

Firewalls

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

Overview

Quality of Service (QoS) on Palo Alto Networks firewalls represents a set of features used to prioritize and adjust quality aspects of network traffic. The variety of options that comes as an integral part of the PAN-OS gives the firewall administrator an ability to regulate traffic in the following ways:

- Prioritize network and application traffic
- Perform traffic profiling to ensure proper bandwidth usage
- Allocate and manage bandwidth sharing among network subnets, classes, or users
- Ensure low latency for mission critical applications

The administrator's capability to shape these four aspects is enabled through the firewall's service quality measurements, such as:

- bandwidth (maximum rate of transfer)
- throughput (actual rate of transfer)
- latency (delay)
- jitter (variance in latency).

Traffic shaping can also be configured based on:

- source and destination address
- source user
- application
- source/destination port combination
- URL category
- Differentiated Services Code Point (DSCP), or Type of Service (ToS) values defined in packet's IP header
- class of service

Administrators can apply QoS separately for clear text and tunneled traffic.

In addition to prioritizing and shaping incoming traffic, Palo Alto Networks firewall has the ability to mark outgoing traffic by modifying DSCP/TOS field of packet header before forwarding it to upstream/downstream devices. This functionality fulfills a dual role: a) the firewall allows intermediate network devices to continue to enforce priority based on DSCP/TOS classification and, b) the firewall can perform continuous, session-based QoS treatment to both, outgoing and return traffic. Marking outgoing traffic based on DSCP/TOS is configured in the security policy, and will not be discussed in this lab. For additional information on the subject, the reader is referred to 'Quality of Service' chapter in the PAN-OS 8.0 Administrator's Guide.

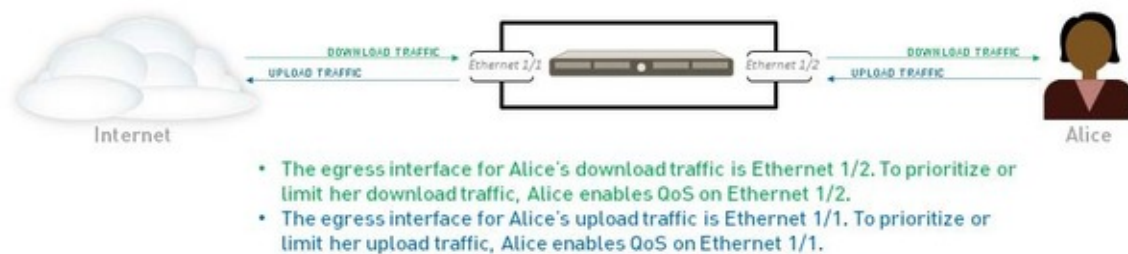
Firewalls

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

Objective

One of the most attractive features of the PAN-OS Quality of Service is traffic shaping based on Application ID. At the time this lab is being written, PAN-OS App-ID engine contains 2,600+ unique application signatures, offering the administrator significant flexibility in planning and deploying the QoS. It is important to remember that many applications rely on either publicly known or proprietary cryptography, hence reducing the firewall's ability to accurately label traversing traffic. Even though the App-ID engine has the ability to identify certain applications that utilize proprietary or publicly known encryption mechanisms (Skype, Bittorrent, Facebook, etc), the best results are achieved if decryption is enabled on the firewall prior to configuring QoS.

The objective of this lab is to demonstrate the simplest case of QoS deployment based on class of service and App-ID. Before we begin, we must familiarize ourselves with the concept of **QoS Egress Interface**: Egress interface for QoS traffic is the interface which traffic leaves the firewall from. QoS is always enabled and enforced on the egress interface for a traffic flow! For example, let's assume that our firewall has two interfaces, Trust and Untrust. If a user on the LAN attempts to upload a large file to Dropbox, the majority of that payload will be leaving the firewall from the firewall's Untrust interface. In this case the Untrust interface is our **egress interface**. In a different scenario, a user is streaming from YouTube or Netflix. The video stream is coming from the Internet and departing the firewall through its Trust interface. Here, Trust interface is our **egress interface**.

The Information You Need and Prerequisites

- ✓ PAN Firewall, preconfigured in VWire, L2, or L3 mode to pass traffic in production
- ✓ Web browser and Internet access

Firewalls

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

Lab Configuration Steps

1. Establish Benchmarks

a. Purpose

To evaluate the effectiveness of App-ID-based Quality of Service, we are going to utilize SpeedTest (<http://legacy.speedtest.net>). The following key points apply:

- SpeedTest is identified by PAN-OS as a web-based application. Since we are demonstrating the firewall's ability to shape traffic based on application signatures, we will select SpeedTest as our matching criterion.
- SpeedTest transfers data in clear text, therefore eliminating the need for enabling outbound decryption on the firewall.
- The **QoS Egress Interface** concept will be confirmed based on SpeedTest's bi-directional data transfer.
- Simplicity: the intent of this lab is to provide a proof of concept, without necessarily addressing real-world complexities, such as application shifts, and other.

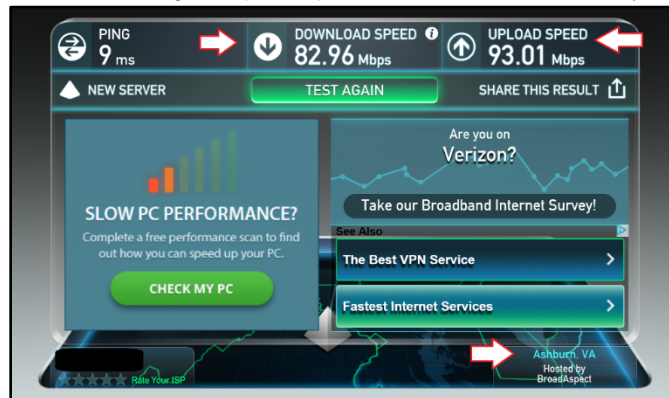
b. Testing

Open a web browser and navigate to <http://legacy.speedtest.net>. Select a server of your choice, or simply click on **Begin Test**. Record the benchmark values for both, download and upload speeds, as well as the test server location.

Update: Ookla has recently redesigned SpeedTest, while PAN application database still relies on the legacy application signature. For this reason, the reader is referred to the legacy web site instead of the current www.speedtest.net. To make QoS work for the newly redesigned service, 'web-browsing' must be used instead of speedtest, as explained in 'Creating QoS Rule' on page #8 below.

Firewalls

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



Firewalls

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

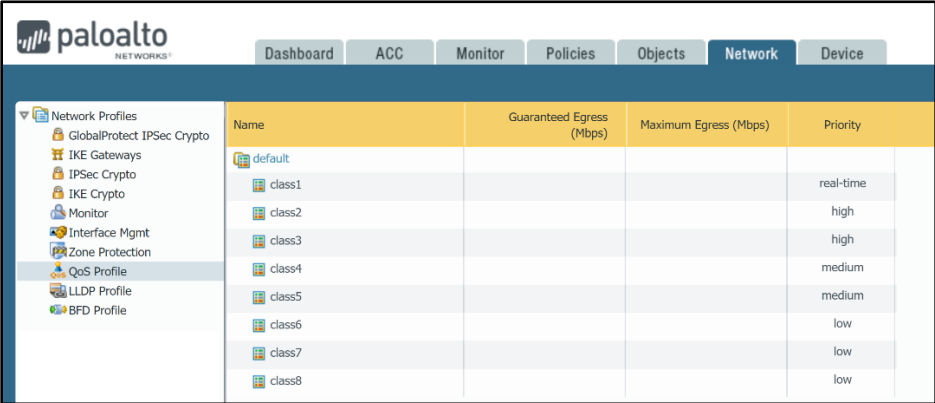
2. Configure QoS Profile

a. Purpose

QoS profile is needed for defining bandwidth limits and priority for classes of service (up to eight). Here, we can define both, guaranteed and maximum bandwidth limits for individual and collective classes. Priorities determine how traffic is treated in the presence of contention.

b. Location

QoS profile is configured in the **Network** tab under **QoS Profile** in the left menu.



Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
default			real-time
class1			high
class2			high
class3			medium
class4			medium
class5			low
class6			low
class7			low
class8			low

c. Building QoS Profiles

- Click on **Network** > **QoS Profile**, then click on **Add** button at the bottom
- Type "Upload Profile" in the **Name** field and leave **Egress Max** and **Egress Guaranteed** fields unaltered.
- Under **Classes** option, click on **Add** button. Select **class5**, leave Priority as **Medium**, then configure **Egress Max** and **Egress Guaranteed** fields as 11 and 5 respectively (Mbps). Our intent here is to limit upload speed to 11 Mbps.

Firewalls

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

QoS Profile

Profile

Profile Name: Upload Profile

Egress Max: 0

Egress Guaranteed: 0

Classes

Class	Priority	Egress Max	Egress Guaranteed
<input checked="" type="checkbox"/> class5	medium	11	5

class 4 is the default class

- iv. Click **OK** button, then click on **Add** button again to create another profile for limiting download speed.
- v. Name this profile “Download Profile”, and leave **Egress Max** and **Egress Guaranteed** fields unchanged.
- vi. Under **Classes** option, click on **Add** button. Select class5, leave Priority as **Medium**, then configure **Egress Max** and **Egress Guaranteed** fields as 22 and 8 respectively. Our intent is to limit download speed to 22 Mbps.

QoS Profile

Profile

Profile Name: Download Profile

Egress Max: 0

Egress Guaranteed: 0

Classes

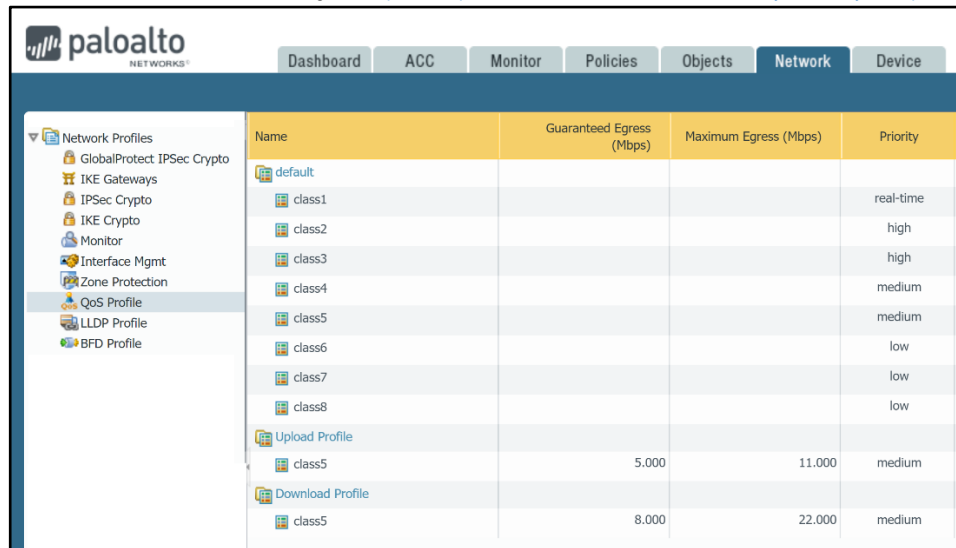
Class	Priority	Egress Max	Egress Guaranteed
<input checked="" type="checkbox"/> class5	medium	22	8

class 4 is the default class

- vii. Click on **OK** to close the dialog box. Your screen should look similar to the snapshot below.

Firewalls

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



Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
default			
class1			real-time
class2			high
class3			high
class4			medium
class5			medium
class6			low
class7			low
class8			low
Upload Profile			
class5	5.000	11.000	medium
Download Profile			
class5	8.000	22.000	medium

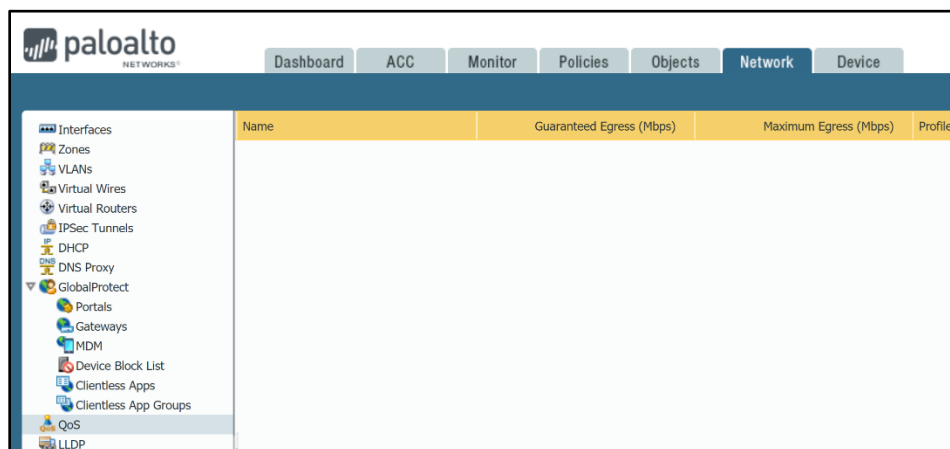
3. Enable QoS on Interfaces

a. Purpose

This is the step where we apply QoS profiles, as defined in previous steps, to the firewall's **Egress Interfaces**. Enabling QoS on an interface assigns bandwidth limits for that interface, and/or to enables the interface to enforce QoS for egress traffic.

b. Location

QoS is applied to interfaces in the **Network** tab under **QoS** in the left menu.



Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile
------	--------------------------	-----------------------	---------

Firewalls

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

c. Assigning QoS Profiles to Interfaces

- i. Click on **Network > QoS**, then click on **Add** button at the bottom
- ii. Under **Physical Interface** tab select the interface that belongs to **Untrust** security zone (Internet facing interface). In our instance that is ethernet1/1 interface.
- iii. Under **Default Profile** section select **default** profile for both, **Clear Text** and **Tunnel Interface** fields.

QoS Interface

Physical Interface | Clear Text Traffic | Tunneled Traffic

Interface Name: ethernet1/1

Egress Max (Mbps): 0

☒ Turn on QoS feature on this interface

Default Profile

Clear Text: default

Tunnel Interface: default

OK Cancel

- iv. Switch to **Clear Text Traffic** tab, then click on **Add** button to create a new entry. Give it a name **Upload Traffic**, then select previously created **Upload Profile** from the dropdown menu under **QoS Profile** field. Leave **Source Interface** and **Source Subnet** fields unchanged. Click on **OK**.

QoS Interface

Physical Interface | Clear Text Traffic | Tunneled Traffic

Egress Guaranteed (Mbps): 0

Egress Max (Mbps): 0

Name	QoS Profile	Source Interface	Source Subnet
Upload Traffic	Upload Profile		any

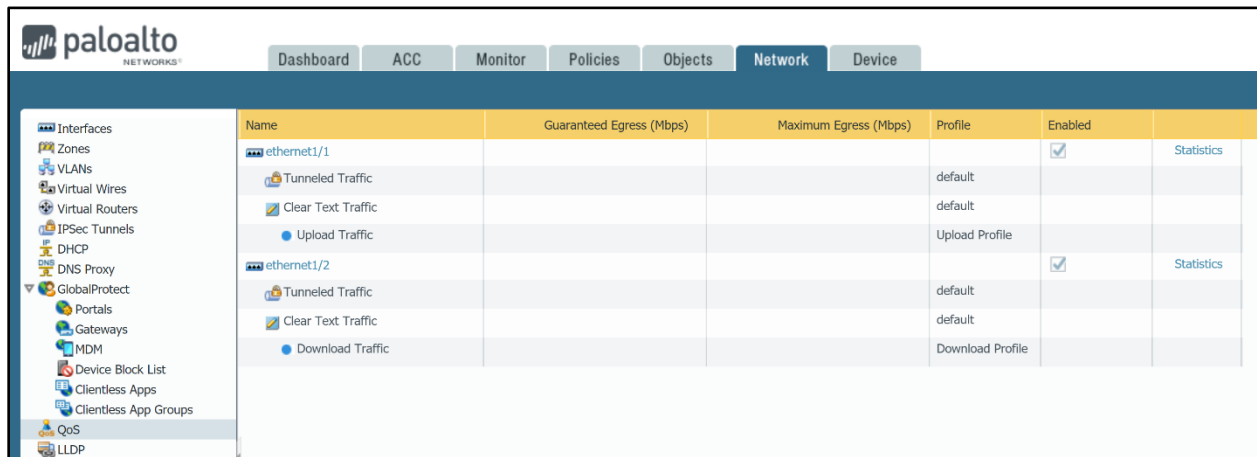
Add Delete

OK Cancel

- i. Repeat steps i-iv one more time to assign appropriate QoS profile to the **Trust** interface (LAN facing interface). Configure everything identically to the previous four steps, except selecting different physical interface (ethernet1/2 in our instance), and assigning previously created **Download Profile** to it. Also, give it a different name- **Download Traffic**, for example. Click on OK, and confirm that your screen looks similar to the screenshot below:

Firewalls

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



Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	Enabled	
ethernet1/1				<input checked="" type="checkbox"/>	Statistics
Tunneled Traffic			default		
Clear Text Traffic			default		
Upload Traffic			Upload Profile		
ethernet1/2				<input checked="" type="checkbox"/>	Statistics
Tunneled Traffic			default		
Clear Text Traffic			default		
Download Traffic			Download Profile		

Firewalls

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

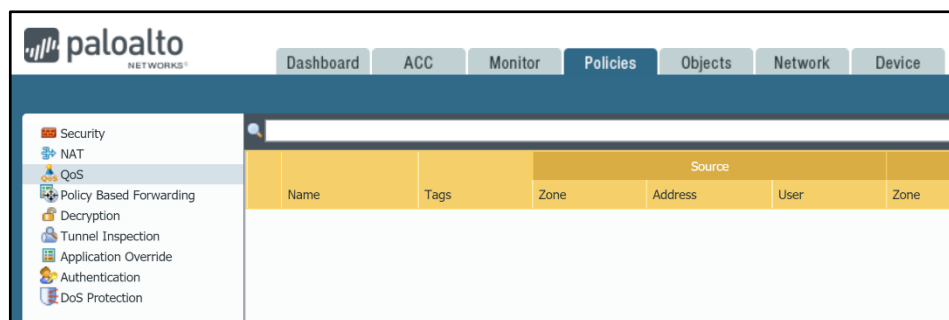
4. Configure QoS Policy

a. Purpose

QoS policy rules are used for assigning specific QoS treatment and class of service to traffic traversing the firewall. QoS rules provide almost identical level of granularity as security rules, and enable a precise approach in defining traffic shaping conditions.

b. Location

QoS rules are defined in the **Policies** tab under **QoS** in the menu on the left.

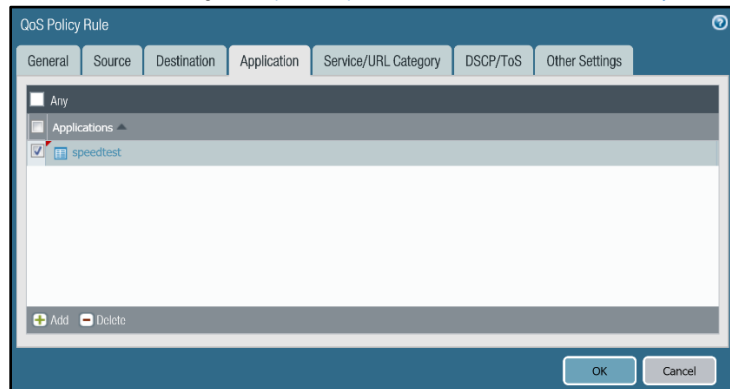


c. Creating QoS Rule

- Click on **Policies > QoS**, then click on **Add** button at the bottom.
- Type "SpeedTest" in the **Name** field, then switch to **Source** tab.
- Define the Source Zone as **Trust** (or any other applicable zone), and specify source addresses, address ranges and/or users, if applicable (use **Any** to apply the QoS rule to the entire network).
- In the **Destination** tab select **Untrust** (or any other applicable zone), and leave the **Destination Address** field empty.
- Under **Application** tab click **Add** button and select SpeedTest from the dropdown menu.

Firewalls

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



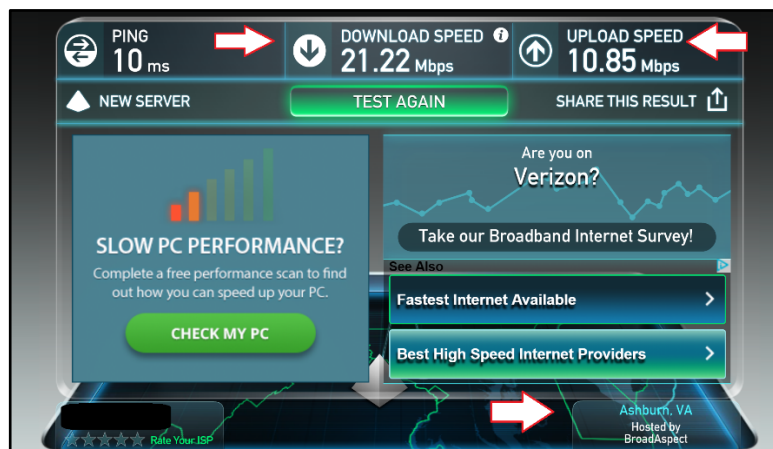
- vi. In the **Other Settings** tab select class 5 from the **Class** menu. Click on **OK**. Your screen should look identical to the screenshot below:

	Name	Source			Destination		Application	Service	DSCP/ToS	Class	Schedule
		Zone	Address	User	Zone	Address					
1	SpeedTest	Trust	any	any	Untrust	any	speedtest	any	any	5	none

- vii. Commit the configuration

5. Test QoS Policy

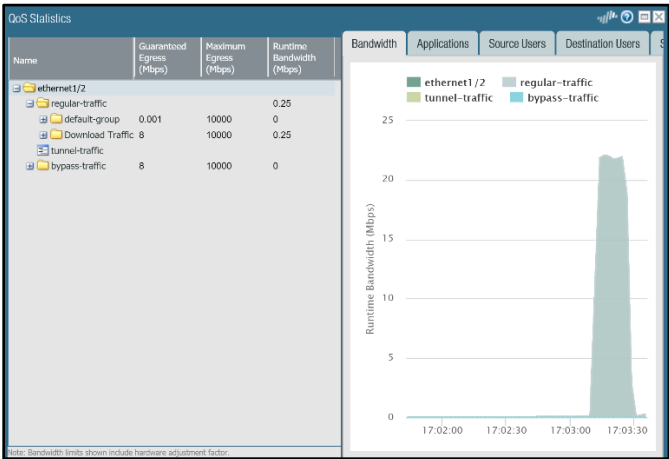
- i. In the web browser, assuming that the previous session is still open, click on **Test Again** button. Make sure that the same test server is selected for consistency, and observe that download and upload speeds are getting capped at approximately 22 and 11 Mbps.



- ii. Repeat the same test one more time. This time observe the QoS statistics under **Network > QoS > Statistics** for both interfaces:

Firewalls

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



Firewalls

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

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)
- c. For access to live Palo Alto Networks boxes for lab practice purposes please go to:
<https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>. This is a no charge service provided by Palo Alto Networks.

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*



Firewalls

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

Last Modified: June 25, 2018

