Sun Mgt Bonus Lab 2: Zone & DoS Protection on Palo Alto NetworksFirewalls

For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Overview

Denial of Service (DoS) and Distributed Denial of Service (DDoS) types of attack are attempts to disrupt network services by overloading the network with unwanted traffic. Palo Alto Networks Operating System (PAN-OS) has built-in features that protect both, the firewall and the network resources from being exhausted by flood, host sweeps, port scans, and packet-based attacks. Mitigation of DoS & DDoS attacks in PAN-OS is achieved by enabling three separate levels of protection:

1. Zone-Based Protection – A comprehensive DoS template used to protect enterprise network from volumetric DoS attacks. It acts as the first line of defense for the network, since it is applied to the entire zone (ingress).
2. DoS (End Host) Protection – A set of policies and profiles that provide high level of granularity in protecting specific end hosts.
3. Application Level DoS Protection – A threat database containing 600+ vulnerability signatures used to prevent application level DoS attacks by utilizing Vulnerability Protection security profiles.

In this lab we will learn how to deploy and test Zone-Based and DoS (End Host) Protection features. Application level DoS protection with Vulnerability profiles will not be covered, since vulnerability security profiles are discussed in the Content-ID module.

Objective

The objective of this exercise is to enforce protection against flood, reconnaissance, and packet-based DoS attacks. This task will be achieved by configuring the firewall to act upon incoming traffic reaching the threshold values for syn packets, host sweep events, and packets with spoofed source IP addresses.

The Information You Need and Prerequisites

To complete these lab steps, you need to have the following prerequisites in place:

- ✓ PAN Firewall, preconfigured to pass traffic in production
- ✓ Threshold values for traffic which you intend to enforce the protection for
- ✓ Traffic generator tool, such as Ostinato, or other

- ✓ Network scanner, such as NetScan, Nmap, or other
- ✓ IP address of your workstation's network adapter
- ✓ IP address range for the servers that you intend to protect

Lab Configuration Steps

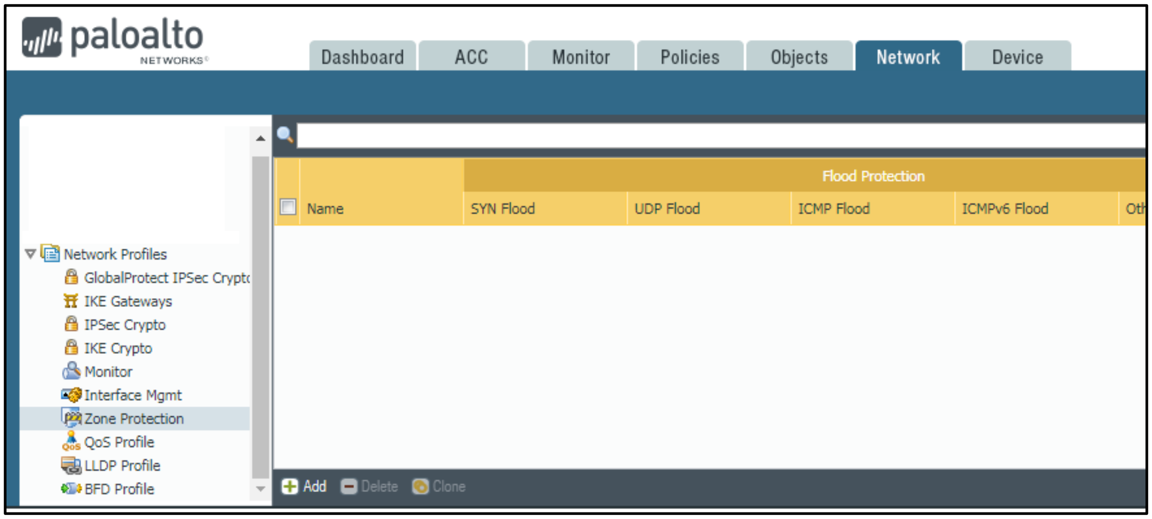
1. Configure Zone Protection

a. Purpose

Zone protection offer protection against flood, reconnaissance, and other packet based attacks. Zone protection profile can be used as a template for applying similar settings to multiple zones. These settings apply to a source (ingress) zone.

b. Location

Zone Protection Profiles are configured in the ***Network*** tab under ***Network Profiles*** group in the left menu.



c. Building Zone Protection Profile

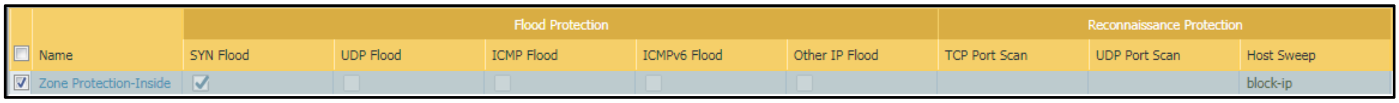
i. Click on ***Network*** > ***Zone Protection***, then click on ***Add*** button
ii. Type "Zone Protection-Inside" in the ***Name*** field.
iii. Enable ***Flood Protection*** > ***SYN*** option, then select ***Random Early Drop*** under the ***Action*** field.

iv. Define Threshold values for Alarm, Activate, and Maximum number of connections per second. In real environments, threshold values should be configured based upon actual data for the environment where DoS protection will be applied. For the purpose of this exercise, we will use the following values: ***Alarm=500, Activate=750, Maximum=1,000***.

v. Click on ***Reconnaissance Protection*** tab, enable ***Host Sweep*** option, set ***Action*** to ***Block-IP***, ***Track By*** to ***Source***, and ***Duration*** to 30 sec. Do not change ***Interval*** and ***Threshold*** values.

vi. Click on ***Packet Based Attack Protection*** tab and select ***Spoofed IP Address*** option.

vii. Click ***OK*** button. Your profile should look like the screenshot below:



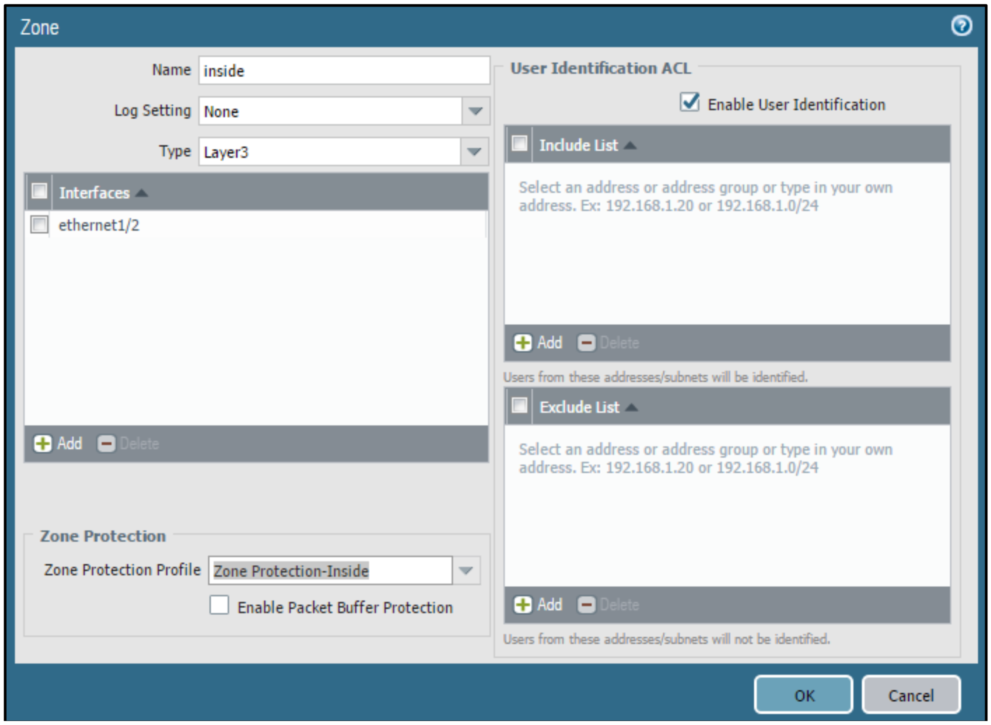
		Flood Protection					Reconnaissance Protection		
□	Name	SYN Flood	UDP Flood	ICMP Flood	ICMPv6 Flood	Other IP Flood	TCP Port Scan	UDP Port Scan	Host Sweep
☑	Zone Protection-Inside	✓	□	□	□	□			block-ip

d. Apply Zone Protection Profile to the Traffic Ingress Zone

i. Click on ***Network*** > ***Zones***, then click on ***inside*** zone (We will be conducting testing from inside the network. In most real-world applications, the profile would be applied to the Outside zone).

ii. Under ***Zone Protection Profile*** select ***Zone Protection-Inside***

iii. Click ***OK*** and ***Commit***.



Name: inside

Log Setting: None

Type: Layer3

□ Interfaces

□ ethernet1/2

Zone Protection

Zone Protection Profile: Zone Protection-Inside

□ Enable Packet Buffer Protection

User Identification ACL

☑ Enable User Identification

□ Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

□ Exclude List

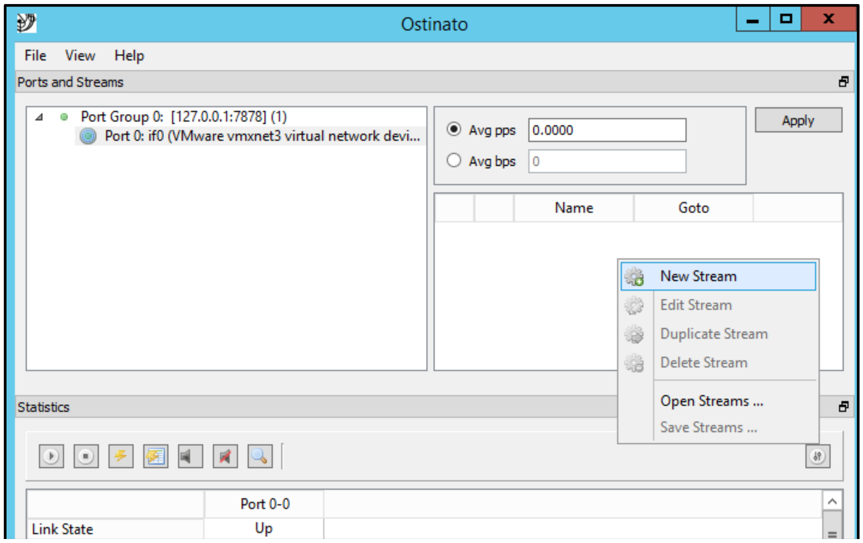
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

e. Test Zone Protection Profile

i. From your desktop, open the Ostinato folder and double-click on Ostinato.exe

ii. Expand ***Port Group 0***, highlight the network adapter connected to LAN and passing traffic, then right-click on the upper right hand window to create a ***New Stream***.



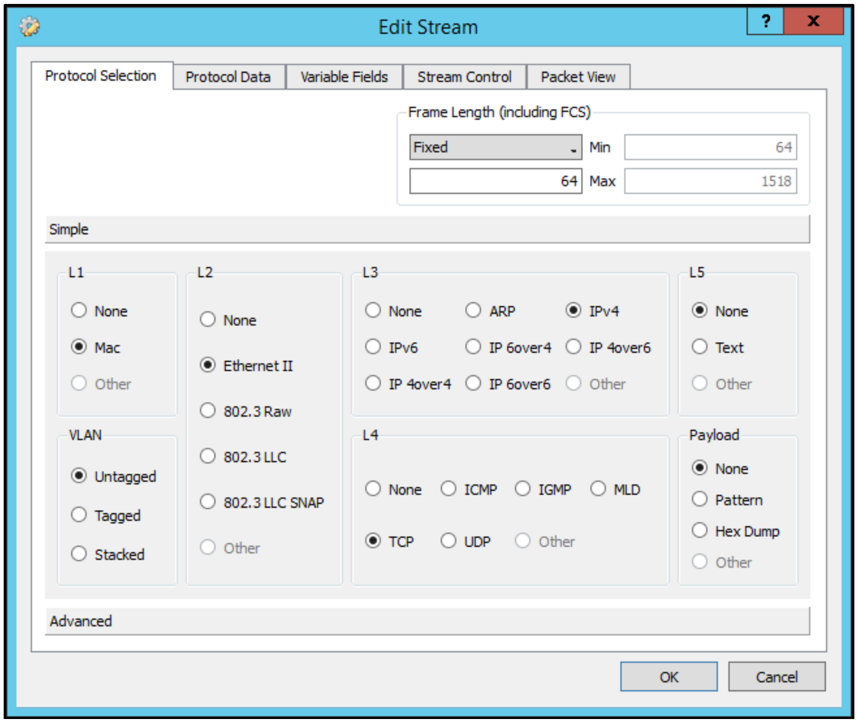
Port Group 0: [127.0.0.1:7878] (1)
Port 0: if0 (VMware vmxnet3 virtual network devi...

● Avg pps 0.0000
○ Avg bps 0

Name	Goto

	Port 0-0
Link State	Up

iii. Configure ***Protocol Selection*** section identically to the screenshot below:



Frame Length (including FCS)
Fixed Min 64
64 Max 1518

Simple

L1: ○ None ● Mac ○ Other

VLAN: ● Untagged ○ Tagged ○ Stacked

L2: ○ None ● Ethernet II ○ 802.3 Raw ○ 802.3 LLC ○ 802.3 LLC SNAP ○ Other

L3: ○ None ○ ARP ● IPv4 ○ IPv6 ○ IP 6over4 ○ IP 4over6 ○ IP 4over4 ○ IP 6over6 ○ Other

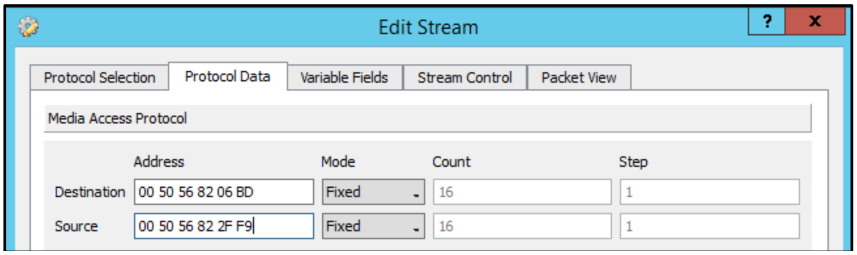
L4: ○ None ○ ICMP ○ IGMP ○ MLD ● TCP ○ UDP ○ Other

L5: ● None ○ Text ○ Other

Payload: ● None ○ Pattern ○ Hex Dump ○ Other

Advanced

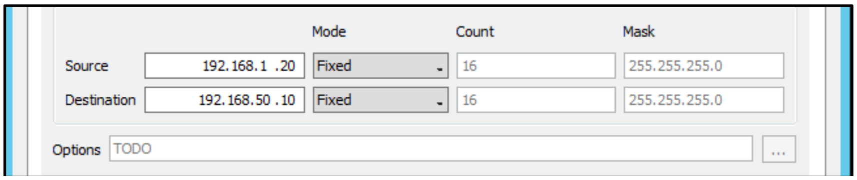
iv. From your desktop, open ***Command Prompt*** and execute ***ipconfig/all*** and ***arp –a*** commands to identify MAC address values for LAN adapter on the local machine and the firewall's ***inside*** interface (next hop). Enter these values in ***Protocol Data > Media Access Protocol*** fields in Ostinato:



Media Access Protocol

	Address	Mode	Count	Step
Destination	00 50 56 82 06 BD	Fixed	16	1
Source	00 50 56 82 2F F9	Fixed	16	1

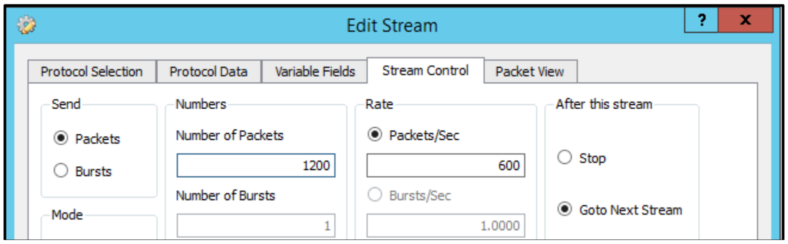
i. Enter ***Source*** and ***Destination*** addresses in ***Protocol Data > Internet Protocol ver 4*** fields. In this example, we will use 192.168.1.20 as ***source*** (your workstation's assigned IP address), and 192.168.50.10 as ***destination*** (we will target a server in the DMZ). Be sure to enter the correct IP addresses for the environment you are testing in.



		Mode	Count	Mask
Source	192.168.1 .20	Fixed	16	255.255.255.0
Destination	192.168.50 .10	Fixed	16	255.255.255.0

Options TODO

ii. Click on ***Stream Control*** tab, then enter 1200 for ***Number of Packets***, and 600 for ***Packets/Sec***:



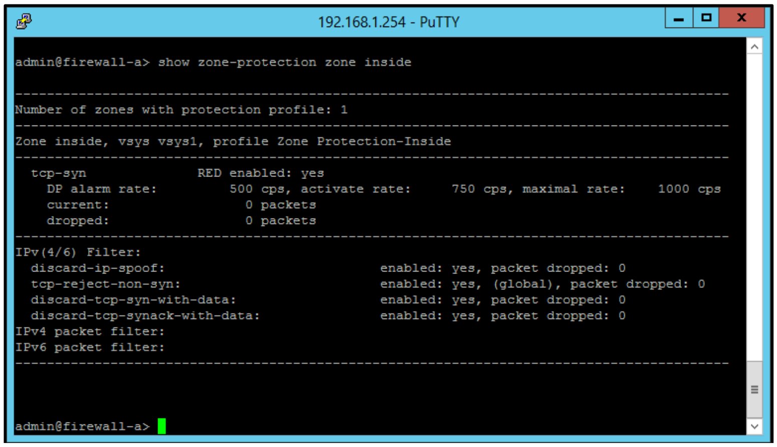
Send
● Packets
○ Bursts
Mode

Numbers
Number of Packets 1200
Number of Bursts 1

Rate
● Packets/Sec 600
○ Bursts/Sec 1.0000

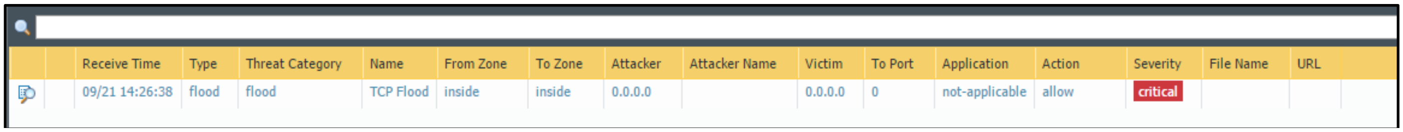
After this stream
○ Stop
● Goto Next Stream

iii. Click on ***OK***, then click ***Apply***. Before we send data stream to the server in DMZ, open a new ***Putty*** session, connect to the firewall, and execute ***show zone-protection zone inside*** command. Observe that all counters are showing zero values.



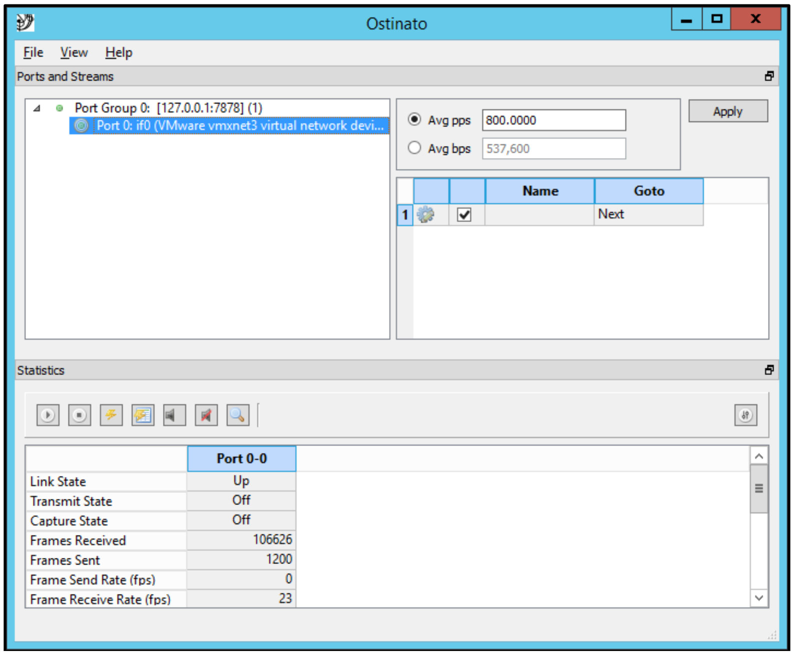
```
admin@firewall-a> show zone-protection zone inside

---------------------------------------------------------------------------------------------
Number of zones with protection profile: 1
---------------------------------------------------------------------------------------------
Zone inside, vsys vsys1, profile Zone Protection-Inside
---------------------------------------------------------------------------------------------
  tcp-syn              RED enabled: yes
    DP alarm rate:         500 cps, activate rate:     750 cps, maximal rate:    1000 cps
    current:                 0 packets
    dropped:                 0 packets
---------------------------------------------------------------------------------------------
IPv(4/6) Filter:
  discard-ip-spoof:                          enabled: yes, packet dropped: 0
  tcp-reject-non-syn:                        enabled: yes, (global), packet dropped: 0
  discard-tcp-syn-with-data:                 enabled: yes, packet dropped: 0
  discard-tcp-synack-with-data:              enabled: yes, packet dropped: 0
IPv4 packet filter:
IPv6 packet filter:
---------------------------------------------------------------------------------------------


admin@firewall-a> 
```

iv. Switch back to Ostinato, highlight ***Port 0-0*** column and click on ***Play*** button to execute the data stream. On firewall's Web-UI, open ***Monitor > Threat*** logs. Observe new ***Flood*** events with Severity- ***Critical*** and action ***Allow***. Values of 0.0.0.0 for the Attacker and Victim fields are expected.



		Receive Time	Type	Threat Category	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Name	URL
		09/21 14:26:38	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	allow	critical		

v. In Ostinato, edit the data stream and change values for ***Stream Control***. Use 2,400 for ***Number of Packets***, and 800 for ***Packets/Sec***. Click on ***OK***, then click on ***Apply***. With ***Port 0-0*** column still highlighted, resend the data by clicking on ***Play*** button.



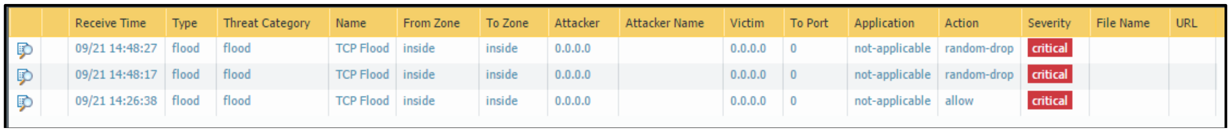
Port Group 0: [127.0.0.1:7878] (1)
Port 0: if0 (VMware vmxnet3 virtual network devi...

● Avg pps 800.0000
○ Avg bps 537,600

			Name	Goto
1		☑		Next

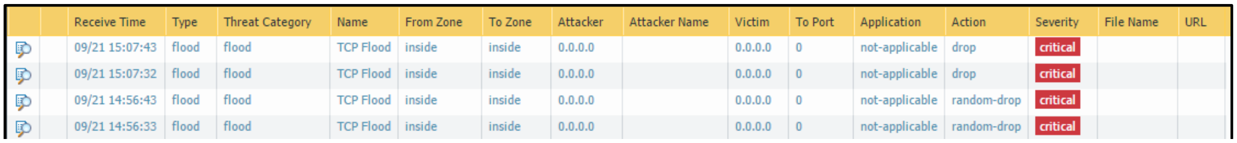
	Port 0-0
Link State	Up
Transmit State	Off
Capture State	Off
Frames Received	106626
Frames Sent	1200
Frame Send Rate (fps)	0
Frame Receive Rate (fps)	23

vi. Switch back to the Web-UI and observe new threat log events. This time the ***Action*** changes to ***Random-Drop***. In Putty, execute ***show zone-protection zone inside*** command again. Notice the increase in tcp-syn dropped packet counters.

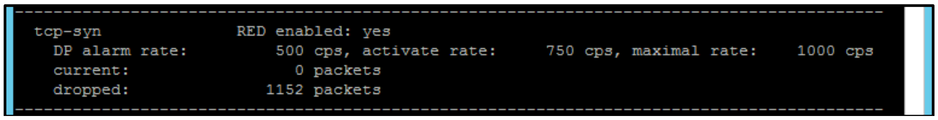


		Receive Time	Type	Threat Category	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Name	URL
		09/21 14:48:27	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	random-drop	critical		
		09/21 14:48:17	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	random-drop	critical		
		09/21 14:26:38	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	allow	critical		

vii. Switch back to Ostinato one more time and update values for Stream Control. Use 4,800 for ***Number of Packets***, and 1,200 for ***Packets/Sec***. Click on OK, then click on Apply. With ***Port 0-0*** column highlighted, resend the data by clicking on Play button again. This time the ***Action*** field in Web-UI changes to ***Drop***. Tcp-Syn packet counters continue to increase in Putty.

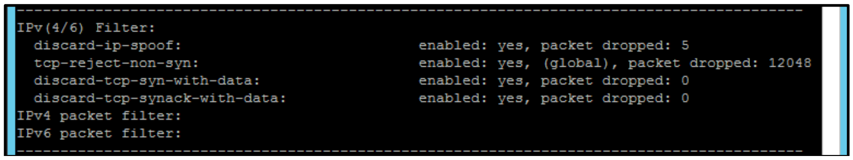


		Receive Time	Type	Threat Category	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Name	URL
		09/21 15:07:43	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical		
		09/21 15:07:32	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical		
		09/21 14:56:43	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	random-drop	critical		
		09/21 14:56:33	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	random-drop	critical		



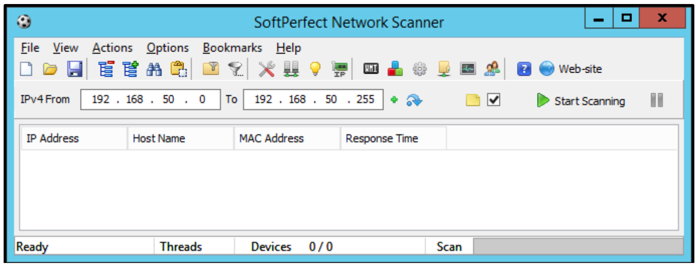
```
--------------------------------------------------------------------------------------
 tcp-syn                RED enabled: yes
   DP alarm rate:            500 cps, activate rate:     750 cps, maximal rate:    1000 cps
   current:                    0 packets
   dropped:                 1152 packets
--------------------------------------------------------------------------------------
```

viii. To test ***Packet Based Attack Protection*** feature, we are going to change source IP from 192.168.1.20 to 192.168.2.20 in Ostinato. In addition, we are going to update both, ***Number of Packets*** and ***Packets/Sec*** variables to 5***.*** Click ***OK***, click on ***Apply***, and resend the stream. The output of ***show zone-protection zone inside*** command reports 5 dropped packets due to IP address spoofing that we have just configured.



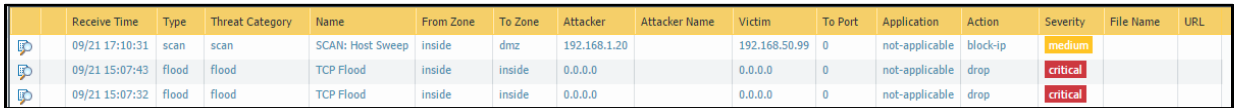
```
--------------------------------------------------------------------------------
IPv(4/6) Filter:
  discard-ip-spoof:                          enabled: yes, packet dropped: 5
  tcp-reject-non-syn:                        enabled: yes, (global), packet dropped: 12048
  discard-tcp-syn-with-data:                 enabled: yes, packet dropped: 0
  discard-tcp-synack-with-data:              enabled: yes, packet dropped: 0
IPv4 packet filter:
IPv6 packet filter:
--------------------------------------------------------------------------------
```

ix. Next, from your desktop execute NetScan.exe. Define 192.168.50.0-255 as the destination range and click on ***Start Scanning.***



IPv4 From 192 . 168 . 50 . 0 To 192 . 168 . 50 . 255

x. Spot a new entry in the Web-UI's ***Threat Logs***. Type- ***Scan***, Name- ***Host Sweep***, Severity- ***Medium***, and action ***Block-IP***.



		Receive Time	Type	Threat Category	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Name	URL
		09/21 17:10:31	scan	scan	SCAN: Host Sweep	inside	dmz	192.168.1.20		192.168.50.99	0	not-applicable	block-ip	medium		
		09/21 15:07:43	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical		
		09/21 15:07:32	flood	flood	TCP Flood	inside	inside	0.0.0.0		0.0.0.0	0	not-applicable	drop	critical		

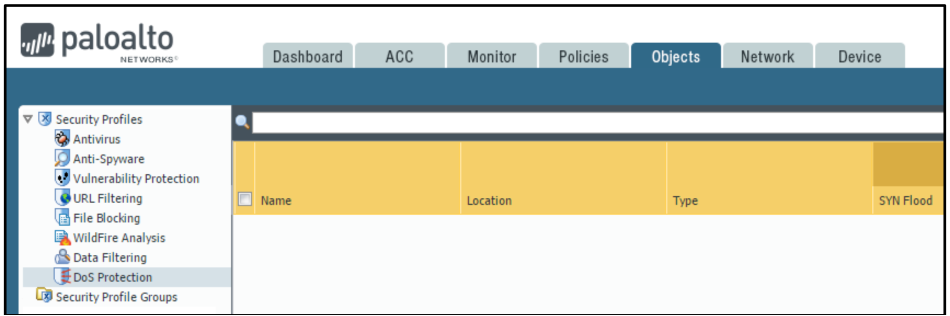
2. Configure DoS (End Host) Protection

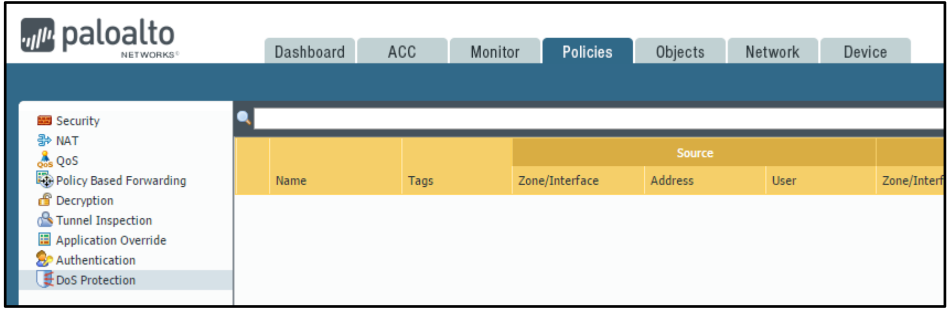
a. Purpose

DoS protection rule base and profiles provide the firewall administrator a granular approach to DoS mitigation. As in ***Security Rules***, DoS Protection rules can be configured to match zone, interface, IP address or user information as match conditions for mitigating the attacks. DoS protection profiles are designed for high precision targeting, to and from certain addresses or address groups, or from certain users. Additionally, DoS policy is used to mitigate individual attacks which have not triggered ***Zone Protection*** policy thresholds.

b. Location

DoS Protection Profiles are configured in the ***Objects*** tab under ***Security Profiles*** group in the left menu. DoS Protection Rules are configured in the ***Policies*** tab under ***DoS Protection***.





c. Building DoS Protection Profile

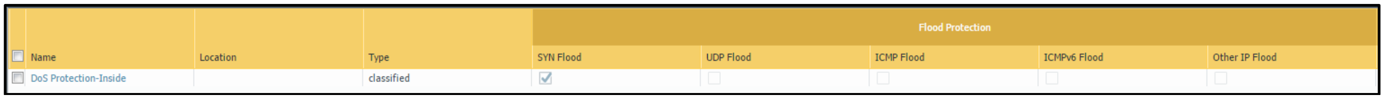
i. Click on ***Objects*** > ***DoS Protection***, then click on ***Add*** button at the bottom

ii. Type "DoS Protection-Inside" in the ***Name*** field, and select ***Type-Classified***.

iii. Enable ***Flood Protection > Syn Flood > SYN*** option, then select ***Random Early Drop*** in the ***Action*** field.

iv. Define Threshold values for Alarm, Activate, and Max Rate number of connections per second. In real-world environments the threshold values should be configured based upon actual data for the environment where DoS protection will be applied. For the purpose of this exercise, we will use the following values: ***Alarm=100, Activate=200, Max Rate=300***. Change ***Block Duration*** to 30 sec. Notice that we are purposely defining low threshold values, as the idea in this step is to test DoS policies and prevent previously defined Zone Protection thresholds from being reached.

v. Click ***OK*** button. Your profile should look like the screenshot below:

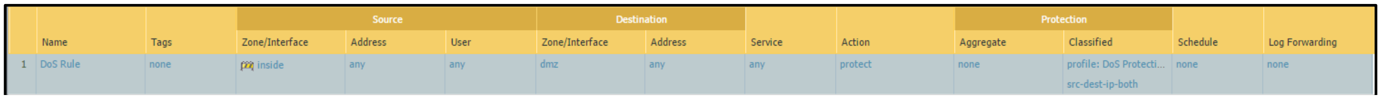


			Flood Protection				
□ Name	Location	Type	SYN Flood	UDP Flood	ICMP Flood	ICMPv6 Flood	Other IP Flood
□ DoS Protection-Inside		classified	☑	□	□	□	□

d. Building DoS Protection Policy

i. Click on ***Policies*** > ***DoS Protection***, then click on ***Add*** button at the bottom.

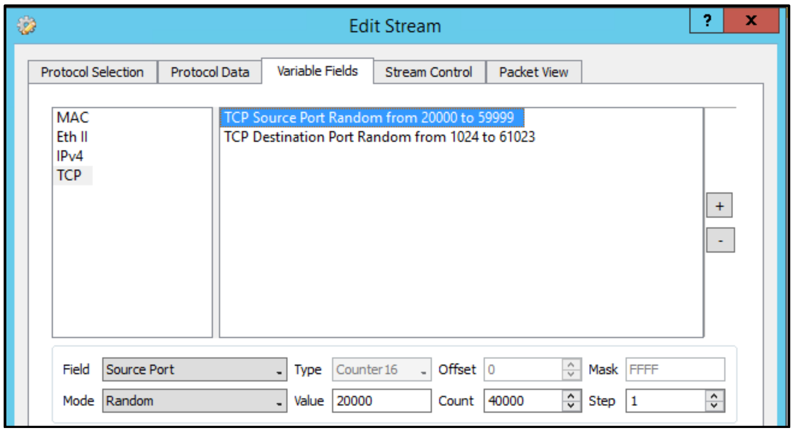
ii. Type "***DoS Rule***" in the ***Name*** field. Under ***Source*** tab select zone ***inside*** and leave ***Source Address*** and ***Source User*** fields unchanged. Define ***dmz*** as the destination zone, and leave ***Destination Address*** field unchanged. Under ***Option/Protection*** tab define Action- ***Protect***. Enable ***Classified*** option, then select ***DoS Protection-Inside*** profile from the menu. Specify ***src-dest-ip-both*** in the ***Address*** field.
Note: Using ***source-IP-only*** and ***src-dest-ip-both*** classifications for internet-facing zones in classified DoS protection policy rules is not recommended practice, because firewall does not have the capacity to store counters for every possible IP address on the internet.



			Source			Destination				Protection			
	Name	Tags	Zone/Interface	Address	User	Zone/Interface	Address	Service	Action	Aggregate	Classified	Schedule	Log Forwarding
1	DoS Rule	none	inside	any	any	dmz	any	any	protect	none	profile: DoS Protecti... src-dest-ip-both	none	none

e. Test DoS Protection Policy

i. Edit the existing data stream in Ostinato: In ***Protocol Data*** > ***Transmission Control Protocol*** > ***Flags*** enable ***SYN*** option; Switch to ***Variable Fields*** and create two ***TCP*** variables for ***source*** and ***destination*** ports, as shown in the screenshot below. This step is needed for creating randomness in data which we are going to send to the server in DMZ.



Edit Stream

TCP Source Port Random from 20000 to 59999
TCP Destination Port Random from 1024 to 61023

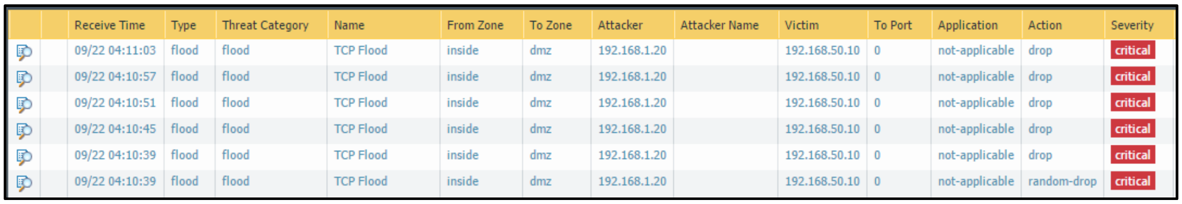
Field: Source Port
Type: Counter16
Offset: 0
Mask: FFFF
Mode: Random
Value: 20000
Count: 40000
Step: 1

ii. Change the values for Stream Control: Use 24,000 for ***Number of Packets***, and 400 for ***Packets/Sec***. Click on OK, then click on Apply.

iii. Before you send the stream to the server, open a new ***Command Prompt*** window and execute ***ping –t 192.168.50.10*** command (replace that IP address that whatever destination you are using).

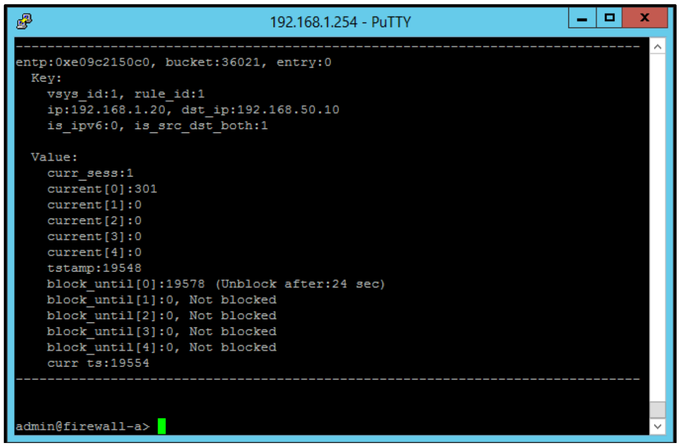
iv. Highlight ***Port 0-0*** column in Ostinato and resend the data by clicking on Play button.

v. Review ***Threat*** logs in Web-UI and notice newly generated ***flood*** events. This time the firewall identifies source and destination IP addresses (***Attacker*** & ***Victim***) due to ***classified*** DoS protection profile.



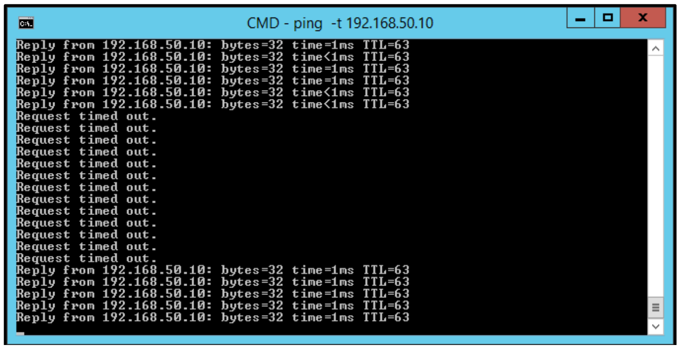
		Receive Time	Type	Threat Category	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
		09/22 04:11:03	flood	flood	TCP Flood	inside	dmz	192.168.1.20		192.168.50.10	0	not-applicable	drop	critical
		09/22 04:10:57	flood	flood	TCP Flood	inside	dmz	192.168.1.20		192.168.50.10	0	not-applicable	drop	critical
		09/22 04:10:51	flood	flood	TCP Flood	inside	dmz	192.168.1.20		192.168.50.10	0	not-applicable	drop	critical
		09/22 04:10:45	flood	flood	TCP Flood	inside	dmz	192.168.1.20		192.168.50.10	0	not-applicable	drop	critical
		09/22 04:10:39	flood	flood	TCP Flood	inside	dmz	192.168.1.20		192.168.50.10	0	not-applicable	drop	critical
		09/22 04:10:39	flood	flood	TCP Flood	inside	dmz	192.168.1.20		192.168.50.10	0	not-applicable	random-drop	critical

vi. Execute ***debug dataplane show dos rule "DoS Rule" classification-table*** command in Putty. Observe both tracked IP addresses and associated blocking timers.



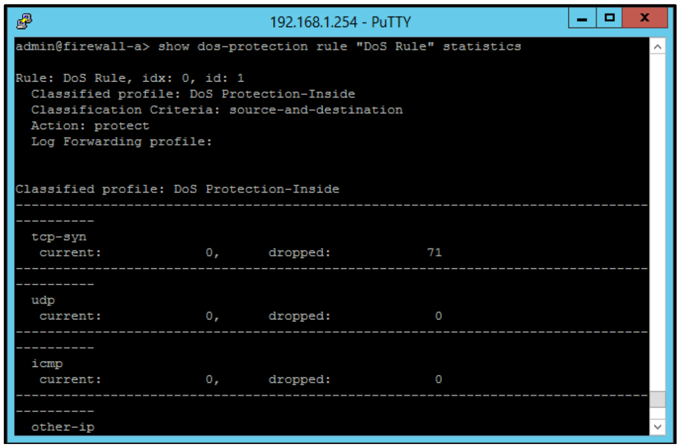
```
--------------------------------------------------------------------------------
entp:0xe09c2150c0, bucket:36021, entry:0
  Key:
    vsys_id:1, rule_id:1
    ip:192.168.1.20, dst_ip:192.168.50.10
    is_ipv6:0, is_src_dst_both:1

  Value:
    curr_sess:1
    current[0]:301
    current[1]:0
    current[2]:0
    current[3]:0
    current[4]:0
    tstamp:19548
    block_until[0]:19578 (Unblock after:24 sec)
    block_until[1]:0, Not blocked
    block_until[2]:0, Not blocked
    block_until[3]:0, Not blocked
    block_until[4]:0, Not blocked
    curr ts:19554
--------------------------------------------------------------------------------


admin@firewall-a>
```

vii. Notice how the continuous ping to 192.168.50.10 gets interrupted for approximately 30 secs, and then it resumes.



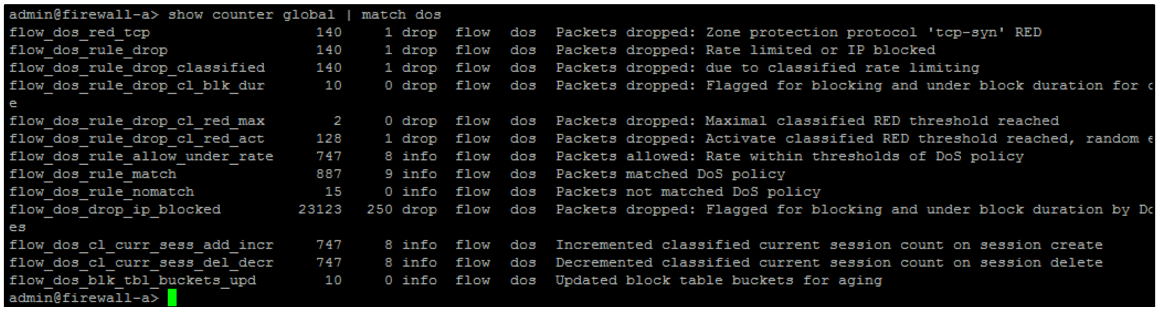
```
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
Reply from 192.168.50.10: bytes=32 time<1ms TTL=63
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
Reply from 192.168.50.10: bytes=32 time<1ms TTL=63
Reply from 192.168.50.10: bytes=32 time<1ms TTL=63
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
Reply from 192.168.50.10: bytes=32 time=1ms TTL=63
```

viii. Execute ***show dos-protection rule "DoS Rule" statistics*** command in Putty, and observe increasing # of dropped syn packets.



```
admin@firewall-a> show dos-protection rule "DoS Rule" statistics

Rule: DoS Rule, idx: 0, id: 1
  Classified profile: DoS Protection-Inside
  Classification Criteria: source-and-destination
  Action: protect
  Log Forwarding profile:


Classified profile: DoS Protection-Inside
--------------------------------------------------------------------------------
----------
  tcp-syn
   current:            0,      dropped:           71
--------------------------------------------------------------------------------
----------
  udp
   current:            0,      dropped:            0
--------------------------------------------------------------------------------
----------
  icmp
   current:            0,      dropped:            0
--------------------------------------------------------------------------------
----------
  other-ip
```

ix. Finally, execute ***show counter global | match dos*** command in Putty, and observe the statistics related to traffic denied by DoS protection mechanisms.



```
admin@firewall-a> show counter global | match dos
flow_dos_red_tcp                   140     1 drop  flow  dos  Packets dropped: Zone protection protocol 'tcp-syn' RED
flow_dos_rule_drop                 140     1 drop  flow  dos  Packets dropped: Rate limited or IP blocked
flow_dos_rule_drop_classified      140     1 drop  flow  dos  Packets dropped: due to classified rate limiting
flow_dos_rule_drop_cl_blk_dur       10     0 drop  flow  dos  Packets dropped: Flagged for blocking and under block duration for c
e
flow_dos_rule_drop_cl_red_max        2     0 drop  flow  dos  Packets dropped: Maximal classified RED threshold reached
flow_dos_rule_drop_cl_red_act      128     1 drop  flow  dos  Packets dropped: Activate classified RED threshold reached, random e
flow_dos_rule_allow_under_rate     747     8 info  flow  dos  Packets allowed: Rate within thresholds of DoS policy
flow_dos_rule_match                887     9 info  flow  dos  Packets matched DoS policy
flow_dos_rule_nomatch               15     0 info  flow  dos  Packets not matched DoS policy
flow_dos_drop_ip_blocked         23123   250 drop  flow  dos  Packets dropped: Flagged for blocking and under block duration by Do
es
flow_dos_cl_curr_sess_add_incr     747     8 info  flow  dos  Incremented classified current session count on session create
flow_dos_cl_curr_sess_del_decr     747     8 info  flow  dos  Decremented classified current session count on session delete
flow_dos_blk_tbl_buckets_upd        10     0 info  flow  dos  Updated block table buckets for aging
admin@firewall-a>
```

Next Steps

If you want to test this on your own and do not have access to a lab environment to do so, you have a couple options:

a. Contact your Sun Management Account Rep to get pricing on a lab bundle. The newly released PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

If you are unsure who your Account Rep is or do not have one yet, you can reach out to **sales@sunmanagement.net** for assistance.

b. Reach out through the free Fuel Users Group (www.fuelusersgroup.org) which at the time this lab is being written is offering limited free access to a virtual lab environment, which they refer to as their “Virtual Test Lab,” in which you can practice the steps outlined above. (Note: The Fuel Users Group may alter or discontinue offering their “Virtual Test Lab” at any time)

If you feel Sun Management brings value to you and your organization with these labs, please keep us in mind for other network and network security related requirements. We are here to help you. Thank you for your business.

Please direct any questions/comments/feedback on this lab exercise to: ***education@sunmanagement.net***

Lab Author: *Bob Pesakovic*
Palo Alto Networks Instructor & Sr. Network Security Engineer, PCNSE, PCNSI

Last Modified: Oct 4, 2017