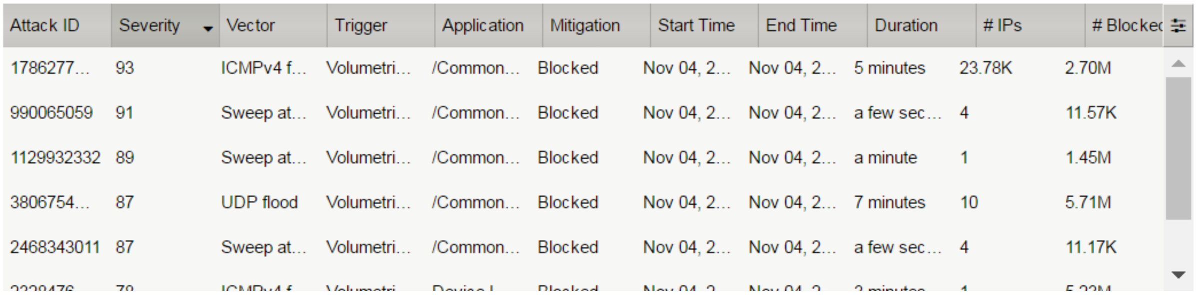
- Open the **Statistics > DoS Visibility** page.

> **Note:** It may take a couple of minutes for the correct data to display.

- In the **Attack Duration** window there are several attacks.



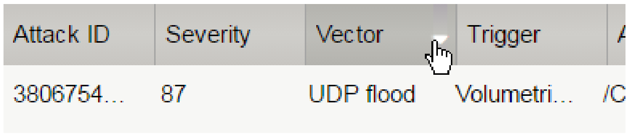
- Mouse over several of the attacks to get additional details of each attack.
- Scroll down in the left-side of the page to view the **Attacks** section.
- You can see the number of high, moderate, and low attacks in addition to the types of attacks (HTTP, DNS, Network) and the severity levels.
- View the details at the bottom of the **Attacks** section.



Attack ID	Severity	Vector	Trigger	Application	Mitigation	Start Time	End Time	Duration	# IPs	# Blocked
1786277…	93	ICMPv4 f…	Volumetri…	/Common…	Blocked	Nov 04, 2…	Nov 04, 2…	5 minutes	23.78K	2.70M
990065059	91	Sweep at…	Volumetri…	/Common…	Blocked	Nov 04, 2…	Nov 04, 2…	a few sec…	4	11.57K
1129932332	89	Sweep at…	Volumetri…	/Common…	Blocked	Nov 04, 2…	Nov 04, 2…	a minute	1	1.45M
3806754…	87	UDP flood	Volumetri…	/Common…	Blocked	Nov 04, 2…	Nov 04, 2…	7 minutes	10	5.71M
2468343011	87	Sweep at…	Volumetri…	/Common…	Blocked	Nov 04, 2…	Nov 04, 2…	a few sec…	4	11.17K
2229476…	78	ICMPv4 f…	Volumetri…	Device l…	Blocked	Nov 04, 2…	Nov 04, 2…	2 minutes	1	5.23M

This table displays details of each attack that has occurred.

- Sort this table by **Vector**.



Attack ID	Severity	Vector	Trigger	A
3806754…	87	UDP flood	Volumetri…	/C

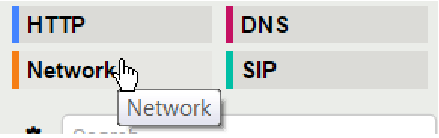
- Scroll down in the left-side of the page to view the **Virtual Servers** section.

You can see the details of device-wide attacks (**Device Level**) and protected object-level attacks (/**Common**/**ServerNet**).

- Scroll down in the left-side of the page to view the Countries section.
- View the details at the bottom of the **Countries** section.

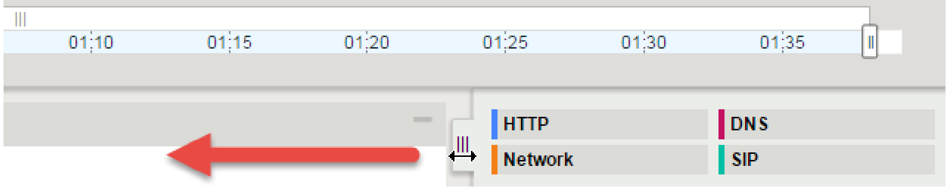
This table displays the attack details from each country.

- View the various widgets in the panel on the right-side of the page.
- Click **Network** to filter out only the network-level attacks (all the attacks so far have been network-level).



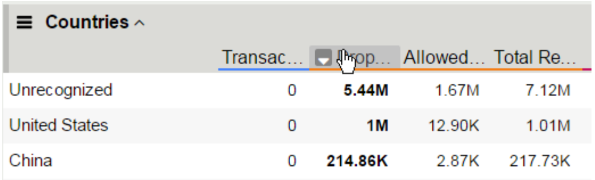
- If it's not already expanded, expand the **Virtual Servers** widget, and then select /**Common/ServerNet**.

- This filters the results to only attacks at this protected object-level. Notice the changes to the map on in the **Countries** section.
- Click /**Common**/**ServerNet** to remove the filter.
- Drag the resize handle on the right-side of the main window as far to the left as possible.



- Expand the **Vectors** widget, and then select **ICMPv4 flood**.
- Expand the **Client IP Addresses** widget.

  Question: How many client IP addresses contributed to this attack?
- Expand the **Countries** widget.
- Sort the countries by **Dropped Requests**.



≡ Countries ^

	Transac…	Drop…	Allowed…	Total Re…
Unrecognized	0	**5.44M**	1.67M	7.12M
United States	0	**1M**	12.90K	1.01M
China	0	**214.86K**	2.87K	217.73K

- Select **China**, and then view the changes to both the **Client IP Addresses** widget and the map.
- At the top of the page open the **Analysis** page.

Note: The requests are still filtered for the ICMPv4 flood results for China.

- Drag the resize handle on the as far to the right as possible.
- Examine the Avg Throughput (Bits per second) graph.
- Place your mouse over the peak in the graph.

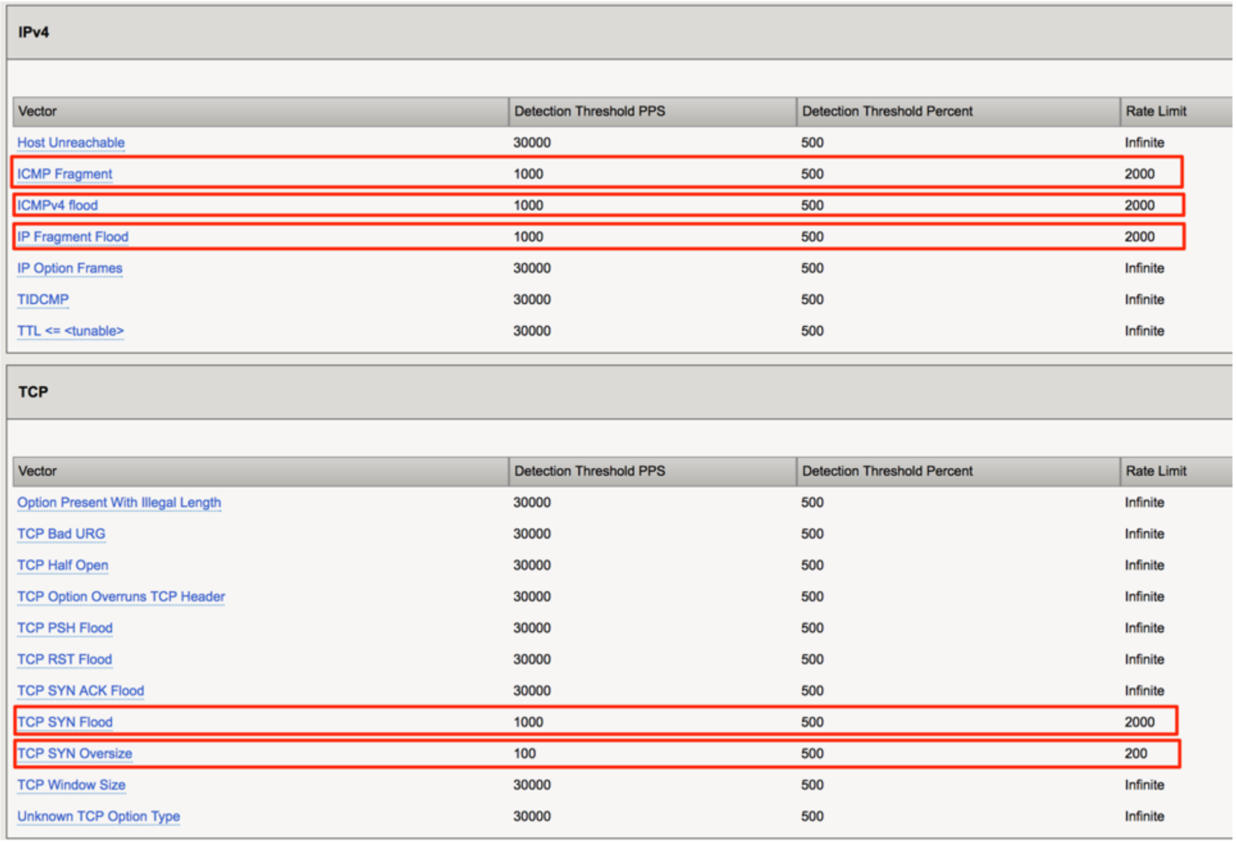
  Question: What is the **Average client in throughput** during the attack?
- Feel free to examine more of the **Dashboard** page and the **Analysis** page.

2.1.4 Lab 4 - Multi-vector Demo

In this simple demo you will launch a small number of network attacks and show the configuration, logging and reporting capabilities of the Hybrid Defender. The point of this demo is to provide context for a UI walkthrough with some live data.

Task 1 - Access DoS Quick Configuration and display the ServerNet protected object

This protected object is defending all ports/protocols for 10.1.20.0/24, which is the network behind the Hybrid Defender. Attacks will be launched at 10.1.20.12, which is an interface on the LAMP server. Verify that the following vectors are configured:



IPv4

Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Host Unreachable	30000	500	Infinite
ICMP Fragment	1000	500	2000
ICMPv4 flood	1000	500	2000
IP Fragment Flood	1000	500	2000
IP Option Frames	30000	500	Infinite
TIDCMP	30000	500	Infinite
TTL <= <tunable>	30000	500	Infinite

TCP

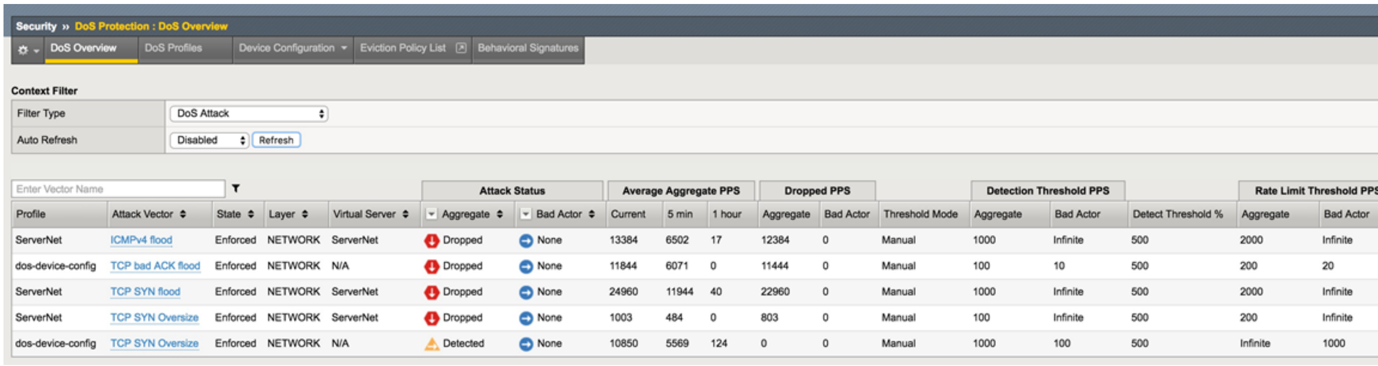
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Option Present With Illegal Length	30000	500	Infinite
TCP Bad URG	30000	500	Infinite
TCP Half Open	30000	500	Infinite
TCP Option Overruns TCP Header	30000	500	Infinite
TCP PSH Flood	30000	500	Infinite
TCP RST Flood	30000	500	Infinite
TCP SYN ACK Flood	30000	500	Infinite
TCP SYN Flood	1000	500	2000
TCP SYN Oversize	100	500	200
TCP Window Size	30000	500	Infinite
Unknown TCP Option Type	30000	500	Infinite

Launch the attacks and show the behavior

- Open the following tabs in the DHD UI:
- **DoS Protection->Quick Configuration->ServerNet**
- **Security->DoS Protection->DoS Overview** (leave the filter at default: 'DoS Attack')
- **Statistics->DoS Visibility**
- Access the Attacker System CLI and run the attack

```
# cd ~/scripts
# sudo bash
# ./multivector.sh
```

  – Click **Refresh** on the DoS Overview page. You will see some attacks mitigated by **Device Configuration** and some mitigated by the more specific settings on the **ServerNet Protected Object**.



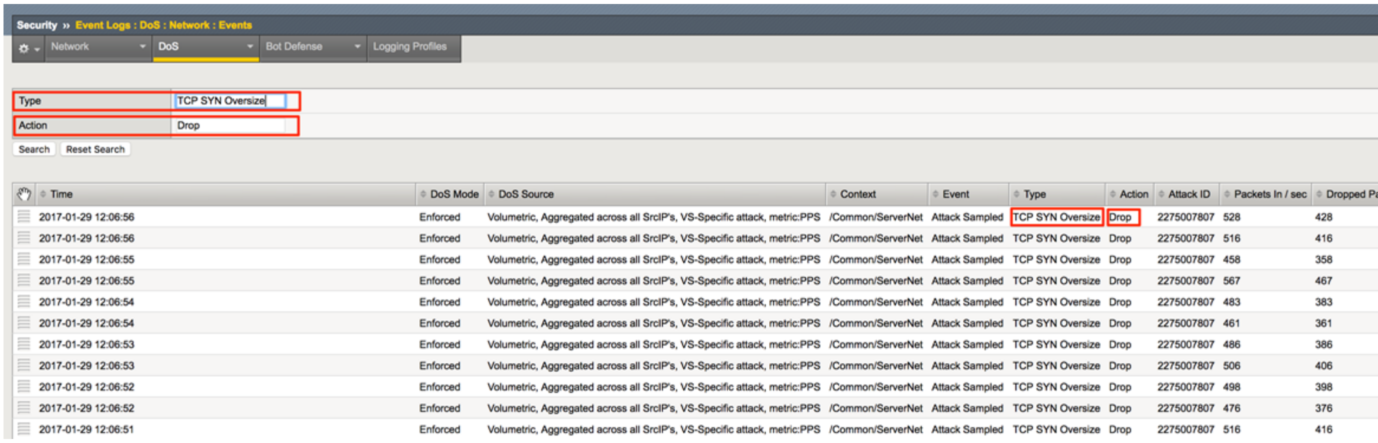
Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	5 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
ServerNet	ICMPv4 flood	Enforced	NETWORK	ServerNet	Dropped	None	13384	6502	17	12384	0	Manual	1000	Infinite	500	2000	Infinite
dos-device-config	TCP bad ACK flood	Enforced	NETWORK	N/A	Dropped	None	11844	6071	0	11444	0	Manual	100	10	500	200	20
ServerNet	TCP SYN flood	Enforced	NETWORK	ServerNet	Dropped	None	24960	11944	40	22960	0	Manual	1000	Infinite	500	2000	Infinite
ServerNet	TCP SYN Oversize	Enforced	NETWORK	ServerNet	Dropped	None	1003	484	0	803	0	Manual	100	Infinite	500	200	Infinite
dos-device-config	TCP SYN Oversize	Enforced	NETWORK	N/A	Detected	None	10850	5569	124	0	0	Manual	1000	100	500	Infinite	1000

Navigate to **Security->Event Logs->DoS->Network->Events**.

- Click on “custom search. . . ” link.
- Drag one of the values from the “Attack Type” column into the custom search builder. From the Action column, drag Drop into the search builder. Click “Search”.



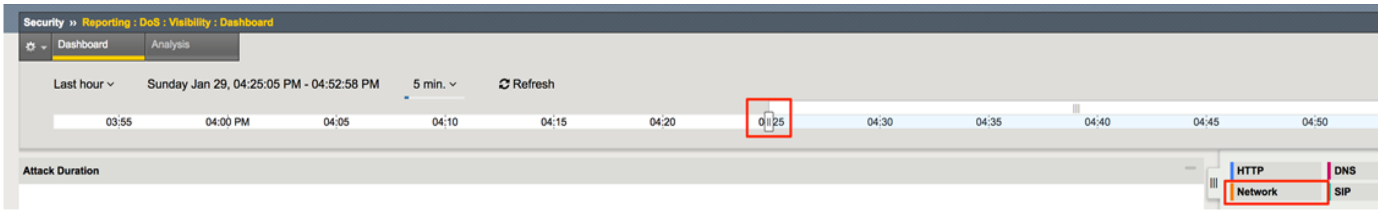
Type: TCP SYN Oversize
Action: Drop

Time	DoS Mode	DoS Source	Context	Event	Type	Action	Attack ID	Packets In / sec	Dropped Pa
2017-01-29 12:06:56	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	528	428
2017-01-29 12:06:56	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	516	416
2017-01-29 12:06:55	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	458	358
2017-01-29 12:06:55	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	567	467
2017-01-29 12:06:54	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	483	383
2017-01-29 12:06:54	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	461	361
2017-01-29 12:06:53	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	486	386
2017-01-29 12:06:53	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	506	406
2017-01-29 12:06:52	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	498	398
2017-01-29 12:06:52	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	476	376
2017-01-29 12:06:51	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	516	416

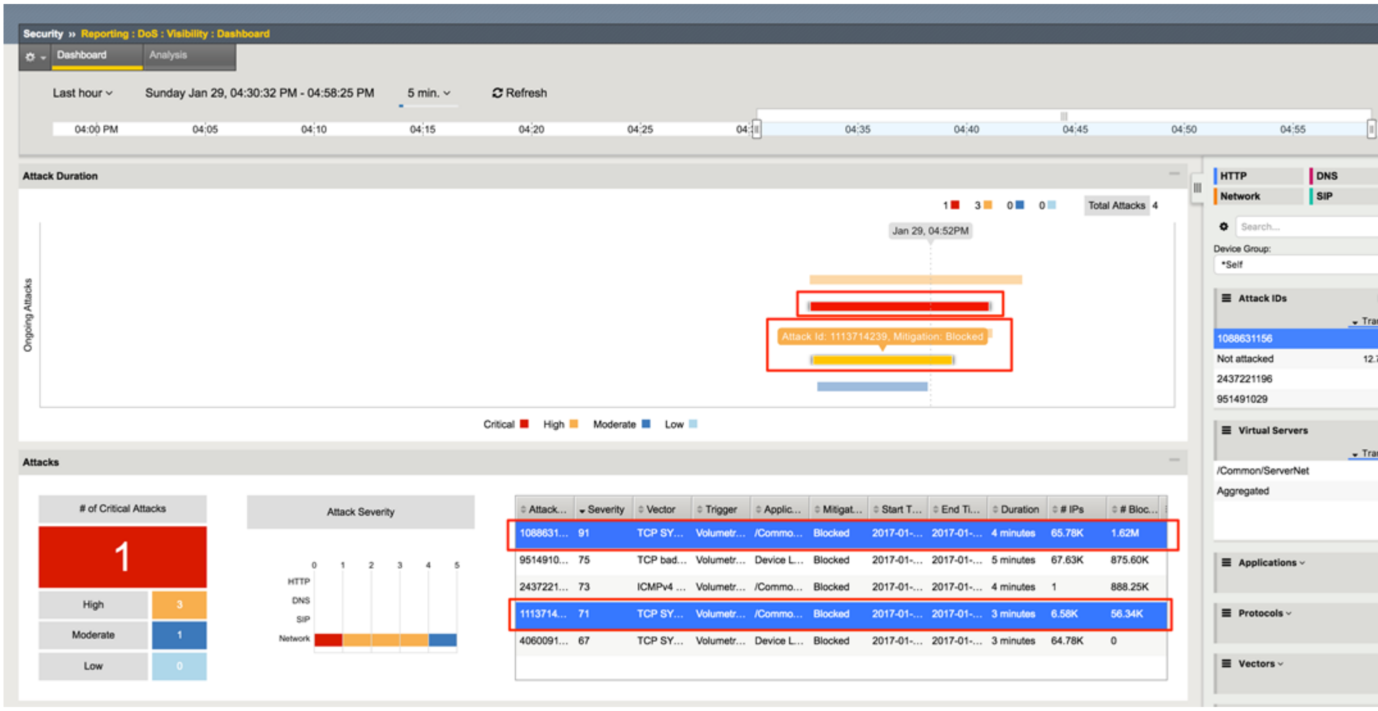
- Further explore the DoS Event logs as needed for your demo. For example, clear the search and identify the “Stop” and “Start” times for an attack, etc.
- In the Hybrid Defender WebUI, access the DoS Visibility reporting tool at **Statistics->DoS Visibility.**

Note: DoS Visibility is a reporting tool, not a real-time monitoring tool. Events are displayed, much like other AVR-based reporting, in 5 minute windows. Do not expect events to be shown here immediately after running an attack. Be aware of this timing when doing a demo. Quicker/real-time monitoring of on-going DoS attacks is best accomplished in the DoS Event Logs and DoS Overview areas of the WebUI

- You should see the attacks in the timeline and a variety of details in the windows. Use the slider to shorten the timeframe if needed, and click the Network filter, to focus on L4 activities.



Note: that you can select events from the timeline and see details about the attacks



Attack...	Severity	Vector	Trigger	Applic...	Mitigat...	Start T...	End Ti...	Duration	# IPs	# Bloc...
1088631...	91	TCP SY...	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	4 minutes	65.78K	1.62M
9514910...	75	TCP bad...	Volumetr...	Device L...	Blocked	2017-01-...	2017-01-...	5 minutes	67.63K	875.60K
2437221...	73	ICMPv4 ...	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	4 minutes	1	888.25K
1113714...	71	TCP SY...	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	3 minutes	6.58K	56.34K
4060091...	67	TCP SY...	Volumetr...	Device L...	Blocked	2017-01-...	2017-01-...	3 minutes	64.78K	0

- Log in to Silverline at https://portal.f5silverline.com.
- Navigate to **Monitor and Analyze > Stats > Hybrid Device**. Locate your device and explore the interface.

2.1.5 Lab 5 - Bad Actor Detection Demo

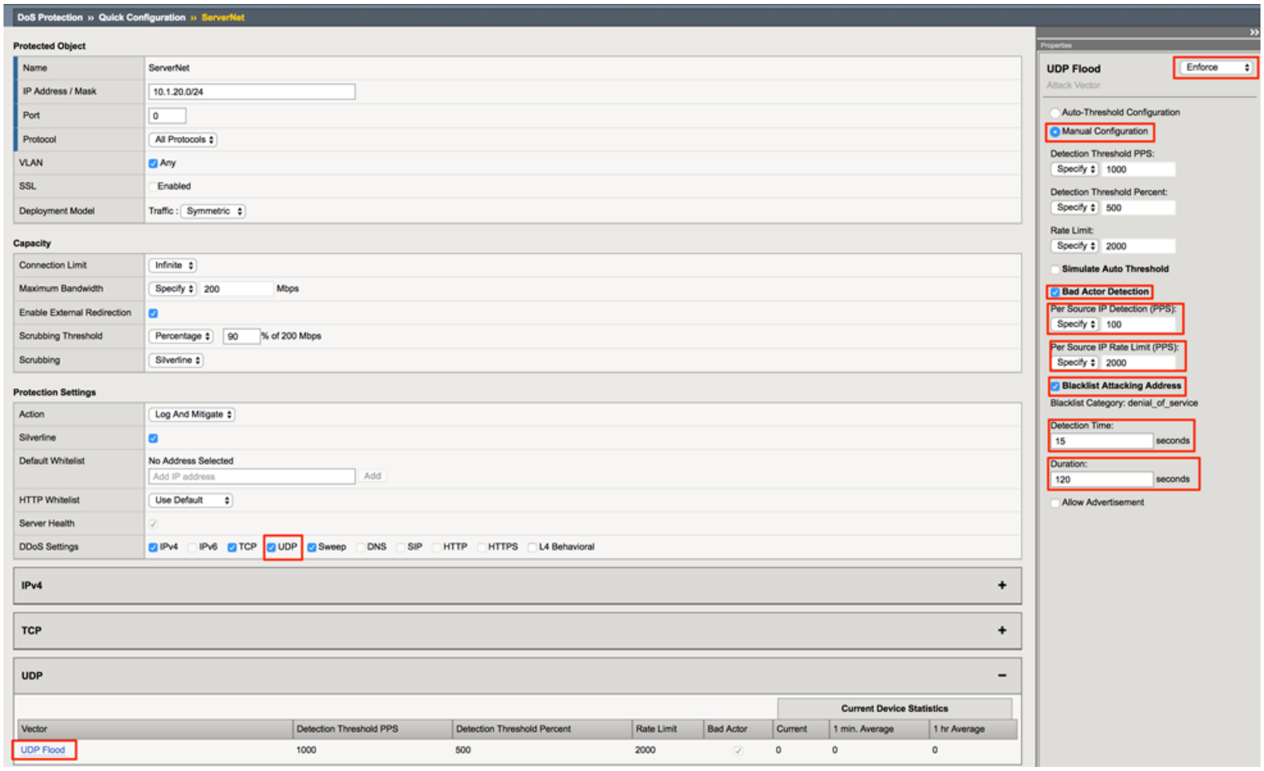
In this demo you will run an attack from specific IP addresses. The Hybrid Defender will be configured to perform bad actor detection, limit the attack on a per-IP basis with more aggressive thresholds and then, based on this detection, automatically blacklist the offending IP address adding them to the (hardware-accelerated) dynamic blacklist

Task 1 - Open the following tabs in the DHD UI:

- **DoS Protection->Quick Configuration->ServerNet**
- **Security->DoS Protection->DoS Overview** (leave filter at default: “DoS Attack”)
- **Statistics->DoS Visibility**
- **Security->Event Logs->Network->IP Intelligence**

Task 2 – Configure the following UDP Flood vectors for ServerNet:

- **DoS Protection->Quick Configuration->ServerNet**



DoS Protection » Quick Configuration » ServerNet

Protected Object

Name	ServerNet
IP Address / Mask	10.1.20.0/24
Port	0
Protocol	All Protocols
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric

Capacity

Connection Limit	Infinite
Maximum Bandwidth	Specify 200 Mbps
Enable External Redirection	☑
Scrubbing Threshold	Percentage 90 % of 200 Mbps
Scrubbing	Silverline

Protection Settings

Action	Log And Mitigate
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default
Server Health	✓
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP ☑ UDP ☑ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

IPv4 +

TCP +

UDP −

					Current Device Statistics		
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
UDP Flood	1000	500	2000	✓	0	0	0

Properties

UDP Flood Enforce

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS: Specify 1000

Detection Threshold Percent: Specify 500

Rate Limit: Specify 2000

□ Simulate Auto Threshold

☑ Bad Actor Detection

Per Source IP Detection (PPS): Specify 100

Per Source IP Rate Limit (PPS): Specify 2000

☑ Blacklist Attacking Address

Blacklist Category: denial_of_service

Detection Time: 15 seconds

Duration: 120 seconds

□ Allow Advertisement

- Access the Attacker system CLI and run the UDP flood attack:

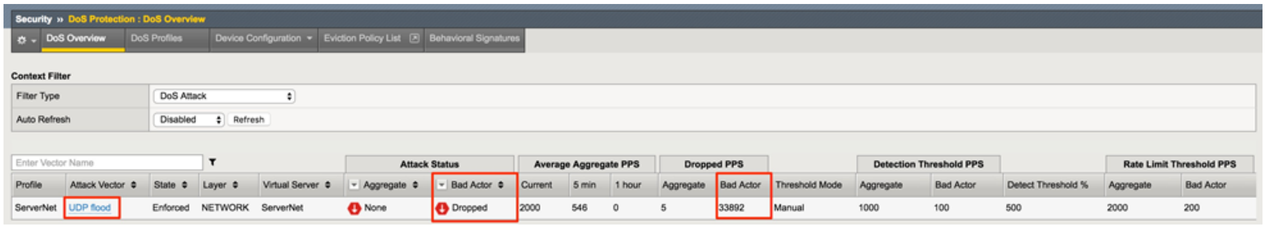
```
# sudo bash
# cd ~/scripts
# ./udp_flood.sh
```

From the menu, select '1' to start the attack

```
root@attacker-a:~/scripts# ./udp_flood.sh

1)Attack start
2)Attack end
3)Quit

# ?
```

Note: This attack is relatively short-lived. You can launch it again if the attack ends and you are not finished showing the various reports. Simply type '1' again, to re-run the attack

- In the Hybrid Defender UI, show the **Security > DoS >DoS Overview** page. Note the blocks by Bad Actor.



Security » DoS Protection : DoS Overview

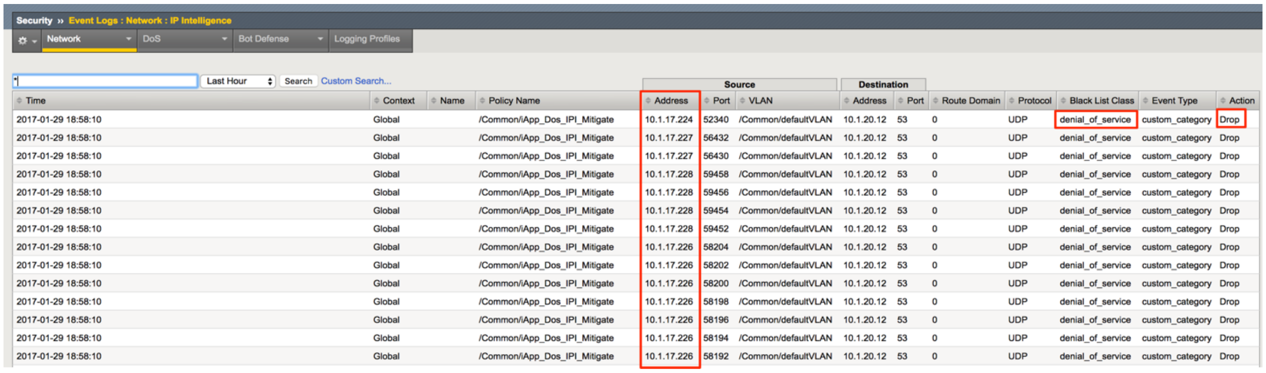
Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled Refresh

Enter Vector Name

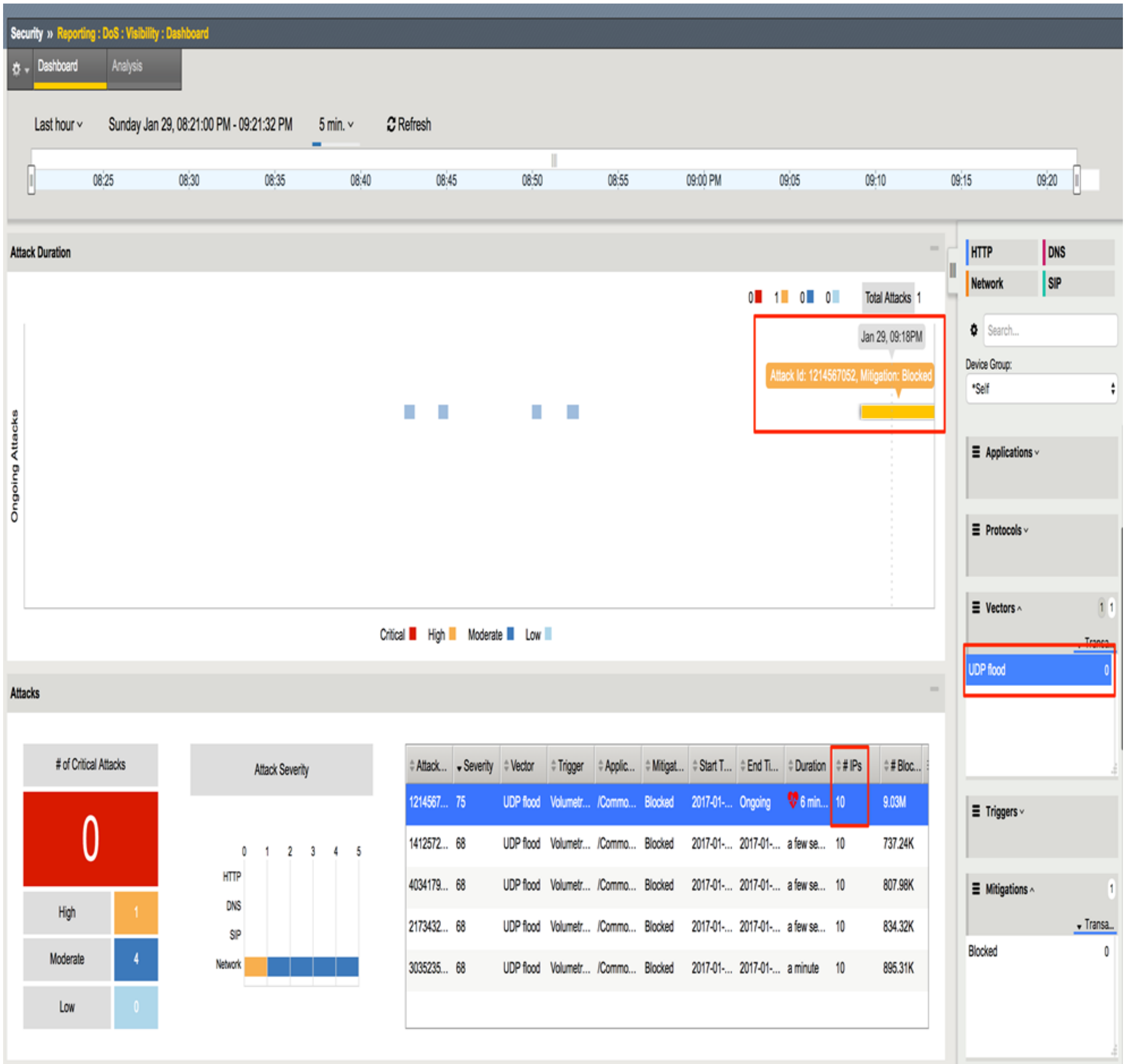
					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	5 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
ServerNet	UDP flood	Enforced	NETWORK	ServerNet	None	Dropped	2000	546	0	5	33892	Manual	1000	100	500	2000	200

- In the Hybrid Defender UI, show the **Security > Events > Network > IP Intelligence** Event Logs. Note the IP addresses that are being added to the denial_of_service blacklist.



				Source			Destination						
Time	Context	Name	Policy Name	Address	Port	VLAN	Address	Port	Route Domain	Protocol	Black List Class	Event Type	Action
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.224	52340	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.227	56432	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.227	56430	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59458	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59456	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59454	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59452	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58204	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58202	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58200	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58198	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58196	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58194	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58192	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop

- In the Hybrid Defender WebUI, show the **Statistics > DoS Visibility**. Expand the Vectors inspector and select UDP Flood. When it updates, select a flood from the timeline. Note in the Attacks panel the #IPs blocked is 10.



Attack...	Severity	Vector	Trigger	Applic...	Mitigat...	Start T...	End Ti...	Duration	# IPs	# Bloc...
1214567...	75	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	Ongoing	6 min...	10	9.03M
1412572...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a few se...	10	737.24K
4034179...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a few se...	10	807.98K
2173432...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a few se...	10	834.32K
3035235...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a minute	10	895.31K

From the menu, select ‘2’ to end the attack

or

```
# sudo bash
# killall -9 hping3
```

2.1.6 Lab 6 - Auto-threshold demo

This demo will simulate a newly configured **Protected Object** where the security administrator is unsure what values to assign to a few common vectors. Note that auto-thresholding is useful at both the **Device and Protected Object** levels.

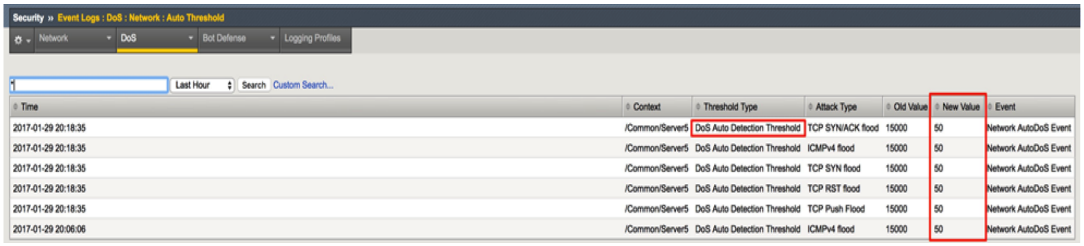
In the interest of having a repeatable demo in an environment where many different types of traffic are executed, we are focusing on the per-VS/per-PO auto-thresholding

Note: This demo may place significant stress on the demo environment. Due to the virtual environment limitations, this may make the DHD UI less responsive. This is unavoidable since for auto-thresholding to block the attack, the attck must be damaging enough to cause stress, which will push the CPU on the VE very high. Rememberthis is a virtual environment under high stress and that the Hybrid Defender appliances mitigate these attacks in dedicated hardware.

- Open the following tabs in the Hybrid Defender WebUI:
- **DoS Protection->Quick Configuration**
- **Security->DoS Protection->DoS Overview** (set filter to Virtual Server->Server5)
- **Security->Event Logs->DoS->Network->Auto Threshold**
- **Statistics->DoS Visibility**
- On the Good Client, if you have not already done so, start the network baselining

```
# cd ~/scripts
# sudo bash
# ./baseline\_l4.sh
```

- 3. In the Hybrid Defender UI, in **Quick Configuration**, select the Server5 Protected Object and verify that the IP and TCP vectors are all at default thresholds with auto-threshold disabled

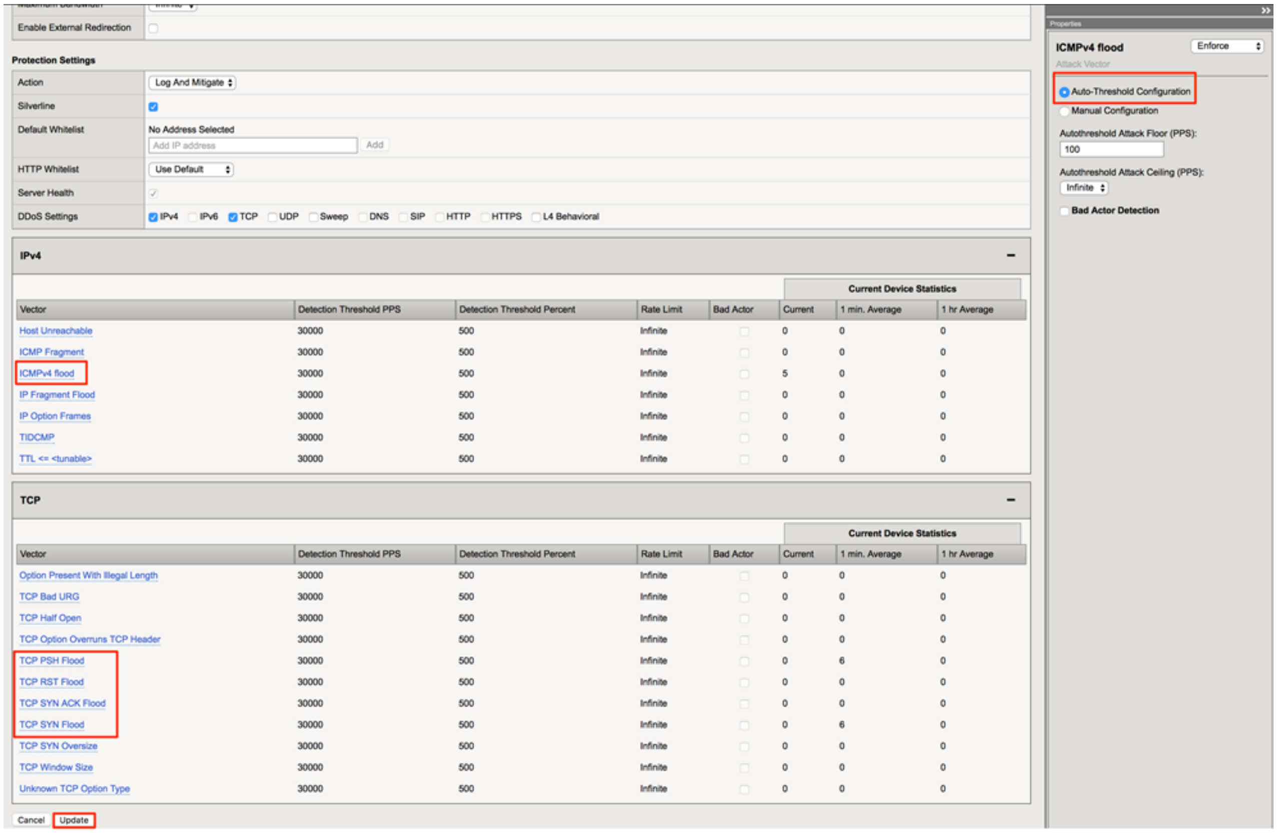


Time	Context	Threshold Type	Attack Type	Old Value	New Value	Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP SYN/ACK flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	ICMPv4 flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP SYN flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP RST flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP Push Flood	15000	50	Network AutoDoS Event
2017-01-29 20:06:06	/Common/Server5	DoS Auto Detection Threshold	ICMPv4 flood	15000	50	Network AutoDoS Event

- In the Hybrid Defender CLI, restart auto-thresholding

```
# cd ~/scripts
# ./autothreshold-reset.sh
```

- In the Hybrid Defender WebUI, in the Server5 Protected Object configuration, enable auto- thresholding for the following vectors: **ICMPv4 Flood, TCP SYN Flood, TCP Push Flood, TCP RST Flood, TCP SYN ACK** Flood by selecting each vector and clicking the Auto- Threshold Configuration radio button. When all vectors are configured, click **Update** at the bottom of the screen



Enable External Redirection	□

Protection Settings

Action	Log And Mitigate
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default
Server Health	✓
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

IPv4

					Current Device Statistics		
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
Host Unreachable	30000	500	Infinite	□	0	0	0
ICMP Fragment	30000	500	Infinite	□	0	0	0
ICMPv4 flood	30000	500	Infinite	□	5	0	0
IP Fragment Flood	30000	500	Infinite	□	0	0	0
IP Option Frames	30000	500	Infinite	□	0	0	0
TIDCMP	30000	500	Infinite	□	0	0	0
TTL <= <tunable>	30000	500	Infinite	□	0	0	0

TCP

					Current Device Statistics		
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
Option Present With Illegal Length	30000	500	Infinite	□	0	0	0
TCP Bad URG	30000	500	Infinite	□	0	0	0
TCP Half Open	30000	500	Infinite	□	0	0	0
TCP Option Overruns TCP Header	30000	500	Infinite	□	0	0	0
TCP PSH Flood	30000	500	Infinite	□	0	6	0
TCP RST Flood	30000	500	Infinite	□	0	0	0
TCP SYN ACK Flood	30000	500	Infinite	□	0	0	0
TCP SYN Flood	30000	500	Infinite	□	0	6	0
TCP SYN Oversize	30000	500	Infinite	□	0	0	0
TCP Window Size	30000	500	Infinite	□	0	0	0
Unknown TCP Option Type	30000	500	Infinite	□	0	0	0

Properties

ICMPv4 flood Enforce

Attack Vector

● Auto-Threshold Configuration

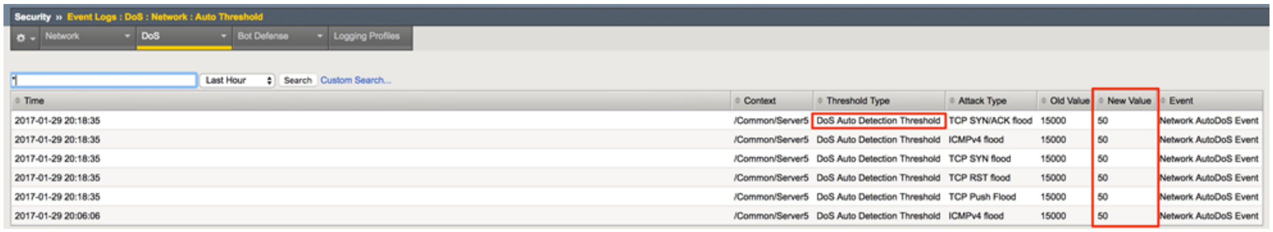
○ Manual Configuration

Autothreshold Attack Floor (PPS): 100

Autothreshold Attack Ceiling (PPS): Infinite

□ **Bad Actor Detection**

- In the Hybrid Defender WebUI, show the Auto Threshold event log (**Security->Event Logs->Dos->Network->Auto Threshold).**



Security » Event Logs : DoS : Network : Auto Threshold

Time	Context	Threshold Type	Attack Type	Old Value	New Value	Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP SYN/ACK flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	ICMPv4 flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP SYN flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP RST flood	15000	50	Network AutoDoS Event
2017-01-29 20:18:35	/Common/Server5	DoS Auto Detection Threshold	TCP Push Flood	15000	50	Network AutoDoS Event
2017-01-29 20:06:06	/Common/Server5	DoS Auto Detection Threshold	ICMPv4 flood	15000	50	Network AutoDoS Event

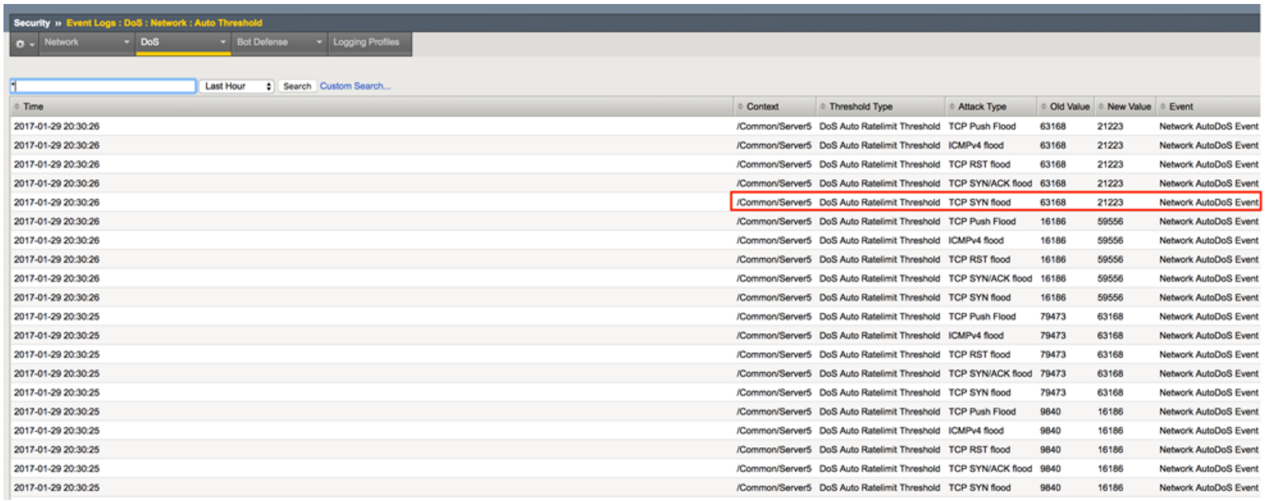
The system is updating the detection thresholds. With auto-thresholding, the system adjusts the detection thresholds based on observed traffic patterns. However, mitigation rate limits are always dynamic based on detected system or protected object stress. If anomalous levels of traffic are running, but there is no stress, the Hybrid Defender will generate alerts but will not block traffic. Under stress, the rate limits are automatically created and adjusted dynamically

- Let's create some stress with a SYN Flood attack. In the Attacker CLI start the auto- threshold SYN flood

```
# cd ~/scripts
# sudo bash
# ./autot\_flood.sh
```

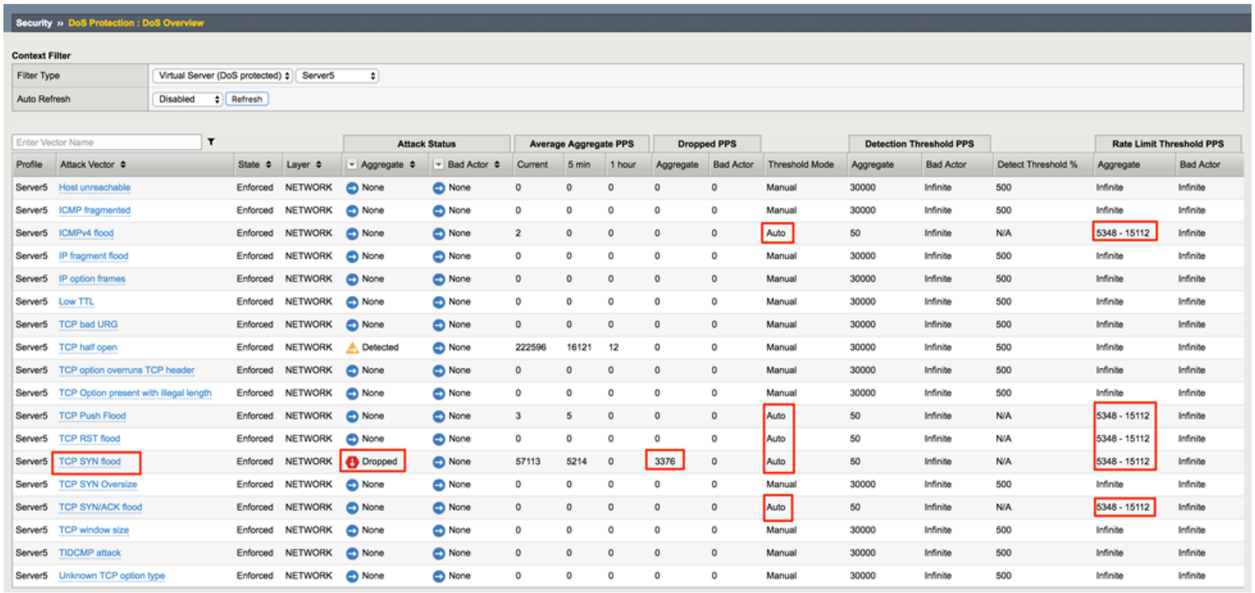
This is a long duration attack. You can terminate it with ctrl-C when finished.

- In the Hybrid Defender WebUI, show the Auto Threshold event log. Now you will see that Rate limits are being automatically set and adjusted to mitigate the flood attack



Time	Context	Threshold Type	Attack Type	Old Value	New Value	Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	63168	21223	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	63168	21223	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	63168	21223	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	63168	21223	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	63168	21223	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	16186	59556	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	16186	59556	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	16186	59556	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	16186	59556	Network AutoDoS Event
2017-01-29 20:30:26	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	16186	59556	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	79473	63168	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	79473	63168	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	79473	63168	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	79473	63168	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	79473	63168	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	9840	16186	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	9840	16186	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	9840	16186	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	9840	16186	Network AutoDoS Event
2017-01-29 20:30:25	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	9840	16186	Network AutoDoS Event

- In the Hybrid Defender WebUI, show the **Security > DoS > DoS Overview** page. Note that the SYN Flood attack is being mitigated and the rate limit thresholds for each of the auto-threshold vectors have been adjusted based on stress, including vectors that are not detecting or blocking an attack

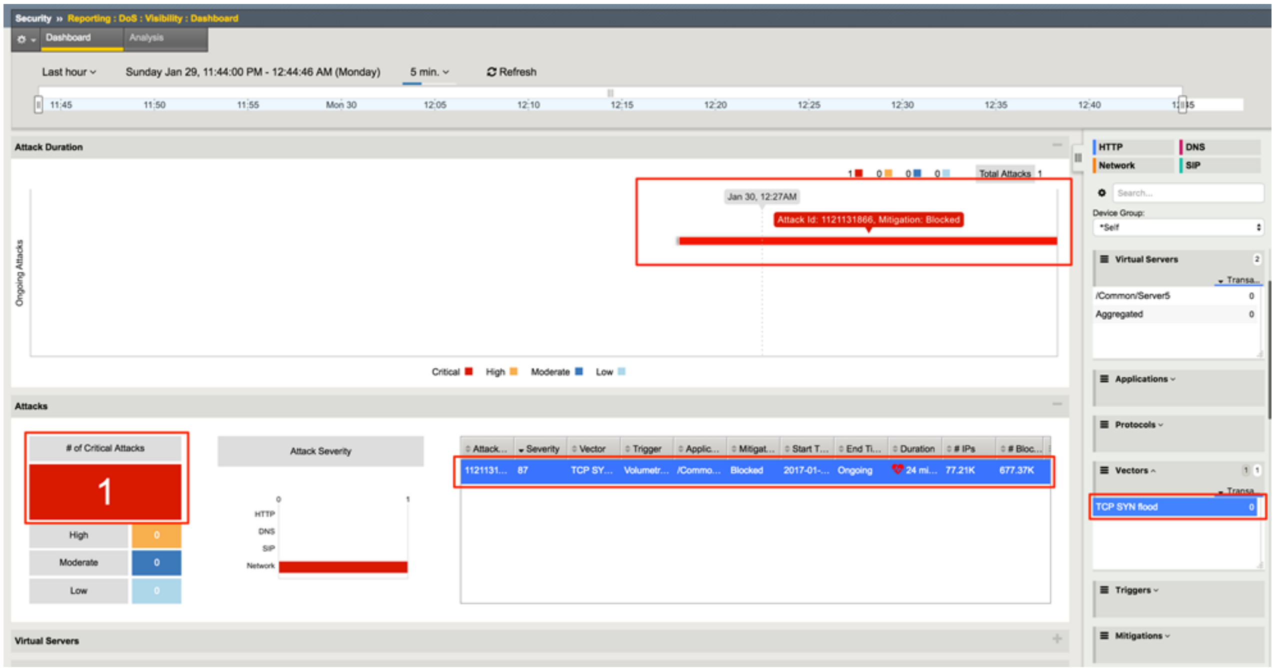


Context Filter

Filter Type	Virtual Server (DoS protected) Server5
Auto Refresh	Disabled

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	5 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
Server5	Host unreachable	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	ICMP fragmented	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	ICMPv4 flood	Enforced	NETWORK	None	None	2	0	0	0	0	Auto	50	Infinite	N/A	5348 - 15112	Infinite
Server5	IP fragment flood	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	IP option frames	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	Low TTL	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP bad URG	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP half open	Enforced	NETWORK	⚠ Detected	None	222596	16121	12	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP option overruns TCP header	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP Option present with illegal length	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP Push Flood	Enforced	NETWORK	None	None	3	5	0	0	0	Auto	50	Infinite	N/A	5348 - 15112	Infinite
Server5	TCP RST flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	50	Infinite	N/A	5348 - 15112	Infinite
Server5	TCP SYN flood	Enforced	NETWORK	Dropped	None	57113	5214	0	3376	0	Auto	50	Infinite	N/A	5348 - 15112	Infinite
Server5	TCP SYN Oversize	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP SYN/ACK flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	50	Infinite	N/A	5348 - 15112	Infinite
Server5	TCP window size	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TIDCMP attack	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	Unknown TCP option type	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite

- Terminate the attack in the Attacker CLI with ctrl-C
- After the attack has ended, in the Hybrid Defender WebUI, show the **DoS Visibility** page. Under **Vectors**, select **TCP SYN Flood**. Identify the Critical attack and show the details



Security » Reporting : DoS : Visibility : Dashboard

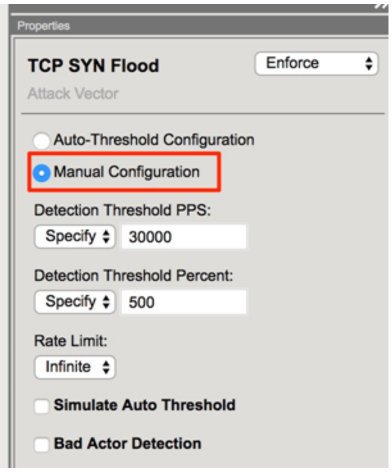
Last hour · Sunday Jan 29, 11:44:00 PM - 12:44:46 AM (Monday) · 5 min.

Attack Id: 1121131866, Mitigation: Blocked

Attack...	Severity	Vector	Trigger	Applic...	Mitigat...	Start T...	End Ti...	Duration	# IPs	# Bloc...
1121131...	87	TCP SY...	Volumetr...	/Commo...	Blocked	2017-01-...	Ongoing	24 mi...	77.21K	677.37K

# of Critical Attacks	1
High	0
Moderate	0
Low	0

- Clean-up. On the Attacker CLI, if the attack is still running be certain to end it with ctrl-C.
- Clean-up. For repeatability, it is necessary to disable the auto-thresholding for the ICMPv4 Flood, TCP RST Flood, TCP Push Flood, TCP SYN ACK Flood and TCP SYN Flood vectors on the Server5 protected object



Properties

TCP SYN Flood · Enforce

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS: Specify 30000

Detection Threshold Percent: Specify 500

Rate Limit: Infinite

□ Simulate Auto Threshold

□ Bad Actor Detection

- Clean-up. After disabling auto-thresholding, clear the learning on the Hybrid Defender CLI with

```
# cd ~/scripts
# ./autothreshold-reset.sh
```

2.1.7 Learn More

F5 DDoS Education

Web based training and product information

- Product Training https://university.f5.com/

- DDoS Protection Reference Architecture
- DDoS Protection Recommended Best Practices
- ***F5 DDoS Hybrid Defender overview and user guide***

***Silverline DDoS Education ***

Web based training and product information

- Product Training https://university.f5.com/

Onboarding Tech. Notes on f5.

3 Class2: Intermediate DDoS Protection

This class covers the following topics:

- Topics here

3.1 DDoS Hybrid Defender Setup

In this module you will learn how to complete the initial setup of F5 Networks DDoS Hybrid Defender

3.1.1 Lab 1 – DDoS Hybrid Defender Setup

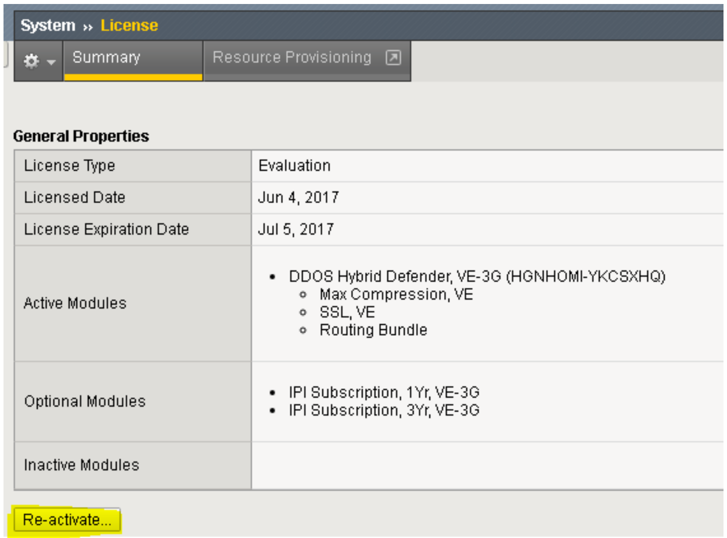
Task 1 – BIG-IP Herculon Hybrid Defender Licensing and Provisioning

Note: When you first power up a F5 DHD device you would go through the steps of Licensing and Provisioning. We have assigned the management IP, hostname, NTP and DNS servers. You will be re-activating the license using a new license key.

Note: For Silverline device registration to function properly there must be some specific considerations. The BIG-IP system must have a unique device ID, which is comprised of attributes like Base MAC and registration key. Hence we are re-licensing the device as all student instances are spun up using the same license.

Use a web browser (Chrome in incognito mode) to log into the WebUI of your DHD at https://10.1.1.245 . or use the bookmarked shortcut. Accept the SSL warning and proceed to connect.

- Username : admin
- Password : f5DEMOs4u
- Click **System>>License** and Click Re-activate

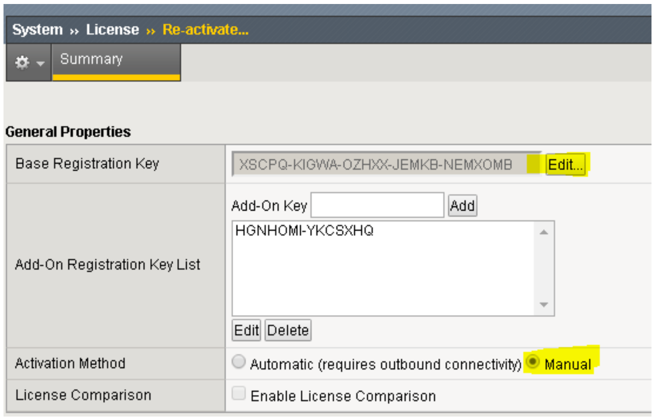


System » License

General Properties

License Type	Evaluation
Licensed Date	Jun 4, 2017
License Expiration Date	Jul 5, 2017
Active Modules	• DDOS Hybrid Defender, VE-3G (HGNHOMI-YKCSXHQ) ∘ Max Compression, VE ∘ SSL, VE ∘ Routing Bundle
Optional Modules	• IPI Subscription, 1Yr, VE-3G • IPI Subscription, 3Yr, VE-3G
Inactive Modules	

- Click **Edit** button, replace the existing key by entering your student license key. Select the "Manual" radio button and Click Next.

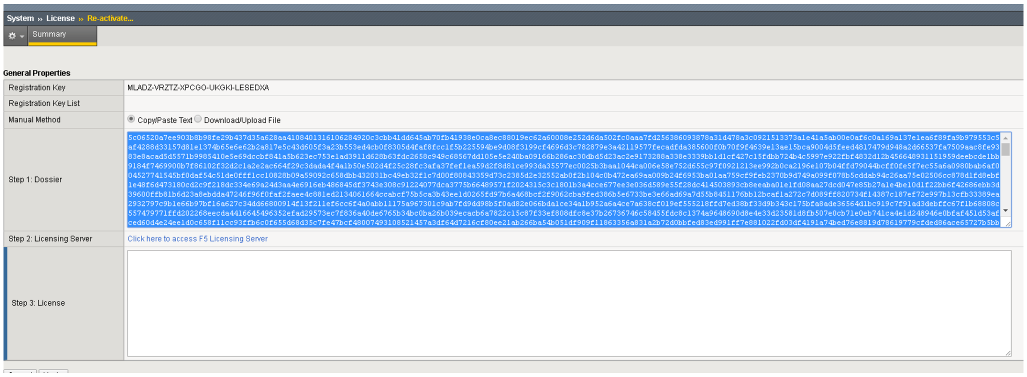


System » License » Re-activate...

General Properties

Base Registration Key	XSCPQ-KIGWA-OZHXX-JEMKB-NEMXOMB Edit...
Add-On Registration Key List	Add-On Key [ ] Add HGNHOMI-YKCSXHQ Edit Delete
Activation Method	○ Automatic (requires outbound connectivity) ● Manual
License Comparison	□ Enable License Comparison

- Select all in the Dossier frame and copy. Click on "Click here to access F5 Licensing Server"



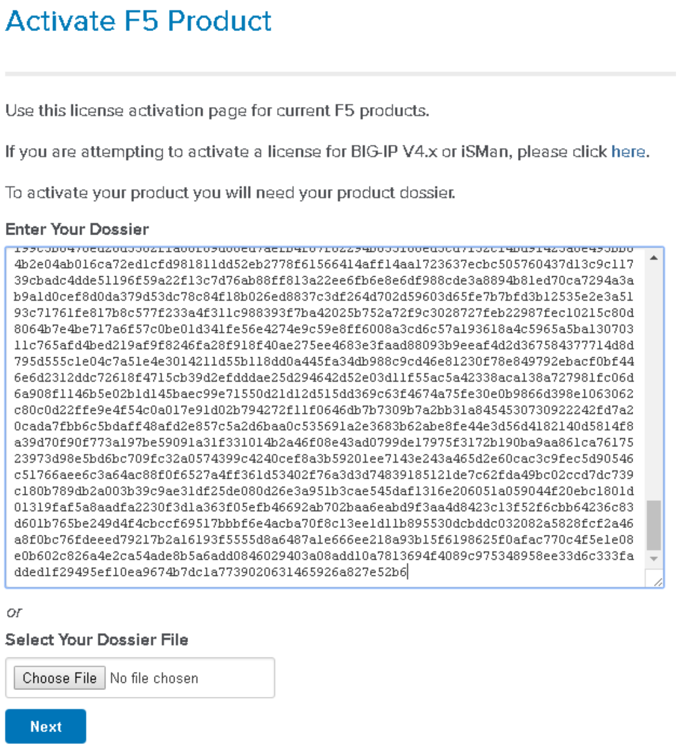
System » License » Re-activate...

General Properties

Registration Key	MLADZ-VRZTZ-XPCGO-UKGKI-LESEDXA
Registration Key List	
Manual Method	● Copy/Paste Text ○ Download/Upload File
Step 1: Dossier	(see below)
Step 2: Licensing Server	Click here to access F5 Licensing Server
Step 3: License	

```
5c06520a7ee903b8b98fe29b437d35a628aa4108401316106284920c3cbb41dd645ab70fb41938e0ca8ec88019ec62a60008e252d6da502fc0aaa7fd256386093878a31d478a3c0921513373a1e41a5ab00e0af6c0a169a137e1ea6f89fa9b979553c5
af4288d33157d81e1374b65e6e62b2a817e5c43d605f3a23b553ed4cb0f8305d4faf8fcc1f5b225594be9d08f3199cf4696d3c782879e3a42119577fecadfda385600f0b70f9f4639e13ae15bca9004d5feed4817479d948a2d66537fa7509aac8fe93
83e8acad5d5571b9985410e5e69dccbf841a5b623ec753e1ad3911d628b63fdc2658c949c68567dd105e5e240ba09166b286ac30dbd5d23ac2e9173288a338e3339bb1d1cf427c15fdbb724b4c5997e922fbf4832d12b456648931151959deebcde1bb
9184f7469900b7f86102f32d2c1a2e2ac664f29c3dada4f4a1b50e502d4f25c28fc3afa37fef1ea59d2f8d81ce993da35577ec0025b3baa1044ca006e58e752d655c97f0921213ee992b0ca2196e107b04ffd79044bcff0fe5f7ec55a6a0980bab6af0
04527741545bf0daf54c51de0fff1cc10828b09a59092c658dbb432031bc49eb32f1c7d00f80843359d73c2385d2e32552ab0f2b104c0b472ea69aa009b24f6953ba01aa759cf9feb2370b9d749a099f078b5cddab94c26aa75e02506cc878d1fd8ebf
1e48f6d473180cd2c9f218dc334e69a24d3aa4e6916eb486845df3743e308c91224077dca3775b66489571f2024315c3c1801b3a4cce677ee3e036d589e55f28dc414503893cb8eeaba01e1fd08aa27dcd047e85b27a1e4be10d1f22bb6f42686ebb3d
39600ffb81b6d23a8ebdda47246f96f0faf2faee4c881ed2134061664ccabcf75b5ca3b43ee1d0265fd97b6a468bcf2f9062cba9fed386b5e6733be3e66ad69a7d55b8451176bb12bcaf1a272c7d089ff820734f14387c187ef72e997b13cfb33389ea
2932797c9b1e66b97bf16a627c34dd66800914f13f211ef6cc6f4a0abb11175a967301c9ab7fd9dd98b5f0ad82e066bda1ce34a1b952a6a4ce7a638cf019ef555218ffd7ed38bf33d9b343c175bfa8ade36564d1bc919c7f91ad3debffc67f1b68808c
557479771ffd202268eecda4416645496352efad29573ec7f836a40de6765b34bc0ba26b039ecacb6a7822c15c87f33ef808dfc8e37b26736746c58455fdc8c1374a9648690d8e4e33d23581d8fb507e0cb71e0eb741ca4e1d248946e0bfaf451d53af
ced60d4e24ee1d0c658f11cc93ffb6c0f655d68d35c7fe47bcf48007493108521457a3df64d7216cf80ee21ab266ba54b051df909f11863356a831a2b72d0bbfed83ed991ff7e881022fd03df4191a74bed76e8819d78619779cfded86ace65727b5bb
```

- You will be taken to the F5 Activation Site. Enter your Dossier that you copied in the step above and click next. Accept User Legal Agreement - Check box to agree to terms of license and click next.



Activate F5 Product

Use this license activation page for current F5 products.

If you are attempting to activate a license for BIG-IP V4.x or iSMan, please click here.

To activate your product you will need your product dossier.

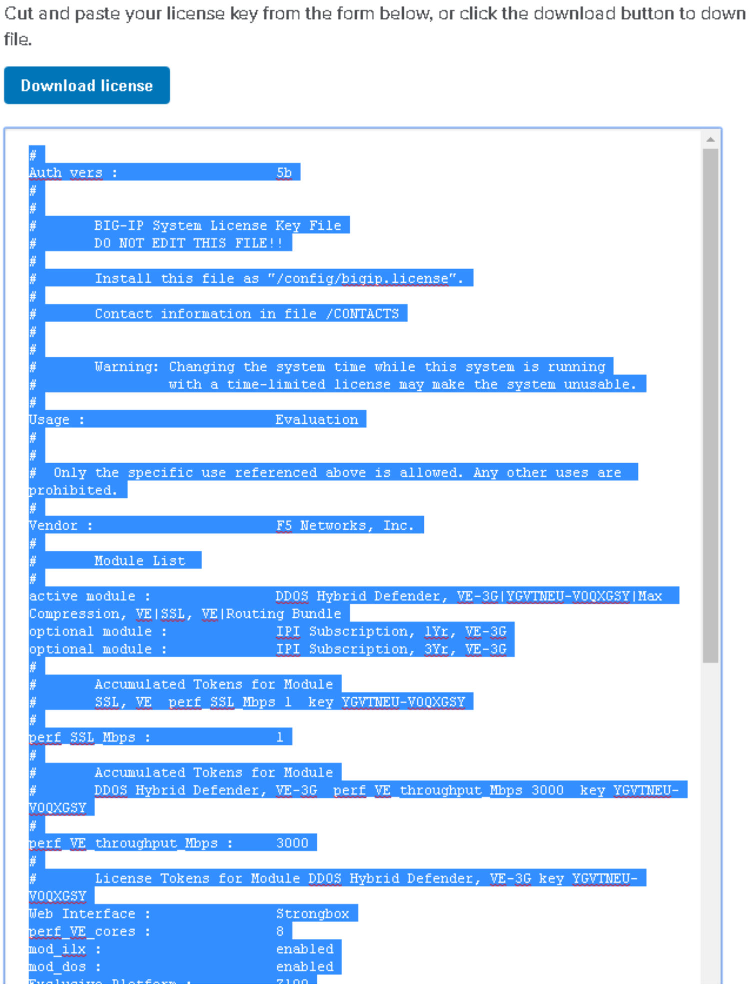
Enter Your Dossier

```
4b2e04ab016ca72ed1cfd981811dd52eb2778f61566414aff14aa1723637ecbc505760437d13c9c117
39cbadc4dde51196f59a22f13c7d76ab88ff813a22ee6fb6e8e6df988cde3a8894b81ed70ca7294a3a
b9a1d0cef8d0da379d53dc78c84f18b026ed8837c3df264d702d59603d65fe7b7bfd3b12535e2e3a51
93c71761fe817b8c577f233a4f311c988393f7ba42025b752a72f9c3028727feb22987fec10215c80d
8064b7e4be717a6f57c0be01d341fe56e4274e9c59e8ff6008a3cd6c57a193618a4c5965a5ba130703
11c765afd4bed219af9f8246fa28f918f40ae275ee4683e3faad88093b9eeaf4d2d367584377714d8d
795d555c1e04c7a51e4e3014211d55b118dd0a445fa34db988c9cd46e81230f78e849792ebacf0bf44
6e6d2312ddc72618f4715cb39d2efdddae25d294642d52e03d11f55ac5a42338aca138a727981fc06d
6a908f1146b5e02b1d145baec99e71550d21d12d515dd369c63f4674a75fe30e0b9866d398e1063062
c80c0d22ffe9e4f54c0a017e91d02b794272f11f0646db7b7309b7a2bb31a8454530730922242fd7a2
0cada7fbb6c5bdaff48afd2e857c5a2d6baa0c535691a2e3683b62abe8fe44e3d56d4182140d5814f8
a39d70f90f773a197be59091a31f331014b2a46f08e43ad0799de17975f3172b190ba9aa861ca76175
23973d98e5bd6bc709fc32a0574399c4240cef8a3b59201ee7143e243a465d2e60cac3c9fec5d90546
c51766aee6c3a64ac88f0f6527a4ff361d53402f76a3d3d74839185121de7c62fda49bc02ccd7dc739
c180b789db2a003b39c9ae31df25de080d26e3a951b3cae545daf1316e206051a059044f20ebc1801d
01319faf5a8aadfa2230f3d1a363f05efb46692ab702baa6eabd9f3aa4d8423c13f52f6cbb64236c83
d601b765be249d4f4cbccf69517bbbf6e4acba70f8c13ee1d11b895530dcbddc032082a5828fcf2a46
a8f0bc76fdeeed79217b2a16193f5555d8a6487a1e666ee218a93b15f6198625f0afac770c4f5e1e08
e0b602c826a4e2ca54ade8b5a6add0846029403a08add10a7813694f4089c975348958ee33d6c333fa
dded1f29495ef10ea9674b7dc1a7739020631465926a827e52b6
```

or

Select Your Dossier File

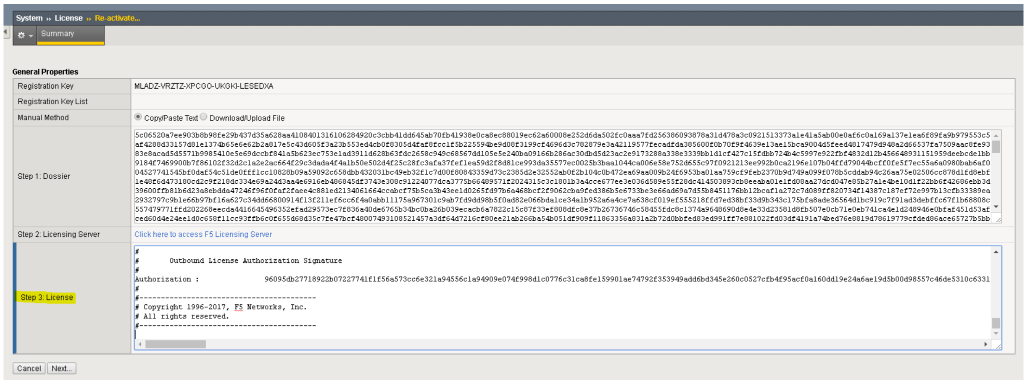
- Select Everything the License frame and copy it.



Cut and paste your license key from the form below, or click the download button to down file.

```
#
Auth vers :                        5b
#
#
#        BIG-IP System License Key File
#        DO NOT EDIT THIS FILE!!
#
#        Install this file as "/config/bigip.license".
#
#        Contact information in file /CONTACTS
#
#
#        Warning: Changing the system time while this system is running
#                 with a time-limited license may make the system unusable.
#
Usage :                            Evaluation
#
#
#   Only the specific use referenced above is allowed. Any other uses are
prohibited.
#
Vendor :                           F5 Networks, Inc.
#
#        Module List
#
active module :                    DDOS Hybrid Defender, VE-3G|YGVTNEU-VOQXGSY|Max
Compression, VE|SSL, VE|Routing Bundle
optional module :                  IPI Subscription, 1Yr, VE-3G
optional module :                  IPI Subscription, 3Yr, VE-3G
#
#        Accumulated Tokens for Module
#        SSL, VE  perf_SSL_Mbps 1  key YGVTNEU-VOQXGSY
#
perf_SSL_Mbps :                    1
#
#        Accumulated Tokens for Module
#        DDOS Hybrid Defender, VE-3G  perf_VE_throughput_Mbps 3000  key YGVTNEU-
VOQXGSY
#
perf_VE_throughput_Mbps :          3000
#
#        License Tokens for Module DDOS Hybrid Defender, VE-3G key YGVTNEU-
VOQXGSY
Web Interface :                    Strongbox
perf_VE_cores :                    8
mod_ilx :                          enabled
mod_dos :                          enabled
Exclusive Platform :               7100
```

- Go back to your F5 DHD management and paste the contents copied from above into Step 3: License and Click Next.



System » License » Re-activate...

General Properties

Registration Key: MLADZ-VRZTZ-XPCGO-UKGKI-LESEDXA

Registration Key List

Manual Method: ● Copy/Paste Text ○ Download/Upload File

Step 1: Dossier

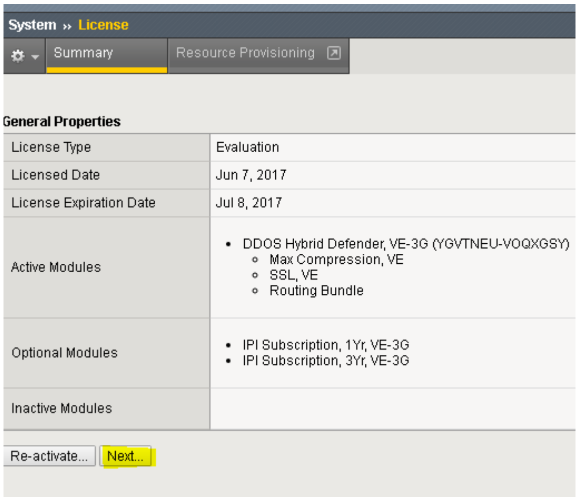
```
5c06520a7ee903b8b98fe29b437d35a628aa4108401316106284920c3cbb41dd645ab70fb41938e0ca8ec88019ec62a60008e252d6da502fc0aaa7fd256386093878a31d478a3c0921513373a1e41a5ab00e0af6c0a169a137e1ea6f89fa9b979553c5
af4288d33157d81e1374b65e6e62b2a817e5c43d605f3a23b553ed4cb0f8305d4faf8fcc1f5b225594be9d08f3199cf4696d3c782879e3a42119577fecadfda385600f0b70f9f4639e13ae15bca9004d5feed4817479d948a2d66537fa7509aac8fe93
83e8acad5d5571b9985410e5e69dccbf841a5b623ec753e1ad3911d628b63fdc2658c949c68567dd105e5e240ba09166b286ac30dbd5d23ac2e9173288a338e3339bb1d1cf427c15fdbb724b4c5997e922fbf4832d12b456648931151959deebcde1bb
9184f7469900b7f86102f32d2c1a2e2ac664f29c3dada4f4a1b50e502d4f25c28fc3afa37fef1ea59d2f8d81ce993da35577ec0025b3baa1044ca006e58e752d655c97f0921213ee992b0ca2196e107b04ffd79044bcff0fe5f7ec55a6a0980bab6af0
04527741545bf0daf54c51de0fff1cc10828b09a59092c658dbb432031bc49eb32f1c7d00f80843359d73c2385d2e32552ab0f2b104c0b472ea69aa009b24f6953ba01aa759cf9feb2370b9d749a099f078b5cddab94c26aa75e02506cc878d1fd8ebf
1e48f6d473180cd2c9f218dc334e69a24d3aa4e6916eb486845df3743e308c91224077dca3775b66489571f2024315c3c1801b3a4cce677ee3e036d589e55f28dc414503893cb8eeaba01e1fd08aa27dcd047e85b27a1e4be10d1f22bb6f42686ebb3d
39600ffb81b6d23a8ebdda47246f96f0faf2faee4c881ed2134061664ccabcf75b5ca3b43ee1d0265fd97b6a468bcf2f9062cba9fed386b5e6733be3e66ad69a7d55b8451176bb12bcaf1a272c7d089ff820734f14387c187ef72e997b13cfb33389ea
2932797c9b1e66b97bf16a627c34dd66800914f13f211ef6cc6f4a0abb11175a967301c9ab7fd9dd98b5f0ad82e066bda1ce34a1b952a6a4ce7a638cf019ef555218ffd7ed38bf33d9b343c175bfa8ade36564d1bc919c7f91ad3debffc67f1b68808c
557479771ffd202268eecda4416645496352efad29573ec7f836a40de6765b34bc0ba26b039ecacb6a7822c15c87f33ef808dfc8e37b26736746c58455fdc8c1374a9648690d8e4e33d23581d8fb507e0cb71e0eb741ca4e1d248946e0bfaf451d53af
ced60d4e24ee1d0c658f11cc93ffb6c0f655d68d35c7fe47bcf48007493108521457a3df64d7216cf80ee21ab266ba54b051df909f11863356a831a2b72d0bbfed83ed991ff7e881022fd03df4191a74bed76e8819d78619779cfded86ace65727b5bb
```

Step 2: Licensing Server: Click here to access F5 Licensing Server

Step 3: License

```
#
#        Outbound License Authorization Signature
#
Authorization :              96095db27718922b07227741f1f56a573cc6e321a94556c1a94909e074f998d1c0776c31ca8fe159901ae74792f353949add6bd345e260c0527cfb4f95acf0a160dd19e24a6ae19d5b00d98557c46de5310c6331
#
#----------------------------------------
# Copyright 1996-2017, F5 Networks, Inc.
# All rights reserved.
#----------------------------------------
```

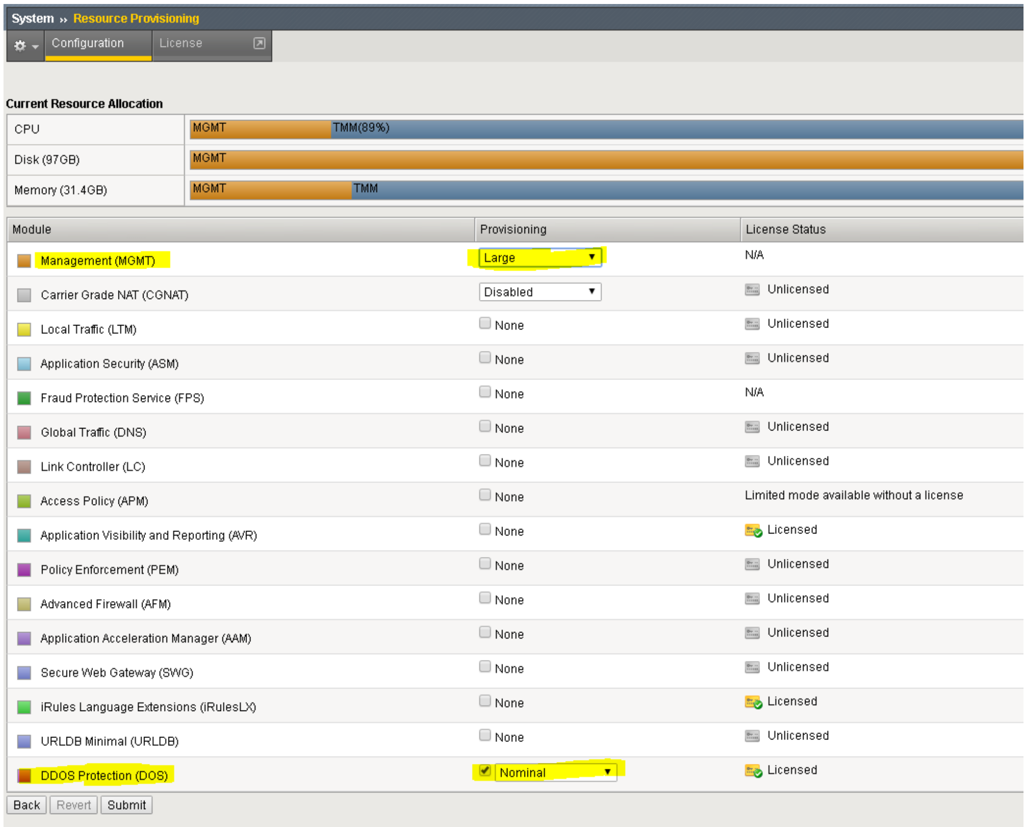
- The bigip will restart daemons and a window will pop up indicating system configuration has changed. Please wait for it to reconnect and click Continue. Your device is now licensed. Click Next.



General Properties

License Type	Evaluation
Licensed Date	Jun 7, 2017
License Expiration Date	Jul 8, 2017
Active Modules	• DDOS Hybrid Defender, VE-3G (YGVTNEU-VOQXGSY) ∘ Max Compression, VE ∘ SSL, VE ∘ Routing Bundle
Optional Modules	• IPI Subscription, 1Yr, VE-3G • IPI Subscription, 3Yr, VE-3G
Inactive Modules	

- On the Resource Provisioning page validate that Management and DDOS Protection are provisioned.
- Click Submit once.



Current Resource Allocation

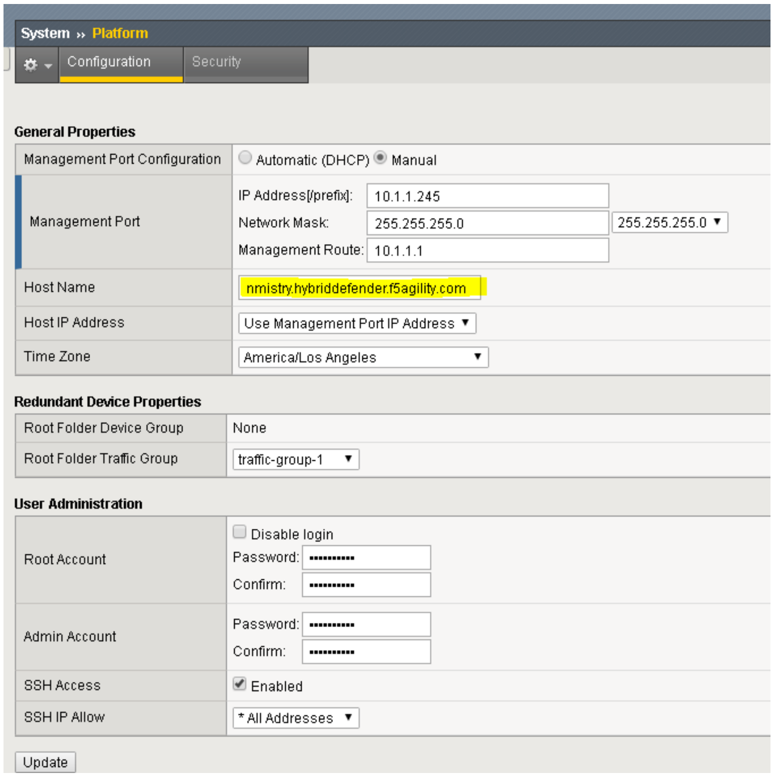
CPU	MGMT TMM(89%)
Disk (97GB)	MGMT
Memory (31.4GB)	MGMT TMM

Module	Provisioning	License Status
Management (MGMT)	Large	N/A
Carrier Grade NAT (CGNAT)	Disabled	Unlicensed
Local Traffic (LTM)	☐ None	Unlicensed
Application Security (ASM)	☐ None	Unlicensed
Fraud Protection Service (FPS)	☐ None	N/A
Global Traffic (DNS)	☐ None	Unlicensed
Link Controller (LC)	☐ None	Unlicensed
Access Policy (APM)	☐ None	Limited mode available without a license
Application Visibility and Reporting (AVR)	☐ None	Licensed
Policy Enforcement (PEM)	☐ None	Unlicensed
Advanced Firewall (AFM)	☐ None	Unlicensed
Application Acceleration Manager (AAM)	☐ None	Unlicensed
Secure Web Gateway (SWG)	☐ None	Unlicensed
iRules Language Extensions (iRulesLX)	☐ None	Licensed
URLDB Minimal (URLDB)	☐ None	Unlicensed
DDOS Protection (DOS)	☑ Nominal	Licensed

Note: The above task ensures that you are using a purpose built DDoS Hybrid Defender. If you are familiar with other F5 Modules/Technology that you have used in the past, you will notice that we have none of those provisioned.

Task 2 – BIG-IP Herculon Hybrid Defender Initial Setup

- Click **System>>Platform**
- Change the hostname to **<yourfirstinitiallastname>.hybriddefender.f5agility.com**. For example, John Smith would register as **jsmith.hybriddefender.f5agility.com**. This is needed so that we can register your DHD to Silverline and uniquely identify it. Click Update.



General Properties

Management Port Configuration	○ Automatic (DHCP) ● Manual
Management Port	IP Address[/prefix]: 10.1.1.245 Network Mask: 255.255.255.0 255.255.255.0 Management Route: 10.1.1.1
Host Name	nmistry.hybriddefender.f5agility.com
Host IP Address	Use Management Port IP Address
Time Zone	America/Los Angeles

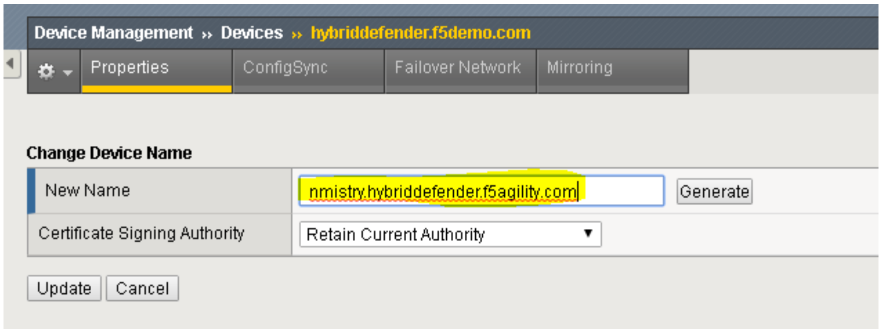
Redundant Device Properties

Root Folder Device Group	None
Root Folder Traffic Group	traffic-group-1

User Administration

Root Account	□ Disable login Password: •••••••••• Confirm: ••••••••••
Admin Account	Password: •••••••••• Confirm: ••••••••••
SSH Access	☑ Enabled
SSH IP Allow	* All Addresses

- Click **Device Management>>Devices** select the device and then click "Change Device Name…". Update the device name to match the hostname you have chosen and click Update



Change Device Name

New Name	nmistry.hybriddefender.f5agility.com
Certificate Signing Authority	Retain Current Authority

- Use Putty Shortcut to ssh to the F5 DHD and login as: root password: f5DEMOs4u

- From the Hybrid Defender shell, restart services with:

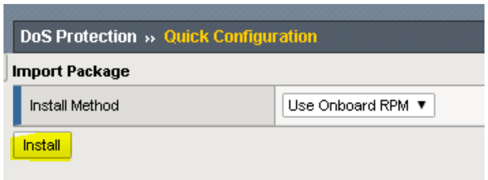
```
# bigstart restart
```

Note: Be patient as services are restarting. The DHD will change state to INOPERATIVE and then to Active. You can check in the ssh window when the prompt changes.

- Click **System>>Configuration>>Device>>NTP** and review that NTP server is configured
- Click **System>>Configuration>>Device>>DNS** and review that DNS server lookup is configured

DDoS Hybrid Defender Configuration

- In the BIG-IP Configuration Utility, open the **DoS Protection>>Quick Configuration** page. Click Install. This installs the onboard package for quick configuration of DDoS Hybrid Defense

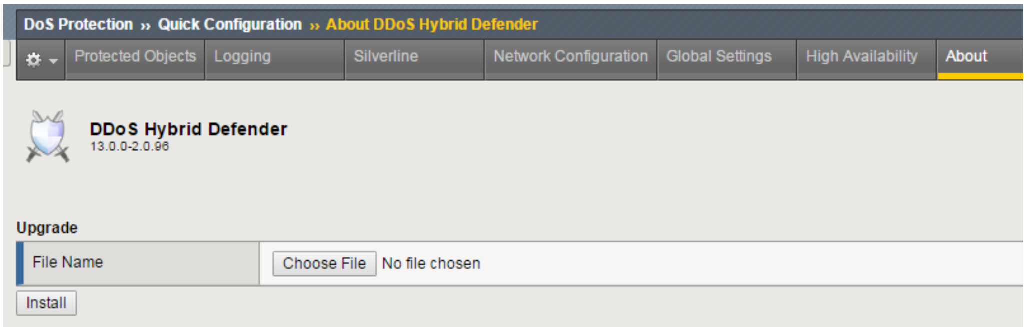


DoS Protection » Quick Configuration

Import Package

Install Method: Use Onboard RPM

- Once the installation is completed. Open the **About** page.
- This page displays the current version of DDoS Hybrid Defender (DHD). You use this page to install and update the iApp LX version for DHD.



DoS Protection » Quick Configuration » About DDoS Hybrid Defender

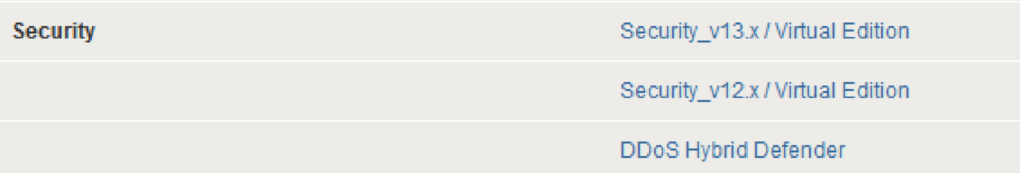
DDoS Hybrid Defender
13.0.0-2.0.96

Upgrade

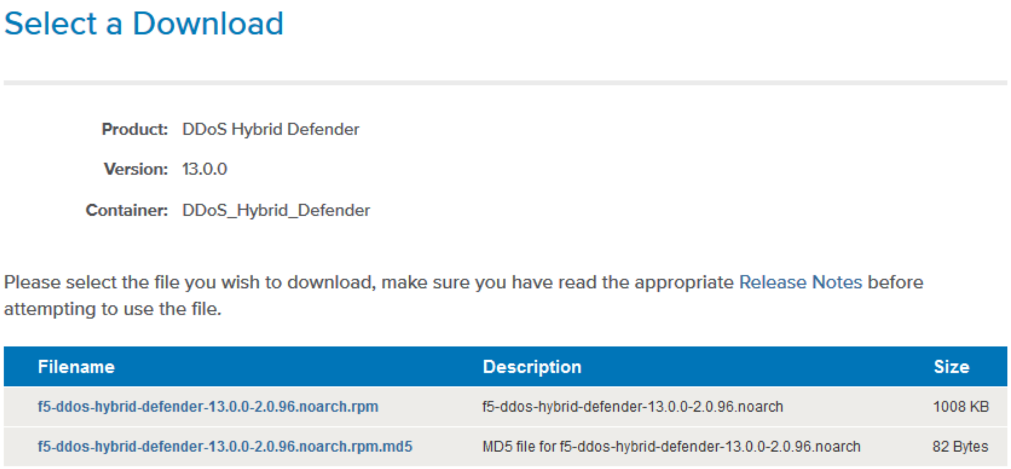
File Name: No file chosen

The System is installed with the latest version of the iApp LX. The below steps are for future reference on how to obtain the latest iApp LX and use the above step to install. Do not download and install during the Agility labs.

- Newer versions of iApp LX packages are made available on the **F5 downloads** site under Security>>DDoS Hybrid Defender.



Security	Security_v13.x / Virtual Edition
	Security_v12.x / Virtual Edition
	DDoS Hybrid Defender



Select a Download

Product: DDoS Hybrid Defender

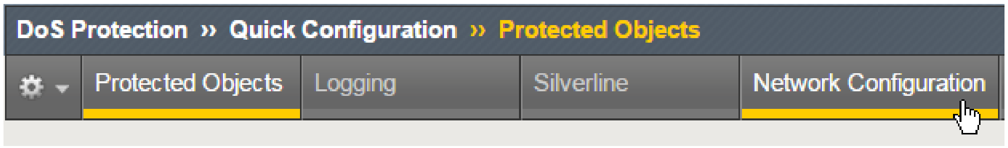
Version: 13.0.0

Container: DDoS_Hybrid_Defender

Please select the file you wish to download, make sure you have read the appropriate Release Notes before attempting to use the file.

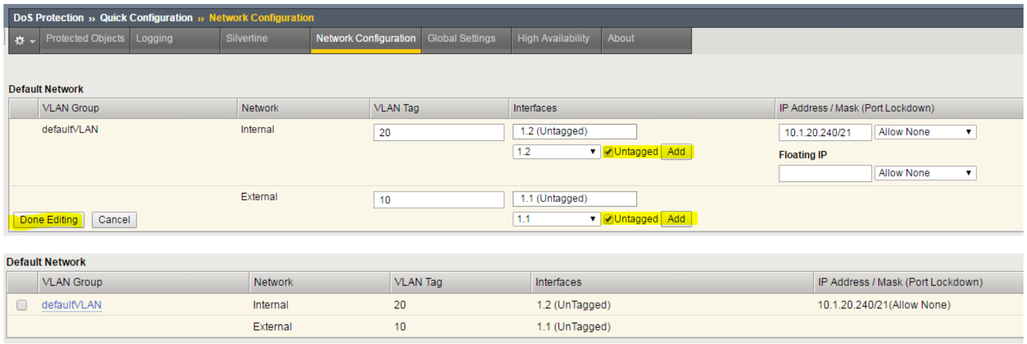
Filename	Description	Size
f5-ddos-hybrid-defender-13.0.0-2.0.96.noarch.rpm	f5-ddos-hybrid-defender-13.0.0-2.0.96.noarch	1008 KB
f5-ddos-hybrid-defender-13.0.0-2.0.96.noarch.rpm.md5	MD5 file for f5-ddos-hybrid-defender-13.0.0-2.0.96.noarch	82 Bytes

- Open the **Network Configuration** page



- In the **Default Network** section click **defaultVLAN**.
- Configure the VLANs using following information, and then click Done Editing. Make sure to Click "Add"

Internal: VLAN Tag	20
Internal: Interfaces	1.2 (Untagged checked) (**Click Add)**
Internal: IP Address / Mask	10.1.20.240/21
External: VLAN Tag	10
External: Interfaces	1.1 (Untagged checked) **(Click Add)**



Default Network

	VLAN Group	Network	VLAN Tag	Interfaces	IP Address / Mask (Port Lockdown)
	defaultVLAN	Internal	20	1.2 (Untagged) 1.2 ▾ ☑Untagged Add	10.1.20.240/21 Allow None ▾ Floating IP Allow None ▾
		External	10	1.1 (Untagged) 1.1 ▾ ☑Untagged Add	

Default Network

	VLAN Group	Network	VLAN Tag	Interfaces	IP Address / Mask (Port Lockdown)
□	defaultVLAN	Internal	20	1.2 (UnTagged)	10.1.20.240/21(Allow None)
		External	10	1.1 (UnTagged)	

- Click **UPDATE**.
- Open the **Network>>VLANs>>VLAN Groups** page and click **defaultVLAN**.

A transparent L2 configuration consistent with recommended practices for most deployments was automatically created.

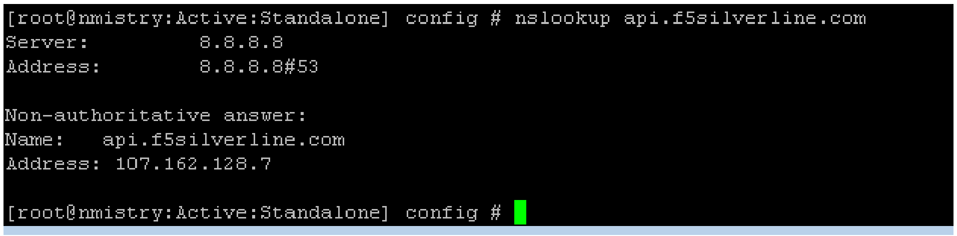
- Open the **Network >> DNS Resolvers >> DNS Resolver** list page and click Create.

- Enter **default_DNS_resolver** for the name and then click Finished.

A DNS resolver is required by bot signatures to allow for proper detection of benign search engines such as Google and Bing. This is a workaround and its setup is planned to be added to the Quick Configuration, it's not included in the version accompanying the installed release for the labs.

- In the BIG-IP putty ssh window verify DNS by typing (or copying and pasting) the following:

```
nslookup api.f5silverline.com
```



```
[root@nmistry:Active:Standalone] config # nslookup api.f5silverline.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   api.f5silverline.com
Address: 107.162.128.7

[root@nmistry:Active:Standalone] config #
```

- Type the following to verify the correct date setting:

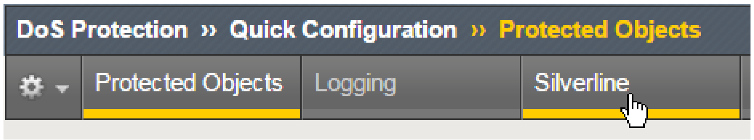
```
date
```

- Do this step only if the BIG-IP system date is not accurate, correct it using the following commands:

```
bigstart stop ntpd
ntpdate pool.ntp.org
bigstart start ntpd
```

Configure Silverline Signaling

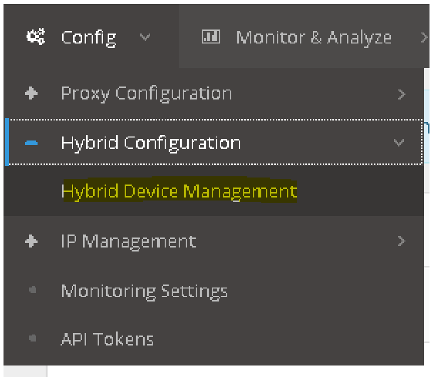
- Use a Firefox web browser and access **https://portal.f5silverline.com**.
- Log in as **dhd2017us@f5agility.com** / **HybridDefense!Wins!**
- In the BIG-IP Configuration Utility, open the **DoS Protection >>Quick Configuration** page.
- Open the **Silverline** page in Dos Protection>>Quick Configuration



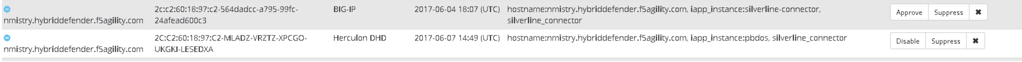
- Configure using following information, and then click Update. **Make sure to use all lowercase for username.**

Username	dhd2017us@f5agility.com
Password	HybridDefense!Wins!
Service Address	https://api.f5silverline.com

- In the Silverline portal browser page, open the **Config>>Hybrid Configuration>>Hybrid Device Management** page.



- Locate your DHD device (<yourfirstinitiallastname>.hybriddefender.f5agility.com) and click Approve for ALL instances of YOUR device

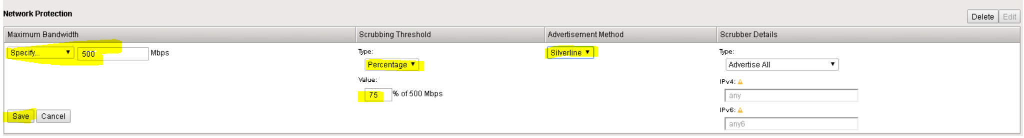


nmistry.hybriddefender.f5agility.com	2c:c2:60:18:97:c2-564dadcc-a795-99fc-24afead600c3	BIG-IP	2017-06-04 18:07 (UTC)	hostname:nmistry.hybriddefender.f5agility.com, iapp_instance:silverline-connector, silverline_connector	Approve Suppress ✖
nmistry.hybriddefender.f5agility.com	2C:C2:60:18:97:C2-MLADZ-VRZTZ-XPCGO-UKGKI-LESEDXA	Herculon DHD	2017-06-07 14:49 (UTC)	hostname:nmistry.hybriddefender.f5agility.com, iapp_instance:pbdos, silverline_connector	Disable Suppress ✖

Configure DHD Device Bandwidth Thresholds

- On the DHD WebUI go to **DoS Protection>>Quick Configuration**. In the Configuration Utility, open the **Protected Objects** page.
- In the **Network Protection** section click Create.
- Configure using following information, and then click **Save**.

Maximum Bandwidth: Specify	500
Scrubbing Threshold: Type	Percentage
Scrubbing Threshold: Value	75
Advertisement Method	Silverline
Scrubber Details: Type	Advertise All



Network Protection

Delete Edit

Maximum Bandwidth	Scrubbing Threshold	Advertisement Method	Scrubber Details
Specify... ▼ 500 Mbps	Type: Percentage ▼ Value: 75 % of 500 Mbps	Silverline ▼	Type: Advertise All ▼ IPv4: any IPv6: any6

Save Cancel

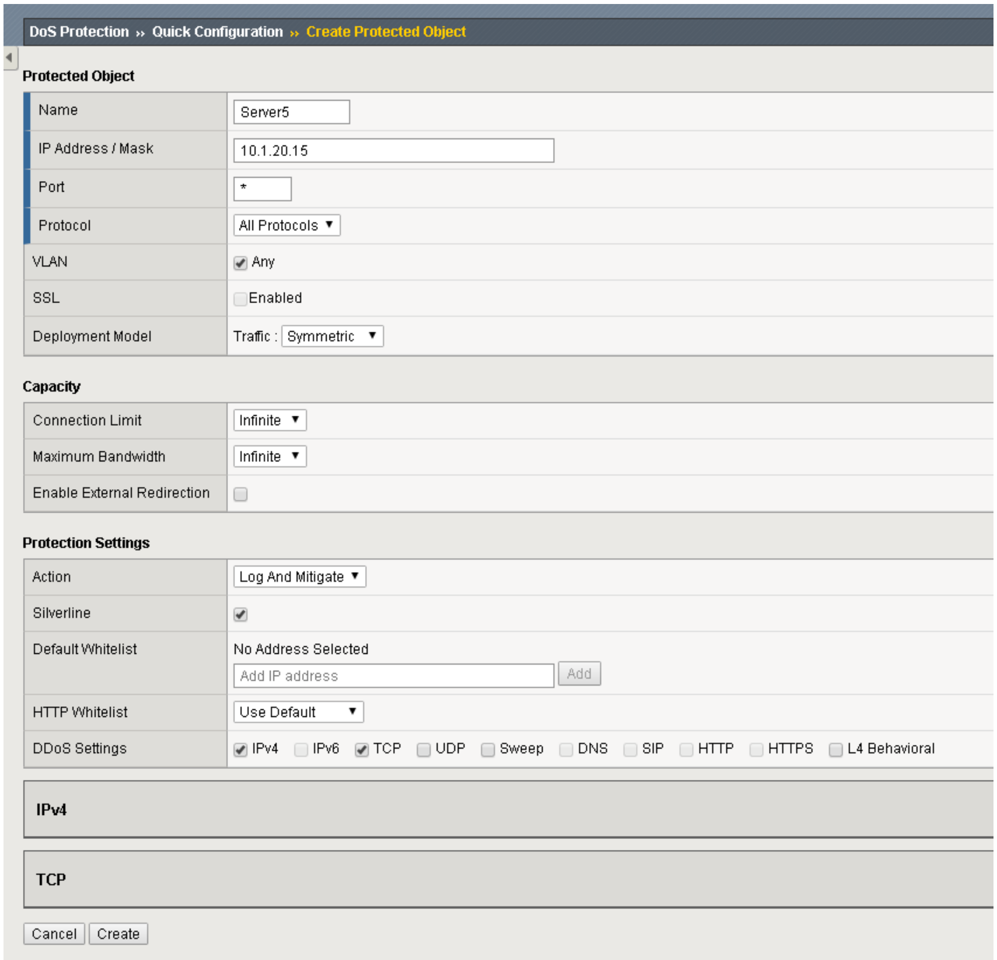
This completes the initial setup for BIG-IP DDoS Hybrid Defender including registration with Silverline.

3.1.2 Lab 2 – Start Baseline Traffic Generation

Task 1 – Create Protected Objects that the baseline traffic will be targeting

- In the BIG-IP Configuration Utility, open the **DoS Protection>>Quick Configuration** page and in the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	Server5
IP Address	10.1.20.15
Port	*
Protocol	All Protocols
VLAN	Any
Protection Settings: Action	Log and Mitigate
Protection Settings: Silverline	Yes (selected)
Protection Settings: DDoS Settings	IPv4, TCP,



DoS Protection » Quick Configuration » Create Protected Object

Protected Object

Name	Server5
IP Address / Mask	10.1.20.15
Port	*
Protocol	All Protocols
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric

Capacity

Connection Limit	Infinite
Maximum Bandwidth	Infinite
Enable External Redirection	□

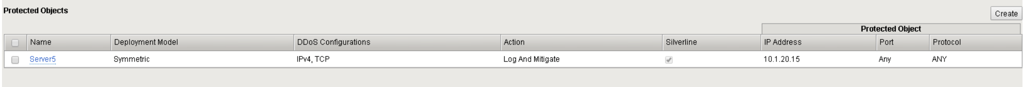
Protection Settings

Action	Log And Mitigate
Silverline	☑
Default Whitelist	No Address Selected Add IP address [Add]
HTTP Whitelist	Use Default
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

IPv4

TCP

- This protected object will be used for Auto-Threshold



Protected Objects

						Protected Object		
□	Name	Deployment Model	DDoS Configurations	Action	Silverline	IP Address	Port	Protocol
□	Server5	Symmetric	IPv4, TCP	Log And Mitigate	✓	10.1.20.15	Any	ANY

Task 2 – Run Scripts to start L4 traffic generation – Good Traffic

- Putty SSH (use the shortcut) to open a shell to the good client system.
- Login as user : ubuntu. The session is preconfigured to authenticate with a certificate.
- Start the auto-threshold baselining script with:

```
# sudo bash
# cd ~/scripts
# ./baseline_l4.sh
```

Note: Ignore the "sudo: unable to resolve host xjumpbox" when you issue the sudo bash command throughout the labs.

3.1.3 Lab 3 – Configuring Network Attack Protection

Task 1 – Disable Device-Level DHD DoS Protection

Disable device-level DoS flood protection, and then issue an ICMPv4 flood and review the results.

- Ssh (putty) into the BIG-IP DHD using the shortcut provided. Resize the BIG-IP putty ssh window by making it wider.
- At the **config** prompt, type (or copy and paste) the following command:

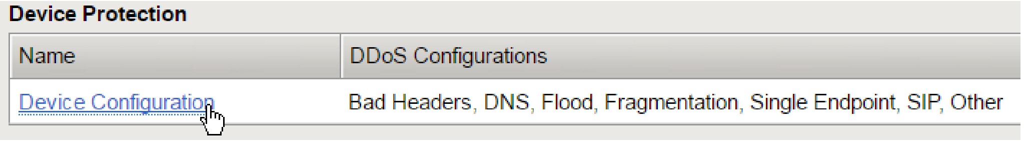
  ```
  tcpdump -i 0.0 host 10.1.20.12
  ```

- Open a second putty window and ssh to the Attacker (use shortcut on the desktop) and log in as **ubuntu**. It will authenticate using the ssh key provided automatically.
- At the **attacker config** prompt, type (or copy and paste) the following command:

  ```
  ping 10.1.20.12
  ```

The attacker can successfully communicate with a back-end resource behind the BIG-IP DHD

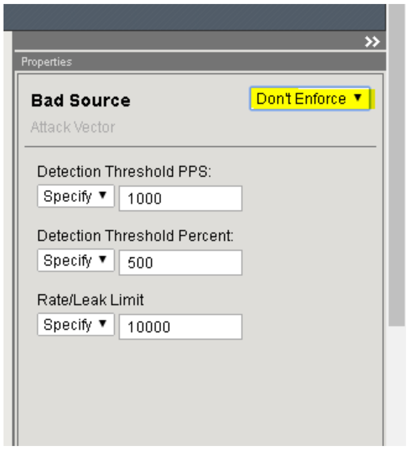
- Examine the tcpdump window and verify ICMP packets are flowing through the BIG-IP DHD.
- Cancel the ping command **(Ctrl+C),** then verify the **tcpdump** stops receiving ICMP packets, and then press **Enter** several times to clear the recent log entries.
- In the Configuration Utility, in the **Device Protection** section click **Device Configuration.**



Device Protection

Name	DDoS Configurations
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other

- In the **Bad Headers** row click the + icon, and then click **Bad Source**.
- On the right-side of the page select the drop-down to "**Don't Enforce**"



Properties

Bad Source Don't Enforce ▼

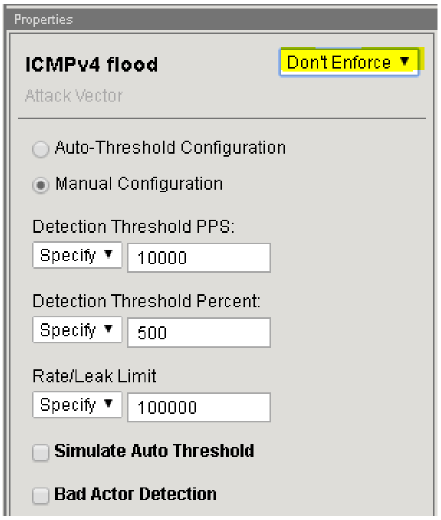
Attack Vector

Detection Threshold PPS:
Specify ▼ 1000

Detection Threshold Percent:
Specify ▼ 500

Rate/Leak Limit
Specify ▼ 10000

- In the **Flood** row click the + icon, and then click **ICMPv4** flood.
- On the right-side of the page select the drop-down to **"Don't Enforce"**



Properties

ICMPv4 flood Don't Enforce ▼

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS:
Specify ▼ 10000

Detection Threshold Percent:
Specify ▼ 500

Rate/Leak Limit
Specify ▼ 100000

□ **Simulate Auto Threshold**

□ **Bad Actor Detection**

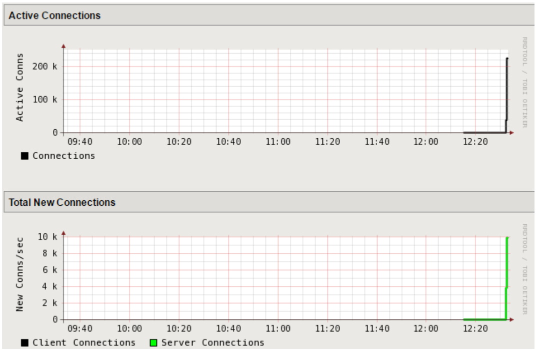
- Click **Update**.
- In the **Attacker** putty window type (or copy and paste) the following:

```
# sudo bash
# cd ~/scripts
# for i in {1..10}; do ./icmpflood.sh; done
```

This script launches 1,000,000 ICMP requests and then repeats for a total of ten occurrences.

- View the **tcpdump** window and verify that ICMP attack traffic is reaching the back-end server.
- Let the attack run for about 15 seconds before moving on.
- In the Configuration Utility, open the **Statistics >> Performance >> Performance page.**
- View the **Active Connections** and **Total New Connections** charts.

  There is a drastic spike in active connections.



- View the **Throughput (bits)** and **Throughput (packets)** charts.

  There is also a drastic spike in both bits per second and packets per second.

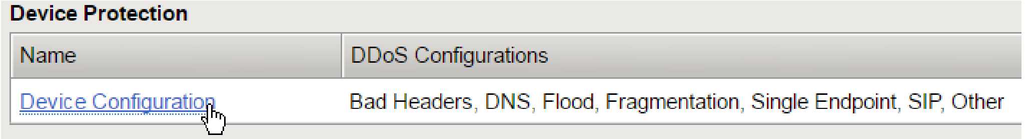
- Open the **Security >> Event Logs >> DoS >> Network >> Events** page.

  The log file is empty as we disabled device-level flood protection vector on BIG-IP DHD.

- In the Attacker putty ssh shell slowly hit Ctrl + C several times until the prompt is back at the /**scripts**.

Task 2 – Re-enable Device-Level DHD DoS Protection

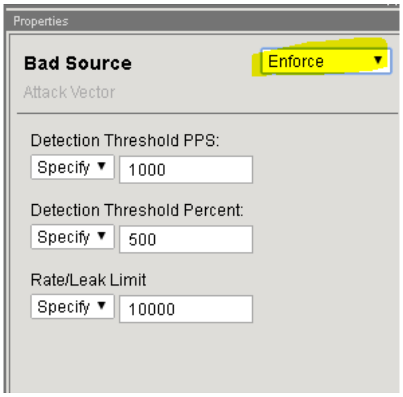
- In the Configuration Utility, in the **Device Protection** section click **Device Configuration.**



Device Protection

Name	DDoS Configurations
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other

- In the **Bad Headers** row click the + icon, and then click **Bad Source**.
- On the right-side of the page select the drop-down to **"Enforce"**



Bad Source Enforce ▾

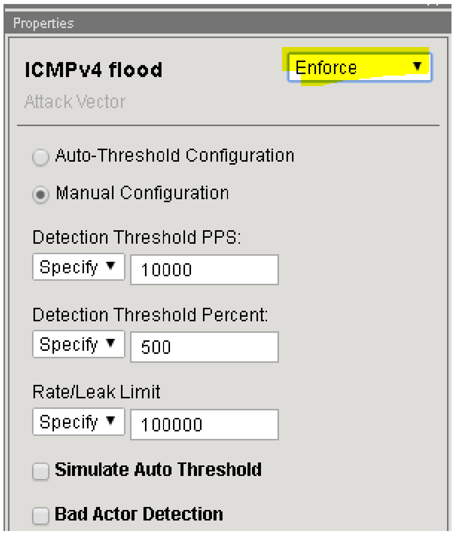
Attack Vector

Detection Threshold PPS:
Specify ▾ 1000

Detection Threshold Percent:
Specify ▾ 500

Rate/Leak Limit
Specify ▾ 10000

- In the **Flood** row click the + icon, and then click **ICMPv4** flood.
- On the right-side of the page select the drop-down to **"Enforce"**



Properties

ICMPv4 flood Enforce

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS:

Specify 10000

Detection Threshold Percent:

Specify 500

Rate/Leak Limit

Specify 100000

□ Simulate Auto Threshold

□ Bad Actor Detection

- Click Update.

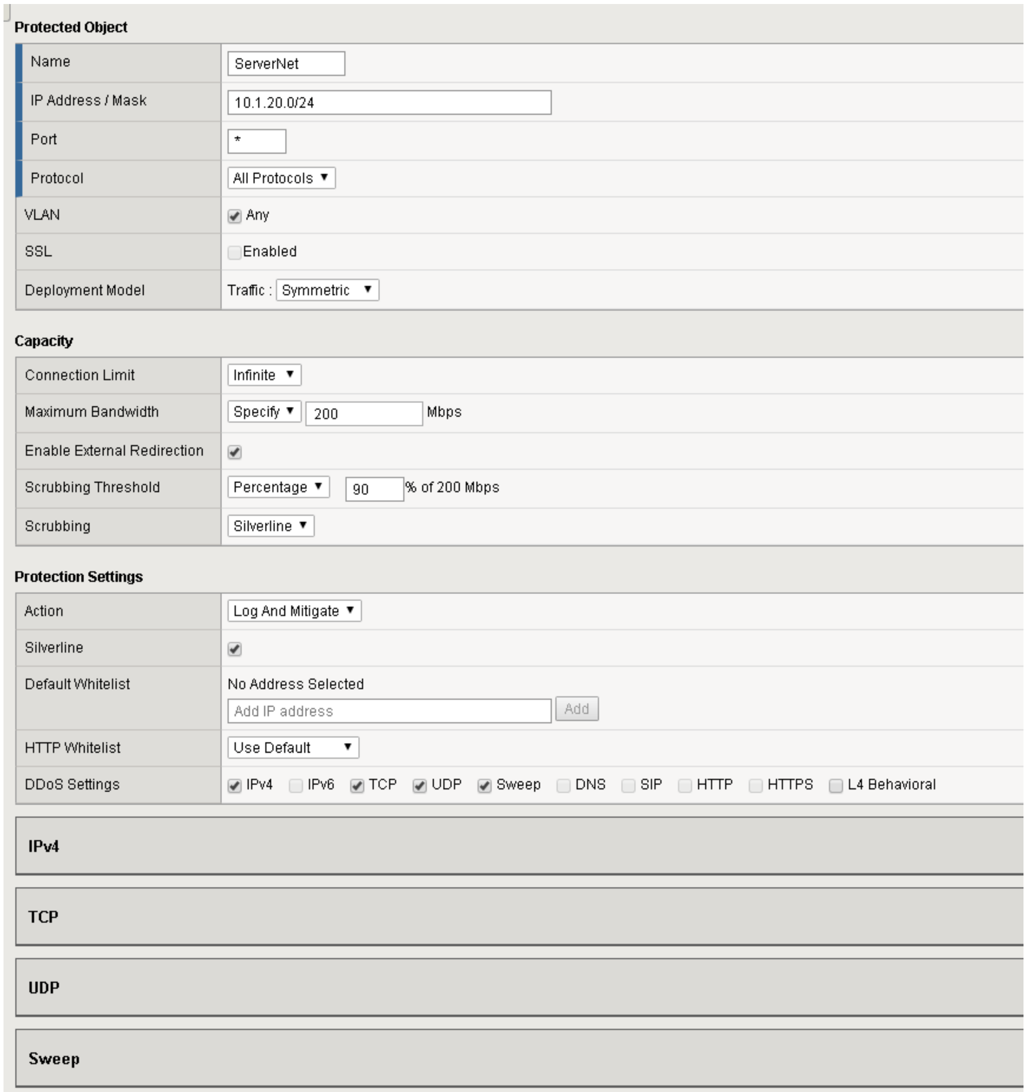
  This returns the configuration back to factory supplied device level enforcement.

Task 3 – Configure Protected Object-Level Network DoS Protection

With the DHD device wide protection provides a line of defense and is enforced for all traffic flowing through the device. For more granular control, we use protected objects and configure mitigation settings for those objects to be enforced. In this task we will configure object-level DoS network multi-vector protection, and then issue an attack and review the results in the next task.

- Go to **Dos Protection>>Quick Configuration**
- On the **Protect Objects** page, in the **Protected Objects section** click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	ServerNet
IP Address	10.1.20.0/24
Port	*
Protocol	All Protocols
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	IPv4,TCP,UDP, Sweep
Maximum Bandwidth: Specify	200
Enable External Redirection	Checked
Scrubbing Threshold: Percentage	90%
Scrubbing	Silverline
Silverline	Checked



Protected Object

Name	ServerNet
IP Address / Mask	10.1.20.0/24
Port	*
Protocol	All Protocols ▼
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric ▼

Capacity

Connection Limit	Infinite ▼
Maximum Bandwidth	Specify ▼ 200 Mbps
Enable External Redirection	☑
Scrubbing Threshold	Percentage ▼ 90 % of 200 Mbps
Scrubbing	Silverline ▼

Protection Settings

Action	Log And Mitigate ▼
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default ▼
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP ☑ UDP ☑ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

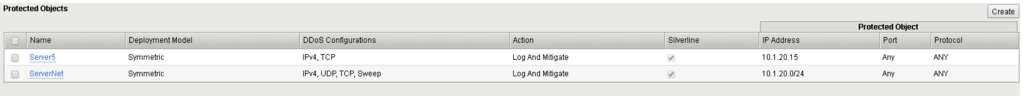
IPv4

TCP

UDP

Sweep

- Verify the newly created protected object:

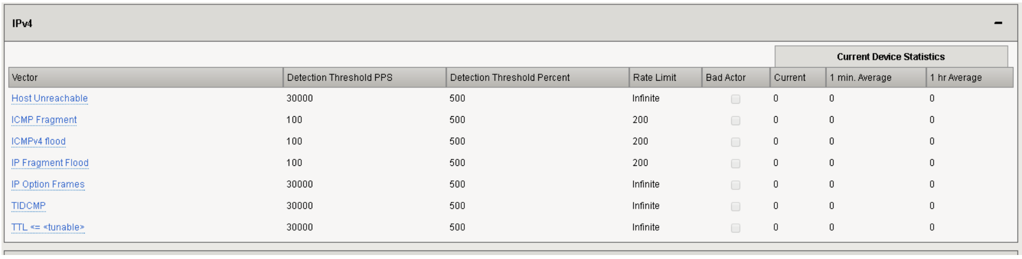


Protected Objects Create

□	Name	Deployment Model	DDoS Configurations	Action	Silverline	Protected Object IP Address	Port	Protocol
□	Server5	Symmetric	IPv4, TCP	Log And Mitigate	☑	10.1.20.15	Any	ANY
□	ServerNet	Symmetric	IPv4, UDP, TCP, Sweep	Log And Mitigate	☑	10.1.20.0/24	Any	ANY

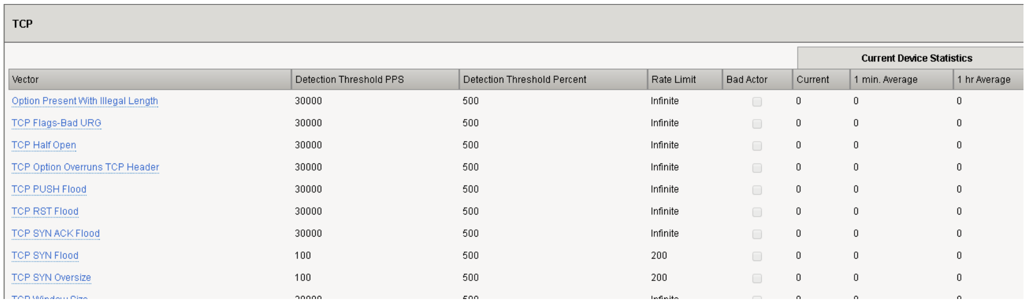
- Click on the **"ServerNet"** object and configure the following vectors and click **Update**.

Vector	Detection Thresh. PPS	Detection Thresh %	Rate Limit
ICMP Fragment	100	500	200
ICMPv4 Flood	100	500	200
IP Fragment Flood	100	500	200
TCP SYN Flood	100	500	200
TCP SYN Oversize	100	500	200



IPv4

					Current Device Statistics		
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
Host Unreachable	30000	500	Infinite	☐	0	0	0
ICMP Fragment	100	500	200	☐	0	0	0
ICMPv4 flood	100	500	200	☐	0	0	0
IP Fragment Flood	100	500	200	☐	0	0	0
IP Option Frames	30000	500	Infinite	☐	0	0	0
TIDCMP	30000	500	Infinite	☐	0	0	0
TTL <= <tunable>	30000	500	Infinite	☐	0	0	0



TCP

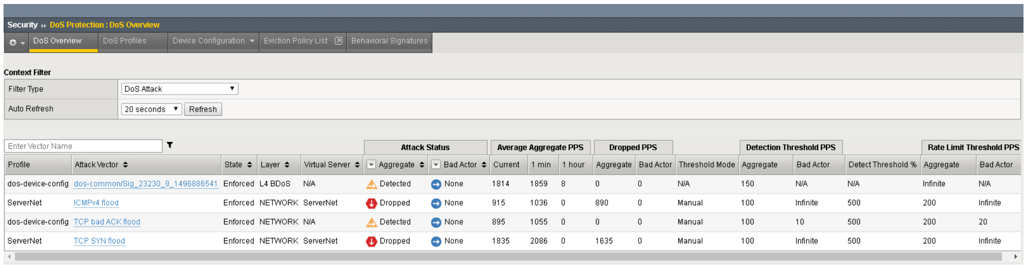
					Current Device Statistics		
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
Option Present With Illegal Length	30000	500	Infinite	☐	0	0	0
TCP Flags-Bad URG	30000	500	Infinite	☐	0	0	0
TCP Half Open	30000	500	Infinite	☐	0	0	0
TCP Option Overruns TCP Header	30000	500	Infinite	☐	0	0	0
TCP PUSH Flood	30000	500	Infinite	☐	0	0	0
TCP RST Flood	30000	500	Infinite	☐	0	0	0
TCP SYN ACK Flood	30000	500	Infinite	☐	0	0	0
TCP SYN Flood	100	500	200	☐	0	0	0
TCP SYN Oversize	100	500	200	☐	0	0	0
TCP Window Size	30000	500	Infinite	☐	0	0	0

Task 4 – Launch the attack and view the results

- Click **DoS Protection>>Quick Configuration->ServerNet**
- Open the following as **new tabs** (right click and select open link in a new tab) in the DHD UI (Google Chrome Window):
- **Security>>DoS Protection>>DoS Overview** (leave the filter at default: 'DoS Attack' and change auto refresh to 20 seconds)
- **Statistics>>DoS Visibility**
- Access the Attacker System CLI/shell and launch the attack:

```
# sudo bash
# cd ~/scripts
# ./multivector.sh
```

The attacks will be detected immediately. Let the attacks run for a couple of minutes. Click Refresh on the DoS Overview page and it will start to populate. You will see some attacks mitigated by Device Configuration and some mitigated by the more specific settings on the ServerNet Protected Object:



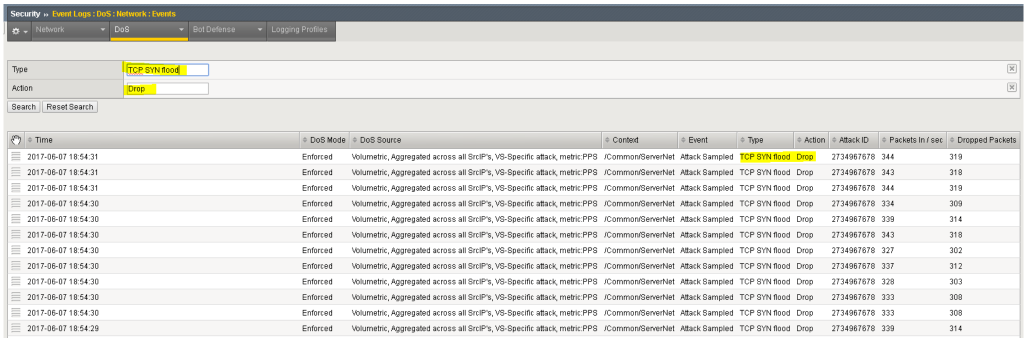
Context Filter

Filter Type: DoS Attack

Auto Refresh: 20 seconds Refresh

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
dos-device-config	dos-common/Sig_23230_9_1496886541	Enforced	L4 BDoS	N/A	Detected	None	1814	1859	8	0	0	N/A	150	N/A	N/A	Infinite	N/A
ServerNet	ICMPv4 flood	Enforced	NETWORK	ServerNet	Dropped	None	915	1036	0	890	0	Manual	100	Infinite	500	200	Infinite
dos-device-config	TCP bad ACK flood	Enforced	NETWORK	N/A	Detected	None	895	1055	0	0	0	Manual	100	10	500	200	20
ServerNet	TCP SYN flood	Enforced	NETWORK	ServerNet	Dropped	None	1835	2086	0	1635	0	Manual	100	Infinite	500	200	Infinite

- Navigate to **Security>>Event Logs>>DoS->Network>>Events**.
- Click on "custom search. . . " link.
- Drag one of the values from the "Attack Type" column into the custom search builder. From the Action column, drag Drop into the search builder. Click "Search"



Type: TCP SYN flood
Action: Drop

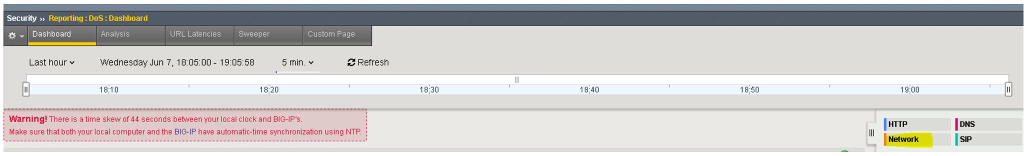
Time	DoS Mode	DoS Source	Context	Event	Type	Action	Attack ID	Packets In / sec	Dropped Packets
2017-06-07 18:54:31	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	344	319
2017-06-07 18:54:31	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	343	318
2017-06-07 18:54:31	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	344	319
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	334	309
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	339	314
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	343	318
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	327	302
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	337	312
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	328	303
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	333	308
2017-06-07 18:54:30	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	333	308
2017-06-07 18:54:29	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN flood	Drop	2734967678	339	314

Further explore the DoS Event logs. For example, clear the search and identify the "Stop" and "Start" times for an attack, etc.

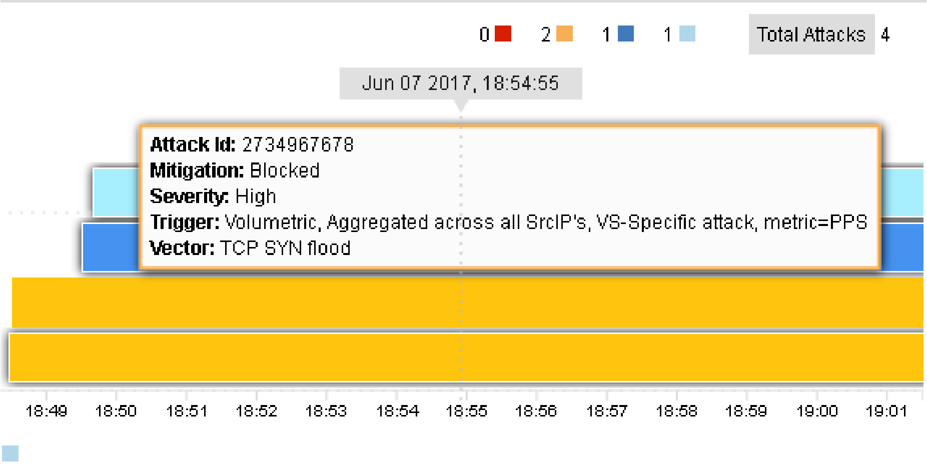
- In the Hybrid Defender WebUI, access the DoS Visibility reporting tool at **Statistics>>DoS Visibility**. If you get a time-skew warning, then please ignore it as it's the Windows PC that can't keep the clock right.

Note: The DoS Visibility is a reporting tool, not a real-time monitoring tool. Events are displayed, much like other AVR-based reporting, in 5 minute windows. Do not expect events to be shown here immediately after running an attack. Quicker/real-time monitoring of on-going DoS attacks is best accomplished in the DoS Event Logs and DoS Overview areas of the WebUI.**

- You should see the attacks in the timeline and a variety of details in the windows. Use the slider to shorten the timeframe if needed, and click the Network filter, to focus on L4 attacks and mitigation.



Warning! There is a time skew of 44 seconds between your local clock and BIG-IP's.
Make sure that both your local computer and the BIG-IP have automatic-time synchronization using NTP.



Attack Id: 2734967678
Mitigation: Blocked
Severity: High
Trigger: Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric=PPS
Vector: TCP SYN flood

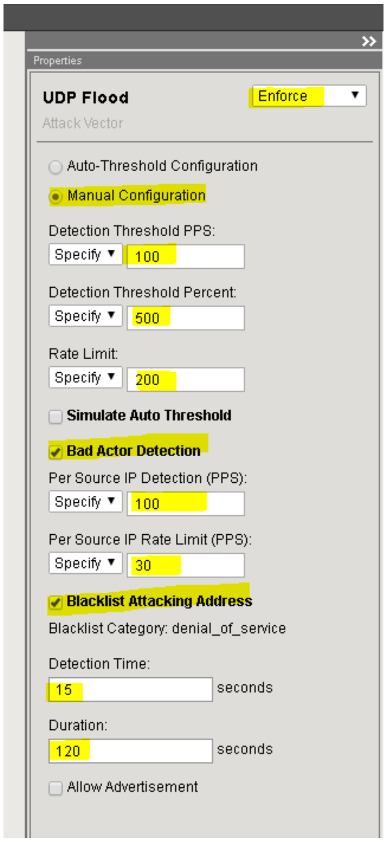
- Stop the attack (Ctrl+C) in the Attacker CLI (ssh window).

Task 5 – Configure Bad Actor Detection

Add bad actor detection for a for the UDP flood protection.

- In the Configuration Utility, open the **DoS Protection >> Quick Configuration** page and in the **Protected Objects** section click **ServerNet**.
- In the **UDP** row click the **+** icon, and then click **UDP Flood**.
- On the right-side of the page configure using the following information in the table, and then click **Update**.
- Set the UDP Flood vector settings:

Setting	Value
Enforce	selected
Manual Configuration	selected
Detection Threshold PPS	100
Detection Threshold Percent	500
Rate Limit	200
Bad Actor Detection	selected
Per Source IP Detection	100 PPS
Per Source IP Rate Limit	30 PPS
Blacklist Attacking Addresses	selected
Detection Time	15 seconds
Duration	120 seconds



UDP Flood
Enforce ▼
Attack Vector

○ Auto-Threshold Configuration
● Manual Configuration

Detection Threshold PPS:
Specify ▼ 100

Detection Threshold Percent:
Specify ▼ 500

Rate Limit:
Specify ▼ 200

□ Simulate Auto Threshold

☑ Bad Actor Detection

Per Source IP Detection (PPS):
Specify ▼ 100

Per Source IP Rate Limit (PPS):
Specify ▼ 30

☑ Blacklist Attacking Address

Blacklist Category: denial_of_service

Detection Time:
15 seconds

Duration:
120 seconds

□ Allow Advertisement

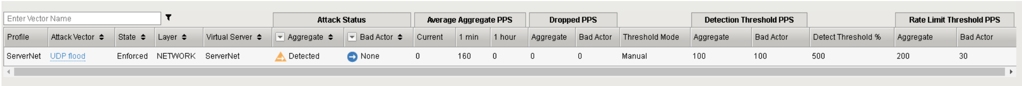
- Open the following in new tabs (Google Chrome - right click and select open link in new tab) in the DHD UI:
- **DoS Protection>>Quick Configuration>>ServerNet**

- **Security>>DoS Protection>>DoS Overview** (leave filter at default: “DoS Attack” and set refresh rate to 20s)
- **Statistics>>DoS Visibility**
- **Security>>Event Logs>>Network->IP Intelligence**
- Access the Attacker system CLI (putty ssh) and run the UDP flood attack:

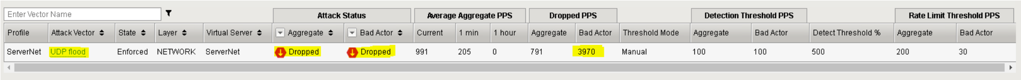
```
# sudo bash
# cd ~/scripts
# ./udp\_flood.sh

From the menu, select ‘1’ to start the attack

root@attacker-a:~/scripts# ./udp\_flood.sh
1) Attack start
2) Attack end
3) Quit

#?
```

Note: This attack is relatively short-lived. You can launch it again if the attack ends and you are not finished showing the various reports. Simply type ‘1’ again, to re-run the attack. You may have to run the attack multiple times using ‘1’.

- In the DoS Overview page observe the blocks by Bad Actor

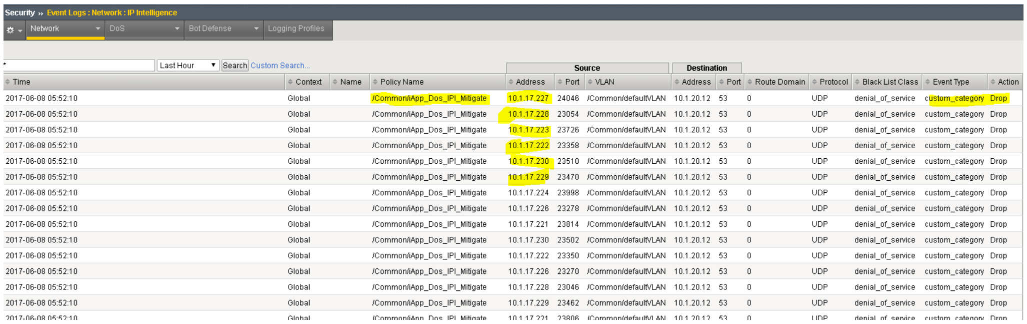


					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
ServerNet	UDP flood	Enforced	NETWORK	ServerNet	⚠ Detected	➜ None	0	160	0	0	0	Manual	100	100	500	200	30



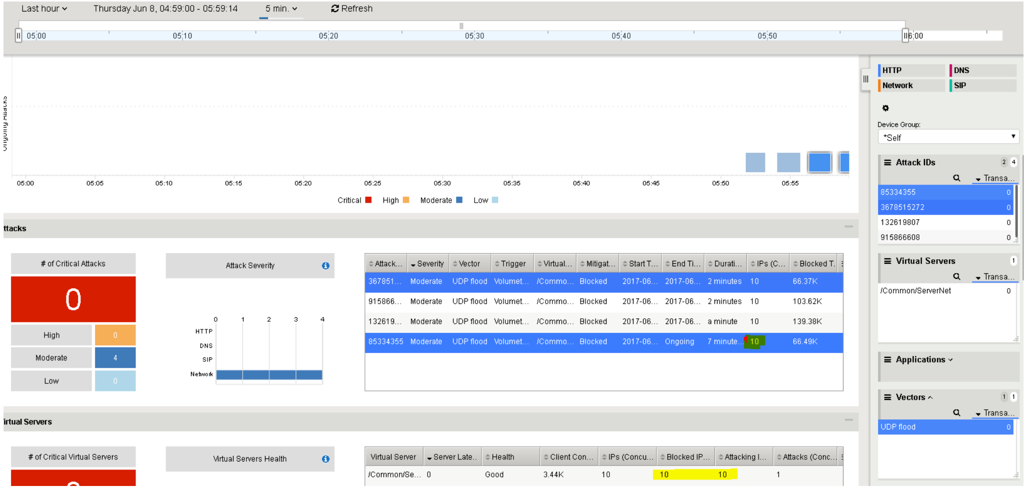
					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
ServerNet	UDP flood	Enforced	NETWORK	ServerNet	Dropped	Dropped	991	205	0	791	3970	Manual	100	100	500	200	30

- In the IP Intelligence Event Logs observe the IP addresses that are being added to the denial_of_service blacklist.



				Source			Destination						
Time	Context	Name	Policy Name	Address	Port	VLAN	Address	Port	Route Domain	Protocol	Black List Class	Event Type	Action
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.227	24046	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	23054	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.223	23726	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.222	23358	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.230	23510	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.229	23470	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.224	23998	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	23278	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.221	23814	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.230	23502	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.222	23350	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	23270	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	23046	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.229	23462	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-06-08 05:52:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.221	23806	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop

- In the DoS Visibility tab expand the Vectors inspector and select UDP Flood. When it updates, select a flood from the timeline. Note in the Attacks panel the #IPs blocked is 10



Attack...	Severity	Vector	Trigger	Virtual...	Mitigat...	Start T...	End Ti...	Durati...	IPs (C...	Blocked T.
367851...	Moderate	UDP flood	Volumet...	/Commo...	Blocked	2017-06...	2017-06...	2 minutes	10	66.37K
915866...	Moderate	UDP flood	Volumet...	/Commo...	Blocked	2017-06...	2017-06...	2 minutes	10	103.62K
132619...	Moderate	UDP flood	Volumet...	/Commo...	Blocked	2017-06...	2017-06...	a minute	10	139.38K
85334355	Moderate	UDP flood	Volumet...	/Commo...	Blocked	2017-06...	Ongoing	7 minute...	10	66.49K

Virtual Server	Server Late..	Health	Client Con...	IPs (Concu...	Blocked IP...	Attacking I...	Attacks (Conc...
/Common/Se...	0	Good	3.44K	10	10	10	1

Attack IDs	Transa...
85334355	0
3678515272	0
132619807	0
915866608	0

Virtual Servers	Transa...
/Common/ServerNet	0

Vectors	Transa...
UDP flood	0

- End the UDP_Flood attack script by typing ‘2’ to kill any still running processes and then ‘3’ to exit the script.
- **Clean-Up : Be sure to stop all hping3 processes by using the following command**:

```
# sudo bash
# killall -9 hping3
```

3.1.4 Lab 4 – Using Auto Thresholding

This exercise will simulate a newly configured Protected Object where the security administrator is unsure what values to assign to a few common vectors. Note that auto-thresholding is useful at both the Device and Protected Object levels

Note: This demo may place significant stress on the demo environment. This may make the DHD UI less responsive. This is unavoidable since for auto-thresholding to block, the attack must be damaging enough to cause stress, which will push the CPU on the Virtual Environment very high. Remember that this is a virtual environment with minimal resources for lab under high stress and that the Hybrid Defender appliances mitigate these attacks in dedicated hardware.**

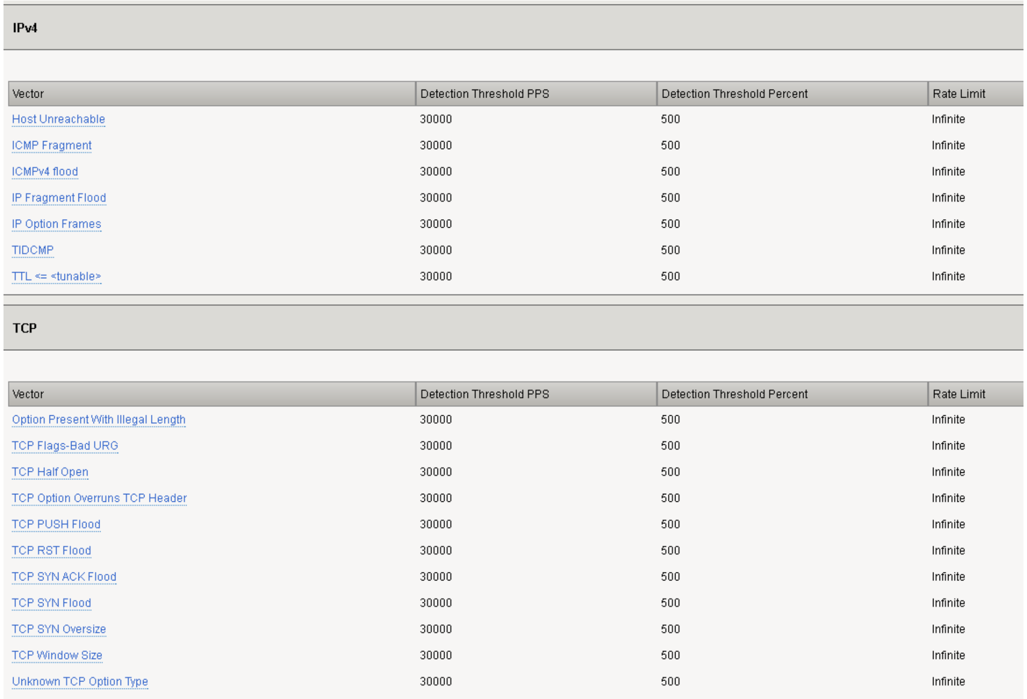
Task 1 – Configure Auto Thresholding

- On the Good Client, if you have not already done so, start the network baselining. This step is needed if you didn’t start the good traffic generation in Exercise 2 or accidently stopped it.

```
# sudo bash
# cd ~/scripts
# ./baseline_l4.sh
```

- In the Hybrid Defender UI, in Quick Configuration, select the Server5 Protected Object and verify that the IP and TCP vectors are all at default thresholds with auto-threshold disabled:

Setting	Value
All Detection Thresholds	30000 pps
All Rate Limits	Infinite
Auto Thresholding	Disabled



IPv4

Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Host Unreachable	30000	500	Infinite
ICMP Fragment	30000	500	Infinite
ICMPv4 flood	30000	500	Infinite
IP Fragment Flood	30000	500	Infinite
IP Option Frames	30000	500	Infinite
TIDCMP	30000	500	Infinite
TTL <= <tunable>	30000	500	Infinite

TCP

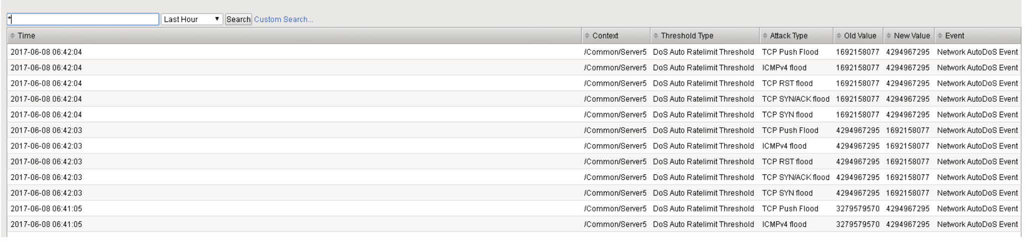
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Option Present With Illegal Length	30000	500	Infinite
TCP Flags-Bad URG	30000	500	Infinite
TCP Half Open	30000	500	Infinite
TCP Option Overruns TCP Header	30000	500	Infinite
TCP PUSH Flood	30000	500	Infinite
TCP RST Flood	30000	500	Infinite
TCP SYN ACK Flood	30000	500	Infinite
TCP SYN Flood	30000	500	Infinite
TCP SYN Oversize	30000	500	Infinite
TCP Window Size	30000	500	Infinite
Unknown TCP Option Type	30000	500	Infinite

- In the Hybrid Defender CLI (BIGIP ssh window), restart auto-thresholding:

```
# tmsh run security dos device-config auto-threshold-relearn
# tmsh run security dos virtual name Server5 auto-threshold-relearn
```

In the Hybrid Defender WebUI, in the **Server5** Protected Object configuration, enable auto-thresholding for the following vectors: **ICMPv4 Flood, TCP SYN Flood, TCP Push Flood, TCP RST Flood, TCP SYN ACK Flood** by selecting each vector and **clicking the Auto-Threshold Configuration radio button**. When all vectors are configured, click **Update** at the bottom of the screen.

- In the Hybrid Defender WebUI, view the Auto Threshold event log by navigation to **Security>>Event Logs>>DoS>>Network>>Auto Threshold**.



Time	Context	Threshold Type	Attack Type	Old Value	New Value	Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:41:05	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	3279579570	4294967295	Network AutoDoS Event
2017-06-08 06:41:05	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	3279579570	4294967295	Network AutoDoS Event

The system is updating the detection thresholds. With auto-thresholding, the system adjust the detection thresholds based on observed traffic patterns. However, mitigation rate limits are always dynamic based on detected system or protected object stress. If anomalous levels of traffic are running, but there is no stress, the Hybrid Defender will generate alerts but will not block traffic. Under stress, the rate limits are automatically created and adjusted dynamically.

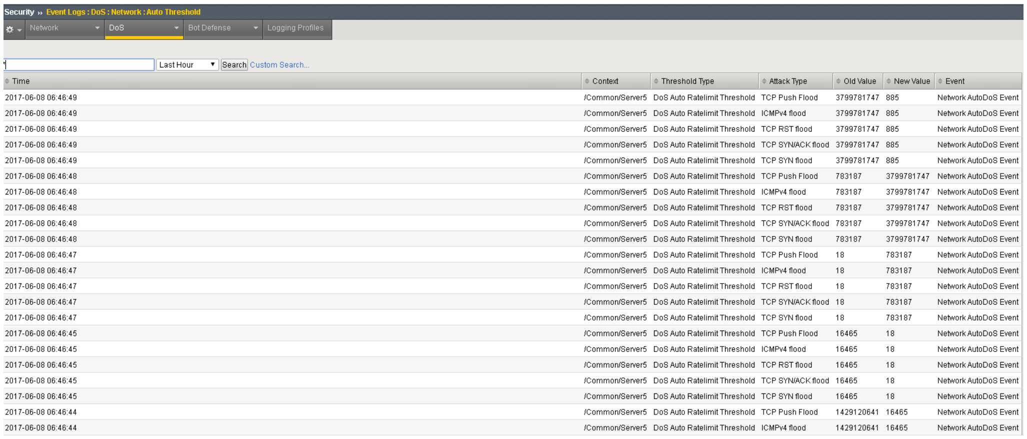
Task 2 – Create Stress to trigger Auto Thresholding and view Reports.

- Let's create some stress with a Flood attack. In the Attacker CLI start the auto-threshold flood:

```
# sudo bash
# cd ~/scripts
# ./autot_flood.sh
```

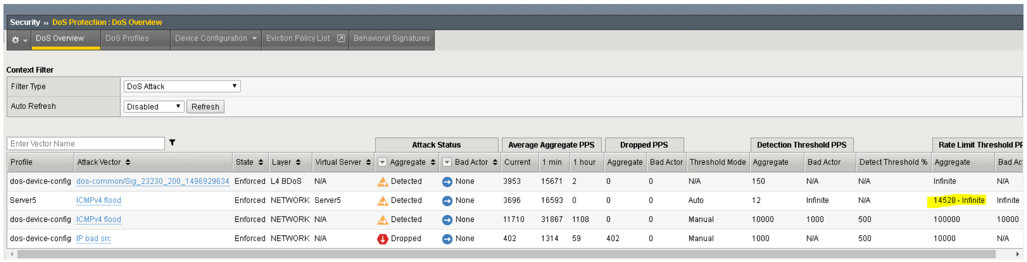
This is a long duration attack. You can terminate it with Ctrl+C when finished.

- In the Hybrid Defender WebUI, review the Auto Threshold event log. You will see that Rate limits are being automatically set and adjusted to mitigate the flood attack.



Time	Context	Threshold Type	Attack Type	Old Value	New Value	Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:44	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	1429120641	16465	Network AutoDoS Event
2017-06-08 06:46:44	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	1429120641	16465	Network AutoDoS Event

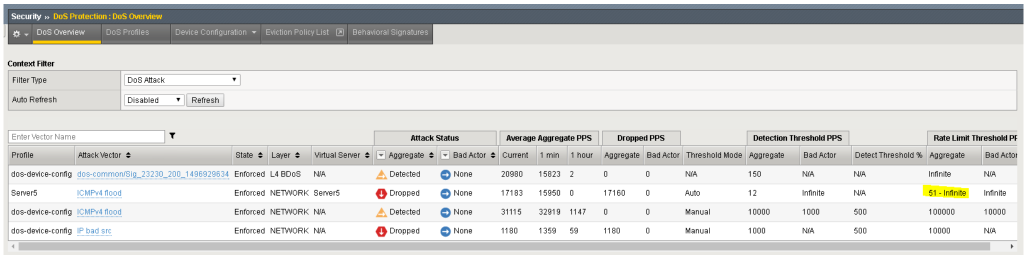
- In the Hybrid Defender WebUI, view the DoS Overview. Note that the ICMP Flood attack is being mitigated and the rate limit thresholds for each of the auto-threshold vectors have been adjusted based on stress, including vectors that are not detecting or blocking an attack.



Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PP	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Ac
dos-device-config	dos-common/Sig_23230_200_1496929634	Enforced	L4 BDoS	N/A	Detected	None	3953	15671	2	0	0	N/A	150	N/A	N/A	Infinite	N/A
Server5	ICMPv4 flood	Enforced	NETWORK	Server5	Detected	None	3696	16593	0	0	0	Auto	12	Infinite	N/A	14528 - Infinite	Infinite
dos-device-config	ICMPv4 flood	Enforced	NETWORK	N/A	Detected	None	11710	31867	1108	0	0	Manual	10000	1000	500	100000	10000
dos-device-config	IP bad src	Enforced	NETWORK	N/A	Dropped	None	402	1314	59	402	0	Manual	1000	N/A	500	10000	N/A

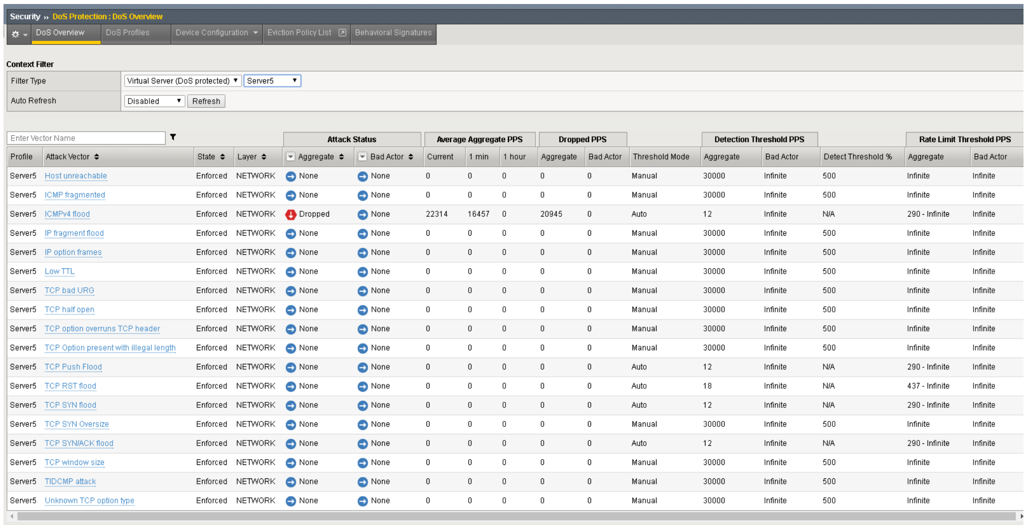


Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PF	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
dos-device-config	dos-common/Sig_23230_200_1496929634	Enforced	L4 BDoS	N/A	Detected	None	20980	15823	2	0	0	N/A	150	N/A	N/A	Infinite	N/A
Server5	ICMPv4 flood	Enforced	NETWORK	Server5	Dropped	None	17183	15950	0	17160	0	Auto	12	Infinite	N/A	51 - Infinite	Infinite
dos-device-config	ICMPv4 flood	Enforced	NETWORK	N/A	Detected	None	31115	32919	1147	0	0	Manual	10000	1000	500	100000	10000
dos-device-config	IP bad src	Enforced	NETWORK	N/A	Dropped	None	1180	1359	59	1180	0	Manual	1000	N/A	500	10000	N/A

- Select the filter type to **Virtual Server (DoS protected)** and **Server5** and view how various Thresholds are dynamically adjusted based on the stress



Security » DoS Protection : DoS Overview

DoS Overview | DoS Profiles | Device Configuration | Eviction Policy List | Behavioral Signatures

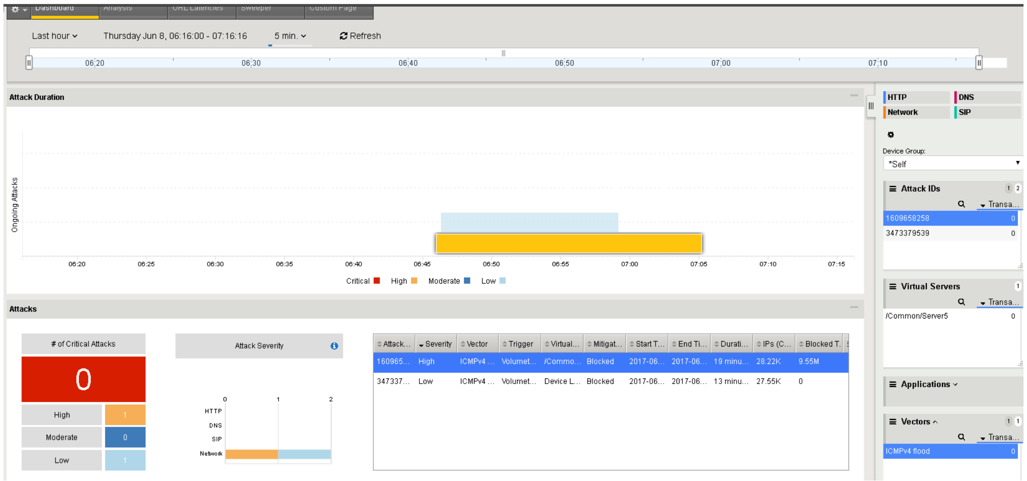
Context Filter

Filter Type	Virtual Server (DoS protected) ▼ Server5 ▼
Auto Refresh	Disabled ▼ Refresh

Enter Vector Name

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
Server5	Host unreachable	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	ICMP fragmented	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	ICMPv4 flood	Enforced	NETWORK	Dropped	None	22314	16457	0	20945	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	IP fragment flood	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	IP option frames	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	Low TTL	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP bad URG	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP half open	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP option overruns TCP header	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP Option present with illegal length	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP Push Flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	TCP RST flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	18	Infinite	N/A	437 - Infinite	Infinite
Server5	TCP SYN flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	TCP SYN Oversize	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP SYN/ACK flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	TCP window size	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TIDCMP attack	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	Unknown TCP option type	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite

- Terminate the attack in the Attacker CLI with Ctrl+C.
- After the attack has ended, in the Hybrid Defender WebUI, navigate to the DoS Visibility page. Under Vectors, select ICMPv4 Flood. View various details.



Last hour ⌄ Thursday Jun 8, 06:16:00 - 07:16:16 5 min. ⌄ Refresh

# of Critical Attacks	
0	
High	1
Moderate	0
Low	1

Attack...	Severity	Vector	Trigger	Virtual...	Mitigat...	Start T...	End Ti...	Durati...	IPs (C...	Blocked T.
160965...	High	ICMPv4 ...	Volumet...	/Commo...	Blocked	2017-06...	2017-06...	19 minu...	28.22K	9.55M
347337...	Low	ICMPv4 ...	Volumet...	Device L...	Blocked	2017-06...	2017-06...	13 minu...	27.55K	0

Device Group: *Self ▼

Attack IDs 1 2

	Transa...
1609658258	0
3473379539	0

Virtual Servers 1

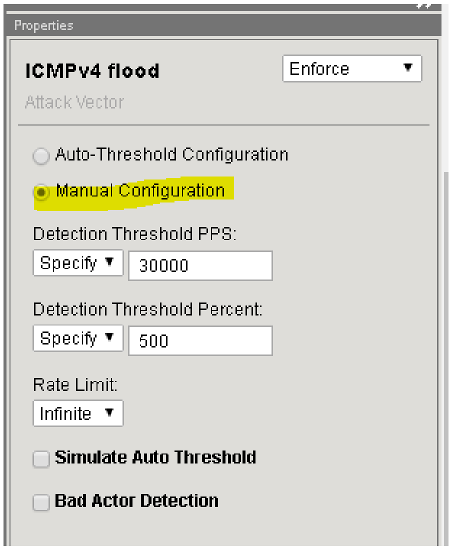
	Transa...
/Common/Server5	0

Applications ⌄

Vectors ^ 1 1

	Transa...
ICMPv4 flood	0

- **Clean-up**: On the Attacker CLI, if the attack is still running be certain to end it with Ctrl-C.
- **Clean-up**: For repeatability, it is necessary to disable the auto-thresholding for the **ICMPv4 Flood, TCP RST Flood, TCP Push Flood, TCP SYN ACK Flood** and **TCP SYN Flood** vectors on the **Server5** protected object. **Switch them back to Manual Configuration.**


Properties

ICMPv4 flood Enforce ▼
Attack Vector

○ Auto-Threshold Configuration
● Manual Configuration

Detection Threshold PPS:
Specify ▼ 30000

Detection Threshold Percent:
Specify ▼ 500

Rate Limit:
Infinite ▼

□ **Simulate Auto Threshold**

□ **Bad Actor Detection**

- **Clean-up**: After disabling auto-thresholding, clear the learning on the Hybrid Defender CLI with:

```
# tmsh run security dos device-config auto-threshold-relearn
# tmsh run security dos virtual name Server5 auto-threshold-relearn
```

- **Clean-up**: Stop the baseline traffic generation from the **good-client** if still running using CTRL+C

3.1.5 Lab 5 – Configuring DNS Attack Protection

DNS DoS attacks come in many flavors and target different resources. DNS query, reverse flood and amplification attacks are some such DNS attacks.

DNS Query Flood

This type of DoS of service attack has a couple possible resource impacts.

- Overwhelm the DNS server's ability to respond by sending too many requests

This can be done just by asking for more requests than the server can reply with and prevent the server from servicing legitimate requests. It doesn't really matter if the clients are spoofed or not, it only matters that the DNS server just can't keep up.

Mitigation Options

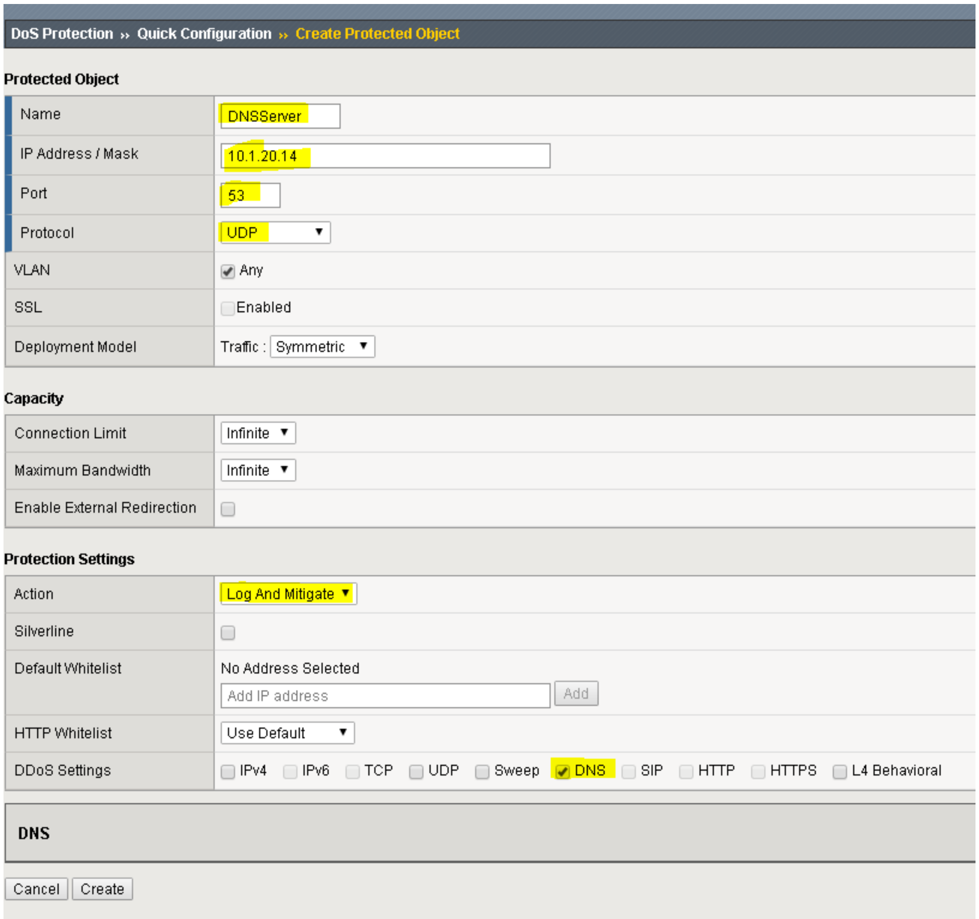
DNS DoS mitigation generally requires an awareness of what you're trying to protect. This allows you to apply the appropriate mitigations and push the problem upstream until the next step is to force it off premises and in to a cloud solution. Load balancing is one remedy to this solution (anycast). Spreading the requests across pools of servers can help mitigate against these types of attacks. DNS Express is another option to increase the capacity of your DNS infrastructure. Layering in DHD DNS DoS vector mitigation also stops common DNS attacks.

Task 1 – Use a Protected Object to Mitigate a DNS Query Flood

- In the BIG-IP Configuration Utility, open the **DoS Protection** > **Quick Configuration** page and in the

- In the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create.**

Name	DNSServer
IP Address	10.1.20.14
Port	53
Protocol	UDP
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	DNS



DoS Protection » Quick Configuration » Create Protected Object

Protected Object

Name	DNSServer
IP Address / Mask	10.1.20.14
Port	53
Protocol	UDP
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric

Capacity

Connection Limit	Infinite
Maximum Bandwidth	Infinite
Enable External Redirection	□

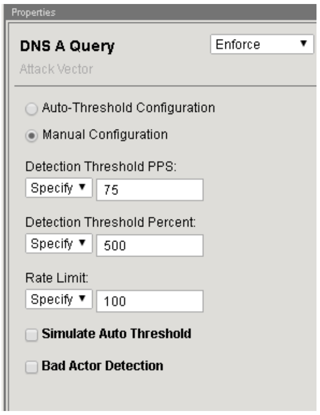
Protection Settings

Action	Log And Mitigate
Silverline	□
Default Whitelist	No Address Selected Add IP address [Add]
HTTP Whitelist	Use Default
DDoS Settings	□ IPv4 □ IPv6 □ TCP □ UDP □ Sweep ☑ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

DNS

- In the **DNS** row click the **+** icon, and then click **DNS A Query**.
- On the right-side of the page configure using the following information, and then click **Create**.

Detection Threshold PPS	Specify: 75
Detection Threshold Percent	Specify: 500
Rate Limit	Specify: 100



Properties

DNS A Query Enforce ▾

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS:

Specify ▾ 75

Detection Threshold Percent:

Specify ▾ 500

Rate Limit:

Specify ▾ 100

□ **Simulate Auto Threshold**

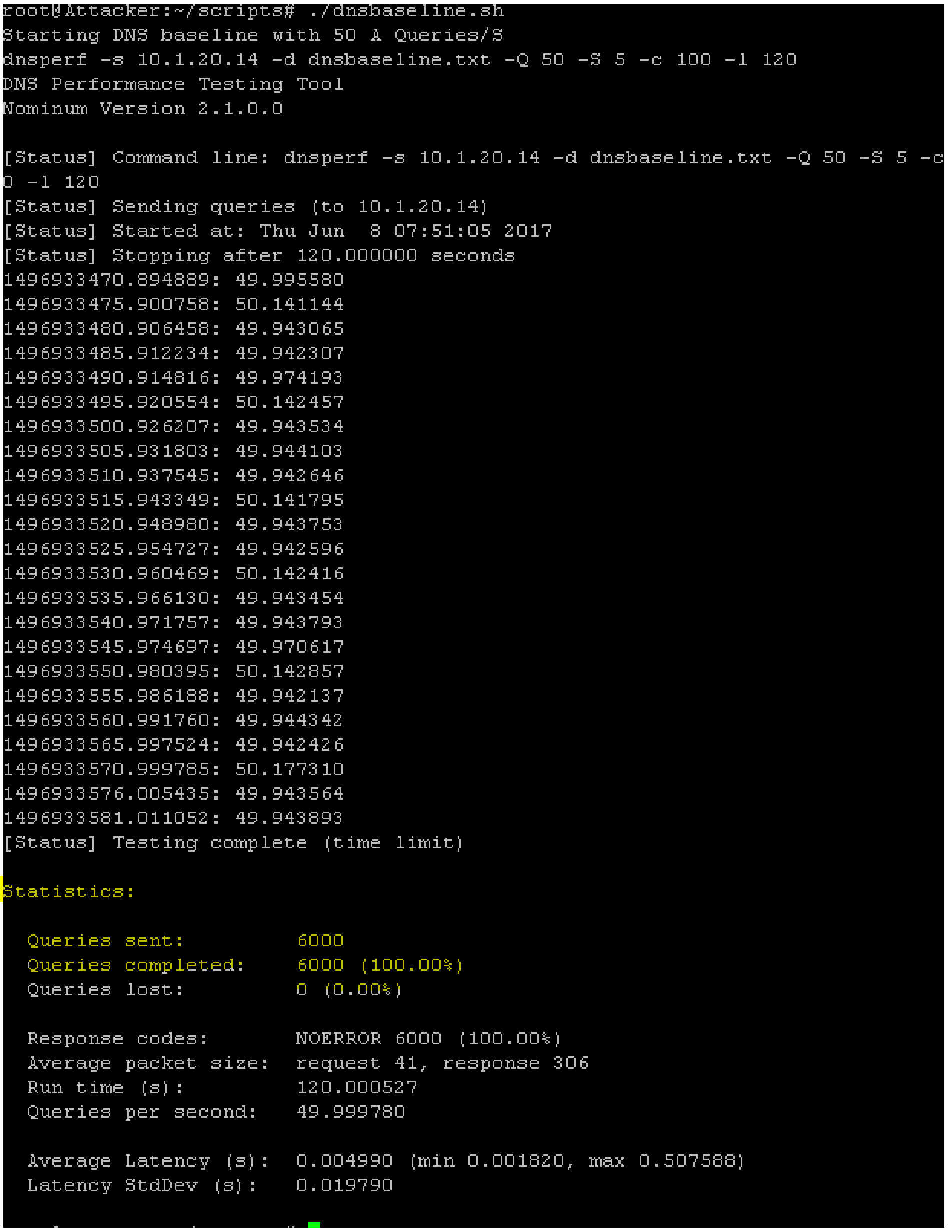
□ **Bad Actor Detection**

Task 2 – Establish a DNS Baseline

- In the **Attacker** putty window type (or copy and paste) the following command:

```
# sudo bash
# cd ~/scripts
# ./dnsbaseline.sh
```

- Continue to run the baseline until you get the following results:



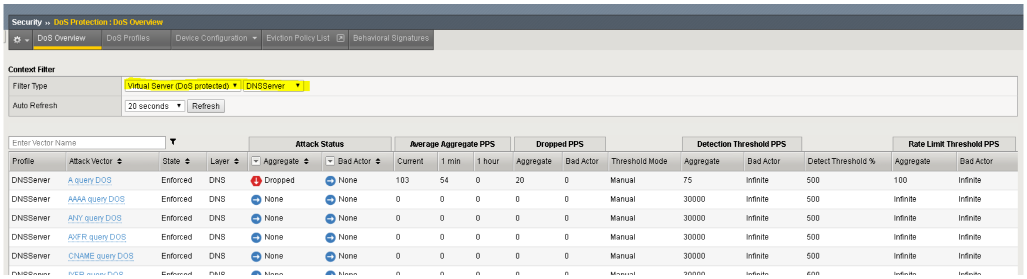
```
root@Attacker:~/scripts# ./dnsbaseline.sh
Starting DNS baseline with 50 A Queries/S
dnsperf -s 10.1.20.14 -d dnsbaseline.txt -Q 50 -S 5 -c 100 -l 120
DNS Performance Testing Tool
Nominum Version 2.1.0.0

[Status] Command line: dnsperf -s 10.1.20.14 -d dnsbaseline.txt -Q 50 -S 5 -c
0 -l 120
[Status] Sending queries (to 10.1.20.14)
[Status] Started at: Thu Jun  8 07:51:05 2017
[Status] Stopping after 120.000000 seconds
1496933470.894889: 49.995580
1496933475.900758: 50.141144
1496933480.906458: 49.943065
1496933485.912234: 49.942307
1496933490.914816: 49.974193
1496933495.920554: 50.142457
1496933500.926207: 49.943534
1496933505.931803: 49.944103
1496933510.937545: 49.942646
1496933515.943349: 50.141795
1496933520.948980: 49.943753
1496933525.954727: 49.942596
1496933530.960469: 50.142416
1496933535.966130: 49.943454
1496933540.971757: 49.943793
1496933545.974697: 49.970617
1496933550.980395: 50.142857
1496933555.986188: 49.942137
1496933560.991760: 49.944342
1496933565.997524: 49.942426
1496933570.999785: 50.177310
1496933576.005435: 49.943564
1496933581.011052: 49.943893
[Status] Testing complete (time limit)

Statistics:

  Queries sent:         6000
  Queries completed:    6000 (100.00%)
  Queries lost:         0 (0.00%)

  Response codes:       NOERROR 6000 (100.00%)
  Average packet size:  request 41, response 306
  Run time (s):         120.000527
  Queries per second:   49.999780

  Average Latency (s):  0.004990 (min 0.001820, max 0.507588)
  Latency StdDev (s):   0.019790
```

Task 3 – Initiate a DNS Attack that Exceeds the Rate Limit

- In the Attacker putty window type (or copy and paste) the following command:

  ```
  ./dnsdosrate.sh
  ```

- Wait for the attack to run for about 30 seconds before moving on.
- In the Configuration Utility, review the **DoS Overview** page



Context Filter

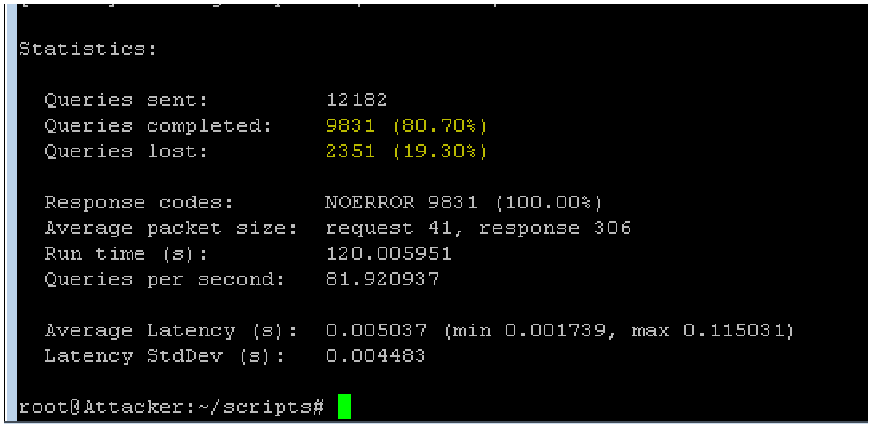
Filter Type: Virtual Server (DoS protected) ▾ DNSServer ▾

Auto Refresh: 20 seconds ▾

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
DNSServer	A query DOS	Enforced	DNS	Dropped	None	103	54	0	20	0	Manual	75	Infinite	500	100	Infinite
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	ANY query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	AXFR query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	CNAME query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	IXFR query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite

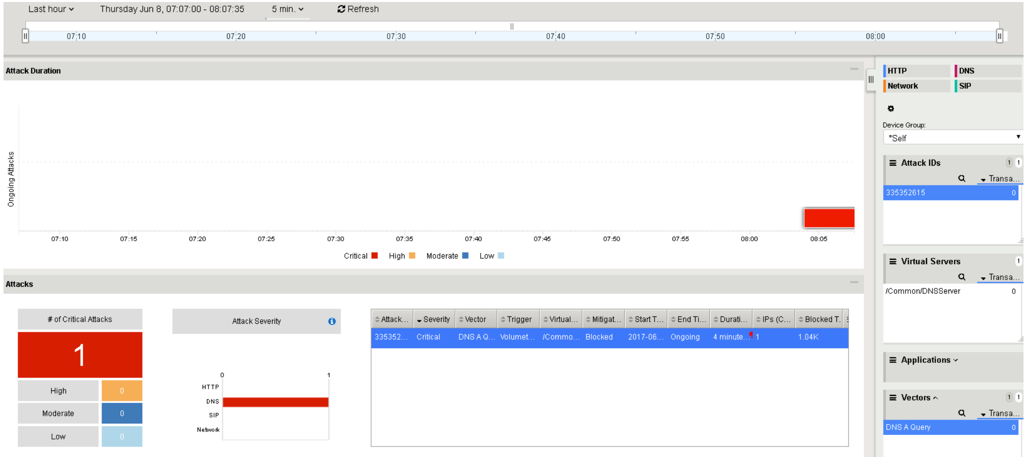
The **A query DOS** attack vector is now dropping attack traffic.

The script will also record the number of drops if any as a result of the attack rate limit being hit.



```
Statistics:

  Queries sent:           12182
  Queries completed:      9831  (80.70%)
  Queries lost:           2351  (19.30%)

  Response codes:         NOERROR 9831 (100.00%)
  Average packet size:    request 41, response 306
  Run time (s):           120.005951
  Queries per second:     81.920937

  Average Latency (s):    0.005037 (min 0.001739, max 0.115031)
  Latency StdDev (s):     0.004483

root@Attacker:~/scripts#
```

In the Configuration Utility open the **Statistics >>DoS Visibility** page. View details in various sections



Device Group: *Self

# of Critical Attacks	
1	
High	0
Moderate	0
Low	0

Attack...	Severity	Vector	Trigger	Virtual...	Mitigat...	Start T...	End Ti...	Durati...	IPs (C...	Blocked T.
335352...	Critical	DNS A Q...	Volumet...	/Commo...	Blocked	2017-06...	Ongoing	4 minute...	1	1.04K

Attack IDs 1 1 — Transa...
335352615 0

Virtual Servers 1 — Transa...
/Common/DNSServer 0

Applications

Vectors 1 1 — Transa...
DNS A Query 0

DNS Reverse flood

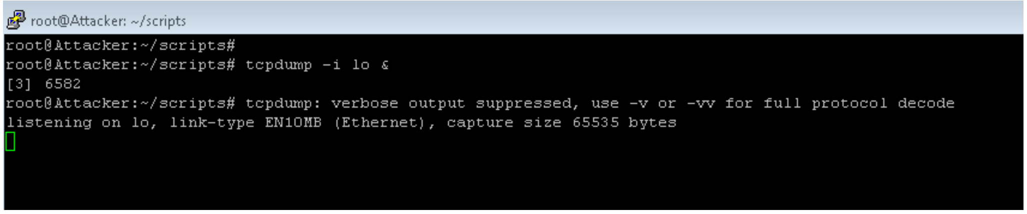
Sometimes DNS responses are used in flooding network resources. A small request has a disproportionately larger response and since the transport protocol is UDP it can easily be spoofed. The outbound pipe can easily get congested responding to a smaller number of requests with large responses.

Task 1 – View DNS Reverse Flood

Use **tcpdump** and **dig** to view DNS request and response packets. A small request produces a large response. You will **open two ssh** sessions to the **attacker**.

- Putty to the Attacker CLI (use the shortcut).
- Putty to the Attacker CLI (use the shortcut).
- In the **first ssh window** on the attacker start a tcpdump using the following command:

```
# sudo bash
# cd ~/scripts
# tcpdump -i lo &
```

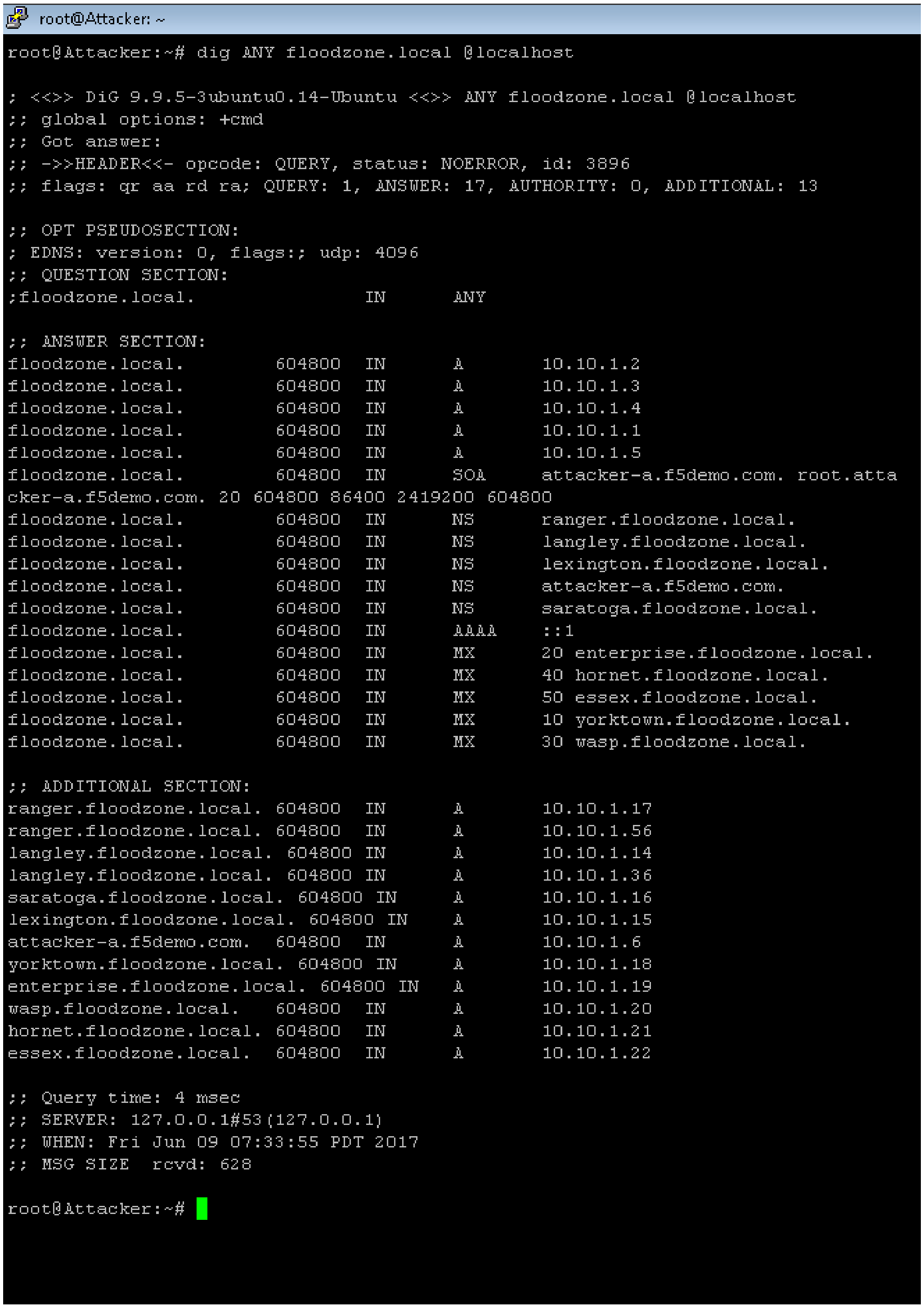


root@Attacker: ~/scripts

```
root@Attacker:~/scripts#
root@Attacker:~/scripts# tcpdump -i lo &
[3] 6582
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
```

- In the **second ssh** window on the attacker issue a dig against the loop back with “ANY”

```
# sudo bash
# cd ~/scripts
# dig ANY floodzone.local @localhost
```



```
root@Attacker:~# dig ANY floodzone.local @localhost

; <<>> DiG 9.9.5-3ubuntu0.14-Ubuntu <<>> ANY floodzone.local @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3896
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 17, AUTHORITY: 0, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;floodzone.local.               IN      ANY

;; ANSWER SECTION:
floodzone.local.        604800  IN      A       10.10.1.2
floodzone.local.        604800  IN      A       10.10.1.3
floodzone.local.        604800  IN      A       10.10.1.4
floodzone.local.        604800  IN      A       10.10.1.1
floodzone.local.        604800  IN      A       10.10.1.5
floodzone.local.        604800  IN      SOA     attacker-a.f5demo.com. root.atta
cker-a.f5demo.com. 20 604800 86400 2419200 604800
floodzone.local.        604800  IN      NS      ranger.floodzone.local.
floodzone.local.        604800  IN      NS      langley.floodzone.local.
floodzone.local.        604800  IN      NS      lexington.floodzone.local.
floodzone.local.        604800  IN      NS      attacker-a.f5demo.com.
floodzone.local.        604800  IN      NS      saratoga.floodzone.local.
floodzone.local.        604800  IN      AAAA    ::1
floodzone.local.        604800  IN      MX      20 enterprise.floodzone.local.
floodzone.local.        604800  IN      MX      40 hornet.floodzone.local.
floodzone.local.        604800  IN      MX      50 essex.floodzone.local.
floodzone.local.        604800  IN      MX      10 yorktown.floodzone.local.
floodzone.local.        604800  IN      MX      30 wasp.floodzone.local.

;; ADDITIONAL SECTION:
ranger.floodzone.local. 604800  IN      A       10.10.1.17
ranger.floodzone.local. 604800  IN      A       10.10.1.56
langley.floodzone.local. 604800 IN      A       10.10.1.14
langley.floodzone.local. 604800 IN      A       10.10.1.36
saratoga.floodzone.local. 604800 IN     A       10.10.1.16
lexington.floodzone.local. 604800 IN    A       10.10.1.15
attacker-a.f5demo.com.  604800  IN      A       10.10.1.6
yorktown.floodzone.local. 604800 IN     A       10.10.1.18
enterprise.floodzone.local. 604800 IN   A       10.10.1.19
wasp.floodzone.local.   604800  IN      A       10.10.1.20
hornet.floodzone.local. 604800  IN      A       10.10.1.21
essex.floodzone.local.  604800  IN      A       10.10.1.22

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jun 09 07:33:55 PDT 2017
;; MSG SIZE  rcvd: 628

root@Attacker:~#
```

- In the **first ssh window** on the attacker view the results of the tcpdump : Notice the difference in the **size of the request (44) vs the response (628).** Your values maybe different. The point is that a small request can generate an enormous response.

```
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or
-vv for full protocol decodelistening on lo, link-type EN10MB
(Ethernet), capture size 65535 bytes
```

```
07:33:55.737892 IP localhost.47406 > localhost.domain: 3896+ [1au] ANY?
floodzone.local. **(44)**

07:33:55.738563 IP localhost.domain > localhost.47406: 3896\* 17/0/13 A
10.10.1.2, A 10.10.1.3, A 10.10.1.4, A 10.10.1.1, A 10.10.1.5, SOA, NS
ranger.floodzone.local., NS langley.floodzone.local., NS
lexington.floodzone.local., NS attacker-a.f5d emo.com., NS
saratoga.floodzone.local., AAAA ::1, MX enterprise.floodzone.local. 20,
MX hornet.floodzone.local. 40, MX ess ex.floodzone.local. 50, MX
yorktown.floodzone.local. 10, MX wasp.floodzone.local. 30 **(628)**
```

- In the **second ssh** window on the attacker issue a dig against the loop back with "ANY" for a larger response.

```
# sudo bash
# cd ~/scripts
# dig ANY ripe.net @localhost +dnssec
```

- In the **first ssh window** on the attacker view the results of the tcpdump : Notice the difference in the size of the request **(37)** vs the response **(2715). Your values maybe different.** The point is that a small request can generate an enormous response.

```
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or
-vv for full protocol decode

listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes

07:43:44.018212 IP localhost.51272 > localhost.domain: 58304+ [1au] ANY?
ripe.net. **(37)**

07:43:44.018889 IP localhost.domain > localhost.51272: 58304$ 18/8/15
RRSIG, SOA, RRSIG, RRSIG, A 193.0.6.139, RRSIG, DNSKEY, DNSKEY, DNSKEY,
RRSIG, DS, NS manus.authdns.ripe.net., NS a2.verisigndns.com., NS
a1.verisigndns.com., NS tinnie.arin.net., NS sns-pb.isc.org., NS
sec3.apnic.net., NS a3.verisigndns.com. **(2715)**
```

- Once you're done, type '**fg**' and '**CTRL+C**' to stop the tcpdump.

```
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or
-vv for full protocol decode listening on lo, link-type EN10MB
(Ethernet), capture size 65535 bytes
```

fg

`tcpdump -i lo`

`^C`

```
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@Attacker:~/scripts#
```

This can easily overwhelm the server or overwhelm the outbound network pipe disrupting traffic responses for legitimate requests and/or other applications.

One industry accepted way to mitigate this type of attack is to rate limit the responses on the DNS servers. More information on Response Rate Limiting can be found here:

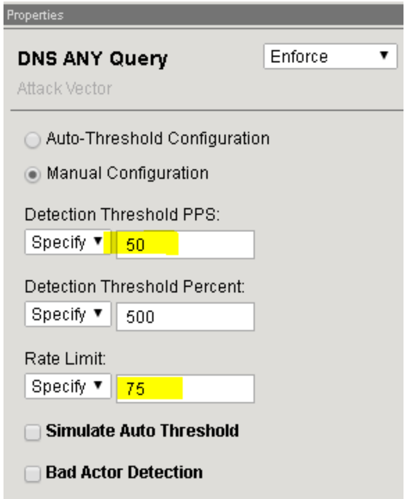
https://www.isc.org/wp-content/uploads/2014/11/DNS-RRL-LISA14.pdf

Because DoS policies are applied to traffic flows on ingress to the DHD, response rate limiting isn't currently available. But you still can limit the types of queries that can disproportionately consume bandwidth. The ANY query used in the previous example is one such example.

Task 2 – Use a Protected Object to Mitigate a DNS Reverse Query Flood

- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page
- In the **Protected Objects** section click **DNSServer**.
- In the **DNS** row click the **+** icon, and then click **DNS ANY Query.**
- On the right-side of the page configure using the following information, and then click **Update**.

Detection Threshold PPS	Specify: 50
Detection Threshold Percent	Specify: 500
Rate Limit	Specify: 75



DNS ANY Query — Enforce
Attack Vector

○ Auto-Threshold Configuration
● Manual Configuration

Detection Threshold PPS: Specify 50

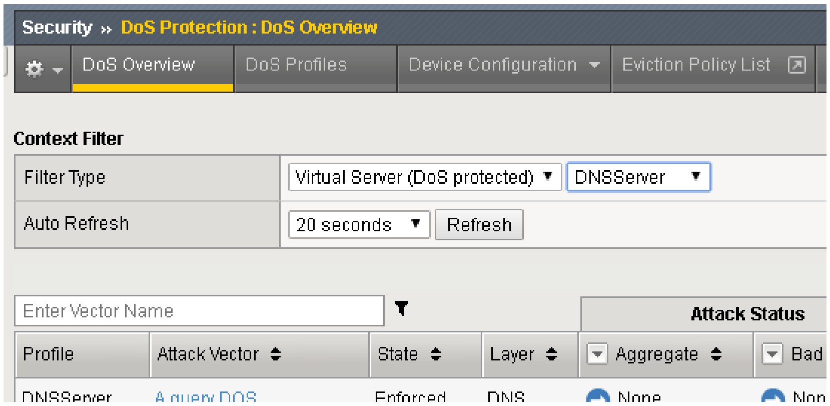
Detection Threshold Percent: Specify 500

Rate Limit: Specify 75

□ Simulate Auto Threshold

□ Bad Actor Detection

- In the BIG-IP Configuration Utility, open the **Security>>DoS Protection>> DoS Overview** page and set the **Filter type** to "**Virtual Server (DoS protected)** / **DNSServer**" Set **Auto-Refresh** to **20 seconds**.



Context Filter

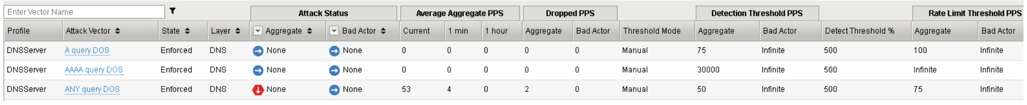
Filter Type	Virtual Server (DoS protected) / DNSServer
Auto Refresh	20 seconds — Refresh

Profile	Attack Vector	State	Layer	Aggregate	Bad
DNSServer	A query DOS	Enforced	DNS	None	Non

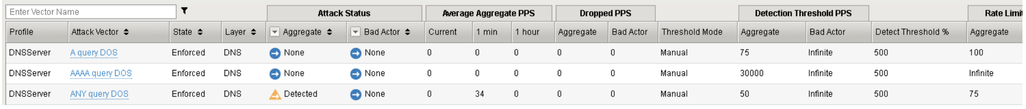
- In the **attacker** ssh window issue dns reverse flood attack as follows:

```
# sudo bash
# cd ~/scripts
# ./dnsReverseFlood.sh
```

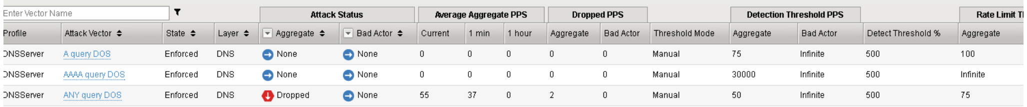
- Observe the DoS Overview as it gradually starts to drop the ANY queries.



Enter Vector Name				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
DNSServer	A query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	75	Infinite	500	100	Infinite
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	ANY query DOS	Enforced	DNS	None	None	53	4	0	2	0	Manual	50	Infinite	500	75	Infinite



Enter Vector Name				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limi
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate
DNSServer	A query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	75	Infinite	500	100
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite
DNSServer	ANY query DOS	Enforced	DNS	⚠ Detected	None	0	34	0	0	0	Manual	50	Infinite	500	75



Enter Vector Name				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit T
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate
DNSServer	A query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	75	Infinite	500	100
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite
DNSServer	ANY query DOS	Enforced	DNS	Dropped	None	55	37	0	2	0	Manual	50	Infinite	500	75

- In the **attacker** ssh window stop the attack by hitting “**CTRL+C**” many times

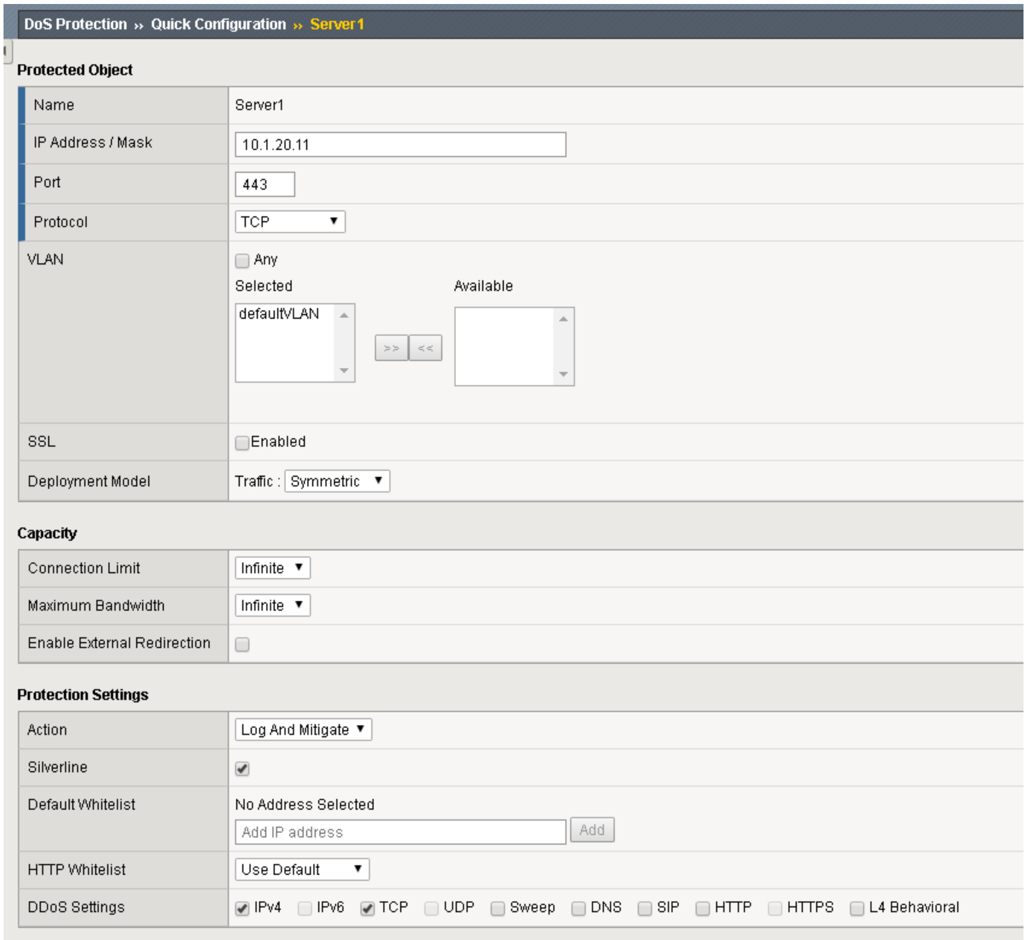
3.1.6 Lab 6 – Configuring L7 Attack Protection

In this exercise we will use a protected object and enforce mitigation for low and slow/encrypted layer 7 attacks.

Task 1 – Create Protected Object and Launch Attack

- In the BIG-IP Configuration Utility, open the **DoS Protection** > **Quick Configuration** page and in the Protected Objects section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	Server1
IP Address	10.1.20.11
Port	443
VLAN (Selected)	defaultVLAN (uncheck ANY)
Protection Settings: Action	Log and Mitigate
Protection Settings: Silverline	Yes (selected)
Protection Settings: DDoS Settings	IPv4, TCP



DoS Protection » Quick Configuration » Server1

Protected Object

Name	Server1
IP Address / Mask	10.1.20.11
Port	443
Protocol	TCP ▼
VLAN	□ Any Selected: defaultVLAN Available:
SSL	□ Enabled
Deployment Model	Traffic : Symmetric ▼

Capacity

Connection Limit	Infinite ▼
Maximum Bandwidth	Infinite ▼
Enable External Redirection	□

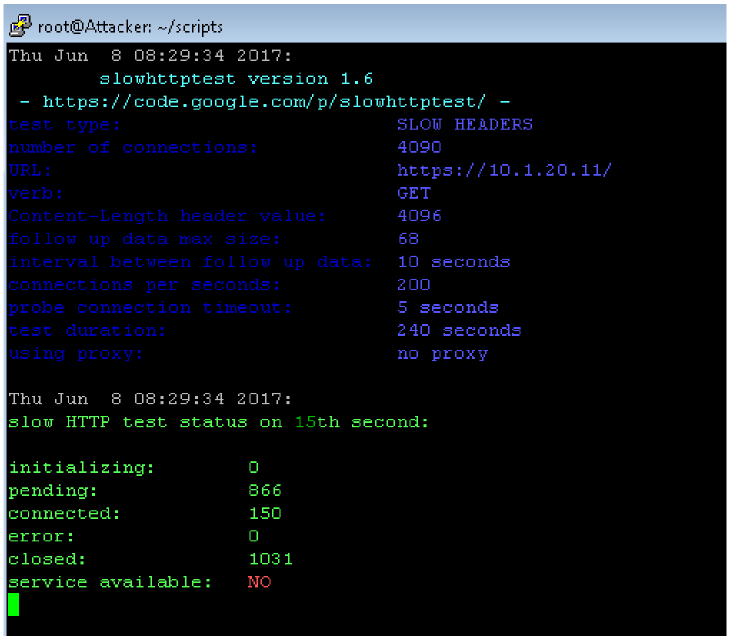
Protection Settings

Action	Log And Mitigate ▼
Silverline	☑
Default Whitelist	No Address Selected Add IP address [Add]
HTTP Whitelist	Use Default ▼
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

- Launch attacks without any layer 7 protection configured
- Open the following in separate tabs in the Hybrid Defender WebUI:
- **DoS Protection>>Quick Configuration**
- **Security>>Reporting>>DoS>>Analysis**
- From a **firefox browser** go to https://10.1.20.11. Ignore SSL warning and Add Exception. Note that this bypasses the Hybrid Defender and accesses the server directly, showing the availability and/or performance of the site directly. Click around a few links. This is the site we will launch an attack against and mitigate.
- Verify that the configuration is providing no L7 protections by taking the server offline with a slowloris attack. Note that apache will try to clean up the slow flows, but they will do so inefficiently and the server is impacted (which will show as an outage, missing objects and/or slower responsiveness). Run the slowloris attack from the Attacker CLI:

```
# sudo bash
# cd ~/scripts
# ./slowloris.sh
```

The tool will rapidly show the site offline (10-15 seconds, with trivial traffic load):

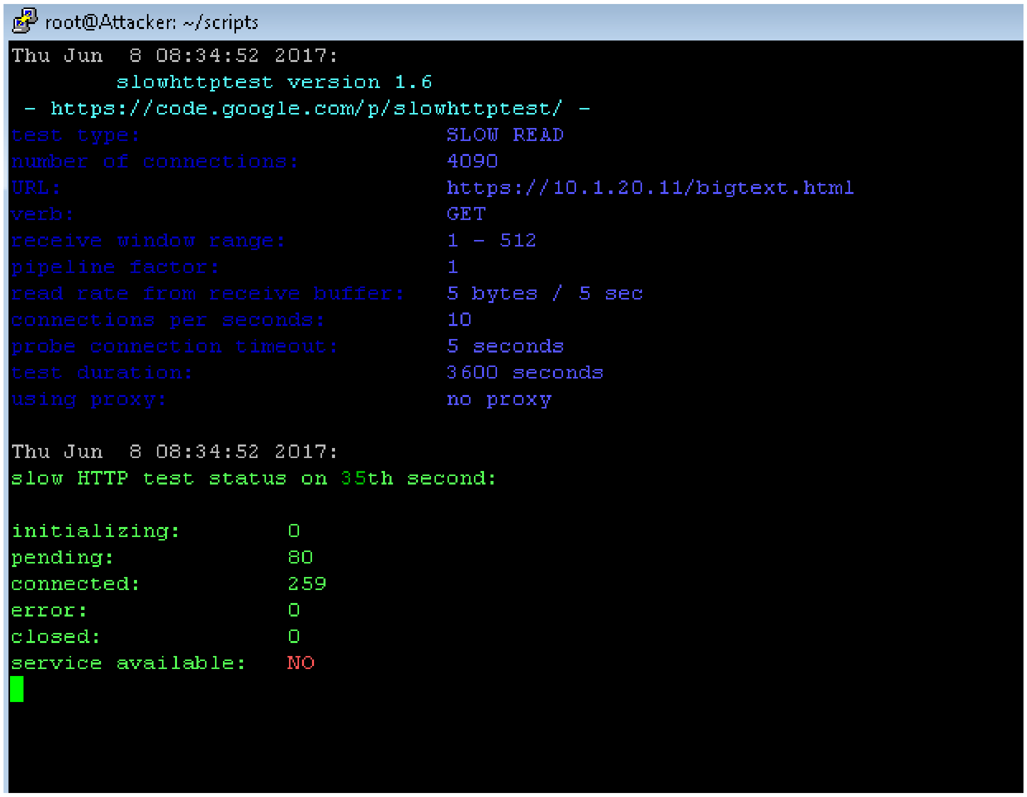


```
Thu Jun  8 08:29:34 2017:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                          SLOW HEADERS
number of connections:              4090
URL:                                https://10.1.20.11/
verb:                               GET
Content-Length header value:        4096
follow up data max size:            68
interval between follow up data:    10 seconds
connections per seconds:            200
probe connection timeout:           5 seconds
test duration:                      240 seconds
using proxy:                        no proxy

Thu Jun  8 08:29:34 2017:
slow HTTP test status on 15th second:

initializing:        0
pending:             866
connected:           150
error:               0
closed:              1031
service available:   NO
```

- Refresh https://10.1.20.11 to show the effects of the attack. [Note that since we are running locally from the Win7 system in a virtualized environment, you may be able to access the site, however it will be slower and often the GIFs will not load. An internet user would not be able to “fight through” the attack to get to the server as often as a system on the local LAN.]
- Stop the slowloris attack by using CTRL+C.
- Start a more effective Slow Read attack.

  This attack is harder for DoS mitigation tools to mitigate and can be very effective even with a tiny number of concurrent connections trickling in very slowly to the server to fly below the radar of network detections. In our example we will open 10 connections per second and read the response data at 1 byte / sec. The attack would be effective even at 1 cps, it would just take a bit longer to build up the connections.
- From the **Attacker** CLI/shell start the slowread attack:

```
# sudo bash
# cd ~/scripts
# ./slowread.sh
```

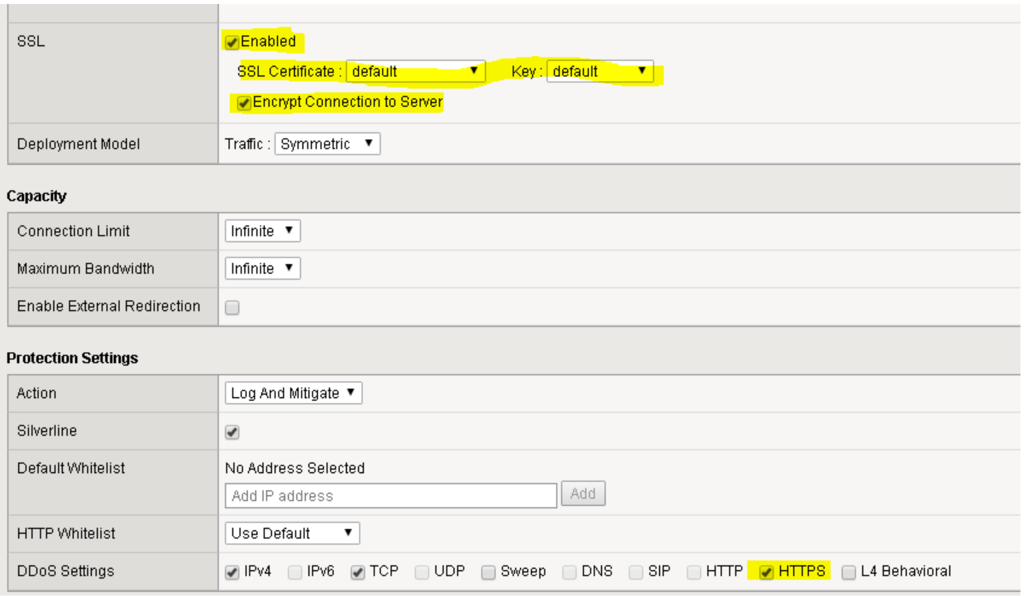


```
root@Attacker: ~/scripts
Thu Jun  8 08:34:52 2017:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW READ
number of connections:            4090
URL:                              https://10.1.20.11/bigtext.html
verb:                             GET
receive window range:             1 - 512
pipeline factor:                  1
read rate from receive buffer:    5 bytes / 5 sec
connections per seconds:          10
probe connection timeout:         5 seconds
test duration:                    3600 seconds
using proxy:                      no proxy

Thu Jun  8 08:34:52 2017:
slow HTTP test status on 35th second:

initializing:        0
pending:             80
connected:           259
error:               0
closed:              0
service available:   NO
```

As soon as the site is down (service available: NO), refresh https://10.1.20.11 to show that it is down/slow/intermittent.

Task 2 – Configure Protection/Mitigation, launch attack and view reports

- In the Hybrid Defender WebUI, access the **Server1** Protected Object.
- Enable SSL.
- Select the default certificate and key. In your environment you would select a valid/cert key for your application.
- Enable '**Encrypt Session to Server**' to avoid any server reconfiguration.
- Enable the **HTTPS** mitigation family.
- Click **Update**.



SSL	☑ Enabled SSL Certificate : default ▼ Key : default ▼ ☑ Encrypt Connection to Server
Deployment Model	Traffic : Symmetric ▼

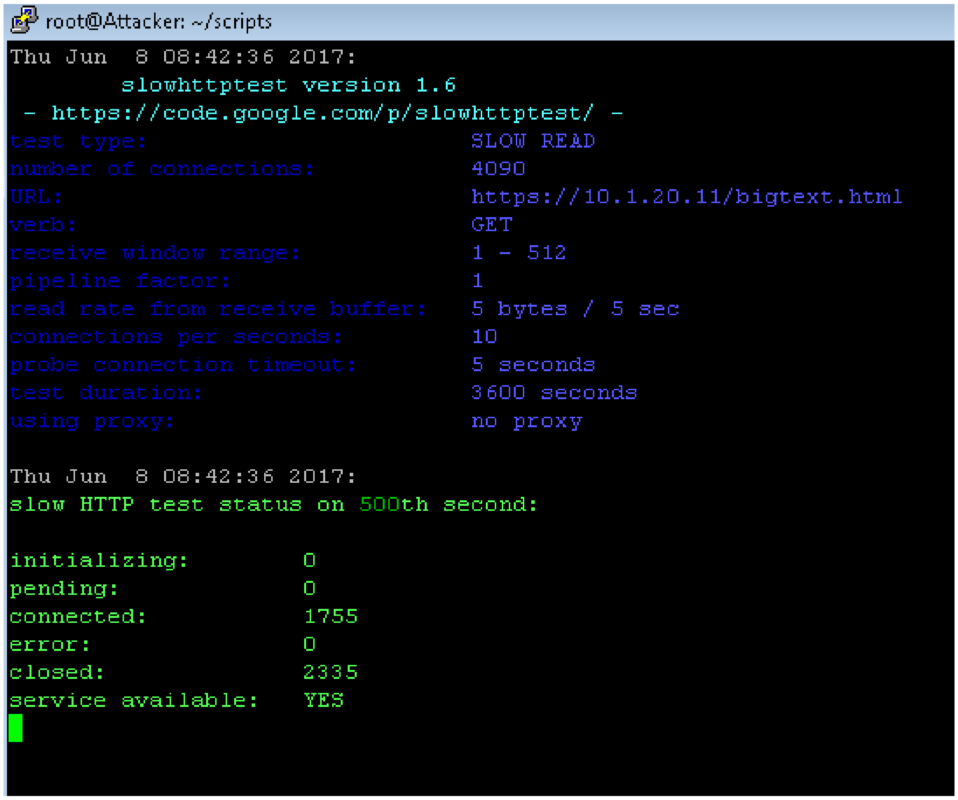
Capacity

Connection Limit	Infinite ▼
Maximum Bandwidth	Infinite ▼
Enable External Redirection	□

Protection Settings

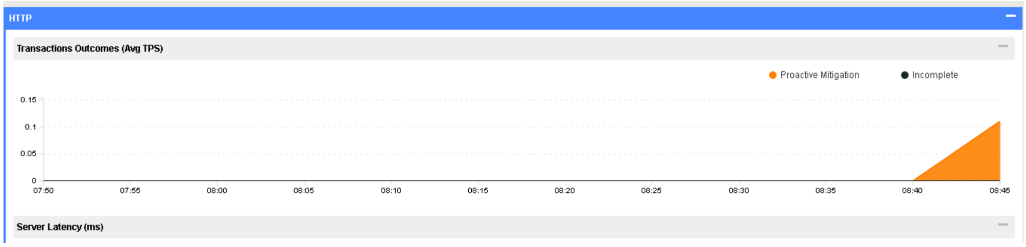
Action	Log And Mitigate ▼
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default ▼
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP ☑ HTTPS □ L4 Behavioral

- View the Attacker CLI/shell. The slow read attack is now no longer showing the site as down (service available: YES) because Proactive Bot Detection has mitigated the attack.



```
root@Attacker: ~/scripts
Thu Jun  8 08:42:36 2017:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW READ
number of connections:            4090
URL:                              https://10.1.20.11/bigtext.html
verb:                             GET
receive window range:             1 - 512
pipeline factor:                  1
read rate from receive buffer:    5 bytes / 5 sec
connections per seconds:          10
probe connection timeout:         5 seconds
test duration:                    3600 seconds
using proxy:                      no proxy

Thu Jun  8 08:42:36 2017:
slow HTTP test status on 500th second:

initializing:        0
pending:             0
connected:           1755
error:               0
closed:              2335
service available:   YES
```

- Refresh https://10.1.20.11 to see that the site behavior has returned to normal.
- You were able to mitigate an encrypted layer 7 attack quickly and with only a few simple steps.
- In the Hybrid Defender WebUI, view various reports in the **Security>>Reporting>>DoS>>Analysis**
- **HTTP Report (Scroll towards the bottom) shows Proactive Mitigation**.



- Stop the Slow Read attack by using CTRL+C.

This concludes your hands on labs. In this class you learned how to mitigated various DDoS attacks using F5 BIGIP Hybrid Defender (DHD).

4

Class 3: DDoS Hybrid Defender

DDoS Hybrid Defender, a hybrid DDoS solution that offers comprehensive protection, high availability, and is easy to deploy and manage. It guards against aggressive volumetric and targeted DDoS attacks, includes hardware-assisted DDoS mitigation, and optionally, connects with Silverline, a cloud-based scrubbing service.

This class covers the following topics:

- Initial Set-up, Device Configuration and working with basic device-level DDoS vectors to mitigate the most commonly encountered attacks. Then we will cover Auto-thresholding, bad actor detection, DNS reflection and amplification, real-time blackholing, mitigation of L7 floods, low-and-slow attacks and behavioral attacks.

4.1 DDoS Hybrid Defender Setup

In this module you will learn how to complete the setup of F5 Networks DDoS Hybrid Defender

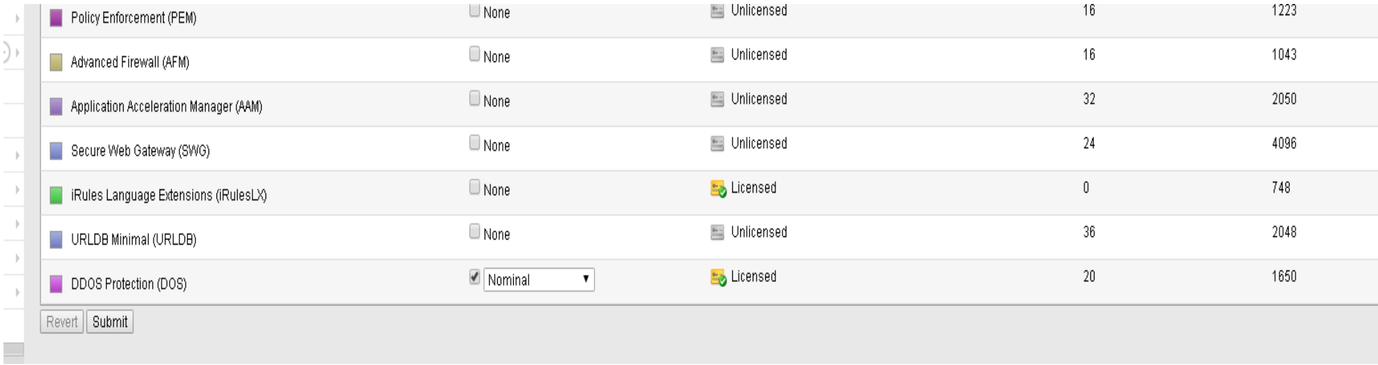
4.1.1 Lab 1 – DDoS Hybrid Defender Setup

Task 1 – Initial Set-up

- Login to the BIG-IP Configuration Utility via the desktop shortcut (DHD WEB GUI). You will land on the welcome page.

Note: When you first power up a F5 DHD device you would go through the steps of Licensing and Provisioning. We have assigned the management IP, hostname, NTP and DNS servers. We have already licenesed the device for you.

- Review and Verify the following: **System -> Configuration -> Device -> NTP** page. This should be already populated with **pool.ntp.org**
- Review and Verify the following: **System -> Configuration -> Device ->DNS** page. This should be already populated with 8.8.8.8
- Click **System** and explore **Resource Provisioning** page.

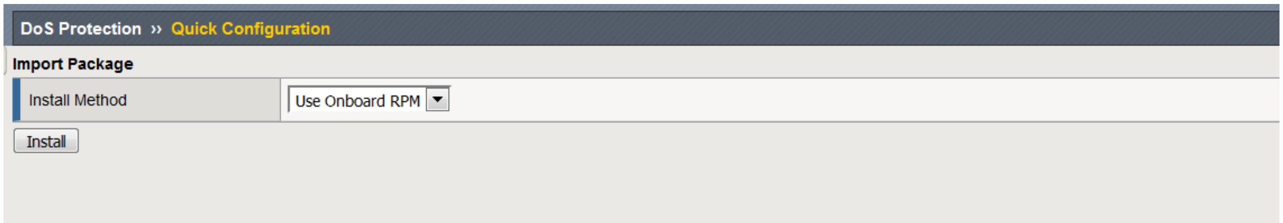


Policy Enforcement (PEM)	□ None	Unlicensed	16	1223
Advanced Firewall (AFM)	□ None	Unlicensed	16	1043
Application Acceleration Manager (AAM)	□ None	Unlicensed	32	2050
Secure Web Gateway (SWG)	□ None	Unlicensed	24	4096
iRules Language Extensions (iRulesLX)	□ None	Licensed	0	748
URLDB Minimal (URLDB)	□ None	Unlicensed	36	2048
DDOS Protection (DOS)	☑ Nominal	Licensed	20	1650

Note: The above task ensures that you are using a purpose built DDoS Hybrid Defender. If you are familiar with other F5 Modules/Technology that you have used in the past, you will notice that we have none of those provisioned. We have a new section DDOS Protection only.

Task 2 – DDoS Hybrid Defender iApp and Base Configuration

- In the BIG-IP Configuration Utility, open **DoS Protection** > **Quick Configuration** page.
- If not already installed, Select Install RPM method of Onboard.
- Click **Install**.

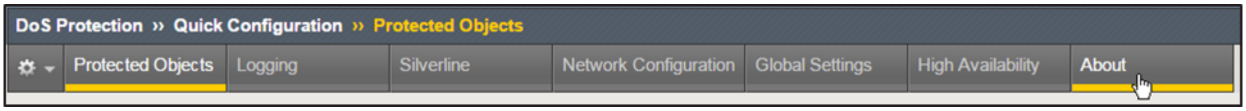


DoS Protection » Quick Configuration

Import Package

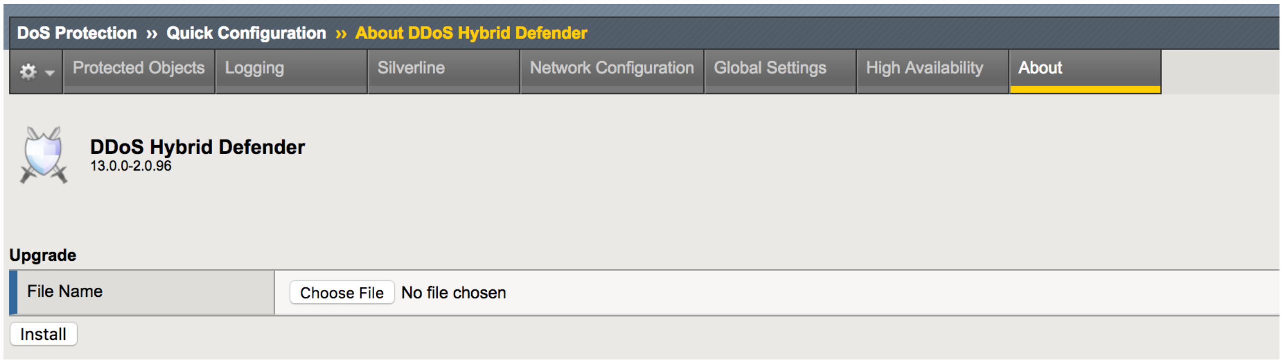
Install Method: Use Onboard RPM

- After the RPM is installed you will see the following:
- Open the About page.



DoS Protection » Quick Configuration » Protected Objects

- This page displays the current version of DDoS Hybrid Defender (DHD). You use this page to install and update the iApp LX version for DHD when newer versions are released.



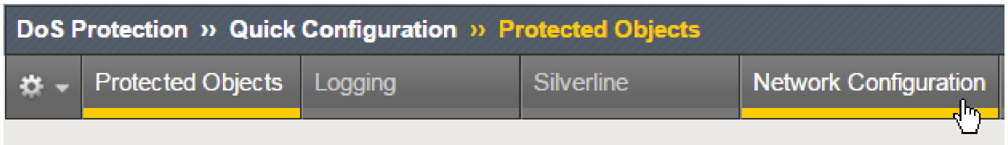
DoS Protection » Quick Configuration » About DDoS Hybrid Defender

DDoS Hybrid Defender
13.0.0-2.0.96

Upgrade

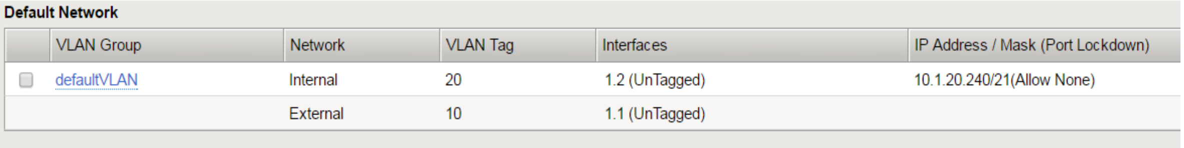
File Name: Choose File No file chosen

- Open the **DoS Protection > Quick Configuration Network Configuration** page.



- In the Default Network section click **default VLAN**.
- Configure the VLANs using following information, and then click **Done Editing**.

Internal: VLAN Tag	20
Internal: Interfaces	1.2 Untagged
Internal: IP Address / Mask	10.1.20.240/21 (Click **Add**)
External: VLAN Tag	10
External: Interfaces	1.1 Untagged (Click **Add**)



Default Network

	VLAN Group	Network	VLAN Tag	Interfaces	IP Address / Mask (Port Lockdown)
□	defaultVLAN	Internal	20	1.2 (UnTagged)	10.1.20.240/21(Allow None)
		External	10	1.1 (UnTagged)	

- At the bottom of the page click **Update** to create the default network.
- Open the **Network > VLANs > VLAN Groups** page and click **defaultVLAN**.

Note: A Bridged (VLAN Group) L2 configuration consistent with recommended practices for most deployments was automatically created. Also called “Bump in the Wire”. F5 can support Routed mode, SPAN and Netflow as well.

- Open the **Network > DNS Resolvers > DNS Resolver** list page and click **Create**.
- Enter **default_DNS_resolver** and then click **Finished**.
- A DNS resolver is required by bot signatures to allow for proper detection of benign search engines such as Google and Bing.
- On the Jumpbox desktop, SSH to the BIG-IP, it will log you in automatically as user `root`, using the shortcut.
- Verify DNS by typing the following:

  ```
  nslookup api.f5silverline.com
  ```

- Verify the Date by typing the following:

  ```
  date
  ```

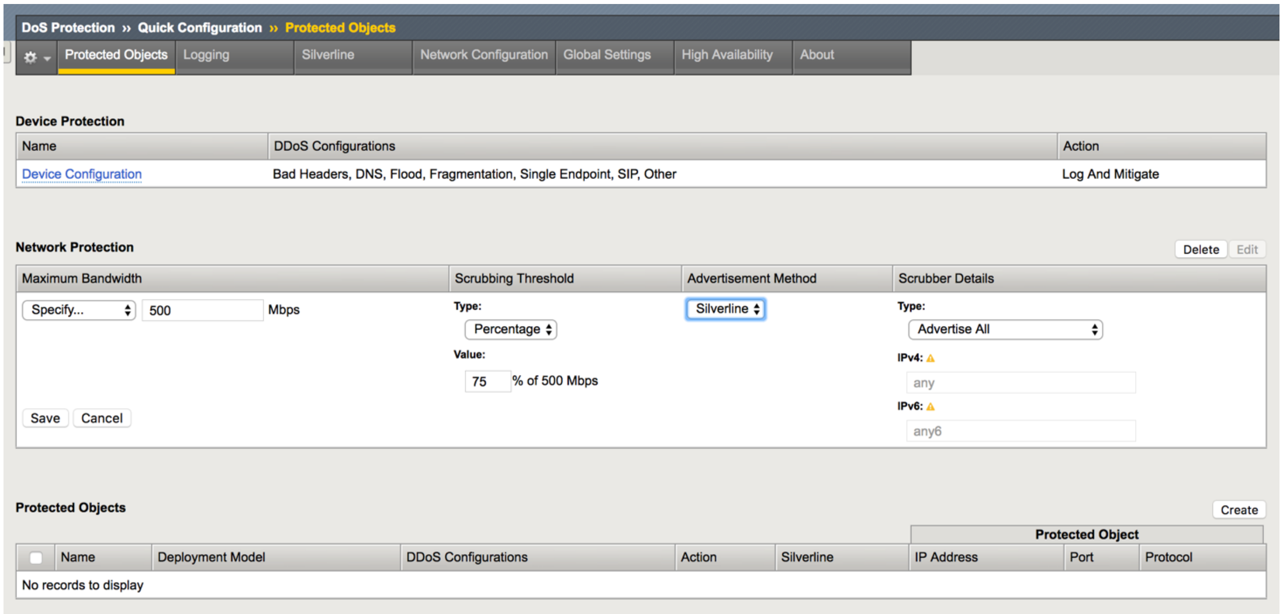
- If the BIG-IP system date is not accurate, correct it using the following commands:

```
bigstart stop ntpd
ntpdate 10.1.1.254
bigstart start ntpd
```

Task 3 – Explore DHD Device Bandwidth Thresholds

- In the **DoS Protection > Quick Configuration** page, open the **Protected Objects** page.

- In the **Network Protection** section click **Create**.
- This page is where you would supply values to protect your bandwidth and integrate with Silverline or use BGP to change your routing to go through a scrubbing center.
- Click **Cancel** when done exploring the available settings.



DoS Protection » Quick Configuration » Protected Objects

Device Protection

Name	DDoS Configurations	Action
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other	Log And Mitigate

Network Protection

Maximum Bandwidth	Scrubbing Threshold	Advertisement Method	Scrubber Details
Specify... 500 Mbps	Type: Percentage Value: 75 % of 500 Mbps	Silverline	Type: Advertise All IPv4: any IPv6: any6

Protected Objects

						Protected Object		
□	Name	Deployment Model	DDoS Configurations	Action	Silverline	IP Address	Port	Protocol
No records to display								

- That completes the initial setup for BIG-IP DDoS Hybrid Defender.

4.1.2 Lab 2 – Configuring Hybrid Defender DDoS protection

Task 1 – Disable Device-Level DHD DoS Protection

In this lab you will disable **Device-level** DoS flood protection, and then issue an ICMPv4 flood and review the results.

- **PuTTY** to the **BIG-IP CLI** (10.1.1.245) from your jumpbox desktop shortcut and resize window by making it wider. You will be logged on as `root`.
- At the **config** prompt, type (or copy and paste) the following command:

```
tcpdump -i 0.0 host 10.1.20.12
```

- **PuTTY** to the **Attacker** host from your jumpbox desktop shortcut. You will be logged in as **root**. I't will use **a pre-loaded public key** as the credentials. Accept the warning.
- At the **config** prompt, type (or copy and paste) the following command:

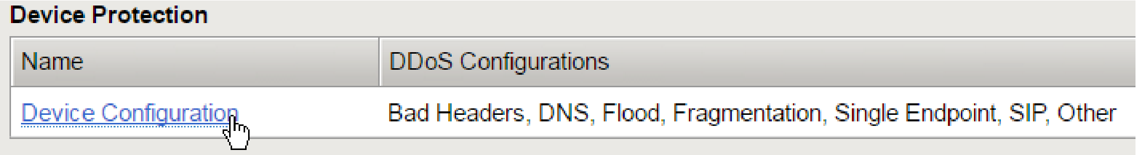
```
ping 10.1.20.12
```

The attacker can successfully communicate with a back-end resource behind the BIG-IP DHD.

- Examine the **tcpdump** window and verify ICMP packets are flowing through the BIG-IP DHD.

Note: The listener for the ICMP packets is the VLAN group.

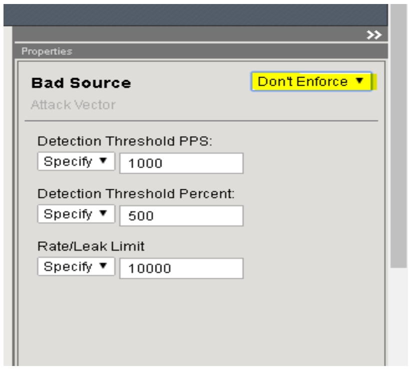
- Cancel the `ping` command, then verify the `tcpdump` stops receiving ICMP packets, and then press **Enter** several times to clear the recent log entries.
- In the Configuration Utility, in the **DoS Protection, Quick Configuration, Device Protection** section click **Device Configuration**.



Device Protection

Name	DDoS Configurations
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other

- In the **Bad Headers** row click the **+** icon, and then click **Bad Source**.
- On the right-side of the page select the drop-down to "Don't Enforce"



Properties

Bad Source
Attack Vector
Don't Enforce ▾

Detection Threshold PPS:
Specify ▾ 1000

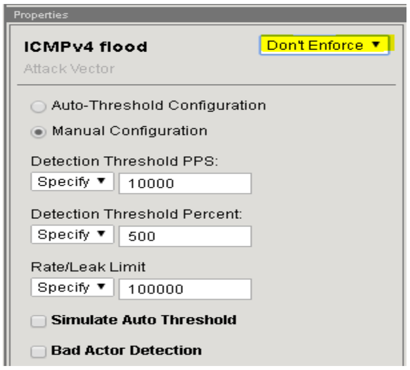
Detection Threshold Percent:
Specify ▾ 500

Rate/Leak Limit
Specify ▾ 10000

- In the **Flood** row click the **+** icon, and then click **ICMPv4 flood**.

Note: If you minimize by clicking the + icon, it will make seeing the other sections easier.

- On the right-side of the page select the drop-down to "Don't Enforce"



Properties

ICMPv4 flood
Attack Vector
Don't Enforce ▾

○ Auto-Threshold Configuration
● Manual Configuration

Detection Threshold PPS:
Specify ▾ 10000

Detection Threshold Percent:
Specify ▾ 500

Rate/Leak Limit
Specify ▾ 100000

□ Simulate Auto Threshold
□ Bad Actor Detection

- Apply the settings above for **TCP SYN flood** and **UDP Flood** and then click **Update**.
- On the Jumpbox in the **Attacker** PuTTY window type (or copy and paste) the following:

```
# cd scripts
# ls
```

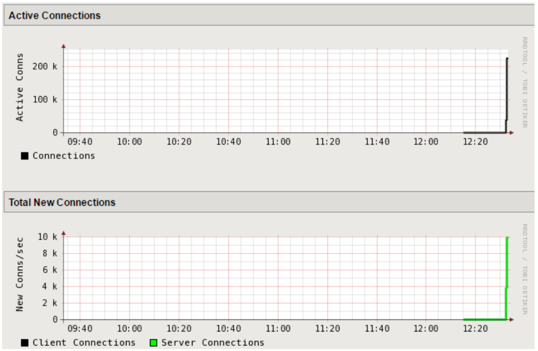
These are the different scripts we'll be using during the exercises to simulate DoS attacks.

- Type (or copy and paste) the following commands:

  `for i in {1..10}; do ./icmpflood.sh; done`

This script launches 1,000,000 ICMP requests and then repeats for a total of ten occurrences.

- View the `tcpdump` window and verify that ICMP attack traffic is reaching the back-end server.
- Let the attack run for about 15 seconds before moving on.
- In the Configuration Utility, open the **Statistics > Performance > Performance** page.
- View the Active Connections and Total New Connections charts.
- There is a drastic spike in active connections.



- View the Throughput (bits) and Throughput (packets) charts.

There is also a drastic spike in both bits per second and packets per second.

- Open the **Security > Event Logs > DoS > Network > Events** page.

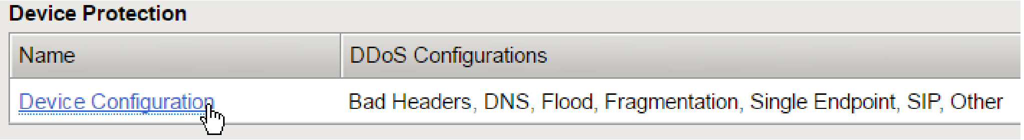
The log file is empty as we disabled device-level flood protection on BIG-IP DHD.

- On the Jumpbox **Attacker** shell slowly type **Ctrl + C** several times until back at the `scripts` prompt.

Task 2 – Re-enable Device-Level DHD DoS Protection

In this task you will re-configure **device-level** DoS protection, and then issue an ICMPv4 flood and review the results.

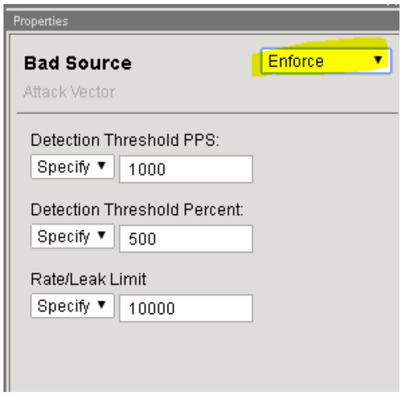
- In the Configuration Utility, in the **Device Protection** section click **Device Configuration.**



Device Protection

Name	DDoS Configurations
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other

- In the **Bad Headers** row click the + icon, and then click **Bad Source**.
- On the right-side of the page select the drop-down to “**Enforce**”



Properties

Bad Source — Enforce ▾

Attack Vector

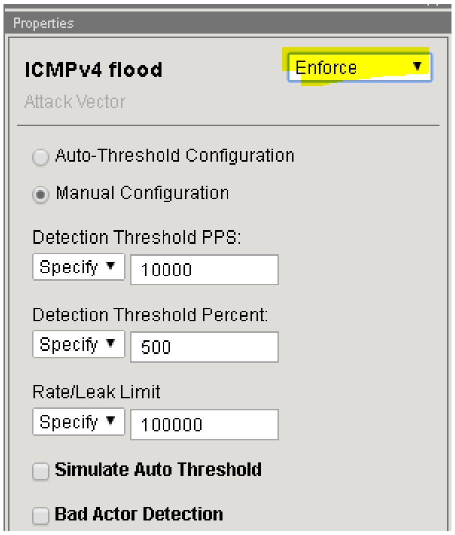
Detection Threshold PPS: Specify ▾ 1000

Detection Threshold Percent: Specify ▾ 500

Rate/Leak Limit Specify ▾ 10000

Note: Bad Source is enabled to be able to add the IP addresses to the blacklist.

- In the **Flood** row click the + icon, and then click **ICMPv4** flood.
- On the right-side of the page select the drop-down to **"Enforce"**



Properties

ICMPv4 flood — Enforce ▾

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS: Specify ▾ 10000

Detection Threshold Percent: Specify ▾ 500

Rate/Leak Limit Specify ▾ 100000

□ **Simulate Auto Threshold**

□ **Bad Actor Detection**

- Apply the settings above for **TCP SYN flood** and **UDP Flood** and then click **Update**.

Note: This returns the configuration back to factory supplied device level enforcement.

Task 3 – Configure Protected Object-Level IPv4 Flood DHD DoS Protection

The DHD device wide protection is enforced for all traffic flowing through the device. For more granular control, we use **protected objects** and configure mitigation settings for those objects to be enforced. In this task you will configure **object-level** DoS IPv4 flood protection, and then issue an ICMPv4 flood and review the results.

- On the Protect Objects page, in the Protected Objects section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	ServerNet
IP Address	10.1.20.0/24
Port	*
Protocol	All Protocols
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	IPv4

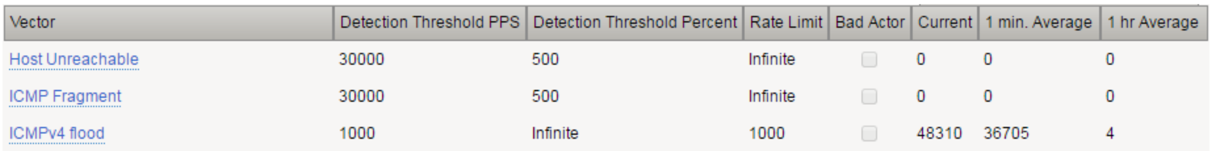
- In the **IPv4** row click the **+** icon, and then click **ICMPv4 flood**.
- On the right-side of the page configure using the following information, and then click **Create** at the bottom of the page.

Detection Threshold PPS	Specify: 1000
Detection Threshold Percent	Infinite
Rate/Leak Limit	Specify: 1000

- On the Jumpbox in the **Attacker** PuTTY window re-run the following command:

```
for i in {1..10}; do ./icmpflood.sh; done
```

- Examine the `tcpdump` window to see if there are any ICMP packets hitting the back-end server.
- Let the attack run for about 30 seconds before moving on.
- In the Configuration Utility, click **DoS Protection** > **Quick Configuration** > **ServerNet**, and then in the **IPv4** row click the **+** icon.



Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
Host Unreachable	30000	500	Infinite	☐	0	0	0
ICMP Fragment	30000	500	Infinite	☐	0	0	0
ICMPv4 flood	1000	Infinite	1000	☐	48310	36705	4

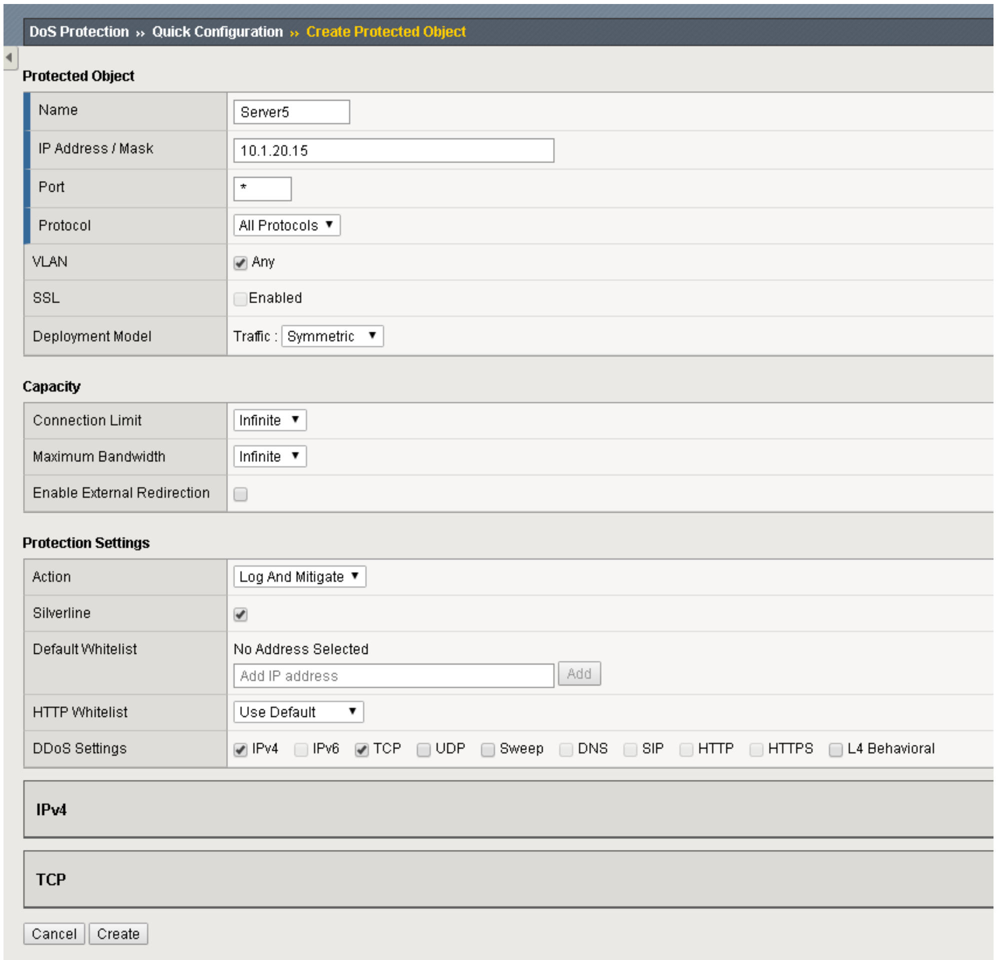
- Open the **Security** > **Event Logs** > **DoS** > **Network** > **Events** page.
- The DoS Source is **Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS**.
- The context column displays /**Common**/**ServerNet**, identifying this is protected object-level protection.
- The action is **Drop**.
- On the Jumpbox Attacker shell slowly type **Ctrl + C** several times until back at the `scripts` prompt.
- In the BIG-IP CLI type **Ctrl + C** to stop the tcpdump.

4.1.3 Lab 3 – Start Baseline Traffic Generation

Task 1 – Create Protected Objects that the baseline traffic will be targeting

- In the BIG-IP Configuration Utility, open the **DoS Protection>>Quick Configuration** page and in the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	Server5
IP Address	10.1.20.15
Port	*
Protocol	All Protocols
VLAN	Any
Protection Settings: Action	Log and Mitigate
Protection Settings: Silverline	(un-selected)
Protection Settings: DDoS Settings	IPv4, TCP



DoS Protection » Quick Configuration » Create Protected Object

Protected Object

Name	Server5
IP Address / Mask	10.1.20.15
Port	*
Protocol	All Protocols ▼
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric ▼

Capacity

Connection Limit	Infinite ▼
Maximum Bandwidth	Infinite ▼
Enable External Redirection	□

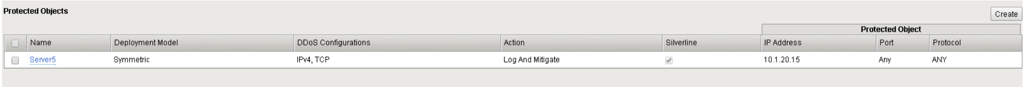
Protection Settings

Action	Log And Mitigate ▼
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default ▼
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

IPv4

TCP

- This protected object will be used for the Auto-Thresholding lab.



Protected Objects

						Protected Object		
□	Name	Deployment Model	DDoS Configurations	Action	Silverline	IP Address	Port	Protocol
□	Server5	Symmetric	IPv4, TCP	Log And Mitigate	✓	10.1.20.15	Any	ANY

Task 2 – Run Scripts to start L4 traffic generation – Good Traffic

- Putty SSH (use the desktop shortcut) to open a shell to the **good client system**.
- Accept the SSH Warning.
- You will be logged in as user : `root`. The session is preconfigured to authenticate with a certificate.

- Start the auto-threshold baselining script with:

```
# cd ~/scripts
# ./baseline_l4.sh
```

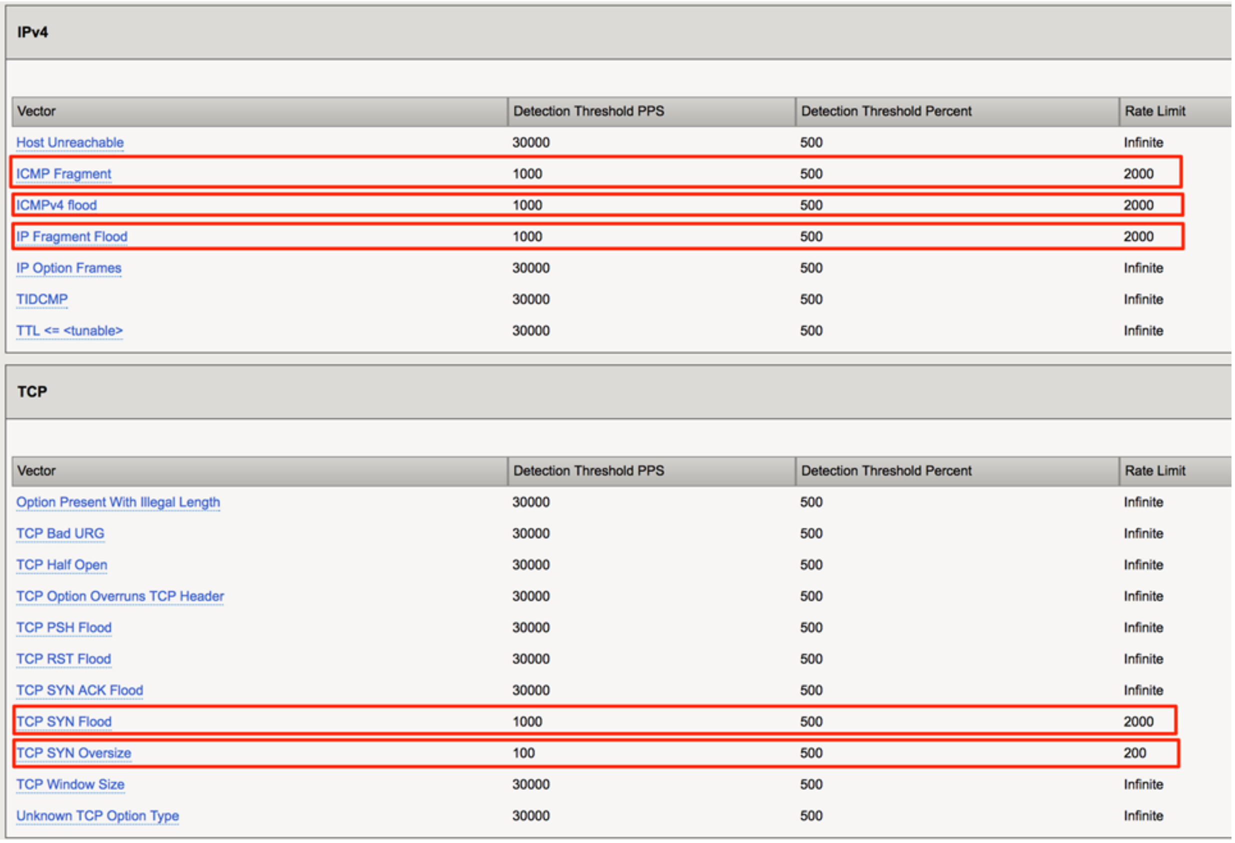
4.1.4 Lab 4 - Multi-vector Demo

In this simple demo you will launch a small number of network attacks and show the configuration, logging and reporting capabilities of the Hybrid Defender. The point of this demo is to provide context for a UI walkthrough with some live data.

Task 1 - Access DoS Quick Configuration and display the ServerNet protected object

This protected object is defending all ports/protocols for 10.1.20.0/24, which is the network behind the Hybrid Defender. Attacks will be launched at 10.1.20.12, which is an interface on the LAMP server. Verify that the following vectors are configured:

- Add the TCP vectors under DDoS Settings.



IPv4

Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Host Unreachable	30000	500	Infinite
ICMP Fragment	1000	500	2000
ICMPv4 flood	1000	500	2000
IP Fragment Flood	1000	500	2000
IP Option Frames	30000	500	Infinite
TIDCMP	30000	500	Infinite
TTL <= <tunable>	30000	500	Infinite

TCP

Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Option Present With Illegal Length	30000	500	Infinite
TCP Bad URG	30000	500	Infinite
TCP Half Open	30000	500	Infinite
TCP Option Overruns TCP Header	30000	500	Infinite
TCP PSH Flood	30000	500	Infinite
TCP RST Flood	30000	500	Infinite
TCP SYN ACK Flood	30000	500	Infinite
TCP SYN Flood	1000	500	2000
TCP SYN Oversize	100	500	200
TCP Window Size	30000	500	Infinite
Unknown TCP Option Type	30000	500	Infinite

- Click **Update** when finished.

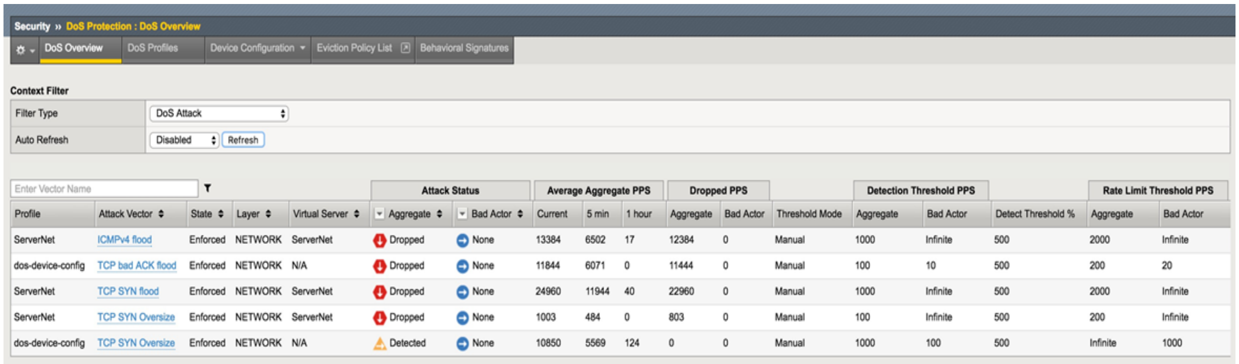
You will now launch the attacks and show the behavior

- Open the following tabs in the DHD UI:
- **DoS Protection->Quick Configuration->ServerNet**
- **Security->DoS Protection->DoS Overview** (leave the filter at default: 'DoS Attack')

- **Statistics->DoS Visibility**
- Access the **Attacker** shell and run the following commands/attack

```
# cd ~/scripts
# ./multivector.sh
```

- Click **Refresh** on the DoS Overview page. You will see some attacks mitigated by **Device Configuration** and some mitigated by the more specific settings on the **ServerNet Protected Object**.



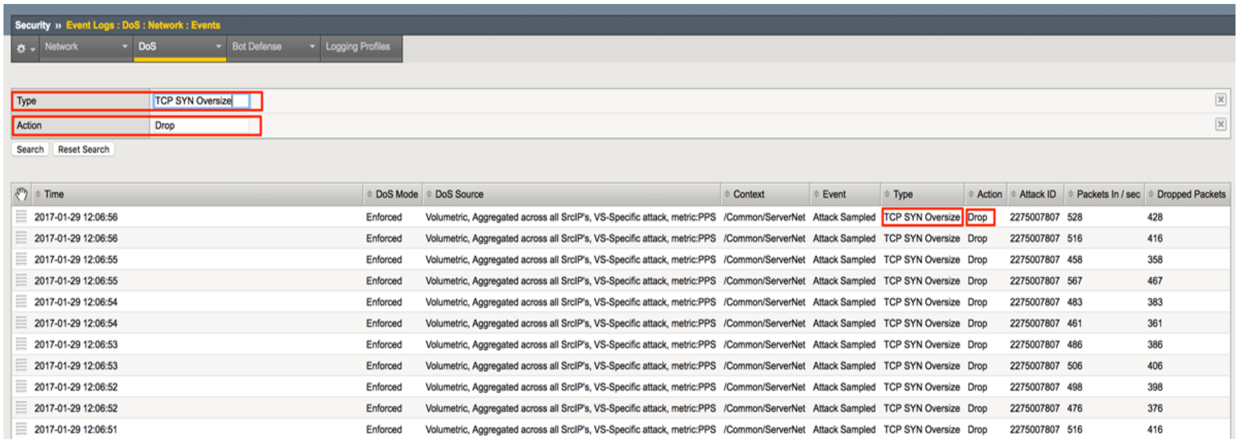
Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	5 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
ServerNet	ICMPv4 flood	Enforced	NETWORK	ServerNet	Dropped	None	13384	6502	17	12384	0	Manual	1000	Infinite	500	2000	Infinite
dos-device-config	TCP bad ACK flood	Enforced	NETWORK	N/A	Dropped	None	11844	6071	0	11444	0	Manual	100	10	500	200	20
ServerNet	TCP SYN flood	Enforced	NETWORK	ServerNet	Dropped	None	24960	11944	40	22960	0	Manual	1000	Infinite	500	2000	Infinite
ServerNet	TCP SYN Oversize	Enforced	NETWORK	ServerNet	Dropped	None	1003	484	0	803	0	Manual	100	Infinite	500	200	Infinite
dos-device-config	TCP SYN Oversize	Enforced	NETWORK	N/A	Detected	None	10850	5569	124	0	0	Manual	1000	100	500	Infinite	1000

Navigate to **Security->Event Logs->DoS->Network->Events**.

- Click on "custom search. . . " link.
- Drag one of the values from the "Attack Type" column into the custom search builder. From the Action column, drag Drop into the search builder. Click "Search".



Type	TCP SYN Oversize
Action	Drop

Time	DoS Mode	DoS Source	Context	Event	Type	Action	Attack ID	Packets In / sec	Dropped Packets
2017-01-29 12:06:56	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	528	428
2017-01-29 12:06:56	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	516	416
2017-01-29 12:06:55	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	458	358
2017-01-29 12:06:55	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	567	467
2017-01-29 12:06:54	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	483	383
2017-01-29 12:06:54	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	461	361
2017-01-29 12:06:53	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	486	386
2017-01-29 12:06:53	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	506	406
2017-01-29 12:06:52	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	498	398
2017-01-29 12:06:52	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	476	376
2017-01-29 12:06:51	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	TCP SYN Oversize	Drop	2275007807	516	416

- Further explore the DoS Event logs. For example, clear the search and identify the "Stop" and "Start" times for an attack, etc.

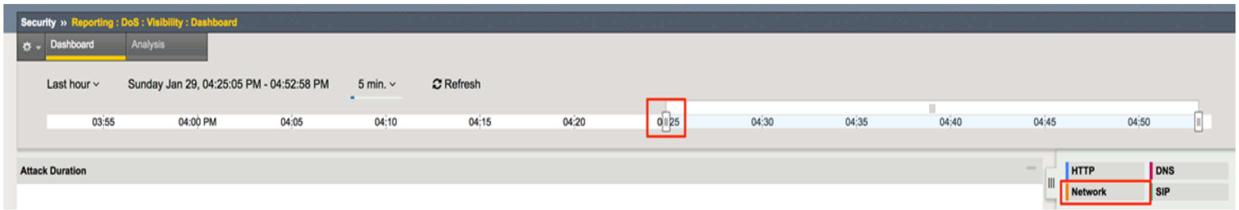
Task 2 – View the DoS Visibility Page

You can now use the new DoS Visibility page to view statistics about the DoS attacks you submitted during this exercise.

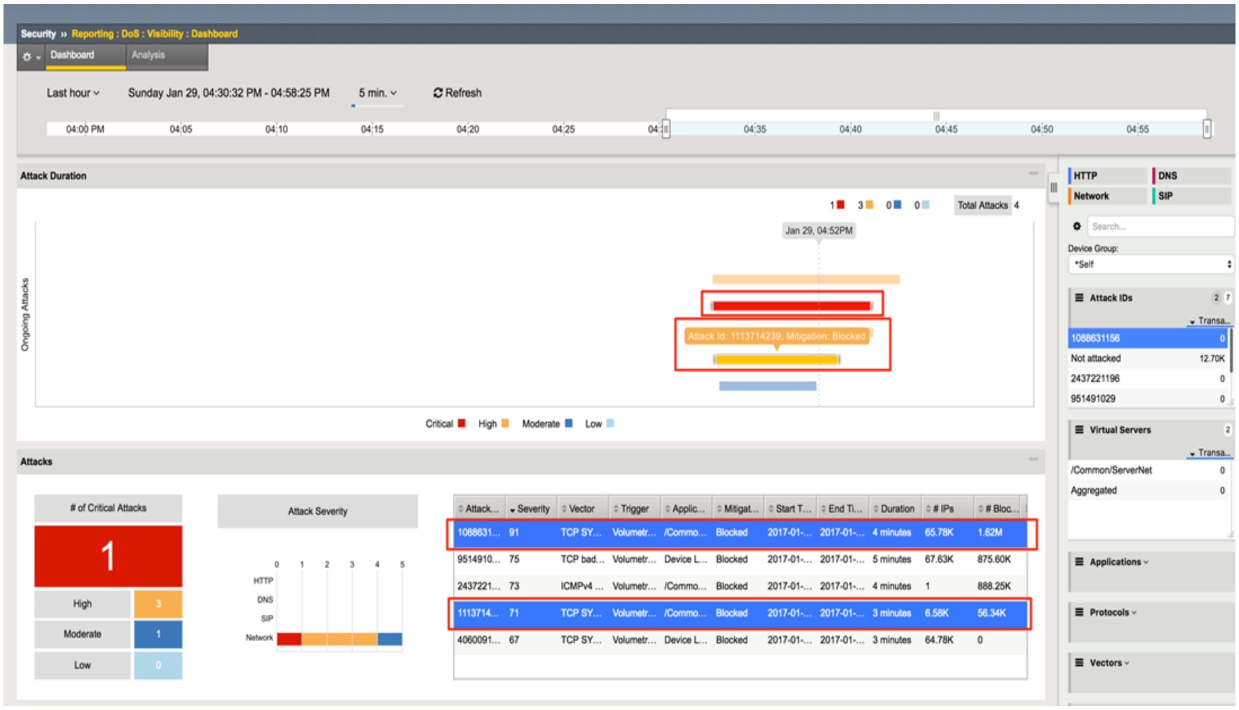
- In the Hybrid Defender WebUI, access the DoS Visibility reporting tool at **Statistics->DoS Visibility.**

Note: DoS Visibility is a reporting tool, not a real-time monitoring tool. Events are displayed, much like other AVR-based reporting, in 5 minute windows. Do not expect events to be shown here immediately after running an attack. Quicker/real-time monitoring of on-going DoS attacks is best accomplished in the DoS Event Logs and DoS Overview areas of the WebUI.

- You should see the attacks in the timeline and a variety of details in the windows. Use the slider to shorten the timeframe if needed. You might have to hit refresh several times.



- You can select events from the timeline and see details about the attacks.

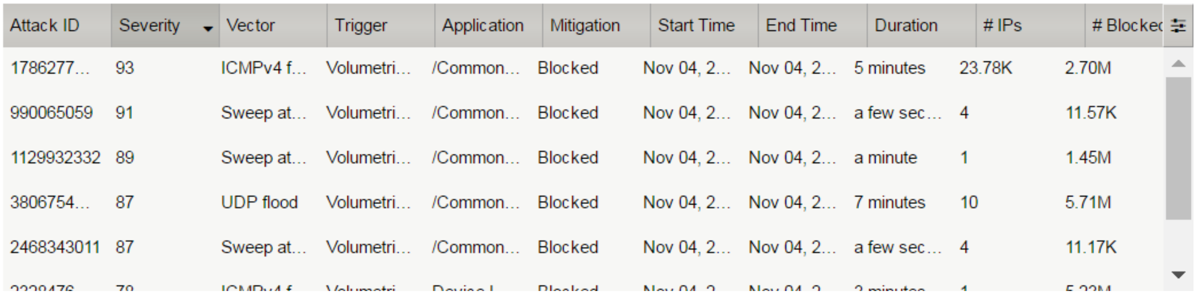


Attack...	Severity	Vector	Trigger	Applic...	Mitigat...	Start T...	End Ti...	Duration	# IPs	# Bloc...
1088631...	91	TCP SY...	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	4 minutes	65.78K	1.62M
9514910...	75	TCP bad...	Volumetr...	Device L...	Blocked	2017-01-...	2017-01-...	5 minutes	67.63K	875.60K
2437221...	73	ICMPv4 ...	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	4 minutes	1	888.25K
1113714...	71	TCP SY...	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	3 minutes	6.58K	56.34K
4060091...	67	TCP SY...	Volumetr...	Device L...	Blocked	2017-01-...	2017-01-...	3 minutes	64.78K	0

Attack IDs	Transa...
1088631156	0
Not attacked	12.70K
2437221196	0
951491029	0

Virtual Servers	Transa...
/Common/ServerNet	0
Aggregated	0

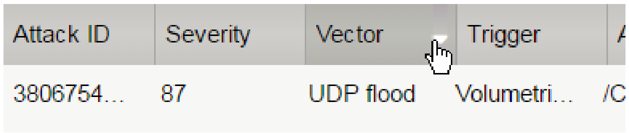
- In the **Attack Duration** window view the attack.
  - Scroll down in the left-side of the page to view the **Attacks** section.
- View the details at the bottom of the **Attacks** section.



Attack ID	Severity	Vector	Trigger	Application	Mitigation	Start Time	End Time	Duration	# IPs	# Blocked
1786277...	93	ICMPv4 f...	Volumetri...	/Common...	Blocked	Nov 04, 2...	Nov 04, 2...	5 minutes	23.78K	2.70M
990065059	91	Sweep at...	Volumetri...	/Common...	Blocked	Nov 04, 2...	Nov 04, 2...	a few sec...	4	11.57K
1129932332	89	Sweep at...	Volumetri...	/Common...	Blocked	Nov 04, 2...	Nov 04, 2...	a minute	1	1.45M
3806754...	87	UDP flood	Volumetri...	/Common...	Blocked	Nov 04, 2...	Nov 04, 2...	7 minutes	10	5.71M
2468343011	87	Sweep at...	Volumetri...	/Common...	Blocked	Nov 04, 2...	Nov 04, 2...	a few sec...	4	11.17K
2228476...	78	ICMPv4 f...	Volumetri...	Device L...	Blocked	Nov 04, 2...	Nov 04, 2...	2 minutes	1	5.23M

This table displays details of each attack that has occurred.

- Sort this table by **Vector**.

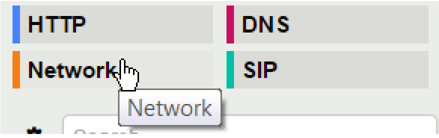


Attack ID	Severity	Vector	Trigger	A
3806754…	87	UDP flood	Volumetri…	/C

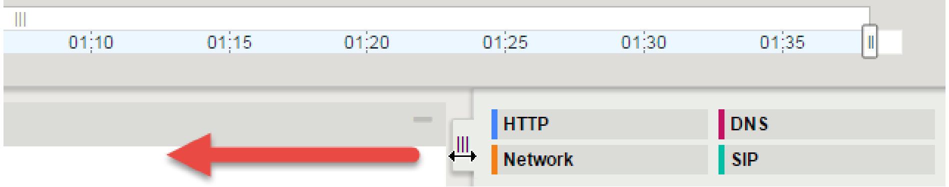
- Scroll down in the left-side of the page to view the **Virtual Servers** section.

  You can see the details of device-wide attacks (**Device Level**) and protected object-level attacks (/**Common**/**ServerNet**).

- Scroll down in the left-side of the page to view the Countries section.
- View the details at the bottom of the **Countries** section. This table displays the attack details from each country.
- View the various widgets in the panel on the right-side of the page.
- Click **Network** to filter out only the network-level attacks (all the attacks so far have been network-level).



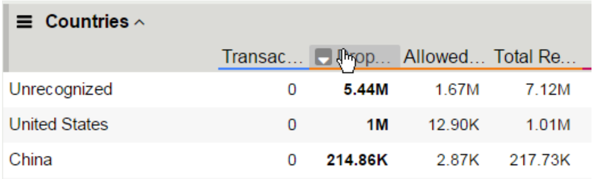
- If it's not already expanded, expand the **Virtual Servers** widget, and then select /**Common/ServerNet**.
- This filters the results to only attacks at this protected object-level. Notice the changes to the map on in the **Countries** section.
- Click /**Common**/**ServerNet** to remove the filter.
- Drag the resize handle on the right-side of the main window as far to the left as possible.



- Expand the **Vectors** widget, and then select **ICMPv4 flood**.
- Expand the **Client IP Addresses** widget.

Question: How many client IP addresses contributed to this attack?

- Expand the **Countries** widget.
- Sort the countries by **Dropped Requests**.



Countries

	Transac…	Drop…	Allowed…	Total Re…
Unrecognized	0	**5.44M**	1.67M	7.12M
United States	0	**1M**	12.90K	1.01M
China	0	**214.86K**	2.87K	217.73K

- Select **China**, and then view the changes to both the **Client IP Addresses** widget and the map.
- At the top of the page open the **Analysis** page.

Note: The requests are still filtered for the ICMPv4 flood results for China.

- Drag the resize handle on the as far to the right as possible.
- Examine the Avg Throughput (Bits per second) graph.
- Place your mouse over the peak in the graph.

Question: What is the **Average client in throughput** during the attack?

- Feel free to examine more of the **Dashboard** page and the **Analysis** page.
- Type **Ctrl + C** to stop the attack.

4.1.5 Lab 5 - Bad Actor Detection Demo

In this demo you will run an attack from specific IP addresses. The Hybrid Defender will be configured to perform bad actor detection, limit the attack on a per-IP basis with more aggressive thresholds and then, based on this detection, automatically blacklist the offending IP address adding them to the (hardware-accelerated) dynamic blacklist.

Task 1 - Open the following tabs in the DHD UI

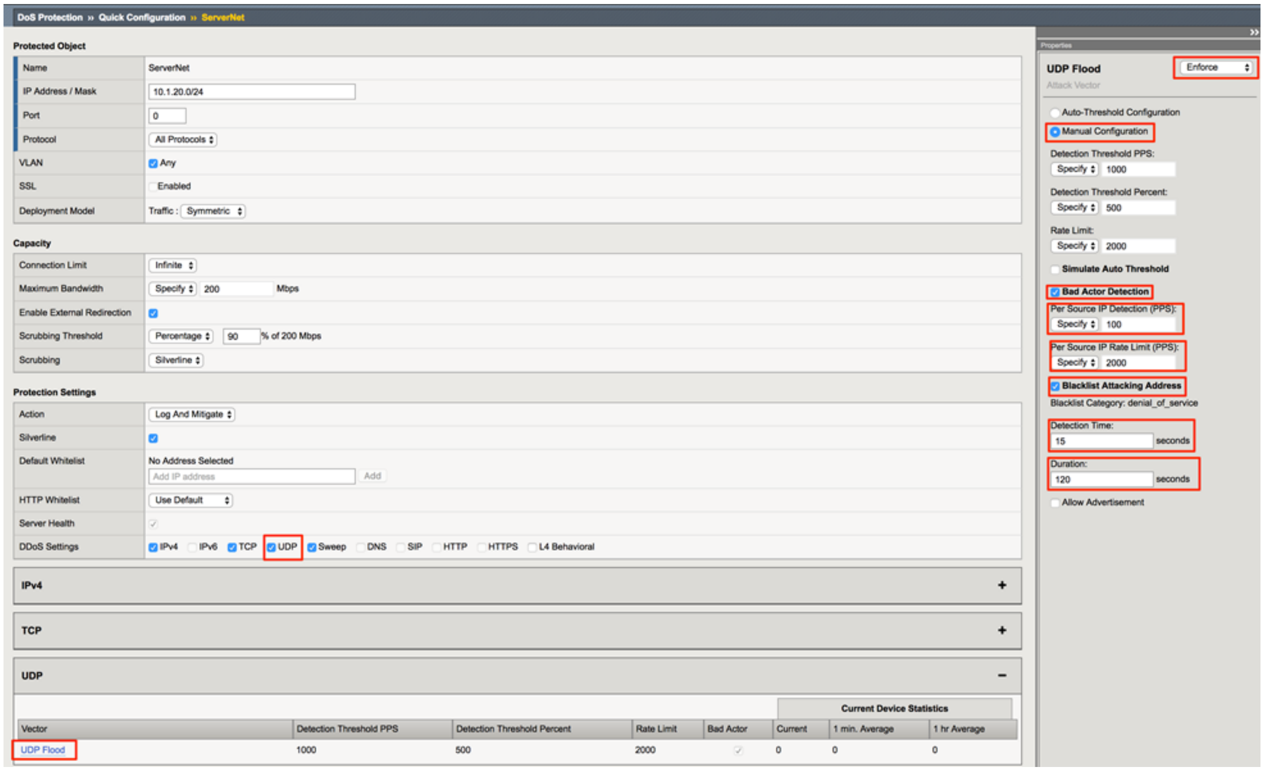
- **DoS Protection->Quick Configuration->ServerNet**
- **Security->DoS Protection->DoS Overview** (leave filter at default: "DoS Attack")
- **Statistics->DoS Visibility**
- **Security->Event Logs->Network->IP Intelligence**

Task 2 – Configure the following UDP Flood vectors for ServerNet

- **DoS Protection->Quick Configuration->ServerNet**

Set the following: DDoS Settings: UDP, Sweep

- Click **UDP Flood**
  - Detection Threshold PPS: 1000
  - Detection Threshold Percent: 500
  - Rate Limit: 2000
- Bad Actor Detection - Check
  - Per Source IP Detection PPS: 100
  - Per Source IP Rate Limit PPS: 2000
- Blacklist Attacking Address
  - Detection Time: 15
  - Duration: 120



DoS Protection » Quick Configuration » ServerNet

Protected Object

Name	ServerNet
IP Address / Mask	10.1.20.0/24
Port	0
Protocol	All Protocols
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric

Capacity

Connection Limit	Infinite
Maximum Bandwidth	Specify 200 Mbps
Enable External Redirection	☑
Scrubbing Threshold	Percentage 90 % of 200 Mbps
Scrubbing	Silverline

Protection Settings

Action	Log And Mitigate
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default
Server Health	✓
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP ☑ UDP ☑ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

IPv4 +

TCP +

UDP −

					Current Device Statistics		
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit	Bad Actor	Current	1 min. Average	1 hr Average
UDP Flood	1000	500	2000	✓	0	0	0

Properties

UDP Flood Enforce

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS: Specify 1000

Detection Threshold Percent: Specify 500

Rate Limit: Specify 2000

□ **Simulate Auto Threshold**

☑ **Bad Actor Detection**

Per Source IP Detection (PPS): Specify 100

Per Source IP Rate Limit (PPS): Specify 2000

☑ **Blacklist Attacking Address**

Blacklist Category: denial_of_service

Detection Time: 15 seconds

Duration: 120 seconds

□ Allow Advertisement

- Click **Update** when finished.
- Access the **Attacker** system CLI and run the UDP flood attack:

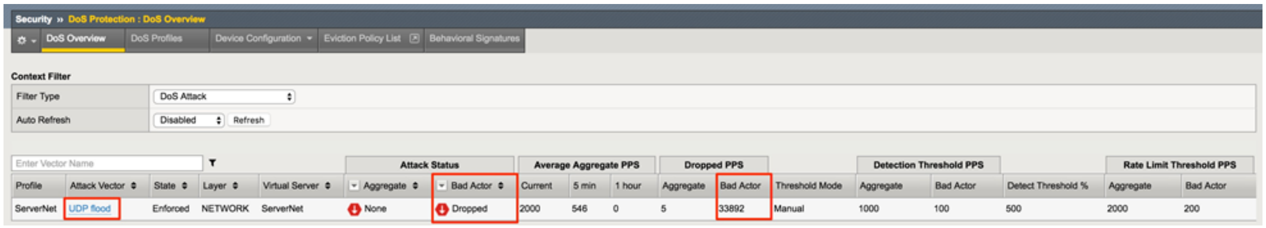
```
# cd ~/scripts
# ./udp_flood.sh
```

From the menu, select '1' to start the attack

```
root@attacker-a:~/scripts# ./udp_flood.sh

1)Attack start
2)Attack end
3)Quit

# ?
```

Note: This attack is relatively short-lived. You can launch it again if the attack ends and you are not finished viewing the various reports. Simply type '1' again, to re-run the attack.

- In the Hybrid Defender UI, show the **Security > DoS Protection >DoS Overview** page. Note the blocks by Bad Actor.



Security » DoS Protection : DoS Overview

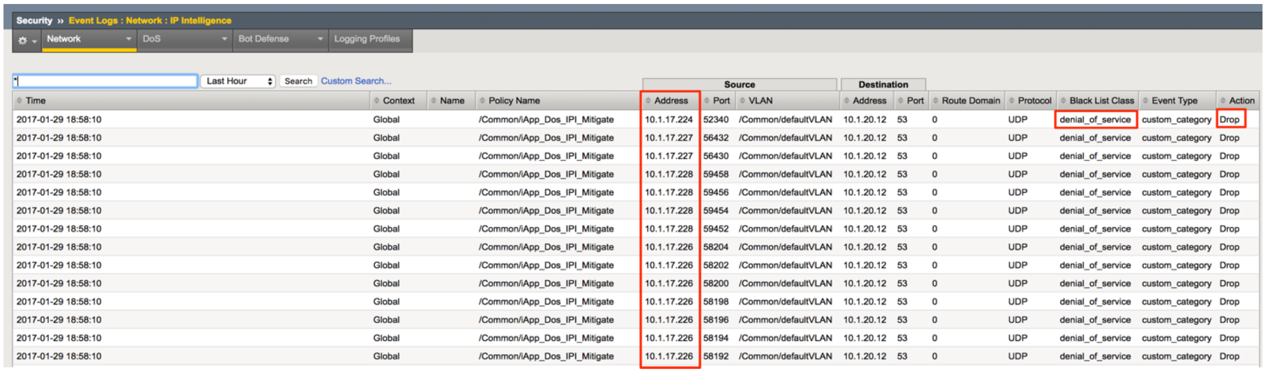
Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled Refresh

Enter Vector Name

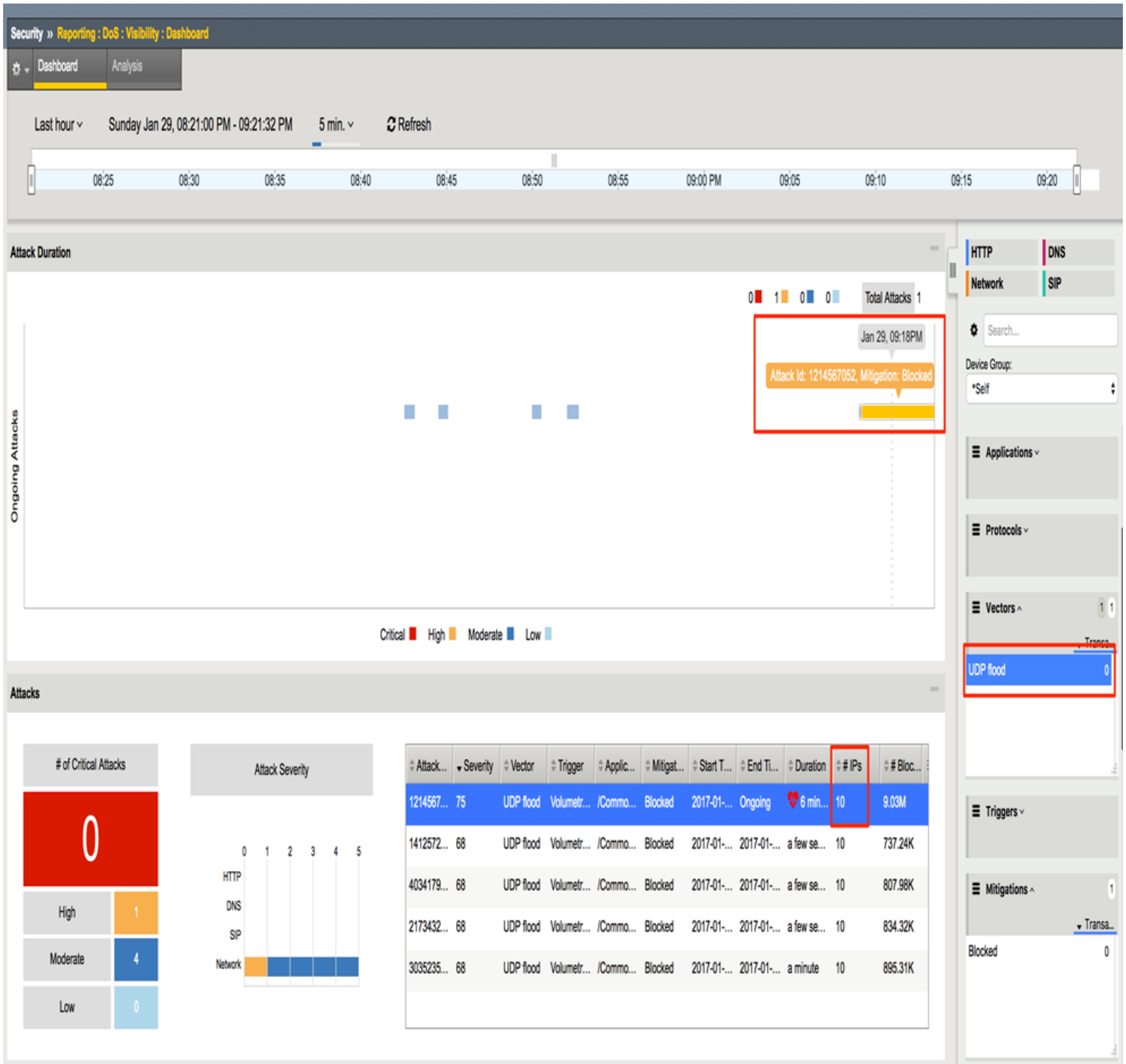
					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	5 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
ServerNet	UDP flood	Enforced	NETWORK	ServerNet	None	Dropped	2000	546	0	5	33892	Manual	1000	100	500	2000	200

- In the Hybrid Defender UI, show the **Security** > **Event Logs** > **Network** > **IP Intelligence** Event Logs. Note the IP addresses that are being added to the denial_of_service blacklist.



				Source			Destination						
Time	Context	Name	Policy Name	Address	Port	VLAN	Address	Port	Route Domain	Protocol	Black List Class	Event Type	Action
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.224	52340	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.227	56432	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.227	56430	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59458	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59456	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59454	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.228	59452	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58204	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58202	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58200	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58198	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58196	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58194	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop
2017-01-29 18:58:10	Global		/Common/iApp_Dos_IPI_Mitigate	10.1.17.226	58192	/Common/defaultVLAN	10.1.20.12	53	0	UDP	denial_of_service	custom_category	Drop

- In the Hybrid Defender WebUI, show the **Statistics** > **DoS Visibility**. Expand the Vectors inspector and select UDP Flood. When it updates, select a flood from the timeline. Note in the Attacks panel the #IPs blocked is 10.



Attack...	Severity	Vector	Trigger	Applic...	Mitigat...	Start T...	End Ti...	Duration	# IPs	# Bloc...
1214567...	75	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	Ongoing	6 min...	10	9.03M
1412572...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a few se...	10	737.24K
4034179...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a few se...	10	807.98K
2173432...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a few se...	10	834.32K
3035235...	68	UDP flood	Volumetr...	/Commo...	Blocked	2017-01-...	2017-01-...	a minute	10	895.31K

From the menu, select ‘2’ to end the attack

or

```
# sudo bash
# killall -9 hping3
```

4.1.6 Lab 6 – Using Auto Thresholding

This exercise will simulate a newly configured Protected Object where the security administrator is unsure what values to assign to a few common vectors. Note that auto-thresholding is useful at both the Device and Protected Object levels.

Note: This demo may place significant stress on the demo environment. This may make the DHD UI less responsive. This is unavoidable since for auto-thresholding to block, the attack must be damaging enough to cause stress, which will push the CPU on the Virtual Environment very high. Remember that this is a virtual environment with minimal resources for lab under high stress and that the Hybrid Defender appliances mitigate these attacks in dedicated hardware.

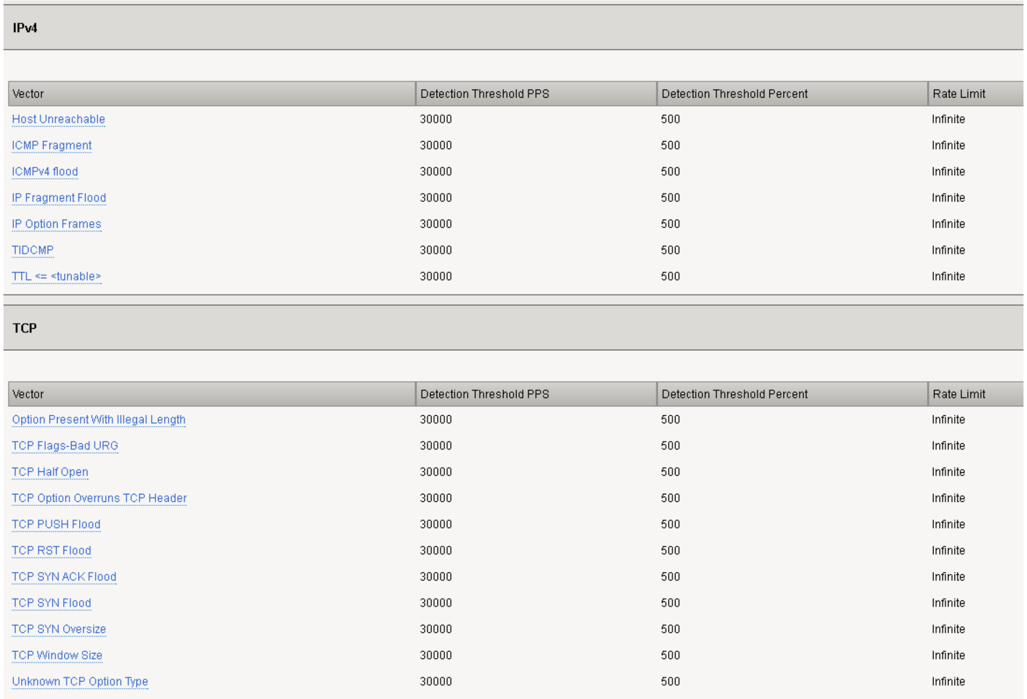
Task 1 – Configure Auto Thresholding

- On the **Good Client**, if you have not already done so, start the network baselining. This step is needed if you didn't start the good traffic generation in Exercise 3 or accidently stopped it.

```
# cd ~/scripts
# ./baseline_l4.sh
```

- In the Hybrid Defender UI, in Quick Configuration, select the **Server5** Protected Object and verify that the IPv4 and TCP vectors are all at default thresholds with auto-threshold disabled:

Setting	Value
All Detection Thresholds	30000 pps
All Rate Limits	Infinite
Auto Thresholding	Disabled



IPv4

Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Host Unreachable	30000	500	Infinite
ICMP Fragment	30000	500	Infinite
ICMPv4 flood	30000	500	Infinite
IP Fragment Flood	30000	500	Infinite
IP Option Frames	30000	500	Infinite
TIDCMP	30000	500	Infinite
TTL <= <tunable>	30000	500	Infinite

TCP

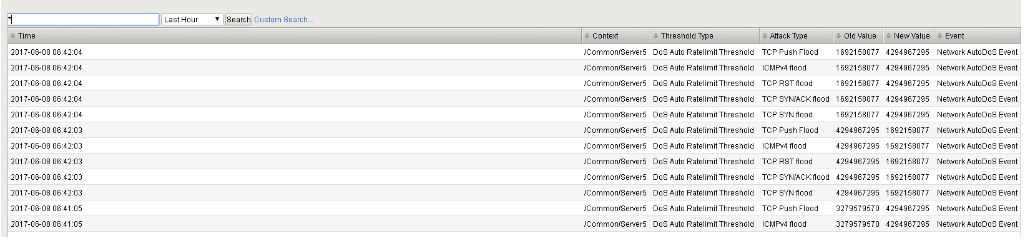
Vector	Detection Threshold PPS	Detection Threshold Percent	Rate Limit
Option Present With Illegal Length	30000	500	Infinite
TCP Flags-Bad URG	30000	500	Infinite
TCP Half Open	30000	500	Infinite
TCP Option Overruns TCP Header	30000	500	Infinite
TCP PUSH Flood	30000	500	Infinite
TCP RST Flood	30000	500	Infinite
TCP SYN ACK Flood	30000	500	Infinite
TCP SYN Flood	30000	500	Infinite
TCP SYN Oversize	30000	500	Infinite
TCP Window Size	30000	500	Infinite
Unknown TCP Option Type	30000	500	Infinite

- In the Hybrid Defender CLI (BIGIP ssh window), restart auto-thresholding:

```
# tmsh run security dos device-config auto-threshold-relearn
# tmsh run security dos virtual name Server5 auto-threshold-relearn
```

In the Hybrid Defender WebUI, in the **Server5** Protected Object configuration, enable auto-thresholding for the following vectors: **ICMPv4 Flood, TCP SYN Flood, TCP Push Flood, TCP RST Flood, TCP SYN ACK Flood** by selecting each vector and **clicking the Auto-Threshold Configuration radio button**. When all vectors are configured, click **Update** at the bottom of the screen.

- In the Hybrid Defender WebUI, view the Auto Threshold event log by navigating to **Security>>Event Logs>>DoS>>Network>>Auto Threshold**.



Time	Context	Threshold Type	Attack Type	Old Value	New Value	Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:04	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	1692158077	4294967295	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:42:03	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	4294967295	1692158077	Network AutoDoS Event
2017-06-08 06:41:05	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	3279579570	4294967295	Network AutoDoS Event
2017-06-08 06:41:05	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	3279579570	4294967295	Network AutoDoS Event

The system is updating the detection thresholds. With auto-thresholding, the system adjusts the detection thresholds based on observed traffic patterns. However, mitigation rate limits are always dynamic based on detected system or protected object stress. If anomalous levels of traffic are running, but there is no stress, the Hybrid Defender will generate alerts but will not block traffic. Under stress, the rate limits are automatically created and adjusted dynamically.

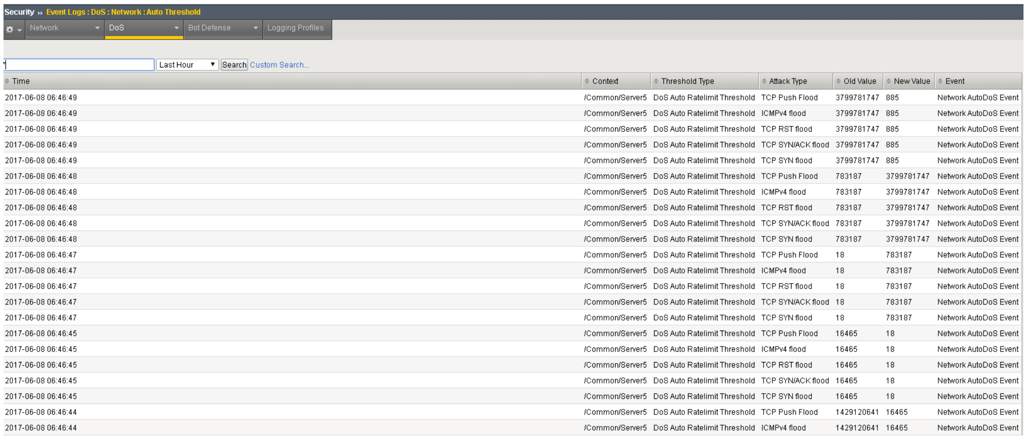
Task 2 – Create Stress to trigger Auto Thresholding and view Reports

- Let's create some stress with a Flood attack. In the **Attacker** CLI start the auto-threshold flood:

```
# cd ~/scripts
# ./autot_flood.sh
```

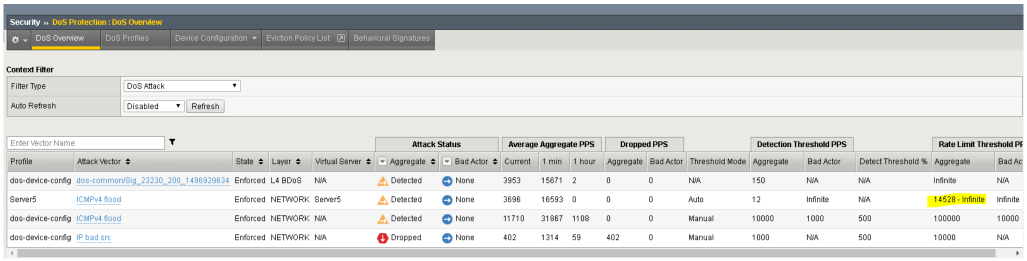
  This is a long duration attack. You can terminate it with Ctrl+C when finished.

- In the Hybrid Defender WebUI, review the Auto Threshold event log. You will see that Rate limits are being automatically set and adjusted to mitigate the flood attack.



Time	Context	Threshold Type	Attack Type	Old Value	New Value	Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:49	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	3799781747	885	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:48	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	783187	3799781747	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:47	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	18	783187	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP RST flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN/ACK flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:45	/Common/Server5	DoS Auto Ratelimit Threshold	TCP SYN flood	16465	18	Network AutoDoS Event
2017-06-08 06:46:44	/Common/Server5	DoS Auto Ratelimit Threshold	TCP Push Flood	1429120641	16465	Network AutoDoS Event
2017-06-08 06:46:44	/Common/Server5	DoS Auto Ratelimit Threshold	ICMPv4 flood	1429120641	16465	Network AutoDoS Event

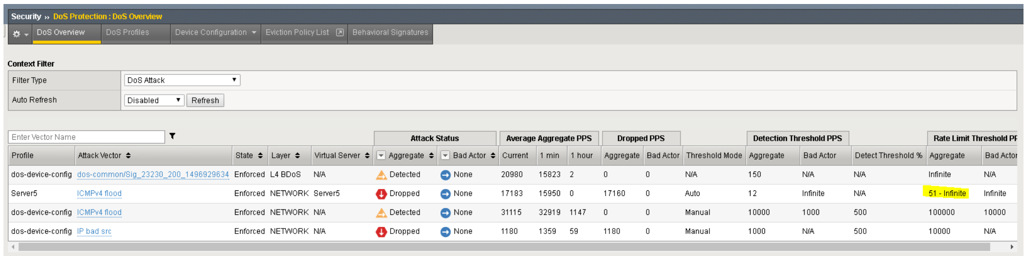
- In the Hybrid Defender WebUI, view the DoS Overview. Note that the ICMP Flood attack is being mitigated and the rate limit thresholds for each of the auto-threshold vectors have been adjusted based on stress, including vectors that are not detecting or blocking an attack.



Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PP	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Ac
dos-device-config	dos-common/Sig_23230_200_1496929634	Enforced	L4 BDoS	N/A	Detected	None	3953	15671	2	0	0	N/A	150	N/A	N/A	Infinite	N/A
Server5	ICMPv4 flood	Enforced	NETWORK	Server5	Detected	None	3696	16593	0	0	0	Auto	12	Infinite	N/A	14528 - Infinite	Infinite
dos-device-config	ICMPv4 flood	Enforced	NETWORK	N/A	Detected	None	11710	31867	1108	0	0	Manual	10000	1000	500	100000	10000
dos-device-config	IP bad src	Enforced	NETWORK	N/A	Dropped	None	402	1314	59	402	0	Manual	1000	N/A	500	10000	N/A

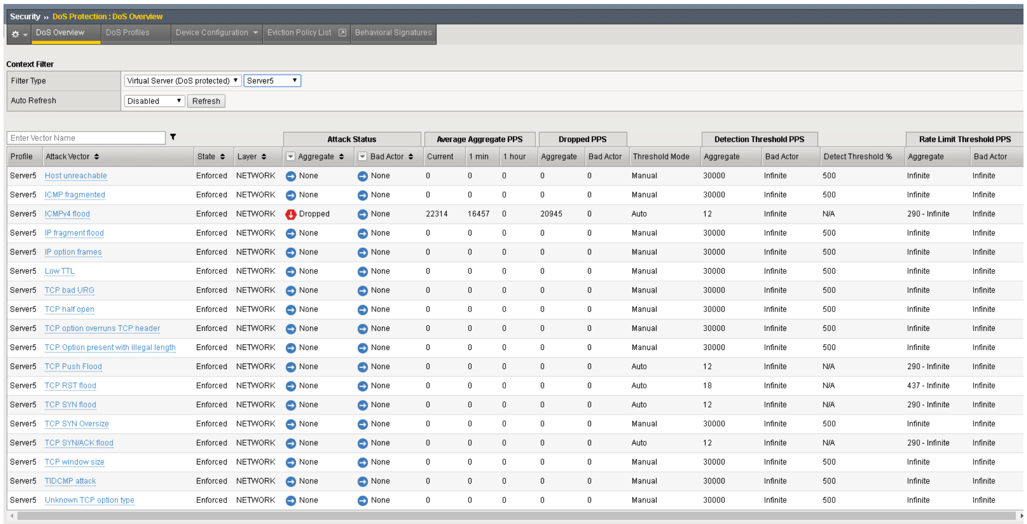


Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PF	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
dos-device-config	dos-common/Sig_23230_200_1496929634	Enforced	L4 BDoS	N/A	Detected	None	20980	15823	2	0	0	N/A	150	N/A	N/A	Infinite	N/A
Server5	ICMPv4 flood	Enforced	NETWORK	Server5	Dropped	None	17183	15950	0	17160	0	Auto	12	Infinite	N/A	51 - Infinite	Infinite
dos-device-config	ICMPv4 flood	Enforced	NETWORK	N/A	Detected	None	31115	32919	1147	0	0	Manual	10000	1000	500	100000	10000
dos-device-config	IP bad src	Enforced	NETWORK	N/A	Dropped	None	1180	1359	59	1180	0	Manual	1000	N/A	500	10000	N/A

- Select the filter type to **Virtual Server (DoS protected)** and **Server5** and view how various thresholds are dynamically adjusted based on the stress.



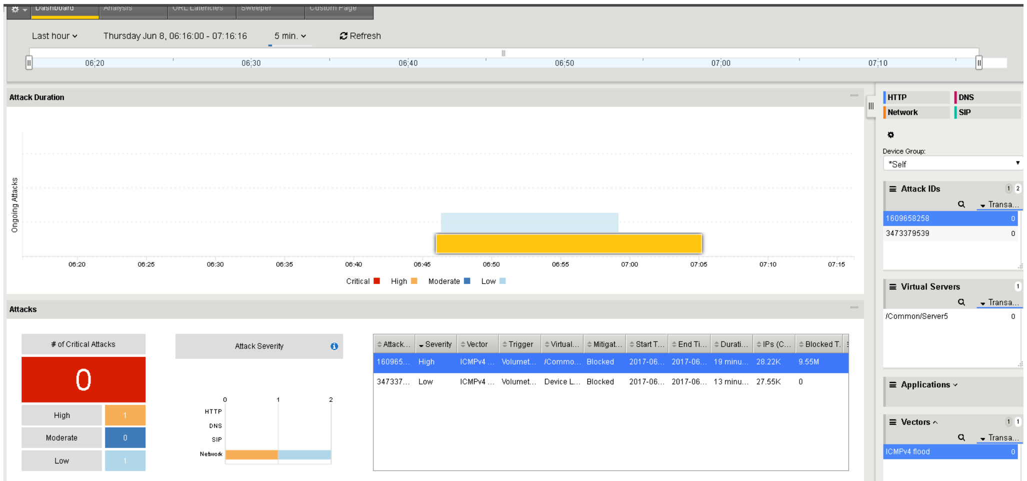
Context Filter

Filter Type	Virtual Server (DoS protected) Server5
Auto Refresh	Disabled

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
Server5	Host unreachable	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	ICMP fragmented	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	ICMPv4 flood	Enforced	NETWORK	Dropped	None	22314	16457	0	20945	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	IP fragment flood	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	IP option frames	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	Low TTL	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP bad URG	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP half open	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP option overruns TCP header	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP Option present with illegal length	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP Push Flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	TCP RST flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	18	Infinite	N/A	437 - Infinite	Infinite
Server5	TCP SYN flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	TCP SYN Oversize	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TCP SYN/ACK flood	Enforced	NETWORK	None	None	0	0	0	0	0	Auto	12	Infinite	N/A	290 - Infinite	Infinite
Server5	TCP window size	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	TIDCMP attack	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
Server5	Unknown TCP option type	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite

- Terminate the attack in the Attacker CLI with Ctrl+C.

- After the attack has ended, in the Hybrid Defender WebUI, navigate to the DoS Visibility page. Under Vectors, select ICMPv4 Flood. View various details.



Thursday Jun 8, 06:16:00 - 07:16:16

Attacks

# of Critical Attacks	
0	
High	1
Moderate	0
Low	1

Attack...	Severity	Vector	Trigger	Virtual...	Mitigat...	Start T...	End Ti...	Durati...	IPs (C...	Blocked T.
160965...	High	ICMPv4 ...	Volumet...	/Commo...	Blocked	2017-06...	2017-06...	19 minu...	28.22K	9.55M
347337...	Low	ICMPv4 ...	Volumet...	Device L...	Blocked	2017-06...	2017-06...	13 minu...	27.55K	0

Device Group: *Self

Attack IDs 1 2

1609658258	0
3473379539	0

Virtual Servers 1

/Common/Server5	0

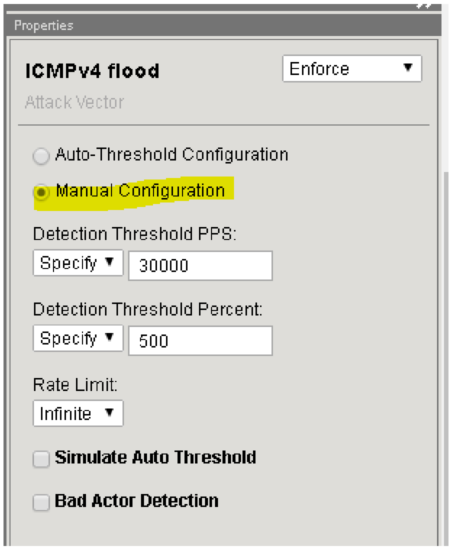
Applications

Vectors 1 1

ICMPv4 flood	0

- **Clean-up**: On the Attacker CLI, if the attack is still running be certain to end it with Ctrl-C.

- **Clean-up**: For repeatability, it is necessary to disable the auto-thresholding for the **ICMPv4 Flood, TCP RST Flood, TCP Push Flood, TCP SYN ACK Flood** and **TCP SYN Flood** vectors on the **Server5** protected object. **Switch them back to Manual Configuration.**



ICMPv4 flood Enforce ▼

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS:

Specify ▼ 30000

Detection Threshold Percent:

Specify ▼ 500

Rate Limit:

Infinite ▼

□ **Simulate Auto Threshold**

□ **Bad Actor Detection**

- **Clean-up**: After disabling auto-thresholding, clear the learning on the Hybrid Defender CLI with:

```
# tmsh run security dos device-config auto-threshold-relearn
# tmsh run security dos virtual name Server5 auto-threshold-relearn
```

- **Clean-up**: Stop the baseline traffic generation from the **good-client** if still running using CTRL+C

4.1.7 Lab 7 – Configuring DNS Attack Protection

DNS DoS attacks come in many flavors and target different resources. DNS query, reverse flood and amplification attacks are some such DNS attacks.

DNS Query Flood

This type of DoS of service attack has a couple possible resource impacts.

- Overwhelm the DNS server's ability to respond by sending too many requests.

This can be done just by asking for more requests than the server can reply with and prevent the server from servicing legitimate requests. It doesn't really matter if the clients are spoofed or not, it only matters that the DNS server just can't keep up.

Mitigation Options

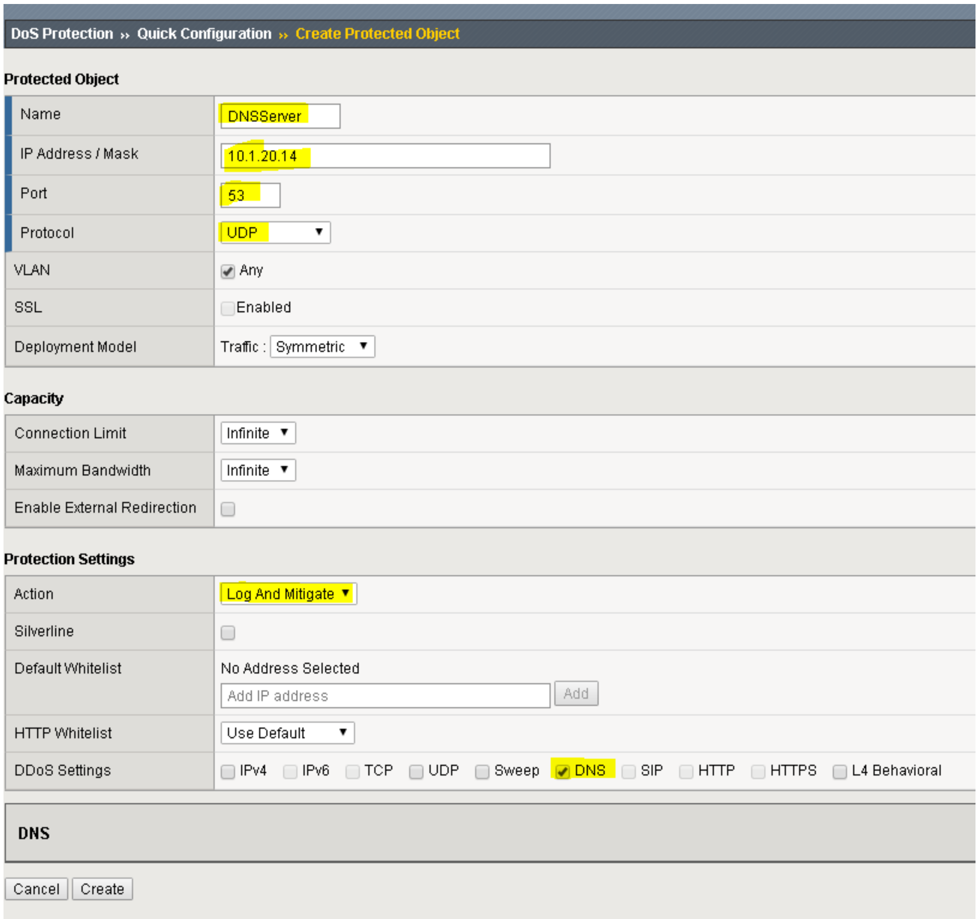
DNS DoS mitigation generally requires an awareness of what you're trying to protect. This allows you to apply the appropriate mitigations and push the problem upstream until the next step is to force it off premises and in to a cloud solution. Load balancing is one remedy to this solution (anycast). Spreading the requests across pools of servers can help mitigate against these types of attacks. DNS Express is another option to increase the capacity of your DNS infrastructure. Layering in DHD DNS DoS vector mitigation also stops common DNS attacks.

Task 1 – Use a Protected Object to Mitigate a DNS Query Flood

- In the BIG-IP Configuration Utility, open the **DoS Protection** > **Quick Configuration** page.

- In the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create.**

Name	DNSServer
IP Address	10.1.20.14
Port	53
Protocol	UDP
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	DNS



DoS Protection » Quick Configuration » Create Protected Object

Protected Object

Name	DNSServer
IP Address / Mask	10.1.20.14
Port	53
Protocol	UDP
VLAN	☑ Any
SSL	□ Enabled
Deployment Model	Traffic : Symmetric

Capacity

Connection Limit	Infinite
Maximum Bandwidth	Infinite
Enable External Redirection	□

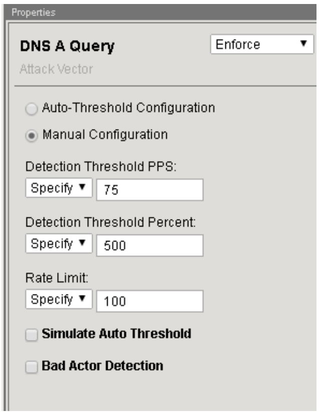
Protection Settings

Action	Log And Mitigate
Silverline	□
Default Whitelist	No Address Selected Add IP address [Add]
HTTP Whitelist	Use Default
DDoS Settings	□ IPv4 □ IPv6 □ TCP □ UDP □ Sweep ☑ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

DNS

- In the **DNS** row click the **+** icon, and then click **DNS A Query**.
- On the right-side of the page configure using the following information, and then click **Create**.

Detection Threshold PPS	Specify: 75
Detection Threshold Percent	Specify: 500
Rate Limit	Specify: 100



Properties

DNS A Query Enforce ▾

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS:
Specify ▾ 75

Detection Threshold Percent:
Specify ▾ 500

Rate Limit:
Specify ▾ 100

□ **Simulate Auto Threshold**

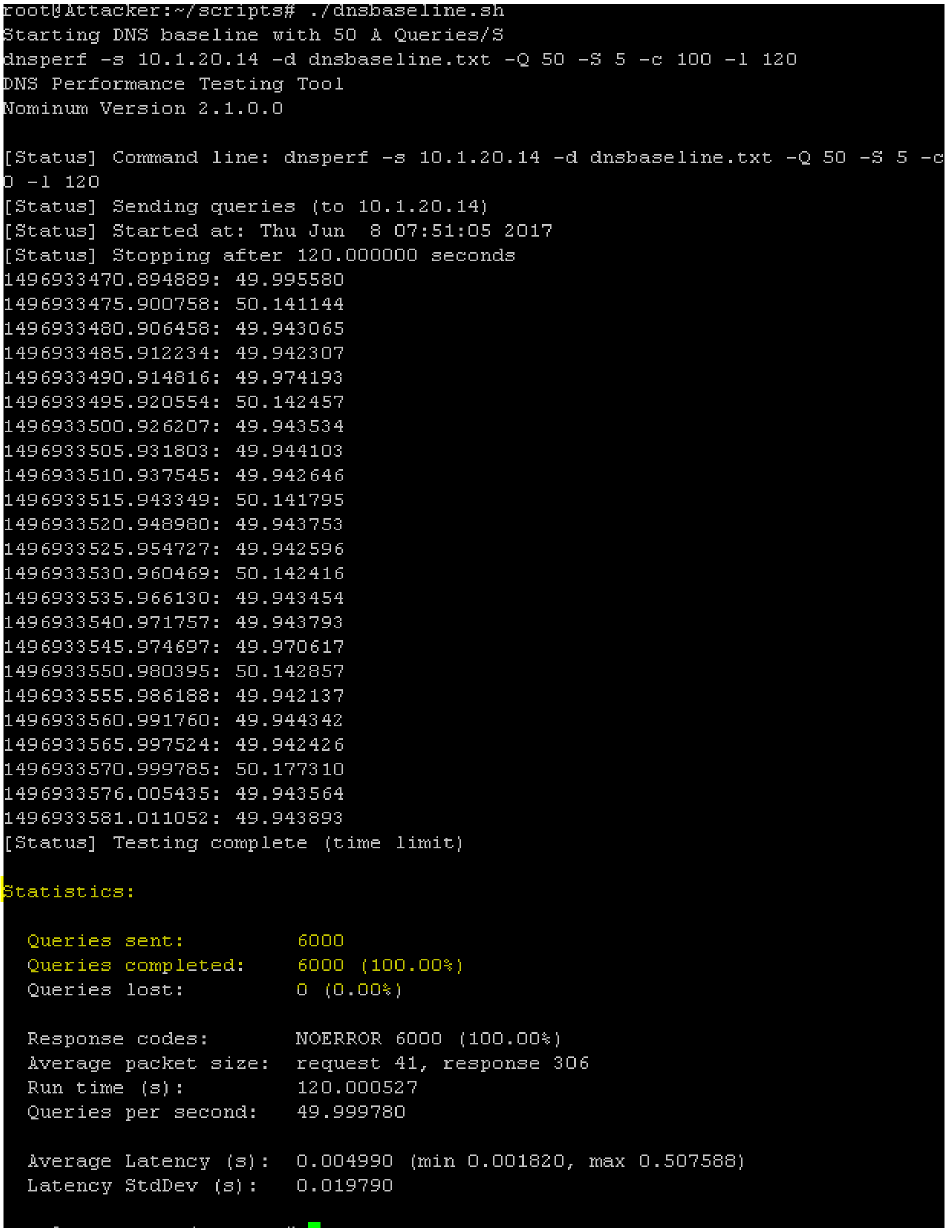
□ **Bad Actor Detection**

Task 2 – Establish a DNS Baseline

- In the **Attacker** putty window type (or copy and paste) the following command:

```
# cd ~/scripts
# ./dnsbaseline.sh
```

- Continue to run the baseline until you get the following results:



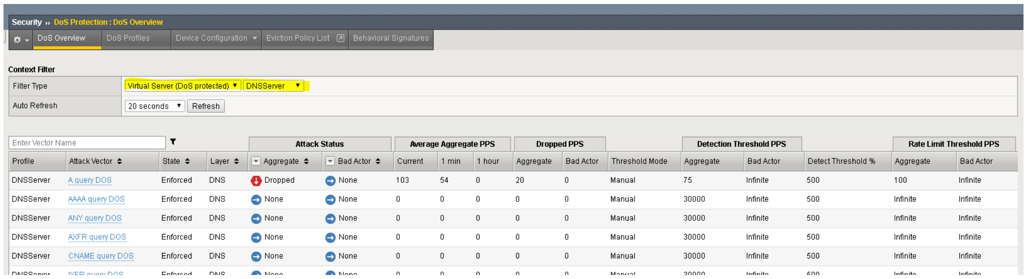
```
root@Attacker:~/scripts# ./dnsbaseline.sh
Starting DNS baseline with 50 A Queries/S
dnsperf -s 10.1.20.14 -d dnsbaseline.txt -Q 50 -S 5 -c 100 -l 120
DNS Performance Testing Tool
Nominum Version 2.1.0.0

[Status] Command line: dnsperf -s 10.1.20.14 -d dnsbaseline.txt -Q 50 -S 5 -c
0 -l 120
[Status] Sending queries (to 10.1.20.14)
[Status] Started at: Thu Jun  8 07:51:05 2017
[Status] Stopping after 120.000000 seconds
1496933470.894889: 49.995580
1496933475.900758: 50.141144
1496933480.906458: 49.943065
1496933485.912234: 49.942307
1496933490.914816: 49.974193
1496933495.920554: 50.142457
1496933500.926207: 49.943534
1496933505.931803: 49.944103
1496933510.937545: 49.942646
1496933515.943349: 50.141795
1496933520.948980: 49.943753
1496933525.954727: 49.942596
1496933530.960469: 50.142416
1496933535.966130: 49.943454
1496933540.971757: 49.943793
1496933545.974697: 49.970617
1496933550.980395: 50.142857
1496933555.986188: 49.942137
1496933560.991760: 49.944342
1496933565.997524: 49.942426
1496933570.999785: 50.177310
1496933576.005435: 49.943564
1496933581.011052: 49.943893
[Status] Testing complete (time limit)

Statistics:

  Queries sent:         6000
  Queries completed:    6000 (100.00%)
  Queries lost:         0 (0.00%)

  Response codes:       NOERROR 6000 (100.00%)
  Average packet size:  request 41, response 306
  Run time (s):         120.000527
  Queries per second:   49.999780

  Average Latency (s):  0.004990 (min 0.001820, max 0.507588)
  Latency StdDev (s):   0.019790
```

Task 3 – Initiate a DNS Attack that Exceeds the Rate Limit

- In the **Attacker** putty window type (or copy and paste) the following command:

  ```
  ./dnsdosrate.sh
  ```

- Wait for the attack to run for about 30 seconds before moving on.
- In the Configuration Utility, review the **DoS Overview** page.
- Change the selection to **Virtual Server** and **DNSServer**.



Security » DoS Protection : DoS Overview

DoS Overview | DoS Profiles | Device Configuration | Eviction Policy List | Behavioral Signatures

Context Filter

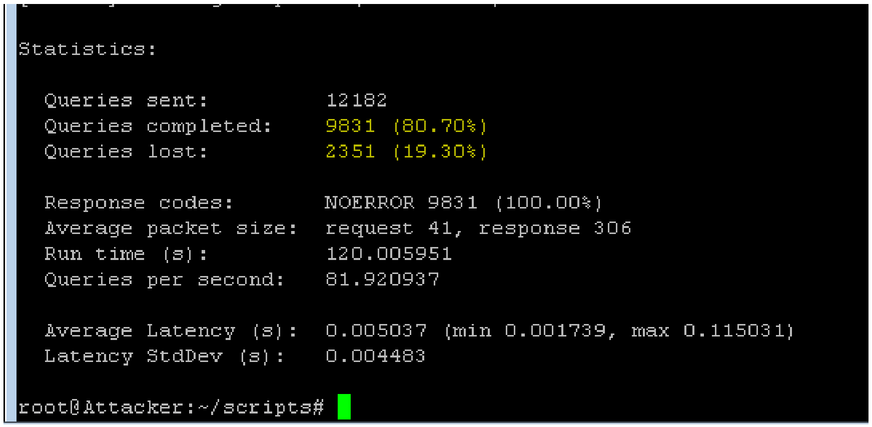
Filter Type	Virtual Server (DoS protected) ▼ DNSServer ▼
Auto Refresh	20 seconds ▼ Refresh

Enter Vector Name

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
DNSServer	A query DOS	Enforced	DNS	Dropped	None	103	54	0	20	0	Manual	75	Infinite	500	100	Infinite
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	ANY query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	AXFR query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	CNAME query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	IXFR query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite

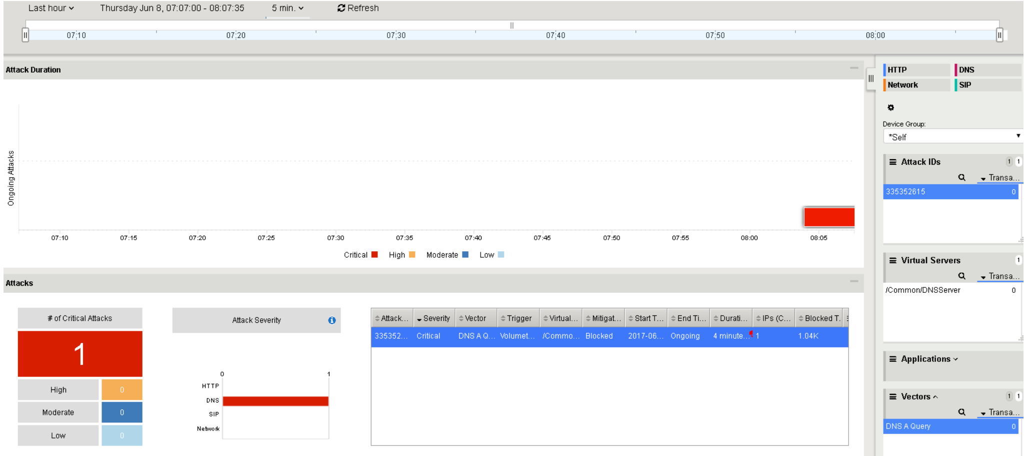
The **A query DOS** attack vector is now dropping attack traffic.

The script will also record the number of drops if any as a result of the attack rate limit being hit.



```
Statistics:

  Queries sent:         12182
  Queries completed:    9831 (80.70%)
  Queries lost:         2351 (19.30%)

  Response codes:       NOERROR 9831 (100.00%)
  Average packet size:  request 41, response 306
  Run time (s):         120.005951
  Queries per second:   81.920937

  Average Latency (s):  0.005037 (min 0.001739, max 0.115031)
  Latency StdDev (s):   0.004483

root@Attacker:~/scripts#
```

- In the Configuration Utility open the **Statistics >>DoS Visibility** page. View details in various sections



Attack...	Severity	Vector	Trigger	Virtual...	Mitigat...	Start T...	End Ti...	Durati...	IPs (C...	Blocked T.
335352...	Critical	DNS A Q...	Volumet...	/Commo...	Blocked	2017-06...	Ongoing	4 minute...	1	1.04K

335352615	0
/Common/DNSServer	0
DNS A Query	0

DNS Reverse flood

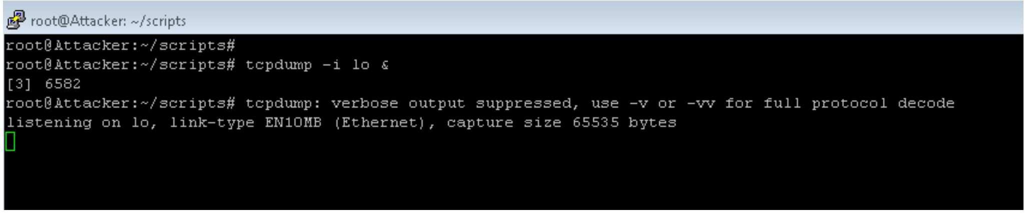
Sometimes DNS responses are used in flooding network resources. A small request has a disproportionately larger response and since the transport protocol is UDP it can easily be spoofed. The outbound pipe can easily get congested responding to a smaller number of requests with large responses.

Task 1 – View DNS Reverse Flood

Use **tcpdump** and **dig** to view DNS request and response packets. A small request produces a large response. You will **open two ssh** sessions to the **attacker**.

- Open two windows via Putty to the **Attacker** CLI (use the shortcut).
- In the **first ssh window** on the attacker start a tcpdump using the following command:

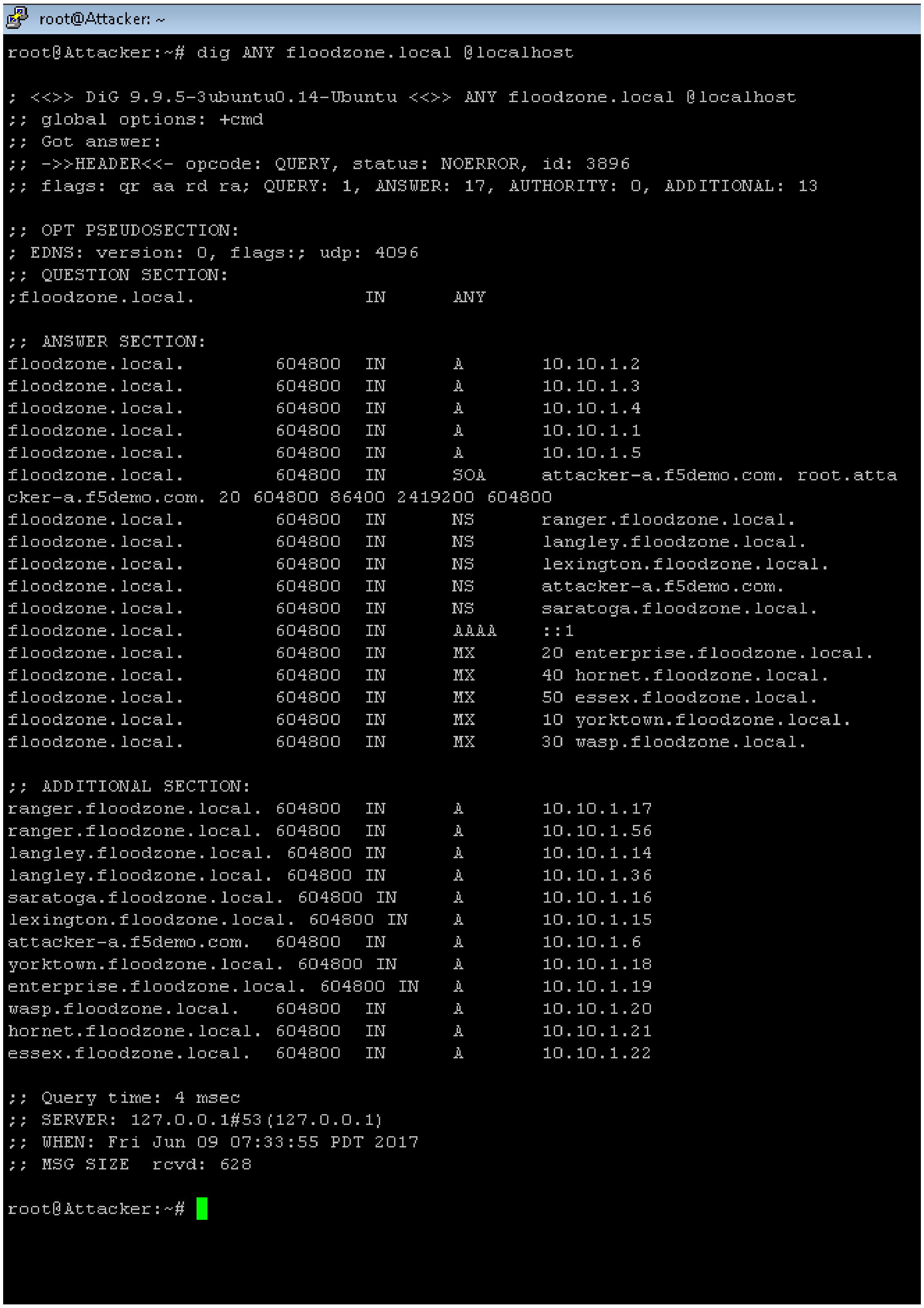
```
# cd ~/scripts
# tcpdump -i lo &
```



```
root@Attacker:~/scripts#
root@Attacker:~/scripts# tcpdump -i lo &
[3] 6582
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
```

- In the **second ssh** window on the attacker issue a dig against the loop back with “ANY”

```
# cd ~/scripts
# dig ANY floodzone.local @localhost
```



```
root@Attacker:~# dig ANY floodzone.local @localhost

; <<>> DiG 9.9.5-3ubuntu0.14-Ubuntu <<>> ANY floodzone.local @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3896
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 17, AUTHORITY: 0, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;floodzone.local.               IN      ANY

;; ANSWER SECTION:
floodzone.local.        604800  IN      A       10.10.1.2
floodzone.local.        604800  IN      A       10.10.1.3
floodzone.local.        604800  IN      A       10.10.1.4
floodzone.local.        604800  IN      A       10.10.1.1
floodzone.local.        604800  IN      A       10.10.1.5
floodzone.local.        604800  IN      SOA     attacker-a.f5demo.com. root.atta
cker-a.f5demo.com. 20 604800 86400 2419200 604800
floodzone.local.        604800  IN      NS      ranger.floodzone.local.
floodzone.local.        604800  IN      NS      langley.floodzone.local.
floodzone.local.        604800  IN      NS      lexington.floodzone.local.
floodzone.local.        604800  IN      NS      attacker-a.f5demo.com.
floodzone.local.        604800  IN      NS      saratoga.floodzone.local.
floodzone.local.        604800  IN      AAAA    ::1
floodzone.local.        604800  IN      MX      20 enterprise.floodzone.local.
floodzone.local.        604800  IN      MX      40 hornet.floodzone.local.
floodzone.local.        604800  IN      MX      50 essex.floodzone.local.
floodzone.local.        604800  IN      MX      10 yorktown.floodzone.local.
floodzone.local.        604800  IN      MX      30 wasp.floodzone.local.

;; ADDITIONAL SECTION:
ranger.floodzone.local. 604800  IN      A       10.10.1.17
ranger.floodzone.local. 604800  IN      A       10.10.1.56
langley.floodzone.local. 604800 IN      A       10.10.1.14
langley.floodzone.local. 604800 IN      A       10.10.1.36
saratoga.floodzone.local. 604800 IN     A       10.10.1.16
lexington.floodzone.local. 604800 IN    A       10.10.1.15
attacker-a.f5demo.com.  604800  IN      A       10.10.1.6
yorktown.floodzone.local. 604800 IN     A       10.10.1.18
enterprise.floodzone.local. 604800 IN   A       10.10.1.19
wasp.floodzone.local.   604800  IN      A       10.10.1.20
hornet.floodzone.local. 604800  IN      A       10.10.1.21
essex.floodzone.local.  604800  IN      A       10.10.1.22

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jun 09 07:33:55 PDT 2017
;; MSG SIZE  rcvd: 628

root@Attacker:~#
```

- In the **first ssh window** on the attacker view the results of the tcpdump : Notice the difference in the **size of the request (44) vs the response (628).** Your values maybe different. The point is that a small request can generate an enormous response.

```
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or
-vv for full protocol decodelistening on lo, link-type EN10MB
(Ethernet), capture size 65535 bytes
```

```
07:33:55.737892 IP localhost.47406 > localhost.domain: 3896+ [1au] ANY?
floodzone.local. **(44)**

07:33:55.738563 IP localhost.domain > localhost.47406: 3896\* 17/0/13 A
10.10.1.2, A 10.10.1.3, A 10.10.1.4, A 10.10.1.1, A 10.10.1.5, SOA, NS
ranger.floodzone.local., NS langley.floodzone.local., NS
lexington.floodzone.local., NS attacker-a.f5d emo.com., NS
saratoga.floodzone.local., AAAA ::1, MX enterprise.floodzone.local. 20,
MX hornet.floodzone.local. 40, MX ess ex.floodzone.local. 50, MX
yorktown.floodzone.local. 10, MX wasp.floodzone.local. 30 **(628)**
```

- In the **second ssh** window on the attacker issue a dig against the loop back with a query to RIPE.NET and with DNSSEC for a larger response.

```
# sudo bash
# cd ~/scripts
# dig ANY ripe.net @localhost +dnssec
```

- In the **first ssh window** on the attacker view the results of the tcpdump : Notice the difference in the size of the request **(37)** vs the response **(2715). Your values maybe different.** The point is that a small request can generate an enormous response.

```
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or
-vv for full protocol decode

listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes

07:43:44.018212 IP localhost.51272 > localhost.domain: 58304+ [1au] ANY?
ripe.net. **(37)**

07:43:44.018889 IP localhost.domain > localhost.51272: 58304$ 18/8/15
RRSIG, SOA, RRSIG, RRSIG, A 193.0.6.139, RRSIG, DNSKEY, DNSKEY, DNSKEY,
RRSIG, DS, NS manus.authdns.ripe.net., NS a2.verisigndns.com., NS
a1.verisigndns.com., NS tinnie.arin.net., NS sns-pb.isc.org., NS
sec3.apnic.net., NS a3.verisigndns.com. **(2715)**
```

- Once you're done, type '**fg**' and '**CTRL+C**' to stop the tcpdump.

```
root@Attacker:~/scripts# tcpdump: verbose output suppressed, use -v or
-vv for full protocol decode listening on lo, link-type EN10MB
(Ethernet), capture size 65535 bytes
```

fg

`tcpdump -i lo`

`^C`

```
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@Attacker:~/scripts#
```

This can easily overwhelm the server or overwhelm the outbound network pipe disrupting traffic responses for legitimate requests and/or other applications.

One industry accepted way to mitigate this type of attack is to rate limit the responses on the DNS servers. More information on Response Rate Limiting can be found here:

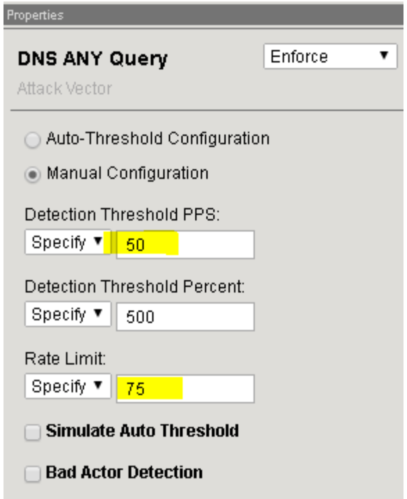
https://www.isc.org/wp-content/uploads/2014/11/DNS-RRL-LISA14.pdf

Because DoS policies are applied to traffic flows on ingress to the DHD, response rate limiting isn't currently available. But you still can limit the types of queries that can disproportionately consume bandwidth. The ANY query used in the previous example is one such example.

Task 2 – Use a Protected Object to Mitigate a DNS Reverse Query Flood

- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page
- In the **Protected Objects** section click **DNSServer**.
- In the **DNS** row click the **+** icon, and then click **DNS ANY Query.**
- On the right-side of the page configure using the following information, and then click **Update**.

Detection Threshold PPS	Specify: 50
Detection Threshold Percent	Specify: 500
Rate Limit	Specify: 75



DNS ANY Query: Enforce

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS: Specify 50

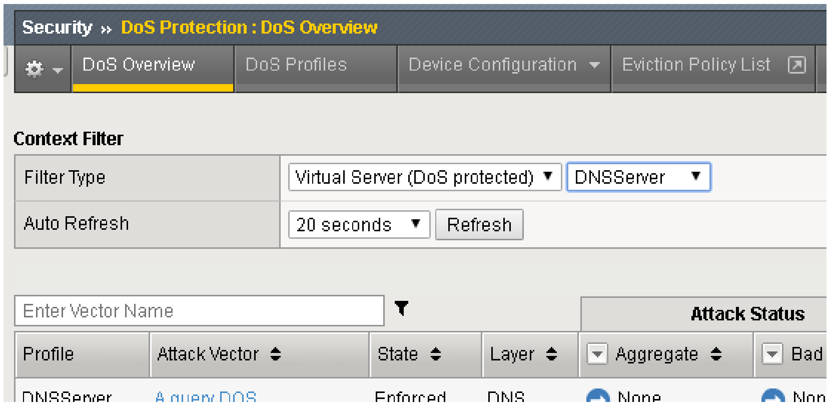
Detection Threshold Percent: Specify 500

Rate Limit: Specify 75

□ Simulate Auto Threshold

□ Bad Actor Detection

- In the BIG-IP Configuration Utility, open the **Security>>DoS Protection>> DoS Overview** page and set the **Filter type** to "**Virtual Server (DoS protected) / DNSServer**" Set **Auto-Refresh** to **20 seconds**.



Context Filter

Filter Type	Virtual Server (DoS protected) DNSServer
Auto Refresh	20 seconds Refresh

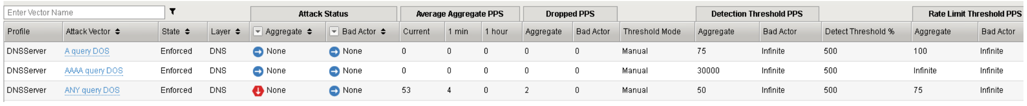
Enter Vector Name

				Attack Status	
Profile	Attack Vector	State	Layer	Aggregate	Bad
DNSServer	A query DOS	Enforced	DNS	None	Non

- In the **attacker** ssh window issue dns reverse flood attack as follows:

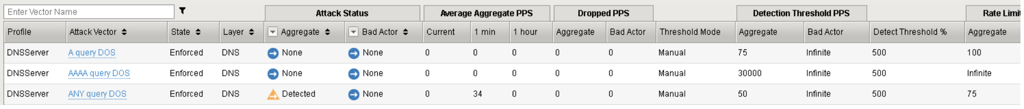
```
# cd ~/scripts
# ./dnsReverseFlood.sh
```

- Observe the DoS Overview as it gradually starts to drop the ANY queries.



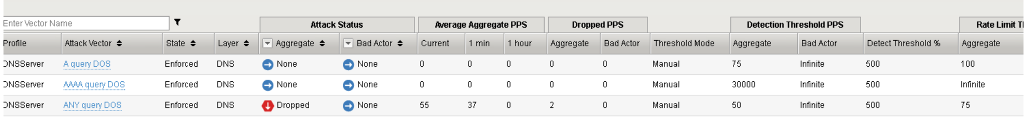
Enter Vector Name

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
DNSServer	A query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	75	Infinite	500	100	Infinite
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNSServer	ANY query DOS	Enforced	DNS	None	None	53	4	0	2	0	Manual	50	Infinite	500	75	Infinite



Enter Vector Name

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limi
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate
DNSServer	A query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	75	Infinite	500	100
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite
DNSServer	ANY query DOS	Enforced	DNS	Detected	None	0	34	0	0	0	Manual	50	Infinite	500	75



Enter Vector Name

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit T
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate
DNSServer	A query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	75	Infinite	500	100
DNSServer	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite
DNSServer	ANY query DOS	Enforced	DNS	Dropped	None	55	37	0	2	0	Manual	50	Infinite	500	75

- In the **attacker** ssh window stop the attack by hitting **CTRL+C** many times

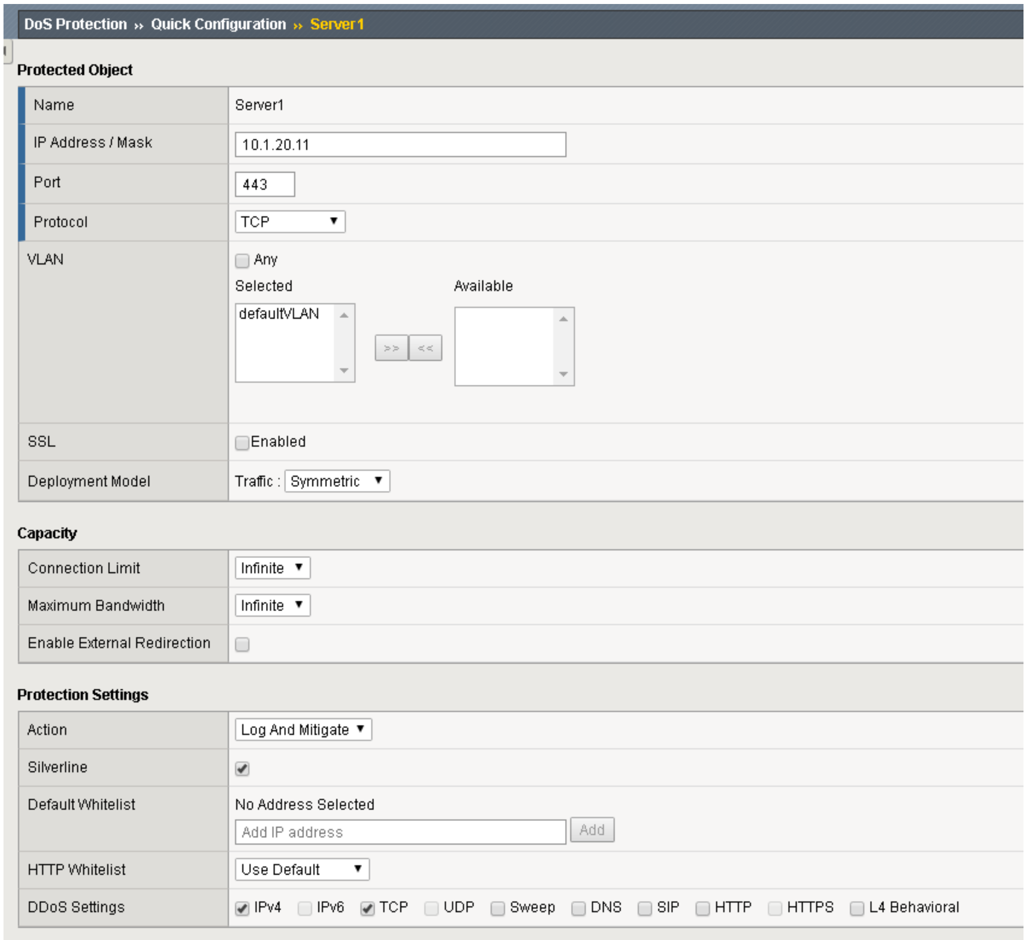
4.1.8 Lab 8 – Configuring L7 Attack Protection

In this exercise we will use a protected object and enforce mitigation for low and slow/encrypted layer 7 attacks.

Task 1 – Create Protected Object and Launch Attack

- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page and in the Protected Objects section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	Server1
IP Address	10.1.20.11
Port	443
VLAN (Selected)	defaultVLAN (uncheck ANY)
Protection Settings: Action	Log and Mitigate
Protection Settings: Silverline	Yes (selected)
Protection Settings: DDoS Settings	IPv4, TCP



DoS Protection » Quick Configuration » Server1

Protected Object

Name	Server1
IP Address / Mask	10.1.20.11
Port	443
Protocol	TCP ▼
VLAN	□ Any Selected: defaultVLAN >> << Available:
SSL	□ Enabled
Deployment Model	Traffic : Symmetric ▼

Capacity

Connection Limit	Infinite ▼
Maximum Bandwidth	Infinite ▼
Enable External Redirection	□

Protection Settings

Action	Log And Mitigate ▼
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default ▼
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP □ HTTPS □ L4 Behavioral

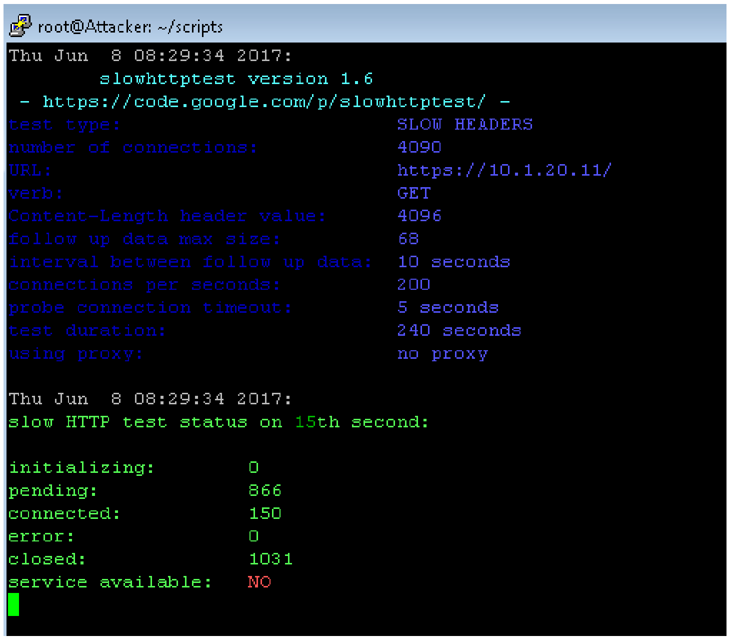
- Launch attacks without any layer 7 protection configured
- Open the following in separate tabs in the Hybrid Defender WebUI:
- **DoS Protection>>Quick Configuration**
- **Security>>Reporting>>DoS>>Analysis**
- From a **Firefox browser** go to https://10.1.20.11. Ignore SSL warning and Add Exception.

Note: This bypasses the Hybrid Defender and accesses the server directly, showing the availability and/or performance of the site directly. Click around a few links. This is the site we will launch an attack against and mitigate.

- Verify that the configuration is providing no L7 protections by taking the server offline with a slowloris attack. Note that apache will try to clean up the slow flows, but they will do so inefficiently and the server is impacted (which will show as an outage, missing objects and/or slower responsiveness). Run the slowloris attack from the Attacker CLI:

```
# cd ~/scripts
# ./slowloris.sh
```

The tool will rapidly show the site offline (10-15 seconds, with trivial traffic load):

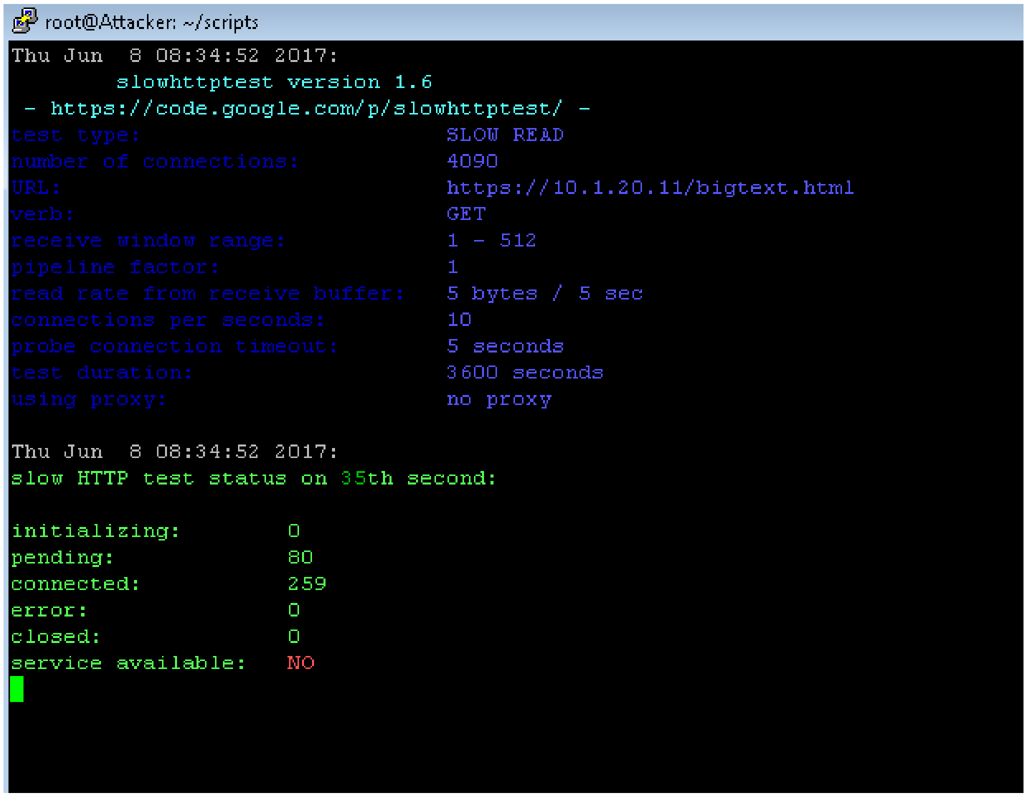


```
Thu Jun  8 08:29:34 2017:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW HEADERS
number of connections:            4090
URL:                              https://10.1.20.11/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          68
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         5 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Thu Jun  8 08:29:34 2017:
slow HTTP test status on 15th second:

initializing:        0
pending:             866
connected:           150
error:               0
closed:              1031
service available:   NO
```

- Refresh https://10.1.20.11 to show the effects of the attack. [Note that since we are running locally from the Win7 system in a virtualized environment, you may be able to access the site, however it will be slower and often the GIFs will not load. An internet user would not be able to "fight through" the attack to get to the server as often as a system on the local LAN.]
- Stop the slowloris attack by using CTRL+C.
- Start a more effective Slow Read attack.

  This attack is harder for DoS mitigation tools to mitigate and can be very effective even with a tiny number of concurrent connections trickling in very slowly to the server to fly below the radar of network detections. In our example we will open 10 connections per second and read the response data at 1 byte / sec. The attack would be effective even at 1 cps, it would just take a bit longer to build up the connections.
- From the **Attacker** CLI/shell start the slowread attack:

```
# cd ~/scripts
# ./slowread.sh
```

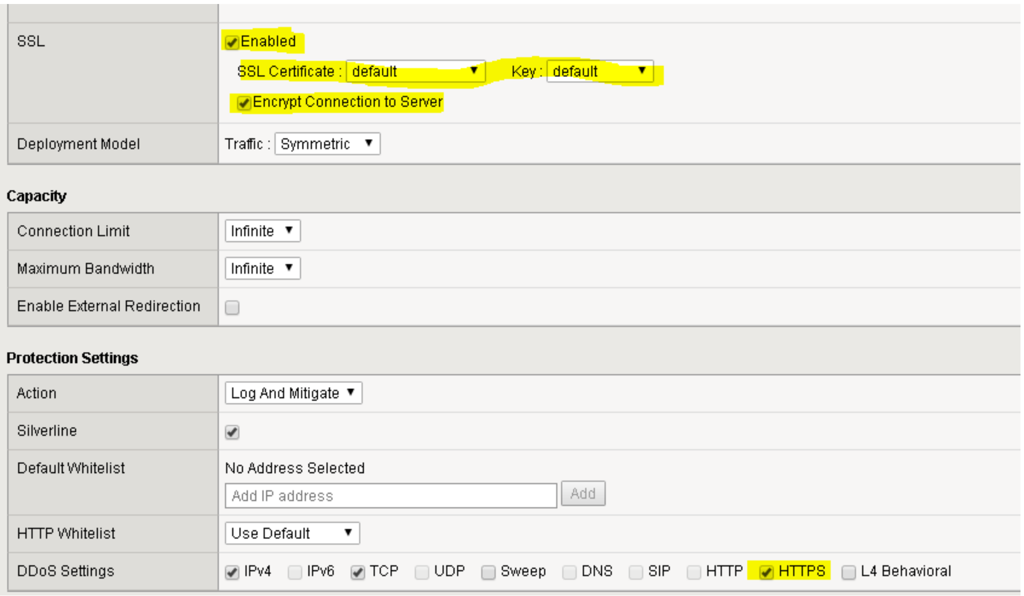


```
Thu Jun  8 08:34:52 2017:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW READ
number of connections:            4090
URL:                              https://10.1.20.11/bigtext.html
verb:                             GET
receive window range:             1 - 512
pipeline factor:                  1
read rate from receive buffer:    5 bytes / 5 sec
connections per seconds:          10
probe connection timeout:         5 seconds
test duration:                    3600 seconds
using proxy:                      no proxy

Thu Jun  8 08:34:52 2017:
slow HTTP test status on 35th second:

initializing:        0
pending:             80
connected:           259
error:               0
closed:              0
service available:   NO
```

As soon as the site is down (service available: NO), refresh https://10.1.20.11 to show that it is down/slow/intermittent.

Task 2 – Configure Protection/Mitigation, launch attack and view reports

- In the Hybrid Defender WebUI, access the **Server1** Protected Object.
- Enable SSL.
- Select the default certificate and key. In your environment you would select a valid/cert key for your application.
- Enable '**Encrypt Session to Server**' to avoid any server reconfiguration.
- Enable the **HTTPS** mitigation family.
- Click **Update**.



SSL	☑ Enabled SSL Certificate : default ▼ Key : default ▼ ☑ Encrypt Connection to Server
Deployment Model	Traffic : Symmetric ▼

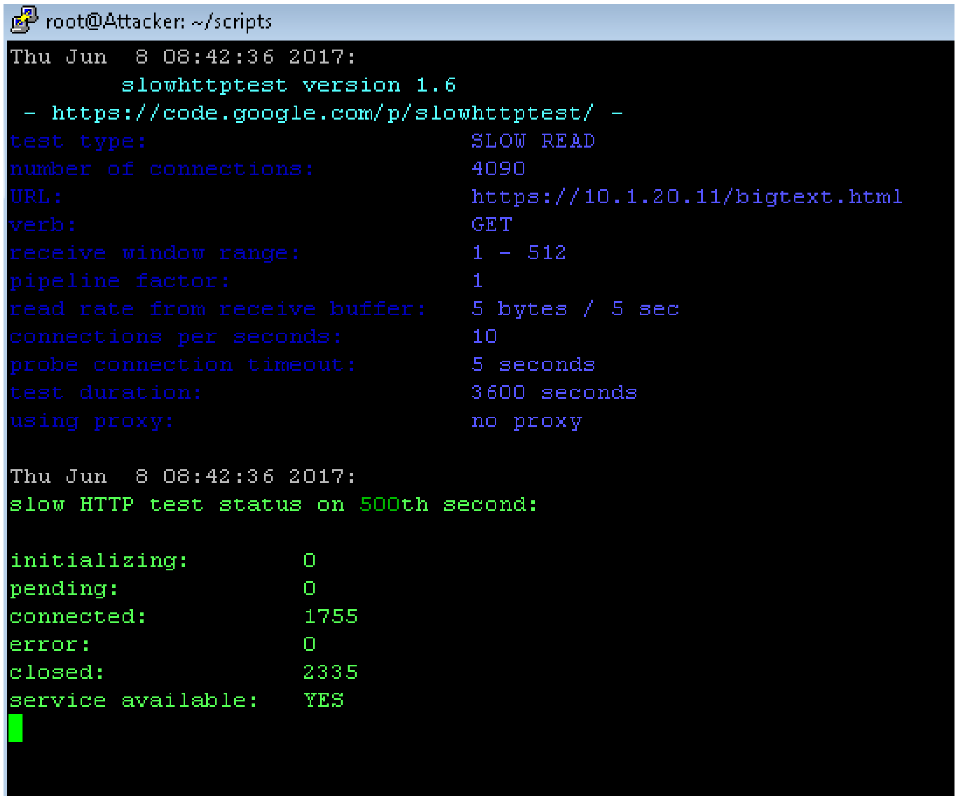
Capacity

Connection Limit	Infinite ▼
Maximum Bandwidth	Infinite ▼
Enable External Redirection	□

Protection Settings

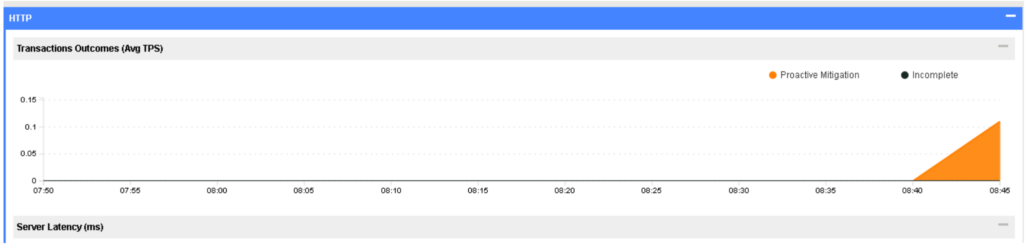
Action	Log And Mitigate ▼
Silverline	☑
Default Whitelist	No Address Selected Add IP address Add
HTTP Whitelist	Use Default ▼
DDoS Settings	☑ IPv4 □ IPv6 ☑ TCP □ UDP □ Sweep □ DNS □ SIP □ HTTP ☑ HTTPS □ L4 Behavioral

- View the Attacker CLI/shell. The slow read attack is now no longer showing the site as down (service available: YES) because Proactive Bot Detection has mitigated the attack.



```
root@Attacker: ~/scripts
Thu Jun  8 08:42:36 2017:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW READ
number of connections:            4090
URL:                              https://10.1.20.11/bigtext.html
verb:                             GET
receive window range:             1 - 512
pipeline factor:                  1
read rate from receive buffer:    5 bytes / 5 sec
connections per seconds:          10
probe connection timeout:         5 seconds
test duration:                    3600 seconds
using proxy:                      no proxy

Thu Jun  8 08:42:36 2017:
slow HTTP test status on 500th second:

initializing:        0
pending:             0
connected:           1755
error:               0
closed:              2335
service available:   YES
```

- Refresh https://10.1.20.11 to see that the site behavior has returned to normal.
- You were able to mitigate an encrypted layer 7 attack quickly and with only a few simple steps.
- In the Hybrid Defender WebUI, view various reports in the **Security>>Reporting>>DoS>>Analysis**
- **HTTP Report (Scroll towards the bottom) shows Proactive Mitigation**.



- Stop the Slow Read attack by using CTRL+C.

4.1.9 Lab 9 – Configuring L7 Behavioral Attack Protection

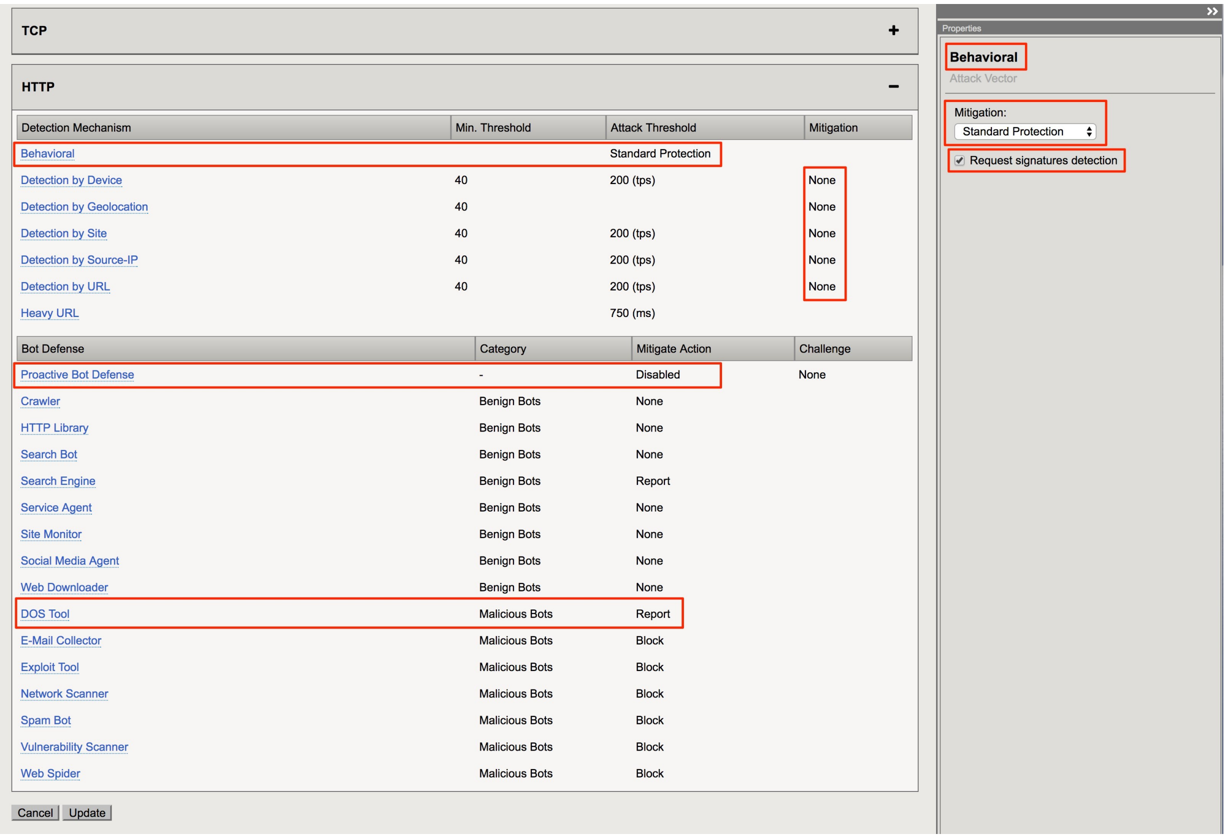
In this exercise we will use a protected object and show how behavioral DDoS works.

Task 1 – Create Protected Object and Launch Attack

- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page and in the Protected Objects section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Name	Auction
IP Address	10.1.20.101
Port / Protocol	80 TCP
VLAN (Selected)	defaultVLAN (uncheck ANY)
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	HTTP

- Make sure **Auction** is with a capital "A".
- Under the HTTP section make the following adjustments:
  - Set Behavioral to Standard Protection.
  - Make sure you check "Request Signature Detection"
  - Set Proactive Bot Defense to "Disabled"
  - Set DOS tool to "Report"



Detection Mechanism	Min. Threshold	Attack Threshold	Mitigation
Behavioral		Standard Protection	
Detection by Device	40	200 (tps)	None
Detection by Geolocation	40		None
Detection by Site	40	200 (tps)	None
Detection by Source-IP	40	200 (tps)	None
Detection by URL	40	200 (tps)	None
Heavy URL		750 (ms)	

Bot Defense	Category	Mitigate Action	Challenge
Proactive Bot Defense	-	Disabled	None
Crawler	Benign Bots	None	
HTTP Library	Benign Bots	None	
Search Bot	Benign Bots	None	
Search Engine	Benign Bots	Report	
Service Agent	Benign Bots	None	
Site Monitor	Benign Bots	None	
Social Media Agent	Benign Bots	None	
Web Downloader	Benign Bots	None	
DOS Tool	Malicious Bots	Report	
E-Mail Collector	Malicious Bots	Block	
Exploit Tool	Malicious Bots	Block	
Network Scanner	Malicious Bots	Block	
Spam Bot	Malicious Bots	Block	
Vulnerability Scanner	Malicious Bots	Block	
Web Spider	Malicious Bots	Block	

Behavioral

Attack Vector

Mitigation: Standard Protection

☑ Request signatures detection

- When finished click **Create**
- From the Good Client CLI, issue the following command.

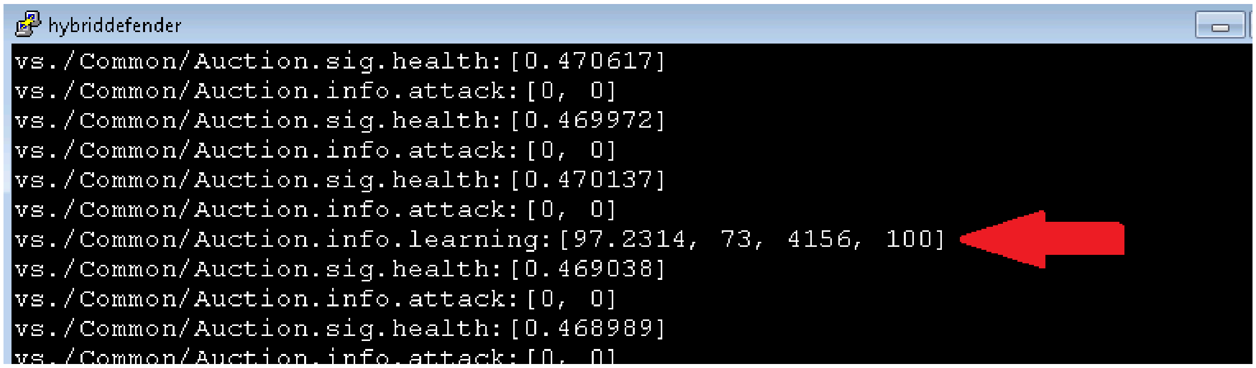
```
~/scripts/generate_clean_traffic.sh
```

Note: This will need to run for approximately 10 minutes.

- From the DHD CLI issue the following commands:

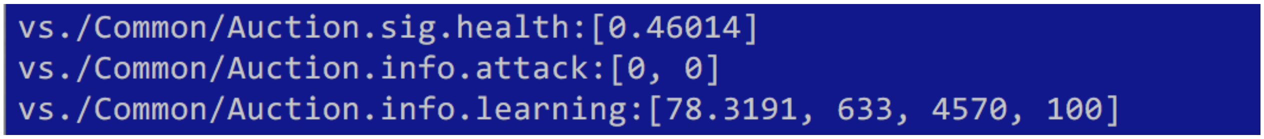
```
#/root/scripts/l7bdos-reset.sh
#/root/scripts/l7-mon.sh
```

- Monitor the window. When you see the following number go to 100, you will move on.



```
vs./Common/Auction.sig.health:[0.470617]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.469972]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.470137]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.info.learning:[97.2314, 73, 4156, 100]
vs./Common/Auction.sig.health:[0.469038]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.468989]
vs./Common/Auction.info.attack:[0, 0]
```

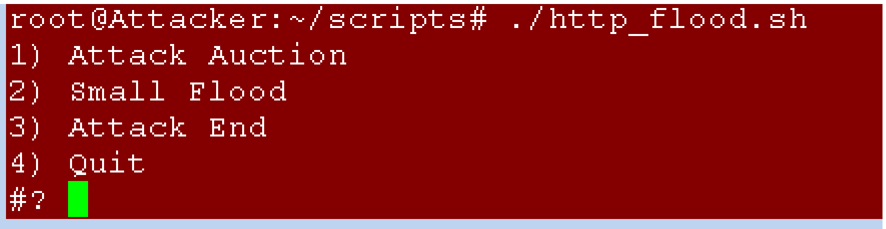
- The health of the Protected Object will be shown. In general, a healthy system will show a value around .45. If the value is .5 consistently, then for some reason no learning is occurring and you should check your configuration and verify that baselining traffic is hitting the protected object in question.
- If the system has detected and is mitigating and attack, or not. This will show in the output of 'info.attack' signal. The two numbers in brackets indicate if there is an attack (1 = yes, 0 = no) and if the system is mitigating that attack (1 = yes, 0 = no).
- The output will also include the 'info.learning' signal, which includes 4 comma-separated values that show the status of the admd behavioral dos learning:



```
vs./Common/Auction.sig.health:[0.46014]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.info.learning:[78.3191, 633, 4570, 100]
```

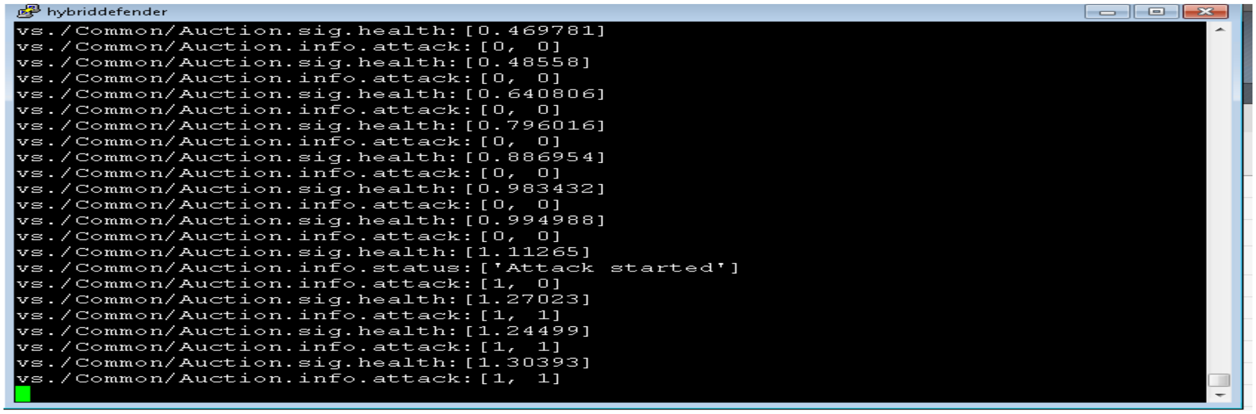
  - signal values: [baseline_learning_confidence, learned_bins_count , good_table_size , good_table_confidence]
  - baseline learning_confidence in % - How confident the system is in the baseline learning.
    - This should be between 80% - 90%
  - learned_bins_count - number of learned bins
    - This should be > 0
  - good_table_size - number of learned requests
    - This should be > 4000
  - good_table_confidence - how confident, as a percentage, the system is in the good table.
    - It must be 100% for behavioral signatures.
- From the Attacker CLI issue the following command:

```
~/scripts/http_flood.sh
```



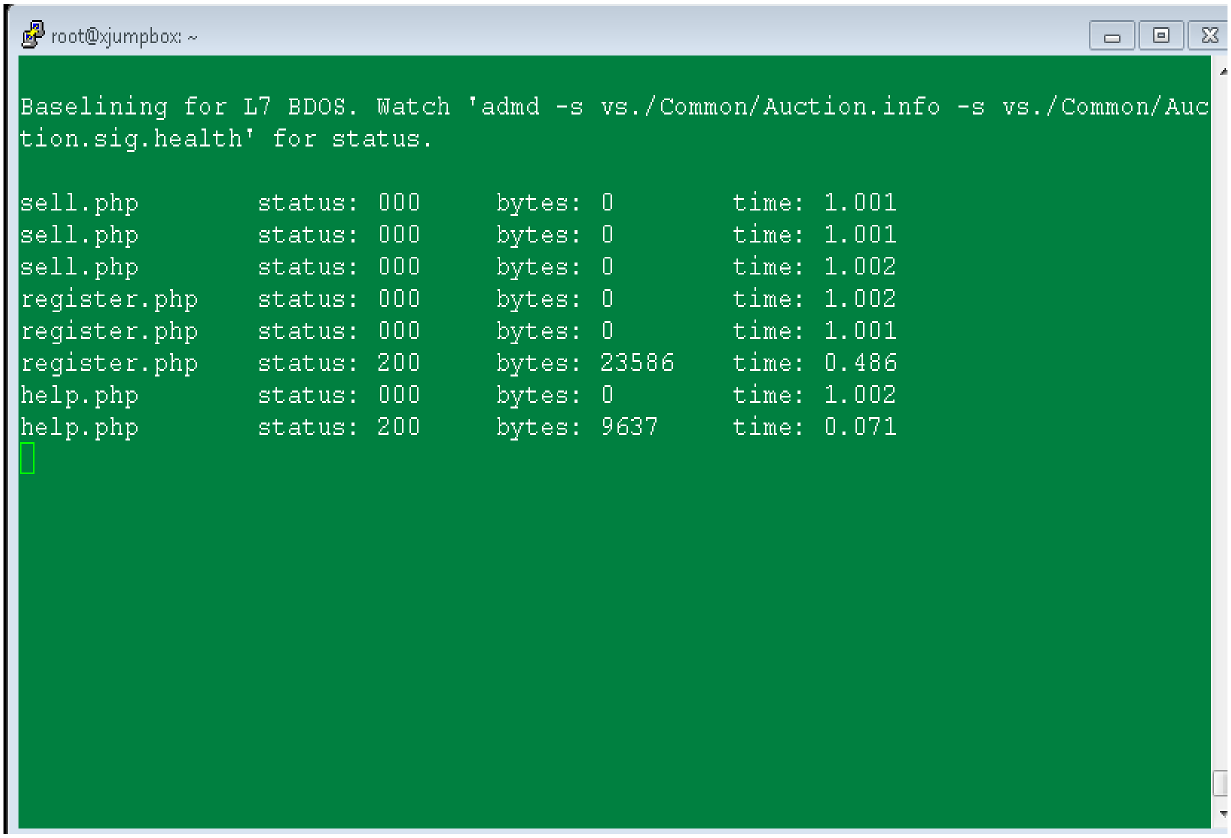
```
root@Attacker:~/scripts# ./http_flood.sh
1) Attack Auction
2) Small Flood
3) Attack End
4) Quit
#?
```

- Choose option **1**, "Attack Auction"
- You will see the attack start in the DHD SSH window:



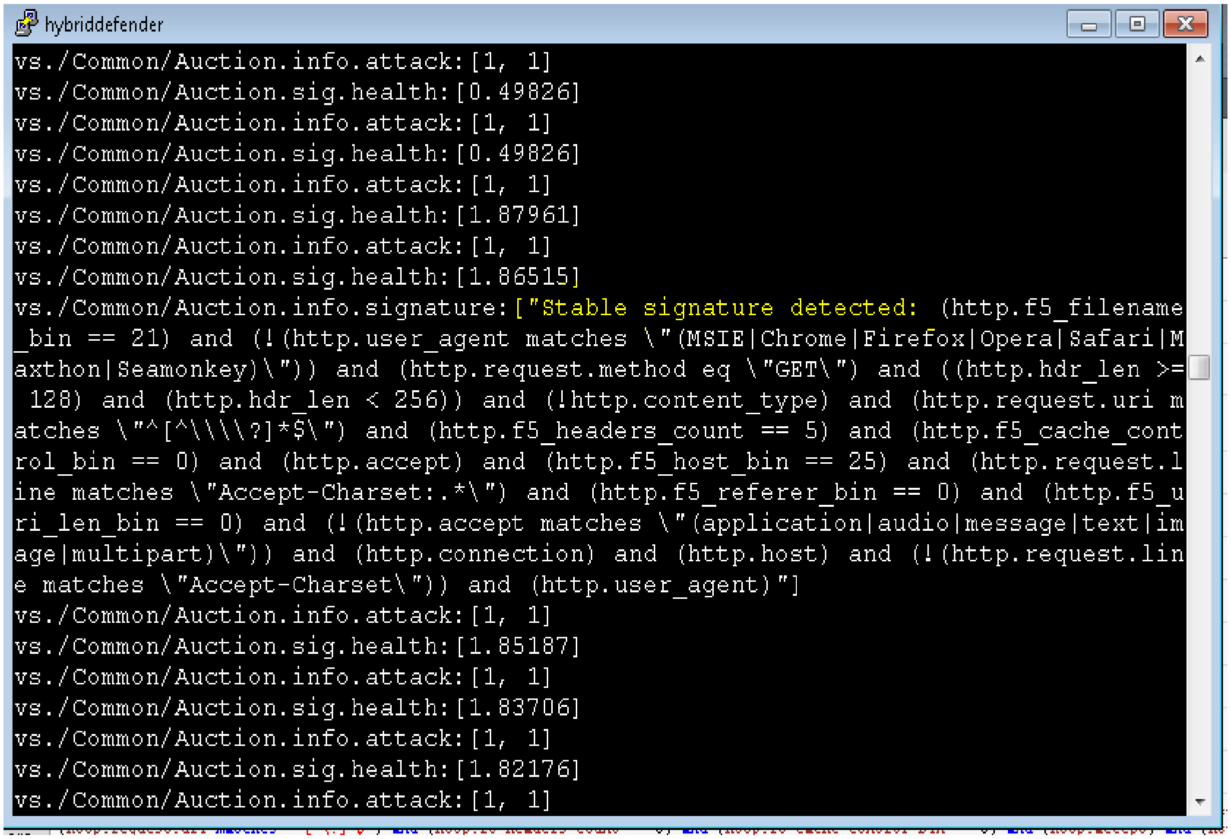
```
vs./Common/Auction.sig.health:[0.469781]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.48558]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.640806]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.796016]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.886954]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.983432]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[0.994988]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.sig.health:[1.11265]
vs./Common/Auction.info.status:['Attack started']
vs./Common/Auction.info.attack:[1, 0]
vs./Common/Auction.sig.health:[1.27023]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[1.24499]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[1.30393]
vs./Common/Auction.info.attack:[1, 1]
```

- In addition you will see the good client start returning a status of 000 as it is unresponsive. It no longer returns a Status 200. Until the DHD starts mitigation.



```
Baselining for L7 BDOS. Watch 'admd -s vs./Common/Auction.info -s vs./Common/Auc
tion.sig.health' for status.

sell.php        status: 000     bytes: 0        time: 1.001
sell.php        status: 000     bytes: 0        time: 1.001
sell.php        status: 000     bytes: 0        time: 1.002
register.php    status: 000     bytes: 0        time: 1.002
register.php    status: 000     bytes: 0        time: 1.001
register.php    status: 200     bytes: 23586    time: 0.486
help.php        status: 000     bytes: 0        time: 1.002
help.php        status: 200     bytes: 9637     time: 0.071
```

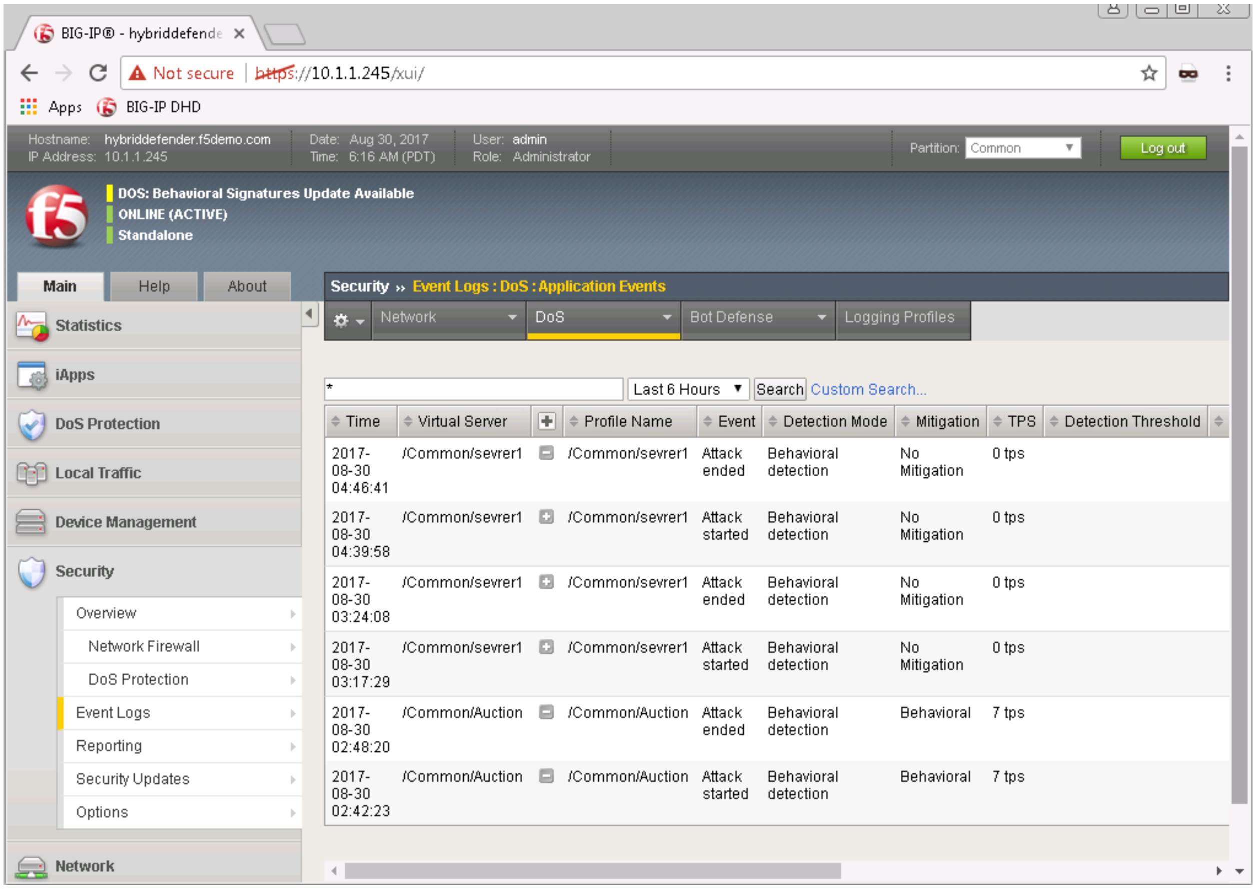
- Once the DHD has enough data a Stable Signature is detected.



```
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[0.49826]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[0.49826]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[1.87961]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[1.86515]
vs./Common/Auction.info.signature:["Stable signature detected: (http.f5_filename
_bin == 21) and (!(http.user_agent matches \"(MSIE|Chrome|Firefox|Opera|Safari|M
axthon|Seamonkey)\")) and (http.request.method eq \"GET\") and ((http.hdr_len >=
 128) and (http.hdr_len < 256)) and (!http.content_type) and (http.request.uri m
atches \"^[^\\\\?]*$\") and (http.f5_headers_count == 5) and (http.f5_cache_cont
rol_bin == 0) and (http.accept) and (http.f5_host_bin == 25) and (http.request.l
ine matches \"Accept-Charset:.*\") and (http.f5_referer_bin == 0) and (http.f5_u
ri_len_bin == 0) and (!(http.accept matches \"(application|audio|message|text|im
age|multipart)\")) and (http.connection) and (http.host) and (!(http.request.lin
e matches \"Accept-Charset\")) and (http.user_agent)"]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[1.85187]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[1.83706]
vs./Common/Auction.info.attack:[1, 1]
vs./Common/Auction.sig.health:[1.82176]
vs./Common/Auction.info.attack:[1, 1]
```

- Let this run for 2 minutes. Stop the attack by pressing “Enter”” a couple of times in the **Attacker** window the choosing option “3” to stop the “Attack”

Note: The DHD does not record the end of the attack right away, it is very conservative, therefore you may have to wait 5 minutes to see the results.



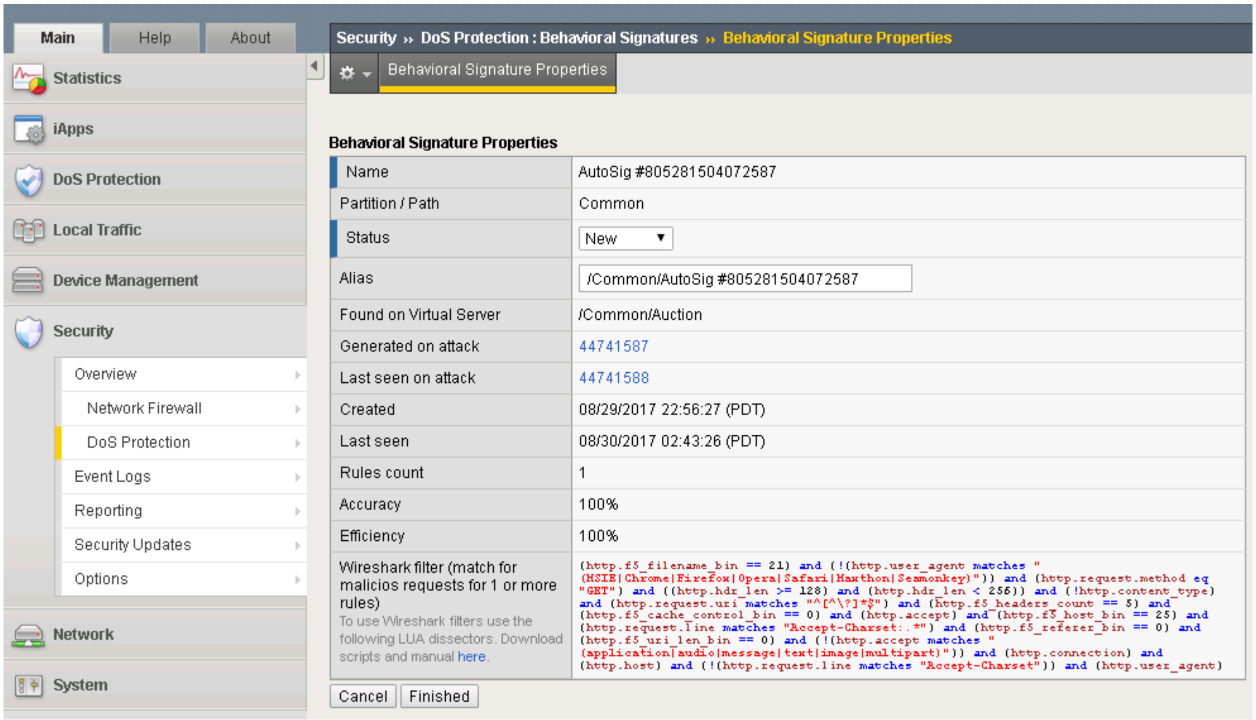
Hostname: hybriddefender.f5demo.com
IP Address: 10.1.1.245
Date: Aug 30, 2017
Time: 6:16 AM (PDT)
User: admin
Role: Administrator
Partition: Common

DOS: Behavioral Signatures Update Available
ONLINE (ACTIVE)
Standalone

Security ›› Event Logs : DoS : Application Events

Time	Virtual Server		Profile Name	Event	Detection Mode	Mitigation	TPS	Detection Threshold
2017-08-30 04:46:41	/Common/sevrer1	⊟	/Common/sevrer1	Attack ended	Behavioral detection	No Mitigation	0 tps	
2017-08-30 04:39:58	/Common/sevrer1	⊞	/Common/sevrer1	Attack started	Behavioral detection	No Mitigation	0 tps	
2017-08-30 03:24:08	/Common/sevrer1	⊞	/Common/sevrer1	Attack ended	Behavioral detection	No Mitigation	0 tps	
2017-08-30 03:17:29	/Common/sevrer1	⊞	/Common/sevrer1	Attack started	Behavioral detection	No Mitigation	0 tps	
2017-08-30 02:48:20	/Common/Auction	⊟	/Common/Auction	Attack ended	Behavioral detection	Behavioral	7 tps	
2017-08-30 02:42:23	/Common/Auction	⊟	/Common/Auction	Attack started	Behavioral detection	Behavioral	7 tps	

- You can see in the top-left that a Behavioral Signature was created.
- Click on this link, then click on the Signature to see it.



Security ›› DoS Protection : Behavioral Signatures ›› Behavioral Signature Properties

Behavioral Signature Properties

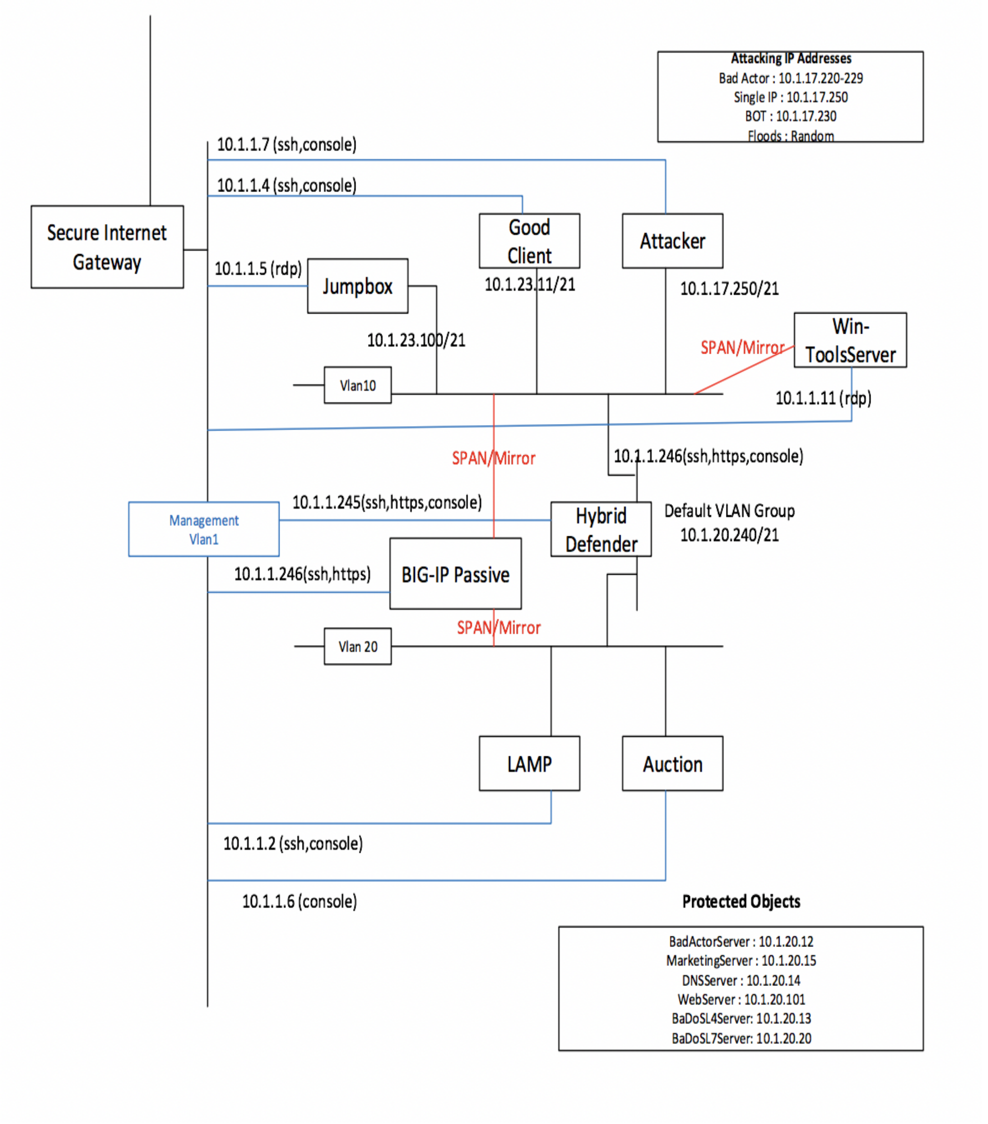
Name	AutoSig #805281504072587
Partition / Path	Common
Status	New
Alias	/Common/AutoSig #805281504072587
Found on Virtual Server	/Common/Auction
Generated on attack	44741587
Last seen on attack	44741588
Created	08/29/2017 22:56:27 (PDT)
Last seen	08/30/2017 02:43:26 (PDT)
Rules count	1
Accuracy	100%
Efficiency	100%
Wireshark filter (match for malicios requests for 1 or more rules) To use Wireshark filters use the following LUA dissectors. Download scripts and manual here.	(http.f5_filename_bin == 21) and (!(http.user_agent matches "(MSIE|Chrome|Firefox|Opera|Safari|Maxthon|Seamonkey)")) and (http.request.method eq "GET") and ((http.hdr_len >= 128) and (http.hdr_len < 256)) and (!http.content_type) and (http.request.uri matches "^[^\?]*$") and (http.f5_headers_count == 5) and (http.f5_cache_control_bin == 0) and (http.accept) and (http.f5_host_bin == 25) and (http.request.line matches "Accept-Charset:.*") and (http.f5_referer_bin == 0) and (http.f5_uri_len_bin == 0) and (!(http.accept matches "(application|audio|message|text|image|multipart)")) and (http.connection) and (http.host) and (!(http.request.line matches "Accept-Charset")) and (http.user_agent)

Cancel Finished

- This concludes the DHD Hands on Labs.

5

5.1 Lab Topology & Environment



5.1.1 Access and Credential Summary

You will be using the Win7 JUMPBOX to access other systems for all labs. You will use Putty that has been preconfigured with appropriate keys to access the Good Client and the Attacker systems. To run scripts, you will need to have root access, requiring you to '**sudo bash**' before running attacks, baselines, etc.

System	Username	Password
Jumpbox	external_user	f5DEMOs4u
Hybrid Defender – WebUI/TMUI	admin	f5DEMOs4u
Hybrid Defender – CLI	root	f5DEMOs4u
Passive BIG-IP – WebUI/TMUI	admin	f5DEMOs4u
Good Client	ubuntu	Use key
Attacker	ubuntu	Use key
Win-ToolsServer	external_user	f5DEMOs4u
WebServer / Auction Server	root	default

5.1.2 Helpful Tips and Tricks

Here are a few tips that you can use during the labs. Since the environment and all its components are running in a virtualized environment with limited shared resources you may encounter some slow performance.

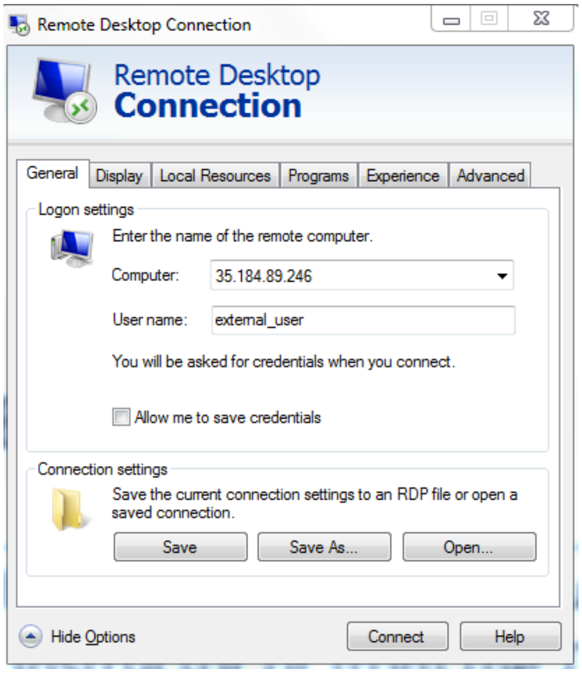
1. When using the Wireshark tool, it will capture a lot of packets. During DDoS attacks the tool will be overwhelmed. Its recommended that you start the capture and then stop it soon so that you can view the data captured easily.
2. If you find that you are not seeing any attacks then go back and check if the Attack you launched is still running. If it has stopped, kindly relaunch it.
3. If an attack is not being detected on the DHD check the value of your detection threshold EPS. For an attack to be detected this value must be lower than the attack being launched. Similarly, the rate/leak limit value sets the threshold for dropping the packets.
4. During automatic/behavioral mitigations labs there is about 10-15 minutes of baseline traffic learning time for the Hybrid Defender. Use that time to ask questions, chat with F5 Engineers and/or your peers about DDoS mitigations, security and what they are doing in their organization. Additionally, browse around the DoS Visibility tool to see some cool graphical reports that were generated.
5. Make sure the name of the Protected Objects you create in various labs matches exactly to what is provided in this guide otherwise the scripts/commands for monitoring learning status will not work as they are tied to specific profile names that get created.
6. You will notice that the commands “**sudo bash**” “**cd f5agility**” are included in each step. If you are already logged in and have root privileges and in the f5agility folder then kindly ignore those steps. If not, then use them. Basically, you need root level access to execute the scripts and be in the f5agility folder/directory.
7. Since the WebUI/TMUI will look the same for the BIG-IP Passive and the Hybrid Defender device make sure that all mitigation/changes are being made to the Hybrid Defender only and the Passive device is used only for visibility.
8. Don’t forget to use CTRL+C to break and stop the attacks so that you get better responses from various tools once you have enough data.
9. When starting a new capture in WireShark always select continue without saving when prompted.
10. Use Right click and “Open in new tab” to browse various DHD menus (Overview, Event Logs,etc) so you don’t have to go back and forth.
11. **STOP** all attacks, good traffic baseline scripts after end of each lab before proceeding to the next lab.
12. Use the PuTTY shortcuts on the desktops to access various shells. The PuTTY window has a title on top so that you know which shell you are in. If you get a Security Alert for the Servers Host Key just click YES to proceed to connect to the shell.

5.1.3 Accessing the Lab Environment

Use RDP client and connect to your Windows Jumpbox IP and the Win-ToolsServer IP

Note: Use the show options to provide

User name: external_user. Password: f5DEMOs4u



Remote Desktop Connection

Remote Desktop Connection

General | Display | Local Resources | Programs | Experience | Advanced

Logon settings

Enter the name of the remote computer.

Computer: 35.184.89.246

User name: external_user

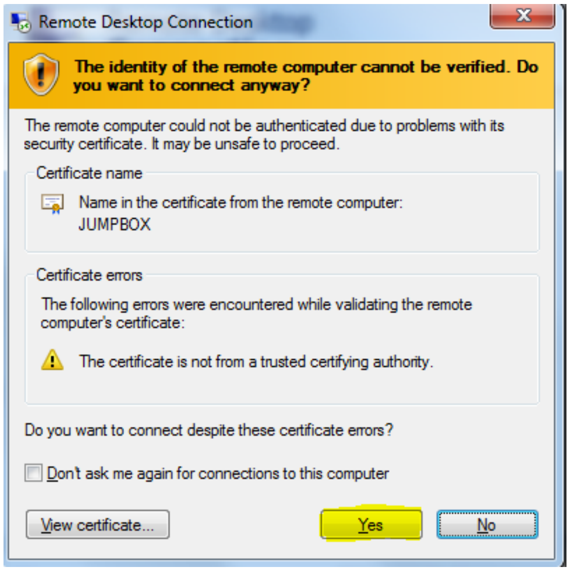
You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Click YES at the warning



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
JUMPBOX

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

⚠ The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

All Exercises/Tasks are to be completed from the Windows Jumpbox. There are various shortcuts – Chrome Incognito, Putty shortcuts, on the Jumpbox that you will use through the exercises.

5.2 Introduction to DDoS Hybrid Defender

F5 DDoS Hybrid Defender (DHD) protects your organization against a wide range of DDoS attacks using a multi-pronged approach. By combining on-premises and cloud technologies, analytics, and advanced methods, DDoS Hybrid Defender is a hybrid solution that detects network and application layer attacks and is easy to deploy and manage.

DDoS Hybrid Defender mitigates against the full spectrum of DDoS attacks including:

- Network capacity attacks
- DNS and SIP protocol volumetric attacks
- HTTP and HTTPS volumetric attacks
- HTTP and HTTPS CPU-based (heavy URL) attacks

You can specify which objects to protect on the network, assigning the appropriate protections to network devices and application servers, and prevent attackers from exhausting network resources and impacting application availability.

Deployments:

The deployment you use for DDoS Hybrid Defender depends on the needs of your organization. For maximum DDoS protection, it is recommended that you deploy DDoS Hybrid Defender inline. However, it can also be deployed out of band, or in locations where symmetric data flows are not guaranteed.

Typical locations for the placement of DDoS Hybrid Defender are at the edge of the network or at the edge of the data center

Inline deployment

DDoS Hybrid Defender provides maximum protection when deployed inline in one of two ways:

- Bridged mode with VLAN groups (This is default and we will use in our labs)
- Routed mode

Out of band deployment

You can deploy DDoS Hybrid Defender out of band in two ways:

- Set up a Layer 2 switch with span ports so that it mirrors traffic onto DDoS Hybrid Defender. (Our passive device is setup this way in our labs)
- Configure network devices so that they send NetFlow data to DDoS Hybrid Defender.

5.3 Module 1: Environment Review

5.3.1 Lab 1.1 – Review Tools and Environment

You are the security engineer for Acme corporation. Your organization has recently seen a lot of outages in your network and applications. Some of these have been due to DDoS attacks and the outages have caused a significant loss of revenue as well as reputational impact. You have made the wise decision to invest in a world class leading edge DDoS mitigation solution and have the F5 DHD installed in your environment. It's been configured in the Layer 2 inline mode and is now available to you to enforce DDoS mitigations.

Tools:

#. In our lab we have an additional DHD available to you in a passive mode. It's basically setup on SPAN ports (out of band deployment) to provide you visibility.

#. The Win-ToolsServer is also installed to listen on SPAN port and has Wireshark available for visibility.

Let's get familiar on how to use these tools.

Note: Not all attacks will be visible in both tools. So, use the tools accordingly. This is done purposefully so that you get into the habit of troubleshooting/fighting attacks in the real world.

Use a web browser (Chrome in incognito mode) to log into the WebUI of the Passive DHD at https://10.1.1.246 or use the bookmarked shortcut. Accept the SSL warning and proceed to connect.

Username: *admin*

Password: *f5DEMOs4u*

- Click **Security>>Event Logs>>DoS>>Network>>Events**
- Click **Security>>DoS Protection>>DoS Overview** (Tip: Right Click and open link in new tab/window)
- You will use the above two screens on the Passive DHD for visibility of traffic/attacks.
- On the Win-Tools Server launch Wireshark by using the shortcut link on desktop and then click on the blue shark fin on top left corner to start capturing data. (Tip: Use the Red Square button to stop captures when needed)

5.3.2 Lab 1.2 – Launch an attack and view traffic

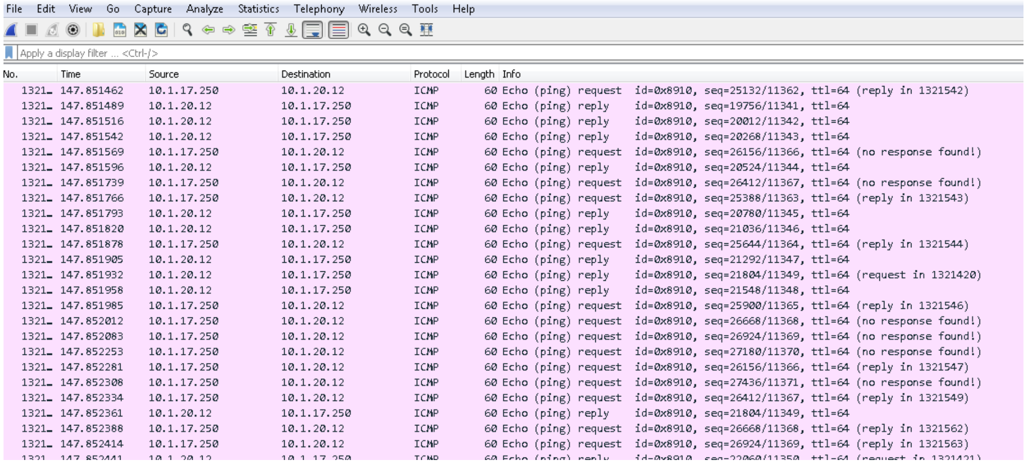
- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

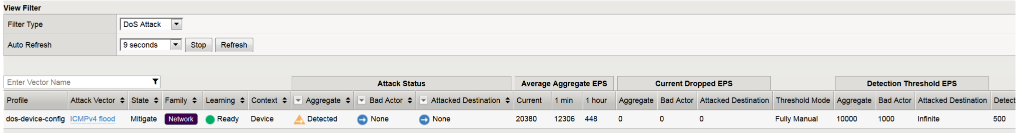
```
# ./lab1-2.sh
```

- View Wireshark and notice the ongoing captures.
- What type of traffic do you notice? As you can see these are all ICMP requests/responses and a lot of them. What are the IP addresses involved? Can you identify the attacking IP? (Tip: Did you review the lab network diagram?)



```
No.     Time          Source         Destination    Protocol  Length Info
  1321… 147.851462    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=25132/11362, ttl=64 (reply in 1321542)
  1321… 147.851489    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=19756/11341, ttl=64
  1321… 147.851516    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=20012/11342, ttl=64
  1321… 147.851542    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=20268/11343, ttl=64
  1321… 147.851569    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26156/11366, ttl=64 (no response found!)
  1321… 147.851596    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=20524/11344, ttl=64
  1321… 147.851739    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26412/11367, ttl=64 (no response found!)
  1321… 147.851766    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=25388/11363, ttl=64 (reply in 1321543)
  1321… 147.851793    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=20780/11345, ttl=64
  1321… 147.851820    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=21036/11346, ttl=64
  1321… 147.851878    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=25644/11364, ttl=64 (reply in 1321544)
  1321… 147.851905    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=21292/11347, ttl=64
  1321… 147.851932    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=21804/11349, ttl=64 (request in 1321420)
  1321… 147.851958    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=21548/11348, ttl=64
  1321… 147.851985    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=25900/11365, ttl=64 (reply in 1321546)
  1321… 147.852012    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26668/11368, ttl=64 (no response found!)
  1321… 147.852083    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26924/11369, ttl=64 (no response found!)
  1321… 147.852253    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=27180/11370, ttl=64 (no response found!)
  1321… 147.852281    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26156/11366, ttl=64 (reply in 1321547)
  1321… 147.852308    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=27436/11371, ttl=64 (no response found!)
  1321… 147.852334    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26412/11367, ttl=64 (reply in 1321549)
  1321… 147.852361    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=21804/11349, ttl=64
  1321… 147.852388    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26668/11368, ttl=64 (reply in 1321562)
  1321… 147.852414    10.1.17.250    10.1.20.12     ICMP          60 Echo (ping) request  id=0x8910, seq=26924/11369, ttl=64 (reply in 1321563)
  1321… 147.852441    10.1.20.12     10.1.17.250    ICMP          60 Echo (ping) reply    id=0x8910, seq=22060/11350, ttl=64 (request in 1321421)
```

In the Passive DHD Windows what do you notice? (Tip: You may need to click Search button/Refresh button or set Auto Refresh)

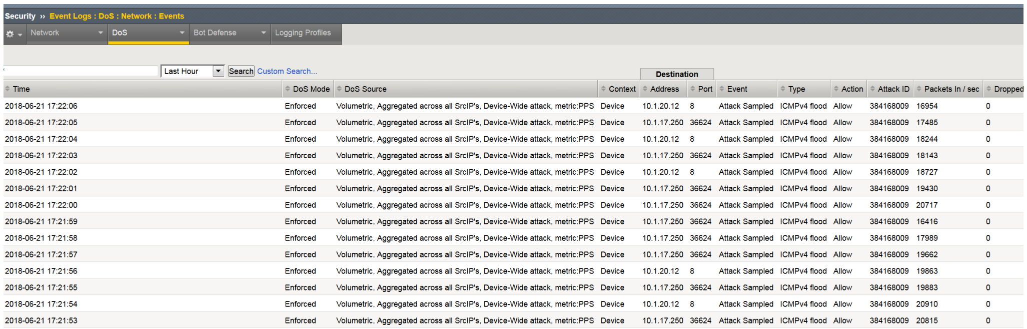


View Filter

Filter Type: DoS Attack

Auto Refresh: 9 seconds

						Attack Status			Average Aggregate EPS			Current Dropped EPS				Detection Threshold EPS			
Profile	Attack Vector	State	Family	Learning	Context	Aggregate	Bad Actor	Attacked Destination	Current	1 min	1 hour	Aggregate	Bad Actor	Attacked Destination	Threshold Mode	Aggregate	Bad Actor	Attacked Destination	Detect
dos-device-config	ICMPv4 flood	Mitigate	Network	● Ready	Device	⚠ Detected	None	None	20380	12306	448	0	0	0	Fully Manual	10000	1000	Infinite	500



Security ›› Event Logs : DoS : Network : Events

				Destination							
Time	DoS Mode	DoS Source	Context	Address	Port	Event	Type	Action	Attack ID	Packets In / sec	Dropped
2018-06-21 17:22:06	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.20.12	8	Attack Sampled	ICMPv4 flood	Allow	384168009	16954	0
2018-06-21 17:22:05	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	17485	0
2018-06-21 17:22:04	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.20.12	8	Attack Sampled	ICMPv4 flood	Allow	384168009	18244	0
2018-06-21 17:22:03	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	18143	0
2018-06-21 17:22:02	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.20.12	8	Attack Sampled	ICMPv4 flood	Allow	384168009	18727	0
2018-06-21 17:22:01	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	19430	0
2018-06-21 17:22:00	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	20717	0
2018-06-21 17:21:59	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	16416	0
2018-06-21 17:21:58	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	17989	0
2018-06-21 17:21:57	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	19662	0
2018-06-21 17:21:56	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.20.12	8	Attack Sampled	ICMPv4 flood	Allow	384168009	19863	0
2018-06-21 17:21:55	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	19883	0
2018-06-21 17:21:54	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.20.12	8	Attack Sampled	ICMPv4 flood	Allow	384168009	20910	0
2018-06-21 17:21:53	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide attack, metric:PPS	Device	10.1.17.250	36624	Attack Sampled	ICMPv4 flood	Allow	384168009	20815	0

As you can see the visibility is better in terms of the Attack Vector and number of packets in/sec on the passive DHD.

It's up to you on which tool you may want to use for the remaining labs. If you are comfortable with WireShark then use that or use the Passive DHD or both. As noted previously you will have to visit both tools to see where you can gather some visibility to fight a real-world DDoS attack.

Use CTRL+C in the attacker shell to stop the attack.

5.4 Module 2: Manual Mitigations

5.4.1 Lab 2.1 – Device Level Protection for Mitigating Attacks.

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-1.sh
```

- On the WireShark start a capture/stop and identify the ongoing attack.
- On the Passive DHD identify the ongoing attack.
- Did you identify the attack? What type of attack is it? What Source IPs and Destinations IPs are involved?
- Let's mitigate this attack using Device Level mitigation.

Log into the DHD https://10.1.1.245 accept the SSL warning and proceed to connect with credentials provided.

- In the Configuration Utility, go to **DoS Protection>>Quick Configuration.**
- In the **Device Protection** section click **Device Configuration.**
- In the **Flood** row click the + icon, and then click **ICMPv4** flood.
- On the right-side of the page select the drop-down to **"Mitigate"**

Parameter	Value
Mitigation	Fully Manual
Detection Threshold EPS	100
Detection Threshold Percent	500
Rate/Leak Limit	500

- On the Hybrid Defender you will now see the attack is being mitigated (Where will you check this? Tip: It's the same places that you are looking on the Passive device). You have successfully mitigated a network flood single vector attack. Use CTRL+C in the attacker window to stop the attack.

5.4.2 Lab 2.2 – Device Level Protections for Mitigating Attacks

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-2.sh
```

- On the WireShark start a capture/stop and identify the ongoing attack.
- On the Passive DHD identify the ongoing attack.
- Did you identify the attack? What type of attack is it? What Source IPs and Destinations IPs are involved?

Mitigate this attack using Device Level mitigation steps like those that you did in Lab 2.1 above.

5.4.3 Lab 2.3 – Device Level Protections for Mitigating Attacks

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-3.sh
```

- On the WireShark start a capture/stop and identify the ongoing attack.
- Did you identify the attack? What type of attack is it? What Source IPs and Destinations IPs are involved? Look closely and you will notice that there is a range of destination IPs that are being targeted and a lot of SYN, Retransmit, Out of Sequence, RST packets. This looks like someone is trying to run a scan against your network. How will you mitigate against this? They are "Sweep"ing your network.
- In the Configuration Utility, in the **Device Protection** section click **Device Configuration.**
- In the **Single Endpoint** row click the + icon, and then click **Single Endpoint Sweep**.
- On the right-side of the page select the drop-down to **"Mitigate"**

Parameter	Value
Detection Threshold EPS	100
Rate/Leak Limit	500
Packet Types (Selected)	All IPv4

- On the Hybrid Defender you will now see the attack is being mitigated. This attack is short lived so make sure you launch it again if it has stopped to see the mitigation. You have successfully mitigated a sweep flood attack. Use CTRL+C in the attacker window to stop the attack.

5.4.4 Lab 2.4 – Device Level Protections for Mitigating Attacks

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-4.sh
```

- On the WireShark start a capture/stop and identify the ongoing attack.
- On the Passive DHD identify the ongoing attack.
- Did you identify the attack? What type of attack is it? What Source IPs and Destinations IPs are involved?
- Use the manual mitigations steps you learned in previous tasks to mitigate against all the attack vectors that you have identified.
- Use CTRL+C in the attacker window to stop the attack.

5.4.5 Lab 2.5 – Device Level Protections for Mitigating Attacks

You received a call that a lot of users are intermittently getting a page cannot be displayed for various applications. Your Network Operations Center has stated that none of their monitoring systems for those applications are reporting any outages. The NOC tools monitor application health using the application URLs like http://10.1.20.12/index.php and so on. Your users are using the application using the FQDNs. You suspect that there is an ongoing DDoS attack and you need to identify it and mitigate against it.

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-5.sh
```

- On the WireShark start a capture/stop and identify the ongoing attack.
- Let's look at an alternate way to see which vector is being triggered so that you can identify the attack. If in your environment you had no tools like the Wireshark or the Passive DHD device, you can still identify the attack. While the event logs, DoS Overview screens are populated only when an attack is detected based on the threshold values set, if the attack doesn't trigger the detection threshold you will not see it in the Overview and Event Logs.
- In the Configuration Utility of the Hybrid Defender, go to **DoS Protection>>Quick Configuration.**
- In the **Device Protection** section click **Device Configuration.**
- In the **DNS** row click the **+** icon, and then view the Current Device Statistics Section. You can see that we are triggering a vector and registering the packets for that vector even though we have the default detection/mitigation configured for it.
- Alternately there is a CLI command also available to view the attack vector that is being triggered. Open a putty shell to the Hybrid Defender (use shortcut on desktop), login with the credentials: root/f5DEMOs4u and then :

```
# cd f5agility
```

```
# ./show_attackvector_stats.sh
```

- Did you identify the attack? What type of attack is it? What Source IPs and Destinations IPs are involved? Hint: (Wireshark) Destination IP, Targeted Port and Protocol used.
- Use the manual mitigations steps you learned in previous tasks to mitigate against the attack vector that you have identified.
- Use CTRL+C in the attacker window to stop the attack.

5.4.6 Lab 2.6 – Protected Object Level Protections for Mitigating Attacks

You mitigated a DNS vector attack above at device level. You have again received a call that a lot of users are intermittently getting a page cannot be displayed for various applications. Your Network Operations Center has stated that none of their monitoring systems for those applications are reporting any outages. The NOC tools monitor application health using the application URLs like http://10.1.20.12/index.php and so on. Your users are using the application using the FQDNs. You suspect that there is an ongoing DDoS attack and you need to identify it and mitigate against it. You don't want to implement a mitigation for a vector device wide and want to specifically mitigate the suspected victim server.

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-6.sh
```

- On the WireShark start a capture/stop and identify the ongoing attack.
- On the Passive DHD identify the ongoing attack.
- Did you identify the attack? What type of attack is it? What Source IPs and Destinations IPs are involved?
- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page.
- In the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create.**

Parameter	Value
Name	DNSServer
IP Address	10.1.20.14
Port	53
Protocol	UDP
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	DNS

- In the **DNS** row click the **+** icon, and then click **DNS A Query**.
- On the right-side of the page configure using the following information, and then click **Create**.

Parameter	Value
Detection Threshold EPS	Specify: 10
Detection Threshold Percent	Specify: 500
Mitigation Threshold EPS	Specify: 100

- On the Hybrid Defender you will now see the attack is being detected/mitigated. You have successfully mitigated a DNS A Query flood. Use CTRL+C in the attacker window to stop the attack.

5.4.7 Lab 2.7 – Protected Object Level Protections for Mitigating Attacks

There has been a high-profile DDoS attack and you must provide Law Enforcement some details on the offending IP addresses. In your environment at any given time you have a few hundred thousands of IP addresses observed on your network. You want to identify a few offending IP addresses and blacklist them so that you can provide the details to Law Enforcement.

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-7.sh
```

- On the WireShark start a capture and identify the ongoing attack.
- Did you identify the attack? What type of attack is it? What Source IPs and Destinations IPs are involved? Make a note of the protocol of attack and the destination IP (target).
- We will build a protected object and use Bad Actor Detection and Black Listing.
- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page
- In the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create.**

Parameter	Value
Name	BadActorServer
IP Address	10.1.20.12
Port	*
Protocol	All
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	UDP

- In the **UDP** row click the **+** icon, and then click **UDP Flood**.
- On the right-side of the page configure using the following information, and then click **Create**.

Parameter	Value
Detection Threshold PPS	Specify: 100
Detection Threshold Percent	Specify: 500
Mitigation Threshold EPS	Specify: 200
Bad Actor Detection	Checked
Per Source IP Detection Threshold	100
Per Source IP Mitigation Threshold	30
Blacklist Attacking Address	Checked
Sustained Attack Detection Time	15
Category Duration Time	120

- On the Hybrid Defender you will now see the attack is being detected/mitigated.
- View the offending IP addresses at **Security>>Event Logs>>Network>>IP Intelligence**
- View the Shun list / Blacklist at **Security>>Event Logs>>Network>>Shun**

- You have successfully identified the Bad Actors and put them in a Blacklist. Use CTRL+C in the attacker window to stop the attack.

5.4.8 Lab 2.8 – Whitelisting

You get a call from your QA team that is running load runner scripts against your application server 10.1.20.12 that they are seeing packets being dropped. You ask them what's the source IP address of the server they are running the load runner script from and they provide you with 10.1.17.225.

- Why do you think their packets are being dropped? Hint: Check the blacklist (**Event Logs>>Network>>Shun**). They have been added to that list. You will now need to maintain the mitigations in place and only allow 10.1.17.225 to not be enforced with any DDoS mitigations going to 10.1.20.12.
- Go to the protected object 10.1.20.12 and add the IP to the whitelist.
- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-7.sh
```

- View the offending IP addresses at **Security>>Event Logs>>Network>>IP Intelligence** and **Security>>Event Logs>>Network>>Shun** and confirm that 10.1.17.225 is not being added to the list.
- You have successfully whitelisted an IP to bypass DDoS mitigations. Use CTRL+C in the attacker window to stop the attack.

5.4.9 Lab 2.9 – BOT Defense for Application Attacks.

HTTP DoS attacks are very popular. Some can be in form of HTTP Floods and some can be low and slow attacks (slow loris, slow post, slow read). They have been used by BOTS to bring down a site. Sometimes even though the BOTS don't bring the site down they demand for you to stand up additional infrastructure to support the traffic they are generating costing your organization a significant spend when it can be mitigated and avoided. Your organization just published a brand-new web application. As soon as it was available to public you started getting calls that the site is sometimes unavailable and slow to respond. Based on the predicted traffic patterns one server was enough to handle the valid user load. The application team viewed the web server logs and noticed that there is 30% additional traffic then predicted from what seems like automated tools. Your IT management has asked you to provide a solution on what's driving up the traffic to the server and potentially mitigate it. You will now learn how to manually mitigate BOT traffic.

- Open a PuTTY shell to the WebServer (use the shortcut on the desktop). Login with credentials: root/default. You will use the webservers log to monitor the requests coming to the server. Once logged into the WebServer shell:

```
# cd /usr/local/apache/logs
```

```
# tail -f access_log
```

- Hit the Enter key a few times so that you can see incoming requests clearly in the blank space.
- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack to simulate BOT traffic:

```
# sudo bash
```

```
# cd f5agility
# ./lab2-9.sh
```

- We are just simulating 25 requests so that it's a controlled environment and you can view the requests/logs.
- View the WebServer shell where you have the tail -f access_log running. Do you see the requests come in? What's the source IP address of the requests?
- As you can see the site is available to everyone including BOTS. You have not set this up on the DHD and hence no BOT protection is applied.
- You will now publish the website through the DHD with needed protections.
- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page and in the Protected Objects section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Parameter	Value
Name	WebServer
IP Address	10.1.20.101
Port	80
VLAN (Selected)	**defaultVLAN (uncheck ANY)**
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	IPv4, TCP, HTTP

- By simply creating the Protected Object and applying HTTP protections the BOT protections are automatically turned on. Everyone will now access the web application through the DHD with mitigations enforced.
- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack to simulate BOT traffic:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab2-9.sh
```

- View the WebServer log (tail -f access_log) in the shell. You will not see requests come through this time from the attacker.
- View the mitigation in **Security>>Event Logs>>Bot Defense>>Requests.** All the requests from the BOT are blocked.
- Open a firefox browser on the Jumpbox and go to http://10.1.20.101. This request will open your web application and its not blocked as it's not a BOT. You will also see the request in the WebServer log shell.
- View the valid request from your browser in the DHD in **Security>>Event Logs>>Bot Defense>>Requests.** You will notice that valid requests are being challenged and allowed only after a valid response. Note: There is a default grace period of 300s when the mitigation is implemented so some requests are allowed as grace. This is Proactive BOT defense in action.
- View the BOT Defense in **Security>>Reporting>>DoS>>Analysis** and look at the graph under HTTP -> Transaction Outcomes. **Please be patient as these graphs are usually populated with a delay.**

  You have successfully mitigated BOT traffic to your application. CTRL+C in all shell windows and close them all.

5.5 Module 3: Automatic Mitigations

5.5.1 Lab 3.1 – Auto Thresholding for Mitigating Attacks.

Your organization is about to launch a new marketing campaign and there is a website that will host the content. You want to make sure that the application is protected against DDoS attacks but are not sure what traffic patterns are or what values to set for detections/rate limits/mitigations. You will create a Protected Object for the marketing website and use automatic mitigations.

- In the BIG-IP Configuration Utility, open the **DoS Protection>>Quick Configuration** page and in the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create**.

Parameter	Value
Name	MarketingServer
IP Address	10.1.20.15
Port	*
Protocol	All Protocols
Protection Settings: Action	Log and Mitigate
Threshold Sensitivity	High
Protection Settings: DDoS Settings	IPv4, TCP,

Generate some good traffic to the marketing server.

- Putty SSH (use the shortcut) to open a shell to the good client system.
- Login as user: ubuntu. The session is preconfigured to authenticate with a certificate.
- Start the auto-threshold baselining script with:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./auto_baseline.sh
```

Let this baseline traffic run for at least 10 minutes before proceeding to the below step.

In our lab we need to roll back the device level protection so that it doesn't mitigate the stress we are generating for the auto-threshold on the MarketingServer.

- In the Configuration Utility, in the **Device Protection** section click **Device Configuration.**
- In the **Flood** row click the + icon, and then click **ICMPv4** flood.
- On the right-side of the page select the drop-down to **"Detect-Only"**

Parameter	Value
Mitigation	Fully Manual
Detection Threshold EPS	Infinite
Detection Threshold Percent	500
Rate/Leak Limit	Infinite

Click **Update** at the bottom of the screen. This will allow our attack to pass through to the automatic mitigation profile of the MarketingServer that we are configuring below.

In the Hybrid Defender WebUI, for the **MarketingServer** Protected Object configuration, enable auto-thresholding for the following vectors: **ICMPv4 Flood, TCP SYN Flood, TCP Push Flood, TCP RST**

Flood, TCP SYN ACK Flood by selecting each vector and **clicking the "Fully Automatic" Configuration radio button**. When all vectors are configured, click **Update** at the bottom of the screen.

- In the Hybrid Defender WebUI, view the Auto Threshold event log by navigation to **Security>>Event Logs>>DoS>>Network>>Auto Threshold**.

  The system is updating the detection thresholds. With auto-thresholding, the system adjusts the detection thresholds based on observed traffic patterns. However, mitigation rate limits are always dynamic based on detected system or protected object stress. If anomalous levels of traffic are running, but there is no stress, the Hybrid Defender will generate alerts but will not block traffic. Under stress, the rate limits are automatically created and adjusted dynamically.

  Generate some stress by launching an attack.

  Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab3-1.sh
```

Keep on refreshing the Auto Threshold event log **Security>>Event Logs>>DoS>>Network>>Auto Threshold** and observe how the values are changing dynamically. Even though our attack is ICMPv4 flood the other vectors that are set to Fully Automatically are also being adjusted dynamically.

View **Security>>DoS Protection>>DoS Overview.** Notice how automatic detection and mitigation is happening as stress varies.

Stop all scripts and attacks using CTRL + C.

5.5.2 Lab 3.2 – Behavioral L4 for Mitigating Attacks

In this lab you will use the Hybrid Defender's network behavioral DoS analysis capabilities and its ability to interpret behavioral history and stress to automatically generate and enforce a precise, dynamic signature. This capability allows the granular filtering of the good from the bad, which is a major challenge in DoS mitigation. The bad must be accurately identified to mitigate the DoS attack, particularly if the attack changes over time. Enforcement of a very precise signature, with enforcement thresholds based on system or network stress signals, dramatically reduces false positives—increasing network and application availability.

- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page
- In the **Protected Objects** section click **Create.**
- Configure a protected object using the following information, and then click **Create.**

Parameter	Value
Name	BaDoSL4Server
IP Address	10.1.20.13
Port	*
Protocol	All Protocols
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	IPv4, TCP, L4 Behavioral

- In the **L4 Behavioral** row click the **+** icon.
- Configure under Dynamic Signatures using the following information, and then click **Create**.

Parameter	Value
Learn Only	Unchecked
Mitigation Sensitivity	High

- Putty SSH (use the shortcut) to open a shell to the good client system.
- Login as user: ubuntu. The session is preconfigured to authenticate with a certificate.
- Start the behavioral L4 baselining script with:

```
# sudo bash
# cd f5agility
# ./baseline_L4.sh
```

You can monitor the learning progress on the DHD.

- Putty SSH (use the shortcut) to open **two shells** to the HybridDefender.
- Login as user: root and password provided.
- View the behavioral L4 baselining learning with following in 1st shell. Notice the learning phase In Progress.

```
# cd f5agility
# ./show_baseline_L4_status.sh
```

- View the behavioral L4 baselining bins populating in 2nd shell.

```
# cd f5agility
# ./show_baseline_L4_bins.sh
```

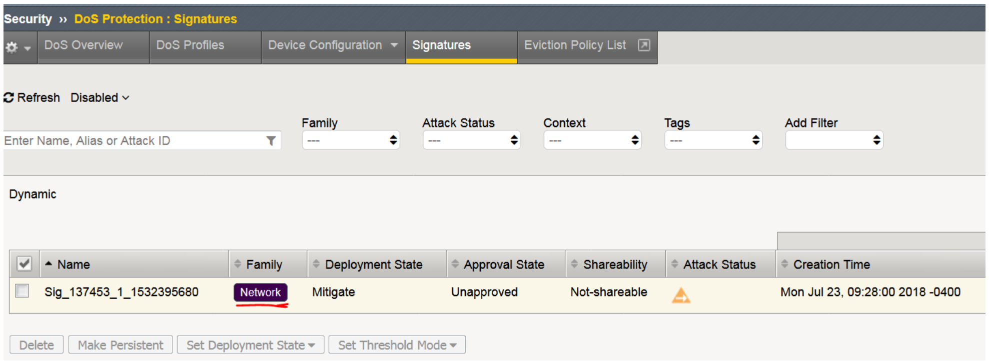
- While the learning is happening, we need to turn off some manual mitigations at Device Level as they will block our attack that is going to create stress to trigger dynamic signatures.
- In the Configuration Utility, in the **Device Protection** section click **Device Configuration.**
- In the **Flood** row click the + icon, and then change click **TCP SYN Flood, TCP SYN Oversize** and change the attack vector to **"Detect-Only"**.
- In the **Single Endpoint** row click the + icon, and then change click **Single Endpoint Sweep** and change the attack vector to **"Detect-Only"**.

Make sure the status is changed from "In Progress" to "Finished" for the learning phase on the DHD before proceeding to the next steps below (about 15 minutes)

- Access the Attacker System CLI/shell and launch the attack:

```
# sudo bash
# cd f5agility
# ./lab3-2.sh
```

On the Hybrid Defender you will now see the attack is being detected/mitigated. . Did you notice the dynamic signatures in DoS Overview window? Give it a couple of minutes and it will show up. You can view the signature **Security>>DoS Protection>>Signatures** under Dynamic Signature section. Click on the "Network" (not the signature hyperlink) to view details of the signature.



☑	Name	Family	Deployment State	Approval State	Shareability	Attack Status	Creation Time
□	Sig_137453_1_1532395680	Network	Mitigate	Unapproved	Not-shareable	⚠	Mon Jul 23, 09:28:00 2018 -0400

Use CTRL+C in all shells - attacker, good traffic, DHD to stop all scripts.

5.5.3 Lab 3.3 – Behavioral L7 for Mitigating Attacks

In this lab you will use the Hybrid Defender's application behavioral DoS analysis capabilities and its ability to interpret behavioral history and stress to automatically generate and enforce a precise, dynamic signature. This capability allows the granular filtering of the good from the bad, which is a major challenge in DoS mitigation. The bad must be accurately identified to mitigate the DoS attack, particularly if the attack changes over time. Enforcement of a very precise signature, with enforcement thresholds based on system, network or application stress signals, dramatically reduces false positives—increasing network and application availability.

- In the BIG-IP Configuration Utility, open the **DoS Protection > Quick Configuration** page and in the
- In the **Protected Objects** section click **Create**.
- Configure a protected object using the following information, and then click **Create.**

Parameter	Value
Name	BaDoSL7Server
IP Address	10.1.20.20
Port	80
Protocol	TCP
Protection Settings: Action	Log and Mitigate
Protection Settings: DDoS Settings	IPv4, TCP, HTTP

- In the **HTTP** row click the **+** icon.
- Click **Behavioral** and in the right pane configure using the following information.

Parameter	Value
Mitigation	Standard Protection
Request Signature Detection	Checked

- Click **Proactive Bot Defense** and in the right pane configure using the following information.

Parameter	Value
Mitigate Action	Disabled

- Click **DOS Tool** and in the right pane configure using the following information, and then click **Create**.

Parameter	Value
Mitigate Action	Report

Putty SSH (use the shortcut) to open **two shells** to the good client system.

- Login as user: ubuntu. The session is preconfigured to authenticate with a key.
- Start the behavioral L7 baselining script in both shells with:

```
# sudo bash
```

```
# cd f5agility
```

```
# ./baseline_L7.sh
```

Select **1) Increasing** in first shell and **2) Alternate** in the second shell.

You will see a few 0000 statuses as there are certain bad requests in the script. But majority of status is 200s.

You can monitor the learning progress on the DHD.

- Putty SSH (use the shortcut) to open a shell to the HybridDefender.
- Login as user: root and password provided.
- View the behavioral L7 baseline learning with following. Notice the learning phase In Progress.

```
# cd f5agility
```

```
# ./show_L7BaDoS_learning.sh
```

- The output is like this:

  ”vs./Common/BaDoSL7Server+/Common/BaDoSL7Server.info.learning:[**62.0614**, 6, 7061, 100]”

- It will be 0.00 for a while (in above example output **62.0614** is the average approximation to the learned baselines)
- For this demo, wait until you have reached at least 80.00-90.00 (**the first number in the output**). This should happen after about 8-10 minutes. Once you see 80.00 and above you can move to next steps.
- The longer it runs, the better it is, because the system is self-adjusting permanently.

Make sure the status is “80.00-90.00” range (the first number in the output) for the learning phase on the DHD before proceeding to the next steps (about 10 minutes). Once you see 80.00 and above you can move on.

- Hit CTRL+C in the DHD Shell and stop this learning status. We will now use this Shell window to see the dynamic signature that is generated.
- Keep this shell window easily viewable. Behavioral L7 mitigation is very dynamic and hence based on the environmental conditions, underlying infrastructure for your lab instance some of you may see the Signature quickly appear and vanish, some may not see it and some will see it longer. Basically, the Signature mitigation is triggered and then by default the offending IP is added to Bad Actor/Shun list and the signature disappears if the system identifies it’s no longer needed for mitigation.

```
# ./show_dos_signature.sh
```

- Access the Attacker System CLI/shell (use putty shortcut on Jumpbox) and launch the attack. Open **TWO** shells**.** In first shell**:**

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab3-3.sh
```

Choose **1) Attack Start – Similarity**

- In Second shell**:**

```
# sudo bash
```

```
# cd f5agility
```

```
# ./lab3-3.sh
```

Choose **2) Attack Start – Score**

As soon as the attack is started you will see that your baseline traffic status of 200s in the good client is now suddenly going to 0000. Wait for a couple of minutes till it returns to a lot more 200s. (Keep the eye on the DHD Shell for Signature)

On the Hybrid Defender Shell you will now see the attack is being mitigated and a signature may appear (see note above).

View Bot Defense logs. **Security>>Event Logs>>Bot Defense>>Requests**

View Bad Actor Log/Blacklist and notice the offending IP is added to the list. **Security>>Event Logs>>Network>>Shun**

Use CTRL+C in all open shell windows (Attacker, Good Client, Hybrid Defender) to STOP all traffic and scripts. Close out all windows

6

Multilayer DDoS Protection

6.1 Introduction

THE PROBLEM

On-premises DDoS defenses can be very effective for blocking most DDoS attacks locally and, being Always-On, can block most attacks immediately. However, they are useless in the case of large volumetric attacks. On the other hand, while Cloud-based DDoS protection (On-Demand) works well for volumetric attacks, it struggles with much slower mitigation response, increased latency, higher operational complexity and the inability to handle HTTPS encrypted attacks due to its asymmetric nature.

THE SOLUTION

Thoroughly and effectively protect your critical web applications from all types of DDoS attacks with a combination of On-Premises and Cloud-Based DDoS services, leveraging multilayer protection techniques that are able to mitigate volumetric attacks, application-level attacks and HTTPS encrypted attacks while minimizing both application downtime and business impact. Intelligent application attacks, encrypted or not, can be handled on-premises with F5's DDoS Hybrid Defender (DHD) which provides next-generation DDoS defense to ensure real-time, Always-ON, protection while large volumetric attacks are handled by F5's Silverline DDoS Protection cloud service which, working On-Demand, detects and mitigates DDoS attacks in real time.

6.1.1 F5 Silverline

F5 Silverline is a cloud-based, fully managed security service for WAF and DDoS protection. F5 Silverline provides Enterprise customers proven security technologies coupled with world-class security professionals. F5's security experts are an extension to the customer's staff and allow them to defeat the largest and most complex attacks.

The primary customer benefits to F5 Silverline include:

- Minimize the risk of data breach and downtime
- Enhance security visibility to their application state
- Reduced operational expense and capital investment required for application security
- Ensure timely detection and fast restoration of services in the event of an attack

6.1.2 F5 DDoS Hybrid Defender

F5® DDoS Hybrid Defender™ (DHD) protects your organization against a wide range of DDoS attacks using a multi-pronged approach. By combining on-premises and cloud technologies, analytics, and advanced methods, DDoS Hybrid Defender is a hybrid solution that detects network and application layer attacks and is easy to deploy and manage.

DDoS Hybrid Defender mitigates against the full spectrum of DDoS attacks including:

- Network capacity attacks
- DNS and SIP protocol volumetric attacks
- HTTP and HTTPS volumetric attacks
- HTTP and HTTPS CPU-based (heavy URL) attacks

You can specify which objects to protect on the network, assigning the appropriate protections to network devices and application servers, and prevent attackers from exhausting network resources and impacting application availability.

Deployments:

The deployment you use for DDoS Hybrid Defender™ depends on the needs of your organization. For maximum DDoS protection, it is recommended that you deploy DDoS Hybrid Defender inline. However, it can also be deployed out of band, or in locations where symmetric data flows are not guaranteed.

Typical locations for the placement of DDoS Hybrid Defender are at the edge of the network or at the edge of the data center

Inline deployment

DDoS Hybrid Defender provides maximum protection when deployed inline in one of two ways:

- Bridged mode with VLAN groups (This is default and we will use in our labs)
- Routed mode

Out of band deployment

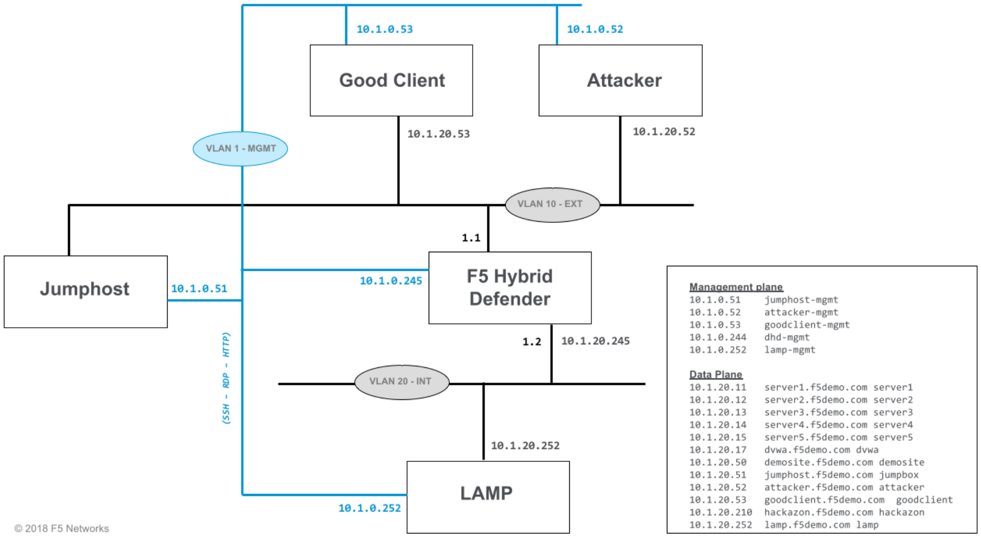
You can deploy DDoS Hybrid Defender out of band in two ways:

- Set up a Layer 2 switch with span ports so that it mirrors traffic onto DHD
- Configure network devices so that they send NetFlow data to DDoS Hybrid Defender

6.2 Hybrid Defender Setup

6.2.1 Getting Started

Lab Diagram



```
Management plane
10.1.0.51    jumphost-mgmt
10.1.0.52    attacker-mgmt
10.1.0.53    goodclient-mgmt
10.1.0.244   dhd-mgmt
10.1.0.252   lamp-mgmt

Data Plane
10.1.20.11   server1.f5demo.com server1
10.1.20.12   server2.f5demo.com server2
10.1.20.13   server3.f5demo.com server3
10.1.20.14   server4.f5demo.com server4
10.1.20.15   server5.f5demo.com server5
10.1.20.17   dvwa.f5demo.com dvwa
10.1.20.50   demosite.f5demo.com demosite
10.1.20.51   jumphost.f5demo.com jumpbox
10.1.20.52   attacker.f5demo.com attacker
10.1.20.53   goodclient.f5demo.com  goodclient
10.1.20.210  hackazon.f5demo.com hackazon
10.1.20.252  lamp.f5demo.com lamp
```

Note: You may have noticed that although clients (goodclient, attacker) and server (LAMP) are siting at the same network subnet [10.1.20.0/24], they're in different VLANs actually (internal - ID 20 vs external - ID 10). Those two VLANs will be grouped toghether (VLAN Group) and act like a single Layer-2 broadcast domain.

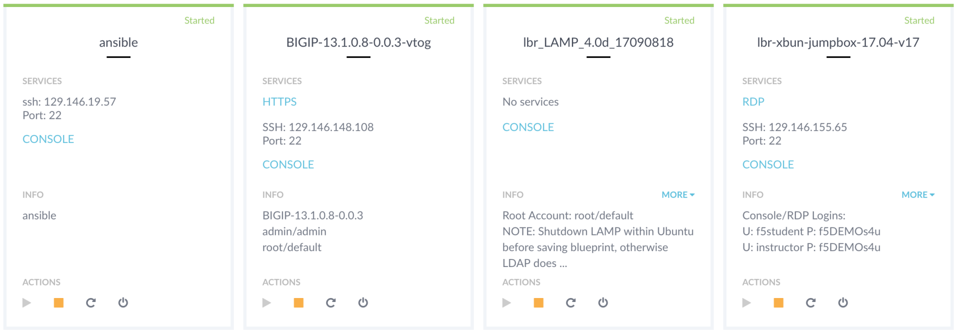
Networking Info

IP addressing, Out of Band management, and credentials for all components:

Component	VLAN/IP Address(es)	Credentials
jumphost	• **Management:** 10.1.0.51 • **internal:** 10.1.20.51	`f5student/[will be provided]`
attacker	• **Management:** 10.1.0.52 • **internal:** 10.1.20.52	`f5student/[will be provided]`
goodclient	• **Management:** 10.1.0.53 • **internal:** 10.1.20.53	`f5student/[will be provided]`
lamp	• **Management:** 10.1.0.252 • **internal:** 10.1.20.252	`f5/[will be provided]`
F5-DHD	• **Management:** 10.1.0.244 • **internal:** 10.1.20.244	`root/[will be provided]`

Accessing the lab environment

1. Open a browser and go to http://training.f5agility.com, then enter your Class# and Student# as provided by your instructor.



Started
ansible
SERVICES
ssh: 129.146.19.57
Port: 22
CONSOLE
INFO
ansible
ACTIONS

Started
BIGIP-13.1.0.8-0.0.3-vtog
SERVICES
HTTPS
SSH: 129.146.148.108
Port: 22
CONSOLE
INFO
BIGIP-13.1.0.8-0.0.3
admin/admin
root/default
ACTIONS

Started
lbr_LAMP_4.0d_17090818
SERVICES
No services
CONSOLE
INFO MORE ▾
Root Account: root/default
NOTE: Shutdown LAMP within Ubuntu before saving blueprint, otherwise LDAP does ...
ACTIONS

Started
lbr-xbun-jumpbox-17.04-v17
SERVICES
RDP
SSH: 129.146.155.65
Port: 22
CONSOLE
INFO MORE ▾
Console/RDP Logins:
U: f5student P: f5DEMOs4u
U: instructor P: f5DEMOs4u
ACTIONS

2. Look for the **jumphost** virtual machine. Use the RDP client of your choice and work from there, you are going to use it for all labs.

Hint: You can use either use the PUTTY client provisioned on your jumphost desktop, or native shell prompt in order to access both **goodclient** and **attacker** virtual machines. Private keys have been configured in advance so you won't need passwords. A few scripts require root access. Don't forget to **sudo** before running attacks, baselines, etc.

---

1. Run the following scripts from both **goodclient** and **attacker** hosts. It's going to sync the tools to be used in the entire lab.

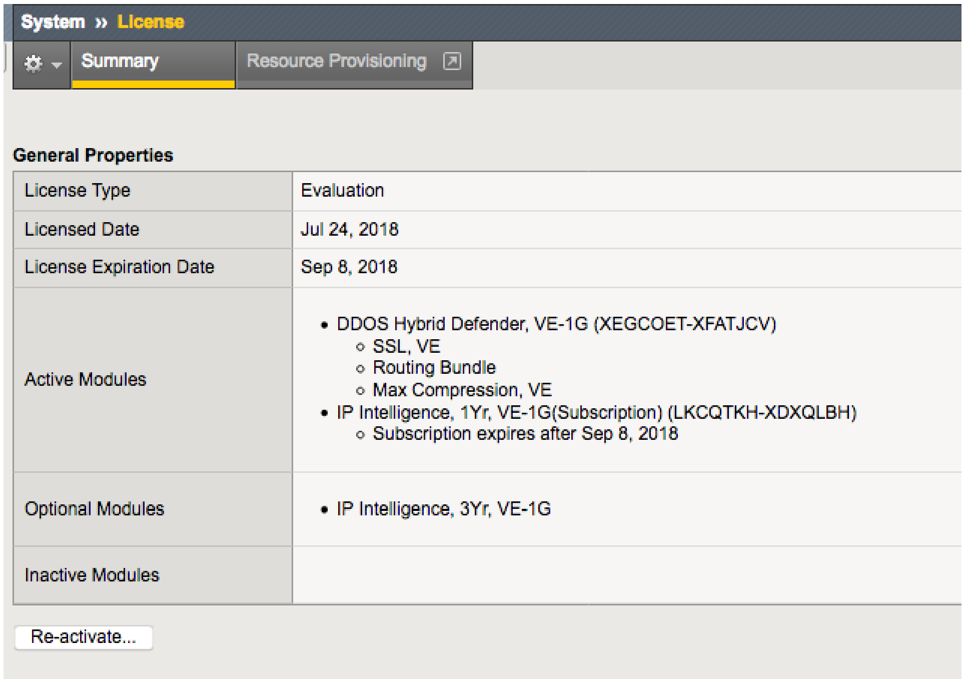
```
~/update_tools.sh
```

6.2.2 Re-License your DHD Device

Important: For Silverline device registration to function properly the Hybrid Defender device must have a unique device ID, which is comprised of unique attributes like Base MAC and registration key.

For the following steps please use the registration key provided by your instructor.

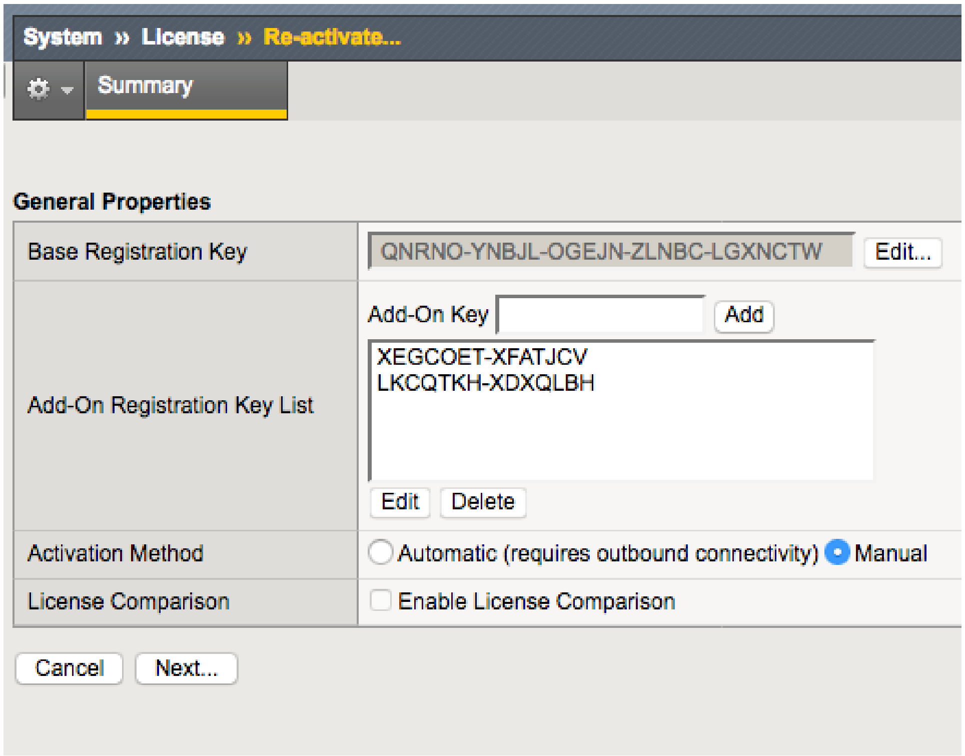
1. Go to System->License and then click on **Re-activate**.



General Properties

License Type	Evaluation
Licensed Date	Jul 24, 2018
License Expiration Date	Sep 8, 2018
Active Modules	• DDOS Hybrid Defender, VE-1G (XEGCOET-XFATJCV) ◦ SSL, VE ◦ Routing Bundle ◦ Max Compression, VE • IP Intelligence, 1Yr, VE-1G(Subscription) (LKCQTKH-XDXQLBH) ◦ Subscription expires after Sep 8, 2018
Optional Modules	• IP Intelligence, 3Yr, VE-1G
Inactive Modules	

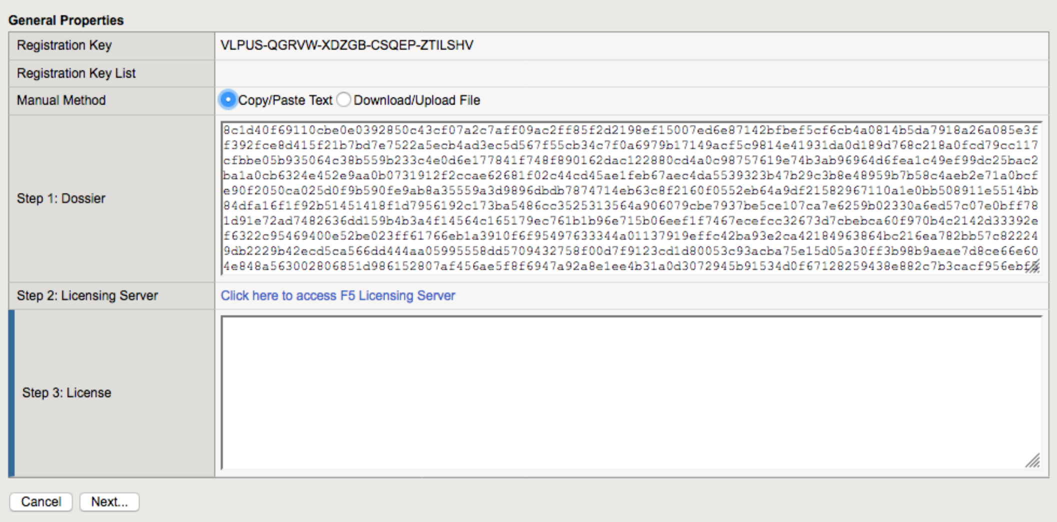
2. Edit the **Base Registration Key**, replacing it by the new license key. The **Activation Method** option must be manual. Then click **Next**.



General Properties

Base Registration Key	QNRNO-YNBJL-OGEJN-ZLNBC-LGXNCTW Edit...
Add-On Registration Key List	Add-On Key Add XEGCOET-XFATJCV LKCQTKH-XDXQLBH Edit Delete
Activation Method	○ Automatic (requires outbound connectivity) ● Manual
License Comparison	□ Enable License Comparison

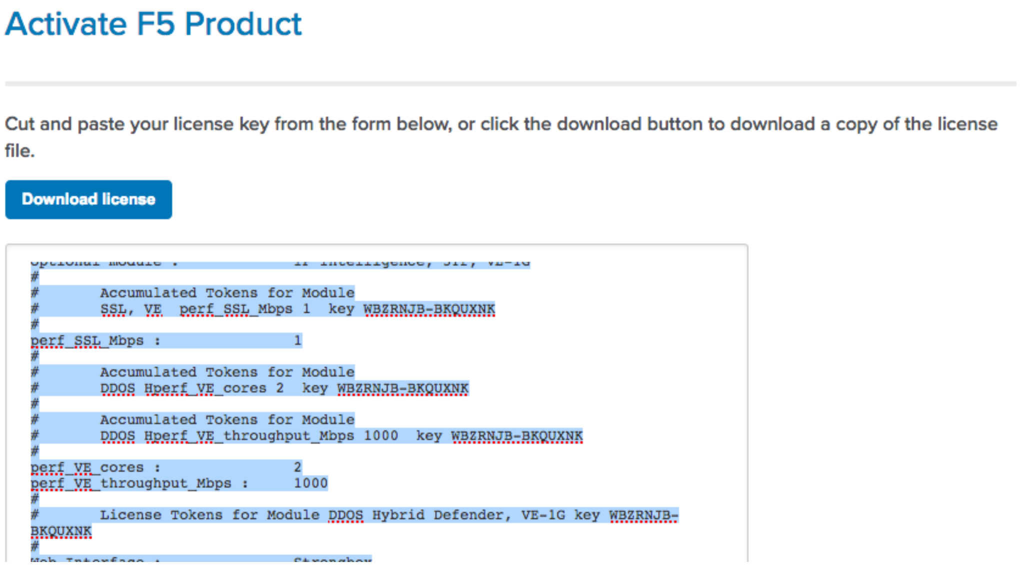
3. Select all in the **Dossier** frame and copy it. Click on **Click here to access F5 Licensing Server**.



General Properties

Registration Key	VLPUS-QGRVW-XDZGB-CSQEP-ZTILSHV
Registration Key List	
Manual Method	● Copy/Paste Text ○ Download/Upload File
Step 1: Dossier	8c1d40f69110cbe0e0392850c43cf07a2c7aff09ac2ff85f2d2198ef15007ed6e87142bfbef5cf6cb4a0814b5da7918a26a085e3f f392fce8d415f21b7bd7e7522a5ecb4ad3ec5d567f55cb34c7f0a6979b17149acf5c9814e41931da0d189d768c218a0fcd79cc117 cfbbe05b935064c38b559b233c4e0d6e177841f748f890162dac122880cd4a0c98757619e74b3ab96964d6fea1c49ef99dc25bac2 ba1a0cb6324e452e9aa0b0731912f2ccae62681f02c44cd45ae1feb67aec4da5539323b47b29c3b8e48959b7b58c4aeb2e71a0bcf e90f2050ca025d0f9b590fe9ab8a35559a3d9896dbdb7874714eb63c8f2160f0552eb64a9df21582967110a1e0bb508911e5514bb 84dfa16f1f92b51451418f1d7956192c173ba5486cc3525313564a906079cbe7937be5ce107ca7e6259b02330a6ed57c07e0bff78 1d91e72ad7482636dd159b4b3a4f14564c165179ec761b1b96e715b06eef1f7467ecefcc32673d7cbebca60f970b4c2142d33392e f6322c95469400e52be023ff61766eb1a3910f6f95497633344a01137919effc42ba93e2ca42184963864bc216ea782bb57c82224 9db2229b42ecd5ca566dd444aa05995558dd5709432758f00d7f9123cd1d80053c93acba75e15d05a30ff3b98b9aeae7d8ce66e60 4e848a563002806851d986152807af456ae5f8f6947a92a8e1ee4b31a0d3072945b91534d0f67128259438e882c7b3cacf956ebf
Step 2: Licensing Server	Click here to access F5 Licensing Server
Step 3: License	

4. Agreee with the contract terms, copy the contents in the license frame, then click **Next** ”.

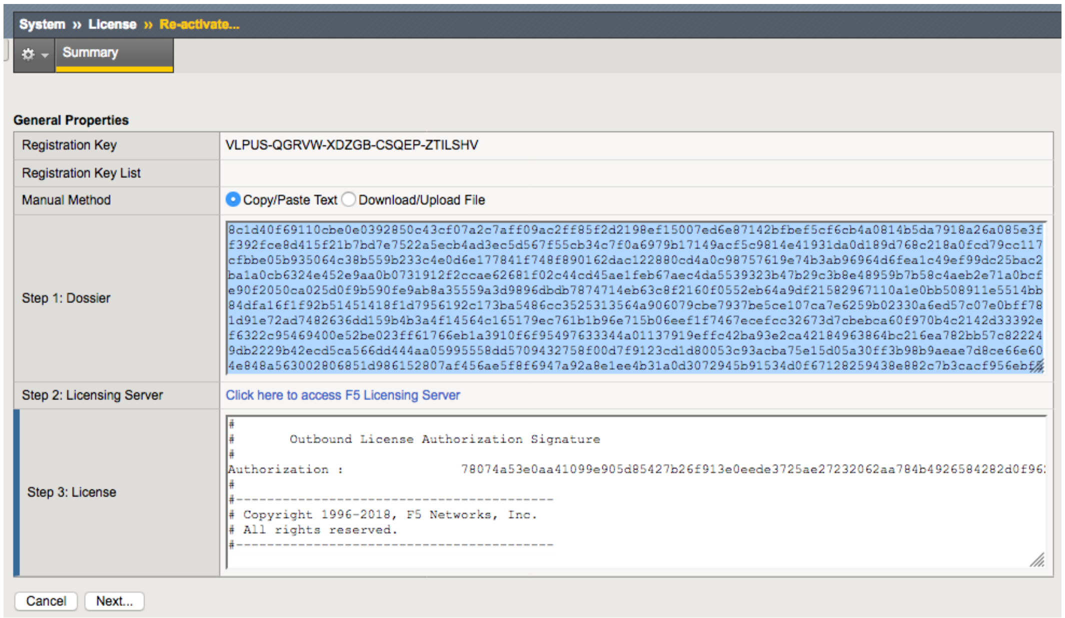


Activate F5 Product

Cut and paste your license key from the form below, or click the download button to download a copy of the license file.

```
Optional Module :                   IP Intelligence, SIT, VE-1G
#
#         Accumulated Tokens for Module
#         SSL, VE  perf_SSL_Mbps 1  key WBZRNJB-BKQUXNK
#
perf_SSL_Mbps :                     1
#
#         Accumulated Tokens for Module
#         DDOS Hperf_VE_cores 2  key WBZRNJB-BKQUXNK
#
#         Accumulated Tokens for Module
#         DDOS Hperf_VE_throughput_Mbps 1000  key WBZRNJB-BKQUXNK
#
perf_VE_cores :                     2
perf_VE_throughput_Mbps :           1000
#
#         License Tokens for Module DDOS Hybrid Defender, VE-1G key WBZRNJB-
BKQUXNK
#
Web Interface :                     Strongbox
```

5. Go back to your F5 DHD and paste the contents copied from the above. **License** and click **Next**.



General Properties

Registration Key	VLPUS-QGRVW-XDZGB-CSQEP-ZTILSHV
Registration Key List	
Manual Method	● Copy/Paste Text ○ Download/Upload File
Step 1: Dossier	8c1d40f69110cbe0e0392850c43cf07a2c7aff09ac2ff85f2d2198ef15007ed6e87142bfbef5cf6cb4a0814b5da7918a26a085e3f f392fce8d415f21b7bd7e7522a5ecb4ad3ec5d567f55cb34c7f0a6979b17149acf5c9814e41931da0d189d768c218a0fcd79cc117 cfbbe05b935064c38b559b233c4e0d6e177841f748f890162dac122880cd4a0c98757619e74b3ab96964d6fea1c49ef99dc25bac2 ba1a0cb6324e452e9aa0b0731912f2ccae62681f02c44cd45ae1feb67aec4da5539323b47b29c3b8e48959b7b58c4aeb2e71a0bcf e90f2050ca025d0f9b590fe9ab8a35559a3d9896dbdb7874714eb63c8f2160f0552eb64a9df21582967110a1e0bb508911e5514bb 84dfa16f1f92b51451418f1d7956192c173ba5486cc3525313564a906079cbe7937be5ce107ca7e6259b02330a6ed57c07e0bff78 1d91e72ad7482636dd159b4b3a4f14564c165179ec761b1b96e715b06eef1f7467ecefcc32673d7cbebca60f970b4c2142d33392e f6322c95469400e52be023ff61766eb1a3910f6f95497633344a01137919effc42ba93e2ca42184963864bc216ea782bb57c82224 9db2229b42ecd5ca566dd444aa05995558dd5709432758f00d7f9123cd1d80053c93acba75e15d05a30ff3b98b9aeae7d8ce66e60 4e848a563002806851d986152807af456ae5f8f6947a92a8e1ee4b31a0d3072945b91534d0f67128259438e882c7b3cacf956ebf
Step 2: Licensing Server	Click here to access F5 Licensing Server
Step 3: License	# # Outbound License Authorization Signature # Authorization : 78074a53e0aa41099e905d85427b26f913e0eede3725ae27232062aa784b4926584282d0f96 # #--- # Copyright 1996-2018, F5 Networks, Inc. # All rights reserved. #---

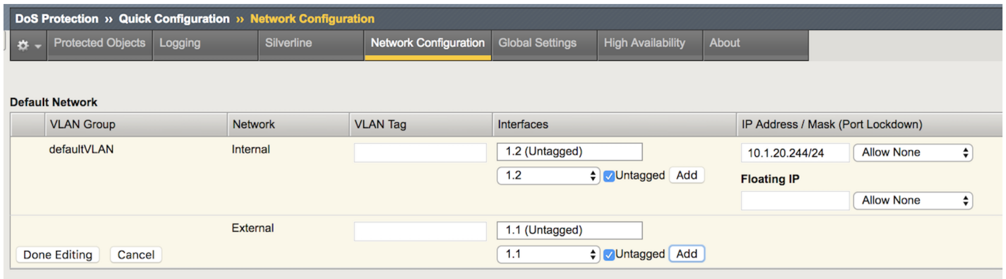
Hint: The BIG-IP will restart daemons and a window will pop up indicating system configuration has changed. Please wait for it to reconnect and click **Continue**. Your device is now licensed. Click **Next**

6.2.3 Perform Initial DHD Network Configuration

1. In the **BIG-IP Configuration Utility**, open the DoS Protection-> Quick Configuration page.
2. Open the Network Configuration page, then In the **Default Network** section click **default-VLAN**.

3. Configure the Default Network settings as follows, the click on **Done Editing**

Internal VLAN tag:	blank
Internal Interfaces:	1.2 (Click untagged/Add)
External VLAN tag:	blank
External Interfaces:	1.1 (Click untagged/Add)
IP Address/Mask:	10.1.20.244/24



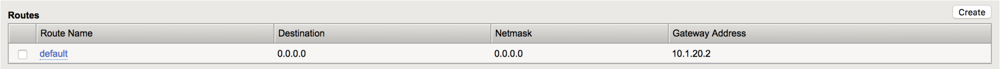
Default Network

VLAN Group	Network	VLAN Tag	Interfaces	IP Address / Mask (Port Lockdown)
defaultVLAN	Internal		1.2 (Untagged) 1.2 ☑Untagged Add	10.1.20.244/24 Allow None Floating IP Allow None
	External		1.1 (Untagged) 1.1 ☑Untagged Add	

1. In the Routes section click **Create**.

2. Configure the route using following information, and then click **Done Editing**, and then click **Update**.

Route name:	default
Destination:	0.0.0.0
Netmask:	0.0.0.0
Gateway Address:	10.1.20.2



Routes

	Route Name	Destination	Netmask	Gateway Address
□	default	0.0.0.0	0.0.0.0	10.1.20.2

1. By this time you should be able to reach the **LAMP** server from both **attacker** and **gooclient** machines. Open up a terminal shell with both machines and confirm the can reach out to the **LAMP** server before moving forward.

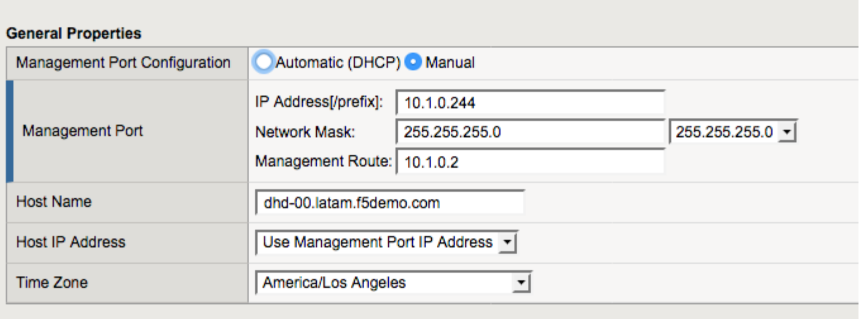
```
f5student@attacker:~$  ping -c 3 server1
PING server1.f5demo.com (10.1.20.11) 56(84) bytes of data.
64 bytes from server1.f5demo.com (10.1.20.11): icmp_seq=1 ttl=64␣
↪time=9.73 ms
64 bytes from server1.f5demo.com (10.1.20.11): icmp_seq=2 ttl=64␣
↪time=6.21 ms
64 bytes from server1.f5demo.com (10.1.20.11): icmp_seq=3 ttl=64␣
↪time=5.88 ms

--- server1.f5demo.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.880/7.277/9.736/1.744 ms
f5student@attacker:~$
```

6.2.4 Register DHD Device with Silverline

For Silverline signaling we will be leveraging both the DHD built-in signaling, as well as bandwidth utilization reporting for Hybrid DDoS protection.

1. Go to System-> Platform menu and change the hostname as below. This will make easier to identify alerts from your particular device in the Silverline Portal. When finished, click **Update**.

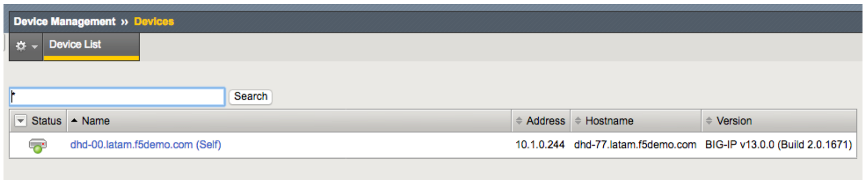
   ```
   dhd-[student#].latam.f5demo.com
   ```

   General Properties

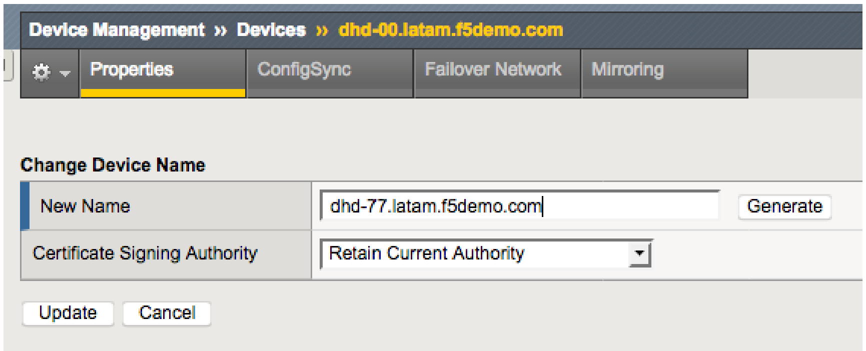
Management Port Configuration	○ Automatic (DHCP) ● Manual
Management Port	IP Address[/prefix]: 10.1.0.244 Network Mask: 255.255.255.0 255.255.255.0 Management Route: 10.1.0.2
Host Name	dhd-00.latam.f5demo.com
Host IP Address	Use Management Port IP Address
Time Zone	America/Los Angeles

2. In Device Management->Devices select the device and then click **Change Device Name**.

Status	Name	Address	Hostname	Version
	dhd-00.latam.f5demo.com (Self)	10.1.0.244	dhd-77.latam.f5demo.com	BIG-IP v13.0.0 (Build 2.0.1671)

3. Update the device name to match the hostname you have chosen. **Important**: Use your student number.

   Change Device Name

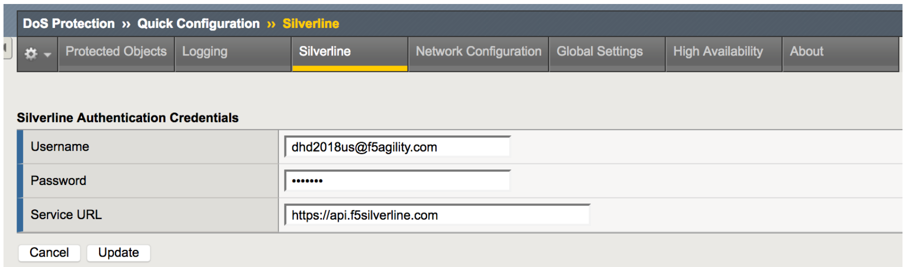
New Name	dhd-77.latam.f5demo.com
Certificate Signing Authority	Retain Current Authority

4. Open a terminal sesson with the Hybrid Defender and restart services:

   ```
   bigstart restart
   ```

5. Now proceed with the Silverline registration. Go to DoS Protection-> Quick Configuration-> Silverline. Fill out the **Authentication Credentials** fields as follows, then click **Update**.

username	dhd2018us@f5agility.com
password	**[will be provided]**
Service URL	https://api.f5silverline.com



DoS Protection » Quick Configuration » Silverline

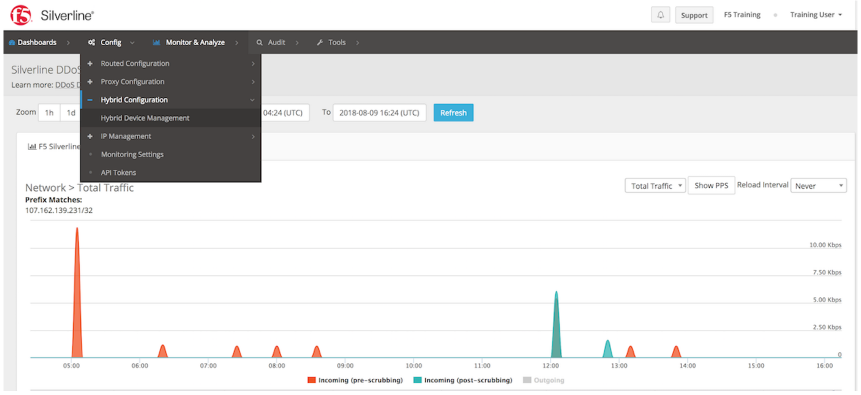
Silverline Authentication Credentials

Username	dhd2018us@f5agility.com
Password	•••••••
Service URL	https://api.f5silverline.com

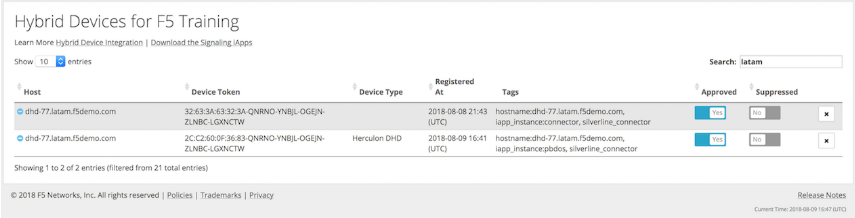
Cancel | Update

Hint: That screen provides no feedback when the authentication actually works, so no worries. Go to the next step unless you got an error message here.

- From another tab in your browser, access the Silverline Portal https://portal.f5silverline.com using same DHD admin account.
- Navigate to Config-> Hybrid Config-> Hybrid Device Management



- Enter the hostname of your DHD device in the Search field. Verify that you have both registrations. Approve them and you're done!



Hybrid Devices for F5 Training

Learn More Hybrid Device Integration | Download the Signaling iApps

Show 10 entries

Search: latam

Host	Device Token	Device Type	Registered At	Tags	Approved	Suppressed	
dhd-77.latam.f5demo.com	32:63:3A:63:32:3A-QNRNO-YNBJL-OGEJN-ZLNBC-LGXNCTW		2018-08-08 21:43 (UTC)	hostname:dhd-77.latam.f5demo.com, iapp_instance:connector, silverline_connector	Yes	No	×
dhd-77.latam.f5demo.com	2C:C2:60:0F:36:83-QNRNO-YNBJL-OGEJN-ZLNBC-LGXNCTW	Herculon DHD	2018-08-09 16:41 (UTC)	hostname:dhd-77.latam.f5demo.com, iapp_instance:pbdos, silverline_connector	Yes	No	×

Showing 1 to 2 of 2 entries (filtered from 21 total entries)

© 2018 F5 Networks, Inc. All rights reserved | Policies | Trademarks | Privacy

Release Notes

Current Time: 2018-08-09 16:47 (UTC)

6.3 Module - Network Level DoS Protection

In this module you will learn how the F5 Hybrid Defender protects from several network level DDoS vectors.

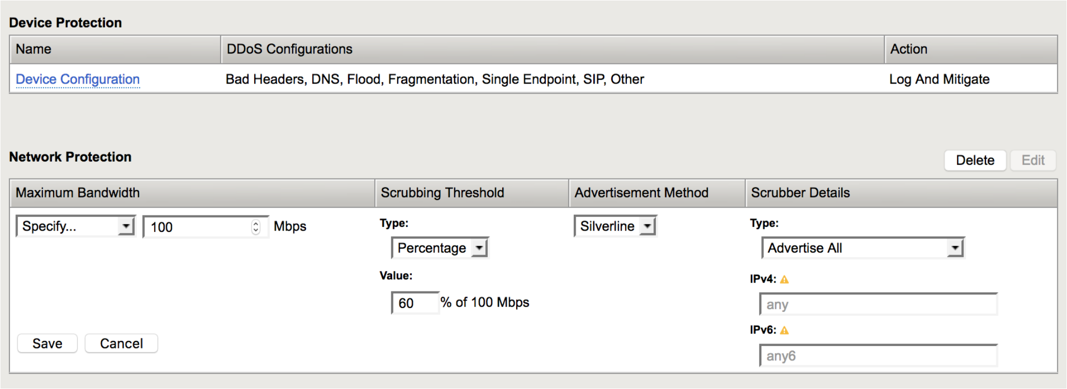
6.3.1 Lab – Launching Network-Level Flood Attacks

The idea in this lab is to observe how poorly the application performs when the network is under attack.

Configure DHD Device Bandwidth Thresholds

1. In the **Configuration Utility**, open the **Protected Objects** page.
2. In the **Network Protection** section click **Create**.
3. Configure as follows then click **Save**.

Maximum Bandwidth: Specify	100
Scrubbing Threshold: Type	Percentage
Scrubbing Threshold: Value	60
Advertisement Method	Silveline
Scrubber Details: Type	Advertise All



Device Protection

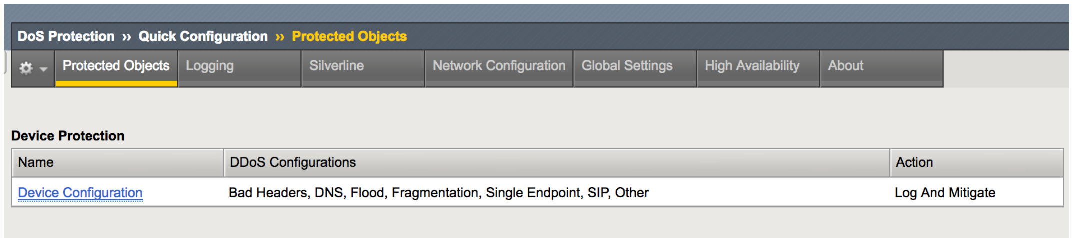
Name	DDoS Configurations	Action
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other	Log And Mitigate

Network Protection

Maximum Bandwidth	Scrubbing Threshold	Advertisement Method	Scrubber Details
Specify... 100 Mbps	Type: Percentage Value: 60 % of 100 Mbps	Silverline	Type: Advertise All IPv4: any IPv6: any6

Turning Device-Level Protection off

1. In the **Configuration Utility**, in the **Device Protection** section click **Device Configuration**.

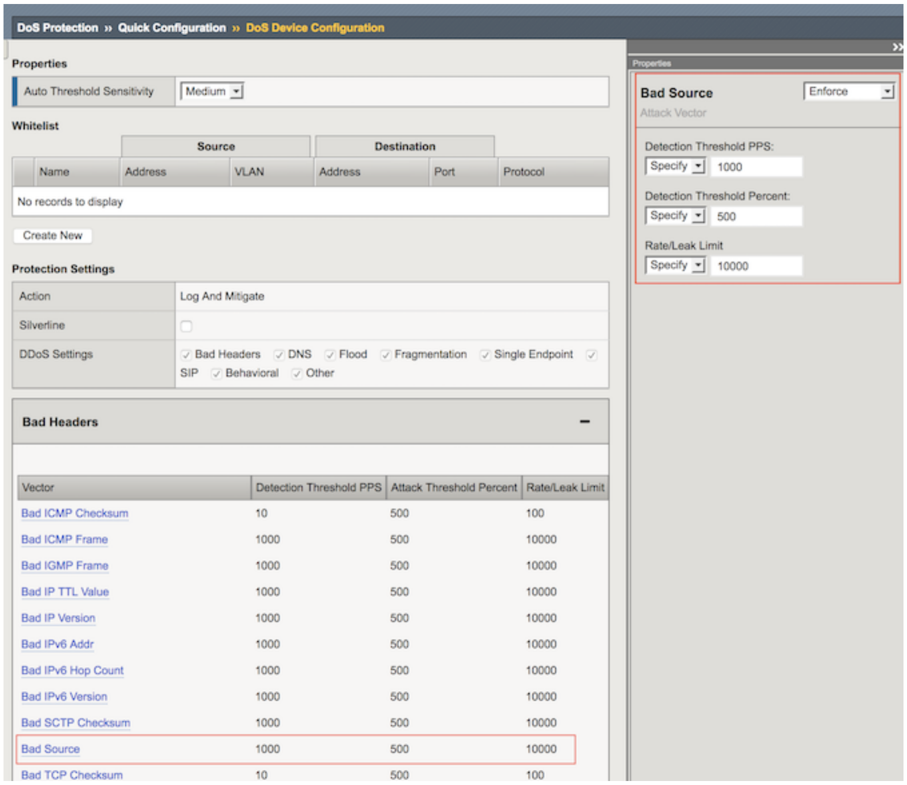


Device Protection

Name	DDoS Configurations	Action
Device Configuration	Bad Headers, DNS, Flood, Fragmentation, Single Endpoint, SIP, Other	Log And Mitigate

2. In the **Bad Headers** row click the **+** icon, and then click **Bad Source**.
3. On the right-side of the page configure using the following information.

Detection Threshold PPS	Infinite
Detection Threshold Percent	Infinite
Rate/Leak Limit	Infinite



DoS Protection » Quick Configuration » DoS Device Configuration

Properties

Auto Threshold Sensitivity	Medium

Whitelist

	Source		Destination		
Name	Address	VLAN	Address	Port	Protocol
No records to display					

Create New

Protection Settings

Action	Log And Mitigate
Silverline	□
DDoS Settings	✓ Bad Headers ✓ DNS ✓ Flood ✓ Fragmentation ✓ Single Endpoint ✓ SIP ✓ Behavioral ✓ Other

Bad Headers

Vector	Detection Threshold PPS	Attack Threshold Percent	Rate/Leak Limit
Bad ICMP Checksum	10	500	100
Bad ICMP Frame	1000	500	10000
Bad IGMP Frame	1000	500	10000
Bad IP TTL Value	1000	500	10000
Bad IP Version	1000	500	10000
Bad IPv6 Addr	1000	500	10000
Bad IPv6 Hop Count	1000	500	10000
Bad IPv6 Version	1000	500	10000
Bad SCTP Checksum	1000	500	10000
Bad Source	1000	500	10000
Bad TCP Checksum	10	500	100

Properties

Bad Source Enforce

Attack Vector

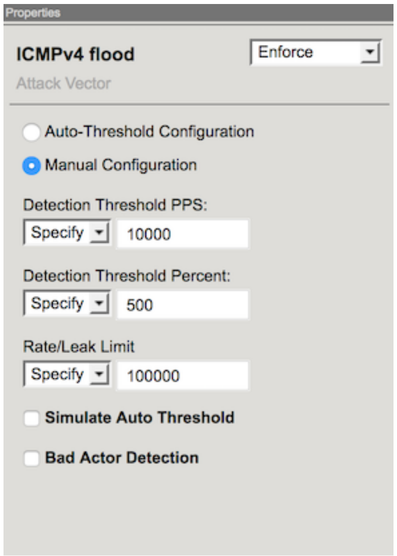
Detection Threshold PPS: Specify 1000

Detection Threshold Percent: Specify 500

Rate/Leak Limit Specify 10000

4. Now In the **Flood** row, click the **+** icon, and then click **ICMPv4 flood**.
5. On the right-side of the page configure using the following information.

Detection Threshold PPS	Infinite
Detection Threshold Percent	Infinite
Rate/Leak Limit	Infinite



Properties

ICMPv4 flood Enforce

Attack Vector

○ Auto-Threshold Configuration

● Manual Configuration

Detection Threshold PPS: Specify 10000

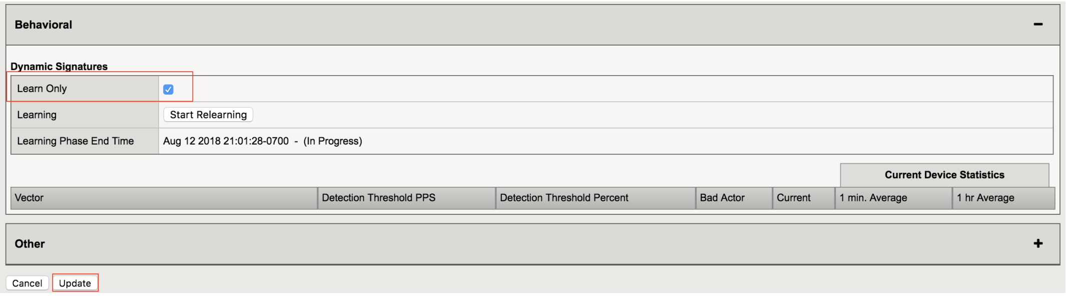
Detection Threshold Percent: Specify 500

Rate/Leak Limit Specify 100000

□ **Simulate Auto Threshold**

□ **Bad Actor Detection**

6. Apply the settings above for TCP SYN flood and UDP Flood.
7. In the **Behavioral** row click on **Learn Only**, then click **Update**.



Behavioral –

Dynamic Signatures

Learn Only	☑
Learning	Start Relearning
Learning Phase End Time	Aug 12 2018 21:01:28-0700 - (In Progress)

				Current Device Statistics		
Vector	Detection Threshold PPS	Detection Threshold Percent	Bad Actor	Current	1 min. Average	1 hr Average

Other +

Cancel Update

8. On the **goodclient**, start the network baselining (Let it running for the entire lab)

   ```
   sudo ~/tools_agility_183/baseline_l4.sh
   ```

Important: In order to assure best performance and good lab results, always use the management network ip addresses/hostnames for remote access (goodclient-mgmt, attacker-mgmt and lamp-mgmt)

```
f5student@goodclient:~$ cd ~/tools_agility_183/
f5student@goodclient:~/tools_agility_183$ ./baseline_l4.sh
/   status: 200     bytes: 3952     time: 0.016
/   status: 200     bytes: 3952     time: 0.019
/   status: 200     bytes: 3952     time: 0.014
/   status: 200     bytes: 3952     time: 0.014
/   status: 200     bytes: 3952     time: 0.018
/   status: 200     bytes: 3952     time: 0.221
/httprequest.php    status: 200     bytes: 699      time: 0.014
/httprequest.php    status: 200     bytes: 699      time: 0.014
```

Launch an ICMP flood Attack on the LAMP Server

Hint: The pentest tool can be used to send several types of DoS Attacks for the most part of the lab, few free to try it out. For some specific exercises there will be custom shell scrtips though.

```
sudo ~/tools_agility_183/pentest
```

```
________ _______  _       _________ _______  ________  _
|  ____  ||  ____ \| \    /|\__   __/|       ||  ____ \| \    /||\  ␣
↪  /|
| |    | || |    \/|  \  | |   | |   | || || || |    \/|  \  | || | ␣
↪ | |
| |____| || |__    |   \ | |   | |   | || || || |__    |   \ | || | ␣
↪ | |
|  ______||  __)   | |\ \| |   | |   | ||_|| ||  __)   | |\ \| || | ␣
↪ | |
| |       | |      | | \   |   | |   | |   | || |      | | \   || | ␣
↪ | |
| |       | |____/\| |  \  |   | |   | |   | || |____/\| |  \  || |__
↪_| |
|/        (_______/|/    \_|   |_|   |/     \||_______/|/    \_||____
↪___|
```

```
Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://
 ↪github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/
 ↪GinjaChris/pentmenu/master/README.md before proceeding

1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>
```

1. Hit option **2** (DOS), then **1** (ICMP Echo Flood)
2. Use Attack options as follows:

Enter target IP/hostname:	server1
Enter Source IP:	r (random)

3. Now open two more terminal sessions with **attacker** and **lamp** servers respectively. On each screen open the **bmon** util for instant traffic stats.

```
eth1
Interfaces                   | RX bps       pps     %| TX bps    ␣
 ↪  pps     %
lo                           |      0         0      |      0    ␣
 ↪    0
eth0                         |     66B        1      |    545B   ␣
 ↪    1
    qdisc none (pfifo_fast)  |      0         0      |    525B   ␣
 ↪    1
->eth1                       |     77B        1      |   1.59MiB ␣
 ↪39.63K
    qdisc none (pfifo_fast)  |      0         0      |   1.59MiB ␣
 ↪39.63K
---------------------?---------------?----------------------------------------
                            (RX Packtes/second)
    5.00 ....|..|.........|......|.........................|......
 ↪...
    4.17 ...|||||||...|...|.||.|||...........|||.......|..||.|.|..
 ↪.||
    3.33 ...||||||||..|..||||||||||..||.....|||||.....|||||||||||.
 ↪|||
    2.50 ...||||||||..|..||||||||||..||.....|||||.....|||||||||||.
 ↪|||
    1.67 .|||||||||||||.|||||||||||||||....|||||||...
 ↪||||||||||||||||
    0.83 ||||||||||||||||||||||||||||||||.|||||||||..
 ↪||||||||||||||||
        1   5    10   15   20   25   30   35   40   45   50   55  ␣
 ↪60
    K                     (TX Packtes/second)
    52.32 ..............||||....|.||..............................
 ↪....
```

```
    43.60 ||.|||||||||||||||||||||||||||||||||..||||||||.
↪|||||||||||||
    34.88␣
↪||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
    26.16␣
↪||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
    17.44␣
↪||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
        8.72␣
↪||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
            1   5   10   15   20   25   30   35   40   45   50  ␣
↪55   60
```

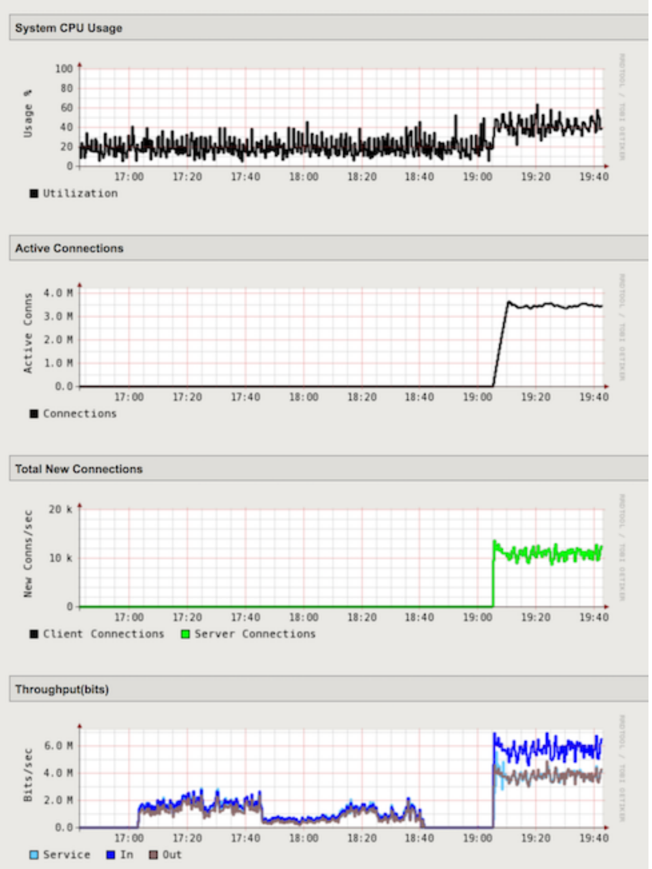
Hint: Use either the RIGHT and LEFT arrow keys to move between Bps and pps metrics. Don't forget selecting the right inteface using the UP/DOWN arrow keys. **Attacker** uses eth1 and **Lamp** uses eth4 for data traffic.

4. Open a terminal session with the **DHD** and use the tcpdump util to verify that ICMP attack traffic is passing through the device.

   ```
   [root@dhd:Active:Standalone] config # tcpdump -i defaultVLAN
   ```

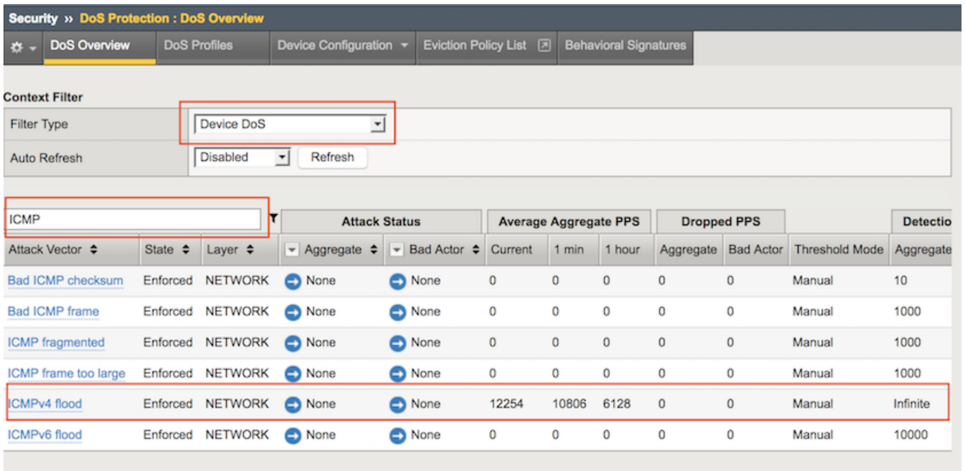
5. Observe the baseline running on goodclient. Since the flood attack is hitting the server hard, the legitimate client sessions are being degraded. Look at the statude code **000** for most requests.

6. In the **Configuration Utility**, open the Statistics-> Performance-> Performance page. As you can see, there is a drastic spike in the traffic.



7. Open the Security-> DoS Protection-> DoS Overview page.

8. In the Filter Type field select **Device DoS**. Then on the left corner search for ICMP.



Context Filter

Filter Type	Device DoS
Auto Refresh	Disabled Refresh

ICMP

			Attack Status		Average Aggregate PPS			Dropped PPS			Detectio
Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate
Bad ICMP checksum	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	10
Bad ICMP frame	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	1000
ICMP fragmented	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	1000
ICMP frame too large	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	1000
ICMPv4 flood	Enforced	NETWORK	None	None	12254	10806	6128	0	0	Manual	Infinite
ICMPv6 flood	Enforced	NETWORK	None	None	0	0	0	0	0	Manual	10000

9. Review the statistics for Current, 1 min. Average, and 1 hr Average.

10. **Open the Security-> Event Logs-> DoS-> Network-> Events page.** The log file is empty as we disabled device-level flood protection on **BIG-IP DHD**.

11. From the attacker terminal session type **Ctrl + C** to stop the ICMP flood.

6.3.2 Lab - Configure Hybrid Defender Flood Protections

This lab teachs you on how to configure DoS protection for common network-level DoS vectors.

Configure Protected Object-Level IPv4 Flood DHD DoS Protection

Configure object-level IPv4 ICMP flood protection, and then issue an ICMP DoS flood and review the results.

1. On the **Protect Objects** page, in the Protected Objects section click **Create**.
2. Configure a protected object using the following information, and then click **Create**:

Name:	ServerNet
IP Address:	10.1.20.0/24
Port:	any
Protocol	All Protocols
Protec. Settings Action:	Advertise All
Protec. Settings DDoS:	IPv4

3. In the IPv4 row click the **+** icon, and then click **ICMPv4 flood**
4. On the right-side of the page configure using the following information, and then click Create.

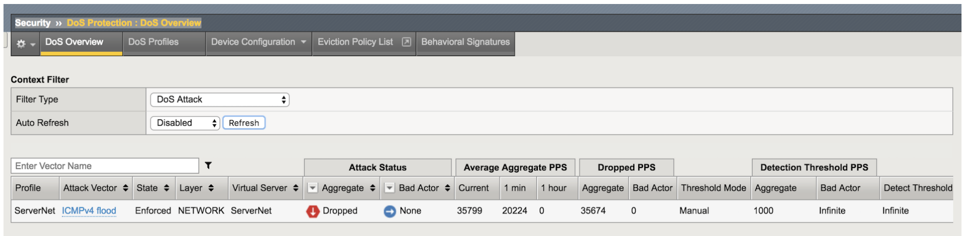
Detection Threshold PPS:	Specify: 1000
Detection Threshold Percent:	Infinite
Rate/Leak Limit:	Specify: 1000

Important: From now on, make sure you have an always-on terminal session with both the **attacker** and **LAMP** servers. Let them running the **bmon** utility, or a **tcpdump**. Those will provide instant and detailed visibility of the ammount of packets comming in/out of both virtual machines.

5. From the **attacker** terminal session launch an ICMPv4 DoS attack using the Pentmenu tool (Options 2, 1) as follows:

target IP/hostname:	server1
source IP:	r[random]

6. Check out the **LAMP** terminal session and observe how many ICMP packets are hitting this server.
7. Before moving on, wait the attack to run for about 30 seconds or so
8. In the **Configuration Utility** go to Security-> DoS Protection-> DoS Overview. You should be able to see the DHD stopping the Attack.



Context Filter

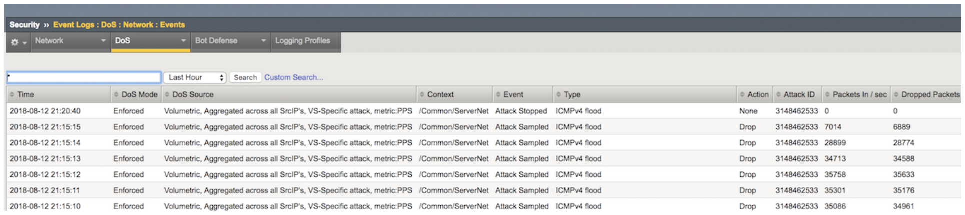
Filter Type	DoS Attack
Auto Refresh	Disabled Refresh

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS		
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold
ServerNet	ICMPv4 flood	Enforced	NETWORK	ServerNet	Dropped	None	35799	20224	0	35674	0	Manual	1000	Infinite	Infinite

9. Now stop the Attack with **Ctrl + C**.
10. Open the Security-> Event Logs-> DoS-> Network-> Events page.

    The DoS Source is Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS.

    - The virtual server column displays /Common/ServerNet, identifying this is a protected object.
    - The type is ICMPv4 flood.
    - The action is Drop.
11. Now check out the Security-> Event Logs-> DoS-> Network-> Events Page.



Time	DoS Mode	DoS Source	Context	Event	Type	Action	Attack ID	Packets In / sec	Dropped Packets
2018-08-12 21:20:40	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Stopped	ICMPv4 flood	None	3148462533	0	0
2018-08-12 21:15:15	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	ICMPv4 flood	Drop	3148462533	7014	6889
2018-08-12 21:15:14	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	ICMPv4 flood	Drop	3148462533	28899	28774
2018-08-12 21:15:13	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	ICMPv4 flood	Drop	3148462533	34713	34588
2018-08-12 21:15:12	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	ICMPv4 flood	Drop	3148462533	35758	35633
2018-08-12 21:15:11	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	ICMPv4 flood	Drop	3148462533	35301	35176
2018-08-12 21:15:10	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	ICMPv4 flood	Drop	3148462533	35086	34961

12. The DHD was able to detect the moment the attack started and stopped, along with all volumetric info.

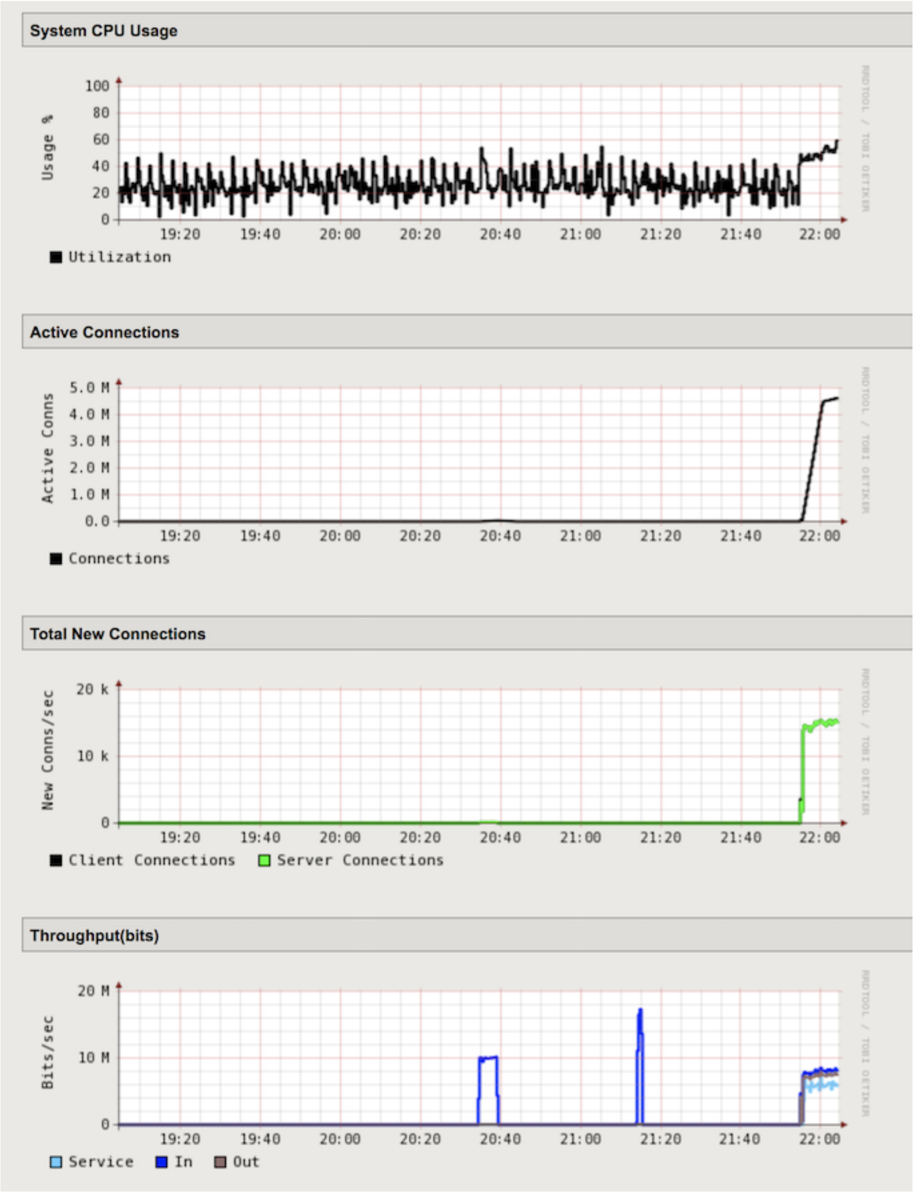
Configure Protected Object-Level UDP Flood Attack Protection

Configure object-level DoS UDP flood protection, and then issue an UPD flood and review the results.

1. From the attacker terminal session launch an UDP flood attack using the Pentmenu tool (Options 2, 7) as follows:

target IP/hostname:	server2
target port (defaults to 80):	default [ENTER]
random string (data to send):	F5Agility2018
source IP:	r[random]

2. Let the attack run for about 30 seconds before moving on.
3. In the **Configuration Utility**, open the Statistics-> Performance-> Performance page. There is a spike in connections and throughput. The BIG-IP system is being hit with the UDP flood attack.



4. Open the DoS Protection-> Quick Configuration page and in the **Protected Objects** section click **ServerNet**.

5. In the **DDoS Settings** row click the **UDP** checkbox. In the UDP row click the **+** icon, and then click **UDP Flood**.

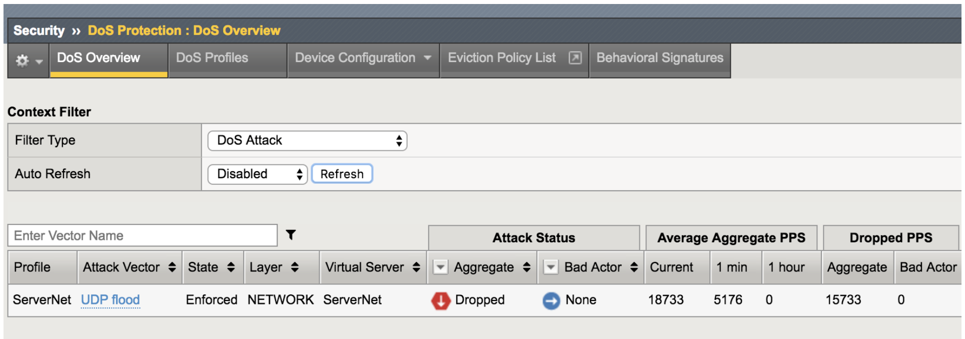
6. On the right-side of the page configure using the following information, and then click **Update**.

Detection Threshold PPS:	Specify: 1000
Detection Threshold Percent:	Infinite
Rate/Leak Limit:	Specify: 3000

7. From the Attacker terminal session launch a new UDP flood attack using the same options and values as previously in this task.

8. Let the attack run for about 30 seconds before moving on.

9. In the **Configuration Utility**, click Security-> DoS Protection-> DoS Overview. You should be able to see the DHD stopping the DNS Attack.



Context Filter

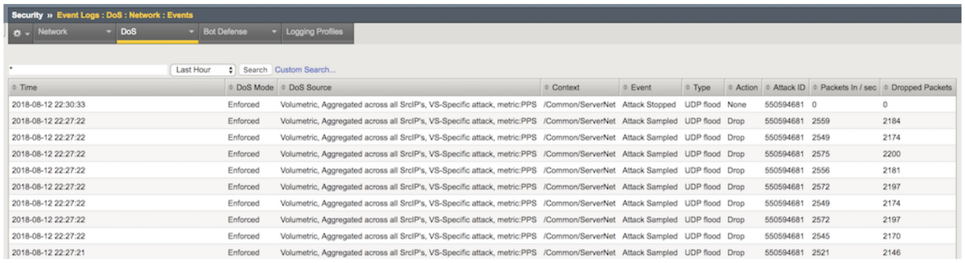
Filter Type	DoS Attack
Auto Refresh	Disabled Refresh

					Attack Status		Average Aggregate PPS			Dropped PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor
ServerNet	UDP flood	Enforced	NETWORK	ServerNet	Dropped	None	18733	5176	0	15733	0

10. Now stop the Attack with **Ctrl + C**.

11. Open the Security-> Event Logs-> DoS-> Network-> Events page.

    - In one minute or so, the virtual server column displays /**Common**/**ServerNet**, identifying this is protected object.
    - The type is UDP flood.
    - The action is Drop.



Time	DoS Mode	DoS Source	Context	Event	Type	Action	Attack ID	Packets In / sec	Dropped Packets
2018-08-12 22:30:33	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Stopped	UDP flood	None	550594681	0	0
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2559	2184
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2549	2174
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2575	2200
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2556	2181
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2572	2197
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2549	2174
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2572	2197
2018-08-12 22:27:22	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2545	2170
2018-08-12 22:27:21	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific attack, metric:PPS	/Common/ServerNet	Attack Sampled	UDP flood	Drop	550594681	2521	2146

Configure Bad Actor Detection

Add bad actor detection for the UDP flood protection

1. In the **Configuration Utility**, open the DoS Protection-> Quick Configuration page and in the **Protected Objects** section click **ServerNet**.

2. In the UDP row click the **+** icon, and then click **UDP Flood**.

3. On the right-side of the page configure using the following information, and then click **Update**.

Bad Actor Detection:	Yes (selected)
Per Source IP Detection (PPS):	Specify: 100
Per Source IP Rate Limit (PPS):	Specify: 30
Blacklist Attacking Address:	Yes (selected)
Detection Time:	30
Duration:	60

4. From the attacker virtual machine launch an UDP flood attack using a single IP address [Pentmenu tool - Options 2, 7]:

target IP/hostname:	server4
target port (defaults to 80):	53
random string (data to send):	F5Agility2018
source IP:	i[interface]

5. Let the attack run for like 30s seconds before moving on.
6. Stop the attack with **Ctrl + C**.
7. Now try to ping the **server4**. Try to ping the same address from the **goodclient** virtual machine. Does it work ???
8. Stop the Attack with **Ctrl + C** and move to the next exercise.

Configure Protected Object-Based Sweep Protection

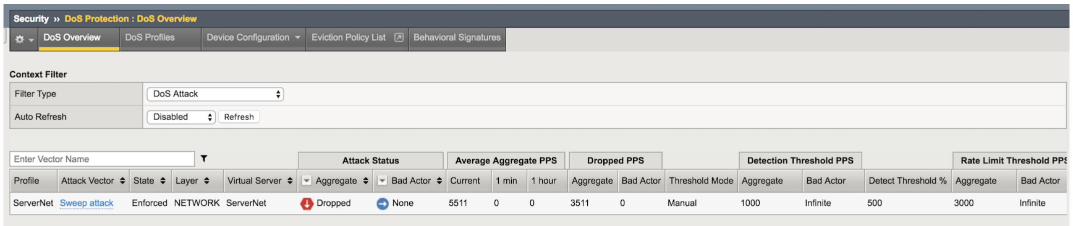
1. In the **Configuration Utility**, open the DoS Protection-> Quick Configuration page and in the **Protected Objects** section click **ServerNet**.
2. In the **DDoS Settings** row click the **Sweep** checkbox.
3. In the **Sweep** row click the **+** icon, and then click **Sweep**.
4. On the right-side of the page configure using the following information, and then click **Update**.

Detection Threshold PPS:	Specify: 1000
Rate/Leak Limit:	Specify: 3000
Packet Types:	Move All IPv4 to the Selected field

5. On the attacker machine type (or copy and paste) the following command:

```
sudo ./sweep.sh
```

6. Let the attack run for like 30s seconds before moving on.
7. Stop the attack with **Ctrl + C**.
8. In the **Configuration Utility**, click Security-> DoS Protection-> DoS Overview. You should be able to see the DHD stopping the Sweep attack.



Context Filter

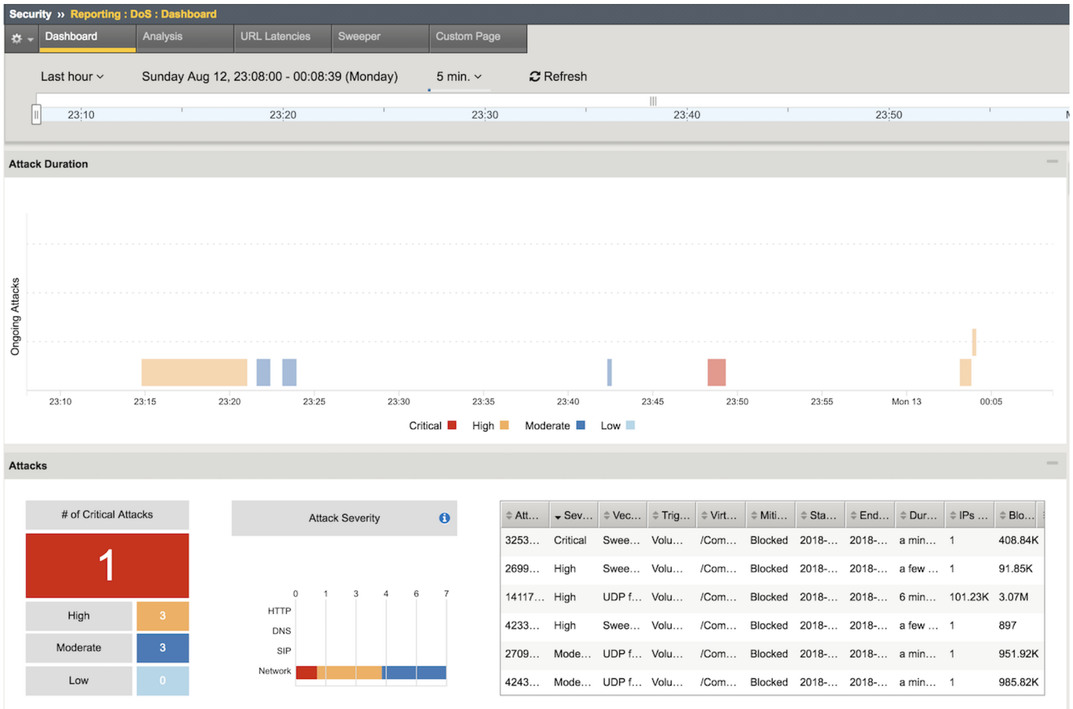
Filter Type: DoS Attack

Auto Refresh: Disabled Refresh

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
ServerNet	Sweep attack	Enforced	NETWORK	ServerNet	Dropped	None	5511	0	0	3511	0	Manual	1000	Infinite	500	3000	Infinite

Check out the DoS Visibility Page

1. Use the **DoS Visibility** page to view statistics about the DoS attacks you submitted during this exercise.



Last hour

Sunday Aug 12, 23:08:00 - 00:08:39 (Monday)

5 min.

# of Critical Attacks	
1	
High	3
Moderate	3
Low	0

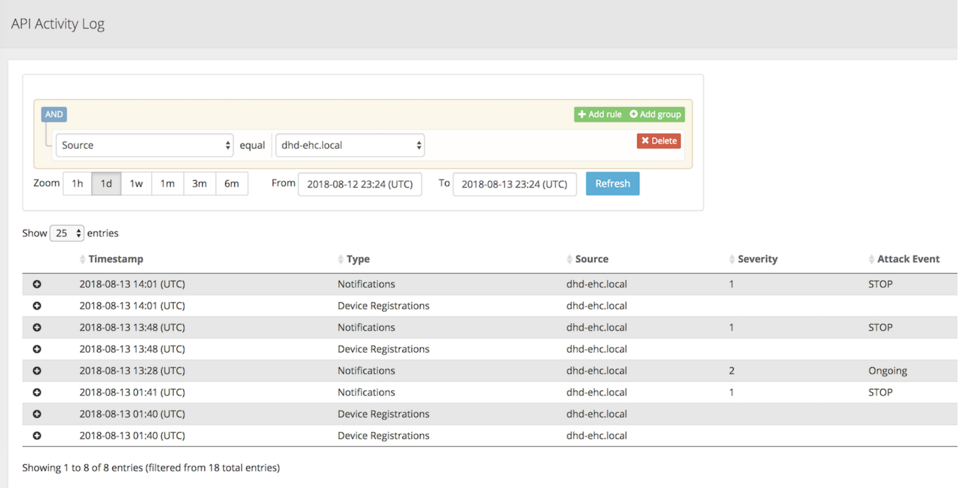
Att…	Sev…	Vec…	Trig…	Virt…	Miti…	Sta…	End…	Dur…	IPs …	Blo…
3253…	Critical	Swee…	Volu…	/Com…	Blocked	2018-…	2018-…	a min…	1	408.84K
2699…	High	Swee…	Volu…	/Com…	Blocked	2018-…	2018-…	a few …	1	91.85K
14117…	High	UDP f…	Volu…	/Com…	Blocked	2018-…	2018-…	6 min…	101.23K	3.07M
4233…	High	Swee…	Volu…	/Com…	Blocked	2018-…	2018-…	a few …	1	897
2709…	Mode…	UDP f…	Volu…	/Com…	Blocked	2018-…	2018-…	a min…	1	951.92K
4243…	Mode…	UDP f…	Volu…	/Com…	Blocked	2018-…	2018-…	a min…	1	985.82K

2. Mouse over several of the attacks to get additional details of each attack.
3. Scroll down in the left-side of the page to view the **Attacks** section.
4. You can see the number of high, moderate, and low attacks in addition to the types of attacks (HTTP, ICMP, etc.) and the severity levels.

Check out the Silverline Portal

Use the Silverline portal to view details about the attacks launched in this exercise.

1. Access the Silverline Portal https://portal.f5silverline.com
2. Open the Audit-> API Activity log page.
3. Enter the hostname of your DHD device in the **Search field** and then check out the activity your Hybrid Defender device has reported back to the Silverline Scrubbing Center.



Source equal dhd-ehc.local

From 2018-08-12 23:24 (UTC) To 2018-08-13 23:24 (UTC)

Show 25 entries

	Timestamp	Type	Source	Severity	Attack Event
⊕	2018-08-13 14:01 (UTC)	Notifications	dhd-ehc.local	1	STOP
⊕	2018-08-13 14:01 (UTC)	Device Registrations	dhd-ehc.local		
⊕	2018-08-13 13:48 (UTC)	Notifications	dhd-ehc.local	1	STOP
⊕	2018-08-13 13:48 (UTC)	Device Registrations	dhd-ehc.local		
⊕	2018-08-13 13:28 (UTC)	Notifications	dhd-ehc.local	2	Ongoing
⊕	2018-08-13 01:41 (UTC)	Notifications	dhd-ehc.local	1	STOP
⊕	2018-08-13 01:40 (UTC)	Device Registrations	dhd-ehc.local		
⊕	2018-08-13 01:40 (UTC)	Device Registrations	dhd-ehc.local		

Showing 1 to 8 of 8 entries (filtered from 18 total entries)

6.3.3 Lab - Preventing DNS DoS Attacks

Use a protected object to mitigate DNS query floods.

Use a Protected Object to Mitigate a DNS Query Flood

1. In the **Protected Objects** section click Create.
2. Configure a protected object using the following information, and then click Create.

Name:	DNS_Server
IP Address:	10.1.20.14/32
Port:	53
Protocol	UDP
Protec. Settings Action:	Log and Mitigate
Protec. Settings DDoS:	DNS

3. In the DNS row click the **+** icon, and then click **DNS A Query**.
4. On the right-side of the page configure using the following information, and then click **Create**.

Detection Threshold PPS:	Specify: 75
Rate Limit	Specify: 100

Establish a DNS Baseline

Use a script to establish a DNS baseline on the BIG-IP DHD.

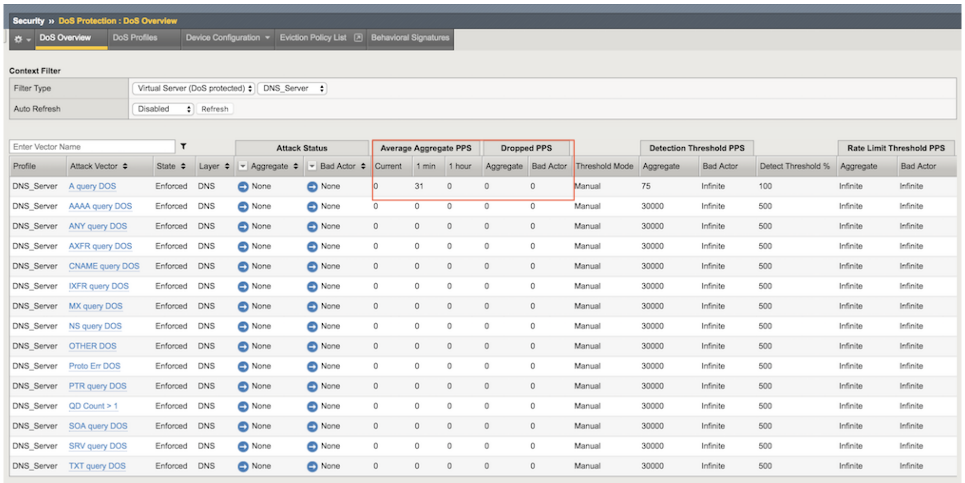
1. From the **goodclient** terminal session run the following commands:

```
sudo ~/tools_agility_183/dnsbaseline.sh
```

2. Let the baseline run until you get the following results:

```
[Status] Testing complete (time limit)

Statistics:

Queries sent:         6000
Queries completed:    6000 (100.00%)
Queries lost:         0 (0.00%)

Response codes:       NXDOMAIN 6000 (100.00%)
Average packet size:  request 41, response 116
Run time (s):         120.000552
Queries per second:   49.999770

Average Latency (s):  0.005793 (min 0.003970, max 0.020681)
Latency StdDev (s):   0.001383
```

3. In the **Configuration Utility**, go to Security-> DoS Protection-> DoS Overview.
4. In the Filter Type select **Virtual Server** with **DNS_Server** protected object, then examine the a statistics for **DNS A Query**.



Context Filter

Filter Type	Virtual Server (DoS protected) · DNS_Server
Auto Refresh	Disabled · Refresh

Enter Vector Name

				Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
DNS_Server	A query DOS	Enforced	DNS	None	None	0	31	0	0	0	Manual	75	Infinite	100	Infinite	Infinite
DNS_Server	AAAA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	ANY query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	AXFR query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	CNAME query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	IXFR query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	MX query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	NS query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	OTHER DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	Proto Err DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	PTR query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	QD Count > 1	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	SOA query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	SRV query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite
DNS_Server	TXT query DOS	Enforced	DNS	None	None	0	0	0	0	0	Manual	30000	Infinite	500	Infinite	Infinite

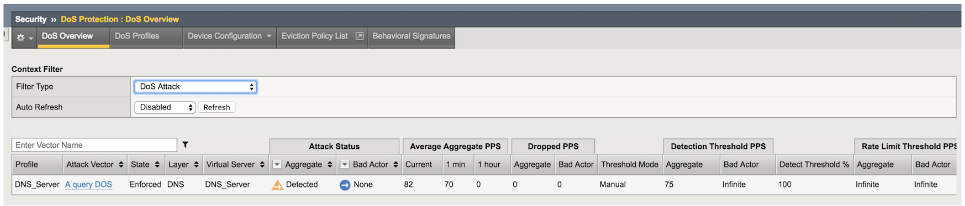
Initiate a DNS Attack

Run a script to generate a DNS DoS alert. This script will send 80 pps of “A” queries just above our detection threshold PPS setting of 75. This is just the threshold that we are alerting at. It has not reached a high enough threshold to determine that we should do something about it.

1. From the attacker terminal session run the following commands:

   ```
   sudo ~/tools_agility_183/dnsdosattack.sh
   ```

2. Wait for the attack to run for about 30 seconds before moving on.
3. In the **Configuration Utility**, open the Security-> DoS Protection-> DoS Overview page.
4. In the Filter Type select **DoS Attack**.



Context Filter

Filter Type	DoS Attack
Auto Refresh	Disabled · Refresh

Enter Vector Name

					Attack Status		Average Aggregate PPS			Dropped PPS			Detection Threshold PPS			Rate Limit Threshold PPS	
Profile	Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor	Threshold Mode	Aggregate	Bad Actor	Detect Threshold %	Aggregate	Bad Actor
DNS_Server	A query DOS	Enforced	DNS	DNS_Server	Detected	None	82	70	0	0	0	Manual	75	Infinite	100	Infinite	Infinite

Note: The A query DOS attack vector will be detected, but not yet blocked. It will take up to a couple minutes to display as Detected.

5. Wait for the attack to complete (if not done yet). Verify the results of the DNS attack from the **attacker** terminal session:

```
[Status] Testing complete (time limit)

Statistics:

Queries sent:          28800
Queries completed:     27217 (94.50%)
Queries lost:          1583 (5.50%)

Response codes:        NXDOMAIN 27217 (100.00%)
Average packet size:   request 41, response 116
```

```
Run time (s):          360.000538
Queries per second:    75.602665

Average Latency (s):   0.004487 (min 0.002909, max 0.036921)
Latency StdDev (s):    0.001372
```

Initiate a DNS Attack that Exceeds the Rate Limit

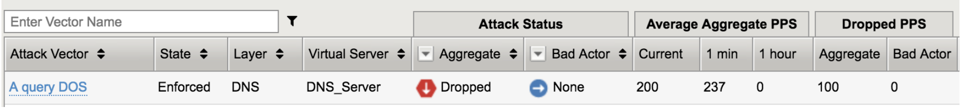
Run another script that initiates a DNS DoS attack that exceeds the rate limit we set earlier.

1. From the attacker terminal session run the following commands:

   ```
   sudo ~/tools_agility_183/dnsdosrate.sh
   ```

2. Wait for the attack to run for about 30 seconds before moving on.

3. In the **Configuration Utility** Review the DoS Overview page -> Security-> DoS Protection-> DoS Overview.



Enter Vector Name				Attack Status		Average Aggregate PPS			Dropped PPS	
Attack Vector	State	Layer	Virtual Server	Aggregate	Bad Actor	Current	1 min	1 hour	Aggregate	Bad Actor
A query DOS	Enforced	DNS	DNS_Server	Dropped	None	200	237	0	100	0

Note: The A query DOS attack vector is now dropping attack traffic.

Also take a look at the script which will record the number of drops if any as a result of the attack rate limit being hit. You should be able to correlate the drops registered with the script with the drops recorded by the Hybrid Defender.

```
Statistics:

Queries sent:          5899
Queries completed:     3504 (59.40%)
Queries lost:          2395 (40.60%)

Response codes:        NXDOMAIN 3504 (100.00%)
Average packet size:   request 41, response 116
Run time (s):          120.000642
Queries per second:    29.199844

Average Latency (s):   0.006696 (min 0.002080, max 0.087619)
Latency StdDev (s):    0.003606
```

4. In the **Configuration Utility** open the Statistics-> DoS Visibility page.

5. View the attack details in the **Attacks** section.

6.4 Module - Application Layer DoS Protection

In this module you will learn how the F5 Hybrid Defender can effectively protect from DoS Attacks at the Application Level.

6.4.1 Lab – Configure Application Layer DoS Defenses

Check out how to detect and mitigate application layer attacks, not matter if it's encrypted or behavioral based.

Create Protected Object for Behavioral DoS Protection

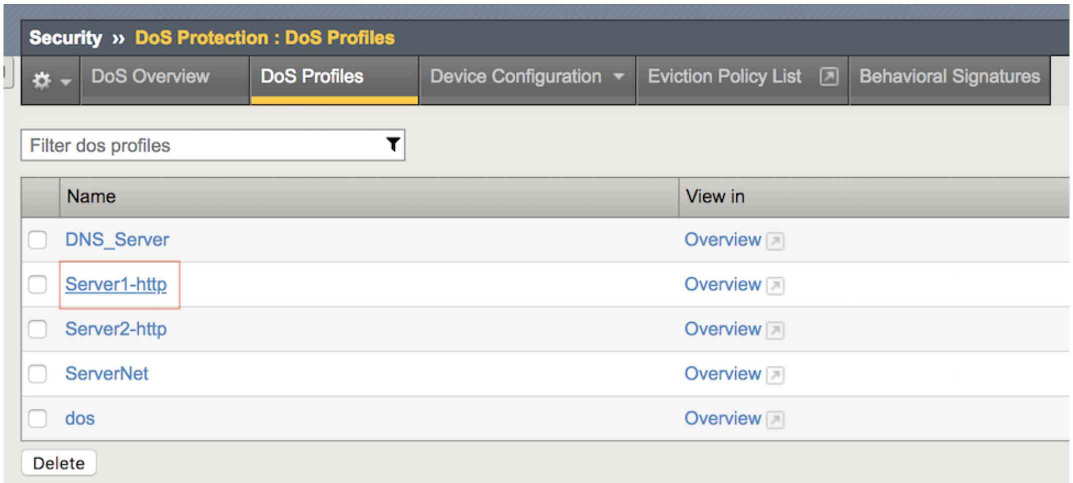
1. In the **BIG-IP Configuration Utility**, open the DoS Protection-> Quick Configuration page and in the **Protected Objects** section click **Create**.
2. Configure the protected object **Server1-http** using the following information:

Name:	Server1-http
IP Address:	10.1.20.11/32
Port:	80
VLAN:	defaultVLAN
Protec. Settings Action:	Log and Mitigate
Protec. Settings Silverline:	Yes (selected)
Protec. Settings DDoS:	IPv4, TCP, HTTP

3. In the HTTP row click the **+** icon, and then click **Behavioral**, then from the **Mitigation** list select **Standard Protection**.
4. In the HTTP section click **Proactive Bot Defense**, then from the **Mitigate Action** list select **Disabled**, finally click **Create**

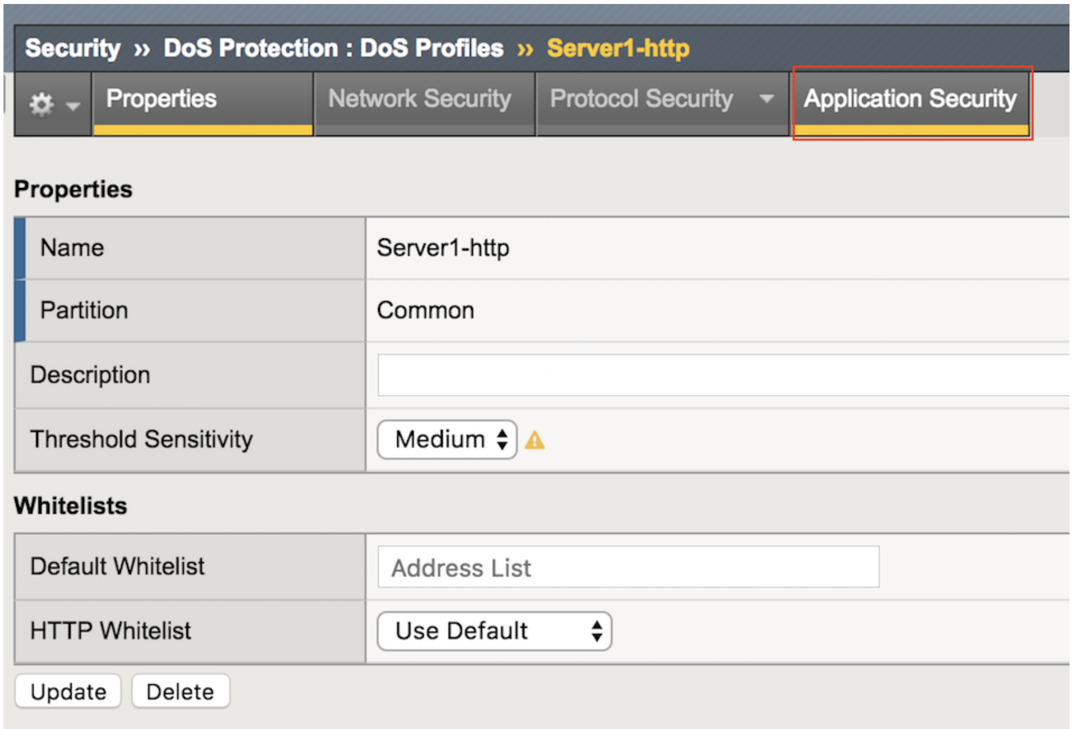
> **Note:** Both the good and bad (attack) traffic are generated with tools that would be blocked by **Proactive Bot Defense**. Please note that by default, the Hybrid Defender will set Proactive Bot Defense to **always**'. That's the reason why we're disabling it, only to allow the scripts to work and generate sample traffic.

5. In the **Protected Objects** section click **Create**.
6. Open the Security-> DoS Protection-> DoS Profiles page and click **Server1-http**.



Name	View in
DNS_Server	Overview
Server1-http	Overview
Server2-http	Overview
ServerNet	Overview
dos	Overview

7. Open the **Application Security** page.



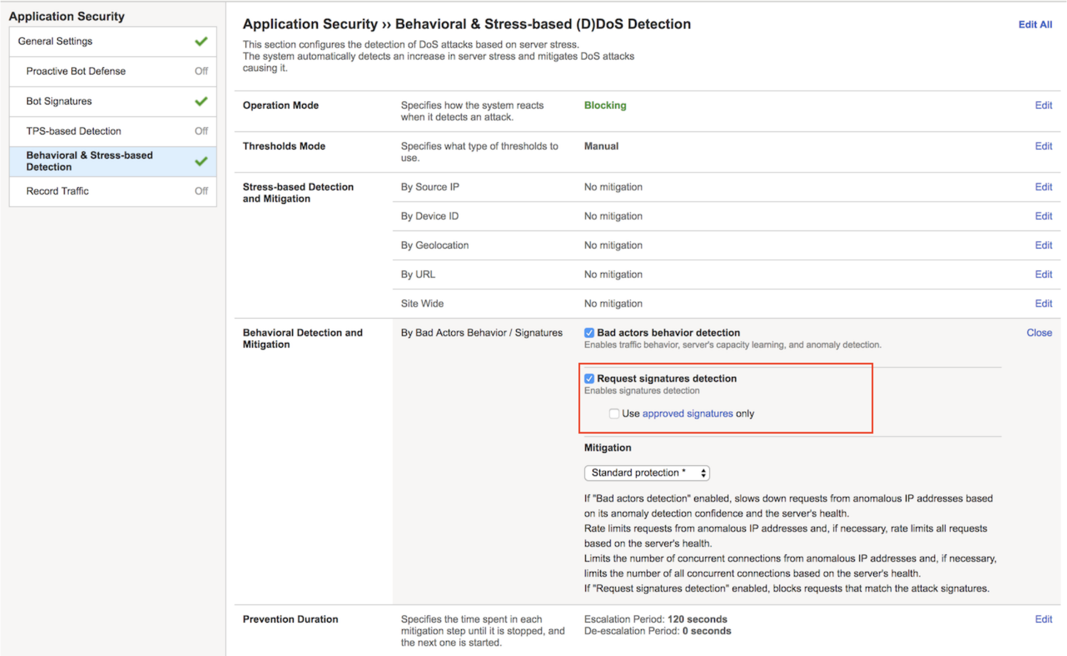
Properties

Name	Server1-http
Partition	Common
Description	
Threshold Sensitivity	Medium

Whitelists

Default Whitelist	Address List
HTTP Whitelist	Use Default

8. Click **Behavioral & Stress-based Detection**, and then for **Behavioral Detection and Mitigation** click **Edit**.
9. Select the **Request signatures detection** checkbox, and then click **Update**.



Application Security ›› Behavioral & Stress-based (D)DoS Detection

This section configures the detection of DoS attacks based on server stress.
The system automatically detects an increase in server stress and mitigates DoS attacks causing it.

Operation Mode	Specifies how the system reacts when it detects an attack.	Blocking	Edit
Thresholds Mode	Specifies what type of thresholds to use.	Manual	Edit
Stress-based Detection and Mitigation	By Source IP	No mitigation	Edit
	By Device ID	No mitigation	Edit
	By Geolocation	No mitigation	Edit
	By URL	No mitigation	Edit
	Site Wide	No mitigation	Edit
Behavioral Detection and Mitigation	By Bad Actors Behavior / Signatures	☑ Bad actors behavior detection Enables traffic behavior, server's capacity learning, and anomaly detection. ☑ Request signatures detection Enables signatures detection □ Use approved signatures only Mitigation Standard protection * If "Bad actors detection" enabled, slows down requests from anomalous IP addresses based on its anomaly detection confidence and the server's health. Rate limits requests from anomalous IP addresses and, if necessary, rate limits all requests based on the server's health. Limits the number of concurrent connections from anomalous IP addresses and, if necessary, limits the number of all concurrent connections based on the server's health. If "Request signatures detection" enabled, blocks requests that match the attack signatures.	Close
Prevention Duration	Specifies the time spent in each mitigation step until it is stopped, and the next one is started.	Escalation Period: **120 seconds** De-escalation Period: **0 seconds**	Edit

Generate L7 Behavioral baseline for Server1-http

Use a script to generate an L7 behavioral DoS baseline for the Hybrid Defender.

1. In the **goodclient** terminal session, type (or copy and paste) the following command:

```
sudo ~/tools_agility_183/generate_clean_traffic.sh
```

Note: This will generate traffic. Please note that it will take at least 15 minutes.

```
f5student@goodclient:~/tools_agility_183$ ./generate_clean_traffic.sh
welcome.php     status: 200     bytes: 1045     time: 0.017
welcome.php     status: 200     bytes: 1045     time: 0.014
welcome.php     status: 200     bytes: 1045     time: 0.014
welcome.php     status: 200     bytes: 1045     time: 0.015
headers.php     status: 200     bytes: 1847     time: 0.014
headers.php     status: 200     bytes: 1847     time: 0.014
httprequest.php status: 200     bytes: 710      time: 0.013
httprequest.php status: 200     bytes: 710      time: 0.014
httprequest.php status: 200     bytes: 710      time: 0.014
httprequest.php status: 200     bytes: 710      time: 0.013
badlinks.html   status: 200     bytes: 1270     time: 0.014
badlinks.html   status: 200     bytes: 1270     time: 0.014
F5_building.jpg status: 200     bytes: 33447    time: 0.019
F5_building.jpg status: 200     bytes: 33447    time: 0.021
bigip4200.jpg   status: 200     bytes: 9753     time: 0.016
bigip4200.jpg   status: 200     bytes: 9753     time: 0.017
viprion2400.jpg status: 200     bytes: 13009    time: 0.016
viprion4800.jpg status: 200     bytes: 10078    time: 0.018
viprion4800.jpg status: 200     bytes: 10078    time: 0.017
```

1. Move on in the exercises while the baseline is being generated.
2. Open a terminal session with the DHD and run the following command:

```
admd -s vs./Common/Server1-http.info -s vs./Common/
Server1-http.sig.health
```

```
[root@dhd-01:Active:Standalone]# admd -s vs./Common/Server1-http.info -s vs./
↪Common/Server1-http.sig.health
vs./Common/Server2-http.sig.health:[0.452373]
vs./Common/Server2-http.sig.health:[0.453407]
vs./Common/Server2-http.sig.health:[0.451726]
vs./Common/Server2-http.sig.health:[0.45372]
vs./Common/Server2-http.sig.health:[0.452021]
vs./Common/Server2-http.sig.health:[0.45349]
```

Important: The results for each health check should **not** be 0.5, otherwise the system ins't learning. Let both terminal sessions opened for the rest of this lab.

Configure DoS Protection for L7 Encrypted Traffic

Launch an encrypted Slowloris attack to the web server and view the results, then configure proper mitigation on the Hybrid Defender.

1. Go to DoS Protection-> Quick Configuration page and in the **Protected Objects** section click **Create**.
2. Configure another **Protected Object** using the following information, and then click **Create**.

Name:	Server2-http
IP Address:	10.1.20.12/32
Port:	80
VLAN:	defaultVLAN
Protec. Settings Action:	Log and Mitigate
Protec. Settings Silverline:	Yes (selected)
Protec. Settings DDoS:	IPv4, TCP, HTTP

3. Now repeat the steps for disabling the Proactive Bot Defense which allows the HTTP request scripts to work.

4. Go to the **HTTP** section and click **Proactive Bot Defense**, then from the **Mitigate Action** list select **Disabled**.

5. In the HTTP section click **DoS Tool**, then from the **Mitigate Action** list select **Report**, and then click **Create**.

6. Now run the monitor script on **server2** as follows. It will be usefull for server health monitoring.

   ```
   ~/tools_agility_183/server2_monitor.sh
   ```

7. Before launching the application layer attack, observe **server2** is currently healthy.

   ```
   welcome.php     status: 200 bytes: 1045     time: 0.018
   bigtext.html    status: 200 bytes: 634965   time: 0.136
   httprequest.php status: 200 bytes: 710      time: 0.017
   ```

   Note: The system is healthy since the web server returns **HTTP Status Code 200** for every request.

8. Now from the **attacker** terminal session run the following command:

   ```
   ~/tools_agility_183/slowloris.sh
   ```

   ```
   Mon Aug 13 11:26:54 2018:
   slowhttptest version 1.6
   - https://code.google.com/p/slowhttptest/ -
   test type:                          SLOW HEADERS
   number of connections:              4090
   URL:                                https://server2.f5demo.com/
   verb:                               GET
   Content-Length header value:        4096
   follow up data max size:            68
   interval between follow up data:    10 seconds
   connections per seconds:            200
   probe connection timeout:           5 seconds
   test duration:                      240 seconds
   using proxy:                        no proxy

   Mon Aug 13 11:26:54 2018:
   slow HTTP test status on 30th second:
   initializing:        0
   pending:             1790
   connected:           150
   error:               0
   ```

```
closed:                 2092
service available:    **NO**
```

9. Observe how the service is impacted as the slowloris attack hits the **server2.f5demo.com**.

```
welcome.php     status: 000 bytes: 0    time: 1.002
bigtext.html    status: 000 bytes: 0    time: 1.002
httprequest.php status: 000 bytes: 0    time: 1.002
```

> **Note:** Since the slowloris attack is being encrypted (https://server2.f5demo.com) we need to setup the certificate and private keys so the traffic can be inspected by the Hybrid Defender..

10. Configure SSL on the protected object to in order to inspect HTTPS traffic.
11. Go to DDoS Protection-> Quick Configuration-> Protected Objects, then click **Server2-http**. Configure the SSL as follows:

Port:	443
SSL:	Enabled
SSL Certificate:	default
Key:	default
Encrypt Connection to Server:	Yes (selected)

12. Disable bot protections so the scripts can be used for testing the server health.
13. On the **Server2-http** Protected Object section go to the **HTTP** row, click the **+** icon, click **Behavioral**
14. Now from the **Mitigation** list select **Standard Protection**.
15. In the HTTPS section click **Proactive Bot Defense**, then from the **Mitigate Action** list select **Disabled**.
16. Now that SSL is also being inspected for this Protected Object, let's run the slowloris script once again and verify if the attack still works.

– Behavioral L7 DoS Mitigation

Once the L7 behavioral baseline has been established, launch an L7 DoS attack and view the results.

1. Now get back to the DHD terminal session.
2. You will need to observe the info.learning signature to ensure that the system has accumulated enough learning details.
3. This signature has 4 comma-separated values for monitoring the learning progress:
   - **Value #1: baseline-learning_confidence** This should be between 80 - 90%
   - **Value #2: learned_bins_count (the number of learned bins)** This should be > 0
   - **Value #3: good_table_size (the number of learned requests)** This should be > 4000

- **Value #4: good_table_confidence (how confident, as a percentage, the system is)**
  It must be 100% for behavioral signatures

  ```
  vs./Common/Server1-http.info.learning:[96.3163, 78, 5355, 100]
  ```

4. If you see the pattern such as that described, it indicates the traffic baseline was already established, then you can move forward with the lab.

5. Once the info.learning values are acceptable based on the details above, from the **attacker** terminal session run the following command:

   ```
   ~/tools_agility_183/http_flood.sh
   ```

6. Select option "1"

7. Now take a look at the **goodclient** terminal session, you should start seeing the effects of the HTTP DoS attack, as requests are starting to fail **(HTTP Status Code 000)**. If you were to examine the **Lamp** server at this time, you would see that it is under severe stress.

   ```
   welcome.php status: 200     bytes: 1045     time: 0.017
   welcome.php status: 200     bytes: 1045     time: 0.029
   welcome.php status: 000     bytes: 0        time: 1.000
   headers.php status: 000     bytes: 0        time: 1.001
   headers.php status: 200     bytes: 1847     time: 0.204
   headers.php status: 200     bytes: 1847     time: 0.258
   headers.php status: 200     bytes: 1847     time: 0.218
   badlinks.html       status: 000     bytes: 0        time: 1.001
   badlinks.html       status: 200     bytes: 1270     time: 0.242
   badlinks.html       status: 200     bytes: 1270     time: 0.272
   badlinks.html       status: 000     bytes: 0        time: 1.002
   bigip4200.jpg       status: 200     bytes: 9318     time: 0.247
   ```

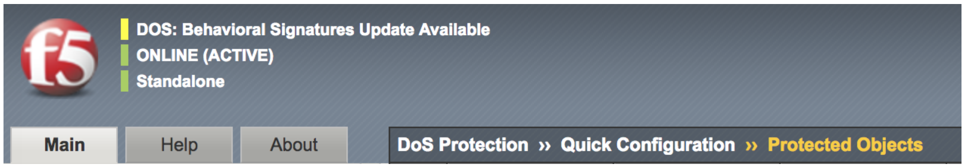
8. Also from the DHD terminal session watch the health signal feed. You should see it climb from ~.5, which is optimal health, to values over 1, indicating an increase in server stress. You will also be able to watch as the system responds and mitigations are engaged.

9. When the system has analyzed the attack traffic, dynamic signatures are created and engaged:

   ```
   vs./Common/Server1-http.sig.health:[0.768427]
   vs./Common/Server1-http.info.attack:[1, 1]
   vs./Common/Server1-http.sig.health:[0.746648]
   vs./Common/Server1-http.info.signature:["Stable signature␣
    ↪detected: (http.f5_filename_bin == 21) and (http.request.method␣
    ↪eq \"GET\") and (!(http.user_agent matches \
    ↪"(MSIE|Chrome|Firefox|Opera|Safari|Maxthon|Seamonkey)\")) and (!
    ↪http.content_type) and ((http.hdr_len->= 128) and (http.hdr_len
    ↪< 256)) and (http.request.uri matches \"^[^\\\\?]*$\") and␣
    ↪(http.f5_headers_count == 5) and (http.f5_cache_control_bin ==␣
    ↪0) and (http.accept) and (http.request.line matches \"Accept-
    ↪Charset:.*\") and (http.f5_host_bin == 4) and (http.f5_referer_
    ↪bin == 0) and (http.f5_uri_len_bin == 0) and (!(http.accept␣
    ↪matches \"(application|audio|message|text|image|multipart)\"))␣
    ↪and (http.connection) and (http.host) and (!(http.request.line␣
    ↪matches \"Accept-Charset\")) and (http.user_agent)"]
   vs./Common/Server1-http.info.attack:[1, 1]
   vs./Common/Server1-http.sig.health:[0.726608]
   vs./Common/Server1-http.info.attack:[1, 1]
   vs./Common/Server1-http.sig.health:[0.709827]
   ```

```
vs./Common/Server1-http.info.attack:[1, 1]
vs./Common/Server1-http.sig.health:[0.691779]
```

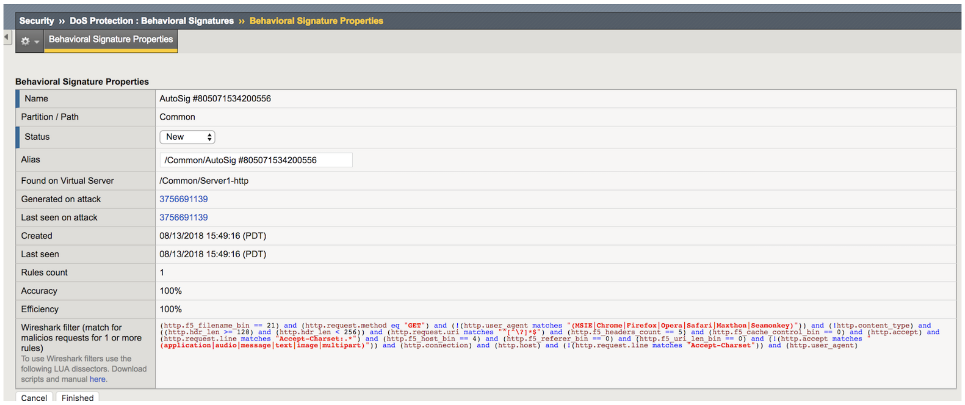
10. In the **Configuration Utility**, notice the indicator at the top-left side of the page.



DOS: Behavioral Signatures Update Available
ONLINE (ACTIVE)
Standalone

11. As you watch the feed, you should see HTTP requests being served again after the dynamic signature kicks in.

12. In the **Configuration Utility** open the Security-> DoS Protection-> Behavioral Signatures page.



Security » DoS Protection : Behavioral Signatures » Behavioral Signature Properties
Behavioral Signature Properties

Behavioral Signature Properties

Name	AutoSig #805071534200556
Partition / Path	Common
Status	New
Alias	/Common/AutoSig #805071534200556
Found on Virtual Server	/Common/Server1-http
Generated on attack	3756691139
Last seen on attack	3756691139
Created	08/13/2018 15:49:16 (PDT)
Last seen	08/13/2018 15:49:16 (PDT)
Rules count	1
Accuracy	100%
Efficiency	100%
Wireshark filter (match for malicios requests for 1 or more rules) To use Wireshark filters use the following LUA dissectors. Download scripts and manual here.	(http.f5_filename_bin == 21) and (http.request.method eq "GET") and (!(http.user_agent matches "(MSIE|Chrome|Firefox|Opera|Safari|Maxthon|Seamonkey)")) and (!http.content_type) and ((http.hdr_len >= 128) and (http.hdr_len < 256)) and (http.request.uri matches "^[^\?]*$") and (http.f5_headers_count == 5) and (http.f5_cache_control_bin == 0) and (http.accept) and (http.request.line matches "Accept-Charset:.*") and (http.f5_host_bin == 4) and (http.f5_referer_bin == 0) and (http.f5_uri_len_bin == 0) and (!(http.accept matches "(application|audio|message|text|image|multipart)")) and (http.connection) and (http.host) and (!(http.request.line matches "Accept-Charset")) and (http.user_agent)

You will see a signature that was created (as seen in the output of the `admd` command earlier). Note the system reports metrics such as Accuracy (an estimate of the percentage of traffic that will be blocked that is definitely hostile) and Efficiency (a measure of how much of the observed DoS traffic is mitigated by that signature). In our lab these values are both at or near 100%. In a real environment the Accuracy should be very high, but sometimes Efficiency will be lower (in a mutating attack) and the system may have to create additional signatures or refine the current one based on effectiveness.

13. Click the new signature.

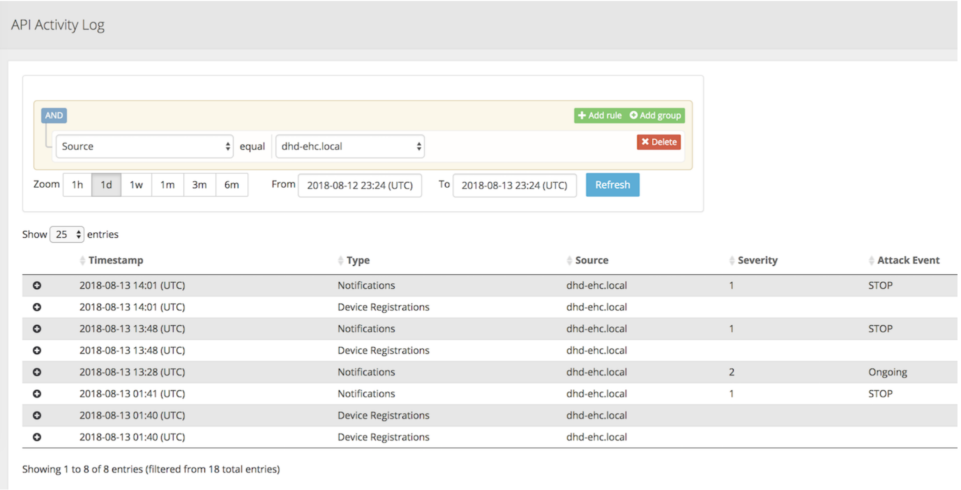
Note the Wireshark filter at the bottom which can be used in conjunction with the Record Traffic feature of F5's L7 DoS to identify exactly which requests the signature matches/will match. This can be helpful if using the "Approved Only" in the DoS profile setting to allow a risk-averse administrator to approve signatures before they begin to filter traffic.

14. Change the Alias value to **Agility2018**, and then click Finished.

– View Silverline Signals

Use the Silverline portal to view details about the L7 DoS attacks that were launched in this exercise.

1. Click **Alerts for Hybrid Defender**.
2. Open the Audit-> API Activity Log page.



Source equal dhd-ehc.local

From 2018-08-12 23:24 (UTC) To 2018-08-13 23:24 (UTC)

Show 25 entries

	Timestamp	Type	Source	Severity	Attack Event
⊕	2018-08-13 14:01 (UTC)	Notifications	dhd-ehc.local	1	STOP
⊕	2018-08-13 14:01 (UTC)	Device Registrations	dhd-ehc.local		
⊕	2018-08-13 13:48 (UTC)	Notifications	dhd-ehc.local	1	STOP
⊕	2018-08-13 13:48 (UTC)	Device Registrations	dhd-ehc.local		
⊕	2018-08-13 13:28 (UTC)	Notifications	dhd-ehc.local	2	Ongoing
⊕	2018-08-13 01:41 (UTC)	Notifications	dhd-ehc.local	1	STOP
⊕	2018-08-13 01:40 (UTC)	Device Registrations	dhd-ehc.local		
⊕	2018-08-13 01:40 (UTC)	Device Registrations	dhd-ehc.local		

Showing 1 to 8 of 8 entries (filtered from 18 total entries)

3. Click the **+** icon to expand one of the entries to view additional attack details.

That completes the hands-on exercise for BIG-IP DDoS Hybrid Defender.

7 F5 Agility 2018: DDoS Attack Protection

F5® DDoS Hybrid Defender™, a hybrid DDoS solution that offers comprehensive protection, high availability, and is easy to deploy and manage. It guards against aggressive volumetric and targeted DDoS attacks, includes hardware-assisted DDoS mitigation, and optionally, connects with Silverline, a cloud-based scrubbing service.

This class covers the following topics:

- Initial Set-up, Device Configuration and working with basic device-level DDoS vectors to mitigate the most commonly encountered attacks. Then we will cover Auto-thresholding, and Mitigation of L7 Behavioral Attacks time permitting.

7.1 Getting Started

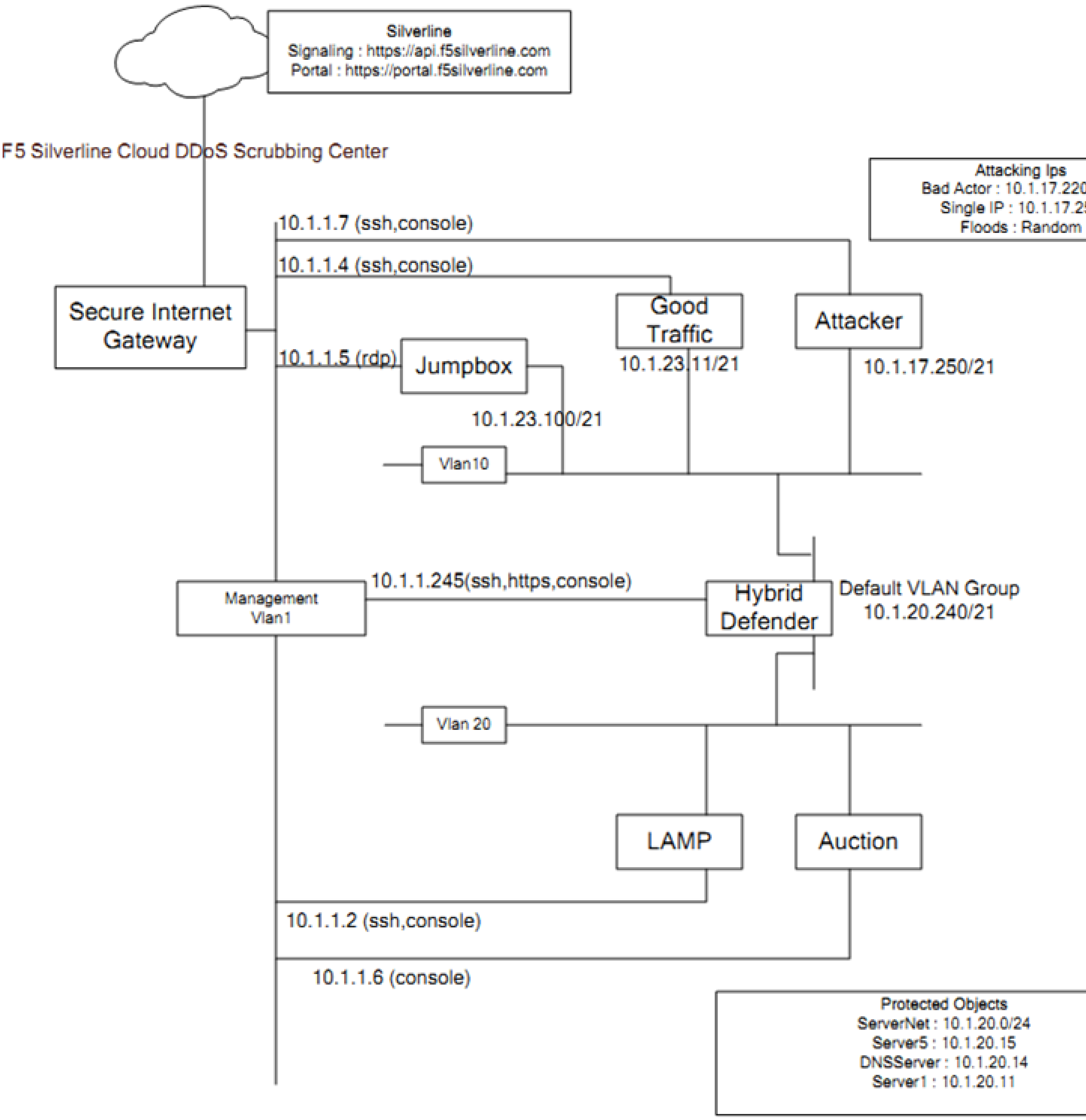
Please follow the instructions provided by the instructor to start your lab and access your jump host.

Note: All work for this lab will be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required. You will use **Putty** that has been preconfigured with appropriate keys in order to access the **DHD CLI**, **Good Client**, and the **Attacker** systems. The shortcuts are on the desktop. You will log in as “root” or “ubuntu”.

7.1.1 Lab Topology

The following components have been included in your lab environment:

- 1 x F5 BIG-IP VE (v14.0) Provisioned as DHD
- 1 x Linux Attacker (Ubuntu 14.04)
- 1 x Linux Good Client (Ubuntu 14.04)
- 1 x Linux LAMP Webserver (xubuntu 14.04)
- 1 x Windows Jumphost


Silverline
Signaling : https://api.f5silverline.com
Portal : https://portal.f5silverline.com
F5 Silverline Cloud DDoS Scrubbing Center
Attacking Ips
Bad Actor : 10.1.17.220
Single IP : 10.1.17.25
Floods : Random
10.1.1.7 (ssh,console)
10.1.1.4 (ssh,console)
Secure Internet Gateway
Good Traffic
Attacker
10.1.1.5 (rdp)
Jumpbox
10.1.23.11/21
10.1.17.250/21
10.1.23.100/21
Vlan10
10.1.1.245(ssh,https,console)
Management Vlan1
Hybrid Defender
Default VLAN Group
10.1.20.240/21
Vlan 20
LAMP
Auction
10.1.1.2 (ssh,console)
10.1.1.6 (console)
Protected Objects
ServerNet : 10.1.20.0/24
Server5 : 10.1.20.15
DNSServer : 10.1.20.14
Server1 : 10.1.20.11

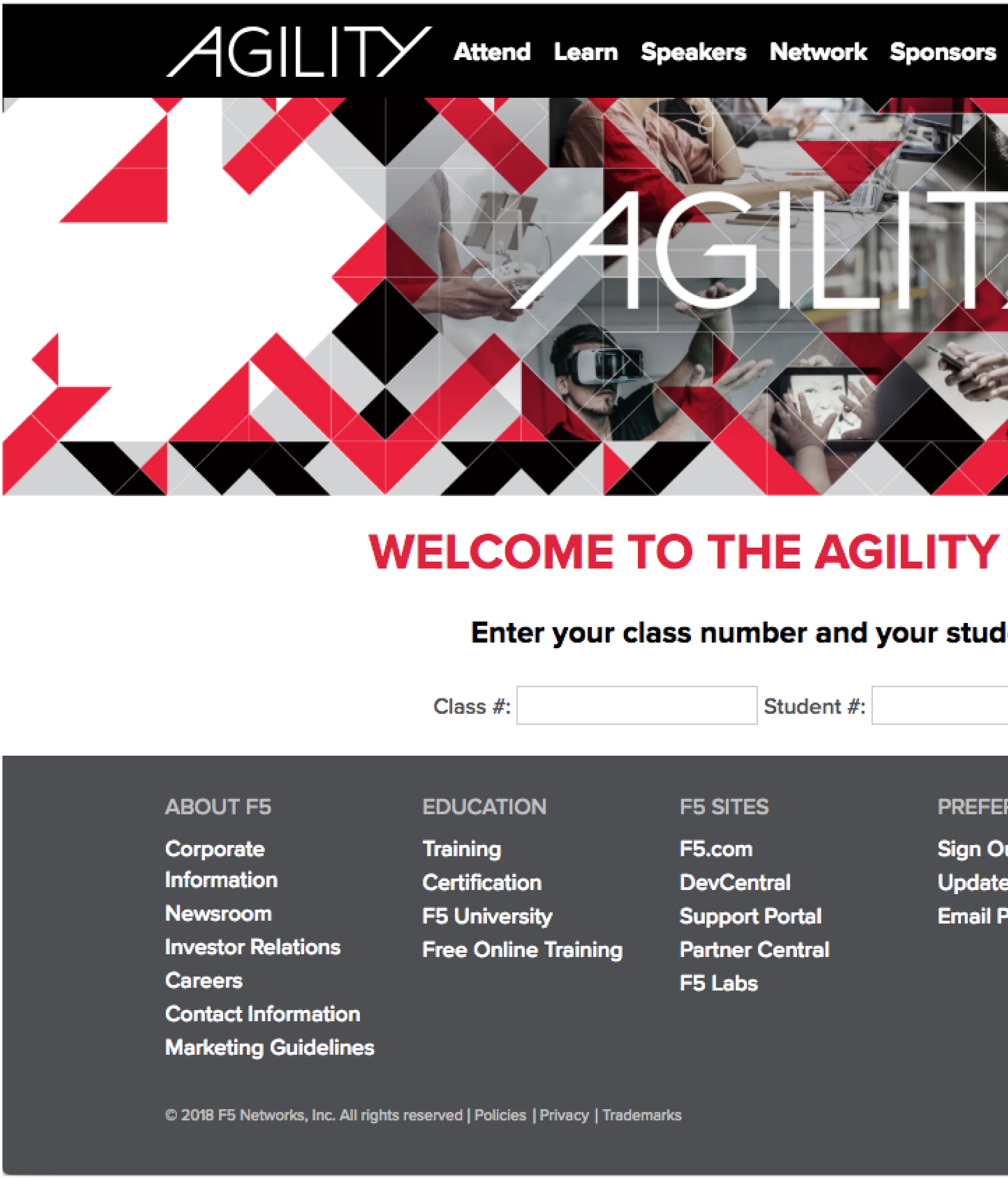
Lab Components

System	Username	Password
Ravello	Given at site	Given at site
Win7 Jumpbox	external_user	f5DEMOs4u
Hybrid Defender - WebUI	admin	f5DEMOs4u
Hybrid Defender - CLI	root	f5DEMOs4u
Good Client	ubuntu	Use key
Attacker	ubuntu	Use key
Lamp CLI	root	default
Lamp X-Server Shell	xubuntu	<no password>

7.1.2 Accessing the Lab Environment

Task 1 – Open your RDP client and connect to your Windows Jumpbox

- A URL will be provided by your Instructor at the training site that will access the training portal.
- In the training portal you will enter the given class number and student number.



WELCOME TO THE AGILITY

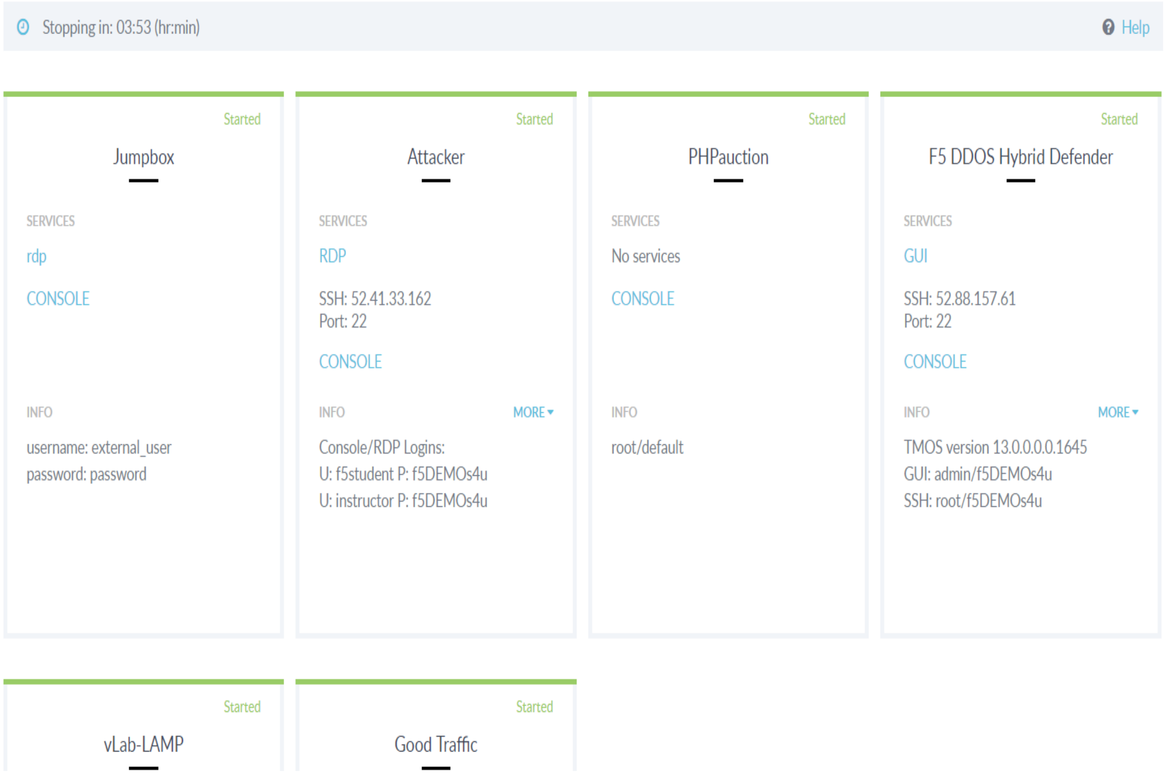
Enter your class number and your stud

Class #: Student #:

© 2018 F5 Networks, Inc. All rights reserved | Policies | Privacy | Trademarks

- Login

- Click the Jumpbox RDP link.



Stopping in: 03:53 (hr:min)

Help

Started

Jumpbox

SERVICES

rdp

CONSOLE

INFO

username: external_user
password: password

Started

Attacker

SERVICES

RDP

SSH: 52.41.33.162
Port: 22

CONSOLE

INFO MORE ▾

Console/RDP Logins:
U: f5student P: f5DEMOs4u
U: instructor P: f5DEMOs4u

Started

PHPauction

SERVICES

No services

CONSOLE

INFO

root/default

Started

F5 DDOS Hybrid Defender

SERVICES

GUI

SSH: 52.88.157.61
Port: 22

CONSOLE

INFO MORE ▾

TMOS version 13.0.0.0.0.1645
GUI: admin/f5DEMOs4u
SSH: root/f5DEMOs4u

Started

vLab-LAMP

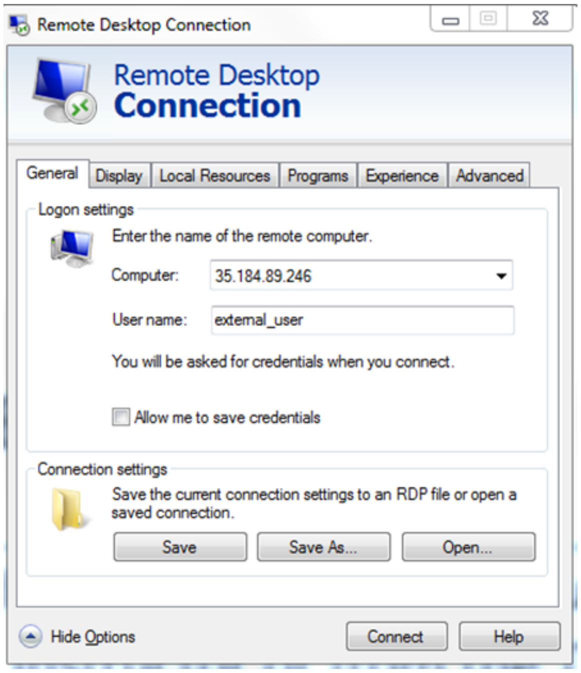
Started

Good Traffic

This will RDP to the Jumpbox where you will work all the labs from.

Note: Use the show options to provide details.

- Login to the Jumpbox
- User name: Jumpbox external_user. Password: f5DEMOs4u



Logon settings

Enter the name of the remote computer.

Computer: 35.184.89.246

User name: external_user

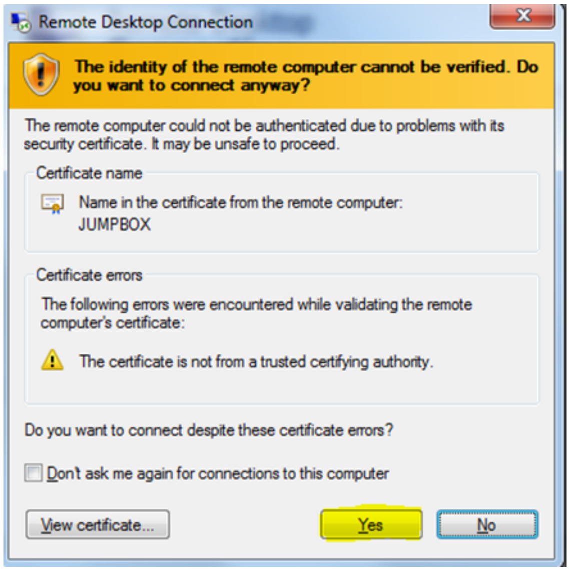
You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

- Click YES at the warning



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
JUMPBOX

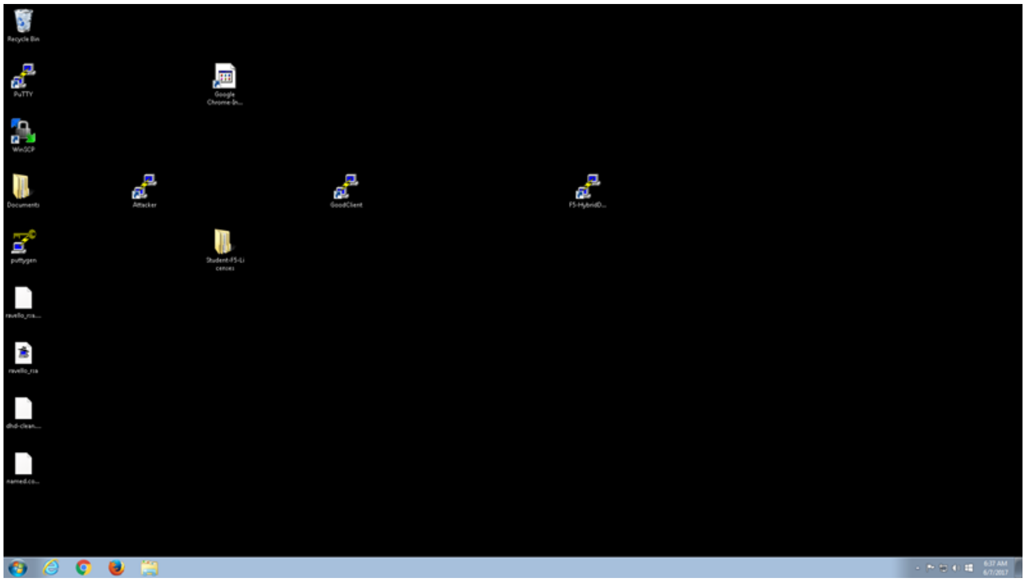
Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer



Note: We need to ensure the Jumpbox and the DDoS Hybrid Defender are in time sync. Please run the following commands from an Elevated Command Prompt. (Administrator)

- net start w32time
- w32tm /config /update /manualpeerlist:10.1.1.245
- net stop w32time && net start w32time

7.2 DDoS Hybrid Defender Setup

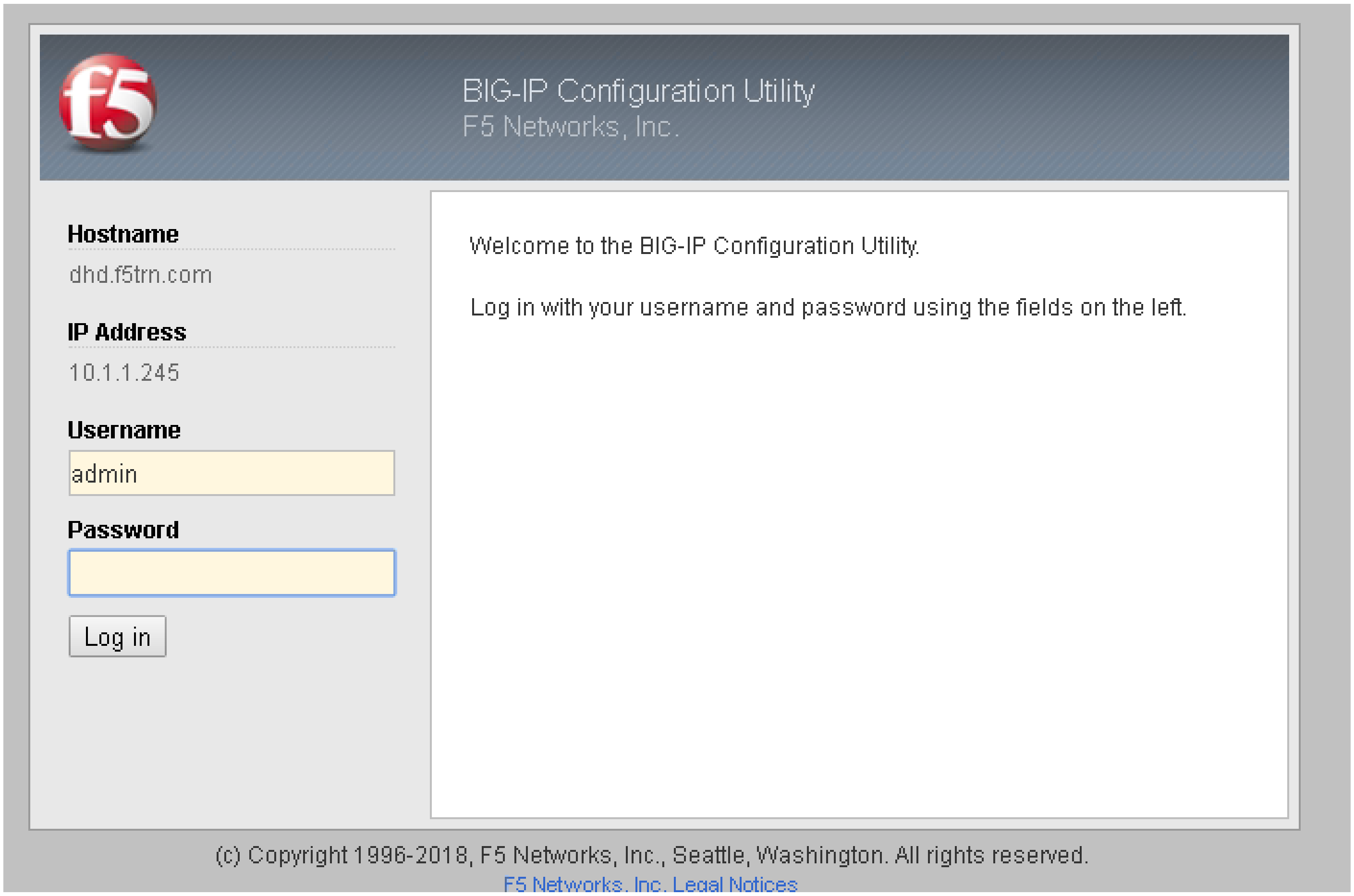
In this module you will learn how to complete the setup of F5 Networks DDoS Hybrid Defender and the initial configuration related to Device Protection.

7.2.1 Lab 1 – DDoS Hybrid Defender Setup

Estimated completion time: 20 minutes

Task 1 – Initial Set-up

- Open the Chrome web browser and access the DHD from the toolbar shortcut.
- Login to the BIG-IP Configuration Utility using the "admin" account.



BIG-IP Configuration Utility
F5 Networks, Inc.

Hostname
dhd.f5trn.com

IP Address
10.1.1.245

Username
admin

Password

Welcome to the BIG-IP Configuration Utility.

Log in with your username and password using the fields on the left.

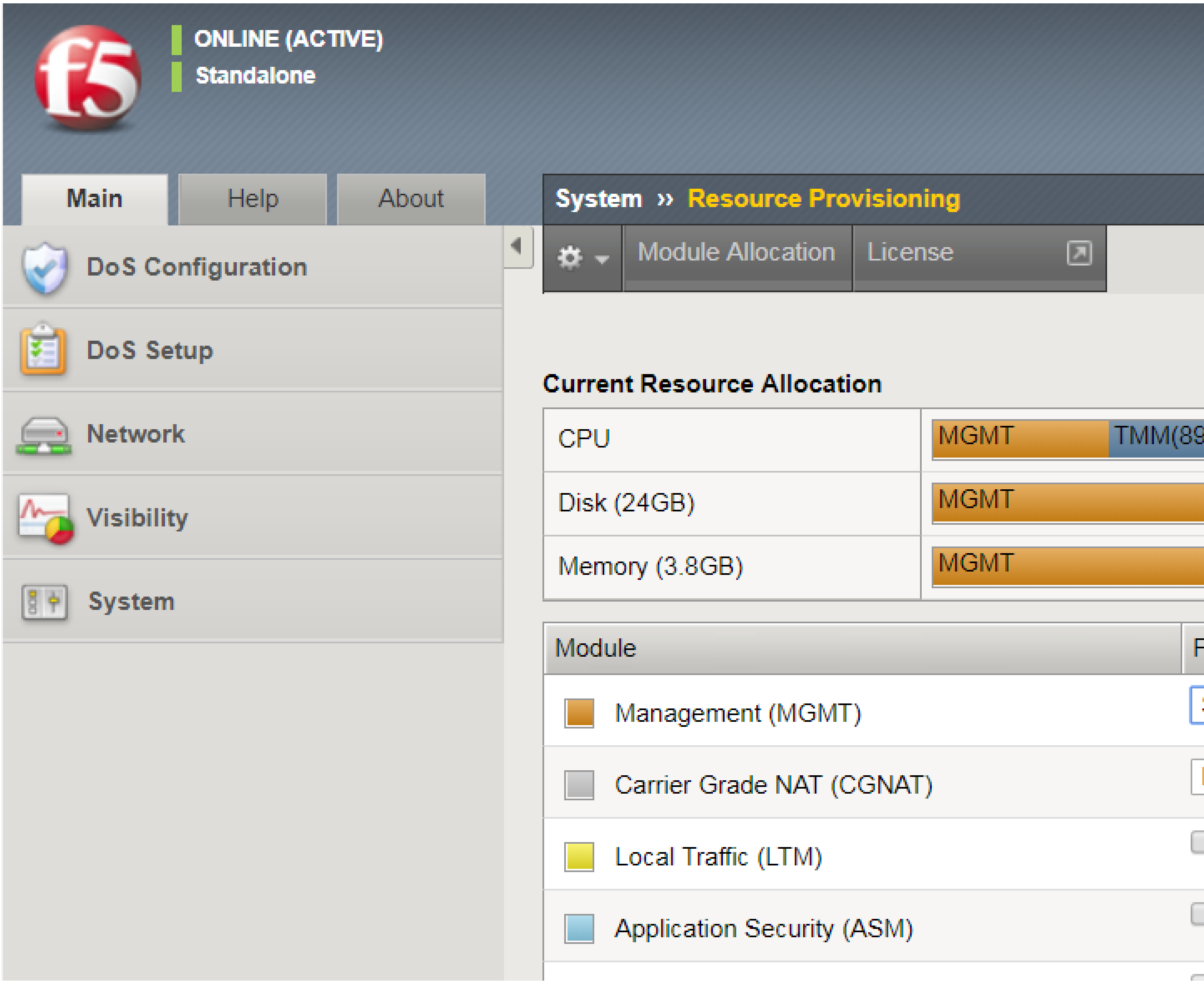
(c) Copyright 1996-2018, F5 Networks, Inc., Seattle, Washington. All rights reserved.
F5 Networks, Inc. Legal Notices

Note: When you first power up a F5 DHD device you would normally go through the steps of licensing, provisioning and basic set-up. We have licensed, assigned the management IP, hostname, NTP and DNS servers for you. Verify DHD and Jumpbox are showing same time.

Note: If you are familiar with the BIG-IP UI, You will notice the menus on the left are consolidated. This is an indication you are working with a DDoS Hybrid defender device.

Expand each panel section to see the components available in each section.

- Dos Configuration: Where most day-to-day configuration takes place.
- Dos Setup: Where one-time or infrequent system Dos configuration is performed.
- Network: The new simplified Security Network Configuration utility to add new network topologies to the system.
- Visibility: Were the Analyst will spend a majority of the time looking at the GUI and logs.
- System: Shows a subset of the system utilities found in the traditional TMUI System menu. (Available in Advanced View on the DHD)

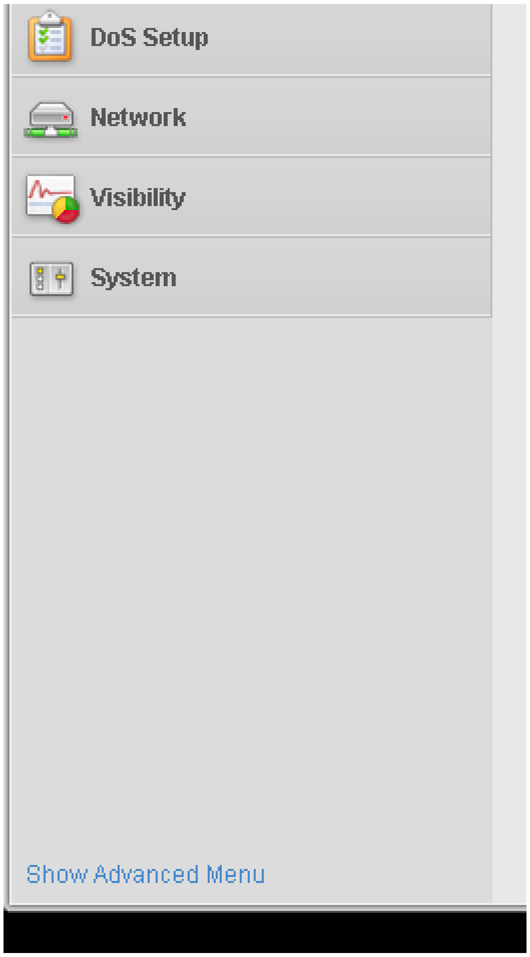


Current Resource Allocation

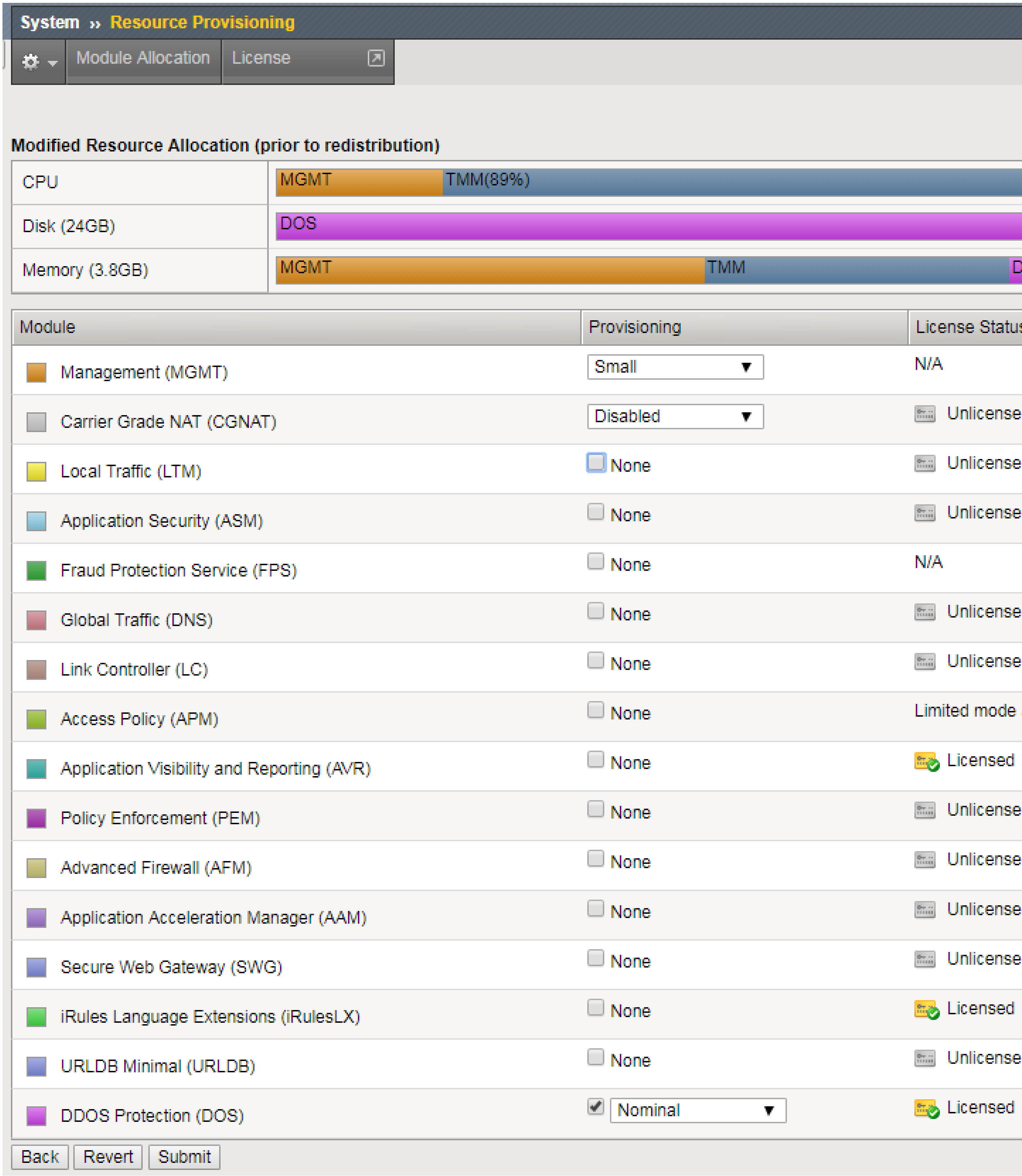
CPU	MGMT TMM(89
Disk (24GB)	MGMT
Memory (3.8GB)	MGMT

Module	F
🟧 Management (MGMT)	
▢ Carrier Grade NAT (CGNAT)	
🟨 Local Traffic (LTM)	
🟦 Application Security (ASM)	

- If you need to access more options, there is a shortcut at the bottom of the Menu page. **Show Advanced Menu**



- Explore the **Resource Provisioning** page



System ›› Resource Provisioning

Modified Resource Allocation (prior to redistribution)

CPU	MGMT TMM(89%)
Disk (24GB)	DOS
Memory (3.8GB)	MGMT TMM D

Module	Provisioning	License Statu
🟧 Management (MGMT)	Small ▼	N/A
⬜ Carrier Grade NAT (CGNAT)	Disabled ▼	Unlicense
🟨 Local Traffic (LTM)	☐ None	Unlicense
🟦 Application Security (ASM)	☐ None	Unlicense
🟩 Fraud Protection Service (FPS)	☐ None	N/A
🟥 Global Traffic (DNS)	☐ None	Unlicense
🟫 Link Controller (LC)	☐ None	Unlicense
🟩 Access Policy (APM)	☐ None	Limited mode
🟦 Application Visibility and Reporting (AVR)	☐ None	Licensed
🟪 Policy Enforcement (PEM)	☐ None	Unlicense
🟨 Advanced Firewall (AFM)	☐ None	Unlicense
🟪 Application Acceleration Manager (AAM)	☐ None	Unlicense
🟦 Secure Web Gateway (SWG)	☐ None	Unlicense
🟩 iRules Language Extensions (iRulesLX)	☐ None	Licensed
🟦 URLDB Minimal (URLDB)	☐ None	Unlicense
🟪 DDOS Protection (DOS)	☑ Nominal ▼	Licensed

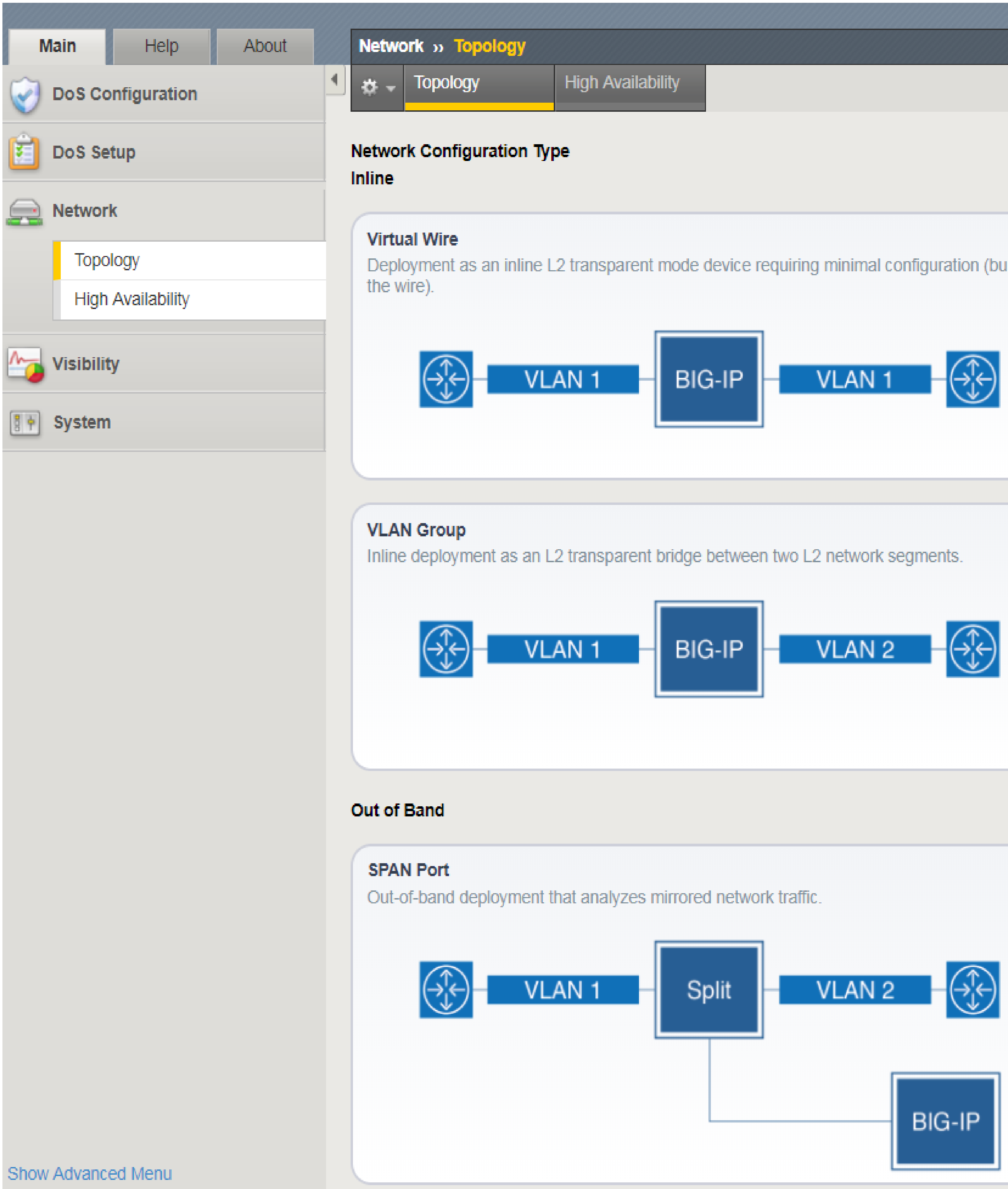
Note: The above task ensures that you are using a purpose built DDoS Hybrid Defender. If you are familiar with other F5 Modules/Technology that you have used in the past, you will notice that we have none of those provisioned.

- When done click **Submit**.

Task 2 – DDoS Hybrid Defender Base Configuration

The architecture and design decisions should have been made already. Based on F5 recommendations we are going to deploy this device in L2 Transparent Mode.

- Click **Network** in the left hand menu. Then Select **Topology**.
- Click **Create** on the upper right side.
- You will notice the various options you can select based on the prior architecture decisions.
- For this classes purpose **Click** on the VLAN Group image.



Network Configuration Type

Inline

Virtual Wire

Deployment as an inline L2 transparent mode device requiring minimal configuration (bu the wire).

VLAN Group

Inline deployment as an L2 transparent bridge between two L2 network segments.

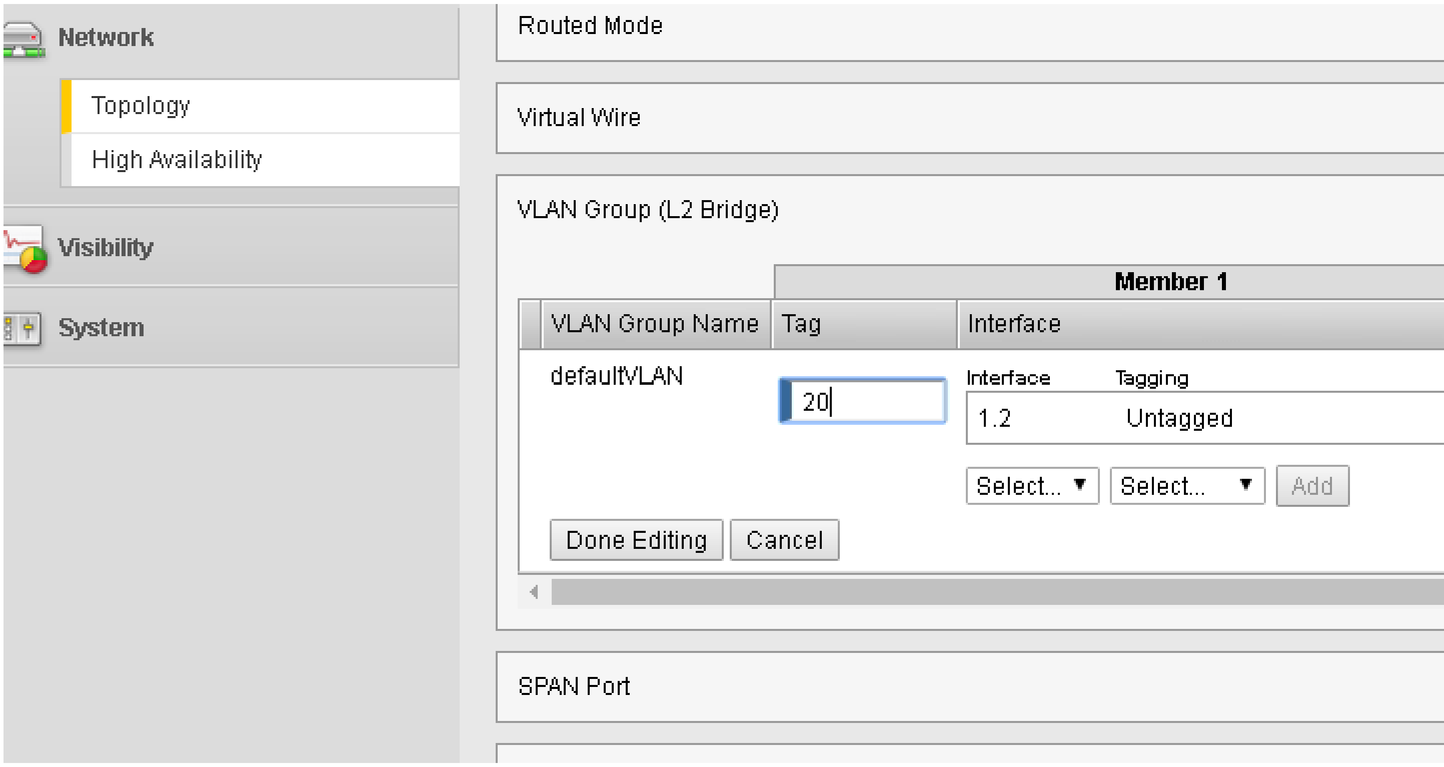
Out of Band

SPAN Port

Out-of-band deployment that analyzes mirrored network traffic.

- Fill out the information from the table below. Then Click **Done Editing** within that section.

VLAN Group Name:	defaultVlan
Internal: VLAN Tag	20
Internal: Interfaces	1.2 Untagged (Click **Add**)
External: VLAN Tag	10
External: Interfaces	1.1 Untagged (Click **Add**)



VLAN Group Name: defaultVLAN
Tag: 20
Interface: 1.2 Tagging: Untagged

- At the bottom of the page click **Finished** to create the default network.

This completes the initial Network Set-Up of DHD.

7.2.2 Lab 2 – Configuring Hybrid Defender DDoS Device Protection

Task 1 – Verify Communication Through the DHD Device.

- **PuTTY** to the **BIG-IP CLI** (10.1.1.245) from your jumpbox desktop shortcut and resize window by making it wider. You will be logged on as `root`.
- At the **config** prompt, type (or copy and paste) the following command:

```
tcpdump -i 0.0 host 10.1.20.12
```

- **PuTTY** to the **Attacker** host from your jumpbox desktop shortcut. Accept the Warning. Enter “ubuntu” as the user. It will use **a pre-loaded public key** as the credentials.
- At the **config** prompt, type (or copy and paste) the following command:

```
ping 10.1.20.12
```

- Examine the **tcpdump** window and verify ICMP packets are flowing through the BIG-IP DHD.

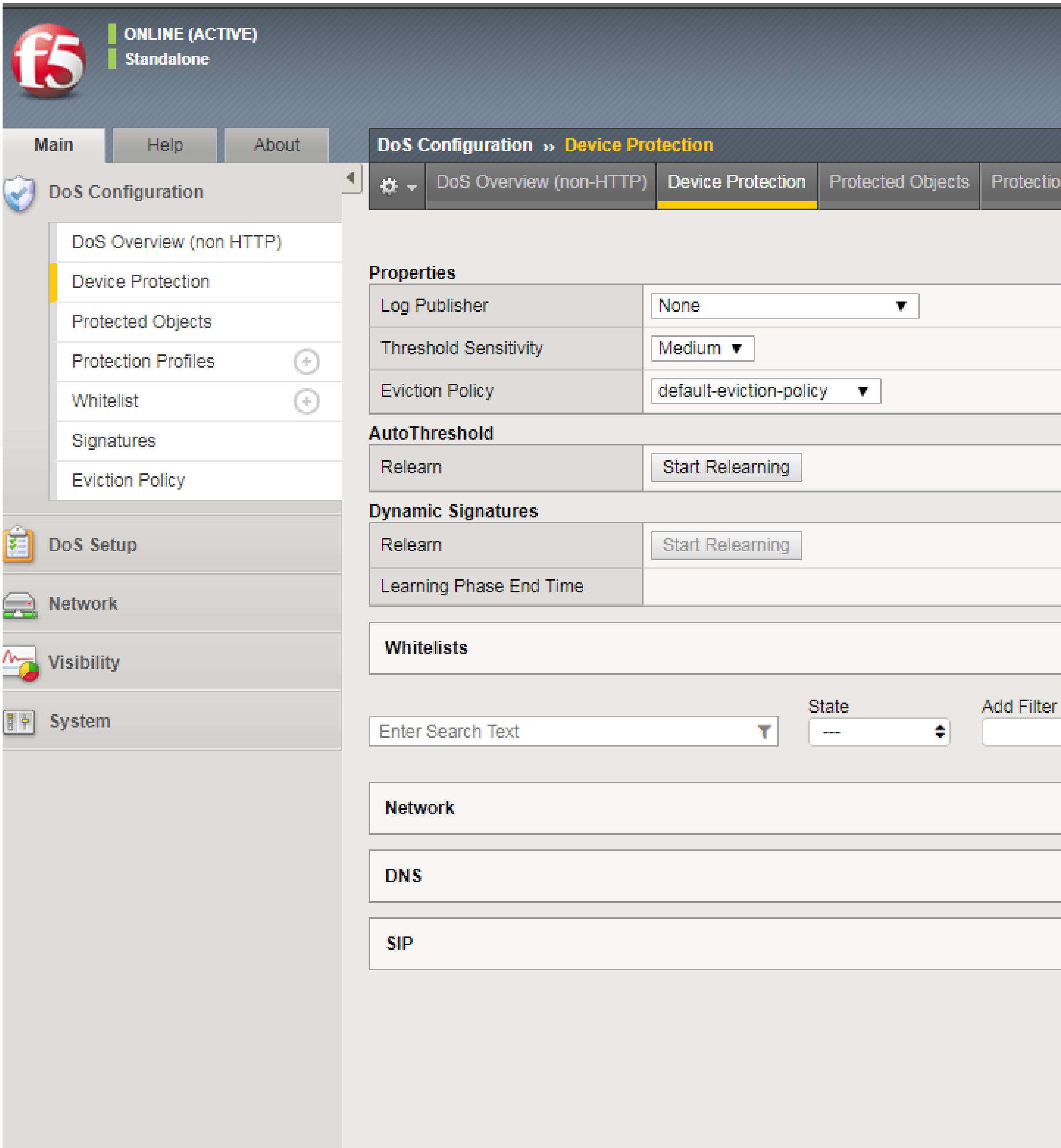
The attacker can successfully communicate with a back-end resource behind the BIG-IP DHD.

Note: The listener for the ICMP packets is the VLAN group.

- Cancel the `ping` command, then verify the `tcpdump` stops receiving ICMP packets, and then press **Enter** several times to clear the recent log entries.

Task 2 – Disable Device-Level DHD DoS Protection

- In the Configuration Utility, in the **DoS Configuration >> Device Protection** section click **Network**.



Properties

Log Publisher	None
Threshold Sensitivity	Medium
Eviction Policy	default-eviction-policy

AutoThreshold

Relearn	Start Relearning

Dynamic Signatures

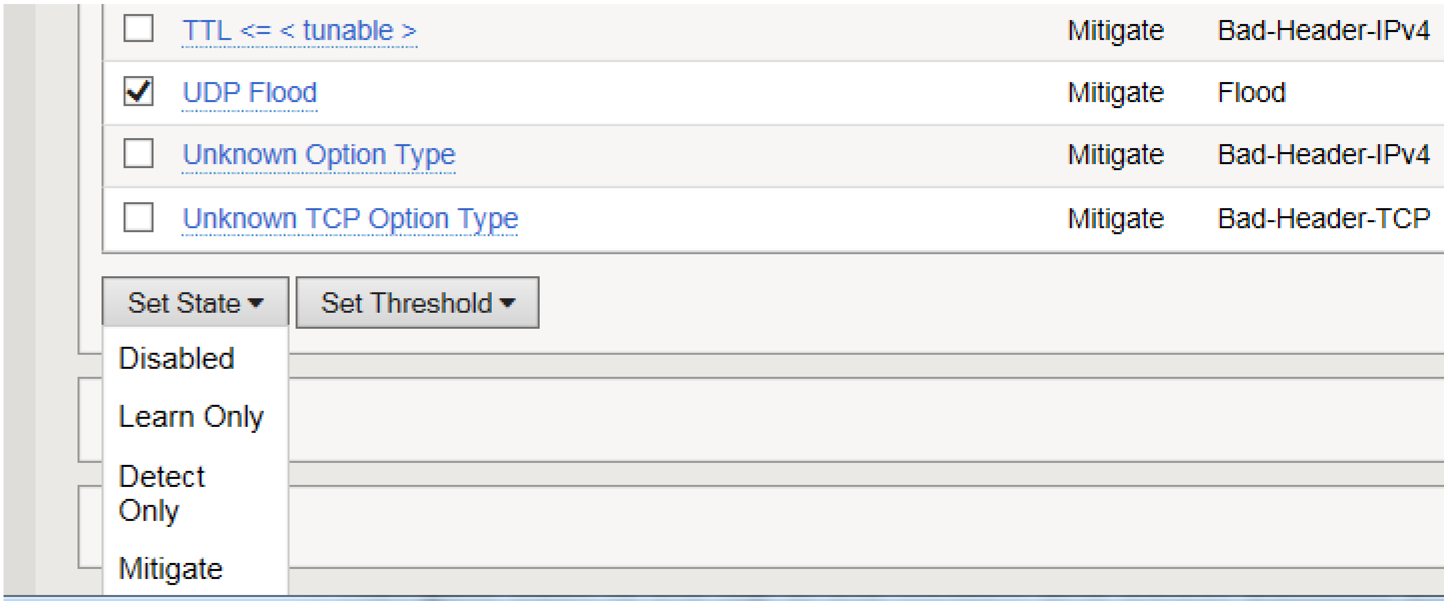
Relearn	Start Relearning
Learning Phase End Time	

State: ---

- On the left side of the page select the checkbox for **ICMPv4 flood** and **UDP Flood**.

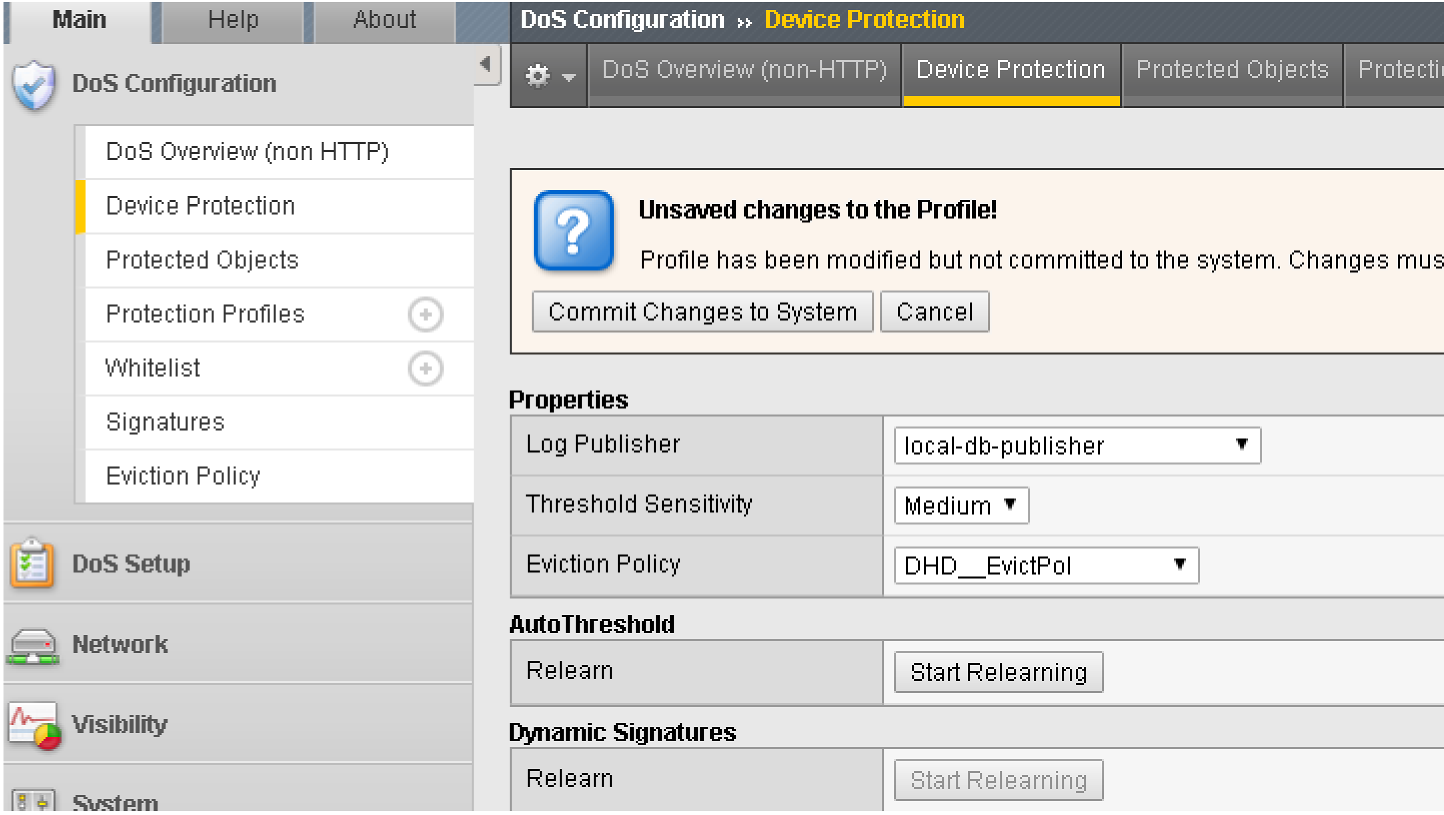
- At the bottom just below the last vector, choose the drop down **Set State** and then select **Disabled**.

Hint: This is the new method for selecting and changing multiple items at one-time. This will be how we will **Set State** and **Set Threshold**.



□	TTL <= < tunable >	Mitigate	Bad-Header-IPv4
☑	UDP Flood	Mitigate	Flood
□	Unknown Option Type	Mitigate	Bad-Header-IPv4
□	Unknown TCP Option Type	Mitigate	Bad-Header-TCP

- Navigate back to the top of the window and Select **Commit Changes to System**



Unsaved changes to the Profile!

Profile has been modified but not committed to the system. Changes mus

Properties

Log Publisher	local-db-publisher
Threshold Sensitivity	Medium
Eviction Policy	DHD__EvictPol

AutoThreshold

Relearn

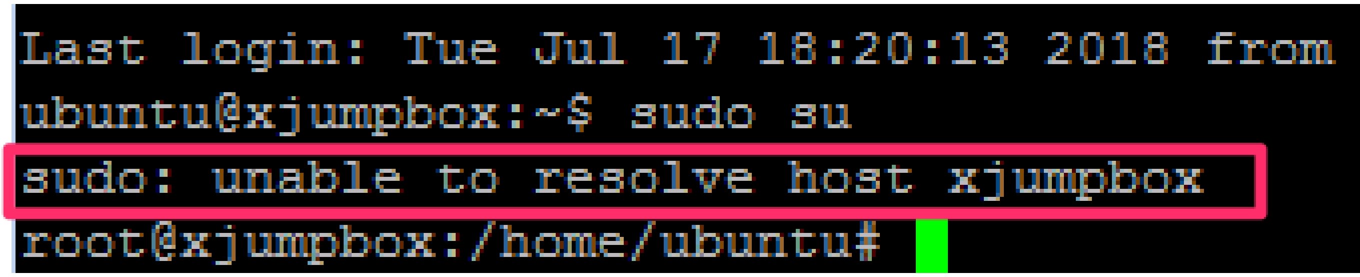
Dynamic Signatures

Relearn

- On the Jumpbox in the **Attacker** PuTTY window type (or copy and paste) the following:

```
# sudo su
# cd scripts
# ls
```

Note: Ignore the “sudo: unable to resolve host” error.



```
Last login: Tue Jul 17 18:20:13 2018 from
ubuntu@xjumpbox:~$ sudo su
sudo: unable to resolve host xjumpbox
root@xjumpbox:/home/ubuntu#
```

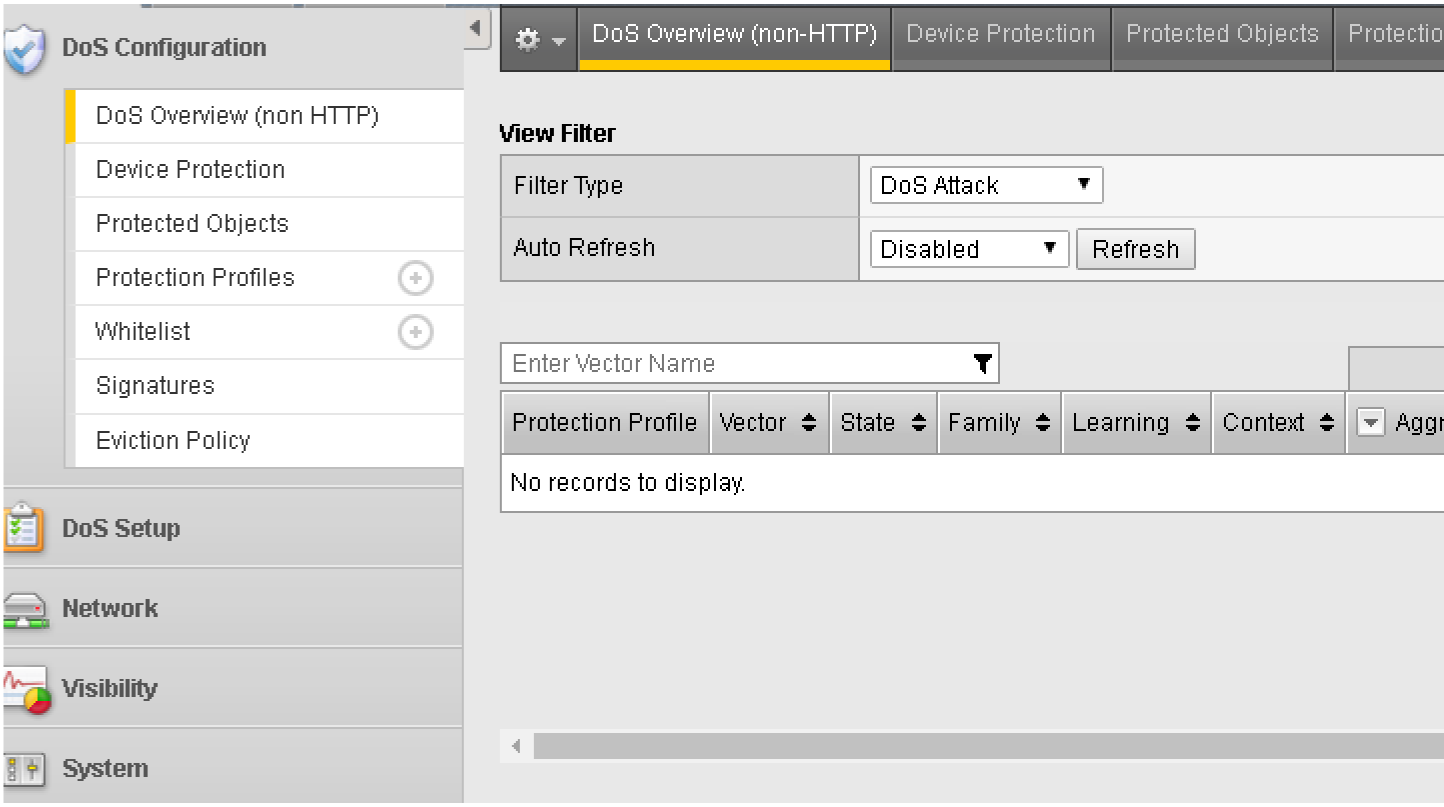
These are some of the different scripts we’ll be using during the exercises to simulate DoS attacks.

- Type (or copy and paste) the following command:

  ```
  for i in {1..10}; do ./icmpflood.sh; done
  ```

This script launches the Attack and then repeats for a total of ten occurrences.

- View the `tcpdump` window and verify that ICMP attack traffic is reaching the back-end server.
- Let the attack run for about 15 seconds before moving on.
- In the Configuration Utility, open the **DoS Configuration** >> **DoS Overview (non HTTP)** page.
- Make sure the Filter Type is “Dos Attack”.
- View the Protection Profile column in the display and notice no results are returned, you disabled those vectors.

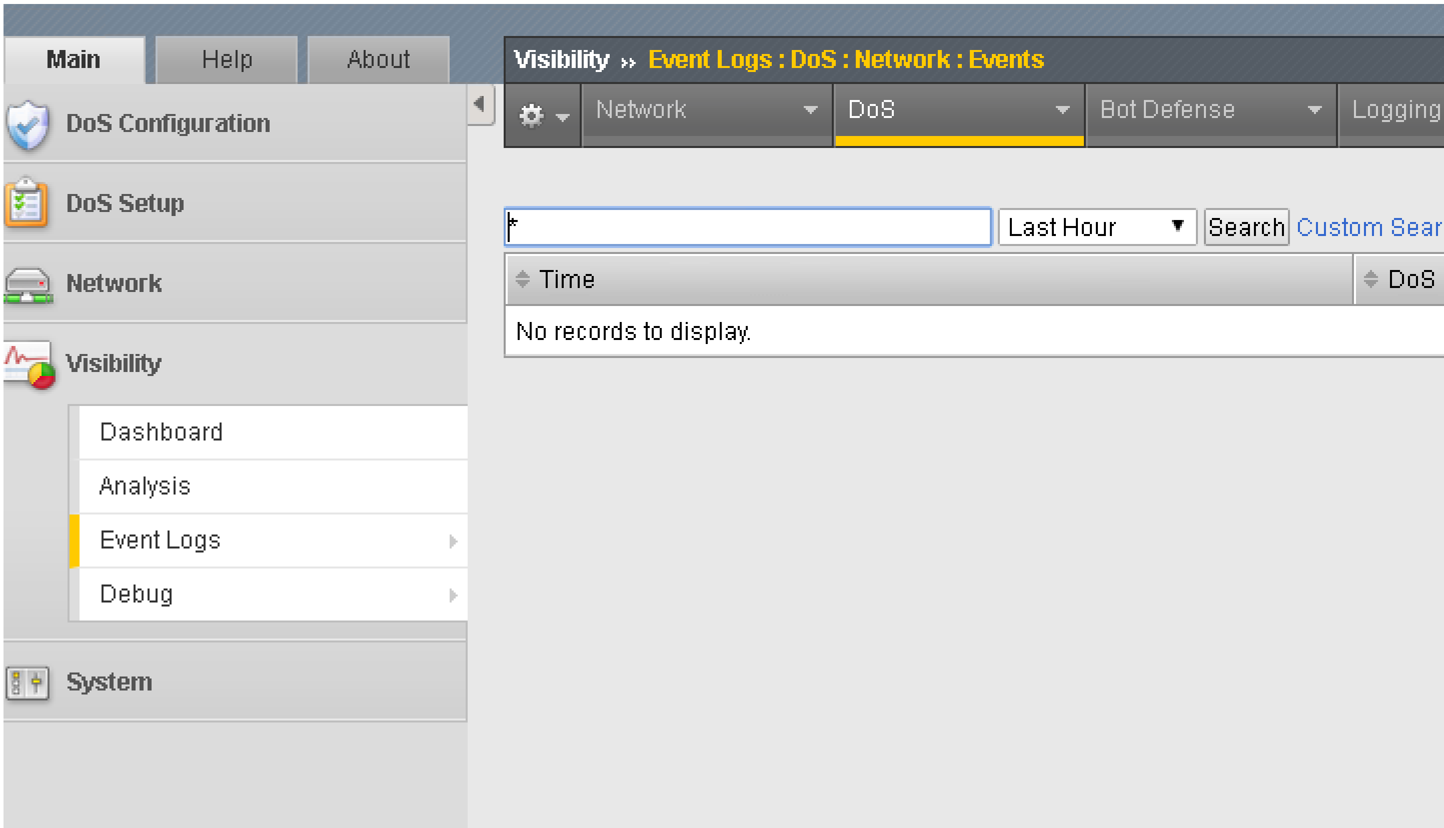


View Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

Protection Profile	Vector	State	Family	Learning	Context	Aggr
No records to display.						

- Navigate to **Visibility** >> **Event Logs** >> **DoS** >> **Network** >> **Events**.



No records to display.

- Go back to the **Attacker** and stop the script. CTRL+C (This needs to be hit several times to break out of the script)

- Notice no logs are captured. We could have chosen **Learn Only** or **Detect Only** and had different results. If you want to test, feel free.

Note: If you want to run the other attacks, use the format above. ./synflood.sh and udp_flood.sh behave similar. If you are not seeing the traffic on the DHD CLI, Stop and Re-Start the tcpdump.

Both of these locations we will return to throughout this course to see how our DHD is viewing these attacks.

Task 3 – Re-enable Device-Level DHD DoS Protection

In this task you will re-configure **device-level** DoS protection and then issue the same command and review the results.

- In the Configuration Utility, in the **DoS Configuration >> Device Protection** under Log Publisher select “local-db-publisher”.
- Next click the **Network** section.
- On the left side of the page select the checkbox for **ICMPv4 flood** and **UDP Flood**.
- At the bottom just below the last vector, chose the drop down **Set State** and then select **Mitigate**.

Note: You have the option of Learn Only and Detect Only as well.

- Navigate back to the top of the window and Select **Commit Changes to System**

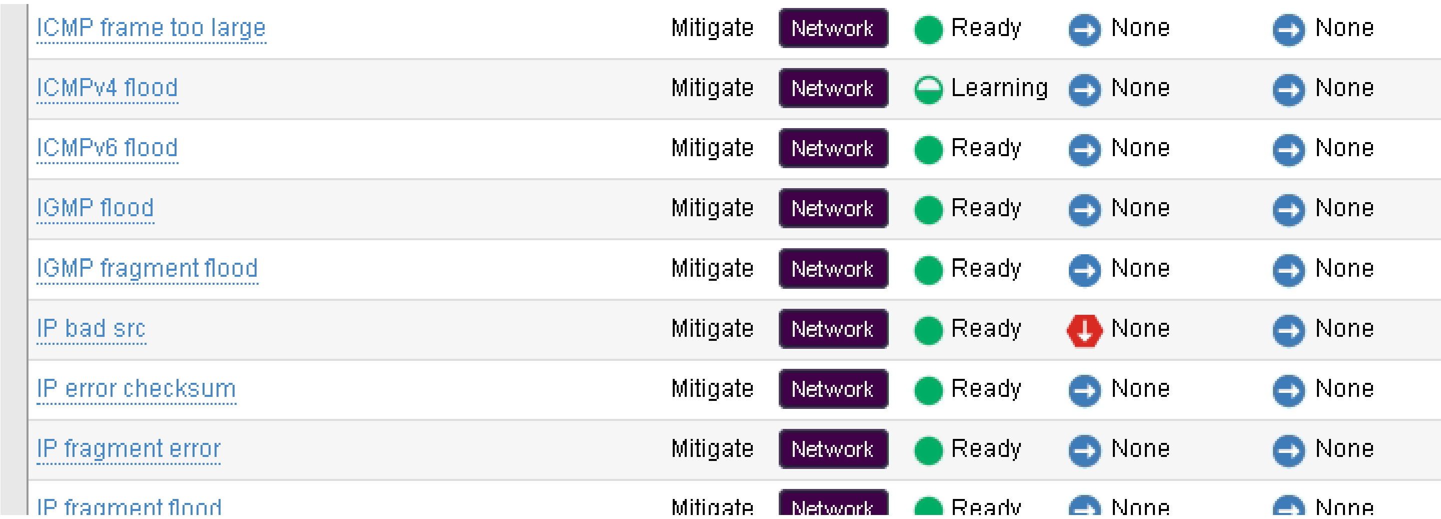
Note: This returns the configuration back to factory supplied device level enforcement.

Task 4 – Attack the DDoS Hybrid Defender again and see what you can tell.

- Type (or copy and paste) the following command:

```
for i in {1..10}; do ./icmpflood.sh; done
```

- In the Configuration Utility, open the **DoS Configuration** >> **DoS Overview (non HTTP)** page.
- Make sure the Filter Type is "Device Dos".
- This page will show the preset vectors for the Device and the Current **Attack Status**, **Average EPS**, **Current Dropped EPS** and the **Detection Thresholds** including the **Threshold Mode**.
- Scroll down until you see ICMPv4 Flood.



ICMP frame too large	Mitigate	Network	● Ready	➡ None	➡ None
ICMPv4 flood	Mitigate	Network	◓ Learning	➡ None	➡ None
ICMPv6 flood	Mitigate	Network	● Ready	➡ None	➡ None
IGMP flood	Mitigate	Network	● Ready	➡ None	➡ None
IGMP fragment flood	Mitigate	Network	● Ready	➡ None	➡ None
IP bad src	Mitigate	Network	● Ready	⬇ None	➡ None
IP error checksum	Mitigate	Network	● Ready	➡ None	➡ None
IP fragment error	Mitigate	Network	● Ready	➡ None	➡ None
IP fragment flood	Mitigate	Network	● Ready	➡ None	➡ None

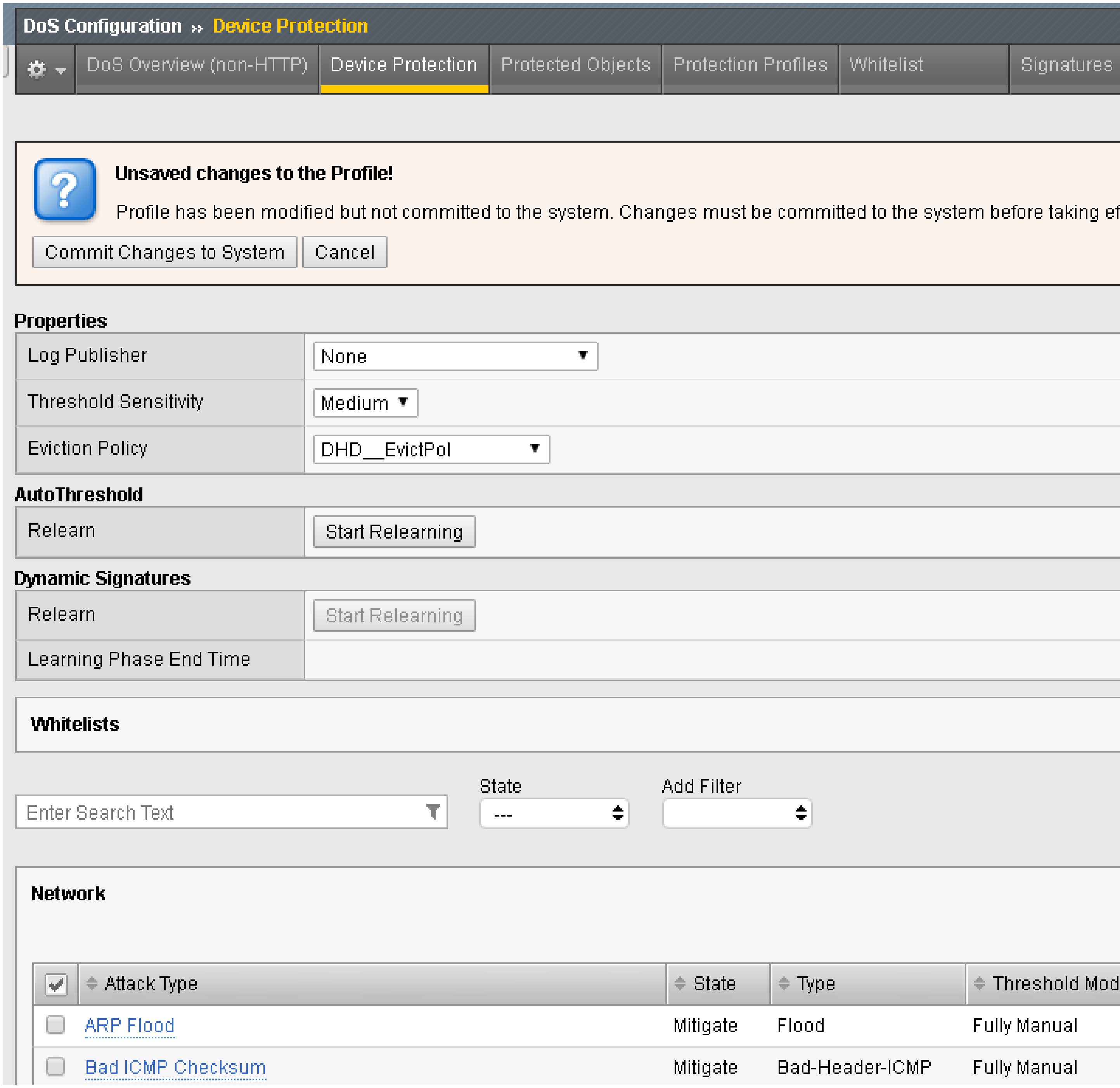
Attention: Why is the DHD not dropping packets?

Hint: Look at the Manual Thresholds set and the current rate of packets. We are not generating enough traffic.

- We need to set a lower threshold Manually.
- In the Configuration Utility, open the **DoS Configuration** >> **Device Protection** page. Scroll down in the **Network** section to ICMPv4 flood. **Click** ICMPv4 flood.

Note: The new fly out page.

- Manually Set The Detection Threshold PPS to 100 and the Mitigation Threshold EPS to 500. Scroll up and **Commit Changes to System**



Unsaved changes to the Profile!

Profile has been modified but not committed to the system. Changes must be committed to the system before taking ef

Properties

Log Publisher	None
Threshold Sensitivity	Medium
Eviction Policy	DHD__EvictPol

AutoThreshold

Relearn	Start Relearning

Dynamic Signatures

Relearn	Start Relearning
Learning Phase End Time	

Whitelists

State: ---

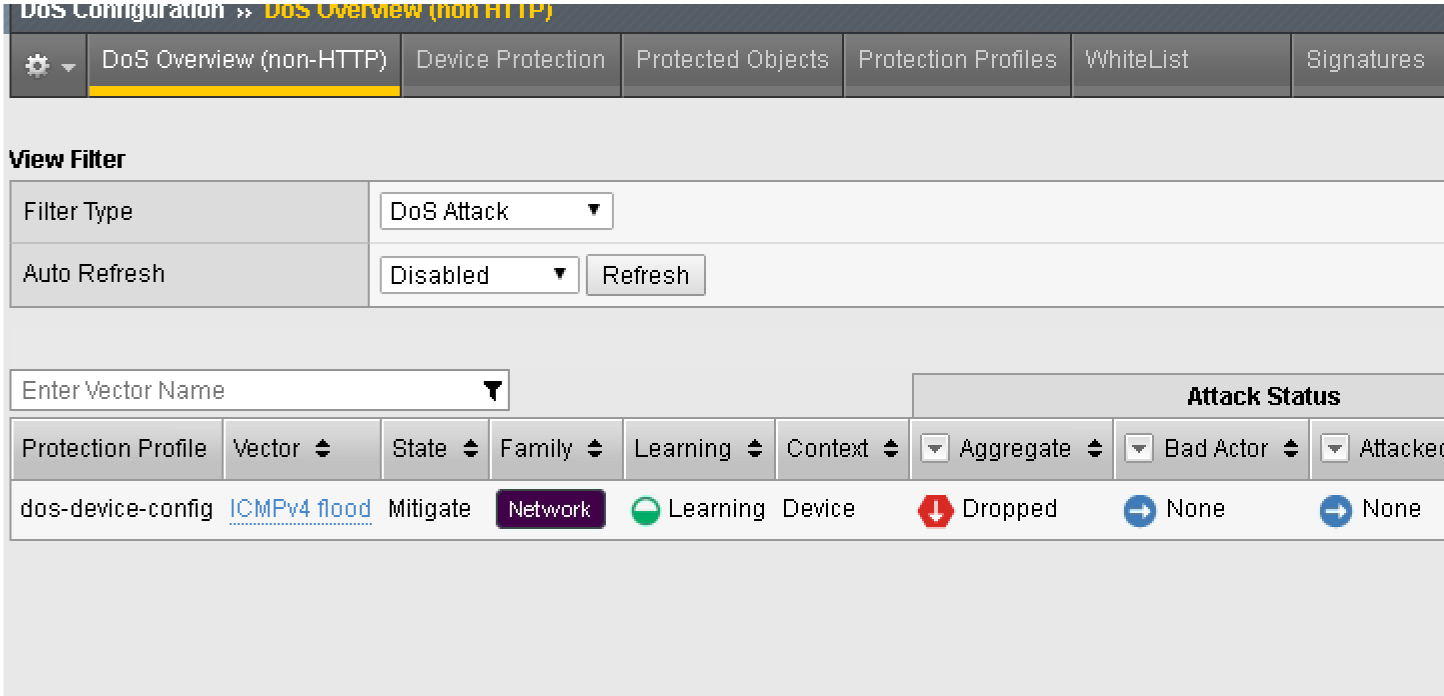
Add Filter:

Network

☑	Attack Type	State	Type	Threshold Mod
□	ARP Flood	Mitigate	Flood	Fully Manual
□	Bad ICMP Checksum	Mitigate	Bad-Header-ICMP	Fully Manual

- Relaunch the Attack from the Attacker CLI.

- In the Configuration Utility, open the **DoS Configuration >> DoS Overview (non HTTP)** page.
- Make sure the Filter Type is “Dos Attack”. See the Dropped traffic with the new thresholds. Alternatively, you can go “Device DoS”, scroll down to ICMPv4 Flood and see the same information.”



DoS Configuration » DoS Overview (non HTTP)

View Filter

Filter Type	DoS Attack ▼
Auto Refresh	Disabled ▼ Refresh

Enter Vector Name

						Attack Status		
Protection Profile	Vector ⬍	State ⬍	Family ⬍	Learning ⬍	Context ⬍	Aggregate ⬍	Bad Actor ⬍	Attacked
dos-device-config	ICMPv4 flood	Mitigate	Network	Learning	Device	Dropped	None	None

- Look at the Protection Profile: dos-device, attack status and various rates.

- You can terminate the Attack with Ctrl+C when finished.

This concludes this section where we looked at setting manual thresholds to mitigate attacks that might not have been mitigated with the default settings.

Note: We did this to only one vector. These same procedure can be applied to all the vectors or selected vectors, depending on your environment.

7.3 DDoS Hybrid Defender Attacks and Mitigations

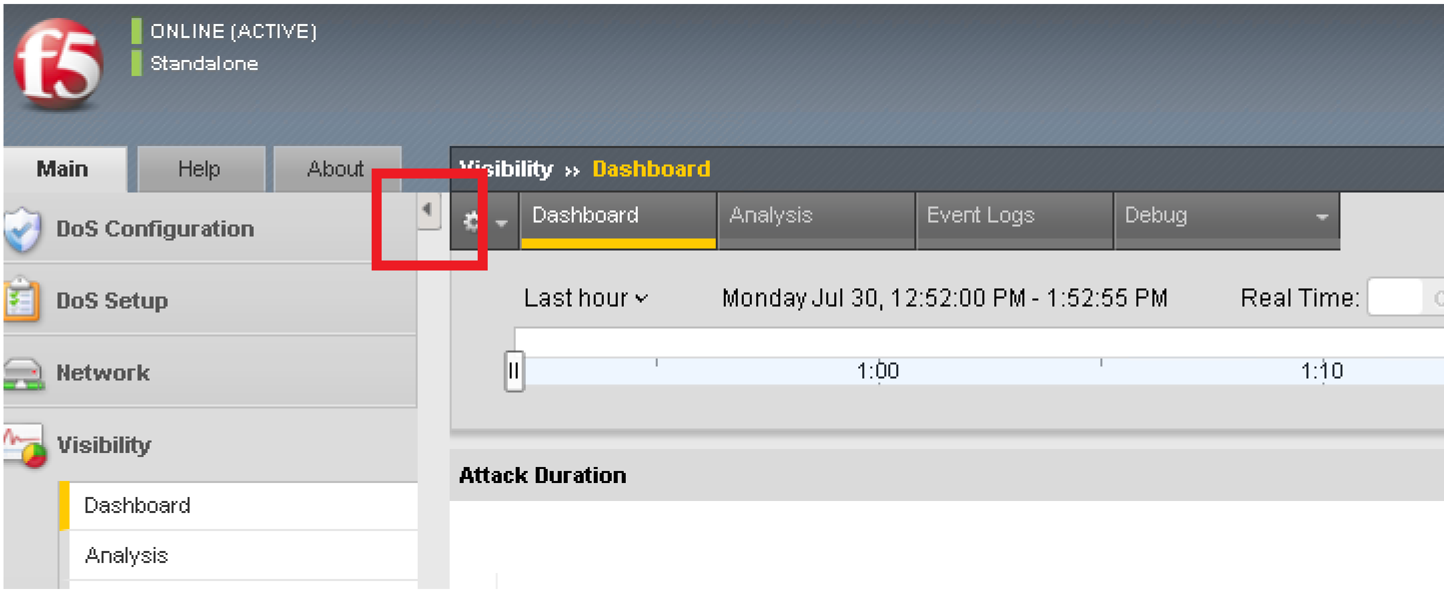
In this module you will create Protected Objects, Set Mitigation Thresholds Manually, and then launch various attacks against the F5 Networks DDoS Hybrid Defender and view the results in the GUI and logs. Then you will allow the DDoS Hybrid Defender to Automatically detect and set Threshold for detection and mitigation, easing the burden on Administartors. Finally, time permitting, we will explore Behavioral mitigations. (Covered in Detail in the Advanced class)

7.3.1 Lab 1 – Quick GUI Overview of the Visibility and Reporting Available

Task 1 – View the New Visibility Page

You can now use the new DHD Visibility page to view the Dashboard, Analysis, Event Logs and Debugging info.

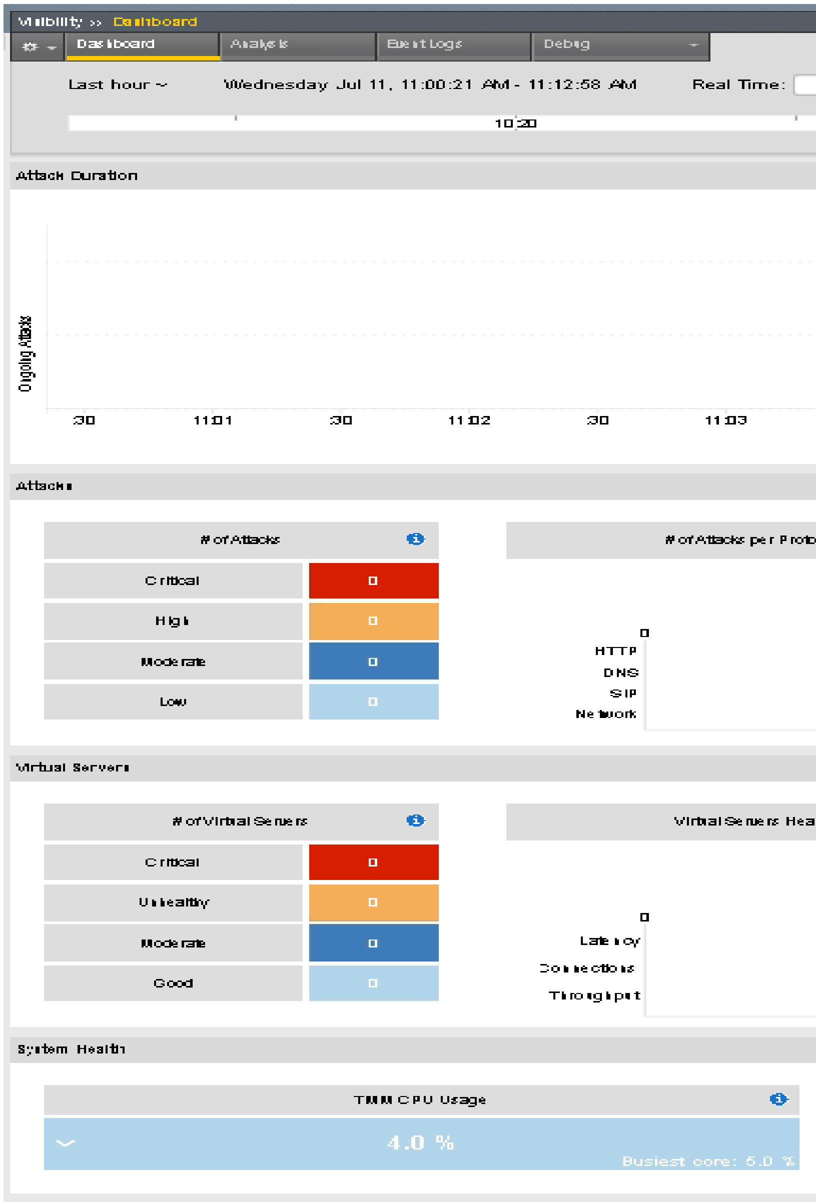
- Take advantage of the expandable window feature to give more screen space to the GUI.



- In the Hybrid Defender Web UI, go to the Visibility >> Dashboard overview.

Note: DoS Visibility Dashboard defaults to not Auto-Refresh. Click the Button to set **Real-Time** to **ON**.

- You should see categories as: Attack Duration, Attacks, Virtual Severs, System Health and Countries.

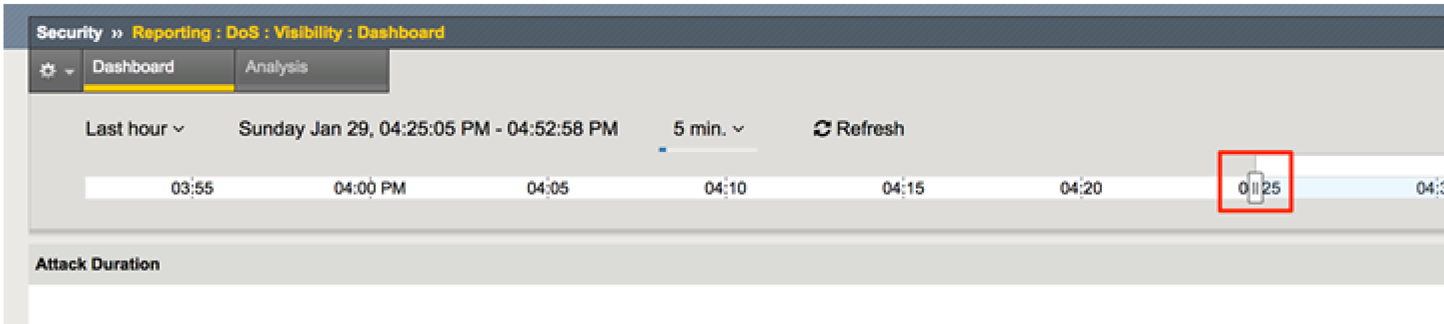


# of Attacks	
Critical	0
High	0
Moderate	0
Low	0

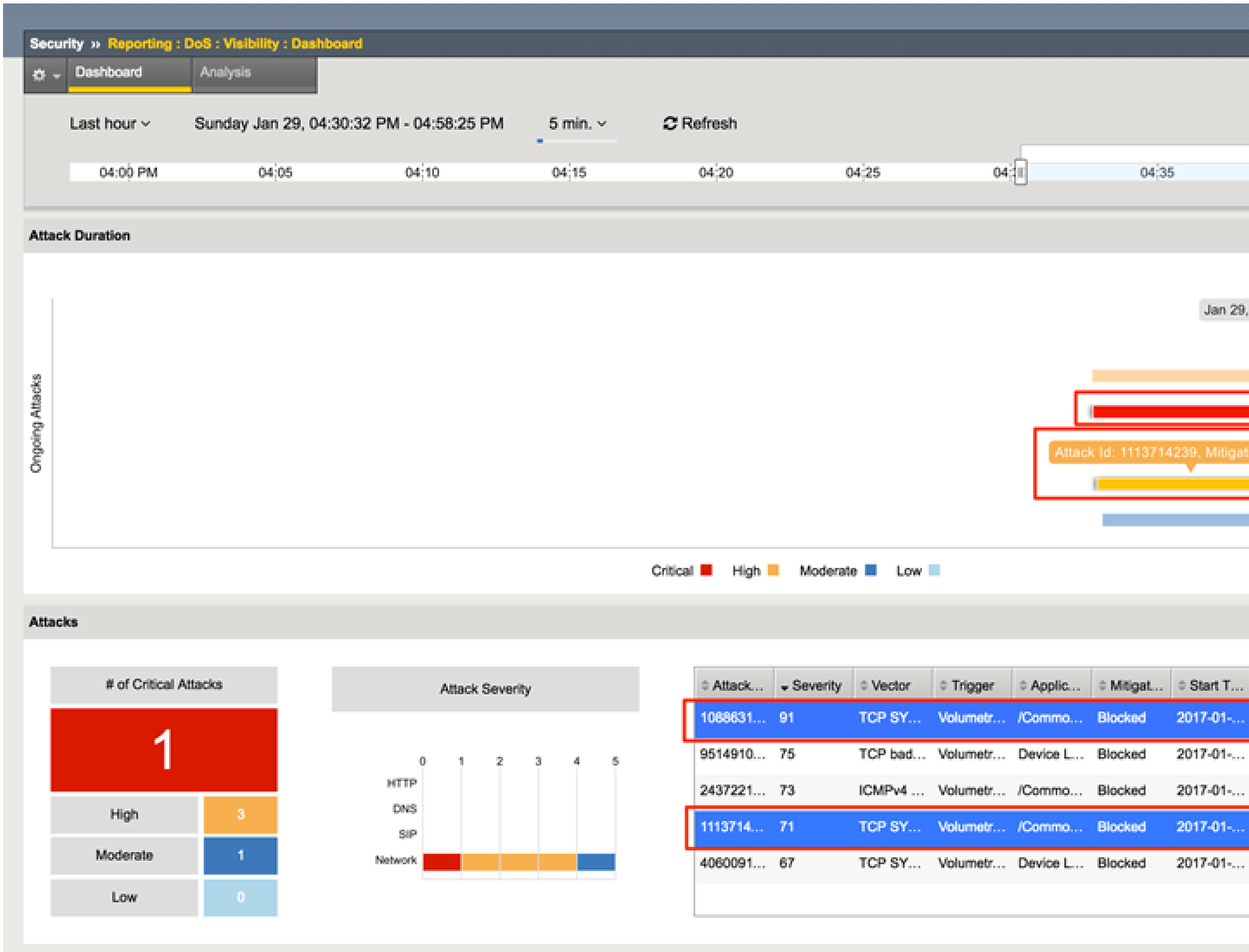
# of Virtual Servers	
Critical	0
Unhealthy	0
Moderate	0
Good	0

Scroll through the Left Pane and explore the windows.

- You can use the slider to shorten the time frame, or filter on the protocol, if desired when viewing attacks if needed.



- Later when we have data and attacks, you will see the different attacks in the **Attack Duration** window. You will be able to hover over for more details.



Attack...	Severity	Vector	Trigger	Applic...	Mitigat...	Start T...
1088631...	91	TCP SY...	Volumetr...	/Commo...	Blocked	2017-01-...
9514910...	75	TCP bad...	Volumetr...	Device L...	Blocked	2017-01-...
2437221...	73	ICMPv4 ...	Volumetr...	/Commo...	Blocked	2017-01-...
1113714...	71	TCP SY...	Volumetr...	/Commo...	Blocked	2017-01-...
4060091...	67	TCP SY...	Volumetr...	Device L...	Blocked	2017-01-...

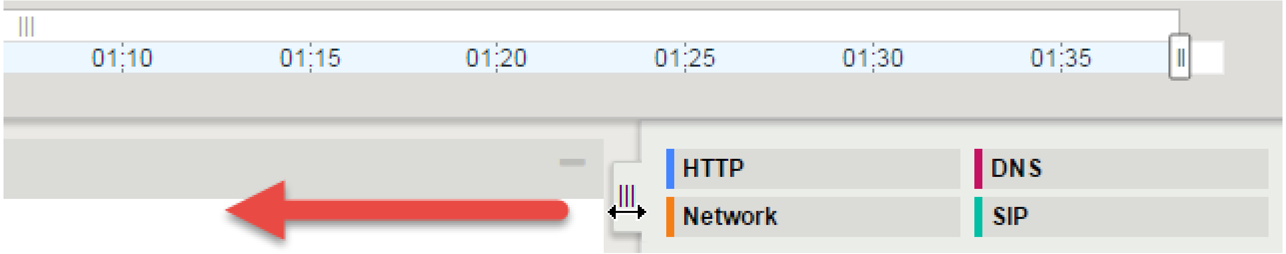
- Scroll down in the left-side of the page to view the **Attacks** section.
- View the details at the bottom of the **Attacks** section.

This table displays details of each attack that has occurred.

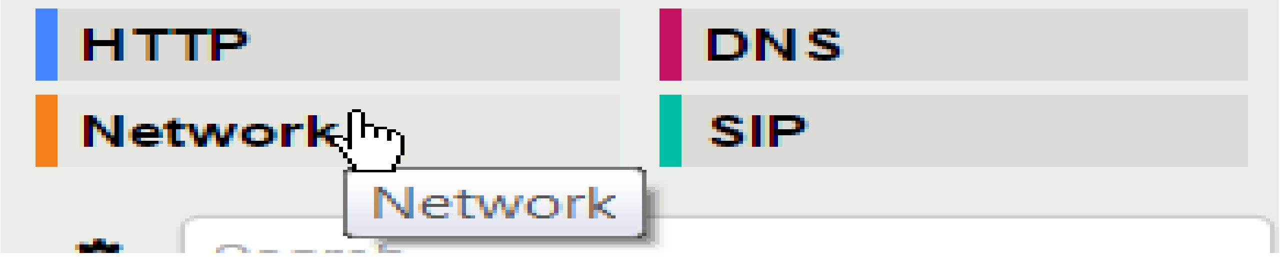
- Examples are; Attack ID, Severity, Vector, Trigger Virtual Server, Start Time, Stop Time. . . etc
- Scroll down in the left-side of the page to view the **Virtual Servers** section.
- You can see the details of **protected object**-level attacks.
- Examples are; Virtual Server, Server Latency, Health, Current Connections, Blocked IP's. . . etc
- Scroll down to the **System Health** section. This table displays the current health of the system.
- Scroll down to the **Countries** section. This table displays the attack details from each country.

Now focus on the Right Panel.

- View the various widgets in the panel on the right-side of the page. The top can be expanded and contracted visa the slider bar.



- Click **Network** to filter out only the network-level attacks (all the attacks so far have been network-level).



- If it's not already expanded, expand the **Virtual Servers** widget, and then select /**Common**/**Server**.
- This filters the results to only attacks at this protected object-level. Notice the changes to the map on in the **Countries** section.
- Continue to Explore and Scroll down the right side. Notice each widget supplies greater detail.

7.3.2 Lab 2 - Multi-vector Attack Demo

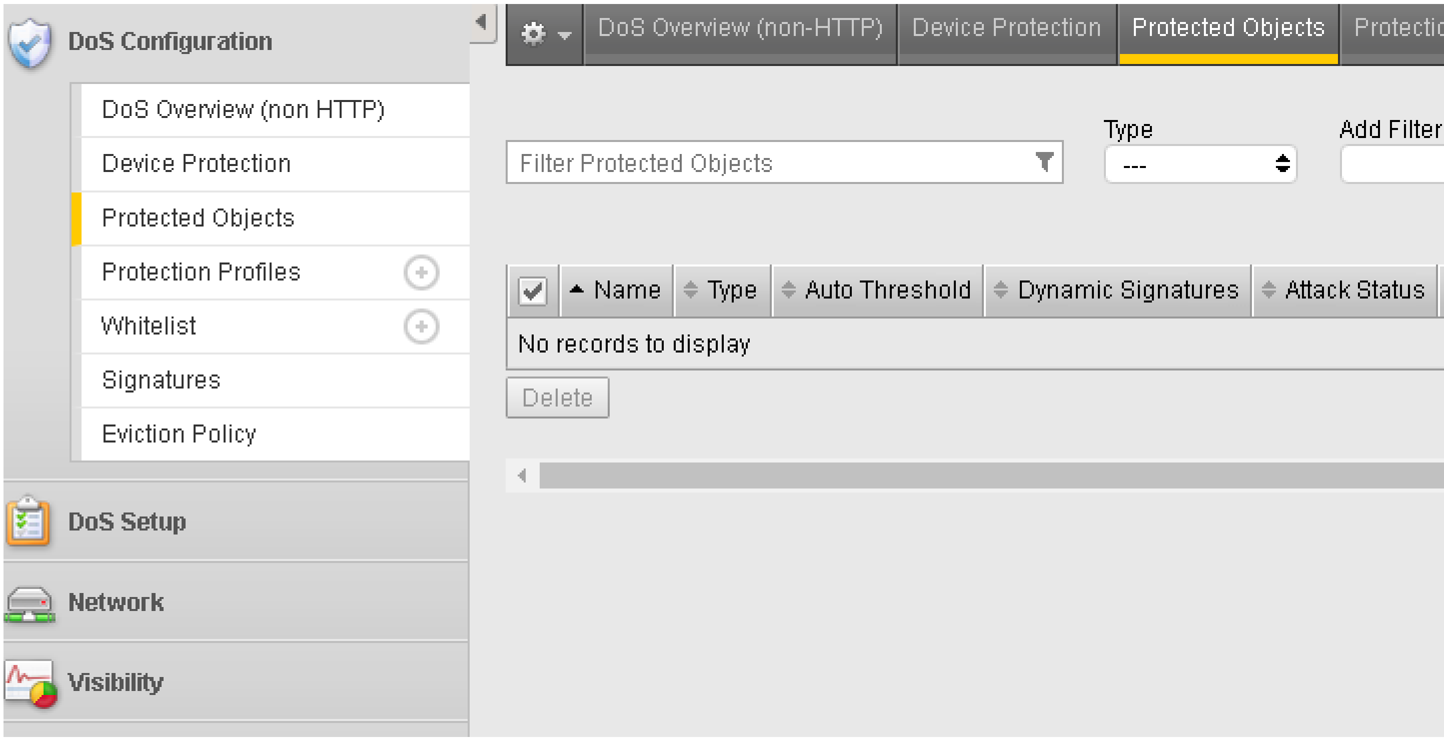
In this simple demo you will launch a small number of network attacks and show the configuration, logging and reporting capabilities of the F5® DDoS Hybrid Defender™. The point of this demo is to provide context for a UI walk-through with more live data and viewing and setting manual thresholds.

Task 1 – Create a Protected Object that the Attacker will be targeting

The DHD device wide protection is enforced for all traffic flowing through the device. For more granular control, we use **Protected Objects** and configure mitigation settings for those objects to be enforced.

In this task you will configure **Object-Level** DoS protection for a network (L4), simulating your Server Network and then issue an attack and review the results.

- In the BIG-IP Configuration Utility, open the **DoS Configuration >> Protected Objects** page and in the **Protected Objects** section click the **Create** dropdown and select **Protected Object**.



No records to display

- Configure the Protected Object using the following information, and then click **Create**.

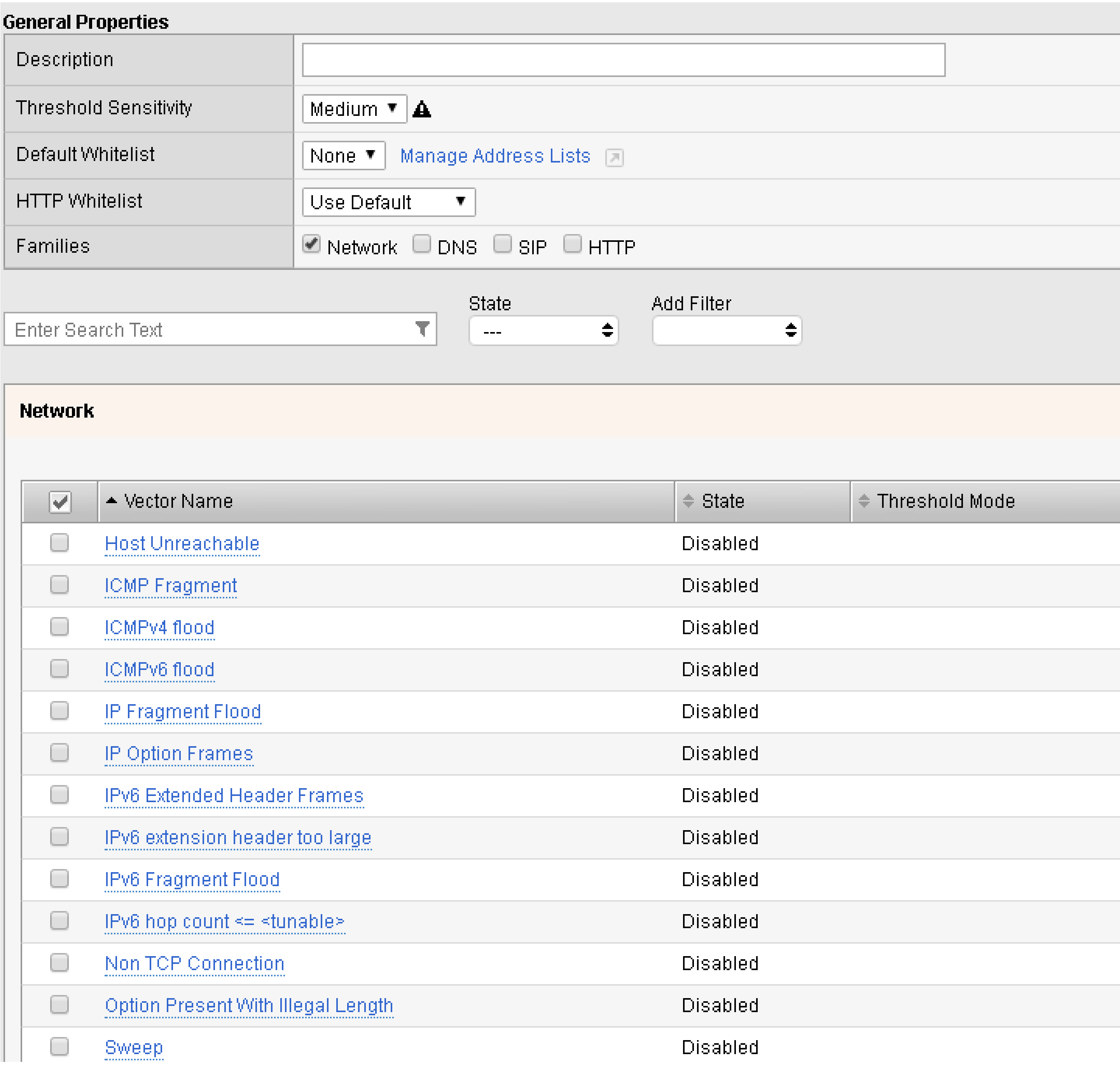
Name	ServerNet
Destination Address	10.1.20.0/24
Port	*All Ports
Protocol	All Protocols
Protection Profile:	dos
Eviction Policy:	Leave Blank
VLAN(s):	defaultVLAN
Logging Profiles:	local-dos

- Click **Save**

This protected object is defending all ports/protocols for 10.1.20.0/24, which is the network behind the Hybrid Defender. Attacks will be launched at 10.1.20.12, which is an interface on the LAMP server.

In the default **dos** profile no sections are selected or enabled for protected objects in the default configuration.

- In the BIG-IP Configuration Utility, open the **DoS Configuration >> Protection Profiles** page. **Click** dos, Then Check the **Network** box under the Families Heading.
- Click the Network Section. Notice all vectors are disabled. Check the top box to select all the vectors, Scroll to the bottom and Select **Mitigate**. Scroll to the top and **Commit Changes to System**.



General Properties

Description	
Threshold Sensitivity	Medium ▼ ⚠
Default Whitelist	None ▼ Manage Address Lists
HTTP Whitelist	Use Default ▼
Families	☑ Network □ DNS □ SIP □ HTTP

Enter Search Text | State: --- | Add Filter:

Network

☑	Vector Name	State	Threshold Mode
□	Host Unreachable	Disabled	
□	ICMP Fragment	Disabled	
□	ICMPv4 flood	Disabled	
□	ICMPv6 flood	Disabled	
□	IP Fragment Flood	Disabled	
□	IP Option Frames	Disabled	
□	IPv6 Extended Header Frames	Disabled	
□	IPv6 extension header too large	Disabled	
□	IPv6 Fragment Flood	Disabled	
□	IPv6 hop count <= <tunable>	Disabled	
□	Non TCP Connection	Disabled	
□	Option Present With Illegal Length	Disabled	
□	Sweep	Disabled	

- Navigate to **DoS Configuration >> Device Protection**. Under Log Publisher select “local-db-publisher” from the drop down. Select **Commit Changes to System**. This publishes our logs to the appropriate location for analysis.

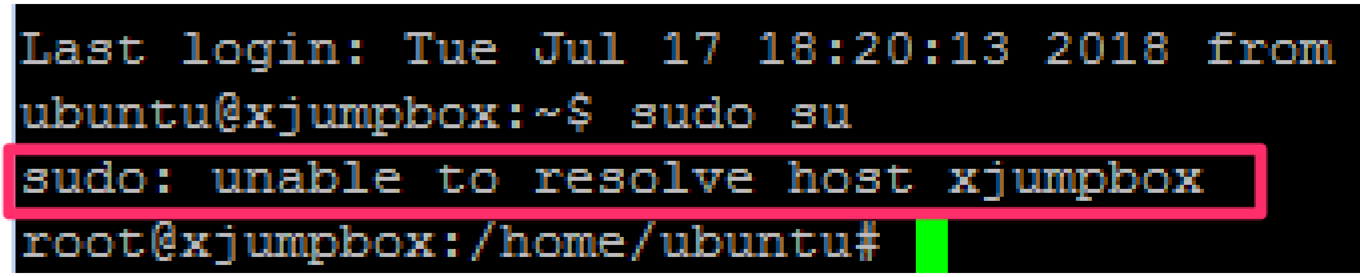
You will now launch the attacks and show the behavior

- Open the following tabs in the DHD UI (Duplicate Tabs to make it easier):
- **DoS Configuration >> DoS Overview >> Filter Type >> Try Both DoS Attack and Device Dos**
- **Visibility >> Dashboard** change Dashboard to **Real Time** which is centered on the timeline.
- **Visibility >> Event Logs >> DoS >> Network >> Events**

- Access the **Attacker** shell and run the following commands/attack (if already in the folder just issue the command)

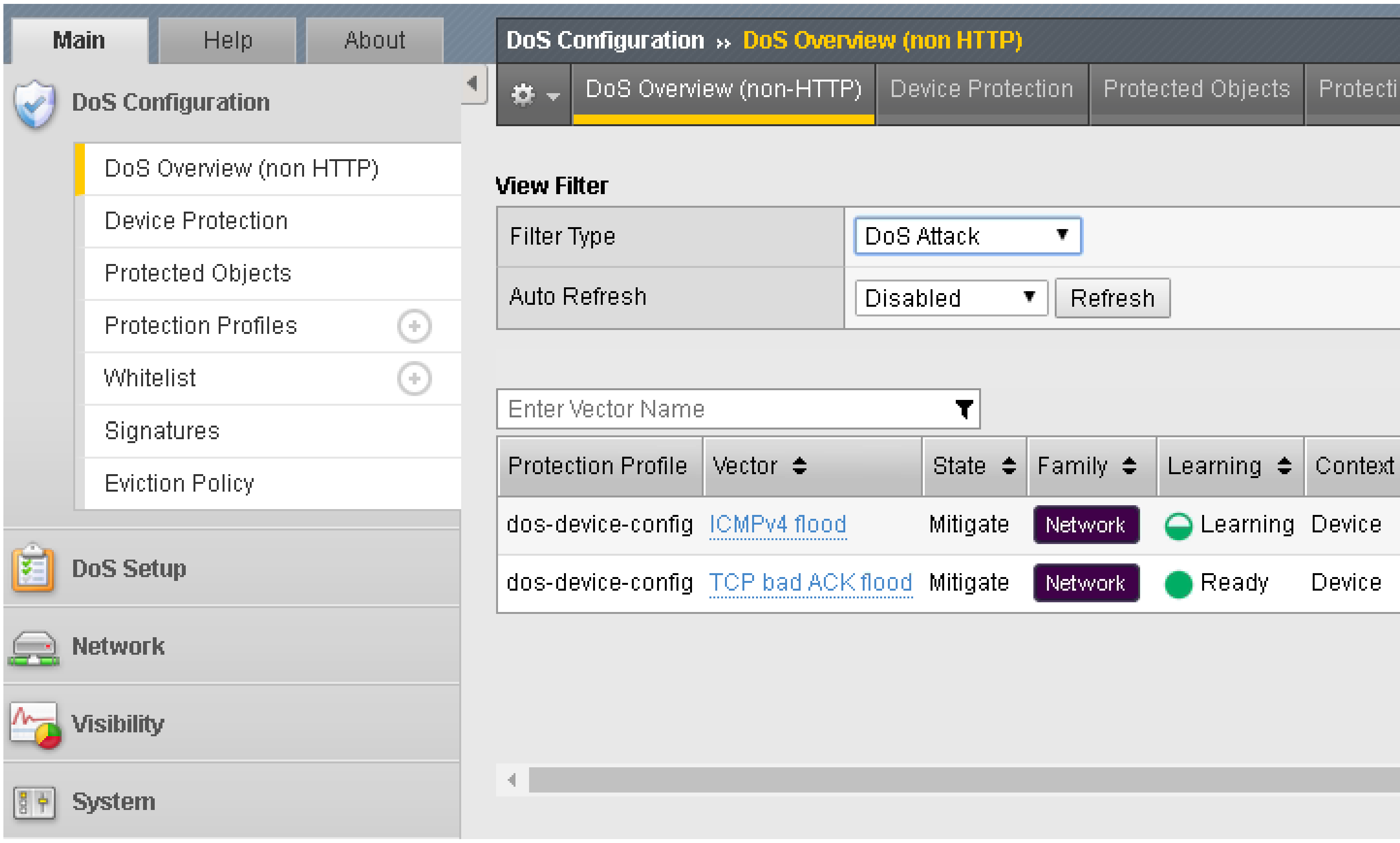
```
# sudo su
# cd ~/scripts
# ./multivector.sh
```

Note: Ignore the “sudo: unable to resolve host” error.



```
Last login: Tue Jul 17 18:20:13 2018 from
ubuntu@xjumpbox:~$ sudo su
sudo: unable to resolve host xjumpbox
root@xjumpbox:/home/ubuntu#
```

- Click **Refresh** on the DoS Overview page. Look at and explore both **DoS Attack** and **Device Dos** filters to refine your results.

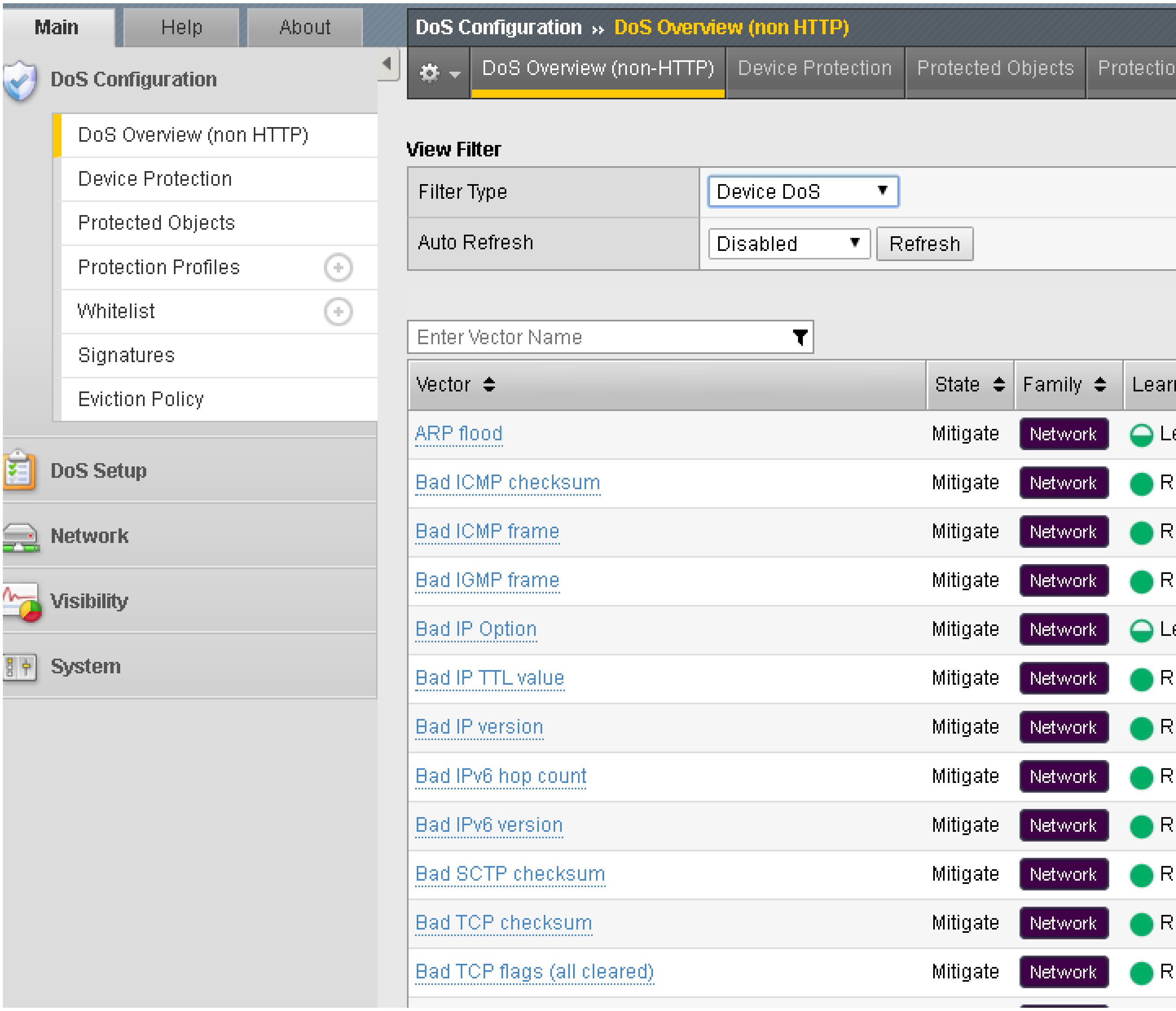


View Filter

Filter Type	DoS Attack
Auto Refresh	Disabled Refresh

Enter Vector Name

Protection Profile	Vector	State	Family	Learning	Context
dos-device-config	ICMPv4 flood	Mitigate	Network	Learning	Device
dos-device-config	TCP bad ACK flood	Mitigate	Network	● Ready	Device



View Filter

Filter Type	Device DoS
Auto Refresh	Disabled

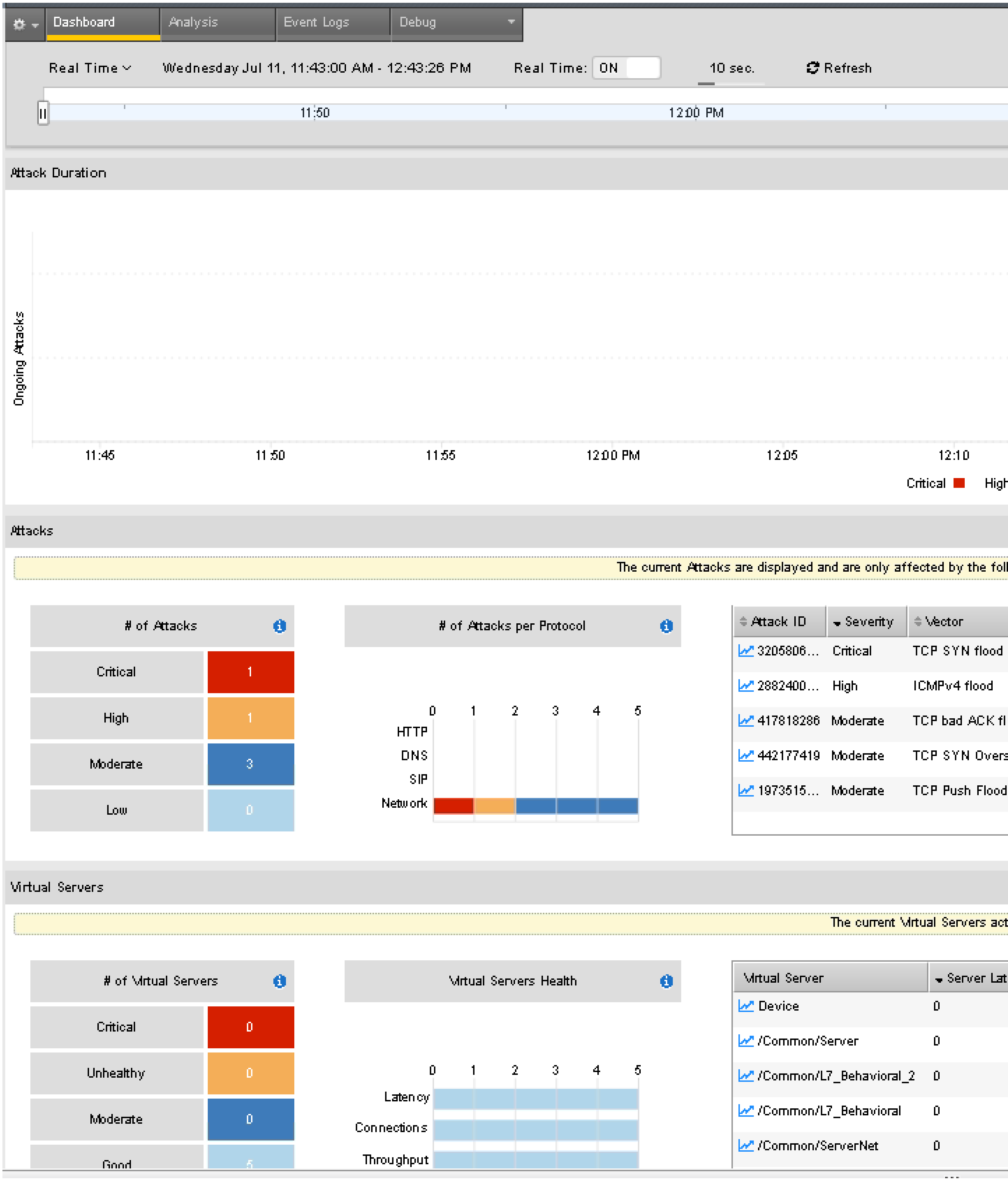
Vector	State	Family	Lear
ARP flood	Mitigate	Network	◒ Le
Bad ICMP checksum	Mitigate	Network	● R
Bad ICMP frame	Mitigate	Network	● R
Bad IGMP frame	Mitigate	Network	● R
Bad IP Option	Mitigate	Network	◒ Le
Bad IP TTL value	Mitigate	Network	● R
Bad IP version	Mitigate	Network	● R
Bad IPv6 hop count	Mitigate	Network	● R
Bad IPv6 version	Mitigate	Network	● R
Bad SCTP checksum	Mitigate	Network	● R
Bad TCP checksum	Mitigate	Network	● R
Bad TCP flags (all cleared)	Mitigate	Network	● R

Note: The screens show different info, why? **Device Dos** shows the status of all vectors for that profile and the current status and rates. Use the last lesson to adjust thresholds of the current attacks to see different results.

Hint: Manual thresholds under **Dos Overview >> Filter Type >> Device DoS**. Scroll down and see all the vectors and rates. Adjust if you desire.

- Change the **View Filter** and see how you get different Views of some of the same data in a different context.
- Make sure you adjust the filter to **Protected Object** and select **ServerNet**. This will show the status of the protected object, not the device level protection.

- Navigate to **Visibility >> Dashboard**. Explore the amount of rich data returned. Hover over the attacks. Scroll down and see what information is supplied.



Attack Duration

Attacks

The current Attacks are displayed and are only affected by the foll

# of Attacks	
Critical	1
High	1
Moderate	3
Low	0

Attack ID	Severity	Vector
3205806…	Critical	TCP SYN flood
2882400…	High	ICMPv4 flood
417818286	Moderate	TCP bad ACK fl
442177419	Moderate	TCP SYN Overs
1973515…	Moderate	TCP Push Flood

Virtual Servers

The current Virtual Servers act

# of Virtual Servers	
Critical	0
Unhealthy	0
Moderate	0
Good	5

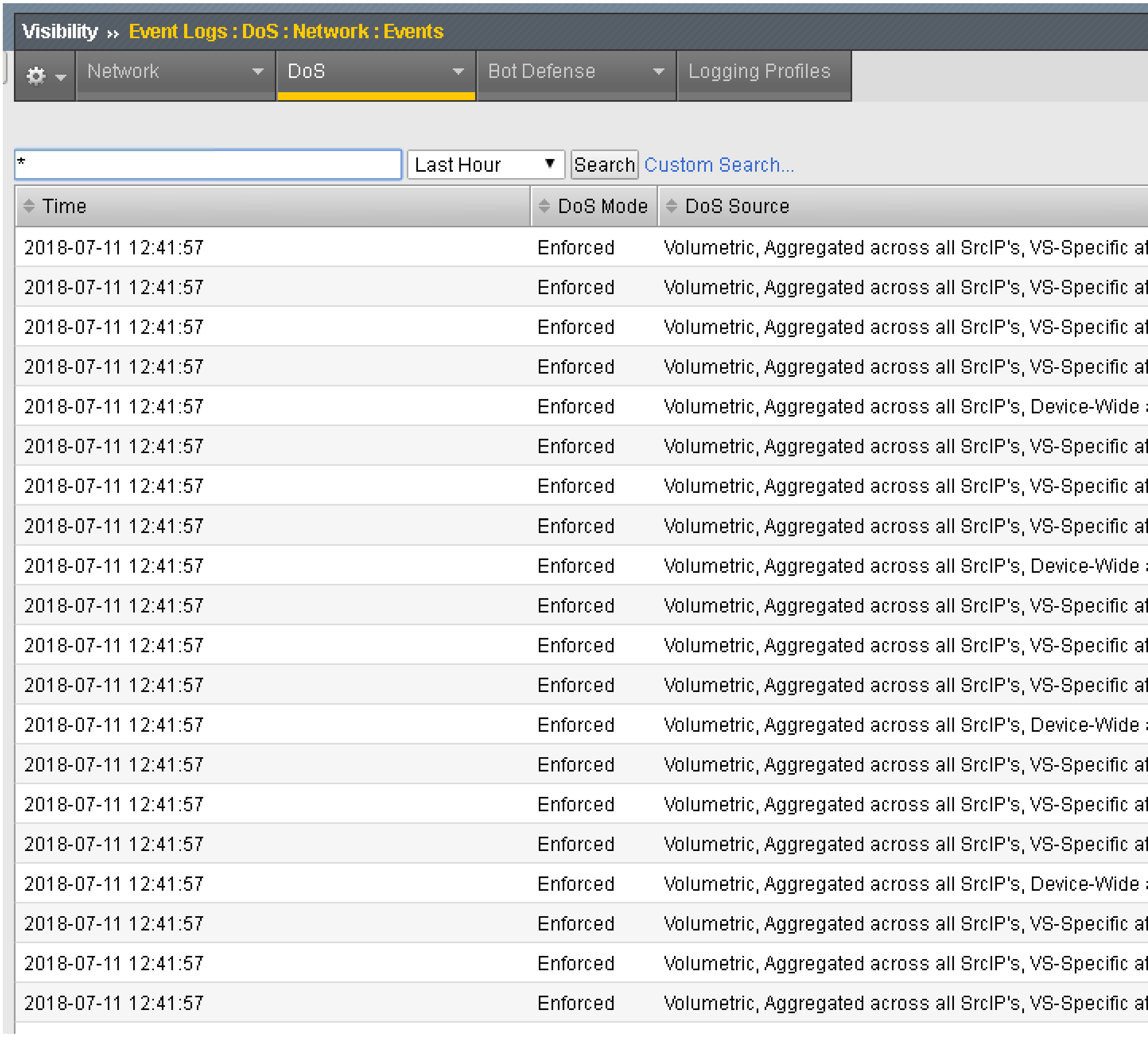
Virtual Server	Server Lat
Device	0
/Common/Server	0
/Common/L7_Behavioral_2	0
/Common/L7_Behavioral	0
/Common/ServerNet	0

- Notice under Attack Duration the red heart symbol. Signifies an ongoing attack. If you don't see it. Use Ctrl - to shrink your screen view. Or use the arrow at the top to expand.

Note: Why is there no data in the Virtual Server Section?

Hint: We only have Device Protection and the Server Network /24 protection set. We will see VS when we configure the next exercise.

- Navigate to **Visibility** >> **Event Logs** >> **DoS** >> **Network** >> **Events**



Time	DoS Mode	DoS Source
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, Device-Wide
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at
2018-07-11 12:41:57	Enforced	Volumetric, Aggregated across all SrcIP's, VS-Specific at

- Further explore the DoS Event logs. For example, clear the search and identify the "Stop" and "Start" times for an attack, type, action, PPS and Dropped Packets etc.

- **Clean-up**: On the Attacker CLI, if the attack is still running be certain to end it with Ctrl-C.
- **Clean-up**: After stopping the attack, delete the ServerNet Protected Object.

7.3.3 Lab 3 – Using Auto Thresholding

This exercise will simulate a newly configured Protected Object where the Security Administrator is unsure what values to assign to a few common vectors. Note that auto-thresholding is useful at both the **Device** and **Protected** Object levels.

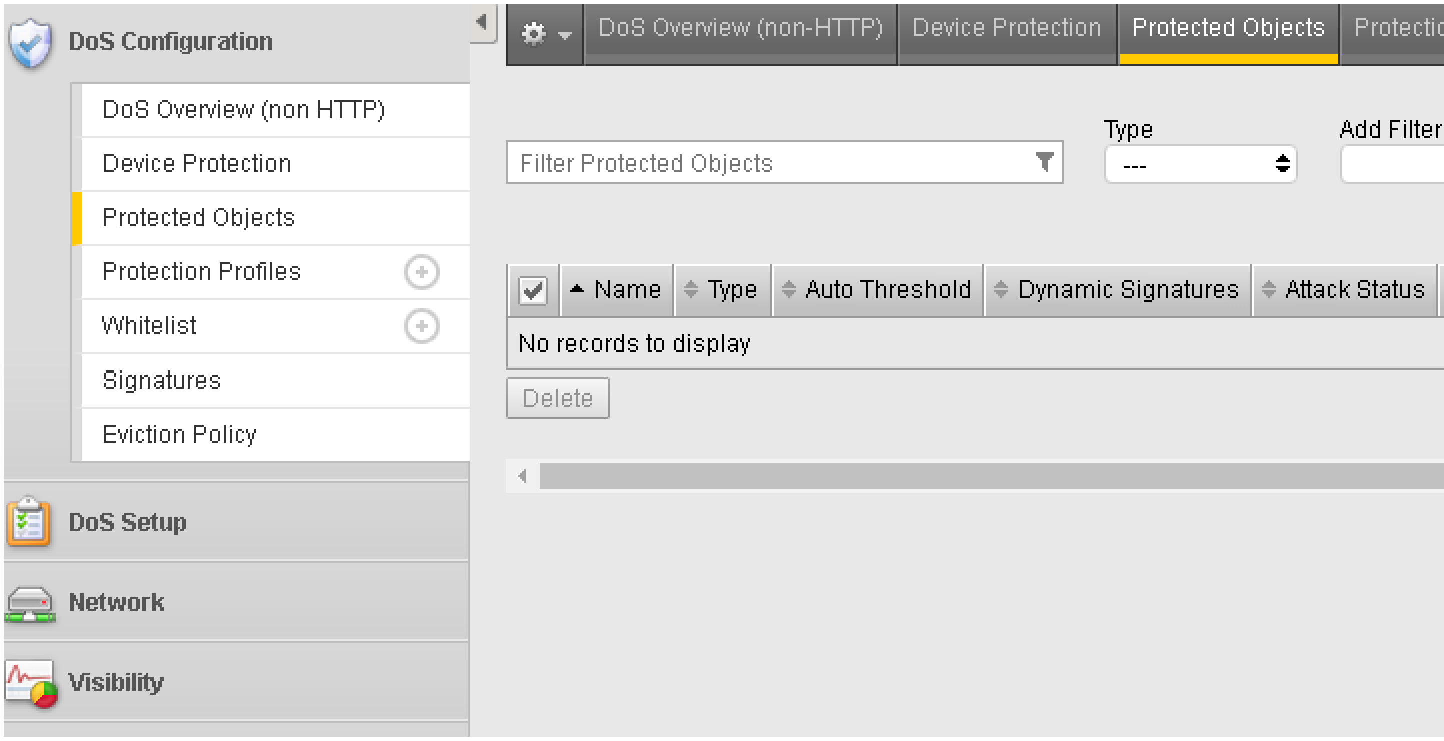
Note: This demo may place significant stress on the demo environment. This may make the DHD UI less responsive. This is unavoidable since for auto-thresholding to block, the attack must be damaging enough to cause stress, which will push the CPU on the Virtual Environment very high. Remember that this is a virtual environment with minimal resources for lab under high stress and that the Hybrid Defender appliances mitigate these attacks in dedicated hardware.

Task 1 – Create Protected Objects that the baseline traffic will be targeting

The DHD device wide protection is enforced for all traffic flowing through the device. For more granular control, we use **Protected Objects** and configure mitigation settings for those objects to be enforced.

In this task you will configure **object-level** DoS protection, and then issue an attack and review the results.

- In the BIG-IP Configuration Utility, open the **DoS Configuration** >> **Protected Objects** page and in the Protected Objects section click the **Create** dropdown and select **Protected Object**



No records to display

- Configure the Protected Object using the following information, and then click **Create**.

Name	Server15
Destination Address	10.1.20.15
Port	*All Ports
Protocol	TCP
Protection Profile:	dos
Eviction Policy:	Blank
VLAN(s):	defaultVLAN
Logging Profiles:	local-dos

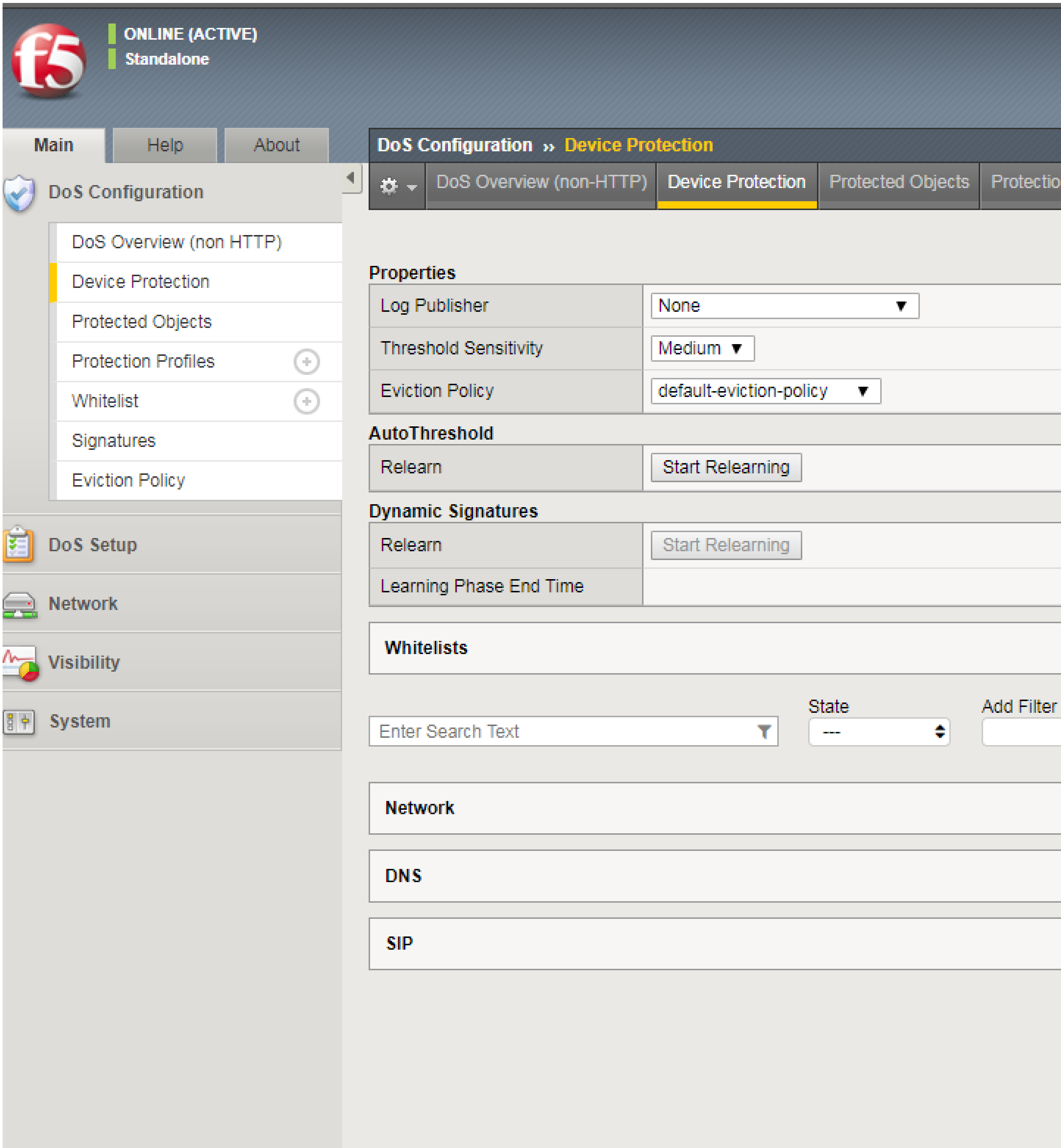
- Click **Save**
- This Protected Object will be used for the Auto-Thresholding lab.

Task 2 – Run Scripts to start L4 traffic generation – Good Traffic

- Putty SSH (use the desktop shortcut) to open a shell to the **good client system**.
- Accept the SSH Warning.
- Enter “ubuntu” as the user. The session is preconfigured to authenticate with a certificate.
- This script will generate baseline traffic against both 10.1.20.14 and 10.1.20.15 (Your Protected Object)
- Start the auto-threshold base-lining script with:

```
# sudo su
# cd ~/scripts
# ./baseline_l4.sh
```

- In the Hybrid Defender UI, in **Dos Configuration >> Device Protection**, **Click** in the AutoThreshold Section **Start Relearning**



Properties

Log Publisher	None
Threshold Sensitivity	Medium
Eviction Policy	default-eviction-policy

AutoThreshold

Relearn	Start Relearning

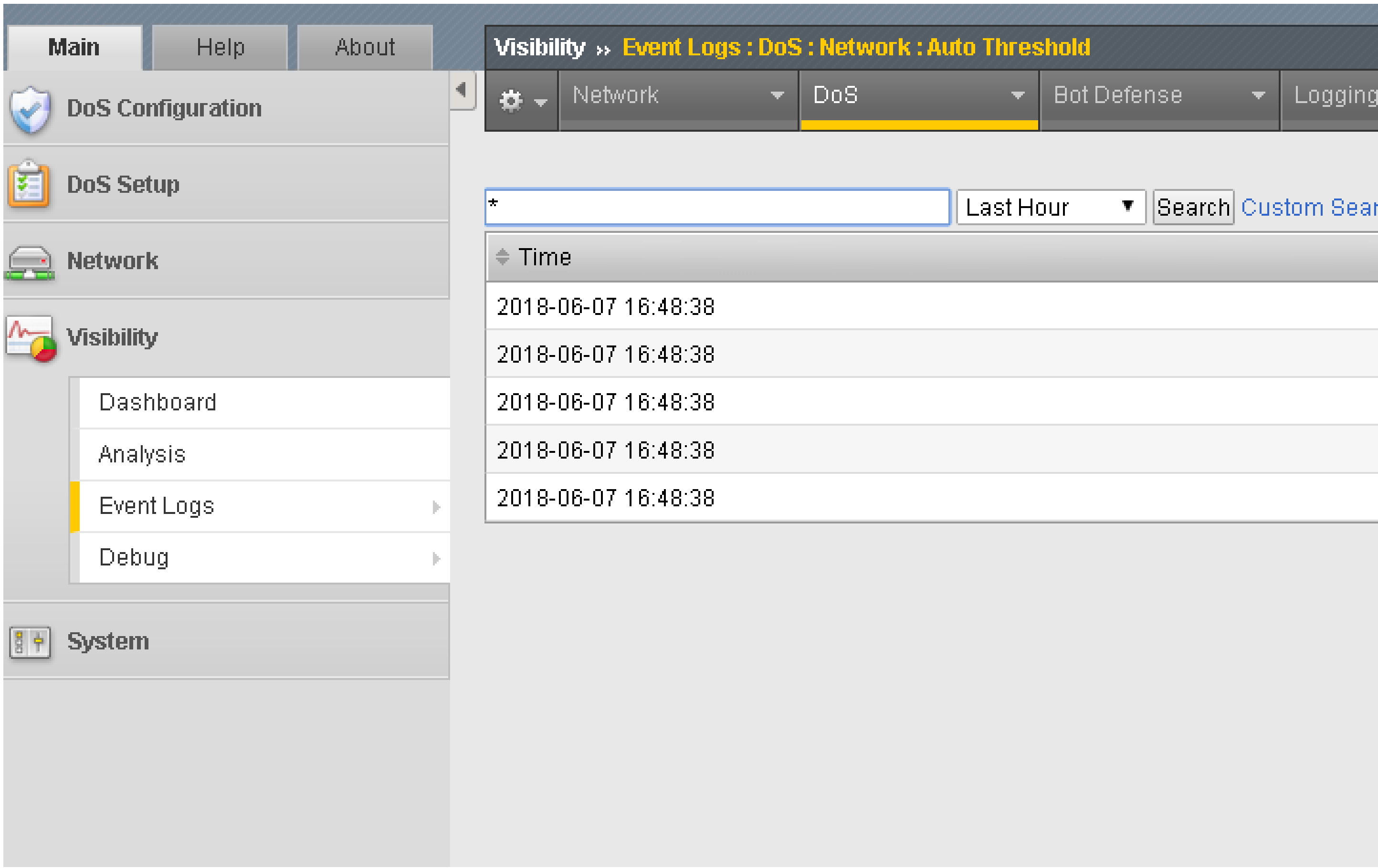
Dynamic Signatures

Relearn	Start Relearning
Learning Phase End Time	

State: ---

In the Hybrid Defender Web UI, Navigate to **Dos Configuration >> Protection Profiles** Select the **dos** profile and Click the **Network** box. We will enable auto-thresholding for the following vectors: **ICMPv4 Flood, TCP SYN Flood, TCP Push Flood, TCP RST Flood, TCP SYN ACK Flood**. If not set to **Fully Automatic** select each vector and clicking the **Set Threshold Mode** drop down and selecting **Fully Automatic**. When all vectors are configured, Go back to the top and Select **Commit Changes to System**.

- In the Hybrid Defender Web UI, view the Auto Threshold event log by navigating to **Visibility >> Event Logs >> DoS >> Network >> Auto Threshold**.



Time
2018-06-07 16:48:38
2018-06-07 16:48:38
2018-06-07 16:48:38
2018-06-07 16:48:38
2018-06-07 16:48:38

Note: The system is updating the detection thresholds. With auto-thresholding, the system adjusts the detection thresholds based on observed traffic patterns.

However, mitigation rate limits are always dynamic based on detected system or protected object stress. If anomalous levels of traffic are running, but there is no stress, the Hybrid Defender will generate alerts but will not block traffic. Under stress, the rate limits are automatically created and adjusted dynamically.

- In the Hybrid Defender UI, navigate to **Dos Configuration >> Dos Overview**, view in Dos Attack or Device Dos, the device sees no attacks.

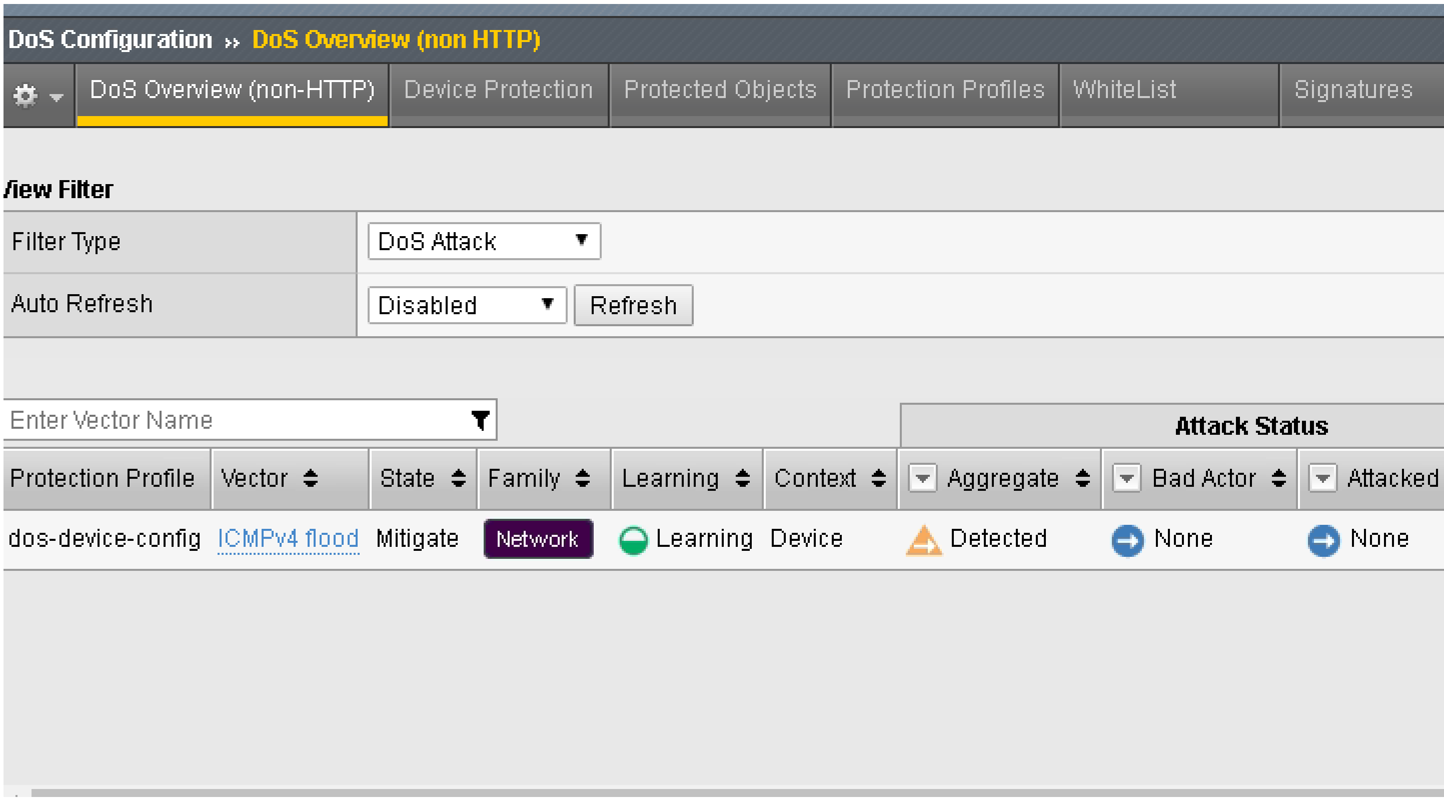
Task 3 – Create Stress to trigger Auto Thresholding and view Reports

- Let's create some stress with a Flood attack. In the **Attacker** CLI start the auto-threshold flood:

```
# sudo su
# cd ~/scripts
# ./autot_flood.sh
```

This is a long duration attack. You can terminate it with Ctrl+C when finished.

- In the Hybrid Defender Web UI, view the Dos Configuration >> DoS Overview. Note that the ICMP Flood attack is being mitigated and the rate limit thresholds for each of the auto-threshold vectors have been adjusted based on stress, including vectors that are not detecting or blocking an attack.



DoS Configuration » DoS Overview (non HTTP)

/iew Filter

Filter Type	DoS Attack ▼
Auto Refresh	Disabled ▼ Refresh

Protection Profile	Vector	State	Family	Learning	Context	Aggregate	Bad Actor	Attacked
						Attack Status		
dos-device-config	ICMPv4 flood	Mitigate	Network	Learning	Device	Detected	None	None

- Select the filter type to **Protected Object** and then Select the Virtual Server **Server15** and view how various thresholds are dynamically adjusted based on the stress. But all the blocking is still being handled by the device-dos.
- Terminate the attack in the Attacker CLI with Ctrl+C.
- After the attack has ended, in the Hybrid Defender Web UI, navigate to the **DoS Visibility** page. Click the **Network** filter. Under Vectors, select ICMPv4 Flood. View the various details.

> **Attention:** If you want to run other attacks and see the UI and logging, adjust settings so you can mitigate attacks. Please do so. This will also be done in the Advanced Class.

- **Clean-up**: On the Attacker CLI, if the attack is still running be certain to end it with Ctrl-C.
- **Clean-up**: After stopping the attack, clear the learning on the Hybrid Defender CLI with:

```
# tmsh run security dos device-config auto-threshold-relearn
# tmsh run security dos virtual name Server15 auto-threshold-relearn
```

- **Clean-up**: Stop the baseline traffic generation from the **good-client** if still running using CTRL+C

7.3.4 Lab 4 – Configuring L7 Attack Protection

In this exercise we will use a protected object and enforce mitigation for low and slow/encrypted layer 7 attacks.

Note: We will first launch attacks with no protection to see the results. Then enable protection and compare the results.

Task 1 – Use Firefox to access Website and use Attacker to bring it down.

- Open the following in separate tabs in the Hybrid Defender Web UI:
- **DoS Configuration >> Dos Overview**
- **Visibility >> Event Logs >> DoS >> Application Events**
- From a the **Firefox browser** on the jumphost go to https://10.1.20.11. Ignore SSL warning and Add Exception.

Note: This bypasses the Hybrid Defender and accesses the server directly, showing the availability and/or performance of the site directly.

Click around a few links. This is the site we will launch an attack against and mitigate.

- Verify that the configuration is providing no L7 protections by taking the server offline with a slowloris attack.

Note: Apache will try to clean up the slow flows, but they will do so inefficiently and the server is impacted (which will show as an outage, missing objects and/or slower responsiveness).

- Run the slowloris attack from the Attacker CLI:

```
# cd ~/scripts
# ./slowloris.sh
```

- The tool will rapidly show the site offline (10-15 seconds, with trivial traffic load)
- Refresh https://10.1.20.11 to show the effects of the attack. Click links on the page.

Note: Since we are running locally from the Win7 system in a virtualized environment, you may be able to access the site, however it will be slower and often the GIFs will not load. An Internet user would not be able to "fight through" the attack to get to the server as often as a system on the local LAN.

- Stop the slowloris attack by using CTRL+C.

Start a more effective Slow Read attack.

Note: This attack is harder for DoS mitigation tools to mitigate and can be very effective even with a tiny number of concurrent connections trickling in very slowly to the server to fly below the radar of network detections. In our example we will open 10 connections per second and read the response data at 1 byte / sec. The attack would be effective even at 1 cps, it would just take a bit longer to build up the connections.

- From the **Attacker** CLI/shell start the slowread attack:

```
# cd ~/scripts
# ./slowread.sh
```

As soon as the site is down (service available: NO) in the Attacker CLI, refresh https://10.1.20.11 to show that it is down/slow/intermittent.

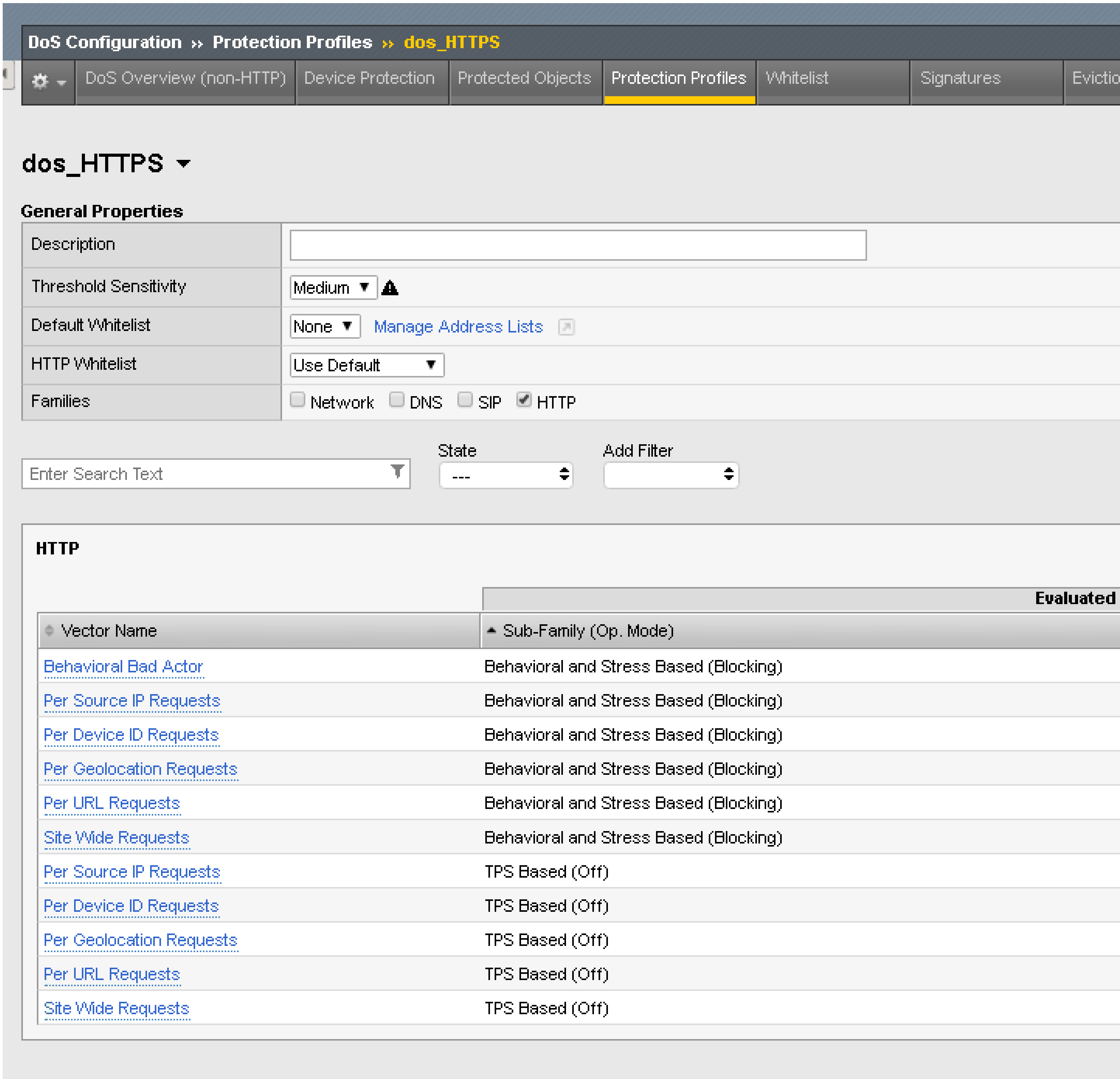
- In the DDoS Hybrid Defender GUI access the tabs you opened previously and notice no attacks were detected.
- Stop the slowread attack by using CTRL+C.

Task 2 – Create Protection Profile for Dos https Object

- In the BIG-IP Configuration Utility, open the **DoS Configuration >> Protection Profiles** page and click the **Create** button.
- Name the profile dos_HTTPS and **select** the HTTP Families Vectors.

Change the settings depicted in the image below.

- Hover in the HTTP box and **Click** in the “”White Space”“
- Click “Per Source IP requests”
- Click the HTTP Group Configuration Link. On the Right Side.
- Under Behavioral and Stress Based Attributes, Set the Operation Mode to **Blocking**
- Leave Threshold Mode in Manual.
- Under Behavioral Based, Set the Mitigation to **Standard Mitigation**
- Ensure Signature Detection is Selected.
- Under Mitigation select Request Blocking “Rate Limit”
- **Commit Changes to System**



dos_HTTPS

General Properties

Description	
Threshold Sensitivity	Medium
Default Whitelist	None — Manage Address Lists
HTTP Whitelist	Use Default
Families	□ Network □ DNS □ SIP ☑ HTTP

HTTP

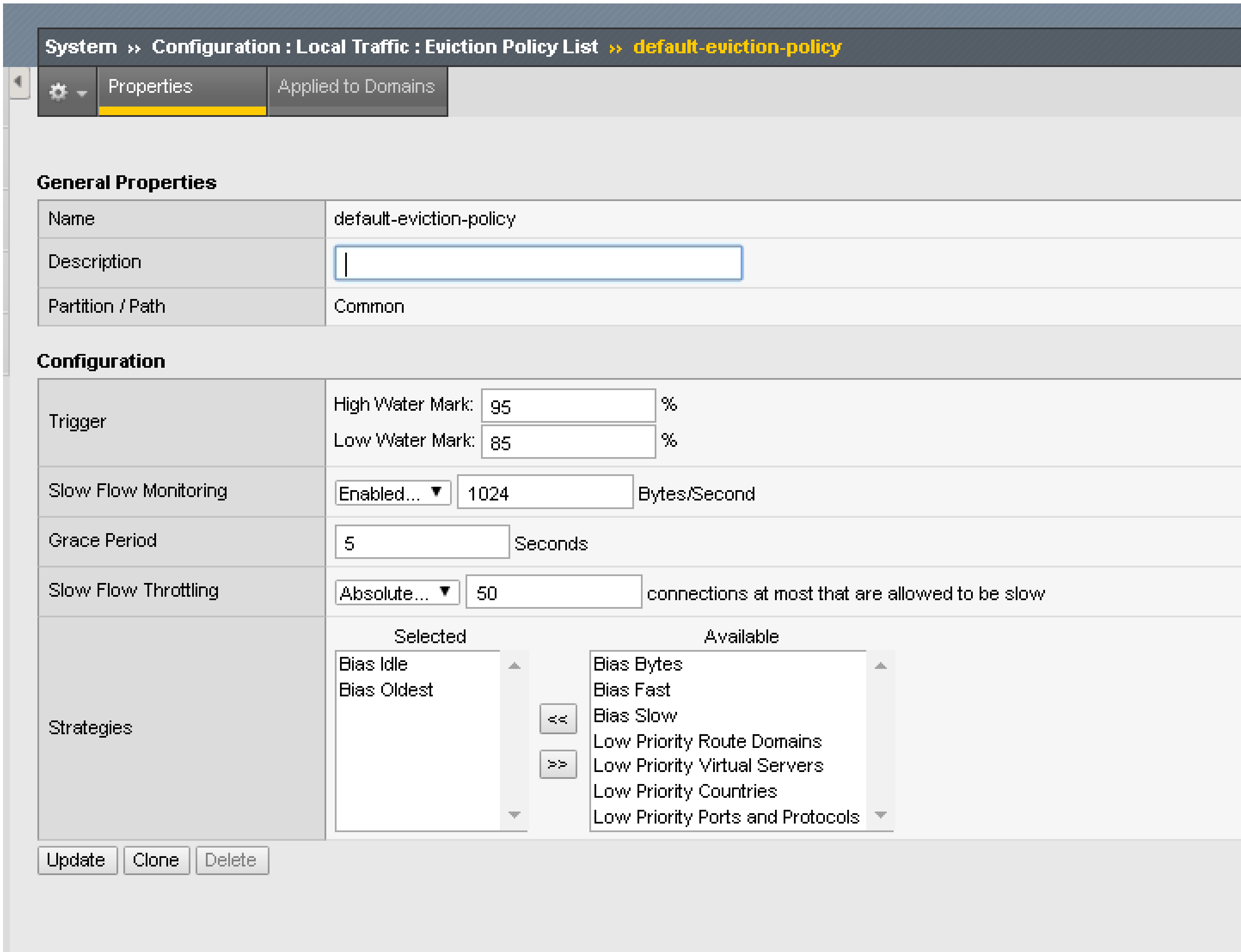
	Evaluated
Vector Name	Sub-Family (Op. Mode)
Behavioral Bad Actor	Behavioral and Stress Based (Blocking)
Per Source IP Requests	Behavioral and Stress Based (Blocking)
Per Device ID Requests	Behavioral and Stress Based (Blocking)
Per Geolocation Requests	Behavioral and Stress Based (Blocking)
Per URL Requests	Behavioral and Stress Based (Blocking)
Site Wide Requests	Behavioral and Stress Based (Blocking)
Per Source IP Requests	TPS Based (Off)
Per Device ID Requests	TPS Based (Off)
Per Geolocation Requests	TPS Based (Off)
Per URL Requests	TPS Based (Off)
Site Wide Requests	TPS Based (Off)

Task 3 – Modify Default Eviction Policy

Important: When making a Slow-Read attack, a client establishes a connection to the Server and sends an appropriate HTTP request, However, the client reads the response at a very slow speed. Some Slow-Read attack clients don't read the response at all for long time and then starts reading data one byte at a time just before the idle connection timeout. The clients sends a Zero window to the server which makes the Server to assume that the client is busy reading the data. As a result, the server to keeps the connection opened for long period of time. Such multiple connections to the Server will consume the resources of the server and can make the server unresponsive to the new and genuine requests.

In order to mitigate such an attack we need to make adjustments to the default-eviction-policy.

- Navigate to Dos Configuration >> Eviction Policy and **Click** on the default-eviction-policy.
- Under “Slow Flow Monitoring” choose “enable” and change the value to 1024.
- Under the “Grace Period” change the default value to 5 Seconds.
- Under “Slow Flow Throttling” change the value to “absolute” and 50 connections as the value.
- Click **Update** when finished.


System ›› Configuration : Local Traffic : Eviction Policy List ›› default-eviction-policy
Properties
Applied to Domains
<<
>>
Update
Clone
Delete

General Properties

Name	default-eviction-policy
Description	
Partition / Path	Common

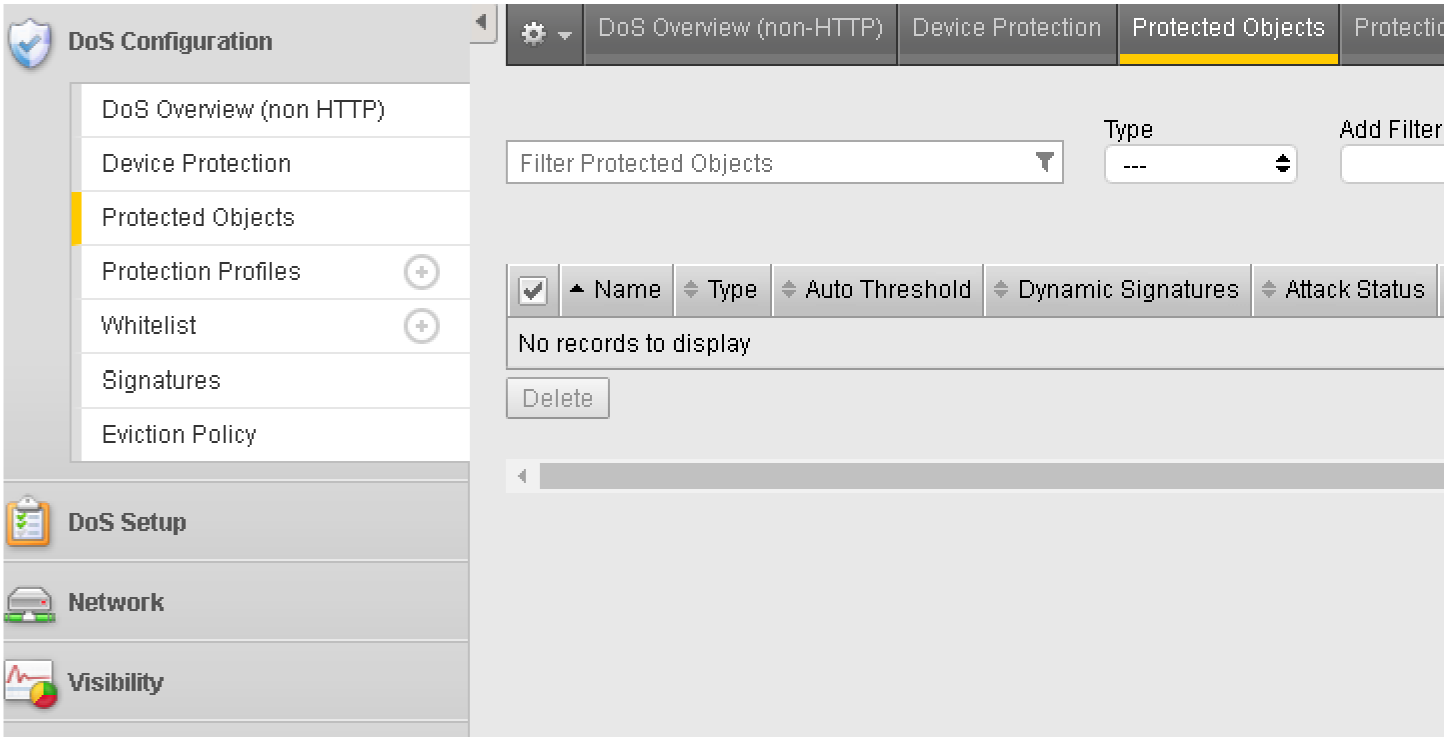
Configuration

Trigger	High Water Mark: 95 % Low Water Mark: 85 %
Slow Flow Monitoring	Enabled... 1024 Bytes/Second
Grace Period	5 Seconds
Slow Flow Throttling	Absolute... 50 connections at most that are allowed to be slow
Strategies	Selected: Bias Idle, Bias Oldest Available: Bias Bytes, Bias Fast, Bias Slow, Low Priority Route Domains, Low Priority Virtual Servers, Low Priority Countries, Low Priority Ports and Protocols

What we are doing here is setting up the policy to recognize and then evict slow flows through the DDoS Hybrid Defender.

Task 3 – Create Protected Object

- In the BIG-IP Configuration Utility, open the **DoS Configuration >> Protected Objects** page and in the **Protected Objects** section click the **Create** dropdown and select **Protected Object**.



No records to display

- Configure a protected object using the following information, and then click **Save**.

Name:	Server_HTTPS
Destination Address:	10.1.20.11
Service Port:	443
Protocol:	TCP
Service Profile:	http
Protection Profile:	dos_HTTPS
Eviction Policy:	default-eviction-policy
VLAN(s):	default_VLAN
Logging Profile(s):	local-dos

Task 4 – Configure Protection/Mitigation

Next we need to modify the VS we created to pass traffic.

- At the bottom of the Menu **Click** the “Show Advanced Menu”” >> Local Traffic >> Virtual Servers >> Virtual Server List >> Select the Server_HTTPS VS.
- Under “”Configuration”” Select **Advanced**
- Ensure the following are Set:
- SSL Profile (Client) to **clientssl**
- SSL Profile (Server) to **serverssl**

- Source Address translation to **none**
- Uncheck Address translation
- Uncheck Port translation
- Set Transparent Next Hop to the Internal Interface Bridge Member of the VLAN. If you have followed along, it will be the interface associated with 1.2
- To figure out interface type "tmsh list net vlan" You want the next hop to be the internal interface.
- Click **Update**

Next we need to modify the Virtual Server Address List Address

- At the bottom of the Menu **Click** the "Show Advanced Menu"" >> Local Traffic >> Virtual Servers >> Virtual Address List >> Select the address 10.1.20.11
- Under **Configuration** disable/ uncheck ARP.
- Click **Update**

Task 5 – Attack Website notice Mitigation/Protection

- From the **Attacker** CLI/shell start the slowread attack:

```
# cd ~/scripts
# ./slowread.sh
```

- From Firefox access the website and click around. You will notice although the website is being DoS'd via slow read, the website remains available.
- If you look in the command window of the Attacker the tool even reports the site off-line, although the site remains available.
- On the DHD CLI run the following command.

```
#tmctl -w 200 virtual_server_stat -s name,clientside.cur_conns,clientside.slow_conns,
↪clientside.slow_killed,serverside.cur_conns,serverside.slow_conns,serverside.slow_
↪killed
```

- Notice as the slow connections increase, the DDoS Hybrid Defender will start killing them.
- **Clean-up**: On the Attacker CLI, if the attack is still running be certain to end it with Ctrl-C.
- **Clean-up**: After stopping the attack, delete the Server Protected Object.

7.3.5 Lab 5 – Configuring L7 Behavioral Attack Protection

In this exercise we will use a protected object and analyze how the DDoS Hybrid Defender reacts and mitigates L7 attacks based on Behavioral Analysis.

Task 1 – Create Protection Profile for Dos Behavioral Object

- In the BIG-IP Configuration Utility, open the **DoS Configuration >> Protection Profiles** page and click the **Create** button.
- Name the profile **dos_behavioral** and **select** the "Network" and "HTTP Families".
- Hover over the Network Box. Click the Pencil in the right corner.

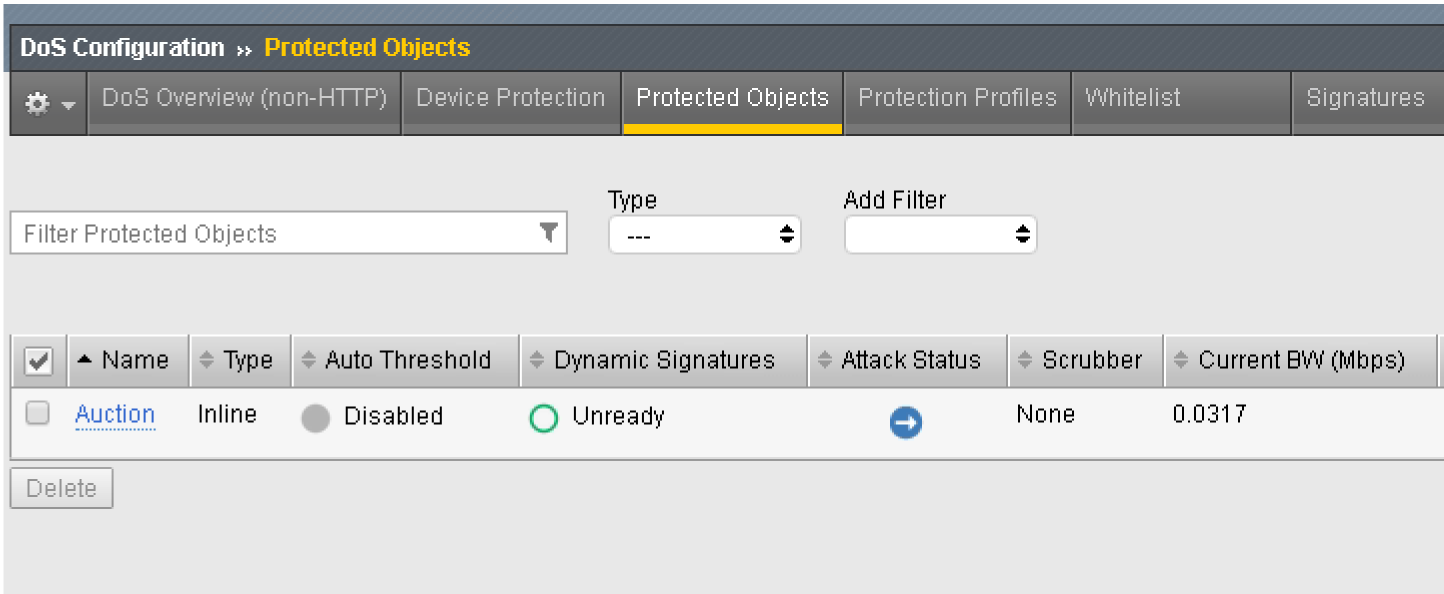
- Ensure Dynamic Signature Enforcement is “enabled”.
- Hover in the HTTP box and **Click** in the “”White Space”“
- Click “Per Source IP Requests” Under Behavioral and Stress Based.
- Click the HTTP Group Configuration Link. On the Right Side.
- Under Behavioral and Stress Based Attributes, Set the Operation Mode to **Blocking**
- Leave Threshold Mode in Manual.
- Under Behavioral Based, Set the Mitigation to **Standard Mitigation**
- Ensure Signature Detection is Selected.
- **Commit Changes to System**
- Go back and click in HTTP again.
- Select “Per Source IP Requests” Under Behavioral and Stress Based, Select Request Blocking (Near the bottom, right).
- **Commit Changes to System**

This places this profile into a behavioral based detection profile. No vectors are used in this demo.

Task 2 – Create Protected Object and Launch Attack

- **In the BIG-IP Configuration Utility, open the DoS Protection >> Quick Configuration page and in the Protected** **Create**.
- Configure a protected object using the following information, and then click **Save**.

Name	Auction
Destination Address	10.1.20.101
Service Port	80
Protocol	TCP
Service Profile:	http
Protection Profile:	dos_behavioral
VLAN(s)	default_VLAN
Logging Profile(s)	local-dos

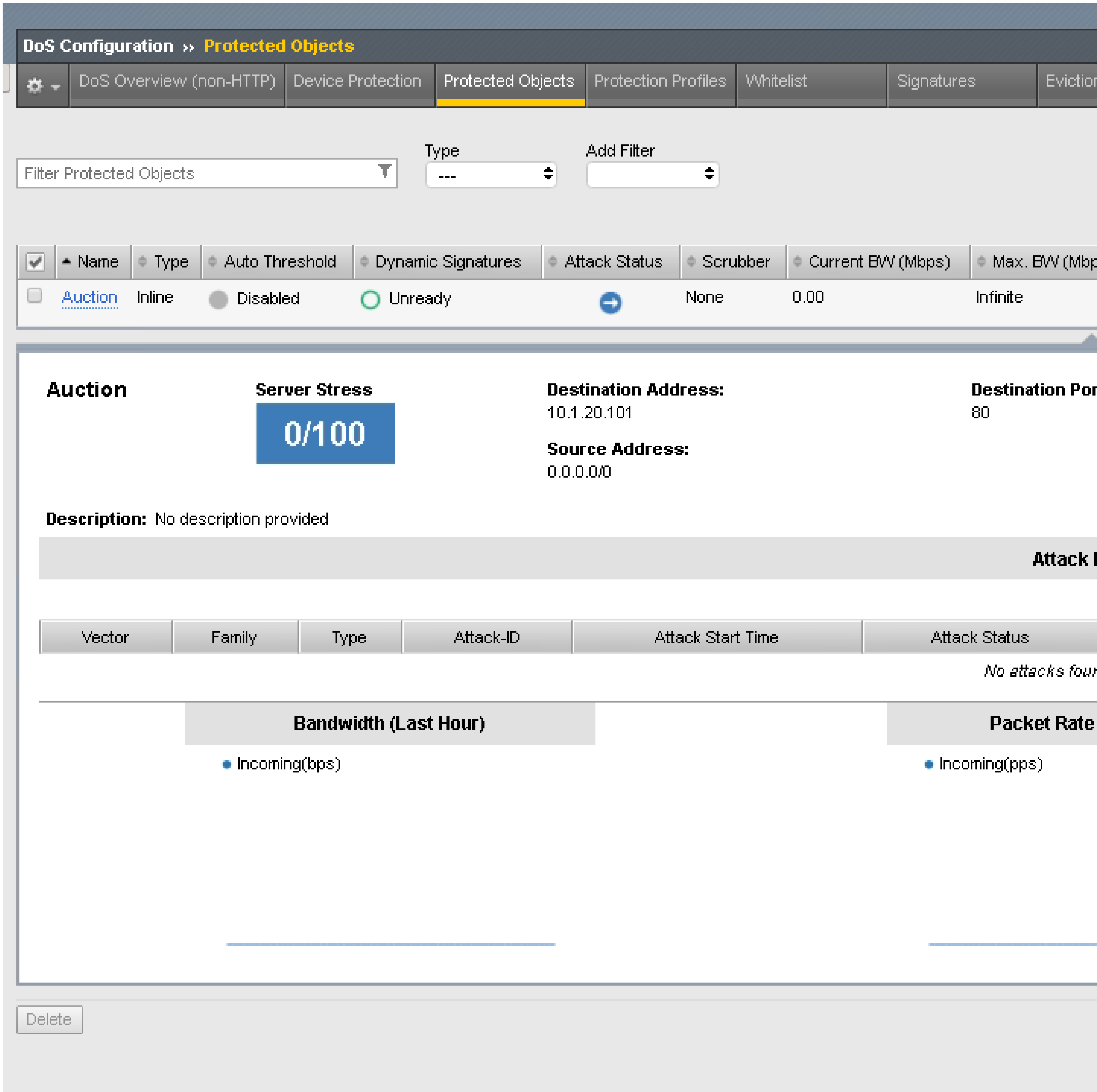


Type: ---

Add Filter:

☑	Name	Type	Auto Threshold	Dynamic Signatures	Attack Status	Scrubber	Current BW (Mbps)
□	Auction	Inline	● Disabled	○ Unready	➔	None	0.0317

- Click in the whitespace of the Protected Object to get additional info that will be useful for detection and mitigation.



Type: ---

Add Filter:

☑	Name	Type	Auto Threshold	Dynamic Signatures	Attack Status	Scrubber	Current BW (Mbps)	Max. BW (Mbp
□	Auction	Inline	● Disabled	○ Unready	➡	None	0.00	Infinite

Auction

Server Stress 0/100

Destination Address: 10.1.20.101

Source Address: 0.0.0.0/0

Destination Por 80

Description: No description provided

Attack I

Vector	Family	Type	Attack-ID	Attack Start Time	Attack Status
					No attacks four

Bandwidth (Last Hour)

● Incoming(bps)

Packet Rate

● Incoming(pps)

Warning: Name needs to be exact or demo will fail.

- Next we need to modify the VS we created earlier to pass traffic.
- At the bottom of the Menu **Click** the "Show Advanced Menu"" >> Local Traffic >> Virtual Servers >> Virtual Server List >> Select the Auction Server.
- Under ""Configuration"" Select **Advanced**

- Ensure the following are Set:
- Source Address translation to none
- Uncheck Address translation
- Uncheck Port translation
- Set Transparent Next Hop to the Internal Interface Bridge Member of the VLAN.
- To figure out interface type “tmsh list net vlan” You want the next hop to be the internal interface.
- Click **Update**
- Next we need to adjust for ARP.
- Go to >> Local Traffic >> Virtual Servers >> Virtual Address List >> Select the Server 10.1.20.101
- Under Configuration Un-Select ARP.
- **Click Update**
- From the Good Client CLI, issue the following command.

```
#sudo su
# cd scripts
#./generate_clean_traffic_101.sh
```

Make sure you are receiving Status Code 200. If you are not receiving a 200, ask for assistance.

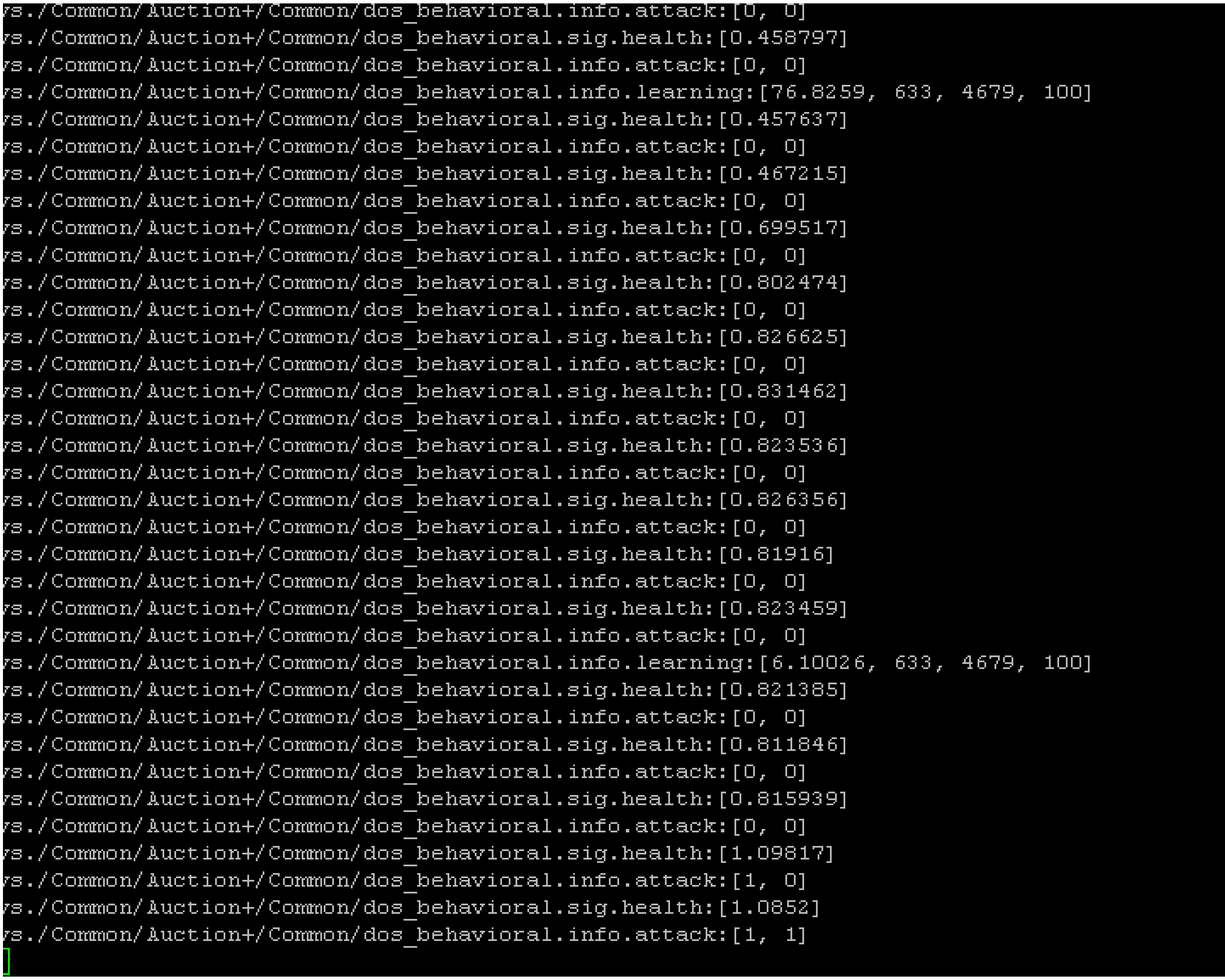
Note: This will need to run for approximately 10 minutes.

- From the DHD CLI issue the following commands:

```
#/root/scripts/l7bdos-reset.sh
#admd -s vs. | grep -e learning -e health -e attack
```

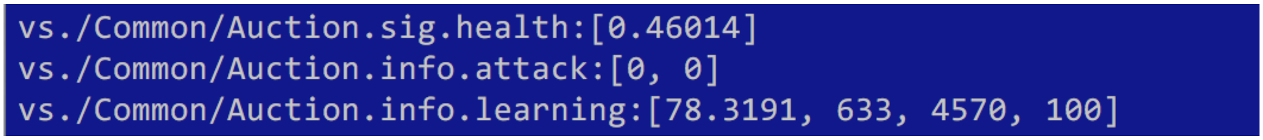
You can use variations of the filters in grep if you are familiar.

- Monitor the window. When you see the following number go to 100, you will move on.



```
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.458797]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.info.learning:[76.8259, 633, 4679, 100]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.457637]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.467215]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.699517]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.802474]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.826625]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.831462]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.823536]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.826356]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.81916]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.823459]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.info.learning:[6.10026, 633, 4679, 100]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.821385]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.811846]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.815939]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[1.09817]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[1, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[1.0852]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[1, 1]
```

- The health of the Protected Object will be shown. In general, a healthy system will show a value around .45. If the value is .5 consistently, then for some reason no learning is occurring and you should check your configuration and verify that baselining traffic is hitting the protected object in question.
- If the system has detected and is mitigating and attack, or not. This will show in the output of 'info.attack' signal. The two numbers in brackets indicate if there is an attack (1 = yes, 0 = no) and if the system is mitigating that attack (1 = yes, 0 = no).
- The output will also include the 'info.learning' signal, which includes 4 comma-separated values that show the status of the admd behavioral dos learning:

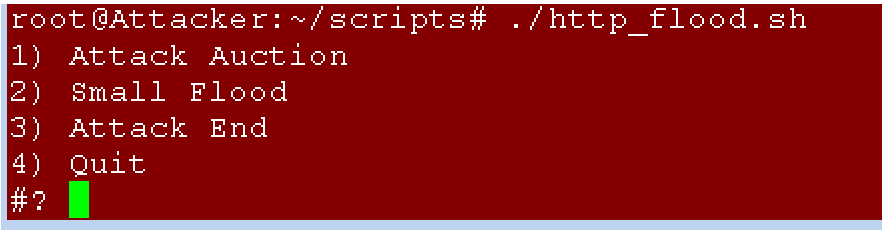


```
vs./Common/Auction.sig.health:[0.46014]
vs./Common/Auction.info.attack:[0, 0]
vs./Common/Auction.info.learning:[78.3191, 633, 4570, 100]
```

- signal values: [baseline_learning_confidence, learned_bins_count , good_table_size , good_table_confidence]

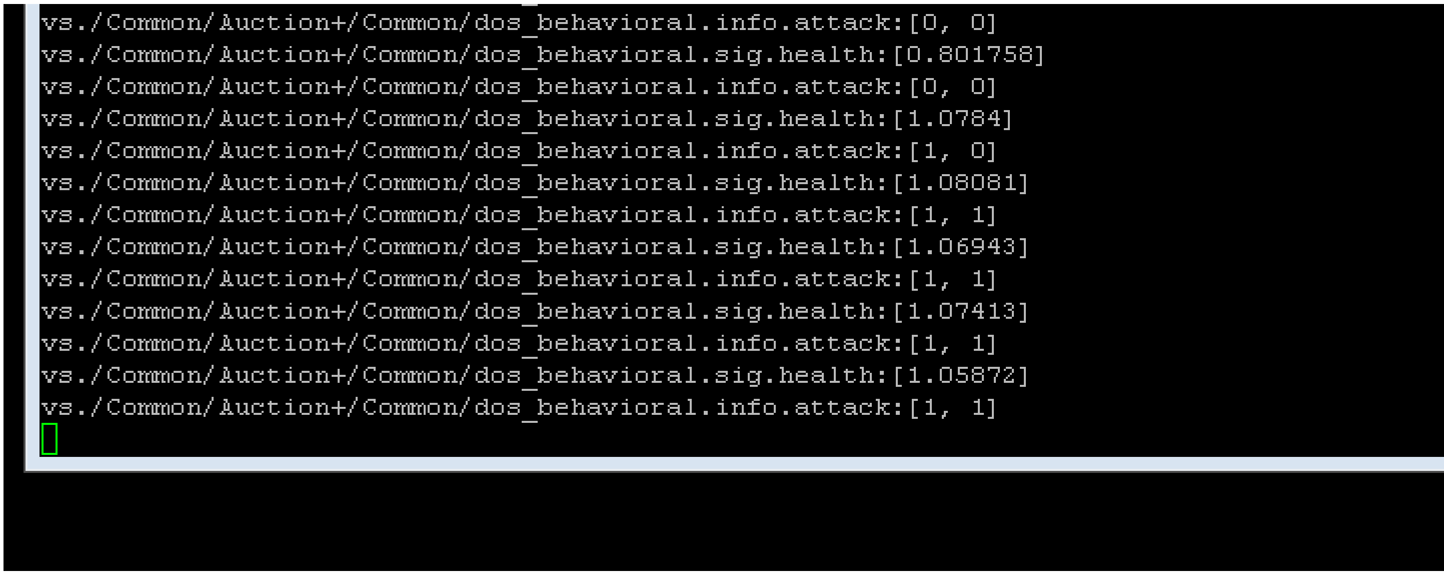
- baseline learning_confidence in % - How confident the system is in the baseline learning.
  - This should be between 80% - 90%
- learned_bins_count - number of learned bins
  - This should be > 0
- good_table_size - number of learned requests
  - This should be > 4000
- good_table_confidence - how confident, as a percentage, the system is in the good table.
  - It must be 100% for behavioral signatures.
- From the Attacker CLI issue the following command:

```
~/scripts/http_flood_101.sh
```



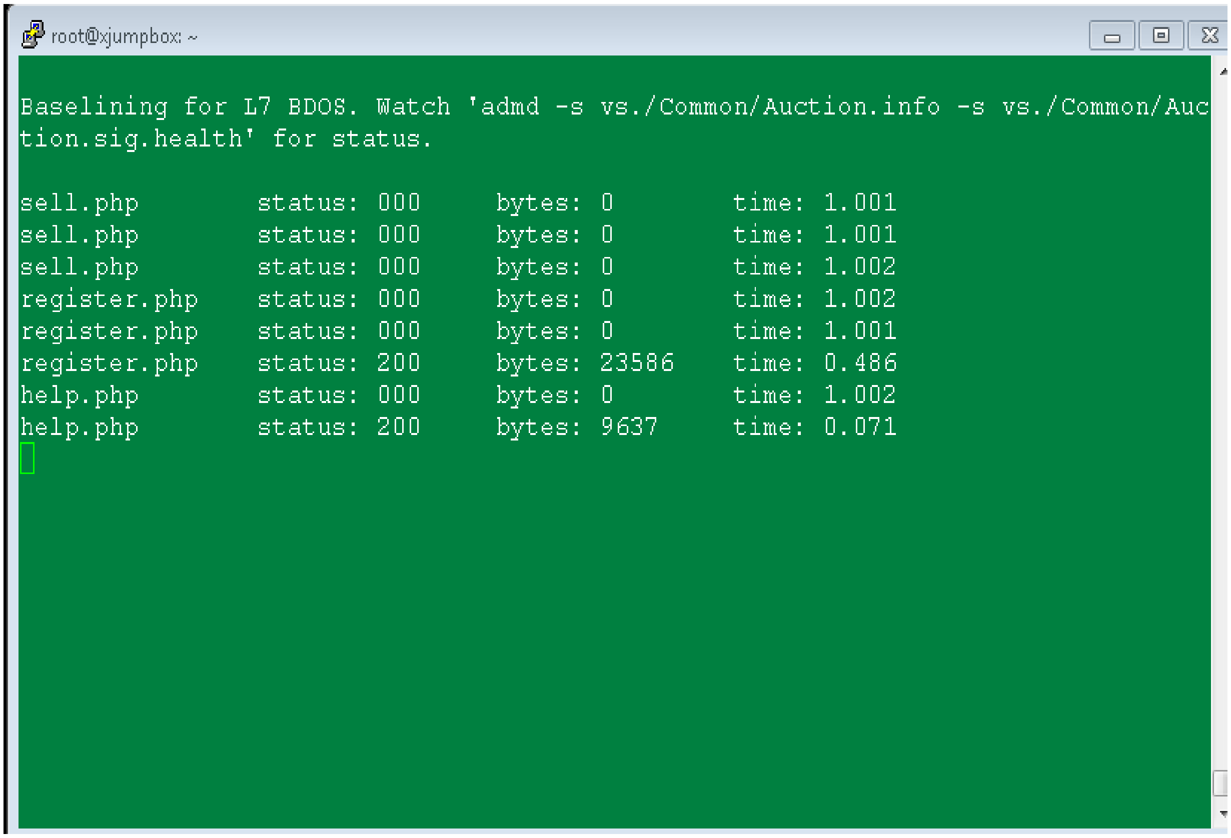
```
root@Attacker:~/scripts# ./http_flood.sh
1) Attack Auction
2) Small Flood
3) Attack End
4) Quit
#?
```

- Choose option **1**, “Attack Auction”
- You will see the attack start in the DDoS Hybrid Defender SSH window:



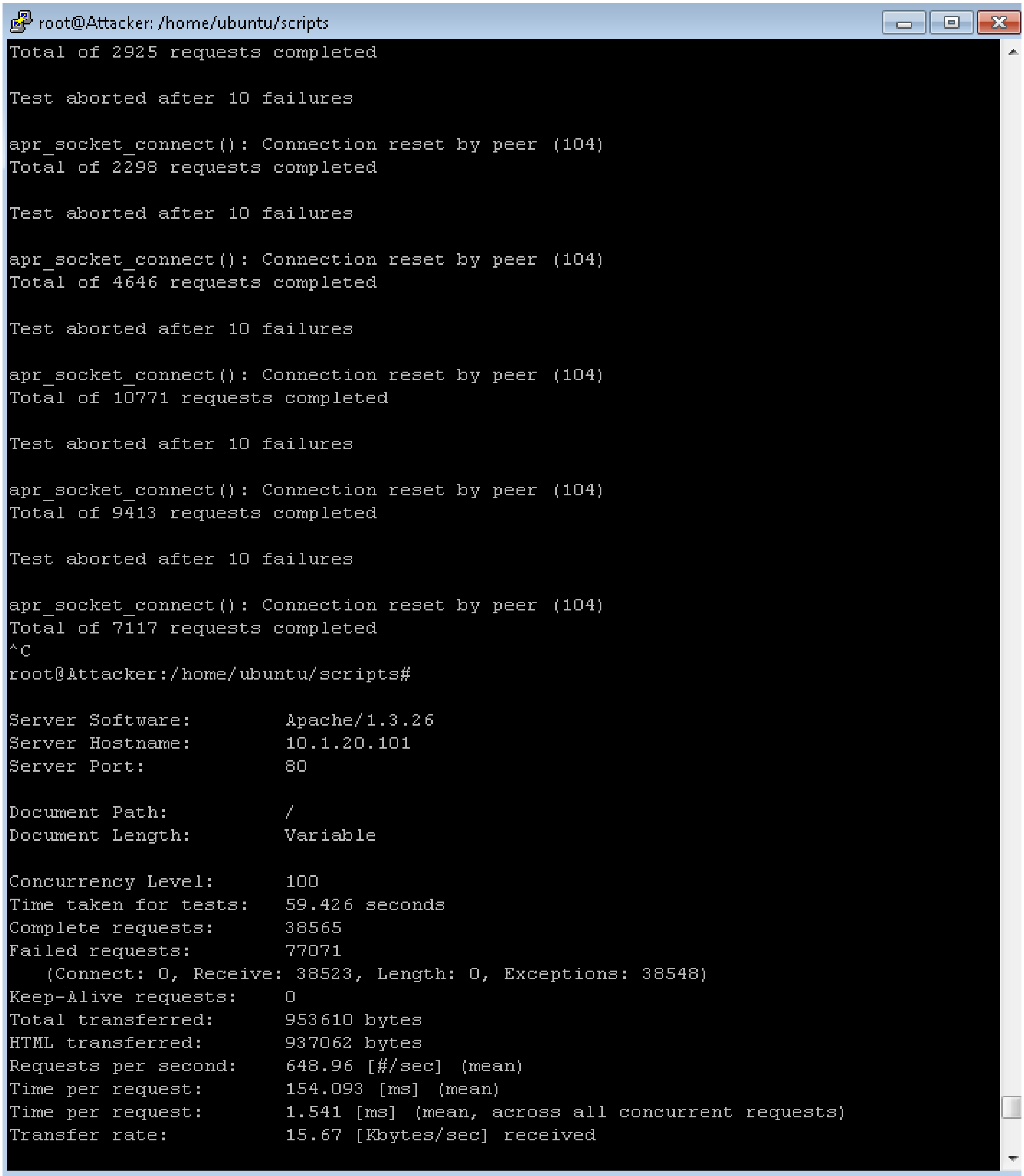
```
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[0.801758]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[0, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[1.0784]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[1, 0]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[1.08081]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[1, 1]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[1.06943]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[1, 1]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[1.07413]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[1, 1]
vs./Common/Auction+/Common/dos_behavioral.sig.health:[1.05872]
vs./Common/Auction+/Common/dos_behavioral.info.attack:[1, 1]
```

- In addition you will see the good client start returning a status of 000 as it is unresponsive. It no longer returns a Status 200. Until the DHD starts mitigation.



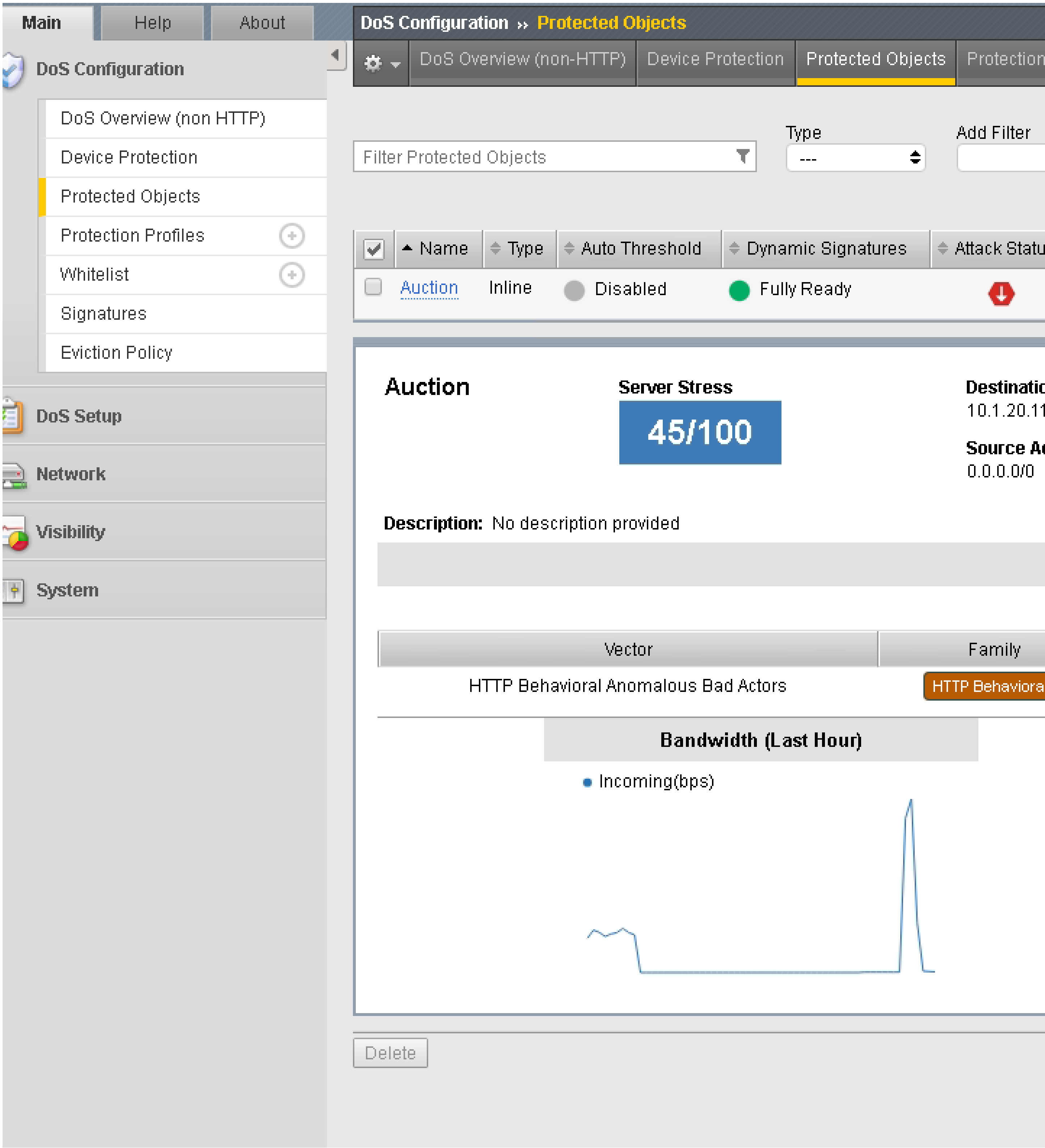
```
Baselining for L7 BDOS. Watch 'admd -s vs./Common/Auction.info -s vs./Common/Auc
tion.sig.health' for status.

sell.php        status: 000     bytes: 0        time: 1.001
sell.php        status: 000     bytes: 0        time: 1.001
sell.php        status: 000     bytes: 0        time: 1.002
register.php    status: 000     bytes: 0        time: 1.002
register.php    status: 000     bytes: 0        time: 1.001
register.php    status: 200     bytes: 23586    time: 0.486
help.php        status: 000     bytes: 0        time: 1.002
help.php        status: 200     bytes: 9637     time: 0.071
```

- You will see the DDoS Hybrid Defender issue a reset when it mitigates the attack.



```
Total of 2925 requests completed

Test aborted after 10 failures

apr_socket_connect(): Connection reset by peer (104)
Total of 2298 requests completed

Test aborted after 10 failures

apr_socket_connect(): Connection reset by peer (104)
Total of 4646 requests completed

Test aborted after 10 failures

apr_socket_connect(): Connection reset by peer (104)
Total of 10771 requests completed

Test aborted after 10 failures

apr_socket_connect(): Connection reset by peer (104)
Total of 9413 requests completed

Test aborted after 10 failures

apr_socket_connect(): Connection reset by peer (104)
Total of 7117 requests completed
^C
root@Attacker:/home/ubuntu/scripts#

Server Software:        Apache/1.3.26
Server Hostname:        10.1.20.101
Server Port:            80

Document Path:          /
Document Length:        Variable

Concurrency Level:      100
Time taken for tests:   59.426 seconds
Complete requests:      38565
Failed requests:        77071
   (Connect: 0, Receive: 38523, Length: 0, Exceptions: 38548)
Keep-Alive requests:    0
Total transferred:      953610 bytes
HTML transferred:       937062 bytes
Requests per second:    648.96 [#/sec] (mean)
Time per request:       154.093 [ms] (mean)
Time per request:       1.541 [ms] (mean, across all concurrent requests)
Transfer rate:          15.67 [Kbytes/sec] received
```

- Explore Dos Configuration >> Protected Objects. Click on the “Attack Status” to expand.



☑	▲ Name	Type	Auto Threshold	Dynamic Signatures	Attack Statu
□	Auction	Inline	● Disabled	● Fully Ready	⬇

Auction

Server Stress

45/100

Destinatio
10.1.20.11

Source Ad
0.0.0.0/0

Description: No description provided

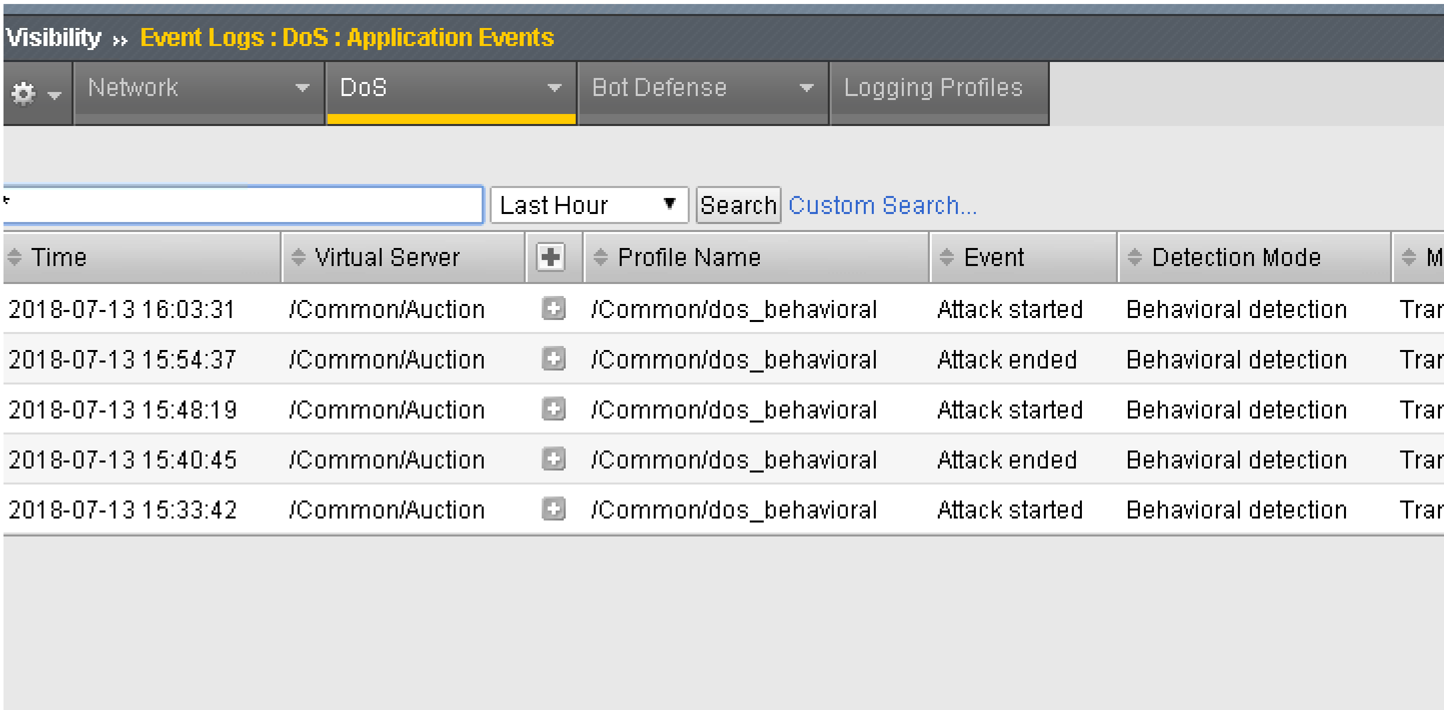
Vector	Family
HTTP Behavioral Anomalous Bad Actors	HTTP Behaviora

Bandwidth (Last Hour)

- Let this run for 2 minutes. Stop the attack by pressing "Enter"" a couple of times in the **Attacker** window the choosing option "3" to stop the "Attack"

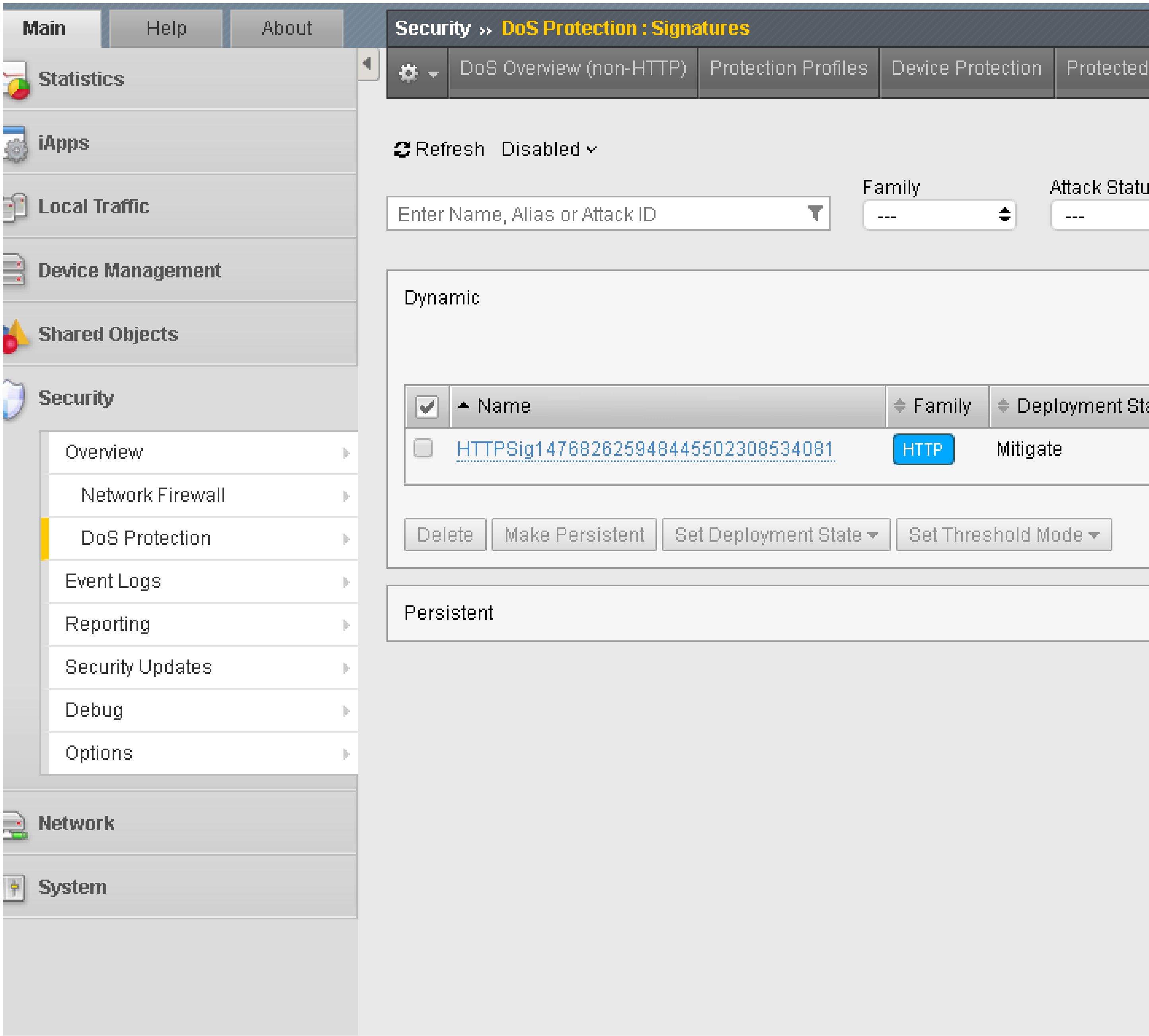
Note: The DDoS Hybrid Defender does not record the end of the attack right away, it is very conservative, therefore you may have to wait 5 minutes to see the results.

- Look at the Event Logs.



Time	Virtual Server		Profile Name	Event	Detection Mode	M
2018-07-13 16:03:31	/Common/Auction	⊞	/Common/dos_behavioral	Attack started	Behavioral detection	Trar
2018-07-13 15:54:37	/Common/Auction	⊞	/Common/dos_behavioral	Attack ended	Behavioral detection	Trar
2018-07-13 15:48:19	/Common/Auction	⊞	/Common/dos_behavioral	Attack started	Behavioral detection	Trar
2018-07-13 15:40:45	/Common/Auction	⊞	/Common/dos_behavioral	Attack ended	Behavioral detection	Trar
2018-07-13 15:33:42	/Common/Auction	⊞	/Common/dos_behavioral	Attack started	Behavioral detection	Trar

- Look at the Signature created. Advanced Menu >> Security >> Dos Protection >> signatures



☑	Name	Family	Deployment Sta
□	HTTPSig147682625948445502308534081	HTTP	Mitigate

- This concludes the DHD Hands on Labs.

8 Introduction to L7 Behavioral DoS

F5's Application Security Manager, Advanced Web Application Firewall, and DDoS Hybrid Defender products all include advanced functionality for defending L7DoS attacks. In this self-paced lab, attendees will have an opportunity to explore L7 Behavioral DoS (BaDOS), leverage BaDOS to mitigate various L7DoS attacks, and examine the built-in reporting and monitoring functions provided by Advanced Web Application Firewall. At the conclusion of the lab, the attendee will have comfort in the basics of BaDOS, how the feature is deployed, and the types of attacks it can be used to mitigate.

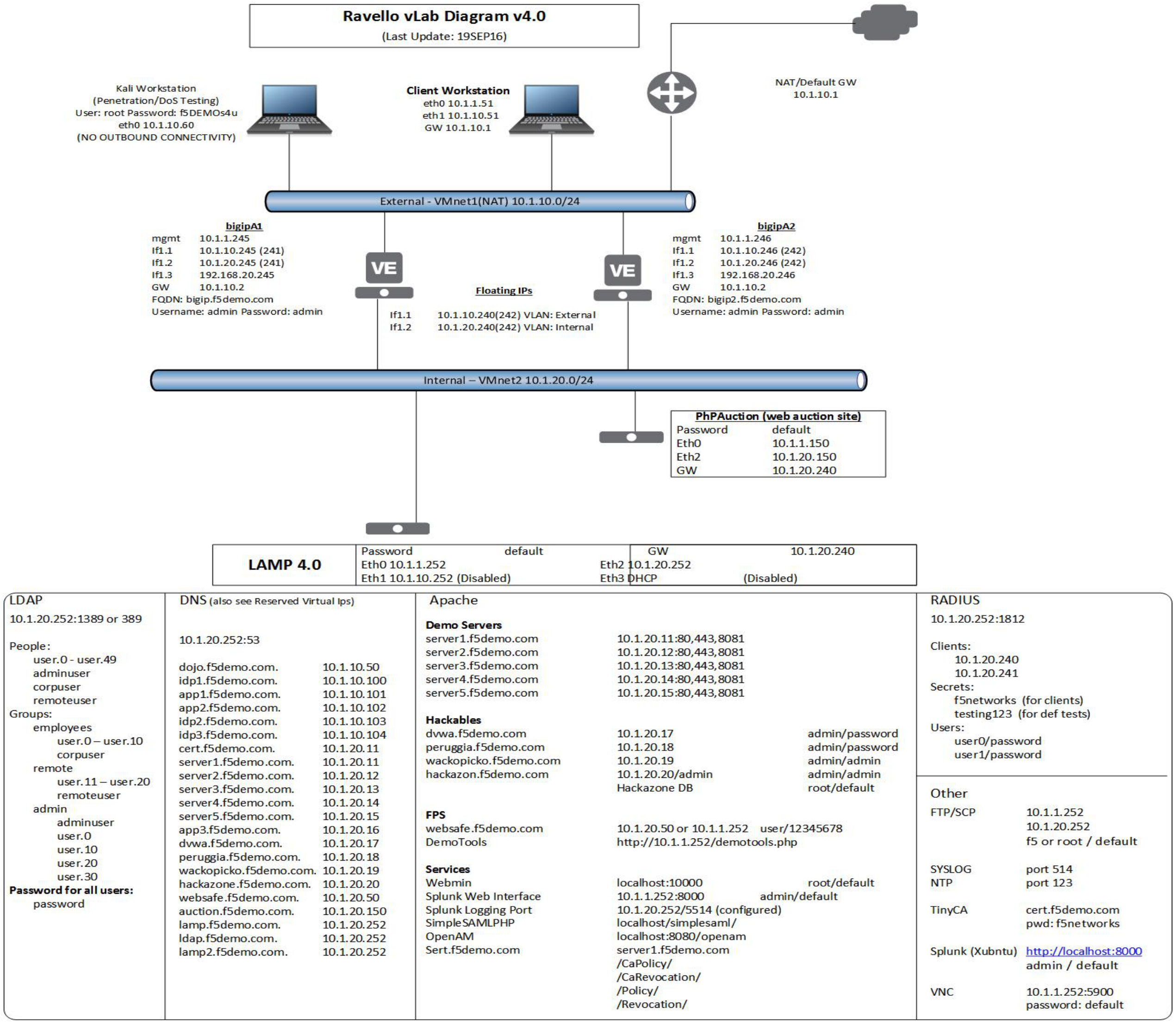
Expected time to complete: 45-60 minutes

8.1 Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

Note: All work for this lab will be performed exclusively from the Linux Workstation jumphost. No installation or interaction with your local system is required.

8.1.1 Lab Topology


Ravello vLab Diagram v4.0
(Last Update: 19SEP16)
Kali Workstation
(Penetration/DoS Testing)
User: root Password: f5DEMOs4u
eth0 10.1.10.60
(NO OUTBOUND CONNECTIVITY)
Client Workstation
eth0 10.1.1.51
eth1 10.1.10.51
GW 10.1.10.1
NAT/Default GW
10.1.10.1
External - VMnet1(NAT) 10.1.10.0/24
VE
VE
Internal – VMnet2 10.1.20.0/24
LAMP 4.0

bigipA1

mgmt	10.1.1.245
If1.1	10.1.10.245 (241)
If1.2	10.1.20.245 (241)
If1.3	192.168.20.245
GW	10.1.10.2

FQDN: bigip.f5demo.com
Username: admin Password: admin

Floating IPs

If1.1	10.1.10.240(242) VLAN: External
If1.2	10.1.20.240(242) VLAN: Internal

bigipA2

mgmt	10.1.1.246
If1.1	10.1.10.246 (242)
If1.2	10.1.20.246 (242)
If1.3	192.168.20.246
GW	10.1.10.2

FQDN: bigip2.f5demo.com
Username: admin Password: admin

PhPAuction (web auction site)

Password	default
Eth0	10.1.1.150
Eth2	10.1.20.150
GW	10.1.20.240

LAMP 4.0

Password	default	GW	10.1.20.240
Eth0 10.1.1.252		Eth2 10.1.20.252	
Eth1 10.1.10.252 (Disabled)		Eth3 DHCP	(Disabled)

LDAP
10.1.20.252:1389 or 389

People:
- user.0 - user.49
- adminuser
- corpuser
- remoteuser

Groups:
- employees
  - user.0 – user.10
  - corpuser
- remote
  - user.11 – user.20
  - remoteuser
- admin
  - adminuser
  - user.0
  - user.10
  - user.20
  - user.30

Password for all users:
password

DNS (also see Reserved Virtual Ips)

10.1.20.252:53

dojo.f5demo.com.	10.1.10.50
idp1.f5demo.com.	10.1.10.100
app1.f5demo.com.	10.1.10.101
app2.f5demo.com.	10.1.10.102
idp2.f5demo.com.	10.1.10.103
idp3.f5demo.com.	10.1.10.104
cert.f5demo.com.	10.1.20.11
server1.f5demo.com.	10.1.20.11
server2.f5demo.com.	10.1.20.12
server3.f5demo.com.	10.1.20.13
server4.f5demo.com.	10.1.20.14
server5.f5demo.com.	10.1.20.15
app3.f5demo.com.	10.1.20.16
dvwa.f5demo.com.	10.1.20.17
peruggia.f5demo.com.	10.1.20.18
wackopicko.f5demo.com.	10.1.20.19
hackazone.f5demo.com.	10.1.20.20
websafe.f5demo.com.	10.1.20.50
auction.f5demo.com.	10.1.20.150
lamp.f5demo.com.	10.1.20.252
ldap.f5demo.com.	10.1.20.252
lamp2.f5demo.com.	10.1.20.252

Apache

Demo Servers		
server1.f5demo.com	10.1.20.11:80,443,8081	
server2.f5demo.com	10.1.20.12:80,443,8081	
server3.f5demo.com	10.1.20.13:80,443,8081	
server4.f5demo.com	10.1.20.14:80,443,8081	
server5.f5demo.com	10.1.20.15:80,443,8081	
Hackables		
dvwa.f5demo.com	10.1.20.17	admin/password
peruggia.f5demo.com	10.1.20.18	admin/password
wackopicko.f5demo.com	10.1.20.19	admin/admin
hackazon.f5demo.com	10.1.20.20/admin	admin/admin
	Hackazone DB	root/default
FPS		
websafe.f5demo.com	10.1.20.50 or 10.1.1.252 user/12345678	
DemoTools	http://10.1.1.252/demotools.php	
Services		
Webmin	localhost:10000	root/default
Splunk Web Interface	10.1.1.252:8000 admin/default	
Splunk Logging Port	10.1.20.252/5514 (configured)	
SimpleSAMLPHP	localhost/simplesaml/	
OpenAM	localhost:8080/openam	
Sert.f5demo.com	server1.f5demo.com /CaPolicy/ /CaRevocation/ /Policy/ /Revocation/	

RADIUS
10.1.20.252:1812

Clients:
- 10.1.20.240
- 10.1.20.241

Secrets:
- f5networks (for clients)
- testing123 (for def tests)

Users:
- user0/password
- user1/password

Other

FTP/SCP	10.1.1.252 10.1.20.252 f5 or root / default
SYSLOG	port 514
NTP	port 123
TinyCA	cert.f5demo.com pwd: f5networks
Splunk (Xubntu)	http://localhost:8000 admin / default
VNC	10.1.1.252:5900 password: default

8.1.2 Lab Components

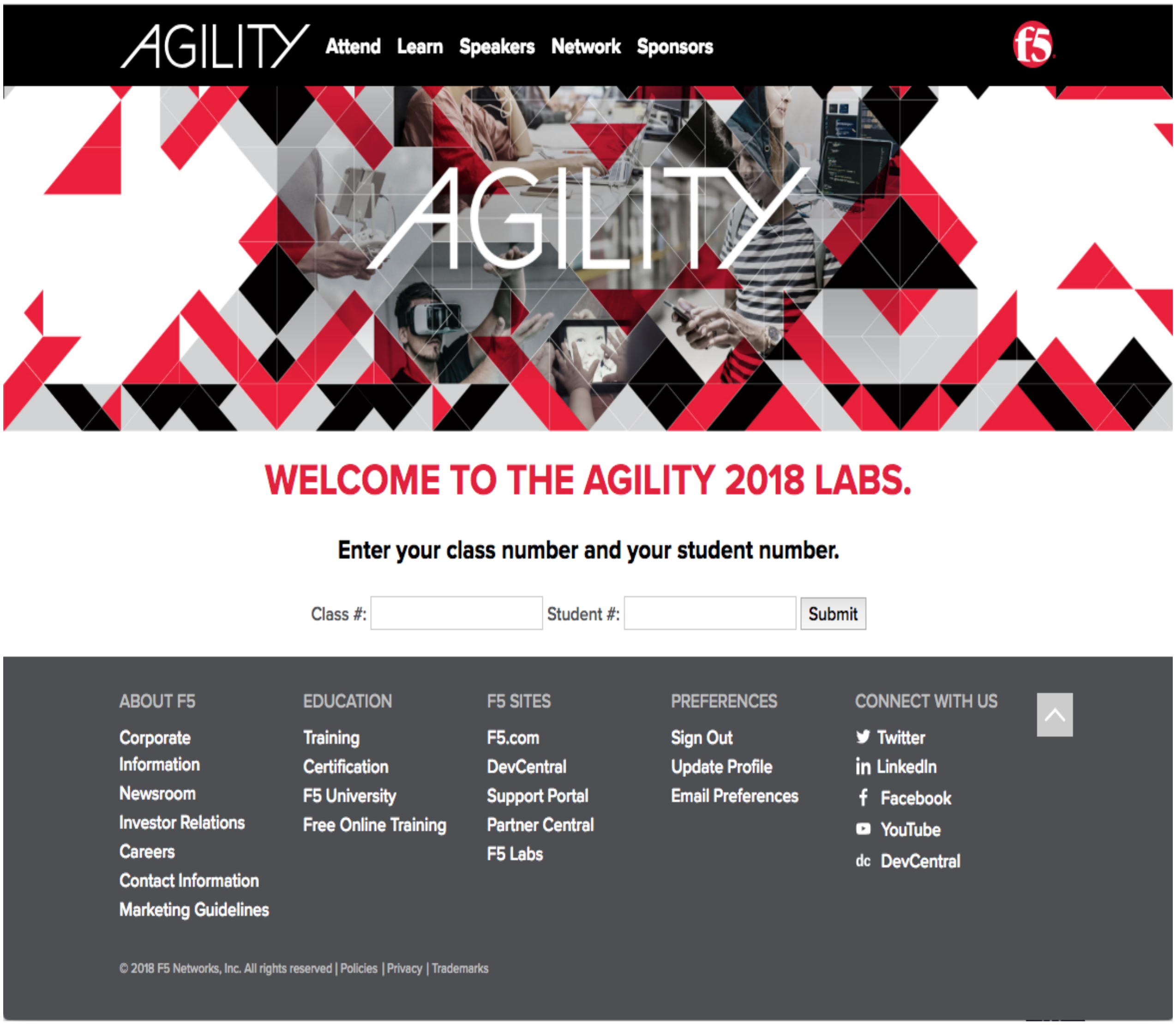
The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials
bigip01	• **Management:** 10.1.1.245 • **Internal:** 10.1.20.245 • **External:** 10.1.10.245	`admin/admin`
bigip02	• **Management:** 10.1.1.246 • **Internal:** 10.1.20.246 • **External:** 10.1.10.246	`admin/admin`
Ubuntu Linux Workstation	• **eth0:** 10.1.1.51 • **eth1:** 10.1.10.51	`f5student/f5DEMOs4u`
Kali Linux Workstation	• **eth0:** 10.1.10.60	`root/f5DEMOs4u`

8.1.3 Accessing Lab Environment

Please follow the instructions below to access the lab environment.

1. Open a browser and go to http://training.f5agililty.com/



WELCOME TO THE AGILITY 2018 LABS.

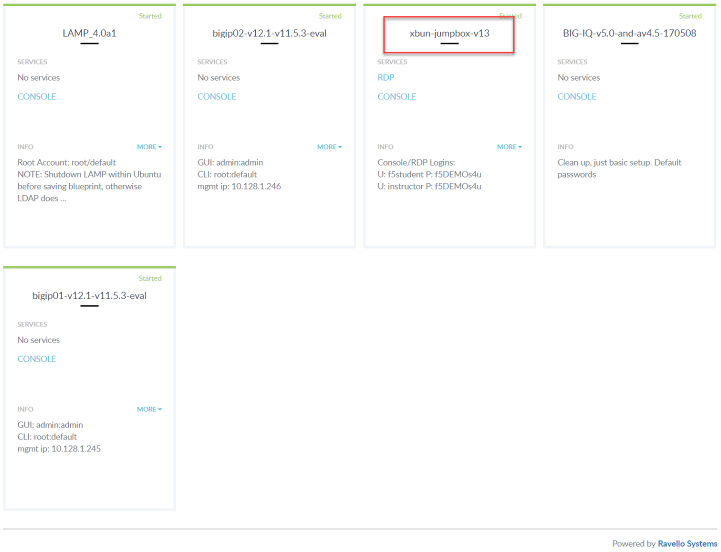
Enter your class number and your student number.

Class #: Student #: Submit

© 2018 F5 Networks, Inc. All rights reserved | Policies | Privacy | Trademarks

2. Use the class number and student number included on the class survey to login to the training portal. Once logged in:

   (a) Look for the **xubuntu-jumpbox-vxx**. You will use the Xubuntu Jumpbox for all the labs. (see below)



LAMP_4.0a1

SERVICES

No services

Root Account: root/default
NOTE: Shutdown LAMP within Ubuntu before saving blueprint, otherwise LDAP does ...

bigip02-v12.1-v11.5.3-eval

SERVICES

No services

GUI: admin:admin
CLI: root:default
mgmt ip: 10.128.1.246

xbun-jumpbox-v13

SERVICES

Console/RDP Logins:
U: f5student P: f5DEMOs4u
U: instructor P: f5DEMOs4u

BIG-IQ-v5.0-and-av4.5-170508

SERVICES

No services

Clean up, just basic setup. Default passwords

bigip01-v12.1-v11.5.3-eval

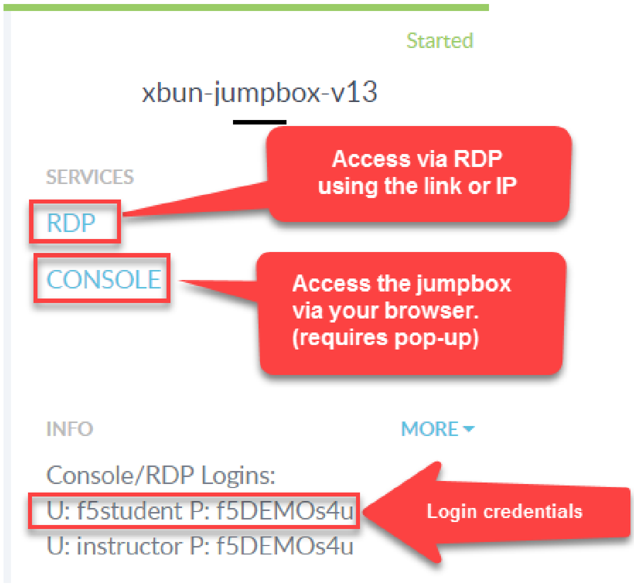
SERVICES

No services

GUI: admin:admin
CLI: root:default
mgmt ip: 10.128.1.245

Powered by Ravello Systems

(b) You can click on **RDP** to RDP to the Xubuntu Jumpbox, or you can select the **CONSOLE** link and access the jumpbox via your browser. **The CONSOLE link requires you turn off pop-up blockers.**



xbun-jumpbox-v13

Access via RDP using the link or IP

Access the jumpbox via your browser. (requires pop-up)

Console/RDP Logins:
U: f5student P: f5DEMOs4u
U: instructor P: f5DEMOs4u

Login credentials

8.2 Base Configuration and Traffic Baseline

In this module, we will configure the base DoS profile and Local Traffic Manager objects used in the remaining modules. Additionally, you will generate traffic needed for Advanced Web Application Firewall Behavioral DoS engine to build a learning baseline.

Objectives:

- Create DoS Profile
- Create Logging Profile and attach to virtual server
- Create iRule for inserting X-Forwarded-For headers and attach to virtual server

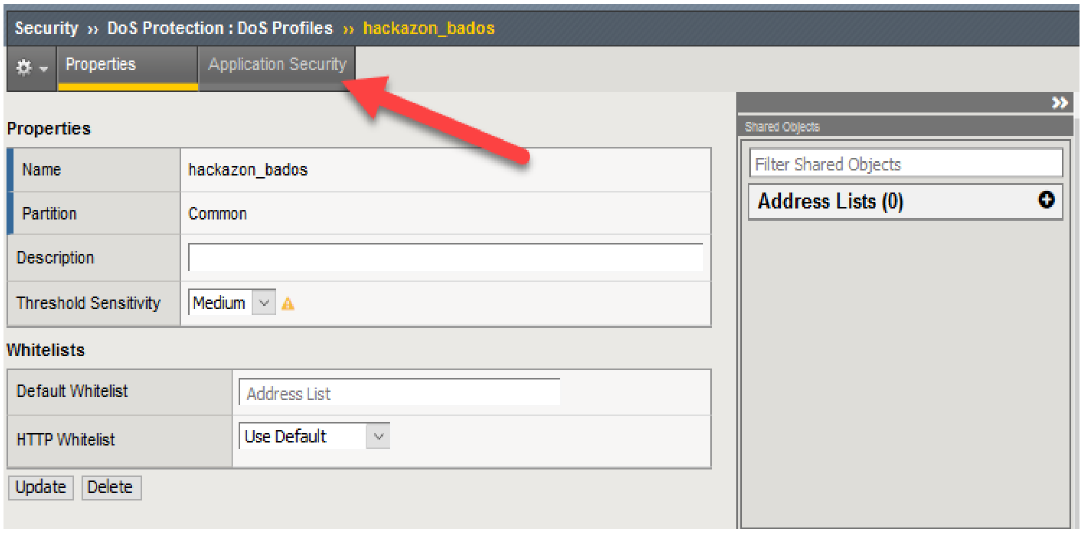
- Generate good traffic to establish BaDOS baseline
- Verify BaDOS learning status

> **Attention:** In this lab, you will configure a number of options to get the lab started. In modules 3 and 4 we will spend time examining the configuration options in more detail. For now, just configure the options as outlined, and we will examine further in later modules.

8.2.1 Set up the DoS profile

In the section you will create a DoS profile with **Behavioral Detection and Analysis** enabled, and attach the DoS profile to the virtual server.

1. Using Chromium Browser on the Xubuntu Jumpbox, open a tab to the GUI on bigip01 (https://10.1.1.245).
2. Navigate to **Security** ›› **DoS Protection : DoS Profiles**
3. Select **Create**. Name your profile **hackazon_bados** and select **Finished**. Open your **hackazon_bados** DoS profile.
4. Select the **Application Security** tab from DoS Profile navigation bar.



Properties

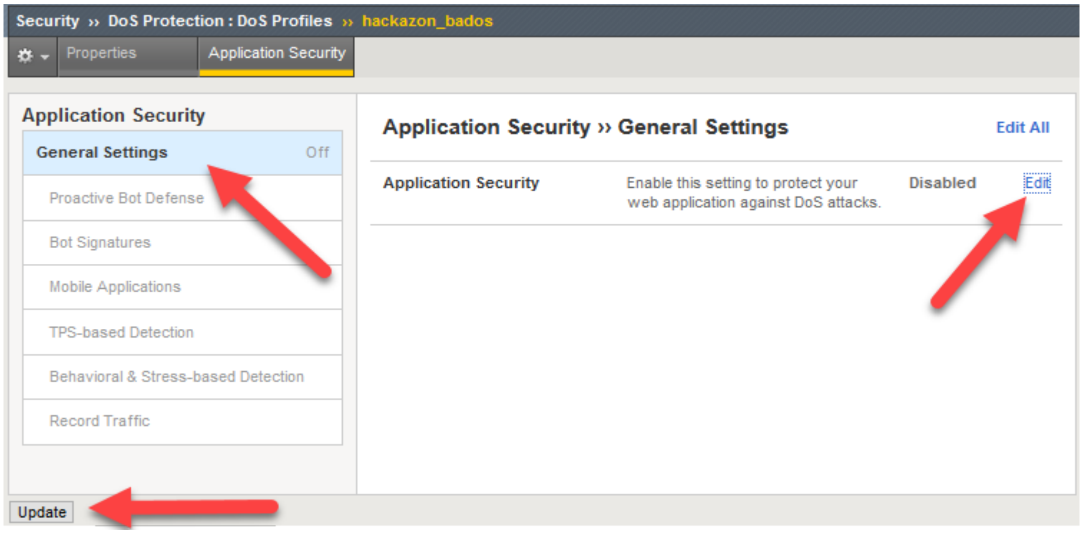
Name	hackazon_bados
Partition	Common
Description	
Threshold Sensitivity	Medium

Whitelists

Default Whitelist	Address List
HTTP Whitelist	Use Default

5. Click **General Settings**, select **Edit** to the right of **Application Security** in the rightmost panel, and check the **Enable** box.

   This will activate the other sections of the DoS profile.



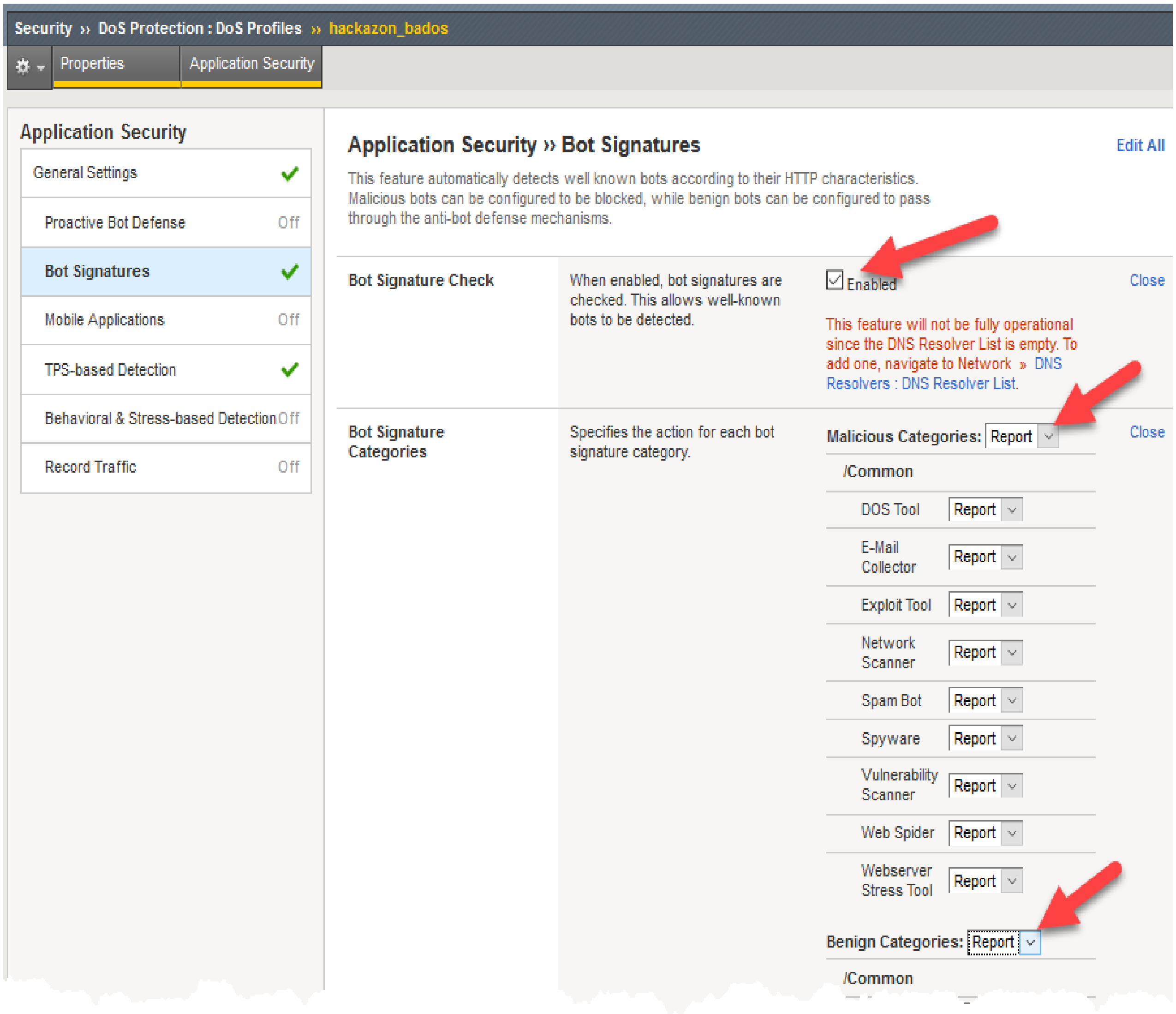
Application Security ›› General Settings

Application Security	Enable this setting to protect your web application against DoS attacks.	Disabled	Edit

Tip: At any point you can save your changes by hitting the **Update** button in the lower left-hand corner

6. Select the **Bot Signatures** section, then select the **Edit** link to the right of **Bot Signature Check**, and check the **Enabled** box.

   Select **Edit** next to **Bot Signature Categories** then change both the **Malicious Categories** and **Benign Categories** to **Report**. This step is necessary because the tools used to generate baseline and attack traffic in this lab will both be categorized as bots.



Security » DoS Protection : DoS Profiles » hackazon_bados

Properties | Application Security

Application Security

General Settings	✓
Proactive Bot Defense	Off
Bot Signatures	✓
Mobile Applications	Off
TPS-based Detection	✓
Behavioral & Stress-based Detection	Off
Record Traffic	Off

Application Security » Bot Signatures Edit All

This feature automatically detects well known bots according to their HTTP characteristics. Malicious bots can be configured to be blocked, while benign bots can be configured to pass through the anti-bot defense mechanisms.

Bot Signature Check — When enabled, bot signatures are checked. This allows well-known bots to be detected. — ☑ Enabled — Close

This feature will not be fully operational since the DNS Resolver List is empty. To add one, navigate to Network » DNS Resolvers : DNS Resolver List.

Bot Signature Categories — Specifies the action for each bot signature category. — Close

Malicious Categories: Report

/Common

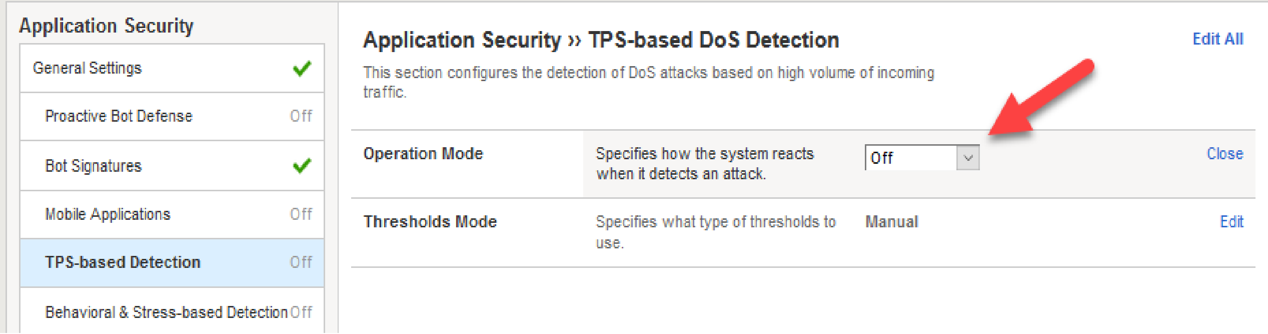
DOS Tool	Report
E-Mail Collector	Report
Exploit Tool	Report
Network Scanner	Report
Spam Bot	Report
Spyware	Report
Vulnerability Scanner	Report
Web Spider	Report
Webserver Stress Tool	Report

Benign Categories: Report

/Common

Attention: The message in red below the **Enabled** box indicates a DNS Resolver has not been set up. The DNS resolver is used to perform DNS reverse lookups as part of bot identity validation, but is not relevant for this lab exercise.

7. Select **TPS-base DoS Detection** and change **Operation Mode** to **Off**.



Application Security

General Settings	✓
Proactive Bot Defense	Off
Bot Signatures	✓
Mobile Applications	Off
TPS-based Detection	Off
Behavioral & Stress-based Detection	Off

Application Security » TPS-based DoS Detection Edit All

This section configures the detection of DoS attacks based on high volume of incoming traffic.

Operation Mode	Specifies how the system reacts when it detects an attack.	Off	Close
Thresholds Mode	Specifies what type of thresholds to use.	Manual	Edit

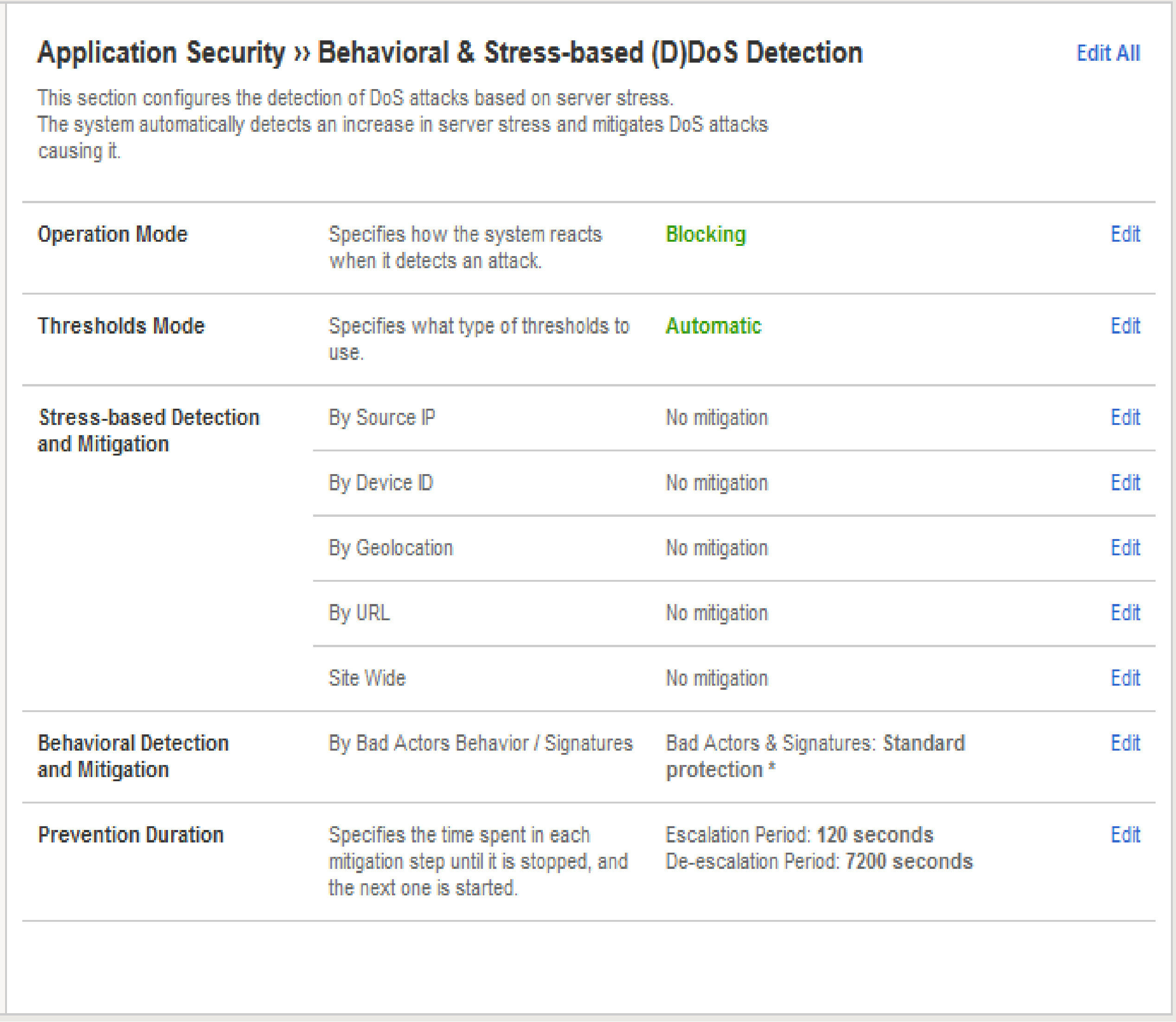
8. Select **Behavioral & Stress-based Detection** and change **Operation Mode** to **Blocking**.

   (a) Set the **Thresholds Mode** to **Automatic**.

   (b) Under **Stress-based Detection and Mitigation** edit **By SourceIP** and uncheck **Request Blocking.** Under **By URL** uncheck **Heavy URL Protection** and **Request Blocking**.

   (c) Under **Behavioral Detection and Mitigation** check the **Request signatures detection** and set the **Mitigation** to **Standard**. For now, please leave **bad actors detection** unchecked.

   (d) Click **Update** in the lower left-hand corner. Collapse all the sections, and **Behavioral & Stress-based Detection** should match the figure below.



Application Security » Behavioral & Stress-based (D)DoS Detection

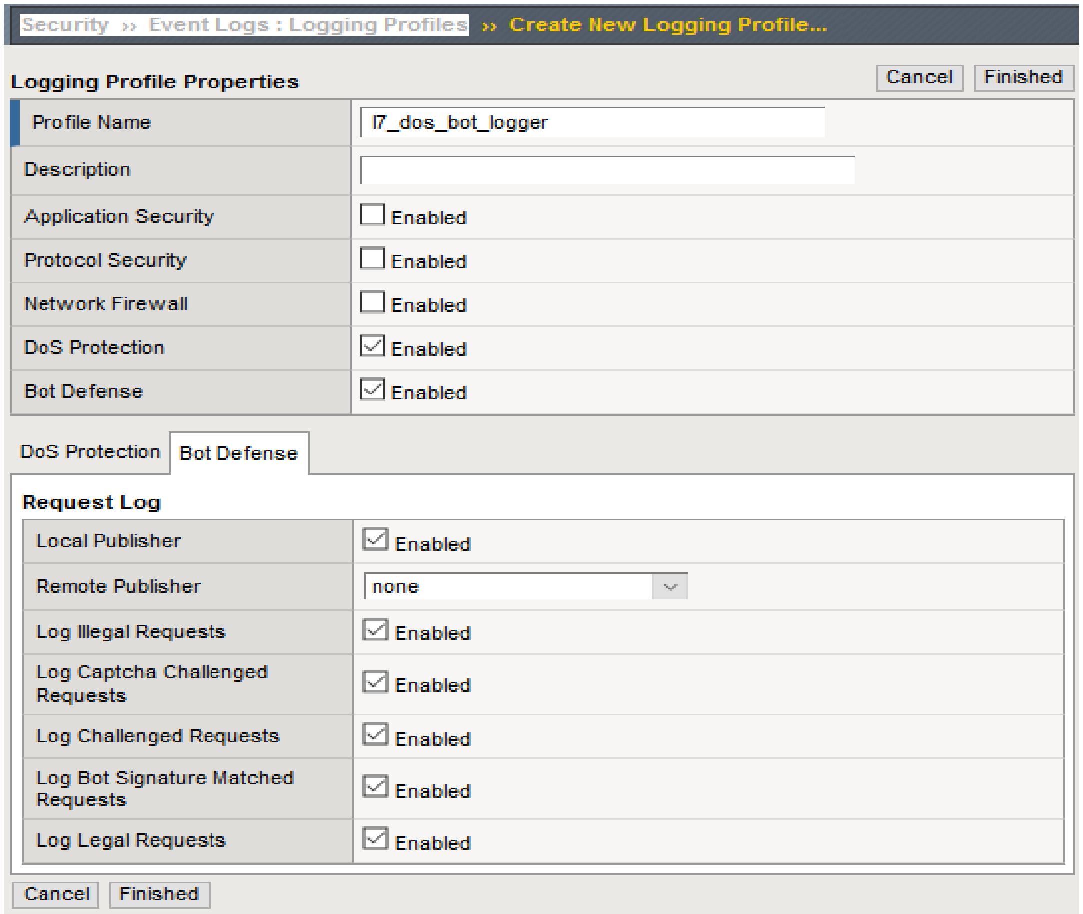
This section configures the detection of DoS attacks based on server stress.
The system automatically detects an increase in server stress and mitigates DoS attacks causing it.

Operation Mode	Specifies how the system reacts when it detects an attack.	Blocking	Edit
Thresholds Mode	Specifies what type of thresholds to use.	Automatic	Edit
Stress-based Detection and Mitigation	By Source IP	No mitigation	Edit
	By Device ID	No mitigation	Edit
	By Geolocation	No mitigation	Edit
	By URL	No mitigation	Edit
	Site Wide	No mitigation	Edit
Behavioral Detection and Mitigation	By Bad Actors Behavior / Signatures	Bad Actors & Signatures: Standard protection *	Edit
Prevention Duration	Specifies the time spent in each mitigation step until it is stopped, and the next one is started.	Escalation Period: 120 seconds De-escalation Period: 7200 seconds	Edit

8.2.2 Create a DoS Logging Profile

Logging profiles are required to enable local and remote logging for Application DoS and Bot events. In this lab, we will use local logging to review events. Below are the steps to configure the logging profile and attach to your test virtual server.

1. Go to **Security** ›› **Event Logs : Logging Profiles** and click **Create** on right-hand side of the configuration screen. Name your profile **l7_dos_bot_logger** then check the **DoS Protection** and **Bot Defense** enable boxes.
2. From the **DoS Protection** tab enable the **Local Publisher**.
3. From the **Bot Defense** tab check ALL the boxes.
4. Click **Finished**.


Security ›› Event Logs : Logging Profiles ›› Create New Logging Profile...
Cancel
Finished

Logging Profile Properties

Profile Name	l7_dos_bot_logger
Description	
Application Security	□ Enabled
Protocol Security	□ Enabled
Network Firewall	□ Enabled
DoS Protection	☑ Enabled
Bot Defense	☑ Enabled

DoS Protection
Bot Defense

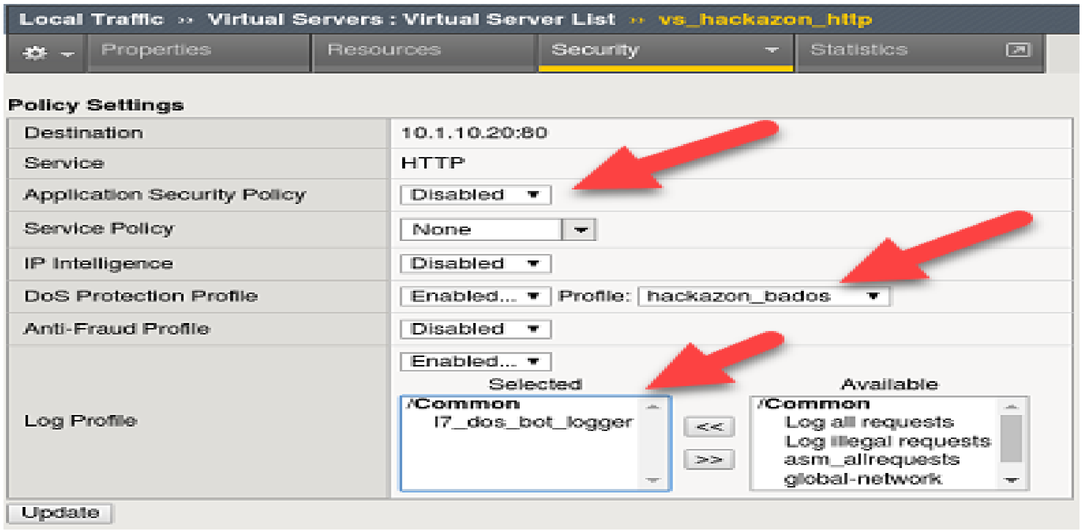
Request Log

Local Publisher	☑ Enabled
Remote Publisher	none
Log Illegal Requests	☑ Enabled
Log Captcha Challenged Requests	☑ Enabled
Log Challenged Requests	☑ Enabled
Log Bot Signature Matched Requests	☑ Enabled
Log Legal Requests	☑ Enabled

8.2.3 Add the DoS profile to a virtual server

Below are the steps to associate this profile with the Local Traffic Manager virtual server processing the application traffic in this lab.

1. Navigate to **Local Traffic > Virtual Servers > Virtual Server List** and select **vs_hackazon_http**. Under the **Security** tab on the top bar select **Policies**.
2. Enable the **DoS Protection Profile** and select the **hackazon_bados** profile.
3. Add **l7_dos_bot_logger** to the **Log Profile** and **Update**
4. For purposes of this lab, **Disable** the **Application Security Policy** and remove **asm_allrequests** from the **Log Profile.**



Local Traffic ›› Virtual Servers : Virtual Server List ›› vs_hackazon_http

Policy Settings

Destination	10.1.10.20:80
Service	HTTP
Application Security Policy	Disabled ▾
Service Policy	None ▾
IP Intelligence	Disabled ▾
DoS Protection Profile	Enabled... ▾ Profile: hackazon_bados ▾
Anti-Fraud Profile	Disabled ▾
Log Profile	Enabled... ▾ Selected: /Common l7_dos_bot_logger << >> Available: /Common Log all requests, Log illegal requests, asm_allrequests, global-network

Update

8.2.4 Create XFF-Mixed_Attacker iRule

Because we do not have dozens of good and bad source IPs available for clients and attackers in this environment, we simulate them by adding an iRule to the virtual server. The iRule adds a randomized X-Forwarded-For (XFF) header to each request.

1. Navigate to **Local Traffic** ›› **iRules** : **iRule List** and select **Create.** Name a new iRule named **XFF_mixed_Attacker_Good_iRule.** Copy and paste the iRule below.

```
when HTTP_REQUEST {
    # Good traffic
     if { [IP::addr [IP::client_addr] equals 10.1.10.52] } {
        set xff 153.172.223.[expr int(rand()*100)]
        HTTP::header insert X-Forwarded-For $xff
    }

    # Attack traffic
     if { [IP::addr [IP::client_addr] equals 10.1.10.53] } {
        set xff 132.173.99.[expr int(rand()*25)]
        HTTP::header insert X-Forwarded-For $xff
    }
 }
```

Advanced Web Application Firewall/Application Security Manager will honor the X-Forwarded-For header by enabling this in the http profile.

8.2.5 Create HTTP Profile to Accept X-Forwarded-For HTTP Header

1. Navigate to **Local Traffic** ›› **Profiles** : **Services** : **HTTP** and click **Create**. Name the new http profile **xff_http**, and click the rightmost checkbox in the row **Accept XFF** to enable a custom setting, then click the checkbox to the immediate right of **Accept XFF** to enable processing of an inbound X-Forwarded-For header.
2. Click **Finished** button at bottom of configuration page.

Tip: Due to a large number of service profiles, occasionally part of the Services menu will get stuck under the browser menu. If that happens, click on **Profiles** on the side-bar, then click **Services** in the top navigation bar to get to the HTTP profile.

8.2.6 Attach iRule and HTTP Profile to Local Traffic Manager Virtual Server

1. Navigate to the **vs_hackazon_http** virtual server. In the **Properties** tab, under **Configuration** section, select **xff_http** for the **HTTP Profile**.
2. Click the **Resources** tab in the virtual server navigation bar, in the **iRules** section select the **Manage** button, and move the **XFF_mixed_Attacker_Good_iRule** from the **Available** to the **Enabled** box.
3. Click **Finished** button at bottom of the Resource Management page.

8.2.7 Generate Traffic to Establish Baseline

Advanced Web Application Firewall's Behavioral DoS feature is based on learning and analyzing all traffic to the web application, building baselines, and then idenitifying anamolies when server stress is detected. As a result, in this lab, we need to generate normal traffic allowing Advanced Web Application Firewall to build a baseline.

You will use the Xubuntu Jumpbox to generate legitimate traffic and bad traffic, eth1 has 10.1.10.51-55 configured and 10.1.10.52 will be the source-IP used for the good traffic script. The source IP will match XFF_mixed_Attacker_Good_iRule created above, and an X-Forwarded-For header will be placed in the HTTP request in the 153.172.223.0/24 IP address range.

In the home directory (/home/f5student) on the Xubuntu Jumpbox, you will find the two scripts used for this lab:

- **baseline_menu.sh** - is used to create baseline traffic
- **AB_DOS.sh** - is used to launch L7 DOS attacks

1. Start baseline traffic, using Xubuntu Jumpbox Terminal application, navigate to the home directory, then type:

```
f5student@xjumpbox~$ ./baseline_menu.sh

- Select option 2 **alternate** and keep it running in the window
```

Tip: This is your valid traffic, and the number of requests will change over time. The requests also change as the script continuously alters the User-Agent header and the requested URI. Both values are randomly taken from files in the "source" directory in the home directory.

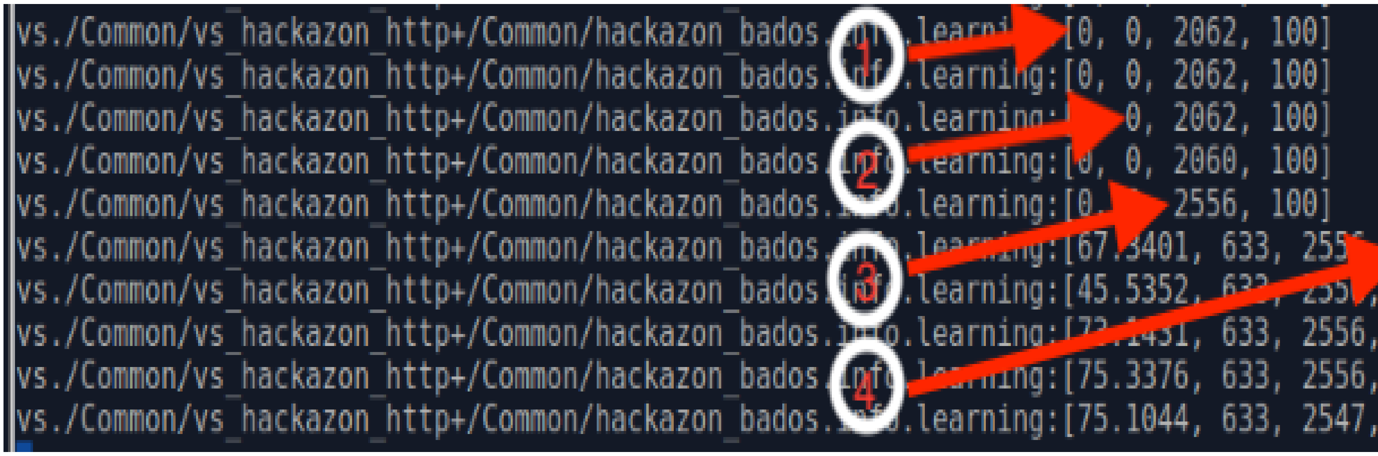
2. Next, validate you are seeing the traffic, and Advanced Web Application Firewall is actively building learning baselines. From a separate Terminal window type:

```
f5student@xjumpbox$~ ssh root@10.1.1.245
```

Then, run the following command:

```
[root@bigipo01:Active:Standalone] config # admd -s vs./Common/vs_hackazon_
↪http+/Common/hackazon_bados.info.learning

- /Common/vs_hackazon_http  - is the name of the virtual server
- /Common/hackazon_bados     - is the name of the DoS profile.
**It may take several minutes for baseline numbers to be generated**
```

Screenshot of sample output below:



```
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[0, 0, 2062, 100]
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[0, 0, 2062, 100]
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[0, 0, 2062, 100]
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[0, 0, 2060, 100]
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[0, 0, 2556, 100]
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[67.3401, 633, 2556
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[45.5352, 633, 2556,
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[7[illegible].1431, 633, 2556,
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[75.3376, 633, 2556,
vs./Common/vs_hackazon_http+/Common/hackazon_bados.info.learning:[75.1044, 633, 2547,
```

Tip: If your aren't getting any output, or seeing no signs of accumulated signals, verify the name of the virtual server and profile in the admd command are accurate.

1. **baseline_learning_confidence**:
   - **Description**: in % how confident the system is in the baseline learning.
   - **Desired Value**: > 90%
2. **learned_bins_count**:
   - **Description**: number of learned bins
   - **Desired Value**: > 0
3. **good_table_size**:
   - **Description**: number of learned requests
   - **Desired Value**: > 2000
4. **good_table_confidence**:
   - **Description**: how confident, as %, the system is in the good table
   - **Desired Value**: Must be 100 for signatures

Note: It may take 5 or more minutes before you begin to get learned baseline numbers. Also, the desired values are the minimum values we would like to see prior to triggering attacks as part of this lab exercise. You can, however, move onto module 3 and 4 in this lab while baselines are being established. **Do not stop baseline traffic script**

To see all of the values available and wide range of interesting statistics, enter the following command from BIG-IP console:

```
admd -s vs./Common/vs_hackazon_http
```

To view Advanced Web Application Firewall layer 7 DoS log, enter the following command from BIG-IP console:

```
tail -f /var/log/dosl7/dosl7d.log
```

Note: The goal of this module is to explain DoS profile configuration options. The module does not contain any exercises. If you are already familar with a the settings in an Application Security DoS profile you can skip to module 4.

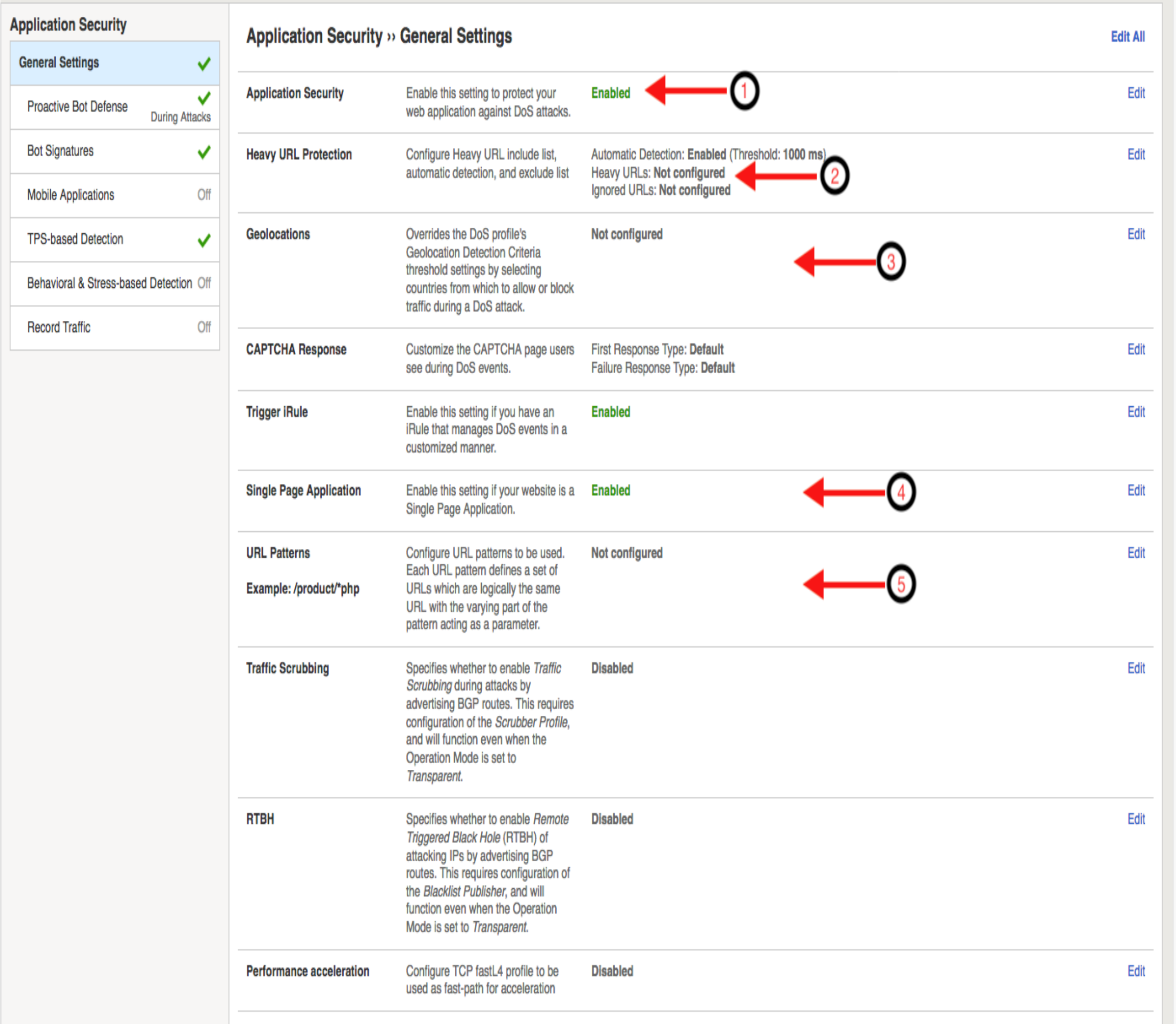
8.3 Application Security DoS Profiles

In this module, we will review the various settings and options that make up a layer 7 DoS profile. We will not review each and every setting, leaving that exercise up to the reader, but instead will focus on key settings which will most likely require attention during a production deployment. More detail on each individual setting can be found by viewing the **Help** on left side of the BIG-IP Configuration Utility (GUI).

8.3.1 Review DoS Profile General Settings

Navigate to **Security** ›› **DoS Protection** ›› **DoS Profiles** and click the DoS profile **hackazon_bados** created earlier for this module.

Settings in this screen are profile wide, and can affect all aspects of the dos configuration.



Application Security

General Settings	✓
Proactive Bot Defense	✓ During Attacks
Bot Signatures	✓
Mobile Applications	Off
TPS-based Detection	✓
Behavioral & Stress-based Detection	Off
Record Traffic	Off

Application Security ›› General Settings

Edit All

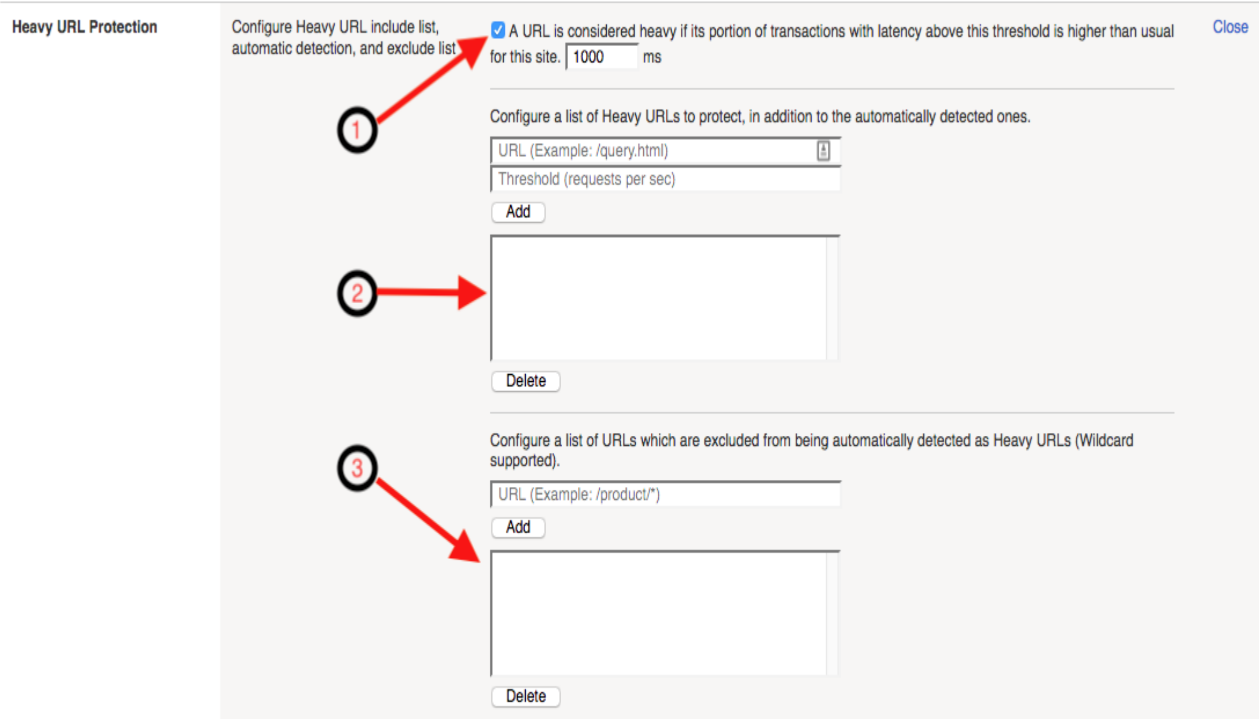
Application Security	Enable this setting to protect your web application against DoS attacks.	Enabled	Edit
Heavy URL Protection	Configure Heavy URL include list, automatic detection, and exclude list	Automatic Detection: **Enabled** (Threshold: **1000 ms**) Heavy URLs: **Not configured** Ignored URLs: **Not configured**	Edit
Geolocations	Overrides the DoS profile's Geolocation Detection Criteria threshold settings by selecting countries from which to allow or block traffic during a DoS attack.	Not configured	Edit
CAPTCHA Response	Customize the CAPTCHA page users see during DoS events.	First Response Type: **Default** Failure Response Type: **Default**	Edit
Trigger iRule	Enable this setting if you have an iRule that manages DoS events in a customized manner.	Enabled	Edit
Single Page Application	Enable this setting if your website is a Single Page Application.	Enabled	Edit
URL Patterns Example: /product/*php	Configure URL patterns to be used. Each URL pattern defines a set of URLs which are logically the same URL with the varying part of the pattern acting as a parameter.	Not configured	Edit
Traffic Scrubbing	Specifies whether to enable *Traffic Scrubbing* during attacks by advertising BGP routes. This requires configuration of the *Scrubber Profile*, and will function even when the Operation Mode is set to *Transparent*.	Disabled	Edit
RTBH	Specifies whether to enable *Remote Triggered Black Hole* (RTBH) of attacking IPs by advertising BGP routes. This requires configuration of the *Blacklist Publisher*, and will function even when the Operation Mode is set to *Transparent*.	Disabled	Edit
Performance acceleration	Configure TCP fastL4 profile to be used as fast-path for acceleration	Disabled	Edit

1. **Application Security**

   This setting enables or disables the DoS profile.

2. **Heavy URL Protection**

   Heavy URL's are application resources which may consume more backend resources with each client request. Additionally, URLs which are not generally considered heavy may become heavy under significant load or attack. As a result, low rate requests targeting these URLs can cause significant DoS attacks, and be difficult to differentiate from legitimate requirements based on rate alone. Advanced Web Application Firewall automatically detects heavy URLs by measuring the latency tail ratio, which is the number of transactions whose latency is consistently greater than the latency threshold defined in this configuration option. A URL is considered heavy if its latency is more than two times the site global average over a 24 hour (default) period.



Heavy URL Protection

Configure Heavy URL include list, automatic detection, and exclude list

☑ A URL is considered heavy if its portion of transactions with latency above this threshold is higher than usual for this site. 1000 ms

Configure a list of Heavy URLs to protect, in addition to the automatically detected ones.

URL (Example: /query.html)

Threshold (requests per sec)

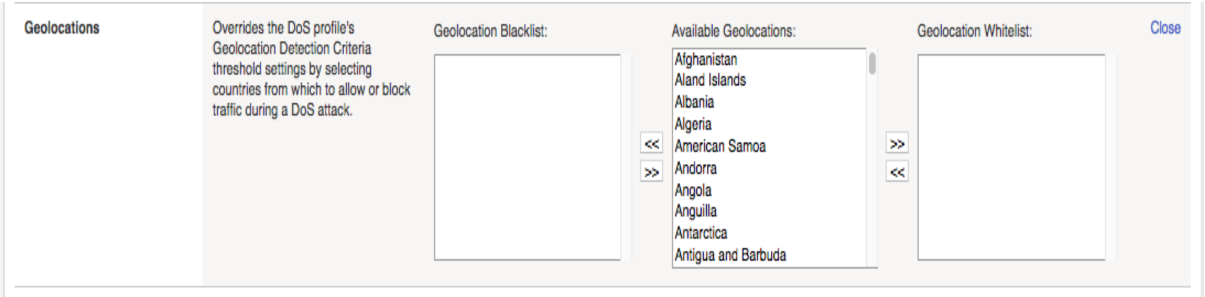
Configure a list of URLs which are excluded from being automatically detected as Heavy URLs (Wildcard supported).

URL (Example: /product/*)

1. Checkbox, enables or disables, automatic detection of the heavy URLs profile-wide. The text box allows for configuration of the baseline threshold that URLs must exceed before being considered for heavy URL determination.
2. This section of the DoS Profile Heavy URL configuration allows an administrator to explictly configure a URL(s) as heavy, whether it is detected as heavy by Advanced Web Application Firewall or not. Use this section to define application resources which are known to be heavier in terms of resource consumption, or known to be less resilient to higher volumes of traffic than the rest of the application.
3. This section of the Dos Profile Heavy URL configuration allows an administrator to explictly configure URL(s) and wildcard URL patterns to be excluded from automatic heavy URL detection. Use this section, to identify URL's which you know may perform slower than average under normal conditions, or URLs you do not wish to have Advanced Web Application Firewall offering heavy URL protection.

Note: To provide mitigation for heavy URLs, you must enable at least one of the URL-based prevention policy methods in the TPS or Stress-based Anomaly sections of the DoS profile.

3. **Geolocations** Geolocations provides options to override the dos profile geolocation detection criteria by explicity whitelisting or blacklisting specific geolocations.



Geolocations

Overrides the DoS profile's Geolocation Detection Criteria threshold settings by selecting countries from which to allow or block traffic during a DoS attack.

4. **Single Page Application** Single Page Applications (SPA) represent a change in application architecture that moves much of the content rendering and routing to client-side code. Application requests which require server-side processing are sent as AJAX requests towards server, and the response is typically JSON/XML; this is different from traditional web applications that send HTTP requests, and generally levergage HTML as the predominant response content type. As a result, Advanced Web Application Firewall needs to modify the way it challenges clients for features like Proactive Bot Defense and capturing Device ID in the TPS/Stress based anomaly detections. Enabling this option modifies Advanced Web Application Firewall's challenge and challenge validation mechanisms. When deploying L7 DoS protections it is important to understand the application architecture, and if protecting a SPA, enabling this option is critical for proper operation.

Note: The goal of this module is to explain the Stress-Based and Behavioral DoS configuration options. The module does not contain any exercises. If you are already familar with a the settings you can skip to module 5.

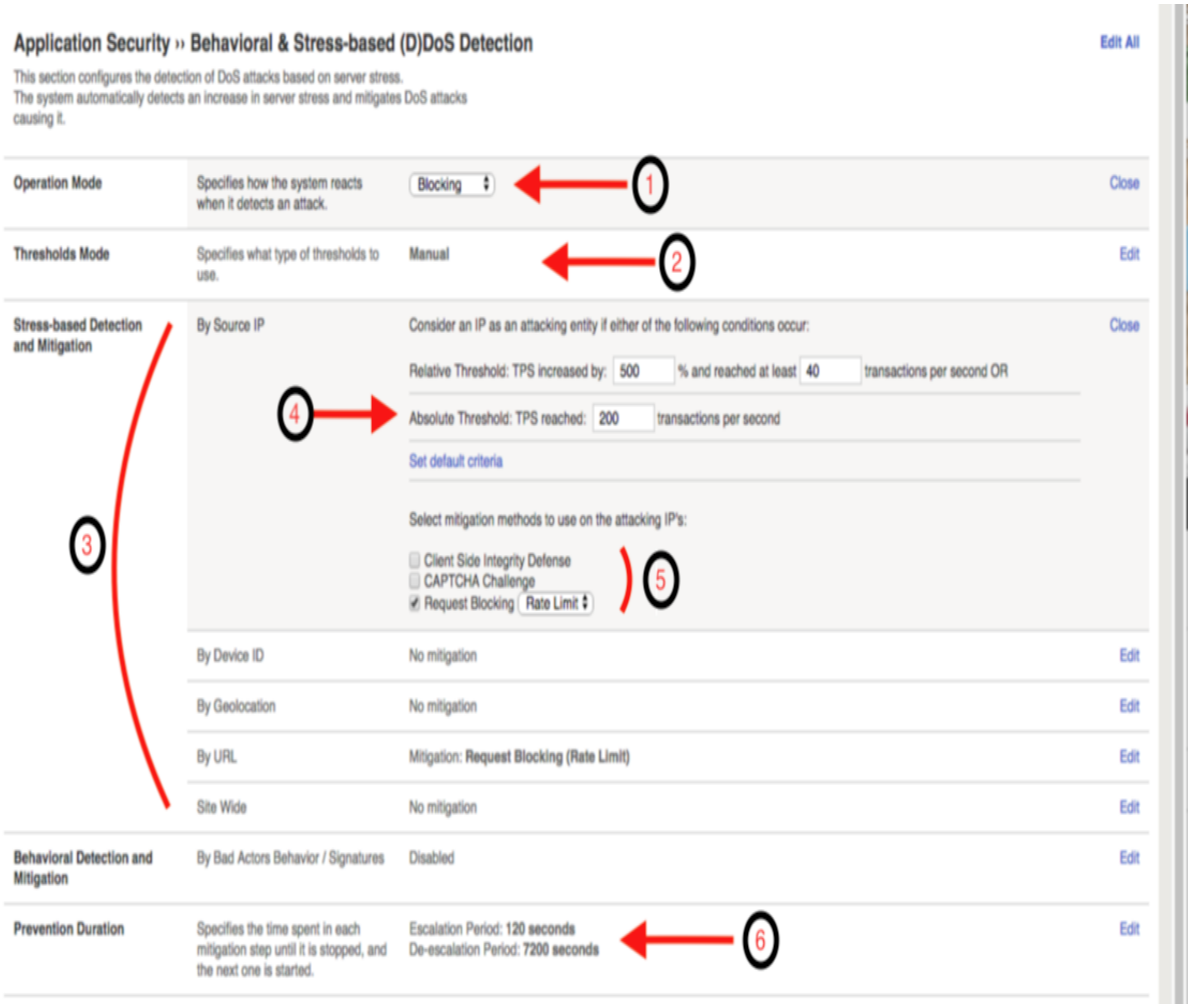
8.4 Stress-Based and Behavioral DoS Profile Settings

In this module, we will review the various settings for configuring Stress-based and Behavioral DoS protections in more detail. We will not review each and every setting, leaving that exercise up to the reader, but instead will focus on key settings which will most likely require attention during a production deployment. More detail on each individual setting can be found by viewing the **Help** on left side of the BIG-IP Configuration Utility (GUI).

8.4.1 Review Stress-Based Dos Profile Settings

To appreciate the powerful nature of Advanced Web Application Firewall's Behavioral DoS feature, it first makes sense to analyze one of the other L7 DoS protection mechanisms. For this exercise, we will examine the options and behaviors of the Stress-based DoS protections available in an Application Security DoS profile.

To review the settings below, navigate to **Security ›› DoS Protection ›› DoS Profiles**, click the DoS profile **hackazon_bados** created earlier for this module, then click **Behavioral & Stress-based Detection** in the **Application Security** navigation menu, and set the **Operation Mode** to **Transparent**.



Application Security ›› Behavioral & Stress-based (D)DoS Detection Edit All

This section configures the detection of DoS attacks based on server stress. The system automatically detects an increase in server stress and mitigates DoS attacks causing it.

Operation Mode	Specifies how the system reacts when it detects an attack.	Blocking	Close
Thresholds Mode	Specifies what type of thresholds to use.	**Manual**	Edit
Stress-based Detection and Mitigation	By Source IP	Consider an IP as an attacking entity if either of the following conditions occur: Relative Threshold: TPS increased by: 500 % and reached at least 40 transactions per second OR Absolute Threshold: TPS reached: 200 transactions per second Set default criteria Select mitigation methods to use on the attacking IP's: ☐ Client Side Integrity Defense ☐ CAPTCHA Challenge ☑ Request Blocking Rate Limit	Close
	By Device ID	No mitigation	Edit
	By Geolocation	No mitigation	Edit
	By URL	Mitigation: **Request Blocking (Rate Limit)**	Edit
	Site Wide	No mitigation	Edit
Behavioral Detection and Mitigation	By Bad Actors Behavior / Signatures	Disabled	Edit
Prevention Duration	Specifies the time spent in each mitigation step until it is stopped, and the next one is started.	Escalation Period: **120 seconds** De-escalation Period: **7200 seconds**	Edit

1. **Operation Mode** Defines the operational mode for the stress-based dos protection feature. Available options include: Blocking, Transparent, Off. Blocking means feature will detect, report, and mitigate. Transparent means feature will detect, report, but will not mitigate. Off means the feature is disabled.
2. **Threshold Mode** Defines how Advanced Web Application Firewall derives thresholds to be used in detecting the TPS component of a stress-based attack. Options include:
   - **Manual**: Administrator explicity configures TPS and percentage thresholds based on their knowledge of the environment or specific requirements.
   - **Automatic**: Advanced Web Application Firewall monitors traffic rates automatically and calculates the thresholds based on normal traffic volume to the application.
3. **Stress-based Detection Options** Advanced Web Application Firewall can trigger an attack if any/all of the following detection methods exceed the thresholds defined or calculated for the detection method:
   - **By Source IP**: A specific source IP has exceeded the thresholds defined in the detection thresholds.
   - **By Device ID**: A specific device has exceeded the thresholds defined in the detection thresholds. Device ID is ASM calculating a fingerprint for a given device. The feature requires Javascript injection for proper operation. However, the feature offers the benefit of detecting a specific

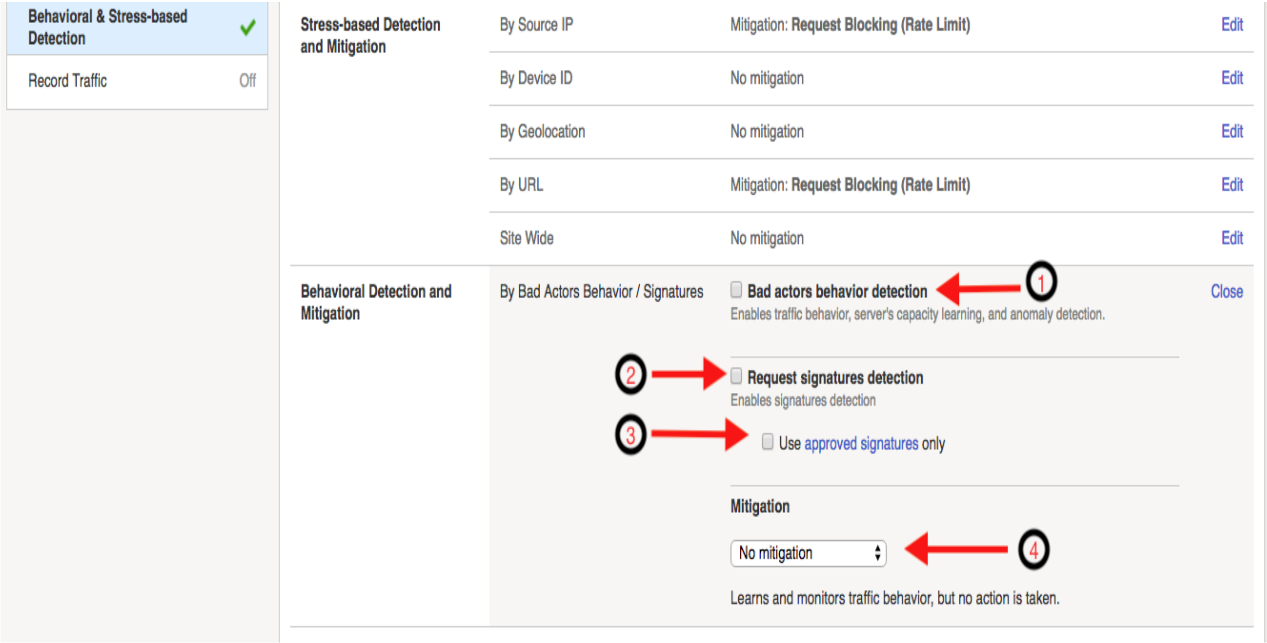
device, even if the attack varies its source IP address.

- **By Geolocation**: A country/geolocation has exceeded the thresholds defined in the detection thresholds.
- **By URL**: Request traffic to a specific (or set of URL's identified in URL patterns section of the DoS Profile General Properties) has exceeded the thresholds defined in the detection thresholds.
- **Site Wide**: Request traffic to the entire web site has exceeded the thresholds defined in the detection thresholds, **and** an attack has not been detected using any of the other detection criteria. Site-wide is considered last resort.

Note: It is important to understand that while stress-based protections are monitoring server latency, and tracking application request volume in short and long term intervals, the detection methods listed above are the only ways to identify when an attack is on-going. This, as you will see, is quite a bit different than they way Advanced Web Application Firewall Behavioral DoS feature identifies attacks and attackers!

8.4.2 Review Behavioral DoS Settings

Having reviewed the options for configuring Stress-based dos mitigation, now let's examine the options required for configuring Advanced Web Application Firewall's Behavioral DOS mitigations.



Behavioral & Stress-based Detection ✓

Record Traffic Off

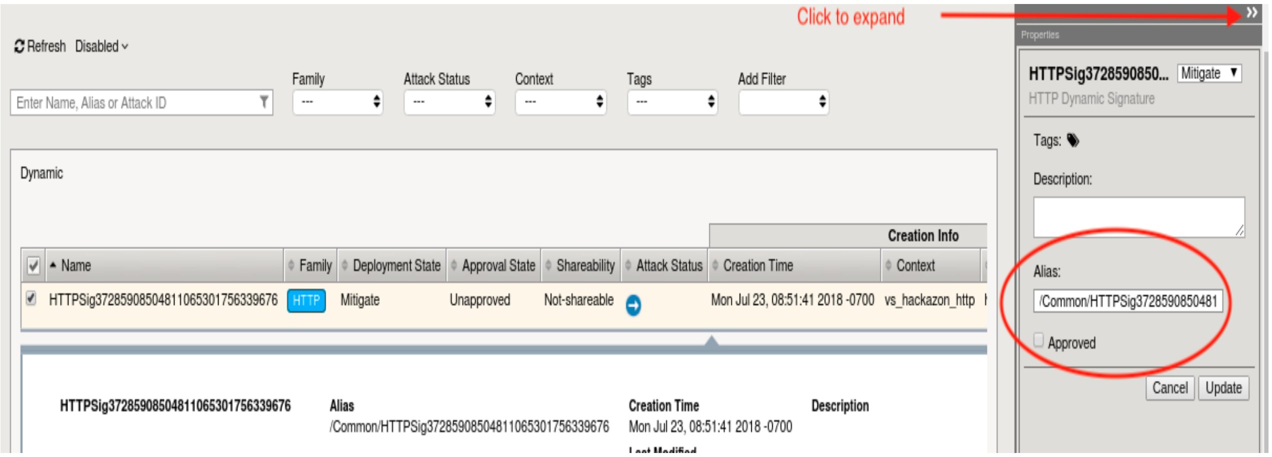
Stress-based Detection and Mitigation	By Source IP	Mitigation: **Request Blocking (Rate Limit)**	Edit
	By Device ID	No mitigation	Edit
	By Geolocation	No mitigation	Edit
	By URL	Mitigation: **Request Blocking (Rate Limit)**	Edit
	Site Wide	No mitigation	Edit
Behavioral Detection and Mitigation	By Bad Actors Behavior / Signatures	□ **Bad actors behavior detection** (1) Enables traffic behavior, server's capacity learning, and anomaly detection. (2) □ **Request signatures detection** Enables signatures detection (3) □ Use approved signatures only **Mitigation** No mitigation (4) Learns and monitors traffic behavior, but no action is taken.	Close

1. **Bad Actors Behavior Detection** Determines whether Behavioral DoS engine tracks and attempts to identify the bad actors contributing to a given set of malicious traffic. When Bad Actor Behavior Detection is enabled, once Advanced Web Application Firewall detects server stress and identifies a set of malicious traffic contributing to the server stress, the Behavioral DoS engine then attempts to identify what source IP addresses are generating the malicious traffic, and what percentage of malicious traffic a given bad actor is contributing. Bad actors, are mitigated at transport layer via slowdown mitigation techniques, and the rate at which they are mitigated is directly related to their percentage of contribution to the malicious traffic set, and the migitation mode selected.

2. **Request Signature Detection** Determines whether Behavioral DoS engine will attempt to generate a traffic signature to block anamolous traffic. Advanced Web Application Firewall Behavioral DoS feature is in a permanent learning state, always tracking application requests, and the construction of these requests, and then comparing to an evolving baseline. When Request Signatures Detection is enabled, once Advanced Web Application Firewall detects server stress, it looks to identify traffic characteristics which have deviated from the baseline. If there are deviating characteristics, the Behavioral DoS engine, then dynamically generates a signature based on these deviating characteristics to block anamolous traffic.

   > **Note:** In addition to generating signatures the Behavioral DoS Engine also continually evaluates the signature for efficacy, minimizing the risk of signature becoming false positive and blocking known good traffic.

3. **Use Approved Signatures Only** By default, when Request Signatures Detection is enabled, Advanced Web Application Firewall will generate and use dynamically generated attack signatures as defined by the mitigation mode selection. By enabling this option, the administrator overrides this behavior, and forces a manual step to review and approve the signature prior to any mitigations taking effect. Signatures can be reviewed from Advanced Web Application Firewall GUI via **Security** -> **DoS Protection** -> **Signatures**.

☑	Name	Family	Deployment State	Approval State	Shareability	Attack Status	Creation Time	Context
☑	HTTPSig37285908504811065301756339676	HTTP	Mitigate	Unapproved	Not-shareable	➜	Mon Jul 23, 08:51:41 2018 -0700	vs_hackazon_http

   HTTPSig37285908504811065301756339676 **Alias** /Common/HTTPSig37285908504811065301756339676 **Creation Time** Mon Jul 23, 08:51:41 2018 -0700 **Description**

   HTTPSig3728590850... Mitigate ▼
   HTTP Dynamic Signature
   Description:
   Alias: /Common/HTTPSig3728590850481
   ☐ Approved

   Once a signature has been approved, the Signature Approval State for the signature will change to “Manually-approved”. When approved signatures only is selected, only signatures which have been approved will be active.

4. **Mitigation** Defines the mitigation mode for Advanced Web Application Firewall Behavioral DoS. Options include:

   - **No Mitigation:**
     - Monitors traffic, generates signatures, and identifies bad actors, but does not perform any mitigation.
   - **Conservative Protection:**
     - **If** Bad Actors Behavior Detection is enabled, slows down bad identified bad actors.
     - **If** Request Signatures Detection is enabled, blocks requests that match attack signatures
   - **Standard Protection:**
     - **If** Bad Actors Behavior Detection is enabled, slows down bad identified bad actors.
     - **If** Request Signatures Detection is enabled, blocks requests that match attack signatures

    - Rate limits all requests based on server health
    - Limits the number of concurrent connections from bad actor IP addresses
    - If necessary, limits the number of all concurrent connections based on server health

- **Aggressive Protection:**
    - **If** Bad Actors Behavior Detection is enabled, slows down bad identified bad actors.
    - **If** Request Signatures Detection is enabled, blocks requests that match attack signatures
    - Rate limits all requests based on server health
    - Limits the number of concurrent connections from bad actor IP addresses
    - If necessary, limits the number of all concurrent connections based on server health
    - **Proactively** performs all protection actions, even before attack detection, increasing impact of protection techniques.

Advanced Web Application Firewall mitigates DoS with the most effective and efficient method available, and as quickly as possible to restore server health. Meaning, the mitigation method will often change over time as more data is learned and analyzed. For example, at the onset of an attack, Advanced Web Application Firewall may apply global rate limiting in an attempt to mitigate an onslaught of traffic. Then, as the signature engine has observed enough traffic to identify malicious traffic and generate a signature, the Behavioral DoS engine will begin mitigating with request signatures and discontinue global rate limiting. Finally, as bad actors are identified, traffic from those sources is mitigated using layer four slowdown mechanisms, and request signatures are only used for traffic matching the signature and not in the bad actor list. This approach allows Advanced Web Application Firewall to perform better under attack, and mimimizes the risk of blocking good traffic while mitigating DoS.

8.4.3 Summarizing Key Points

After reviewing several options for both Stress-based and Behavioral DoS features, the goal of this section is to call out some key points which might be overlooked when reviewing configuration options:

- All DoS features are complementary to Advanced Web Application Firewall web application firewall (WAF) and bot protection features. DoS features mitigate traffic that exceeds a certain rate or induces server-side stress. This traffic is, many times, completely legitimate traffic which will not trigger a WAF block.
- Heavy URL, TPS-based DoS, Stress-based DoS, and Behavioral DoS features can all be configured concurrently, complementing one another, or separate and independent of one another.
- Both Stress-based and Behavioral DoS protection features continually monitor application server performance for signs of server stress. Both features will consider server stress as a key component in detecting an attack, and neither will trigger a mitigation if the server is perceived to be healthy.
- Stress-based and TPS based DoS features can detect DoS attacks across a pre-defined set of detection criteria (source IP, URL, device ID, geolocation, site). Behavioral DoS is not constrained to a pre-defined set of detection criteria, but instead is a self adjusting dynamic DoS defense system which can detect DoS across hundreds of traffic predicates. As a result, Behavioral DoS, is much more effective in mitigating multi-vector layer seven DoS attacks which mutate over time. Conversely, TPS and/or Stress-based DoS features are much better at defining specific rate limits for traffic entering your application.

8.5 Request Signatures

In this module you will be initiating a L7 DDoS attack on the hackazon virtual server, from eth1, using 10.1.10.53 as the source IP address. This source IP will match XFF_mixed_Attacker_Good_iRule, and an X-Forward-For header will be inserted in the HTTP request in the 132.173.99.0/24 IP address range.

Once the attack begins the BIG-IP WAF (ASM) will immediately switch into attack mode due to the server health deteriorating almost immediately. As the server gets totally overwhelmed, you may at first notice the good script dropping requests. *That's why BaDoS first mitigates with a global rate limit just to protect the server*. In a short time, the good script will go back to all 200 OK responses. During this time Behavioral DoS identifies anamolous traffic and generates **Dynamic Signatures** matching only the malicious traffic. Once mitigation is in effect, the server health will rapidly improve and application performance will return to normal.

1. Using Chromium Browser on the Xubuntu Jumpbox, open tab to the GUI on bigip01 (https://10.1.1.245)

2. Navigate to **Security** ›› **DoS Protection:Signatures** and click on the **Dynamic** box, then set the **Refresh** value to **20 secs**.

3. Open another tab/window in Chromium Browser, and go to **Security** ››**Reporting : DoS : Dashboard**. The dashboard is NOT real time in may take up to 10 minutes for traffic to display.

4. Revisit the Terminal window you opened earlier which is monitoring behavioral DoS learning signals. Verify the first number (baseline_learning_confidence) is at or above 80%. Normally, above 90% would be ideal, but for the purposes of this lab over 80% will suffice.

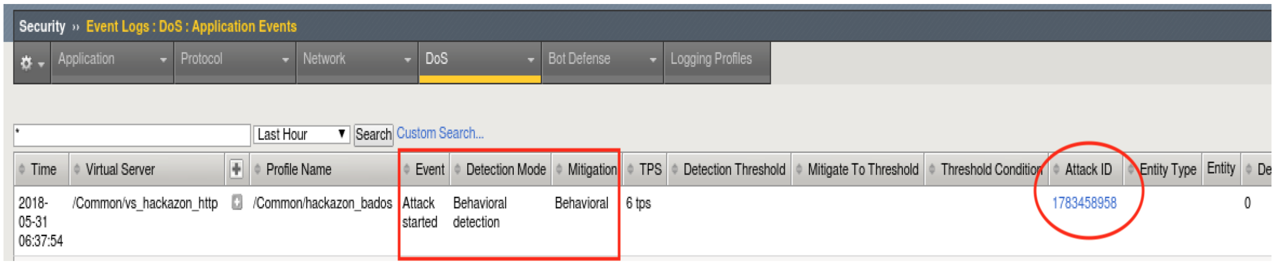
5. Revisit the Terminal window you opened earlier which is still running the baseline traffic generation script. Make note of the normal, pre-attack, response time for each request.

6. From Xubuntu Jumpbox open a NEW Terminal window. From your home directory enter:

```
f5student@xjumpbox~$ ./AB_DOS.sh

- Select **2** - Attack start - score
```

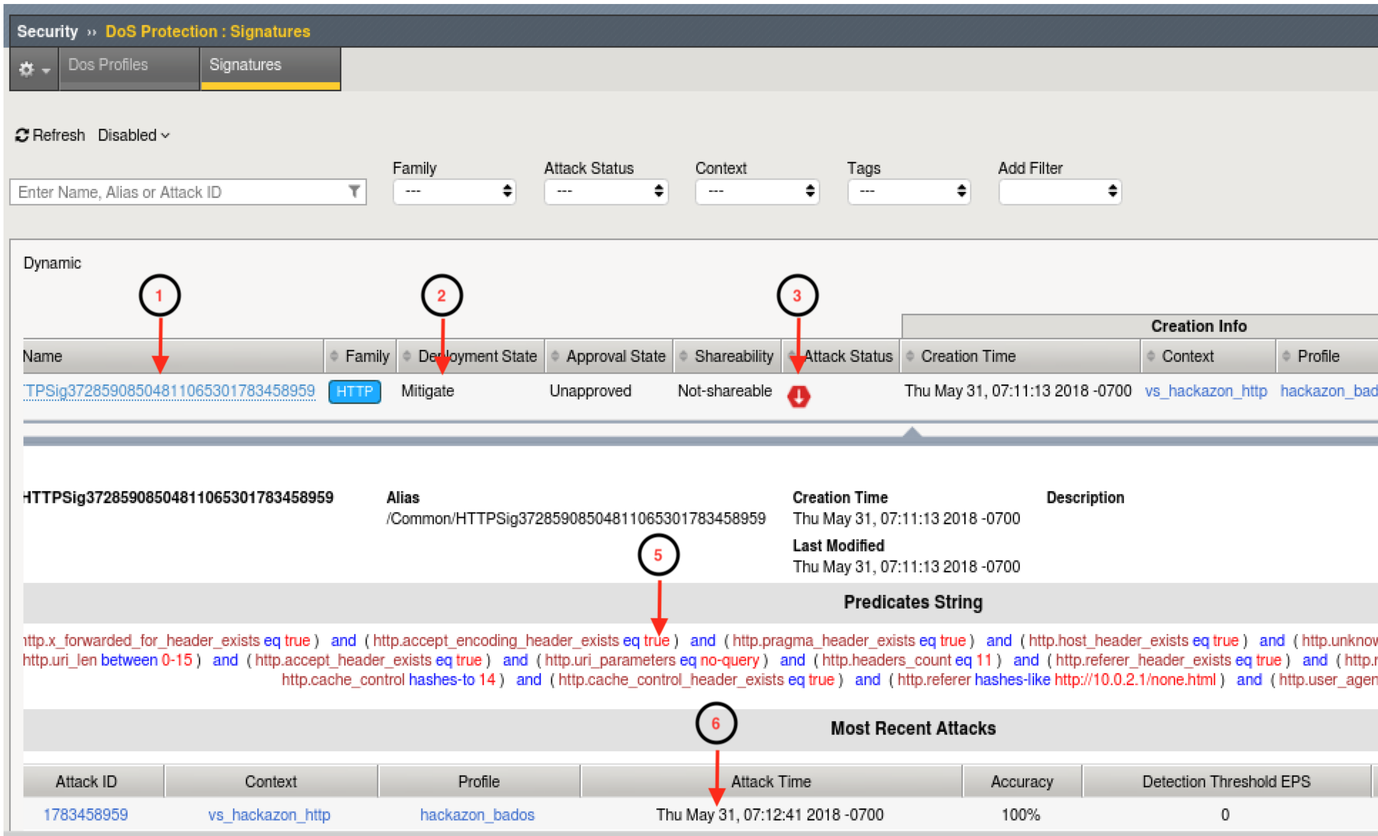
7. Using Chromium Browser on the Xubuntu Jumpbox, open another tab to the GUI on bigip01, and navigate to **Security** ›› **Event Logs** ›› **DoS** ›› **Application Events**

8. Almost immediately you should see an attack has started, and Advanced Web Application Firewall has assigned an Attack ID to the event. You will see something similar to the screenshot below:



Time	Virtual Server	+	Profile Name	Event	Detection Mode	Mitigation	TPS	Detection Threshold	Mitigate To Threshold	Threshold Condition	Attack ID	Entity Type	Entity	De
2018-05-31 06:37:54	/Common/vs_hackazon_http		/Common/hackazon_bados	Attack started	Behavioral detection	Behavioral	6 tps				1783458958			0

9. Review the **Dyanmic Signatures** UI page opened in step #2. It might take a few moments for a dynamic signature(s) to generate, but shortly after the attack has been detected a signature should be created. Once a signature(s) is generated, if you click on the signature (NOT on the blue link, but somewhere on the signature bar), you will get the details about the signature in Wireshark format. Also, you can examine the current status of the signature (mitigating or not), and statistics on recent attacks which used the signature.



Name	Family	Deployment State	Approval State	Shareability	Attack Status	Creation Time	Context	Profile
TPSig37285908504811065301783458959	HTTP	Mitigate	Unapproved	Not-shareable	⬇	Thu May 31, 07:11:13 2018 -0700	vs_hackazon_http	hackazon_bad

HTTPSig37285908504811065301783458959

Alias
/Common/HTTPSig37285908504811065301783458959

Creation Time
Thu May 31, 07:11:13 2018 -0700

Last Modified
Thu May 31, 07:11:13 2018 -0700

Description

Predicates String

ıttp.x_forwarded_for_header_exists eq true) and (http.accept_encoding_header_exists eq true) and (http.pragma_header_exists eq true) and (http.host_header_exists eq true) and (http.unknow
http.uri_len between 0-15) and (http.accept_header_exists eq true) and (http.uri_parameters eq no-query) and (http.headers_count eq 11) and (http.referer_header_exists eq true) and (http.r
http.cache_control hashes-to 14) and (http.cache_control_header_exists eq true) and (http.referer hashes-like http://10.0.2.1/none.html) and (http.user_agen

Most Recent Attacks

Attack ID	Context	Profile	Attack Time	Accuracy	Detection Threshold EPS
1783458959	vs_hackazon_http	hackazon_bados	Thu May 31, 07:12:41 2018 -0700	100%	0

- **Signature ID**: Signature ID generated for this signature. You can use the signature ID in DoS Analysis/Dashboard views (explored in module 6) to get more details on actions taken by this signature.
- **Deployment State**: current state of the signature. Options include:
  - **Mitigate** - Collect stats, learn, alert, and mitigate. All thresholds and threshold actions are applied, and rate limiting occurs if the device is under high stress.
  - **Detect Only** - Collects stats, learn, and alert. Develops dynamic signatures without enforcing any thresholds or limits.
  - **Learn Only** - Collect stats and learn. Develops dynamic signatures without enforcing any thresholds or limits
  - **Disabled** - No stat collection or mitigation, totally disables the signature.
- **Attack Status** - the state of the signature with respect to ongoing attacks. Specifically, defines whether this particular signature is being used to mitigate an on-going attack.
- **Attack ID** - the attack ID for the attack that generated this signature. Clicking the attack ID will take you to the DoS Analysis views filtered on this attack ID.
- **Predicates List** - the conditions for the request to be associated with this signature. Includes one or more match ,expresssions, joined by logical operators, which the system uses to match traffic causing a DoS attack.
- **Attack History** - provides an account of all attacks in which this signature has been used to mitigate.

Note: Dynamic Attack signatures generated will remain in the list up to the max number of signatures supported, and will be will re-used whenever an attack is detected, and traffic matches the conditions defined in the signature

10. With the attack script still running, examine the output of the baseline script. You should be getting HTTP 200 OK responses, and the response time should be inline with pre-attack response times. Also, verify you can use browse to http://hackazon.f5demo.com without issue.
11. In the window where you are running the attack script, enter **CTRL-C**, then type **4** to kill the attack script cleanly.
12. Using Chromium Browser, navigate to **Security** ›› **DoS Protection:Signatures** and click on the **Dynamic** box. Then click the check box next to the Name column to select all signatures, and click delete to remove all attack signatures created during this module.
13. Leave **baseline_menu.sh** script running.

8.6 Bad Actor Detection

In the last module, you used request signature detection to mitigate an application layer DoS attack. You also saw the Behavioral DoS engine deploy global rate limiting to bring the servers back to health while signatures were being generated, then mitigate targeted attack traffic with the newly generated signature. In this module, we will leverage Bad Actor Detection to throttle known bad actors.

1. Navigate to **Security** ›› **DoS Protection : DoS Profiles** and click the hackazon_bados profile we created earlier.
2. Click the **Application Security** tab, and then click **Behavioral & Stress-based Detection** button in the Application Security panel.
3. Click the **Edit** link to the right of the **Behavioral Detection and Mitigation** section, then check the checkbox for **Bad actors behavior detection**, and uncheck the box next to **request signatures detection**
4. Scroll down, and click the **Update** button.
5. From the Xubuntu Jumpbox open another Terminal window. Then:

```
f5student@xjumpbox$~ ssh root@10.1.1.245
```

6. From the SSH session, run the following command:

```
[root@bigipo01:Active:Standalone] config # watch ipidr -l /Common/vs_
↪hackazon_http+/Common/hackazon_bados
```

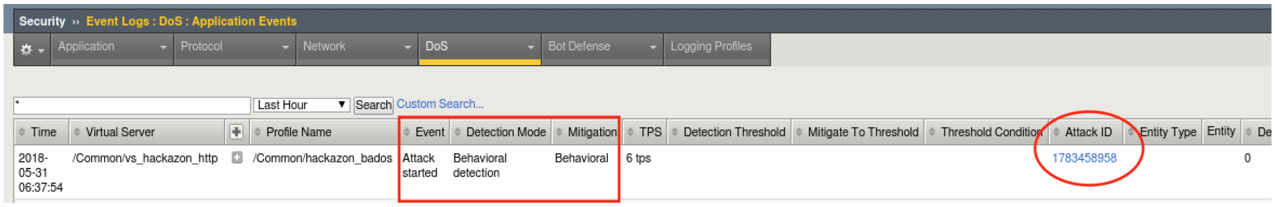
   Initially, because no attack is active, the IP list will be empty. Keep this command running in one of the Terminal windows. Things are about to change!

7. Using the Terminal window on the Xubuntu Jumpbox from the previous module, or a new one, re-run the attack script using the following command:

```
f5student@xjumpbox~$ ./AB_DOS.sh

- Select **2** - Attack start - score
```

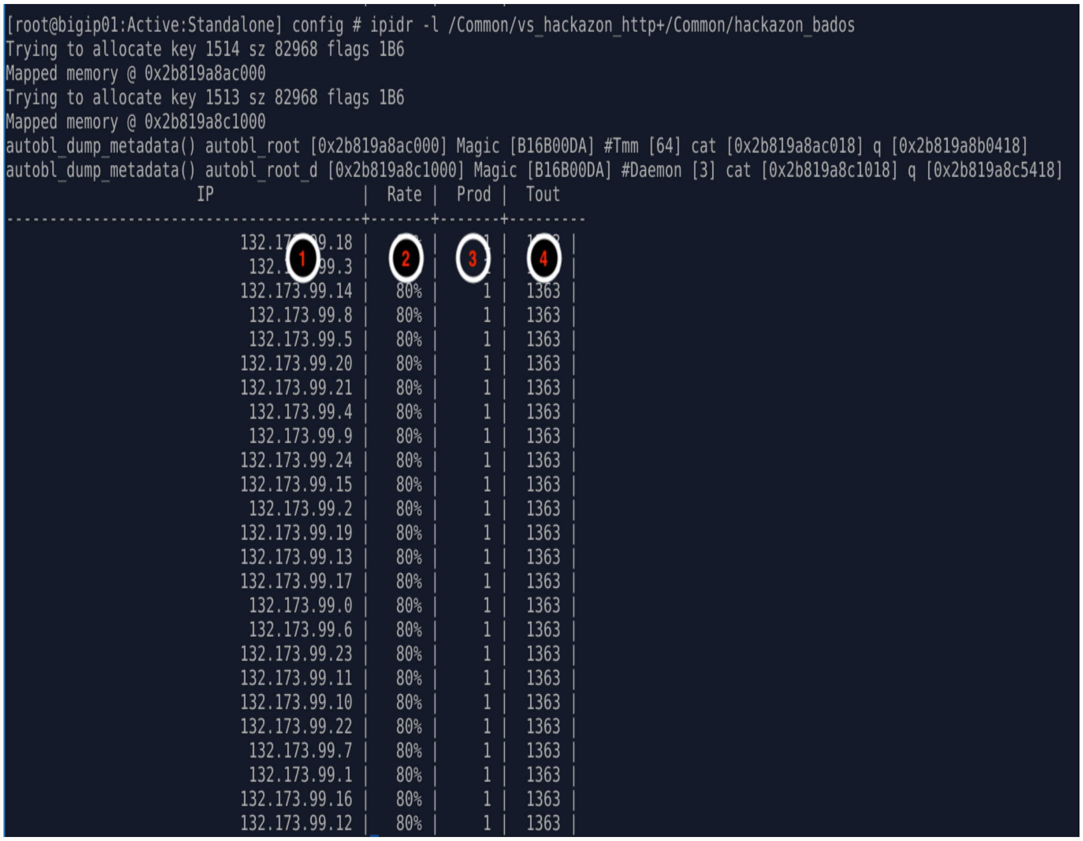
8. Using Chromium Browser on the Xubuntu Jumpbox, open another tab to the GUI on bigip01, and navigate to **Security** ›› **Event Logs** ›› **DoS** ›› **Application Events**

9. Almost immediately you should see an attack has started, and Advanced Web Application Firewall has assigned an Attack ID to the event. You will see something similar to the screenshot below:



Time	Virtual Server		Profile Name	Event	Detection Mode	Mitigation	TPS	Detection Threshold	Mitigate To Threshold	Threshold Condition	Attack ID	Entity Type	Entity	De
2018-05-31 06:37:54	/Common/vs_hackazon_http		/Common/hackazon_bados	Attack started	Behavioral detection	Behavioral	6 tps				1783458958			0

10. From the Terminal window started in step #6, monitor the output of the ipidr command, and the status of the IP greylist. You should see something similar to the image below:



```
[root@bigip01:Active:Standalone] config # ipidr -l /Common/vs_hackazon_http+/Common/hackazon_bados
Trying to allocate key 1514 sz 82968 flags 1B6
Mapped memory @ 0x2b819a8ac000
Trying to allocate key 1513 sz 82968 flags 1B6
Mapped memory @ 0x2b819a8c1000
autobl_dump_metadata() autobl_root [0x2b819a8ac000] Magic [B16B00DA] #Tmm [64] cat [0x2b819a8ac018] q [0x2b819a8b0418]
autobl_dump_metadata() autobl_root_d [0x2b819a8c1000] Magic [B16B00DA] #Daemon [3] cat [0x2b819a8c1018] q [0x2b819a8c5418]
                     IP                   |  Rate |  Prod |  Tout
------------------------------------------+-------+-------+---------
                           132.17  9.18 |       |     1 |  1  3 |
                            132.   99.3 |       |       |       |
                           132.173.99.14 |   80% |     1 |  1363 |
                            132.173.99.8 |   80% |     1 |  1363 |
                            132.173.99.5 |   80% |     1 |  1363 |
                           132.173.99.20 |   80% |     1 |  1363 |
                           132.173.99.21 |   80% |     1 |  1363 |
                            132.173.99.4 |   80% |     1 |  1363 |
                            132.173.99.9 |   80% |     1 |  1363 |
                           132.173.99.24 |   80% |     1 |  1363 |
                           132.173.99.15 |   80% |     1 |  1363 |
                            132.173.99.2 |   80% |     1 |  1363 |
                           132.173.99.19 |   80% |     1 |  1363 |
                           132.173.99.13 |   80% |     1 |  1363 |
                           132.173.99.17 |   80% |     1 |  1363 |
                            132.173.99.0 |   80% |     1 |  1363 |
                            132.173.99.6 |   80% |     1 |  1363 |
                           132.173.99.23 |   80% |     1 |  1363 |
                           132.173.99.11 |   80% |     1 |  1363 |
                           132.173.99.10 |   80% |     1 |  1363 |
                           132.173.99.22 |   80% |     1 |  1363 |
                            132.173.99.7 |   80% |     1 |  1363 |
                            132.173.99.1 |   80% |     1 |  1363 |
                           132.173.99.16 |   80% |     1 |  1363 |
                           132.173.99.12 |   80% |     1 |  1363 |
```

1. **IP**: IP address that is member of the greylist
2. **Rate**: Probability of drop for an ingress packet. Higher number equals higher drop rate at the TCP layer. As drop rate goes up, retransmit rates increase, and subsequently TCP window sizes adjust closer to zero. Also, note this behavior will be different if the client IP is learned through a layer 7 header. If so, the behavior will be an HTTP rate limit versus TCP based mitigations.
3. **Prod**: Number of stat producers. In this environment, this should always be 1.
4. **Tout**: Time-out/TTL. Prior to releasing an IP address from the greylist, Advanced Web Application Firewall will quarantine the IP address for a period of time. During this time, TCP slowdown methods will discontinue, and HTTP rate limiting will take over. If during the quarantine period, the IP address triggers more attack traffic, the IP will be removed from quarantine and placed back in greylist. Quarantined IP addresses are visible in the DoS Dashboard/Analytics views in the Mitigation panel.

11. With the attack script still running, examine the output of the baseline script. You should be getting HTTP 200 OK responses, and the response time should be inline with pre-attack response times. Also, verify you can use browse to http://hackazon.f5demo.com without issue.
12. In the window where you are running the attack script, enter **CTRL-C**, then type **4** to kill the attack script cleanly.
13. Leave baseline_menu.sh script running.

8.7 Bad Actor Detection and Request Signatures

In the previous modules, we examined both request signature detection and bad actor detection mitigations individually. In this module, we will enable both mitigations together, and explore how they operate in tandem to mitigate a DoS attack. Additionally, we will use Advanced Web Application Firewall's DoS Reporting tools to further inspect the details of each attack.

1. Using Chromium Browser on the Xubuntu Jumpbox, open another tab to the GUI on bigip01
2. Navigate to **Security ›› DoS Protection : DoS Profiles** and click the **hackazon_bados** profile we created earlier.
3. Click the **Application Security** tab, and then click the **Behavioral & Stress-based Detection** button in the Application Security panel.
4. Click the **Edit** link to the right of the **Behavioral Detection and Mitigation** section, then uncheck the checkbox next to **Bad actors behavior detection**, and check the box next to **Request signatures detection**
5. Scroll down, and click **Update** button.
6. Navigate to **Security ›› Reporting ›› DoS ›› Dashboard**
7. From the **DoS Dashboard** select the refresh drop down and set value to 1 min, and grab the slider bar at the top and drag it as far right as possible.
8. On the right side of the **DoS Dashboard**, grab the handle just to the right of the HTTP and Network filter labels, and pull left to the midway point of the screen.
9. Using the inner-most vertical scroller on the right-hand side of the screen, scroll down until you see the **Transaction Outcomes** dynamic panel. Click the panel to expand, then click the three vertical lines to the left of the Transaction Outcomes label. Click on **Columns**, and click the green icon to remove all row labels except the following:

- Transactions
- Attacks
- Valid Transactions
- Mitigated Transactions
- Blocked Transactions
- Imcomplete Transactions

10. Repeat the same process to filter the **Behavioral Signatures** dynamic panel.
11. With the baseline traffic still running, examine both the **Transaction Outcomes** and **Behavior Signatures** panels. You should see all transactions have an outcome of **Passthrough**. Also, the center column of the main dashboard view should show no current attacks in progress. Keep this window open.

12. From the Xubuntu Jumpbox open another Terminal window, or return to a previously opened window. Then:

```
f5student@xjumpbox$~ ssh root@10.1.1.245
```

13. From the SSH session, run the following command:

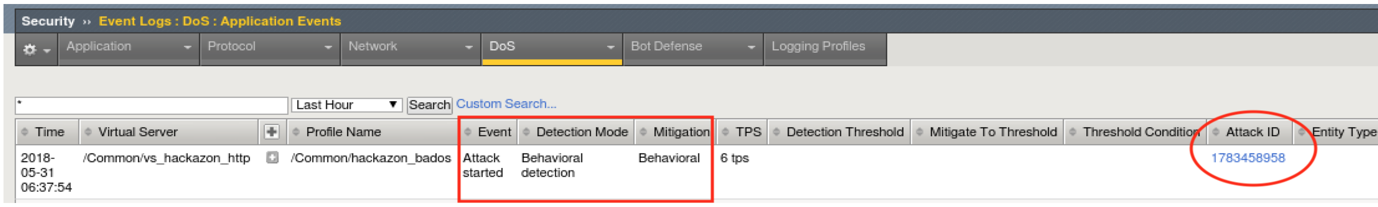
```
[root@bigipo01:Active:Standalone] config # watch ipidr -l /Common/vs_
↪hackazon_http+/Common/hackazon_bados
```

14. From the Xubuntu Jumpbox open another Terminal window, or return to a previously opened window. Then, re-run the attack script using the following command:

```
f5student@xjumpbox~$ ./AB_DOS.sh

- Select **2** - Attack start - score
```

15. Open another tab to the GUI on bigip01, and navigate to **Security** ›› **Event Logs** ›› **DoS** ›› **Application Events**

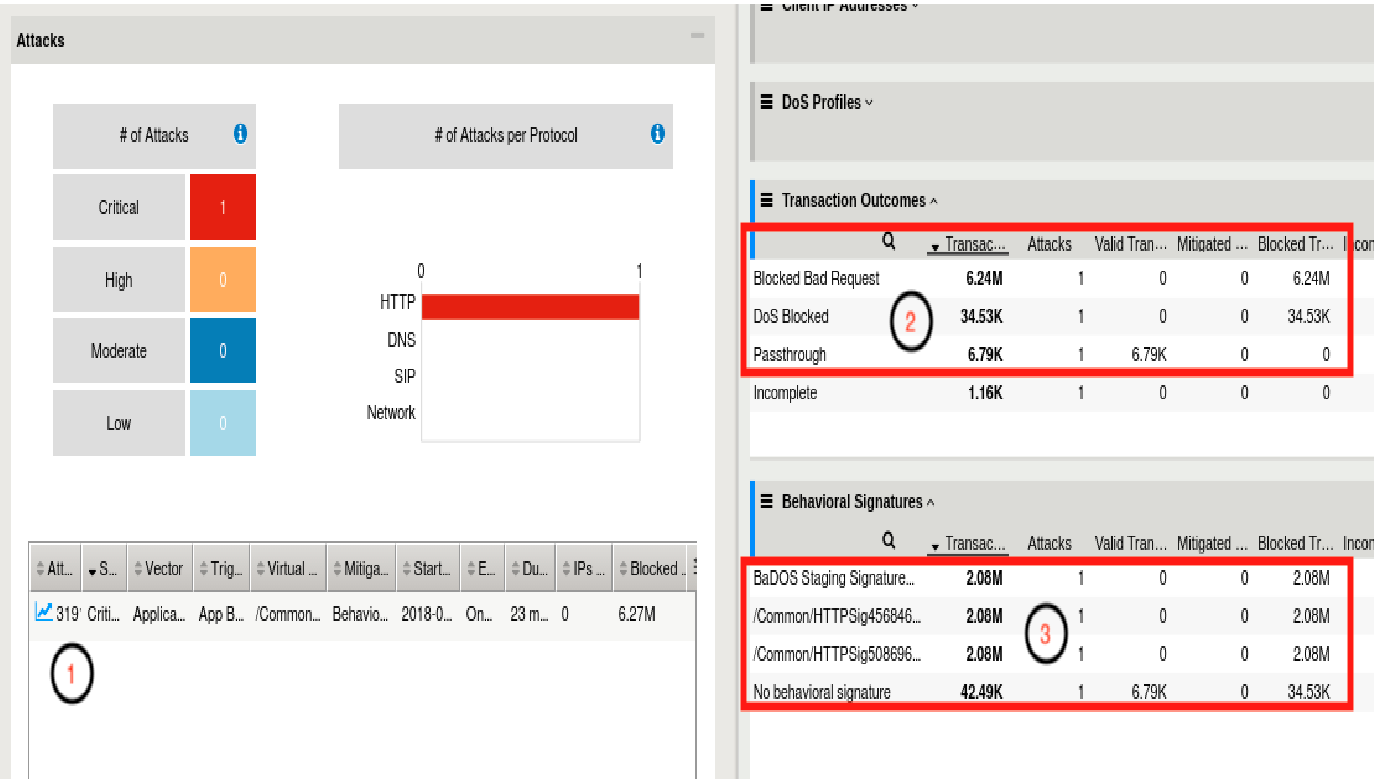
16. Almost immediately you should see an attack has started, and Advanced Web Application Firewall has assigned an Attack ID to the event. You will see something similar to the screenshot below:



Time	Virtual Server		Profile Name	Event	Detection Mode	Mitigation	TPS	Detection Threshold	Mitigate To Threshold	Threshold Condition	Attack ID	Entity Type
2018-05-31 06:37:54	/Common/vs_hackazon_http		/Common/hackazon_bados	Attack started	Behavioral detection	Behavioral	6 tps				1783458958	

17. Open another tab to the GUI on bigip01, and navigate to **Security** ›› **DoS Protection : Signatures**, and click on the **Dynamic** box, then set the **Refresh** value to **20 secs**. In a few moments, you should see request signatures being generated.

18. Return to the browser tab opened to the DoS Reporting Dashboard. Monitor the **Transaction Outcomes** and **Behavioral Signatures** dynamic panels. After a few minutes, you will begin to see signature based mitigations, and your dashboard should like similar to the image below:



Critical	1
High	0
Moderate	0
Low	0

Att...	S...	Vector	Trig...	Virtual ...	Mitiga...	Start...	E...	Du...	IPs ...	Blocked ...
319'	Criti...	Applica...	App B...	/Common...	Behavio...	2018-0...	On...	23 m...	0	6.27M

Transaction Outcomes

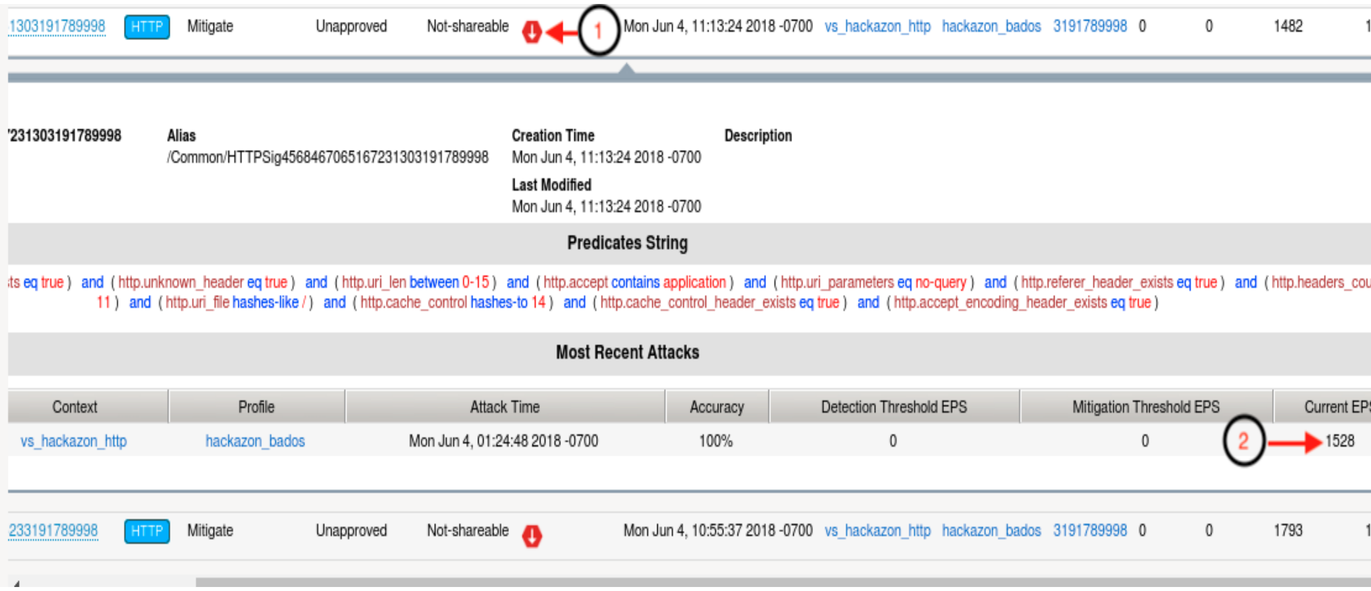
	Transac...	Attacks	Valid Tran...	Mitigated ...	Blocked Tr...	Incom
Blocked Bad Request	6.24M	1	0	0	6.24M	
DoS Blocked	34.53K	1	0	0	34.53K	
Passthrough	6.79K	1	6.79K	0	0	
Incomplete	1.16K	1	0	0	0	

Behavioral Signatures

	Transac...	Attacks	Valid Tran...	Mitigated ...	Blocked Tr...	Incon
BaDOS Staging Signature...	2.08M	1	0	0	2.08M	
/Common/HTTPSig456846...	2.08M	1	0	0	2.08M	
/Common/HTTPSig508696...	2.08M	1	0	0	2.08M	
No behavioral signature	42.49K	1	6.79K	0	34.53K	

1. DoS Dashboard view shows an attack has been triggered. Select the attack, click the filter icon in upper right hand corner of Attacks table, and you can adjust the columns to view.
2. This attack was initially mitigated with HTTP global rate limiting before a signature can be generated, accounted for in the **DoS Blocked** row. Then, as an attack signature is generated, all attack traffic should begin to be blocked with the request signature(s), evident by looking at the **Blocked Bad Request** row in transaction outcomes. At this point, if you refresh the dashboard, DoS Blocked counts should remain static, and Blocked Bad Request counters should be incrementing.
3. Behavioral DoS will generate and adjust signatures as the traffic changes. This panel shows the signatures, referenced by signature name, that have been used to mitigate this attack.

19. Look back at the browser tab showing the Dynamic Request Signatures. You should now see that not only have signatures been generated, but they are active in mitigating a current attack. See below:



1303191789998 HTTP Mitigate Unapproved Not-shareable Mon Jun 4, 11:13:24 2018 -0700 vs_hackazon_http hackazon_bados 3191789998 0 0 1482 1

'231303191789998

Alias
/Common/HTTPSig4568467065167231303191789998

Creation Time
Mon Jun 4, 11:13:24 2018 -0700

Last Modified
Mon Jun 4, 11:13:24 2018 -0700

Description

Predicates String

ts eq true) and (http.unknown_header eq true) and (http.uri_len between 0-15) and (http.accept contains application) and (http.uri_parameters eq no-query) and (http.referer_header_exists eq true) and (http.headers_cou
11) and (http.uri_file hashes-like /) and (http.cache_control hashes-to 14) and (http.cache_control_header_exists eq true) and (http.accept_encoding_header_exists eq true)

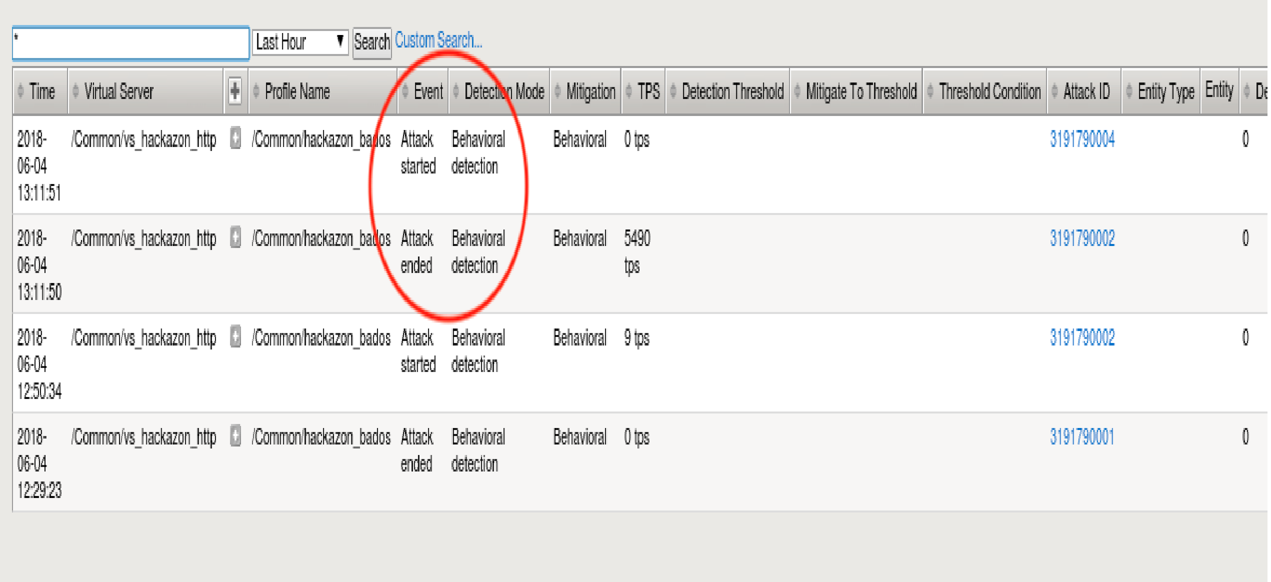
Most Recent Attacks

Context	Profile	Attack Time	Accuracy	Detection Threshold EPS	Mitigation Threshold EPS	Current EP
vs_hackazon_http	hackazon_bados	Mon Jun 4, 01:24:48 2018 -0700	100%	0	0	1528

233191789998 HTTP Mitigate Unapproved Not-shareable Mon Jun 4, 10:55:37 2018 -0700 vs_hackazon_http hackazon_bados 3191789998 0 0 1793 1

1. The Attack Status icon has changed to red, and shows “mitigated-with-attackid”.
2. Most recent attacks should show an incrementing **Current EPS** (Events Per Second) counter.

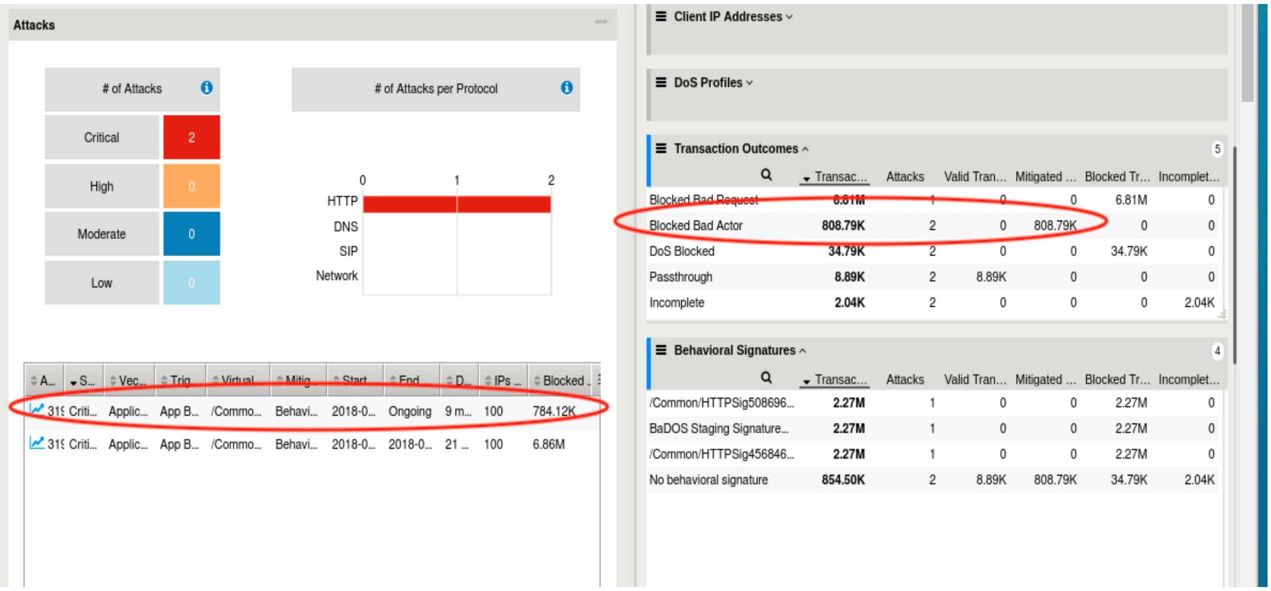
20. Using a different browser tab, navigate to **Security** ›› **DoS Protection : DoS Profiles** and click the hackazon_bados profile. As you did earlier, edit the **Behavioral Detection and Mitigation** section. This time, check the checkbox next to **Bad actors behavior detection**, then click **Update**.
21. Return to the browser tab monitoring the DoS event logs. Soon, you will see Advanced Web Application Firewall ends the current attack, and immediately triggers a new attack. Your DoS Application Events log should look similar to the below image:



Time	Virtual Server	+	Profile Name	Event	Detection Mode	Mitigation	TPS	Detection Threshold	Mitigate To Threshold	Threshold Condition	Attack ID	Entity Type	Entity	De
2018-06-04 13:11:51	/Common/vs_hackazon_http		/Common/hackazon_bados	Attack started	Behavioral detection	Behavioral	0 tps				3191790004		0	
2018-06-04 13:11:50	/Common/vs_hackazon_http		/Common/hackazon_bados	Attack ended	Behavioral detection	Behavioral	5490 tps				3191790002		0	
2018-06-04 12:50:34	/Common/vs_hackazon_http		/Common/hackazon_bados	Attack started	Behavioral detection	Behavioral	9 tps				3191790002		0	
2018-06-04 12:29:23	/Common/vs_hackazon_http		/Common/hackazon_bados	Attack ended	Behavioral detection	Behavioral	0 tps				3191790001		0	

22. Return to the browser tab opened to the DoS Reporting Dashboard. Monitor the **Transaction Outcomes** and **Behavioral Signatures** dynamic panels. After a few minutes, you will begin to see transactions being mitigated with **Blocked Bad Actor**. Shortly after you begin seeing transactions being mitigated via bad actor detection the Blocked Bad Request row should stop incrementing blocked transactions. Also, you should now see another attack has been triggered in the Attacks table. Your

DoS dashboard should look similar to below image:



Attacks

# of Attacks	
Critical	2
High	0
Moderate	0
Low	0

A...	S...	Vec...	Trig	Virtual	Mitig...	Start	End	D...	IPs ...	Blocked ...
31!	Criti...	Applic...	App B...	/Commo...	Behavi...	2018-0...	Ongoing	9 m...	100	784.12K
31!	Criti...	Applic...	App B...	/Commo...	Behavi...	2018-0...	2018-0...	21 ...	100	6.86M

Client IP Addresses

DoS Profiles

Transaction Outcomes 5

	Transac...	Attacks	Valid Tran...	Mitigated ...	Blocked Tr...	Incomplet...
Blocked Bad Request	6.81M	1	0	0	6.81M	0
Blocked Bad Actor	808.79K	2	0	808.79K	0	0
DoS Blocked	34.79K	2	0	0	34.79K	0
Passthrough	8.89K	2	8.89K	0	0	0
Incomplete	2.04K	2	0	0	0	2.04K

Behavioral Signatures 4

	Transac...	Attacks	Valid Tran...	Mitigated ...	Blocked Tr...	Incomplet...
/Common/HTTPSig508696...	2.27M	1	0	0	2.27M	0
BaDOS Staging Signature...	2.27M	1	0	0	2.27M	0
/Common/HTTPSig456846...	2.27M	1	0	0	2.27M	0
No behavioral signature	854.50K	2	8.89K	808.79K	34.79K	2.04K

Note: Request Signatures **blocked** L7 requests that match the signature using a layer seven drop. Bad Actors are **mitigated** at layer three and four.

23. Return to the Terminal window from step #13 above. You should see the IP greylist again adding attacking IP addresses.

24. Return to the browser tab monitoring the Dyamic Request Signatures, and examine the attack status for the attack signatures and EPS counter. You should see the attack status as **Detected**, not mitigating, and EPS should be 0. This attack is now being mitigated excusively by bad actors as in the previous module.

8.7.1 Bonus

The exercise above shows Request Signatures and Bad Actor Detection working in tandem to mitigate an attack. However, we have a relatively small set of attackers, so almost immediately Advanced Web Application Firewall will identify all the bad actors, and the attack will be 100% mitigated with bad actor detection. In the real world, it is highly likely the set of attackers will be very large and dynamic. So, it is quite possible, that as soon as bad actors are detected, the attacking sources will change. At that point, you will see an attack being mitigated by both request signatures and bad actors. Try the below steps to simulate this activity.

1. Return to the iRule configured in module 1 (*Create XFF-Mixed_Attacker iRule*)

2. Modify line #10 to match below and click **Update**

```
1  when HTTP_REQUEST {
2     # Good traffic
3        if { [IP::addr [IP::client_addr] equals 10.1.10.52] } {
4           set xff 153.172.223.[expr int(rand()*100)]
5           HTTP::header insert X-Forwarded-For $xff
6        }
7
8     # Attack traffic
```

```
     if { [IP::addr [IP::client_addr] equals 10.1.10.53] } {
        set xff 112.173.99.[expr int(rand()*1000)]
        HTTP::header insert X-Forwarded-For $xff
  }
}
```

3. Return to the browser tab monitoring the DoS Dashboard. Shortly, after the iRule change you should now see the **Blocked Bad Request** counter incrementing again. In time, Advanced Web Application Firewall will begin to learn all the new IP's as well, but you should have enough time to see both mitigations active concurrently.
4. Return to the browser tab monitoring the Dynamic Request Signatures. You should now see the attack signatures are again active and mitigating the attack until all new sources have been learned by bad actor detection.

This completes the Introduction to L7 Behavioral DoS Self Guided Lab. Thanks for attending the session, and have a great week at F5 Agility 2018!