Palo Alto Networks
Firewall 8.0 Essentials:
Configuration and Management

Lab Guide

PAN-OS® 8.0

EDU-210

Courseware Version A

Palo Alto Networks® Technical Education

Palo Alto Networks, Inc.

https://www.paloaltonetworks.com

Table of Contents

Typographical Conventions

This guide uses the following typographical conventions for special terms and instructions.

Convention	Meaning	Example
Bolding	Names of selectable items in the web interface	Click **Security** to open the Security Rule Page

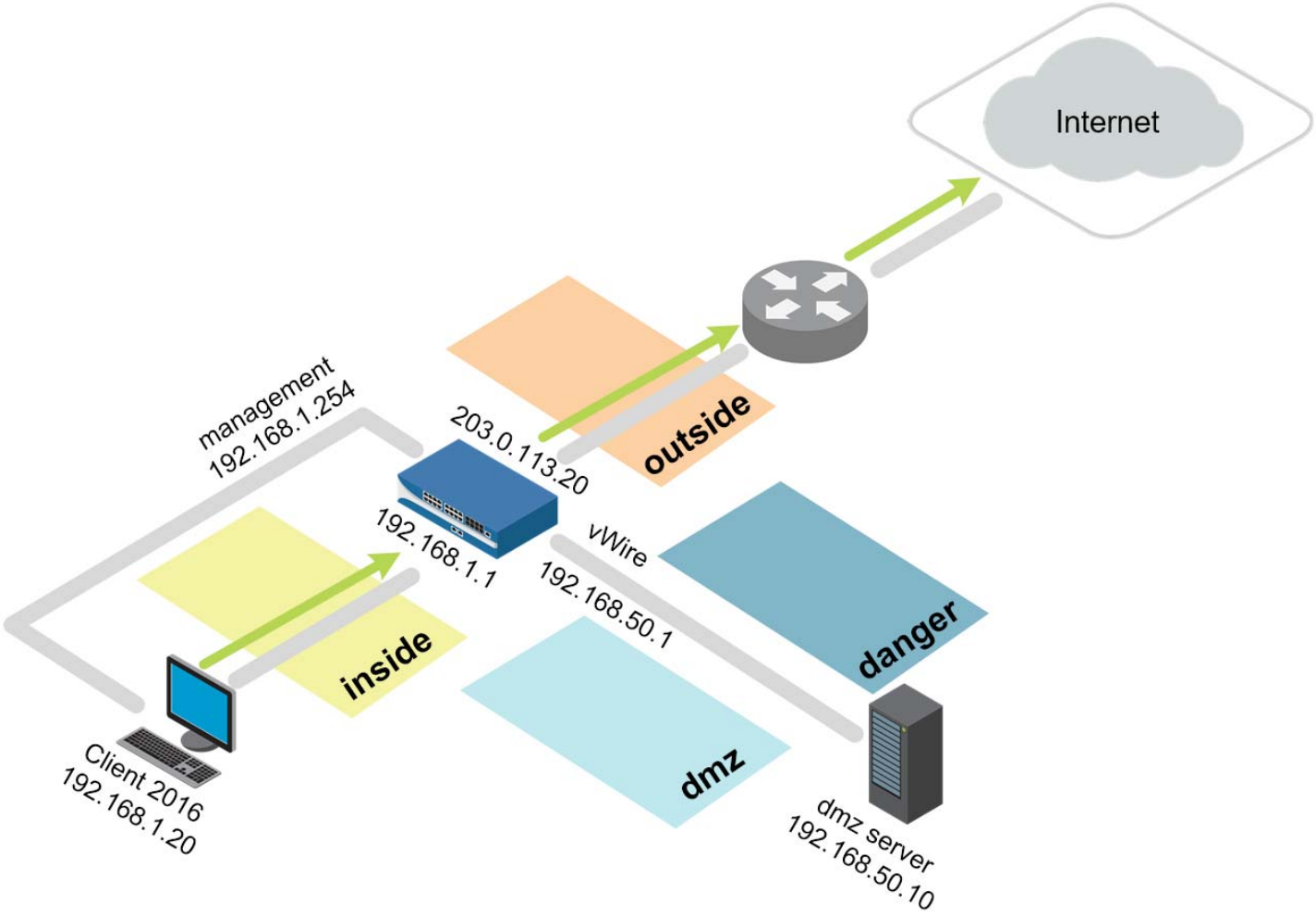
`Courier` font	Text that you enter and coding examples	Enter the following command:
		`a:\setup`
		The `show arp all` command yields this output:
		`username@hostname> show arp`
		`<output>`

Click	Click the left mouse button	Click **Administrators** under the Device tab
Right-click	Click the right mouse button	Right-click the number of a rule you want to copy, and select **Clone Rule**
< > (text enclosed in angle brackets)	Parameter in the Lab Settings Handout	Click **Add** again and select **<Internal Interface>**

How to Use This Lab Guide

The Lab Guide contains exercises that correspond to modules in the Student Guide. Each lab exercise consists of step-by-step, task-based labs. The final lab is based on a scenario that you will interpret and use to configure a comprehensive firewall solution.

The following diagram provides a basic overview of the lab environment:



1. Lab: Initial Configuration

Lab Objectives

- Load a configuration.
- Create an administrator role.
- Create a new administrator and apply an administrator role.
- Observe the newly created role permissions via the CLI and WebUI.
- Create and test a commit lock.
- Configure DNS servers for the firewall.
- Schedule dynamic updates.

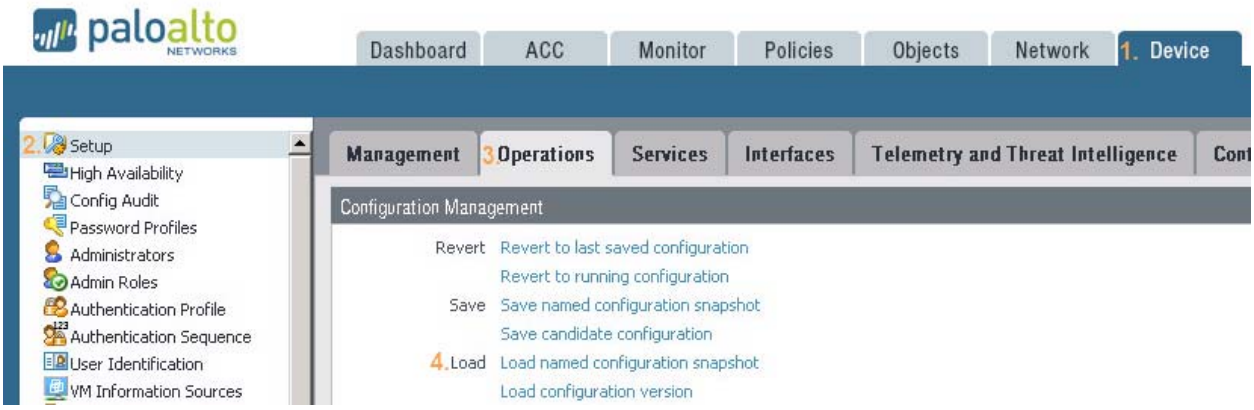
1.0 Connect to Your Student Firewall

1. Launch a browser and connect to `https://192.168.1.254`.
2. Log in to the Palo Alto Networks firewall using the following:

Parameter	Value #
Name	`admin`
Password	`admin`

1.1 Apply a Baseline Configuration to the Firewall

1. In the Palo Alto Networks firewall WebUI, select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



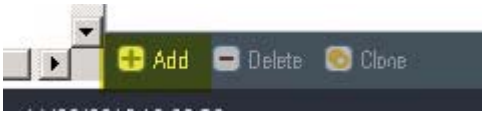
3. Click the drop-down list next to the Name text box and select **edu-210-lab-01**.
4. Click **OK**. After some time, a confirmation that the configuration has been loaded appears.
5. Click **Close**.
6. Click the **Commit** link at the top right of the WebUI. Click **Commit** and wait until the commit process is complete. Click **Close** to continue.

Note: Continue if warned about a full commit.

1.2 Add an Admin Role Profile

Admin Role Profiles are custom roles that determine the access privileges and responsibilities of administrative users.

1. Select **Device > Admin Roles**. 

2. Click **Add** in the lower-left corner of the panel to create a new administrator role:


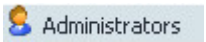
3. Enter the name `policy-admins-profile`.
4. Click the **Web UI** tab. Click the ✓ icon to disable the following:

Parameter	Value #
Monitor	⊗ #
Network	⊗
Device	⊗
Privacy	⊗

5. Click the **XML API** tab and verify that all items are ⊗ disabled.
6. Click the **Command Line** tab and verify that the selection is **none**.
7. Click 

to continue.

1.3 Add an Administrator Account

1. Select **Device > Administrators**. 

2. Click 

in the lower-left corner of the panel to open the Administrator configuration window.
3. Configure the following:

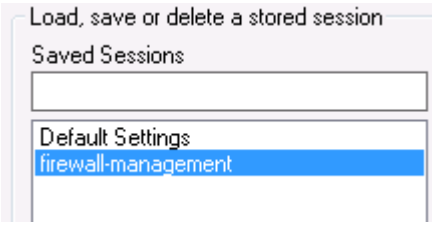
Parameter	Value
Name	`policy-admin#`
Authentication Profile	**None**
Password	`paloalto#`

Parameter	Value
Administrator Type	Role Based
Profile	**policy-admins-profile**
Password Profile	**None**

4. Click **OK**.
5. Commit all changes.

1.4 Test the policy-admin User

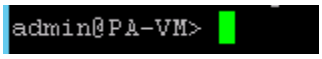
1. Open **PuTTY** from the Windows desktop.
2. Double-click **firewall-management**:



3. Log in using the following information:

Parameter	Value #
Name	`admin`
Password	`admin`

The role assigned to this account is allowed CLI access, so the connection should succeed.



4. Close the **PuTTY** window and then open **PuTTY** again.
5. Open an SSH connection to **firewall-management**.
6. Log in using the following information (the window will close if authentication is successful):

Parameter	Value #
Name	`policy-admin`
Password	`paloalto`

The PuTTY window closes because the admin role assigned to this account denies CLI access.

7. Open a *different* browser (not a tab) in private/incognito mode and browse to `https://192.168.1.254`. A Certificate Warning might appear.
8. Click through the Certificate Warning. The Palo Alto Networks firewall login page opens.
9. Log in using the following information (this action must be done in a different browser):

Parameter	Value #
Name	`policy-admin`
Password	`paloalto`

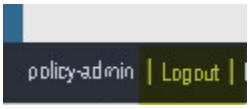
10. **Close** the Welcome window if one is presented.
11. Explore the available functionality of the WebUI. Notice that several tabs and functions are excluded from the interface because of the Admin Role assigned to this user account.

1.5 Take a Commit Lock and Test the Lock

The web interface supports multiple concurrent administrator sessions by enabling an administrator to lock the candidate or running configuration so that other administrators cannot change the configuration until the lock is removed.

1. From the WebUI where you are logged in as *policy-admin*, click the **transaction lock** icon to the right of the Commit link. The Locks windows opens.

2. Click **Take Lock**. A Take lock window opens.
3. Set the Type to **Commit**, and click **OK**. The policy-admin lock is listed in the Locks window.
4. Click **Close** to close the Locks window.
5. Click the **Logout** button on the bottom-left corner of the WebUI:



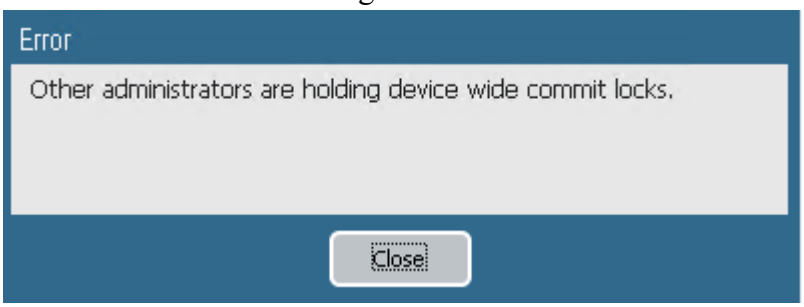
6. Close the policy-admin browser window.
7. Return to the WebUI where you are logged in as *admin*.
8. Click the **Device > Administrators** link. The WebUI refreshes. Notice the lock icon in the upper-right corner of the WebUI. 

9. Click 

to add another administrator account.
10. Configure the following:

Parameter	Value
Name	`test-lock#`
Authentication Profile	**None**
Password	`paloalto#`
Administrator Type	Role Based
Profile	**policy-admins-profile**
Password Profile	**None**

11. Click **OK**. The new test-lock user is listed.
12. Commit all changes. Although you could add a new administrator account, you are not allowed to commit the changes because of the Commit lock set by the policy-admin user:



13. Click **Close**.
14. Click the **transaction lock** icon in the upper-right corner:

15. Select the **policy-admin** lock and click **Remove Lock**:

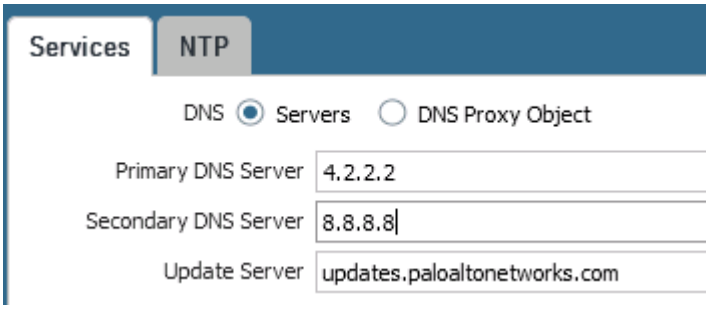
Note: The user that took the lock or any superuser can remove a lock.

16. Click **OK** and the lock is removed from the list.
17. Click **Close**.
18. Commit all changes. You can now commit the changes.
19. Select the **test-lock** user and then click Delete to delete the test-lock user.
20. Click **Yes** to confirm the deletion.
21. Commit all changes.

1.6 Verify the Update and DNS Servers

The DNS server configuration settings are used for all DNS queries that the firewall initiates in support of FQDN address objects, logging, and firewall management.

1. Select **Device > Setup > Services**.
2. Open the Services window by clicking the  icon in the upper-right corner of the Services panel:



3. Verify that **4.2.2.2** is the Primary DNS Server and that **8.8.8.8** is the Secondary DNS Server.
4. Verify that **updates.paloaltonetworks.com** is the Update Server.
5. Click **OK**.

1.7 Schedule Dynamic Updates

Palo Alto Networks regularly posts updates for application detection, threat protection, and GlobalProtect data files through dynamic updates.

1. Select **Device > Dynamic Updates**. 

2. Locate and click the hyperlink on the far right of **Antivirus**:

   The scheduling window opens. Antivirus signatures are released daily.
3. Configure the following:

Parameter	Value
Recurrence	**Daily#**
Time	**01:02**
Action	**download-and-install#**

4. Click **OK**.
5. Locate and click the hyperlink on the far right of **Application and Threats**. The scheduling window opens. Application and Threat signatures are released weekly.
6. Configure the following:

Parameter	Value
Recurrence	**Weekly#**
Day	**wednesday**
Time	**01:05**
Action	**download-and-install#**

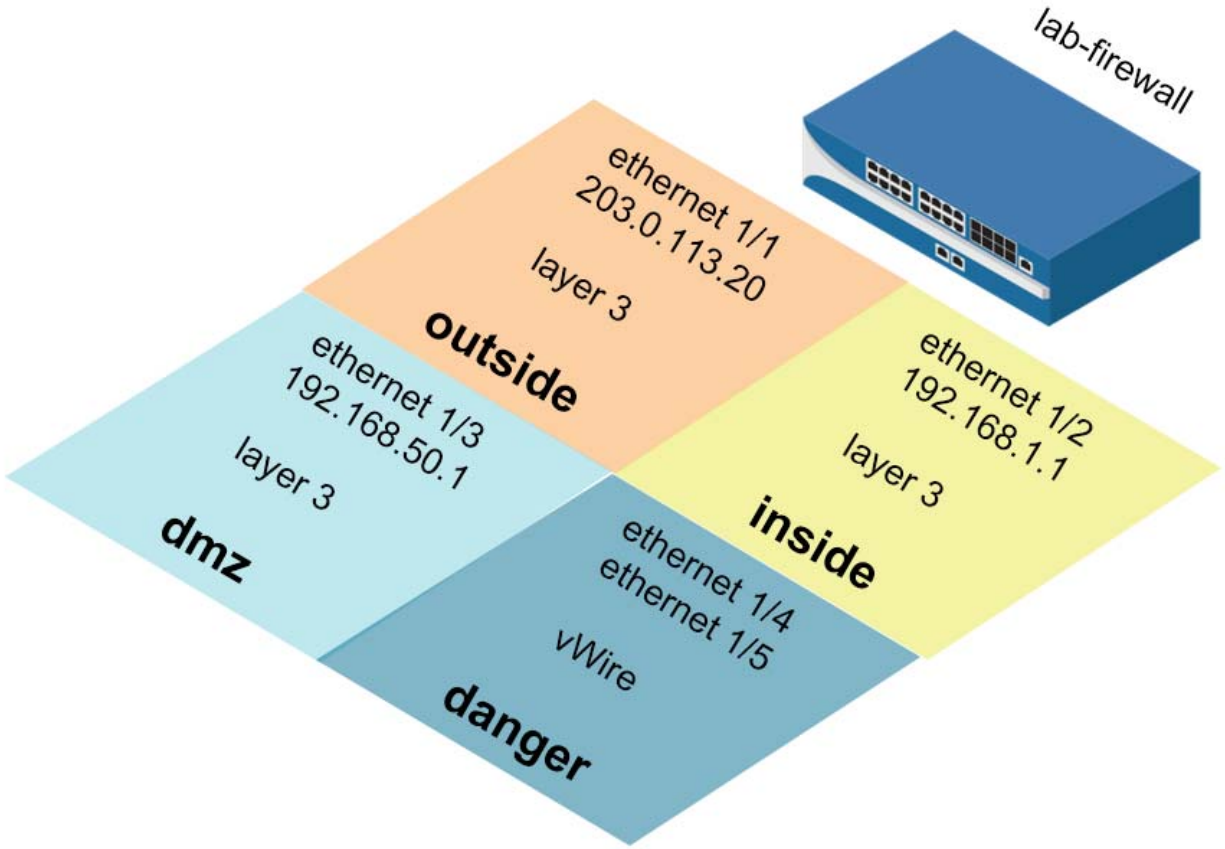
7. Click **OK**.
8. Locate and click the hyperlink on the far right of **WildFire**. The scheduling window opens. WildFire signatures can be available within five minutes.
9. Configure the following:

Parameter	Value
Recurrence	**Every Minute#**
Action	**download-and-install#**

10. Click **OK**.
11. Commit all changes.

Stop. This is the end of the Initial Configuration lab.

2. Lab: Interface Configuration

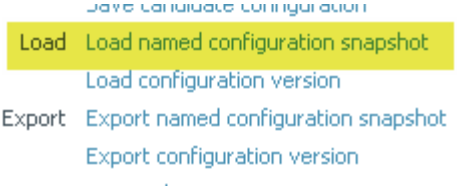


Lab Objectives

- Create Security zones two different ways and observe the time saved.
- Create Interface Management Profiles to allow ping and responses pages.
- Configure Ethernet interfaces to observe DHCP client options and static configuration.
- Create a virtual router and attach configured Ethernet interfaces.
- Test connectivity with automatic default route configuration and static configuration.

2.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-02** and click **OK**.
4. Click **Close**.
5. Commit all changes.

2.1 Create New Security Zones

Security zones are a logical way to group physical and virtual interfaces on the firewall in order to control and log the traffic that traverses your network through the firewall. An interface on the firewall must be assigned to a Security zone before the interface can process traffic. A zone can have multiple interfaces of the same type (for example, Tap, Layer 2, or Layer 3 interfaces) assigned to it, but an interface can belong to only one zone.

1. Select **Network > Zones**. Zones
2. Click Add to create a new zone. The Zone configuration window opens.
3. Configure the following:

Parameter	Value
Name	`outside#`
Type	**Layer3**

4. Click **OK** to close the Zone configuration window. The outside zone is the only zone created in this task. You will add an Ethernet interface to this zone in a later lab step.

2.2 Create Interface Management Profiles

An Interface Management Profile protects the firewall from unauthorized access by defining the services and IP addresses that a firewall interface permits. You can assign an Interface Management Profile to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (Aggregate, VLAN, Loopback, and Tunnel interfaces).

1. Select **Network > Network Profiles > Interface Mgmt**. Interface Mgmt
2. Click Add to open the Interface Management Profile configuration window.
3. Configure the following:

Parameter	Value
Name	`ping-response-pages#`
Permitted Services	☑ Ping ☑ Response Pages

4. Click **OK** to close the Interface Management Profile configuration window.

5. Click 

to create another Interface Management Profile.
6. Configure the following:

Parameter	Value
Name	`ping#`
Permitted Services	 #

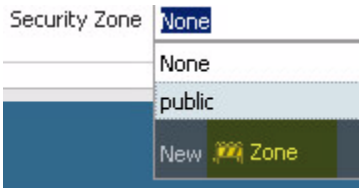
7. Click **OK** to close the Interface Management Profile configuration window.

2.3 Configure Ethernet Interfaces

1. Select **Network > Interfaces > Ethernet**.
2. Click to open **ethernet1/2**.
3. Configure the following:

Parameter	Value#
Comment	`inside interface`
Interface Type	**Layer3**
Virtual Router	**None**

4. Click the **Security Zone** drop-down list and select **New Zone**:



The Zone configuration window opens.

5. Configure the following:

Parameter	Value
Name	`inside#`
Type	Select **Layer3**

6. Click **OK** to close the Zone configuration window.
7. Click the Ethernet Interface **IPv4** tab.
8. Configure the following:

Parameter	Value
Type	**Static**
IP	Click **Add** and type `192.168.1.1/24#`

9. Click the **Advanced** tab.
10. Click the **Management Profile** drop-down list and select **ping-response-pages**.
11. Click **OK** to close the Ethernet Interface configuration window.
12. Click to open **ethernet1/3**.
13. Configure the following:

Parameter	Value#
Comment	`dmz interface`
Interface Type	**Layer3**
Virtual Router	**None**

14. Click the **Security Zone** drop-down list and select **New Zone**. The Zone configuration window opens.
15. Configure the following:

Parameter	Value
Name	`dmz`
Type	**Layer3** should be selected

16. Click **OK** to close the Zone configuration window.
17. Click the **IPv4** tab.
18. Configure the following:

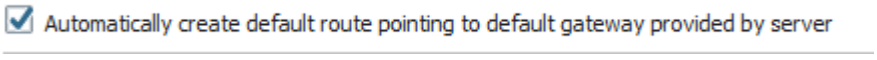
Parameter	Value
Type	**Static**
IP	Click **Add** and type `192.168.50.1/24#`

19. Click the **Advanced** tab.
20. Click the **Management Profile** drop-down list and select **ping**.
21. Click **OK** to close the Ethernet Interface configuration window.
22. Click to open **ethernet1/1**.
23. Configure the following:

Parameter	Value#
Comment	`outside interface`
Interface Type	**Layer3**
Virtual Router	**None**
Security Zone	**outside**

24. Click the **IPv4** tab and configure the following:

Parameter	Value
Type	**DHCP Client**

Note the 

option. This option will automatically install a default route based on DHCP-option 3.

25. Click **OK** to close the Ethernet Interface configuration window.
26. Click to open **ethernet1/4**.
27. Configure the following:

Parameter	Value#
Comment	`vWire danger`
Interface Type	**Virtual Wire**
Virtual Wire	**None**

28. Click the **Security Zone** drop-down list and select **New Zone**. The Zone configuration window opens.
29. Configure the following:

Parameter	Value
Name	`danger`
Type	**Virtual Wire** should be selected

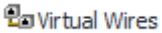
30. Click **OK** twice to close the Zone and Ethernet Interface configuration windows.
31. Click to open **ethernet1/5**.
32. Configure the following:

Parameter	Value#
Comment	`vWire danger`
Interface Type	**Virtual Wire**
Virtual Wire	**None**
Security Zone	**danger**

33. Click **OK** to close the Ethernet Interface configuration window.

2.4 Create a Virtual Wire

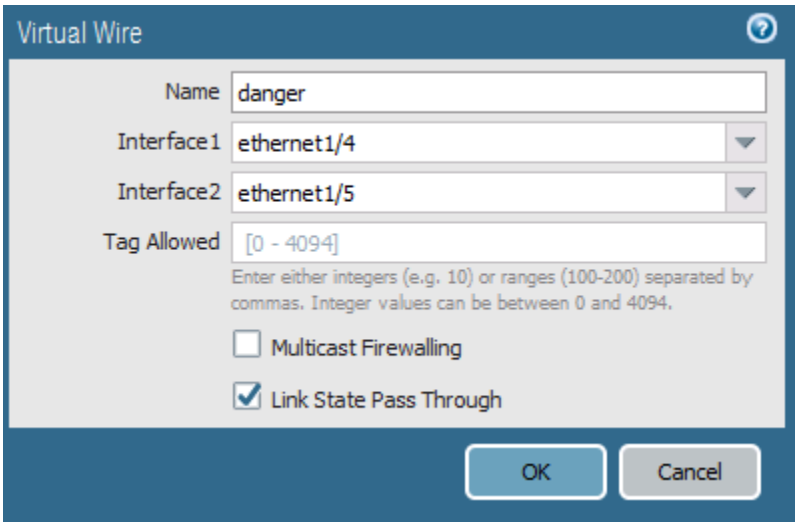
A virtual wire interface binds two Ethernet ports together. A virtual wire interface allows all traffic or just selected VLAN traffic to pass between the ports. No other switching or routing services are available.

1. Select **Network > Virtual Wires**. 

2. Click 

and configure the following:

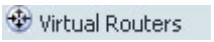
Parameter	Value#
Name	`danger`
Interface 1	**ethernet1/4**
Interface 2	**ethernet1/5**



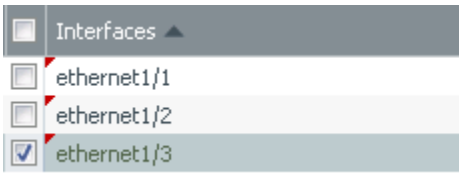
3. Click **OK**.

2.5 Create a Virtual Router

The firewall requires a virtual router to obtain routes to other subnets either using static routes that you manually define, or through participation in Layer 3 routing protocols that provide dynamic routes.

1. Select **Network > Virtual Routers**. 

2. Click the **default** virtual router.
3. Rename the default router `lab-vr`.
4. **Add** the following interfaces: **ethernet1/1**, **ethernet1/2**, and **ethernet1/3**.

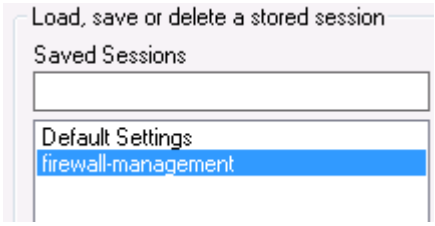


Note: This step also can be completed via each Ethernet Interface configuration window.

5. Click **OK**.
6. Commit all changes.

2.6 Test Connectivity

1. Open **PuTTY** from the Windows desktop.
2. Double-click **firewall-management**:



3. Log in using the following information:

Parameter	Value #
Name	`admin`
Password	`admin`

4. Enter the command `ping source 203.0.113.21 host 8.8.8.8`.
   Because a default route was automatically installed, you should be getting replies from 8.8.8.8:

```
admin@PA-VM> ping source 203.0.113.21 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 203.0.113.21 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=18.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=17.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=16.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=14.5 ms
```

5. On the lab environment Windows desktop, open a command-prompt window.
6. Type the command `ping 192.168.1.1`:

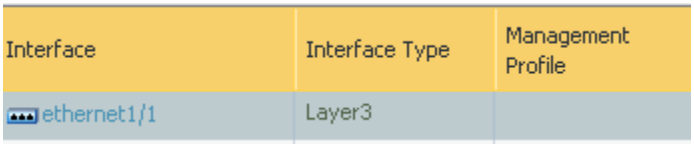
```
C:\Windows\System32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=26ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=31ms TTL=64
```

7. Verify that you get a reply before proceeding.
8. Close the command-prompt window.

2.7 Modify Outside Interface Configuration

1. Select **Network > Interfaces > Ethernet**.
2. Select but, do not open: **ethernet1/1**.

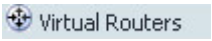


3. Click  then click **Yes**.
4. Click and open **ethernet 1/1**.
5. Configure the following:

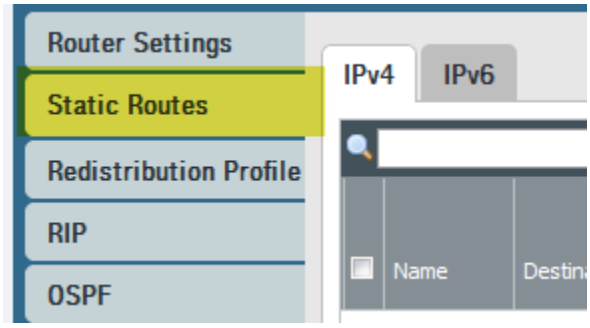
Parameter	Value
Comment	`outside interface`
Interface Type	**Layer3**
Virtual Router	**lab-vr**
Security Zone	**outside**

6. Click the **IPv4** tab and configure the following:

Parameter	Value
Type	**Static**
IP	`203.0.113.20/24`

7. Click **OK** to close the Ethernet Interface configuration window.
8. Select **Network > Virtual Routers**. 

9. Click to open the **lab-vr** virtual router.
10. Click the **Static Routes** vertical tab:



11. Click  to configure the following static route:

Parameter	Value#
Name	`default-route#`
Destination	`0.0.0.0/0#`
Interface	**ethernet1/1**
Next Hop	**IP Address**
Next Hop IP Address	`203.0.113.1`

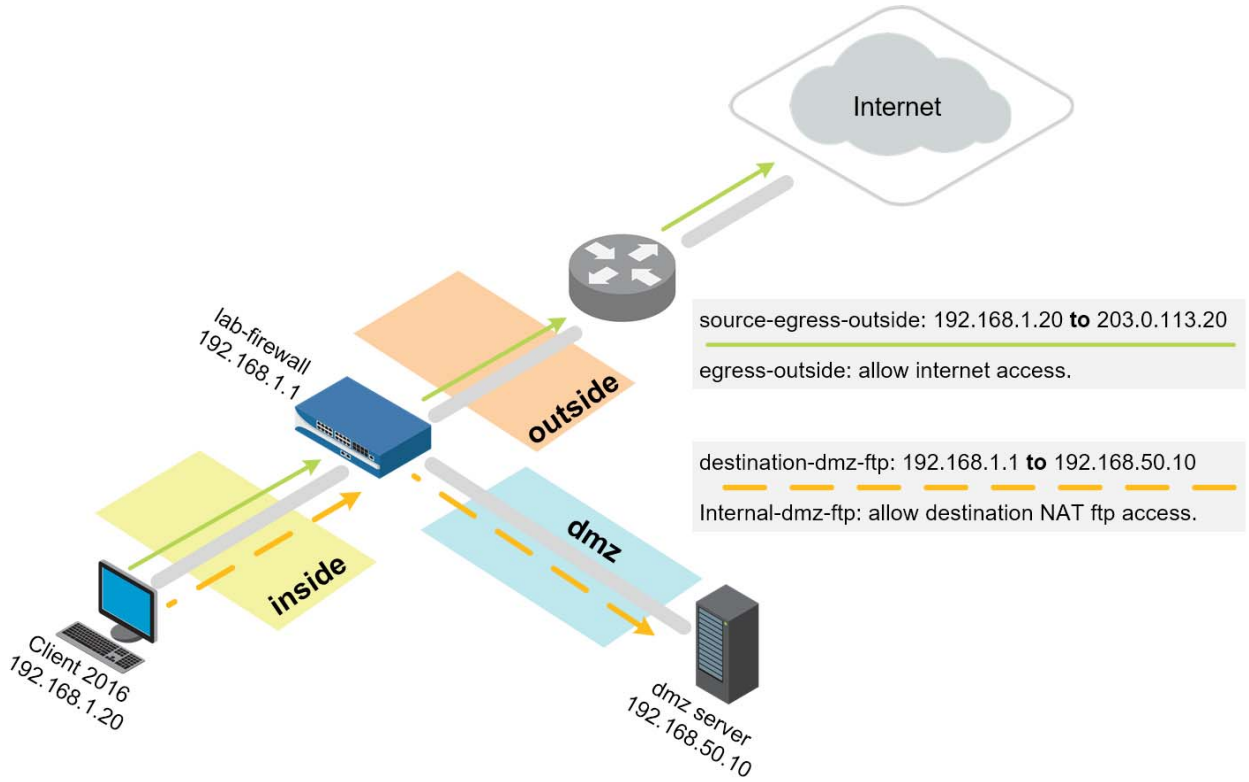
12. Click **OK** to add the static route and then click **OK** again to close the Virtual Router – lab-vr configuration window.
13.  all changes.
14. Make the PuTTY window that was used to ping 8.8.8.8 the active window.
15. Type the command `ping source 203.0.113.20 host 8.8.8.8`.
    You should be able to successfully ping 8.8.8.8.

```
admin@PA-VM> ping source 203.0.113.20 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 203.0.113.20 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=56.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=14.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=14.0 ms
```

16. Close the **PuTTY** window.

Stop. This is the end of the Interface Configuration lab.

3. Lab: Security and NAT Policies

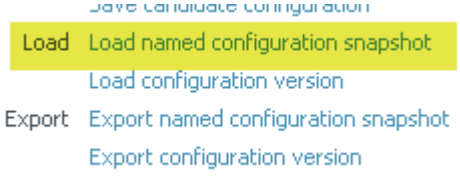


Lab Objectives

- Create tags for later use with Security policy rules.
- Create a basic source NAT rule to allow outbound access and an associated Security policy rule to allow the traffic.
- Create a destination NAT rule for FTP server and an associated Security policy rule to allow the traffic.

3.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-03** and click **OK**.
4. Click **Close**.
5. Commit all changes.

3.1 Create Tags

Tags allow you to group objects using keywords or phrases. Tags can be applied to Address objects, Address Groups (static and dynamic), zones, services, Service Groups, and policy rules. You can use a tag to sort or filter objects, and to visually distinguish objects because they can have color. When a color is applied to a tag, the Policies tab displays the object with a background color.

1. Select **Objects > Tags**. 

2. Click 

to define a new tag.
3. Configure the following:

Parameter	Value#
Name	Select **danger**
Color	**Purple**

4. Click **OK** to close the Tag configuration window.
5. Click 

again to define another new tag.
6. Configure the following:

Parameter	Value#
Name	`egress`
Color	**Blue**

7. Click **OK** to close the Tag configuration window.
8. Click 

again to define another new tag.
9. Configure the following:

Parameter	Value#
Name	Select **dmz**
Color	**Orange**

10. Click **OK** to close the Tag configuration window.
11. Click 

again to define another new tag.
12. Configure the following:

Parameter	Value#
Name	internal
Color	**Yellow**

13. Click **OK** to close the Tag configuration window.

3.2 Create a Source NAT Policy

1. Select **Policies > NAT**. 

2. Click 

to define a new source NAT policy.
3. Configure the following:

Parameter	Value#
Name	`source-egress-outside#`
Tags	**egress**

4. Click the **Original Packet** tab and configure the following:

Parameter	Value#
Source Zone	**inside**
Destination Zone	**outside**
Destination Interface	**ethernet1/1**

5. Click the **Translated Packet** tab and configure the following:

Parameter	Value#
Translation Type	**Dynamic IP And Port**
Address Type	**Interface Address**
Interface	**ethernet1/1**
IP Address	Select **203.0.113.20/24** (Make sure to *select* the interface IP address, do not *type* it.)

6. Click **OK** to close the NAT Policy Rule configuration window.

You will not be able to access the internet yet because you still need to configure a Security policy to allow traffic to flow between zones.

3.3 Create Security Policy Rules

Security policy rules reference Security zones and enable you to allow, restrict, and track traffic on your network based on the application, user or user group, and service (port and protocol).

1. Select **Policies > Security**. 

2. Click  to define a Security policy rule.
3. Configure the following:

Parameter	Value#
Name	`egress-outside`
Rule Type	**universal (default)**
Tags	**egress**

4. Click the **Source** tab and configure the following:

Parameter	Value#
Source Zone	**inside**
Source Address	**Any**

5. Click the **Destination** tab and configure the following:

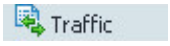
Parameter	Value#
Destination Zone	**outside**
Destination Address	**Any**

6. Click the **Application** tab and verify that  is checked.
7. Click the **Service/URL Category** tab and verify that  is selected.
8. Click the **Actions** tab and verify the following:

Parameter	Value#
Action Setting	**Allow**
Log Setting	**Log at Session End**

9. Click **OK** to close the Security Policy Rule configuration window.
10.  all changes.

3.4 Verify Internet Connectivity

1. Test internet connectivity by opening a different browser in private/incognito mode and browse to `msn.com` and `shutterfly.com`.
2. In the WebUI select **Monitor > Logs > Traffic**. 
3. Traffic log entries should be present based on the internet test. Verify that there is allowed traffic that matches the Security policy rule **egress-outside**:

Destination	To Port	Application	Action	Rule
159.127.41...	443	ssl	allow	egress-outside
162.248.16...	443	ssl	allow	egress-outside
162.248.16...	443	ssl	allow	egress-outside

3.5 Create FTP Service

When you define Security policy rules for specific applications, you can select one or more services that limit the port numbers that the applications can use.

1. In the WebUI select **Objects > Services**. 

2. Click 

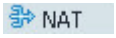
to create a new service using the following:

Parameter	Value#
Name	`service-ftp`
Destination Port	`20-21`

3. Click **OK** to close the Service configuration window.

3.6 Create a Destination NAT Policy

You are configuring destination NAT in the lab to get familiar with how destination NAT works, not because it is necessary for the lab environment.

1. In the WebUI select **Policies > NAT**. 

2. Click 

to define a new destination NAT policy rule.
3. Configure the following:

Parameter	Value#
Name	`destination-dmz-ftp`
Tags	**internal**

4. Click the **Original Packet** tab and configure the following:

Parameter	Value#
Source Zone	**inside**
Destination Zone	**inside**
Destination Interface	**ethernet1/2**
Service	**service-ftp**

Parameter	Value#
Destination Address	`192.168.1.1`

5. Click the **Translated Packet** tab and configure the following:

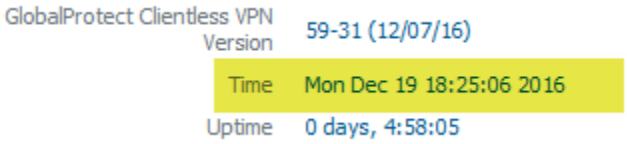
Parameter	Value#
Destination Address Translation	Select the check box
Translated Address	`192.168.50.10` (address of DMZ Server)

6. Click **OK** to close the NAT Policy configuration window.

3.7 Create a Security Policy Rule

1. Click the **Dashboard** tab. 

2. Annotate the current time referenced by the firewall:



3. Select **Policies > Security**. 

4. Click 

to define a new Security policy rule.
5. Configure the following:

Parameter	Value#
Name	`internal-dmz-ftp`
Rule Type	**universal (default)**
Tags	**internal**

6. Click the **Source** tab and configure the following:

Parameter	Value#
Source Zone	**inside**

7. Click the **Destination** tab and configure the following:

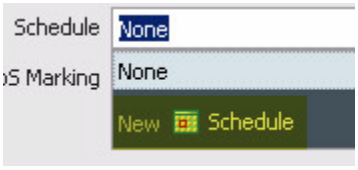
Parameter	Value#
Destination Zone	**dmz**

Parameter	Value#
Destination Address	`192.168.1.1`

8. Click the **Service/URL Category** tab and configure the following:

Parameter	Value#
Service	**service-ftp**

9. Click the **Actions** tab and verify that **Allow** is selected.
10. Locate the **Schedule** drop-down list and select **New Schedule**:



By default, Security policy rules are always in effect (all dates and times). To limit a Security policy to specific times, you can define schedules and then apply them to the appropriate policy rules.

11. Configure the following:

Parameter	Value#
Name	`internal-dmz-ftp`
Recurrence	**Daily**
Start Time	5 minutes from the time annotated in Step 2.
End time	2 hours from the current firewall time.

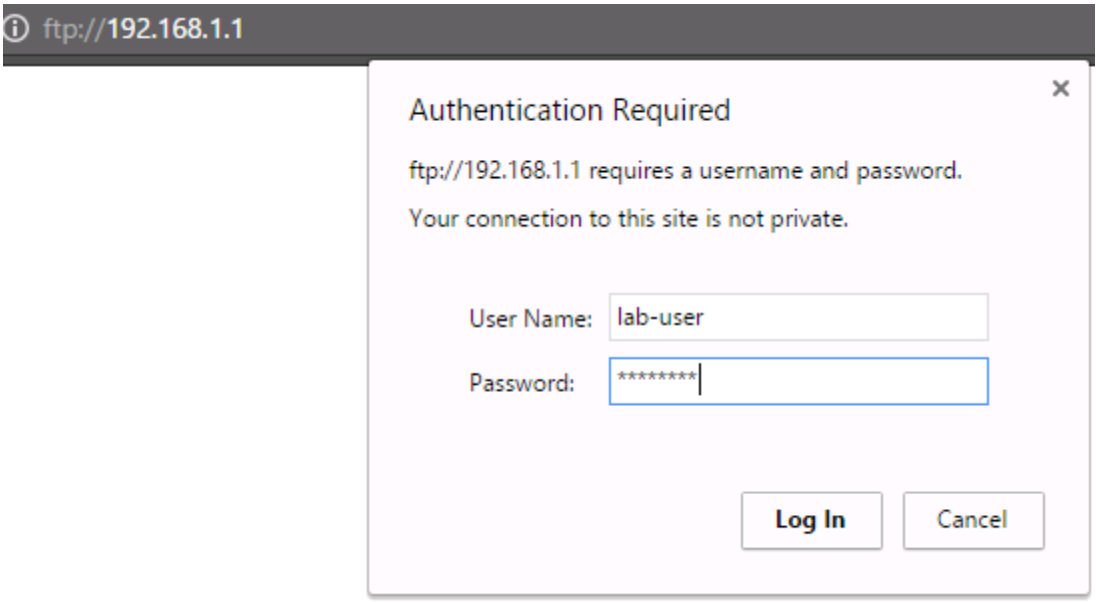
Note: Input time in a 24-hour format.

12. Click **OK** to close the Schedule configuration window.
13. Click **OK** to close the Security Policy Rule configuration window.
14. Commit all changes.

3.8 Test the Connection

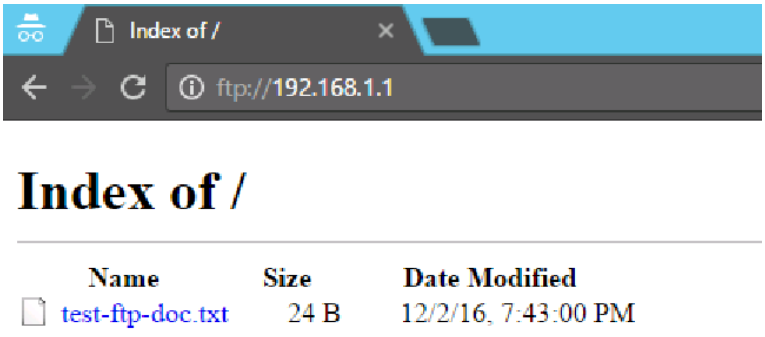
1. Wait for the scheduled time to start for the internal-dmz-ftp Security policy rule.
2. Open a new Chrome browser window in private mode and browse to `ftp://192.168.1.1`.
3. At the prompt for login information, enter the following:

Parameter	Value#
User Name	`lab-user`
Password	`paloalto`



192.168.1.1 is the inside interface address on the firewall. The firewall is not hosting the FTP server. The fact that you were prompted for a username indicates that FTP was successfully passed through the firewall using destination NAT.

4. Verify that you can view the directory listing and then close the Chrome browser window:



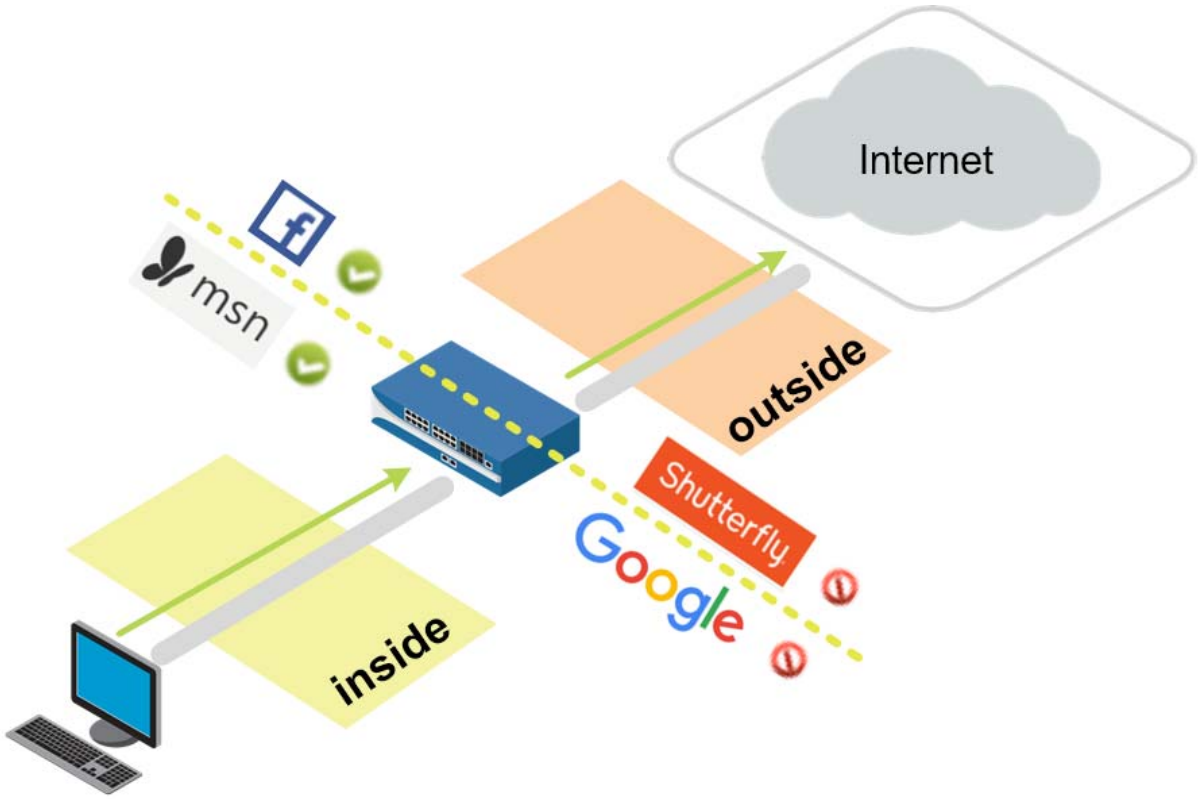
5. In the WebUI select **Monitor > Logs > Traffic**. 

6. Find the entries where the application ftp has been allowed by rule internal-dmz-ftp. Notice the Destination address and rule matching:

Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
192.168.1.1	23859	ftp	allow	internal-dmz-ftp	tcp-fin	432
192.168.1.1	53944	ftp	allow	internal-dmz-ftp	tcp-fin	432
192.168.1.1	21	ftp	allow	internal-dmz-ftp	tcp-fin	880

Stop. This is the end of the Security and NAT Policies lab.

4. Lab: App-ID

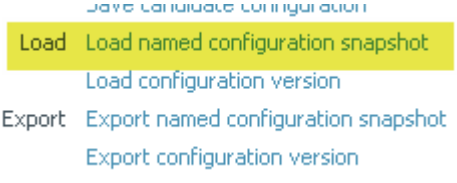


Lab Objectives

- Create an application-aware Security policy rule.
- Enable interzone logging.
- Enable the application block page for blocked applications.
- Test application blocking with different applications
- Understand what the signature *web-browsing* really matches.
- Migrate older port-based rule to application-aware.
- Review logs associated with the traffic and browse the Application Command Center (ACC).

4.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-04** and click **OK**.
4. Click **Close**.
5. Commit all changes.

4.1 Create App-ID Security Policy Rule

1. Select **Policies > Security**. Security
2. Select the **egress-outside** Security policy rule without opening it.
3. Click Clone. The Clone configuration window opens.
4. On the Rule order drop-down list, select **Move top**.
5. Click **OK** to close the Clone configuration window.
6. With the original **egress-outside** Security policy rule still selected, click Disable. Notice that the egress-public rule is now grayed out and in italic fonts:

7. Click to open the cloned Security policy rule named **egress-outside-1**.
8. Configure the following:

Parameter	Value#
Name	`egress-outside-app-id`

9. Click the **Application** tab and configure the following:

Parameter	Value#

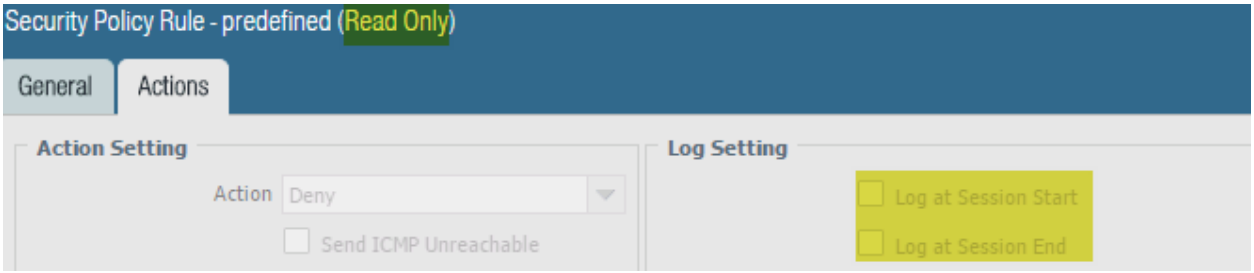
Applications	`dns`
	`facebook-base`
	`ssl`
	`web-browsing`

10. Click **OK** to close the Security Policy Rule configuration window.

4.2 Enable Interzone Logging

The intrazone-default and interzone-default Security policy rules are read-only by default.

1. Click to open the **interzone-default** Security policy rule. 5 interzone-defaul
2. Click the **Actions** tab. Note that Log at Session Start and Log at Session End are deselected, and cannot be edited:



3. Click **Cancel**.
4. With the **interzone-default** policy rule selected but not opened, click 

. The Security Policy Rule – predefined window opens.
5. Click the **Actions** tab.
6. Select **Log at Session End**.
7. Click **OK**.

4.3 Enable the Application Block Page

1. Select **Device > Response Pages**. 

2. Click **Disabled** to the right of Application Block Page:


3. Select the **Enable Application Block Page** check box. 

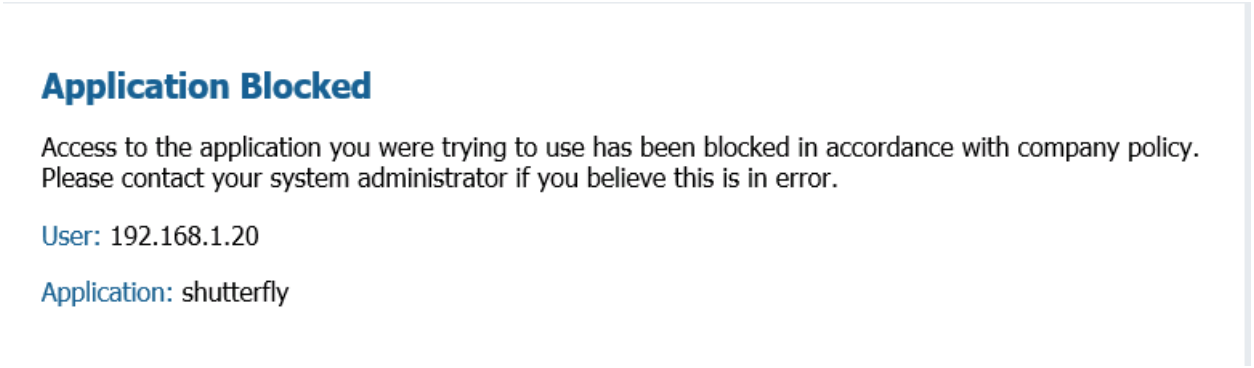
4. Click **OK**. The Application Block Page should now be enabled:


5. 

all changes.

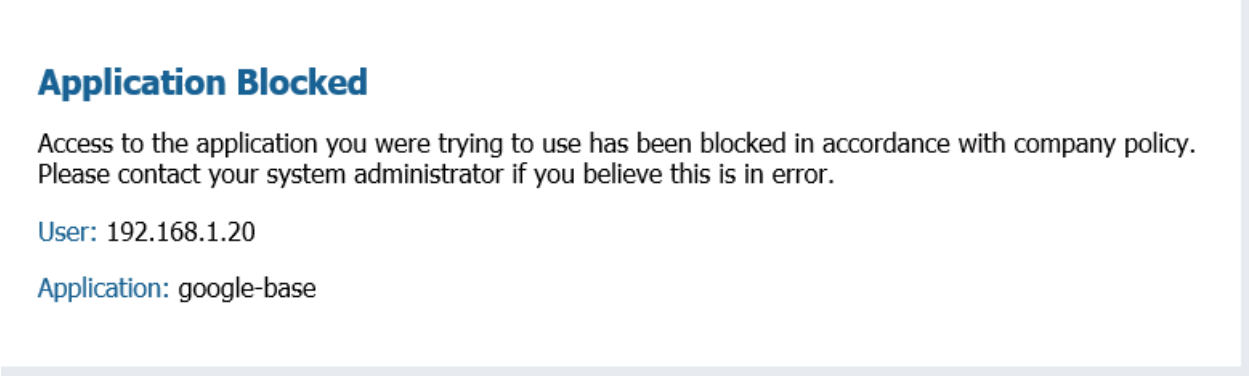
4.4 Test Application Blocking

1. Open a new browser window in private/incognito mode. You should be able to browse to `www.facebook.com` and `www.msn.com`.
2. Use private/incognito mode in a browser to connect to `http://www.shutterfly.com`. An Application Blocked page opens, indicating that the *shutterfly* application has been blocked:

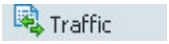


Why could you browse to Facebook and MSN but not to Shutterfly? MSN currently does not have an Application signature. Therefore, it falls under the Application signature web-browsing. However, an Application signature exists for Shutterfly and it is not currently allowed in any of the firewall Security policy rules.

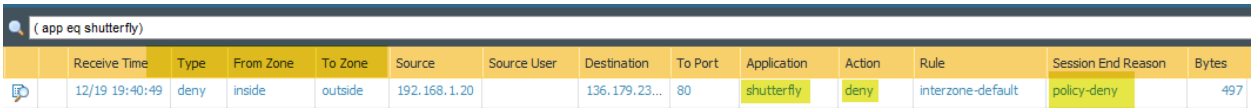
3. Browse to `google.com` and verify that google-base is also being blocked:



4.5 Review Logs

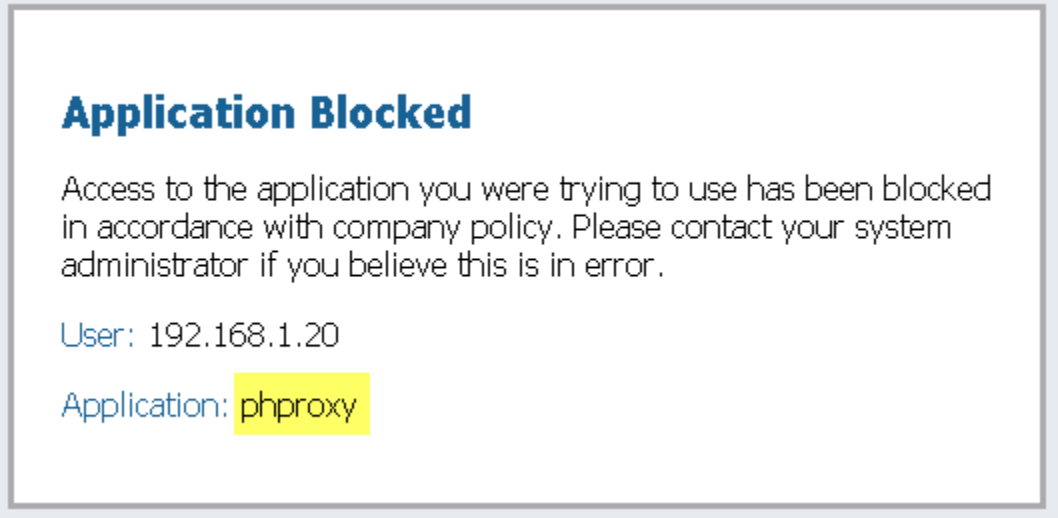
1. Select **Monitor > Logs > Traffic**. 

2. Type `( app eq shutterfly )` in the filter text box.
3. Press the **Enter** key.
   Only log entries whose Application is shutterfly are displayed.



4.6 Test Application Blocking

1. Try to work around the firewall's denial of access to Shutterfly by using a web proxy. In private/incognito mode in a browser, browse to `avoidr.com`.
2. Enter `www.shutterfly.com` in the text box near the bottom and click **Go**. An application block page opens showing that the phproxy application was blocked:



4.7 Review Logs

1. Select **Monitor > Logs > Traffic**. Traffic
2. Type `( app eq phproxy )` in the filter text box. The Traffic log entries indicates that the phproxy application has been blocked:

(app eq phproxy)

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason
	12/02 12:01:31	deny	private	public	192.168.1.20		74.208.215...	80	phproxy	reset-both	interzone-default	policy-deny
	12/02 12:01:31	deny	private	public	192.168.1.20		74.208.215...	80	phproxy	reset-both	interzone-default	policy-deny

Based on the information from your log, Shutterfly and phproxy are denied by the interzone-default Security policy rule.

Note: If the logging function of your interzone-default rule is not enabled, no information would be provided via the Traffic log.

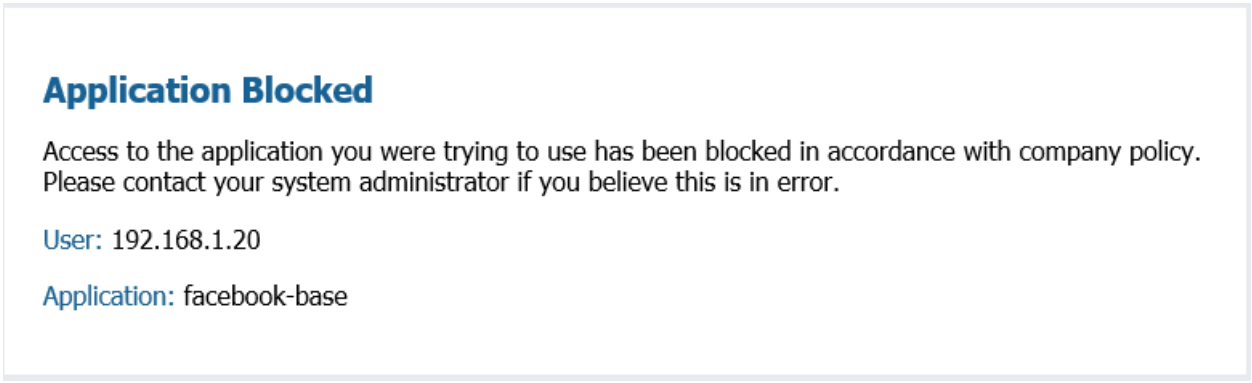
4.8 Modify the App-ID Security Policy Rule

1. In the WebUI select **Policies > Security**. Security
2. Add `shutterfly` and `google-base` to the egress-outside-app-id Security policy rule.
3. Remove facebook-base from the egress-outside-app-id Security policy rule.
4. Commit all changes.

4.9 Test App-ID Changes

1. Open a browser in private/incognito mode and browse to w`ww.shutterfly.com` and `google.com`. The application block page is no longer presented.

2. Open a new browser in private/incognito mode and browse to `www.facebook.com`
   The application block page now appears for facebook-base. **Note:** Do not use any previously used browser windows because browser caching can cause incorrect results.



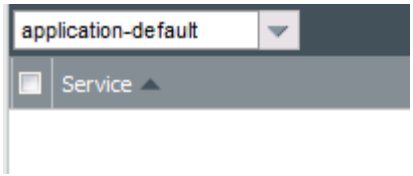
3. Close all browser windows except for the firewall WebUI.
   Note: The web-browsing Application signature only covers browsing that does not match any other Application signature.

4.10 Migrate Port-Based Rule to Application-Aware Rule

1. In the WebUI select **Policies > Security**. 

2. Click to open the **internal-dmz-ftp** Security policy rule:

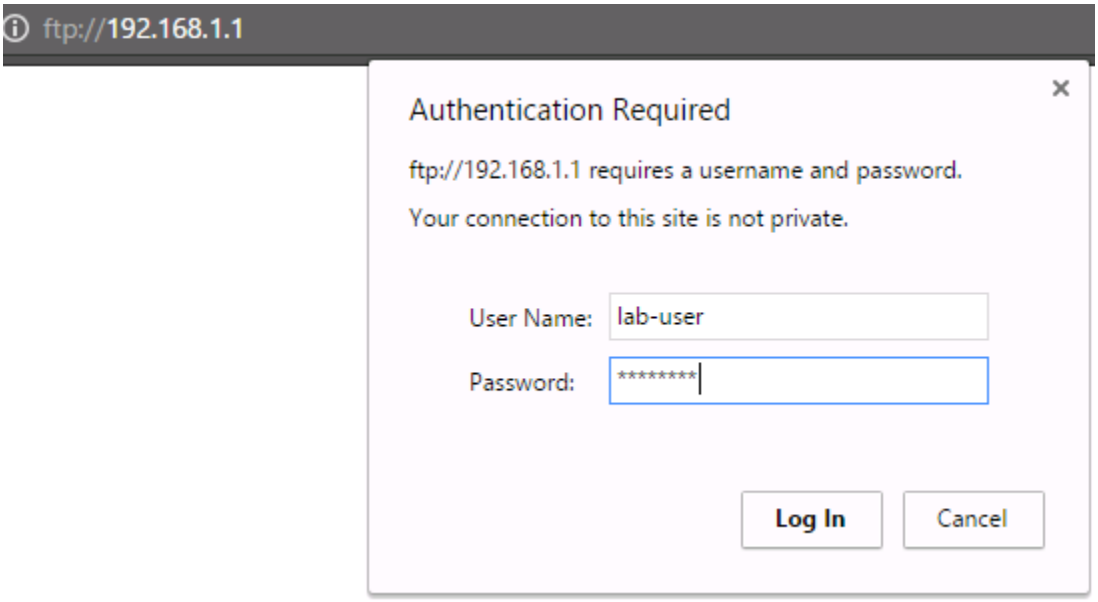
3. Click the **Application** tab and add `ftp`.
4. Click the **Service/URL Category** tab.
5. Delete **service-ftp** and select **application-default**.



   Selecting application-default does not change the service behavior because, in the application database, FTP is allowed only on ports 20 and 21 by default.
6. Click **OK**.
7. 

   all changes.
8. Open a new Chrome browser window in private mode and browse to `ftp://192.168.1.1`.
9. At the prompt for login information, enter the following (Credentials may be cached from previous login):

Parameter	Value#
User Name	`lab-user`
Password	`paloalto`



Notice that the connection succeeds and that you can log in to the FTP server with the updated Security policy rule.

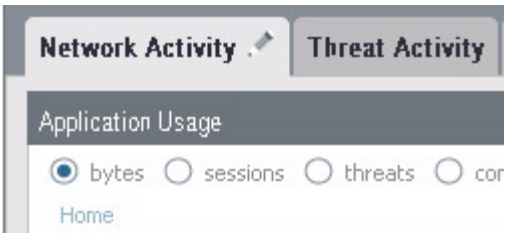
4.11 Observe the Application Command Center

The Application Command Center (ACC) is an analytical tool that provides actionable intelligence on activity within your network. The ACC uses the firewall logs as the source for graphically depicting traffic trends on your network. The graphical representation enables you to interact with the data and visualize the relationships between events on the network, including network use patterns, traffic patterns, and suspicious activity and anomalies.

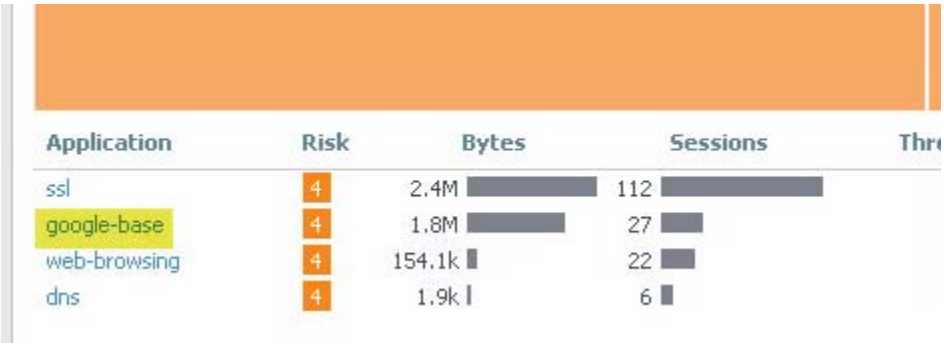
1. Click the **ACC** tab to access the Application Command Center:

2. Note that the upper-right corner of the ACC displays the total risk level for all traffic that has passed through the firewall thus far:

3. On the **Network Activity** tab, the Application Usage pane shows application traffic generated so far (because log aggregation is required, 15 minutes might pass before the ACC displays all applications).

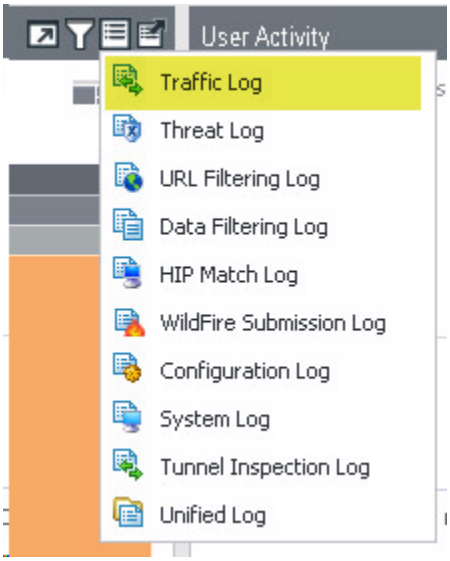


4. You can click any application listed in the Application Usage pane; *google-base* is used in this example:

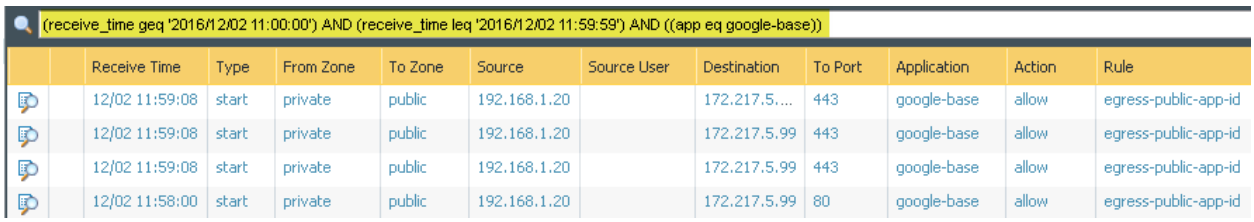


Notice that the Application Usage pane updates to present only google-base information.

5. Click the  icon and select **Traffic Log**:

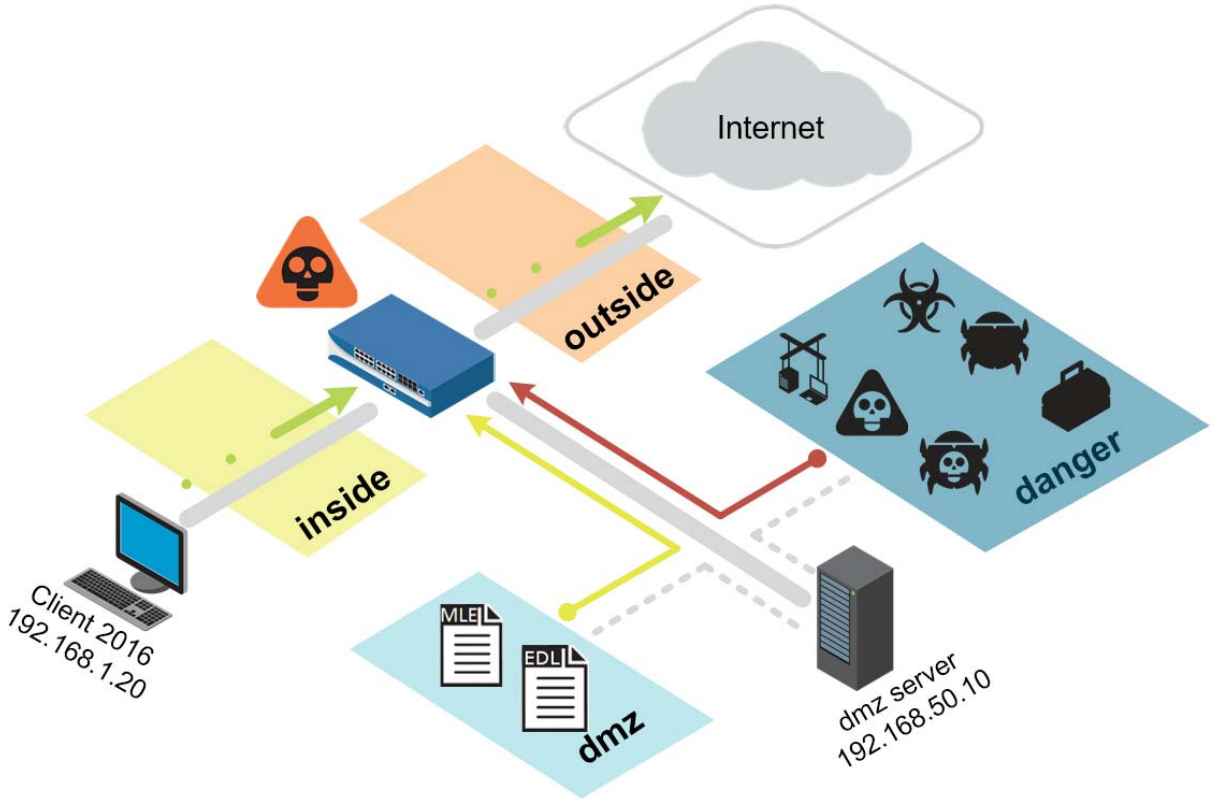


Notice that the WebUI generated the appropriate log filter and jumped to the applicable log information for the google-base application:



Stop. This is the end of the App-ID lab.

5. Lab: Content-ID

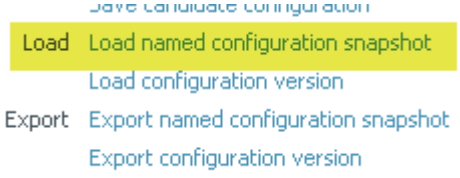


Lab Objectives

- Configure and test an Antivirus Security Profile.
- Configure and test an Anti-Spyware Security Profile.
- Configure and test the DNS sinkhole feature with an External Dynamic List.
- Configure and test a Vulnerability Security Profile.
- Configure and test a File Blocking Security Profile.
- Use the Virtual Wire mode and configure the danger zone.
- Generate threats and observe the actions taken.

5.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



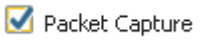
3. Select **edu-210-lab-05** and click **OK**.

4. Click **Close**.
5.  all changes.

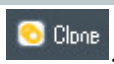
5.1 Create Security Policy Rule with an Antivirus Profile

Use an Antivirus Profile object to configure options to have the firewall scan for viruses on traffic matching a Security policy rule.

1. Select **Objects > Security Profiles > Antivirus**. 
2. Click  to create an Antivirus Profile.
3. Configure the following:

Parameter	Value#
Name	`lab-av`
Packet Capture	
Decoder	Set the Action column for http to **reset-server**

4. Click **OK** to close the Antivirus Profile configuration window.
5. Select **Policies > Security**. 
6. Select the **egress-outside-app-id** Security policy rule without opening it:

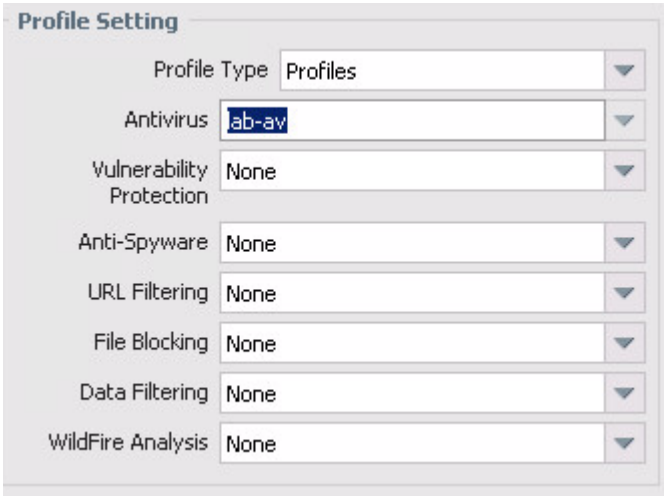

7. Click  . The Clone configuration window opens.
8. Select **Move top** from the **Rule Order** drop-down list.
9. Click **OK** to close the Clone configuration window.
10. With the original egress-outside-app-id still selected, click  .
11. Click to open the cloned Security policy rule named **egress-outside-app-id-1**.
12. Configure the following:

Parameter	Value#
Name	`egress-outside-av`
Tags	**egress**

13. Click the **Application** tab and configure the following:

Parameter	Value#
Applications	

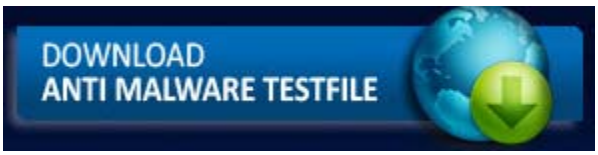
14. Click the **Actions** tab and configure the following:

Parameter	Value#
Profile Type	**Profiles**
Profile Setting	

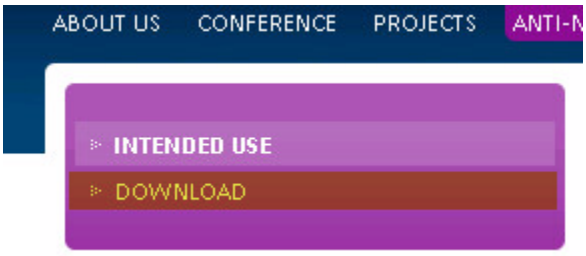
15. Click **OK** to close the Security Policy Rule configuration window.
16. Commit all changes.

5.2 Test Security Policy Rule

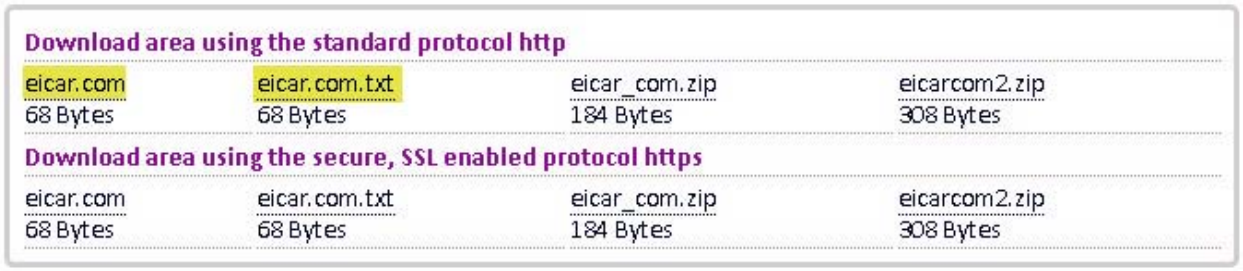
1. On your desktop, open a new browser in private/incognito mode and browse to `http://www.eicar.org`.
2. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner:



3. Click the **Download** link on the left of the web page:



4. Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using standard HTTP and *not* SSL-enabled HTTPS. The firewall will not be able to detect the viruses in an HTTPS connection until decryption is configured.



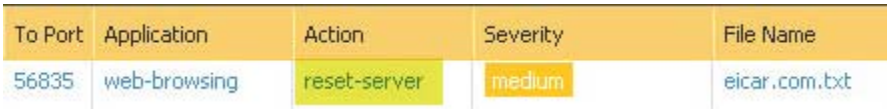
5. If prompted, **Save** the file. Do *not* open or run the file.

6. Close the browser window.

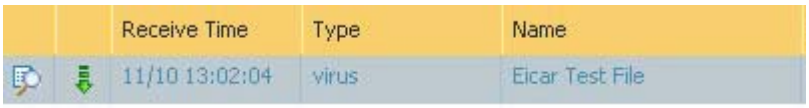
5.3 Review Logs

1. In the WebUI select **Monitor > Logs > Threat**. 

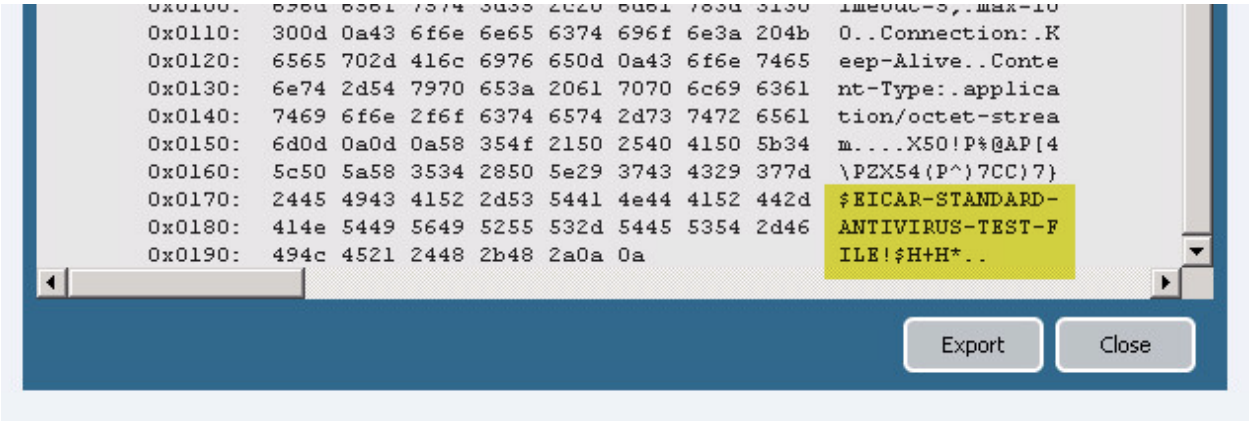
2. Find the log message that detected the **Eicar Test File**. Notice that the action for the file is **reset-server**:



3. Click the  icon on the left side of the entry for the **Eicar Test File** to display the packet capture (pcap):



Here is an example of what a pcap might look like:



Captured packets can be exported in pcap format and examined with an offline analyzer for further investigation.

4. After viewing the pcap, click **Close**.

5.4 Create Security Policy Rule with an Anti-Spyware Profile

1. Select **Objects > Security Profiles > Anti-Spyware**. 

2. Click  to create an Anti-Spyware Profile.

3. Configure the following:

Parameter	Value#
Name	`lab-as`
Rules tab	Click **Add** and create a rule with these parameters:  ▪ Rule Name: `med-low-info` ▪ Action: Select **Alert** ▪ Severity: Select only the **Medium**, **Low**, and **Informational** check boxes Click **OK** to save the rule. Click **Add** and create another rule with these parameters:

Parameter	Value#
	▪ Rule Name: `crit-high` ▪ Action: Select **Alert** ▪ Severity: Select only the **Critical** and **High** check boxes Click **OK** to save the rule.

4. Click **OK** to close the Anti-Spyware Profile window.
5. Select **Policies > Security**. 

6. Select the **egress-outside-av** Security policy rule without opening it.
7. Click 

. The Clone configuration window opens.
8. Select **Move top** from the **Rule Order** drop-down list.
9. Click **OK** to close the Clone configuration window.
10. With the original egress-outside-av still selected, click 

.
11. Click to open the cloned Security policy rule named **egress-outside-av-1**.
12. Configure the following:

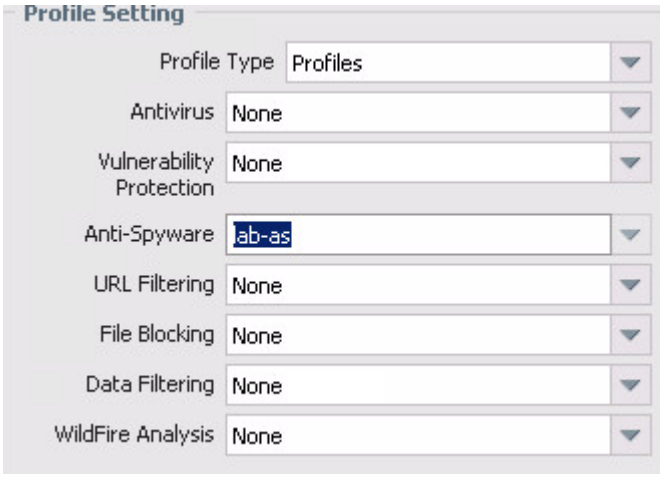
Parameter	Value#
Name	`egress-outside-as`
Tags	**egress**

13. Click the **Source** tab and configure the following:

Parameter	Value#
Source Zone	

14. Click the **Actions** tab and configure the following:

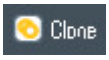
Parameter	Value#
Profile Type	**Profiles**

Parameter	Value#
Profile Setting	

15. Click **OK** to close the Security Policy Rule configuration window.

5.5 Create DMZ Security Policy

Because the management interface uses the inside interface as the gateway, you need to allow this traffic via a Security policy rule.

1. Select the **internal-dmz-ftp** Security policy rule without opening it.
2. Click  . The Clone configuration window opens.
3. Select **Move top** from the **Rule Order** drop-down list.
4. Click **OK** to close the Clone configuration window.
5. With the original internal-dmz-ftp still selected, click  .
6. Click to open the cloned Security policy rule named **internal-dmz-ftp-1**.
7. Configure the following:

Parameter	Value#
Name	`internal-inside-dmz`
Tags	**internal**

8. Click the **Destination** tab and configure the following:

Parameter	Value#
Destination Address	

9. Click the **Application** tab and configure the following:

Parameter	Value#

Applications	`web-browsing`
	`ssl`
	`ssh`
	`ftp`

10. Click **OK** to close the Security Policy Rule configuration window.
11. Select **Policies > NAT**. NAT
12. Select the **destination-dmz-ftp** NAT policy rule without opening it.
13. Click Disable.
14. Commit all changes.

5.6 Configure DNS-Sinkhole External Dynamic List

An External Dynamic List is an object that references an external list of IP addresses, URLs, or domain names that can be used in policy rules. You must create this list as a text file and save it to a web server that the firewall can access. By default, the firewall uses its management port to retrieve the list items.

1. Select **Objects > External Dynamic Lists**. External Dynamic Lists
2. Click Add to configure a new External Dynamic List.
3. Configure the following:

Parameter	Value#
Name	`lab-dns-sinkhole`
Type	**Domain List**
Source	`http://192.168.50.10/dns-sinkhole.txt` (This is hosted on the DMZ server.)
Repeat	**Five Minute**

Note: This list currently only contains reddit.com.

4. Click **OK** to close the External Dynamic Lists configuration window.

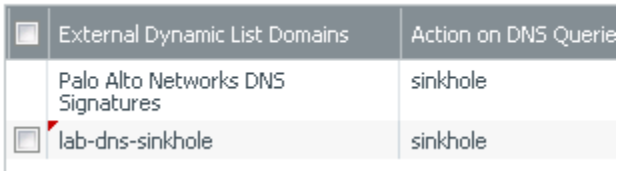
5.7 Anti-Spyware Profile with DNS Sinkhole

The DNS sinkhole action provides administrators with a method of identifying infected hosts on the network using DNS traffic, even when the firewall is north of a local DNS server (i.e., the firewall cannot see the originator of the DNS query).

1. Select **Objects > Security Profiles > Anti-Spyware**.

2. Click to open the Anti-Spyware Profile named **lab-as**.
3. Click the **DNS Signatures** tab.
4. Click 

and select **lab-dns-sinkhole**.
5. Set the **Action on DNS Queries** to **sinkhole**:



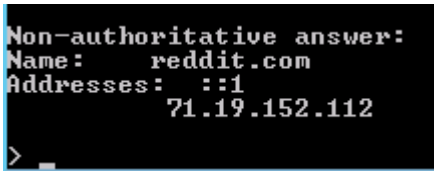
6. Verify that the **Sinkhole IPv4** is set to 71.19.152.112.
7. Click **OK** to close the Anti-Spyware Profile configuration window.
8. 

all changes.

5.8 Test Security Policy Rule

1. From the Windows desktop, open a command-prompt window.
2. Type the `nslookup` command and press the **Enter** key.
3. Type the command `server 8.8.8.8` and press the **Enter** key:

4. At the `nslookup` command prompt, type `reddit.com`. and press the **Enter** key:



Notice that the reply for reddit.com is 71.19.152.112. The request has been sinkholed.

5.9 Review Logs

1. Select **Monitor > Logs > Threat**. 

2. Identify the **Suspicious Domain** log entry. Notice that the action is **sinkhole**. Note that you will not see an entry for this activity in the Traffic log because the Windows system did not try to initiate a connection to 71.19.152.112:

5.10 Create Security Policy Rule with a Vulnerability Protection Profile

A Security policy rule can include specification of a Vulnerability Protection Profile that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

1. Select **Objects > Security Profiles > Vulnerability Protection**. 

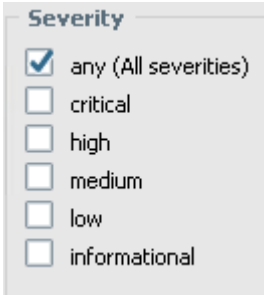
2. Click 

to create a Vulnerability Protection Profile.
3. Configure the following:

Parameter	Value#
Name	`lab-vp`

4. On the **Rules** tab, click 

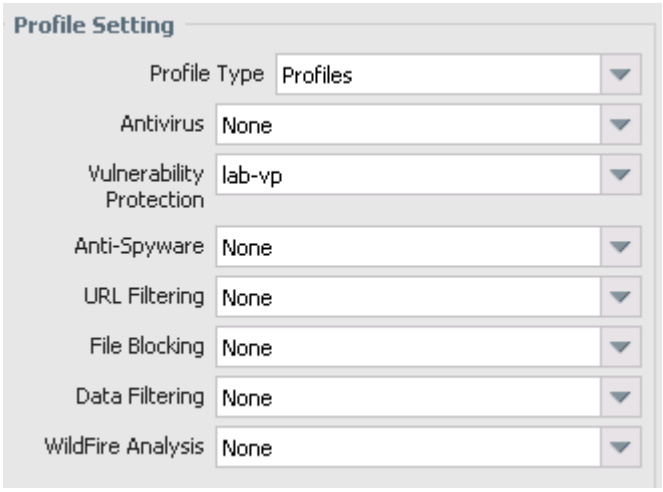
to create a rule.
5. Configure the following:

Parameter	Value#
Name	`lab-vp-rule`
Packet Capture	
Severity	

6. Click **OK** twice.
7. Select **Policies > Security**. 

8. Click to open the **internal-inside-dmz** Security policy rule.
9. Click the **Actions** tab and configure the following:

Parameter	Value#
Profile Type	**Profiles**

Parameter	Value#
Profile Setting	

10. Click **OK** to close the Security Policy Rule configuration window.
11. Commit all changes.

5.11 Test Security Policy Rule

1. On the Windows desktop, double-click the **lab** folder and then the **bat files** folder.
2. Double-click ftp-brute.bat.

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-03 13:25 Coordinated Universa
l Time
Nmap scan report for 192.168.50.10
Host is up (0.00s latency).
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 2050 guesses in 602 seconds, average tps: 3.4

Nmap done: 1 IP address (1 host up) scanned in 603.41 seconds
```

Note: This action launches an FTP brute force attack at the DMZ FTP server. The script is expected to take about *10 minutes* to complete.

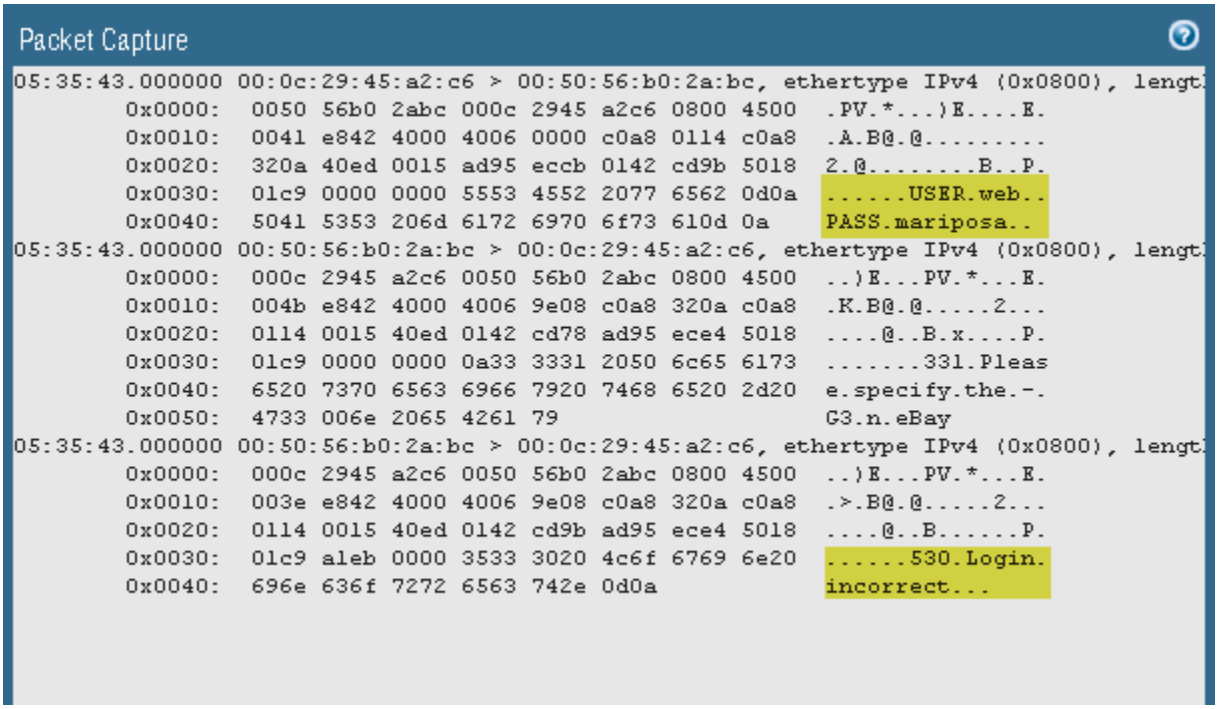
5.12 Review Logs

1. Select **Monitor > Logs > Threat**. Threat
2. Notice that you now have logs reflecting the FTP brute force attempt. However, the firewall is only set to alert:

		Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
		12/03 05:35:43	vulnerability	FTP: login Brute Force attempt	private	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high
		12/03 05:35:43	vulnerability	FTP: login Brute Force attempt	private	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high

3. Click the icon to the left of any log entry to open the packet capture.

4. Notice the username and password that was attempted along with the 530 response from the FTP server.



5.13 Update Vulnerability Profile

1. Select **Objects > Security Profiles > Vulnerability Protection**. Vulnerability Protection
2. Click to open the **lab-vp** Profile.
3. Click to open the **lab-vp-rule** rule and configure the following:

Parameter	Value#
Action	**Reset Both**
Severity	**high**

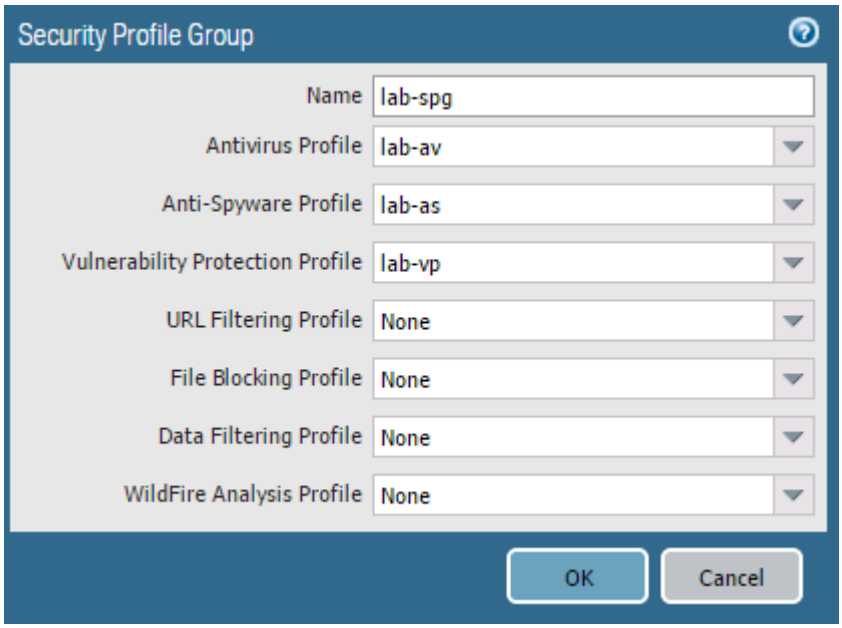
4. Click **OK** twice.
5. Commit all changes.
6. Rerun ftp-brute.bat and review the logs to confirm that the new FTP brute force attempts are reset.

5.14 Group Security Profiles

The firewall supports the ability to create Security Profile Groups, which specify sets of Security Profiles that can be treated as a unit and then added to Security policy rules.

1. Select **Objects > Security Profile Groups**. Security Profile Groups

2. Click  to open the Security Profile Group configuration window.
3. Configure the following:

Parameter	Value#
Name	`lab-spg`
Profiles	

4. Click **OK**.
5. Select **Policies > Security**. 
6.  the following rules:

Parameter	Value#
Security Policy Rules	**egress-outside-as** **egress-outside-av**

7. Click  to define a Security policy rule.
8. Configure the following:

Parameter	Value#
Name	`egress-outside-content-id`
Rule Type	**universal (default)**
Tags	**egress**

9. Click the **Source** tab and configure the following:

Parameter	Value#
Source Zone	**inside**
Source Address	**Any**

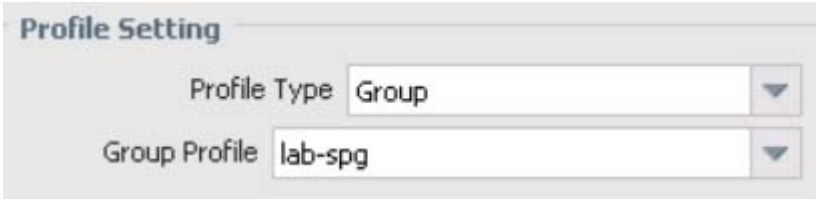
10. Click the **Destination** tab and configure the following:

Parameter	Value#
Destination Zone	**outside**
Destination Address	**Any**

11. Click the **Application** tab and verify that 

is checked.
12. Click the **Service/URL Category** tab and verify that 

is selected.
13. Click the **Actions** tab and configure the following:

Parameter	Value#
Action Setting	**Allow**
Log Setting	**Log at Session End**
Profile Setting	

14. Click **OK** to close the Security Policy Rule configuration window.

5.15 Create a File Blocking Profile

A Security policy rule can include specification of a File Blocking Profile that blocks selected file types from being uploaded or downloaded, or generates an alert when the specified file types are detected.

1. In the WebUI select **Objects > Security Profiles > File Blocking**. 

2. Click 

to open the File Blocking Profile configuration window.
3. Configure the following:

Parameter	Value#
Name	`lab-file-blocking`

4. Click 

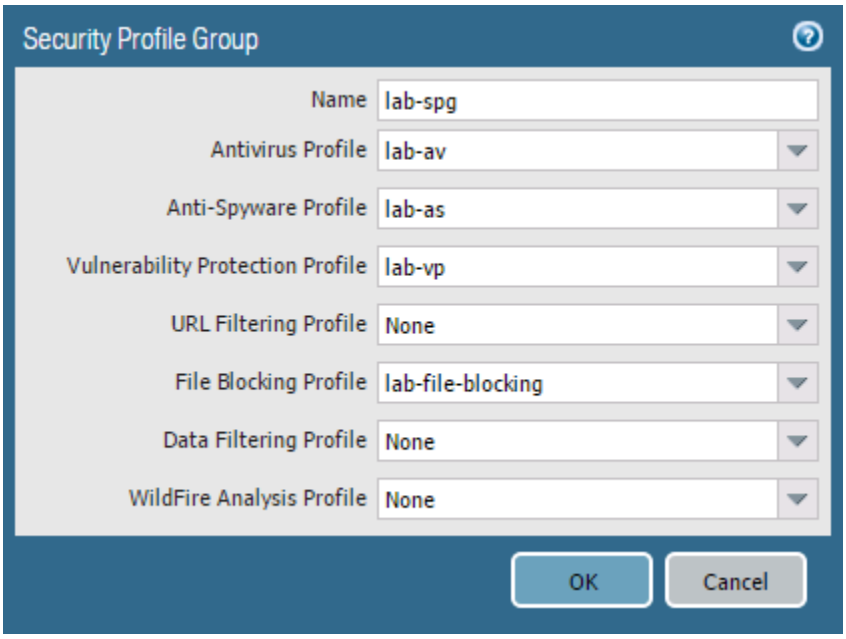
and configure the following.

Parameter	Value#
Name	`block-pdf`
Applications	**any**
File Types	`pdf`
Direction	**both**
Action	**block**

5. Click **OK** to close the File Blocking Profile configuration window.

5.16 Modify Security Profile Group

1. Select **Objects > Security Profile Groups**. Security Profile Groups
2. Click to open the **lab-spg** Security Profile Group.
3. Add the newly created File Blocking Profile:



4. Click **OK**.
5. Commit all changes.

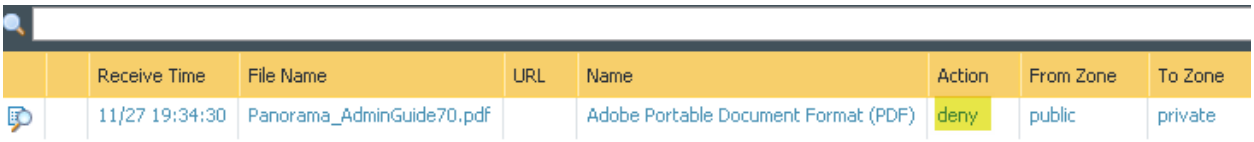
5.17 Test the File Blocking Profile

1. Open a new browser window in private/incognito mode and browse to `http://www.panedufiles.com/`.
2. Click the **Panorama_AdminGuide.pdf** link. The download fails.

Note: If you get "failed to download pdf" and not the block page, then refresh the browser window.

3. Select **Monitor > Logs > Data Filtering**. 

4. Find the log entry for the PDF file that has been blocked:



	Receive Time	File Name	URL	Name	Action	From Zone	To Zone
	11/27 19:34:30	Panorama_AdminGuide70.pdf		Adobe Portable Document Format (PDF)	deny	public	private

Note: The Action column is located on the far right. The column can be moved via drag-and-drop using the mouse cursor.

5.18 Multi-Level-Encoding

Multi-Level-Encoding can be used to block content that is not inspected by the firewall because of the file being encoded five or more times.

1. In the WebUI select **Objects > Security Profiles > File Blocking**. 

2. Click to open the **lab-file-blocking** File Blocking Profile.
3. Click 

and configure the following:

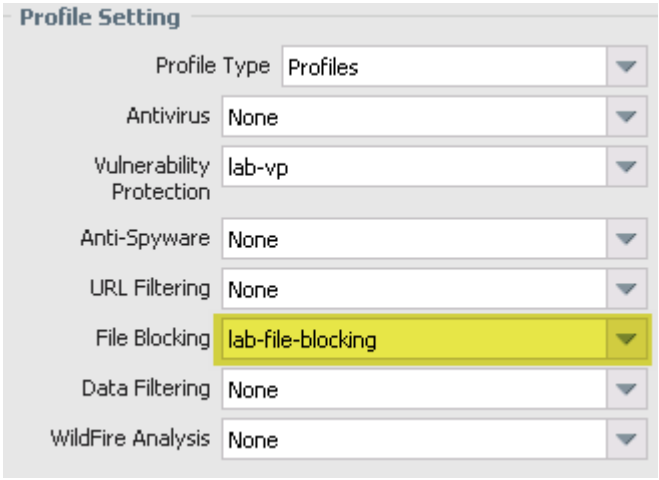
Parameter	Value#
Name	`block-mle`
Applications	**any**
File Types	`Multi-Level-Encoding`
Direction	**both**
Action	**block**

4. Click **OK** to close the File Blocking Profile configuration window.

5.19 Modify Security Policy Rule

1. In the WebUI select **Policies > Security**. 

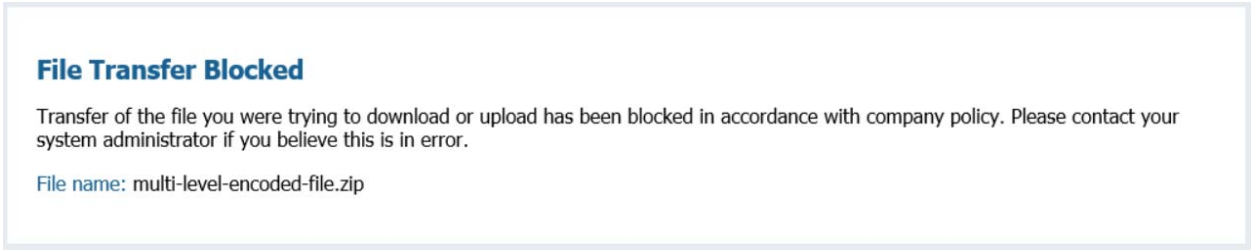
2. Click to open the **internal-inside-dmz** Security policy rule.
3. Click the **Actions** tab and configure the following:

Parameter	Value#
Profile Setting	

4. Click **OK** to close the Security Policy Rule configuration window.
5.  all changes.

5.20 Test the File Blocking Profile with Multi-Level-Encoding

1. Open a new browser in private/incognito mode and browse to `http://192.168.50.10/mle.zip`. The URL links to a file that is compressed five times.



2. The file is blocked in accordance with the new file blocking rule.

5.21 Modify Security Policy Rule

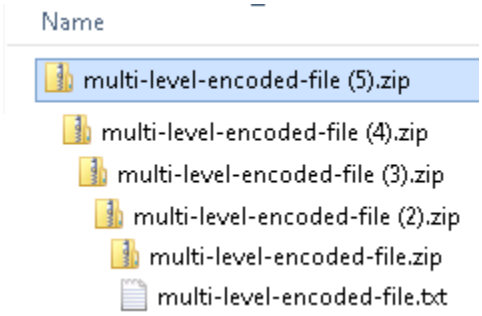
1. In the WebUI select **Objects > Security Profiles > File Blocking**. 

2. Click to open the **lab-file-blocking** File Blocking Profile.
3. Select the **block-mle** rule:

4. Click Delete.
5. Click **OK** to close the File Blocking Profile configuration window.
6. Commit all changes.

5.22 Test the File Blocking Profile with Multi-Level-Encoding

1. Open a new browser in private/incognito mode and browse to `http://192.168.50.10/mle.zip`. The URL links to a file that is compressed five times. The file is no longer blocked.
2. Save and open the file to exam the contents:



5.23 Create Danger Security Policy Rule

Create a Security policy rule that references the danger Security zone for threat and traffic generation.

1. Select **Policies > Security**. Security
2. Click Add and configure the following:

Parameter	Value#
Name	`danger-simulated-traffic`

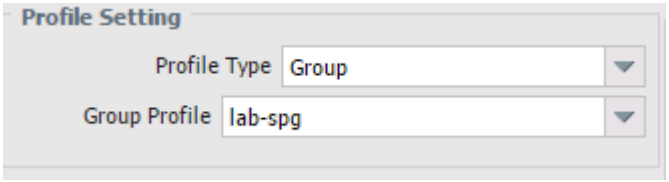
3. Click the **Source** tab and configure the following:

Parameter	Value#
Source Zone	danger

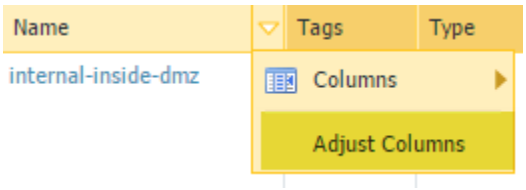
4. Click the **Destination** tab and configure the following:

Parameter	Value#
Destination Zone	danger

5. Click the **Actions** tab and configure the following:

Parameter	Value#
Profile Setting	

6. Click **OK** to close the Security Policy Rule configuration window.
7. Hover over the **Name** column header and select **Adjust Columns** from the drop-down list:



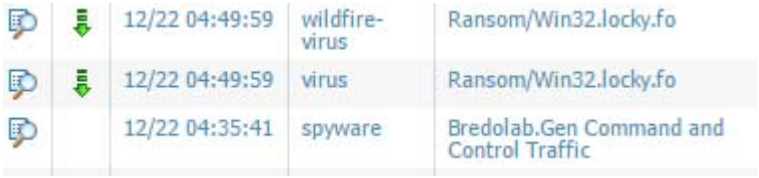
8. Commit all changes.

5.24 Generate Threats

1. On the Windows desktop, open **PuTTY** and double-click **traffic-generator**.
2. Enter the following information when prompted:

Parameter	Value#
Password	`Pal0Alt0`

3. In the PuTTY window, type the command `sh /tg/malware.sh`.
4. Select **Monitor > Logs > Threat**. Threat
5. Type the following filter `(severity neq informational)`.
6. Notice the threats currently listed from the generated traffic:

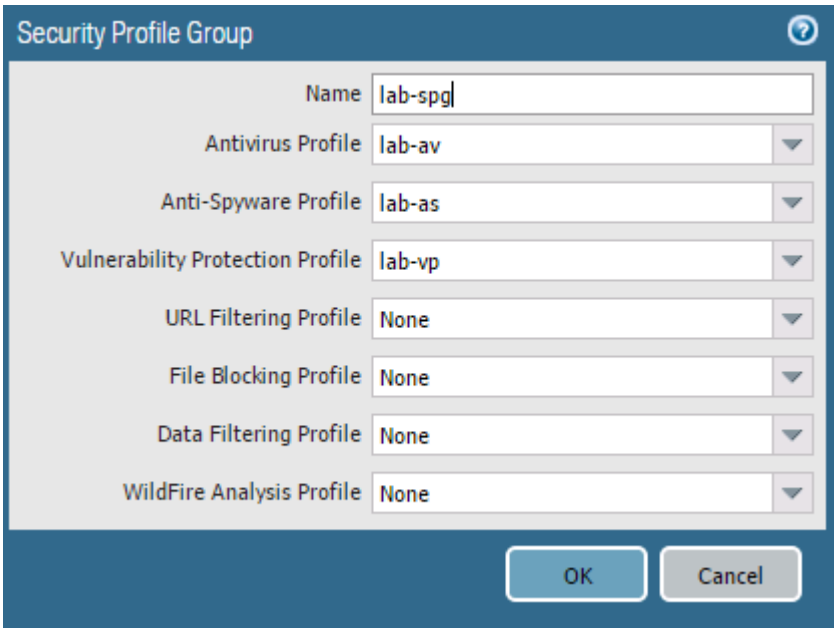


7. Select **Monitor > Logs > Data Filtering**. Data Filtering
8. Notice the blocked files:

		12/22 04:50:04	locky.exe	Windows Executable (EXE)
		12/22 04:50:04	locky.exe	Microsoft PE File
		12/22 04:47:48	YhXTUeGQ.jar	ZIP
		12/22 04:47:38	e8TFVhMb.xap	ZIP
		12/22 04:40:13	YhXTUeGQ.jar	ZIP
		12/22 04:40:03	e8TFVhMb.xap	ZIP
		12/22 04:31:30	e8TFVhMb.xap	ZIP

5.25 Modify Security Profile Group

1. Select **Objects > Security Profile Groups**. Security Profile Groups
2. Click to open the **lab-spg** Security Profile Group.
3. Remove the File Blocking Profile:



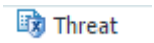
4. Click **OK**.
5. Commit all changes.

5.26 Generate Threats

1. On the Windows desktop, open **PuTTY** and double-click **traffic-generator**.
2. Enter the following information when prompted:

Parameter	Value#
Password	`Pal0Alt0`

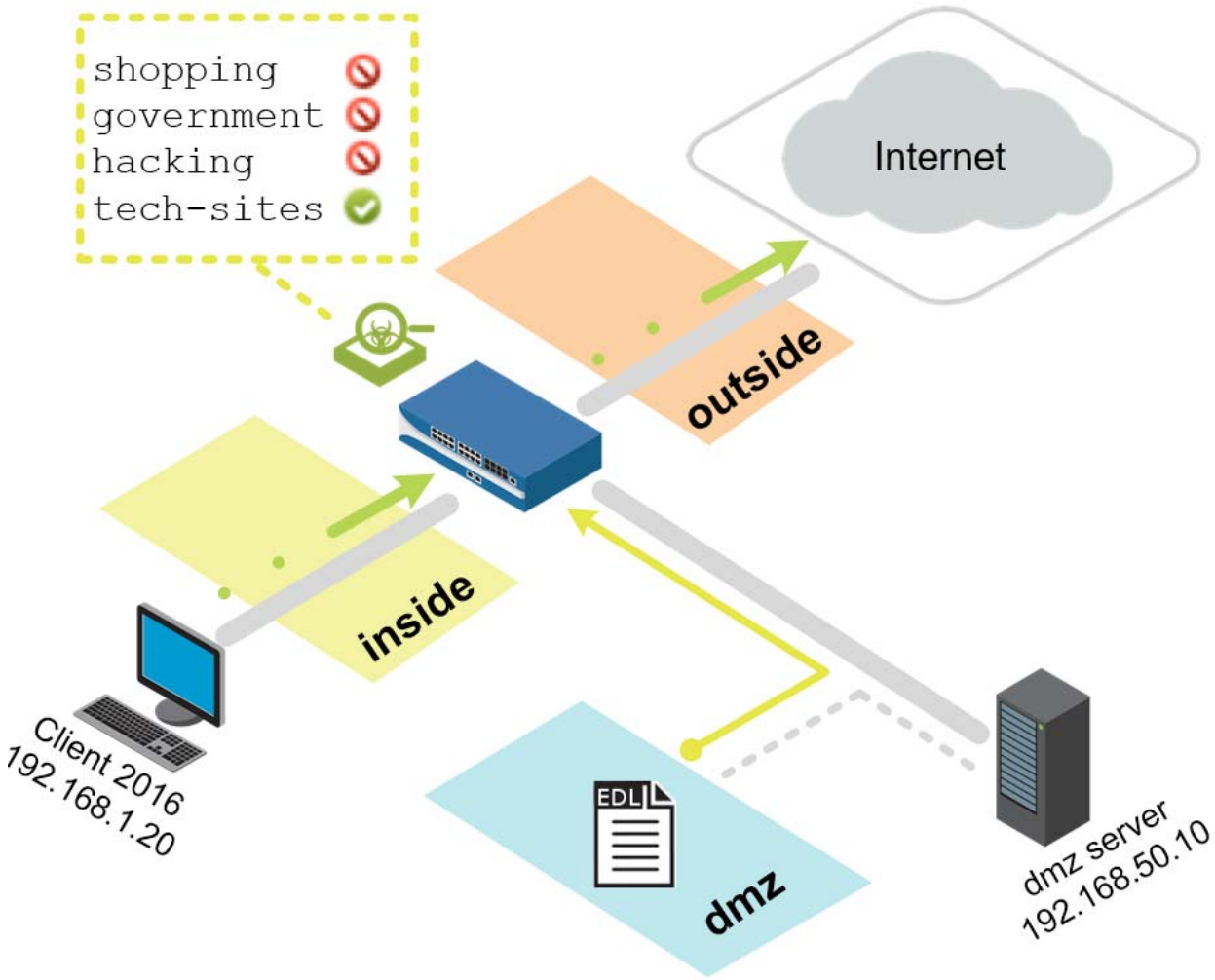
3. In the PuTTY window, type the command `sh /tg/malware.sh`.

4. Select **Monitor > Logs > Threat**. 

5. Input the following filter `(severity neq informational)`.
6. Notice that the blocked files are now being detected as a virus:

Stop. This is the end of the Content-ID lab.

6. Lab: URL Filtering

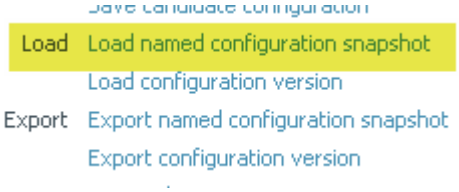


Lab Objectives

- Create a custom URL category and use it as a Security policy rule match criterion and as part of a URL Filtering Profile.
- Configure and use an External Dynamic List as a URL block list.
- Create a URL Filtering Profile and observe the difference between using url-categories in a Security policy versus a profile.
- Review firewall log entries to identify all actions and changes.

6.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-06** and click **OK**.
4. Click **Close**.
5. Commit all changes.

6.1 Create a Security Policy Rule with a Custom URL Category

Use a custom URL Category object to create your custom list of URLs and use it in a URL Filtering Profile or as match criteria in Security policy rules. In a custom URL Category, you can add URL entries individually, or import a text file that contains a list of URLs.

1. Select **Objects > Custom Objects > URL Category**. URL Category
2. Click Add to create a custom URL Category.
3. Configure the following:

Parameter	Value#
Name	`tech-sites`

Sites	`newegg.com`
	`engadget.com`
	`techradar.com`
	`*.newegg.com`
	`*.engadget.com`
	`*.techradar.com`

4. Click **OK** to close the Custom URL Category configuration window.
5. Select **Policies > Security**. Security
6. Select the **egress-outside-content-id** Security policy rule without opening it:

7. Click Clone. The Clone configuration window opens.
8. Select **Move top** from the Rule Order drop-down list.
9. Click **OK** to close the Clone configuration window.
10. With the original egress-outside-content-id Security policy rule still selected, click Disable.
11. Notice that the egress-outside-content-id is now grayed out and in italic font:

12. Click to open the cloned Security policy rule named **egress-outside-content-id-1**.
13. Configure the following:

Parameter	Value#
Name	`egress-outside-url`

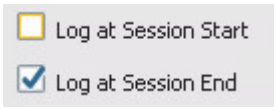
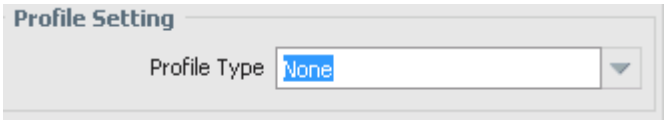
14. Click the **Application** tab and configure the following:

Parameter	Value#
Applications	

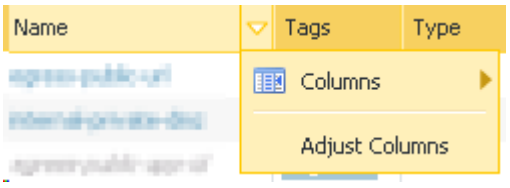
15. Click the **Service/URL Category** tab and configure the following:

Parameter	Value#
URL Category	

16. Click the **Actions** tab and configure the following:

Parameter	Value#
Action Setting	**Reset both client and server**
Log Setting	
Profile Setting	

17. Click **OK** to close the Security Policy Rule configuration window.
18. Hover over the **Name** column and click the **down-arrow**:



19. Expand the **Columns** menu using the right-arrow and select the **URL Category** check box. The URL Category column is displayed.
20. Enable the rule **egress-outside**. 

21.  all changes.

Note: Because you created a rule that resets traffic, you need to enable the egress-outside rule to allow everything else.

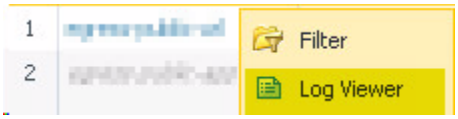
6.2 Test Security Policy Rule

1. Open a browser in private/incognito mode and browse to `newegg.com`:

   The URL is blocked by the Security policy rule named egress-outside-url.
2. In the same browser window verify that techradar.com is blocked.
3. In the same browser window, check if https://www.engadget.com also is blocked. Note that this was an SSL connection. Because the firewall is not decrypting traffic, the connection is reset without a URL block page. If the firewall intercepted this connection and displayed the URL block page, the browser would assume a man-in-the-middle attack might be in progress.

6.3 Review Logs

1. Hover over the **egress-outside-url** Security policy rule, click the down-arrow, and select **Log Viewer** to open the Traffic log:



2. Notice that the firewall adds `( rule eq 'egress-outside-url' )` to the Traffic log filter text box:

3. The **URL Category** column can be added to the Traffic log to provide additional information.
4. Select the **URL Filtering** log. 

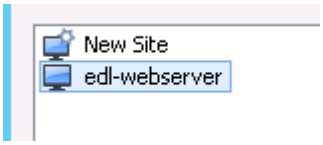
5. Notice that URL Filtering log includes the **Category** and **URL** columns by default:

Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
tech-sites	www.engadget....			192.168.1.20		54.148.25.129	ssl	block-url
tech-sites	www.engadget....			192.168.1.20		54.148.25.129	ssl	block-url
tech-sites	www.engadget....			192.168.1.20		54.148.25.129	ssl	block-url
tech-sites	www.techradar....			192.168.1.20		89.167.143.23	web-browsing	block-url
tech-sites	www.techradar....			192.168.1.20		89.167.143.23	web-browsing	block-url

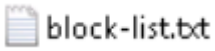
6.4 Configure an External Dynamic List

An External Dynamic List is an object that references an external list of IP addresses, URLs, or domain names that can be used in policy rules.

1. Open WinSCP on the Windows desktop.
2. Double-click the list item **edl-webserver**.

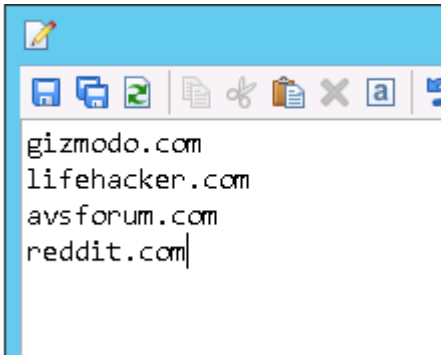


3. Locate the text file in the right window pane named **block-list.txt**.



4. Right-click the **block-list.txt** file and select **Edit**.
5. Verify that the following URLs exist, each followed by a line break:

```
gizmodo.com
lifehacker.com
avsforum.com
reddit.com
```



6. **Save**  and **Close**  the file.
7. Close the WinSCP window.
8. In the WebUI select **Objects > External Dynamic Lists**. 

9. Click  to configure a new External Dynamic List.

10. Configure the following:

Parameter	Value#
Name	`url-block-list`

Parameter	Value#
Type	**URL List**
Source	`http://192.168.50.10/block-list.txt`
Repeat	**Five Minute**

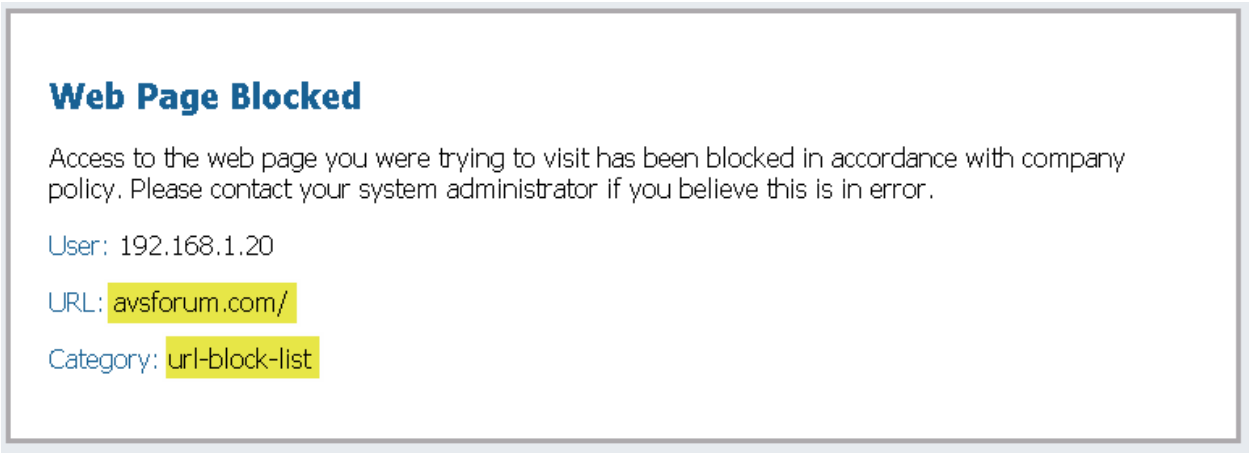
11. Click **OK** to close the External Dynamic Lists configuration window.
12. Go to **Policies > Security**. 

13. Click to open the Security policy rule named **egress-outside-url**.
14. Click the **Service/URL Category** tab.
15. Add the newly created External Dynamic List to the **URL Category** list:


16. Click **OK** to close the Security Policy Rule configuration window.
17. 

all changes.

6.5 Test Security Policy Rule

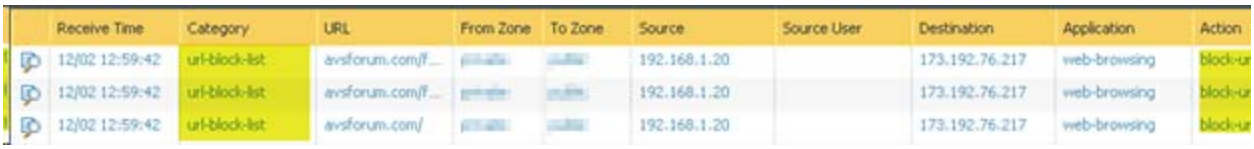
1. Open a browser in private/incognito mode and browse to `avsforum.com`:


The URL is blocked by the Security policy rule named egress-outside-url.
2. In the same browser window verify that gizmodo.com and lifehacker.com also are blocked.

6.6 Review Logs

1. In the WebUI select **Monitor > Logs > URL Filtering**. 

2. Notice the new category and action:



6.7 Create a Security Policy Rule with URL Filtering Profile

1. Select **Objects > Security Profiles > URL Filtering**. 

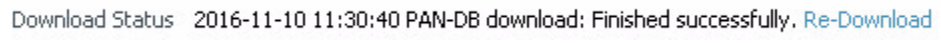
2. Click 

to define a URL Filtering Profile.
3. Configure the following:

Parameter	Value#
Name	`lab-url-filtering`

4. Click the **Categories** tab.
5. Search the Category field for the following three categories and set the **Site Access** to **block**:

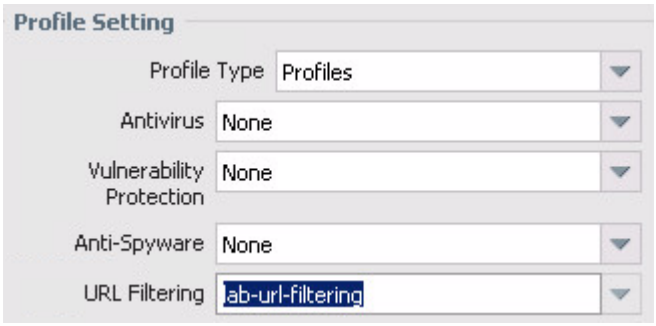

`shopping`
`government`
`hacking`
6. Search for url-block-list and tech-sites. Notice that your custom URL categories are also listed and they are set to a Site Access of "allow." Leave them set to "allow."
7. Click **OK** to close the URL Filtering Profile window.
8. Select **Device > Licenses**. 

9. Under the PAN-DB URL Filtering header, click **Download Now** (or **Re-Download**). A warning might appear; click **Yes**.
10. Select the region nearest the location of your firewall and click **OK**.
After the download completes, a Download Successful window appears.
11. Click **Close** to close the download status window. The WebUI should now show a message similar to the following:


12. Select **Policies > Security**. 

13. Click to open the Security policy rule named **egress-outside-url**.
14. Click the **Service/URL Category** tab.
15. Select 

above the **URL Category** list.
16. Click the **Actions** tab and configure the following:

Parameter	Value#
Action	**Allow**
Profile Setting	

17. Click **OK** to close the Security Policy Rule configuration window.
18. Disable the egress-outside rule. 
    Note: You can disable the egress-outside rule because the URL Filtering Profile is being used and the egress-outside-url Security policy rule now allows traffic.
19. Commit all changes.

6.8 Test Security Policy Rule with URL Filtering Profile

1. Open a different browser (not a new tab) in private/incognito mode and browse to `www.newegg.com`. The URL www.newegg.com belongs to the shopping URL category. Based on the Security policy rule named egress-outside-url, the URL is now allowed even though you chose to block the shopping category because your custom URL category has newegg.com listed and is set to "allow," and your custom category is evaluated before the Palo Alto Networks URL categories.
2. In the same browser window verify that `http://www.transportation.gov` (government), `http://www.amazon.com` (Shopping), and `http://www.2600.org` (hacking) are blocked.
3. Close all browser windows except for the firewall WebUI.

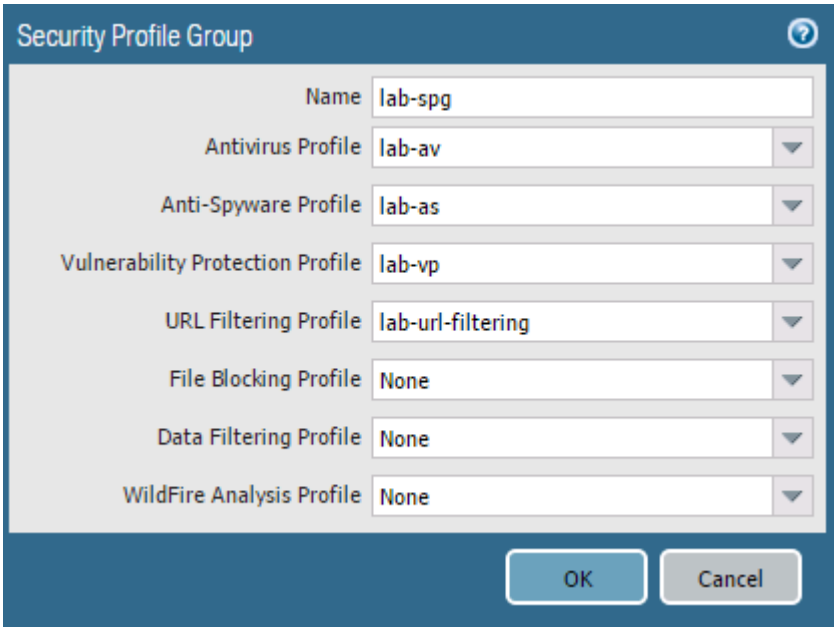
6.9 Review Logs

1. Select **Monitor > Logs > URL Filtering**. 
2. Review the actions taken on the following entries:

6.10 Modify Security Profile Group

1. In the WebUI select **Objects > Security Profile Groups**. 

2. Click to open the **lab-spg** Security Profile Group.
3. Add the newly created URL Filtering Profile:



4. Click **OK**.
5. Select **Policies > Security**. 

6. Select the **egress-outside-content-id** Security policy rule without opening it.
7. Click 

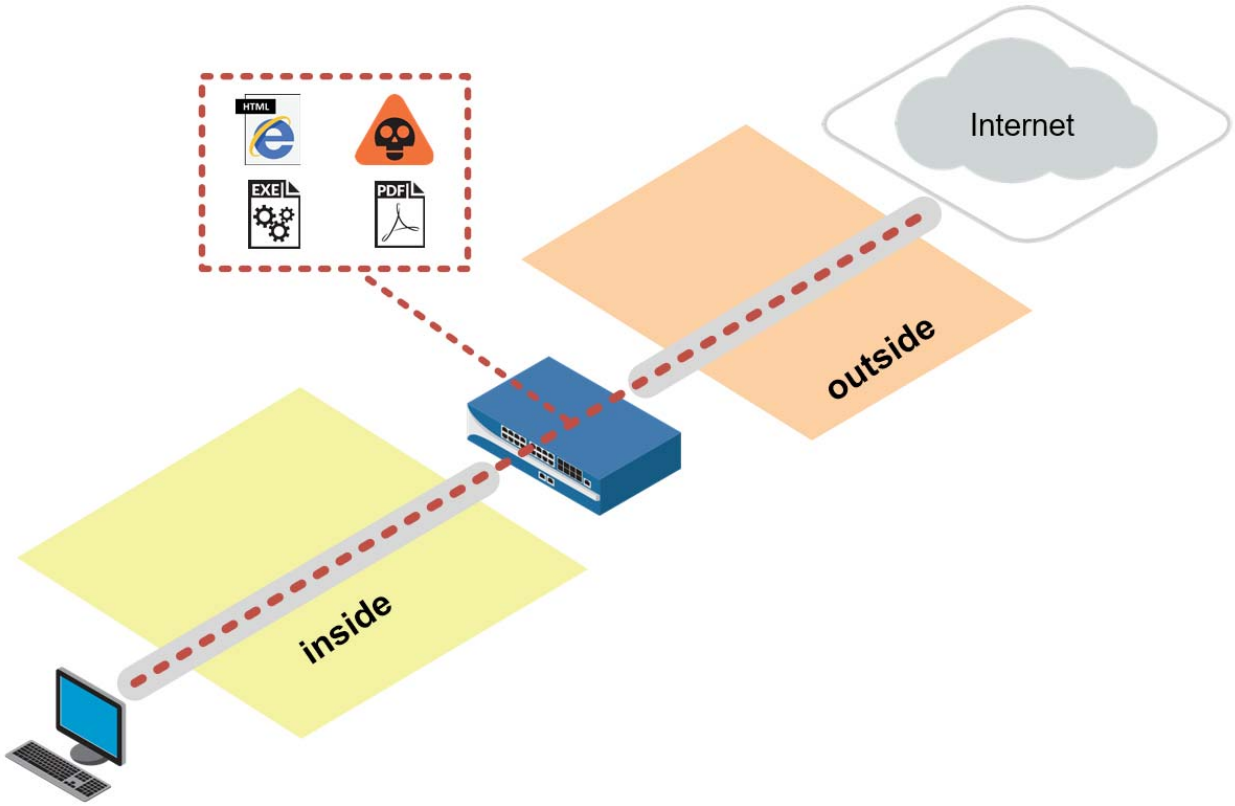
.
8. Select the **egress-outside-url** Security policy rule without opening it.
9. Click 

.
10. 

all changes.

Stop. This is the end of the URL Filtering lab.

7. Lab: Decryption

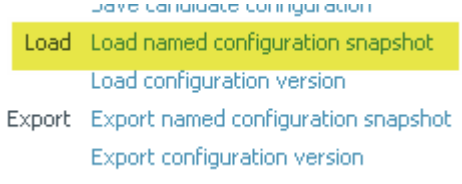


Lab Objectives

- Observe firewall behavior without decryption.
- Create Forward Trust and Untrust certificates.
- Create a custom decryption category.
- Create a Decryption policy.
- Observe firewall behavior after decryption is enabled.
- Review logs.

7.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



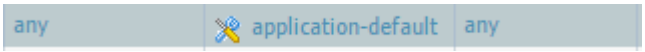
3. Select **edu-210-lab-07** and click **OK**.
4. Click **Close**.

5. Commit all changes.

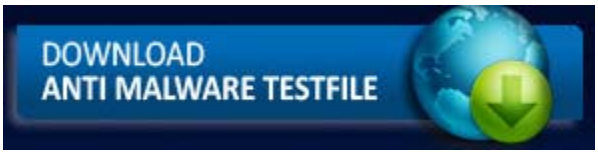
7.1 Test Firewall Behavior Without Decryption

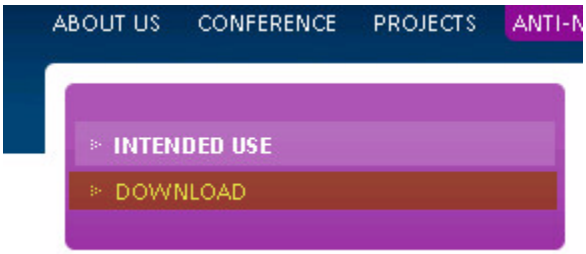
For this lab, you will use the Internet Explorer browser. Chrome has its own virus detection system and Firefox has its own certificate repository.

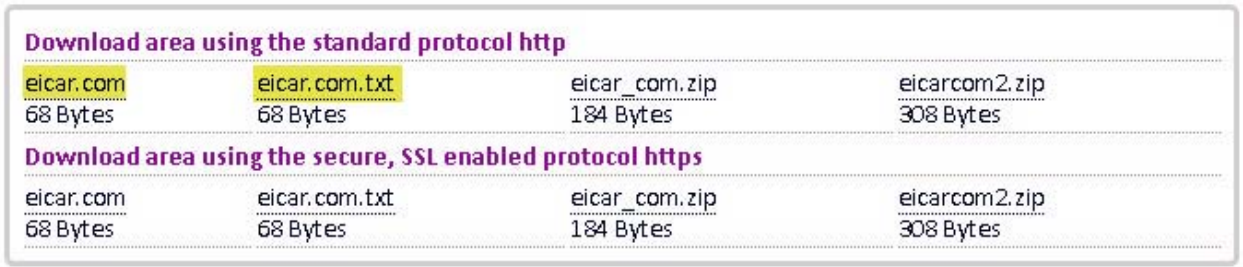
1. Select **Policies > Security**. 

2. Click **application-default** in the Service column in the egress-outside-content-id Security policy rule. 

3. In the Service window, change application-default to 

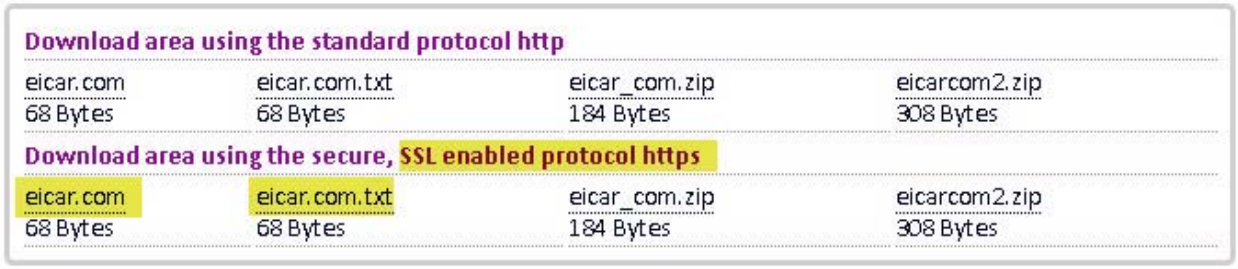
.
4. Click **OK** in the Service configuration window.
5. Commit all changes.
6. On the Windows desktop, open a browser in private/incognito mode and browse to `http://www.eicar.org`.
7. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner:


8. Click the **Download** link on the left of the web page:


9. Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using the standard HTTP protocol and *not* the SSL-encrypted HTTPS protocol. The firewall will not be able to detect the viruses in an HTTPS connection until decryption is configured.


10. If prompted, **Save** the file. Do *not* open or run the file.

11. Go back in the browser and download one of the test files using HTTPS:

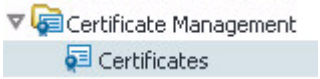


12. Notice that the download is not blocked because the connection is encrypted and the virus is hidden.
13. Close all browser windows except for the firewall WebUI.

7.2 Create Two Self-Signed Certificates

Certificates need to be generated so that the firewall can decrypt traffic.

1. In the WebUI select **Device > Certificate Management > Certificates**:



2. Click 

at the bottom of the page to create a new CA certificate.
3. Configure the following:

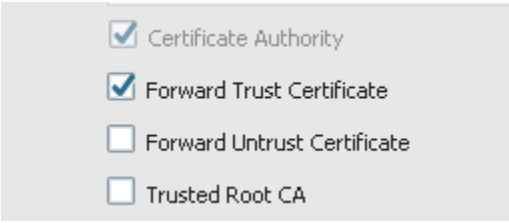
Parameter	Value#
Certificate Name	`trusted-ca#`
Common Name	`192.168.1.1#`
Certificate Authority	 #

4. Click **Generate** to create the certificate.
5. Click **OK** to close the Generate Certificate success window.
6. Click 

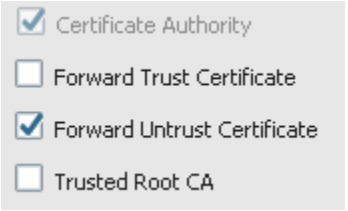
at the bottom of the page to create another CA certificate.
7. Configure the following:

Parameter	Value#
Certificate Name	`untrusted-ca#`
Common Name	`untrusted#`
Certificate Authority	 #

8. Click **Generate** to create the certificate.
9. Click **OK** to dismiss the Generate Certificate success window.
10. Click **trusted-ca** in the list of certificates to edit the certificate information.
11. Select the **Forward Trust Certificate** check box and click **OK**:



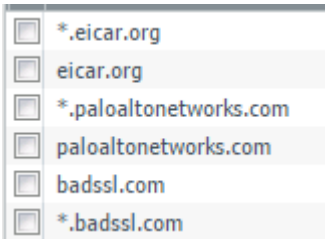
12. Click **untrusted-ca** in the list of certificates to edit the certificate information.
13. Select the **Forward Untrust Certificate** check box and click **OK**:



7.3 Create Custom Decryption URL Category

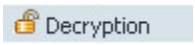
Create a custom URL Category to ensure we are only decrypting intended traffic.

1. In the WebUI select **Objects > Custom Objects > URL Category**. 
2. Click  to open the Custom URL Category configuration window.
3. Configure the following:

Parameter	Value#
Name	`lab-decryption`
Sites	

4. Click **OK** to close the Custom URL Category configuration window.

7.4 Create Decryption Policy

1. In the WebUI select **Policies > Decryption**. 

2. Click 

to create a Decryption policy rule.
3. Configure the following:

Parameter	Value#
Name	`decrypt-url-cat`

4. Click the **Source** tab and configure the following:

Parameter	Value#
Source Zone	**inside**

5. Click the **Destination** tab and configure the following:

Parameter	Value#
Destination Zone	**outside**

6. Click the **Service/URL Category** tab and configure the following:

Parameter	Value#
URL Category	

7. Click the **Options** tab and configure the following:

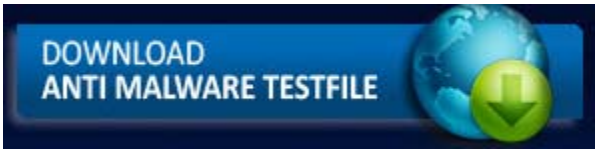
Parameter	Value#
Action	
Type	

8. Click **OK** to close the Decryption Policy Rule window.
9. 

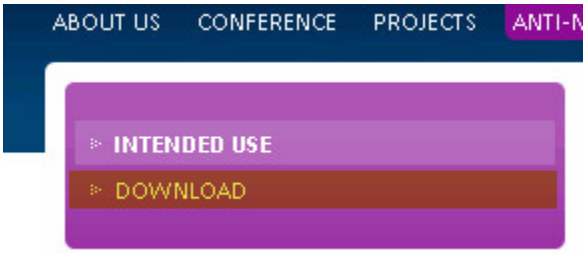
all changes.

7.5 Test AV Security Profile with the Decryption Policy

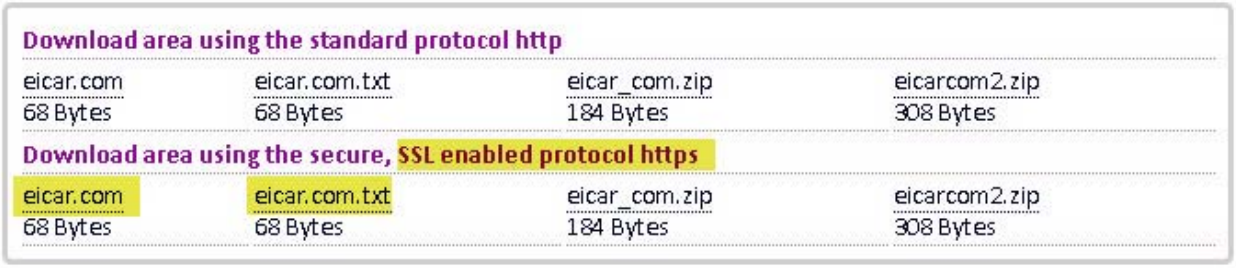
1. On the Windows desktop, open a browser in private/incognito mode and browse to `http://www.eicar.org`.
2. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner:



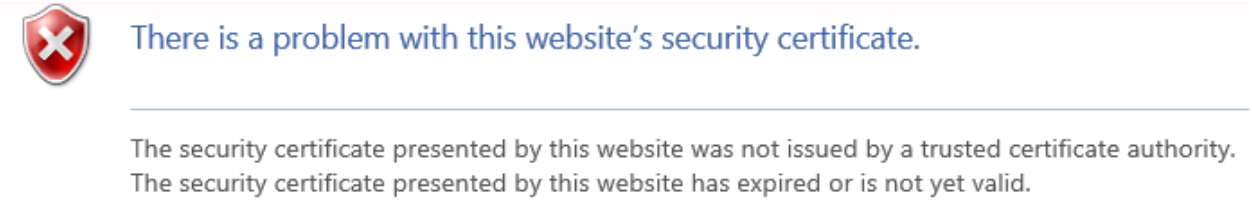
3. Click the **Download** link on the left of the web page:



4. Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using HTTPS:



A certificate issue is presented:

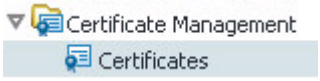


Note: The endpoint (Windows desktop) does not trust the certificate generated by the firewall.

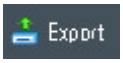
5. Close all browser windows except for the firewall WebUI.

7.6 Export the Firewall Certificate

1. In the WebUI select **Device > Certificate Management > Certificates**.



2. Select but do not open **trusted-ca**. 

3. Click 

to open the Export Certificate configuration window.
4. Click **OK** to export the trust-ca certificate.

7.7 Import the Firewall Certificate

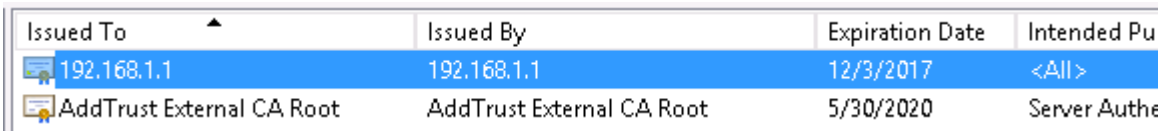
1. On your desktop, double-click the  certificates icon.
2. Under Certificates (Local Computer), expand **Trusted Root Certification Authorities** and select the **Certificates** folder:

3. Select **Action > All Tasks > Import**. 

4. The Certificate Import Wizard opens. Click **Next**.
5. **Browse** for the exported trusted-ca certificate:

6. Click **Next**.
7. Verify that the following is configured:

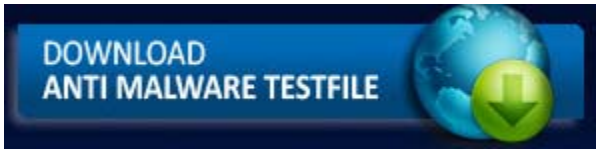
8. Click **Next**, click **Finish**, and then click **OK** in the status window.
9. Notice that the trusted-ca certificate is now imported:



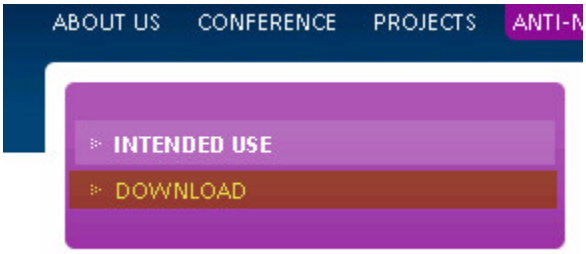
10. Close the Microsoft Management Console. Click **No** when asked to save console settings.

7.8 Test the Decryption Policy

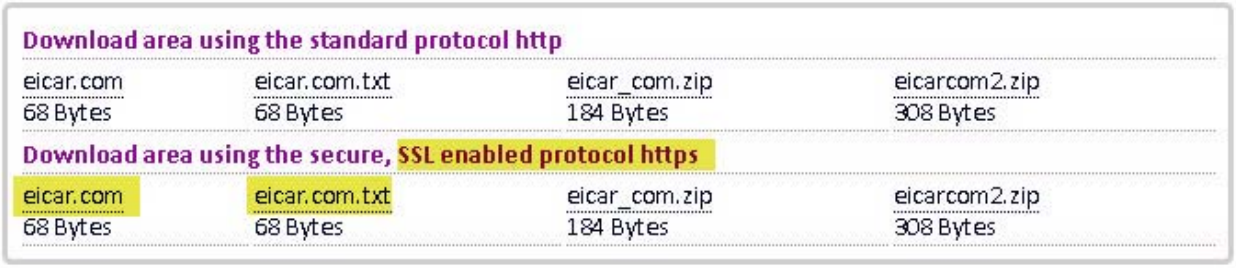
1. On the Windows desktop, open a browser (not Firefox) in private/incognito mode and browse to `http://www.eicar.org`.
2. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner.



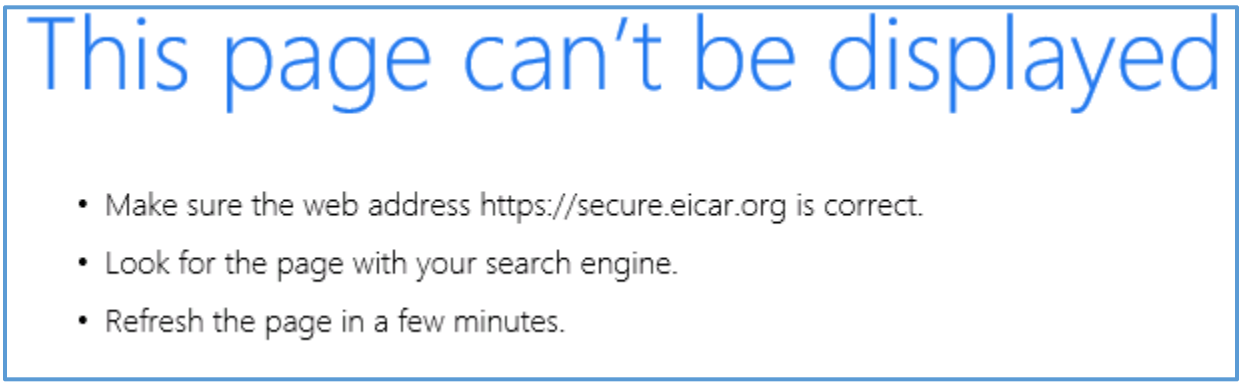
3. Click the **Download** link on the left of the web page.



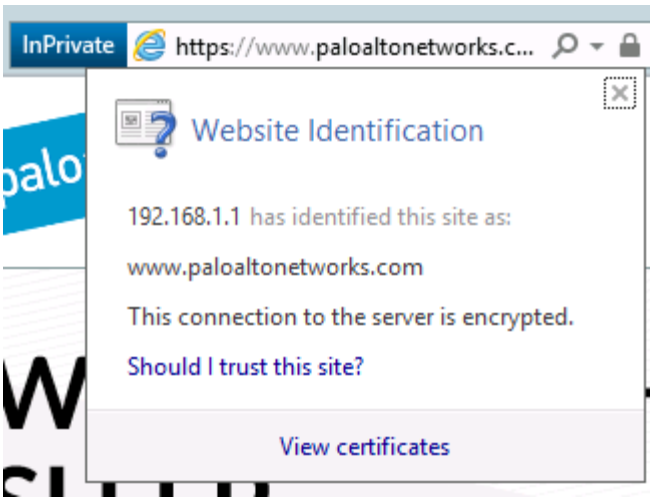
4. Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using HTTPS:



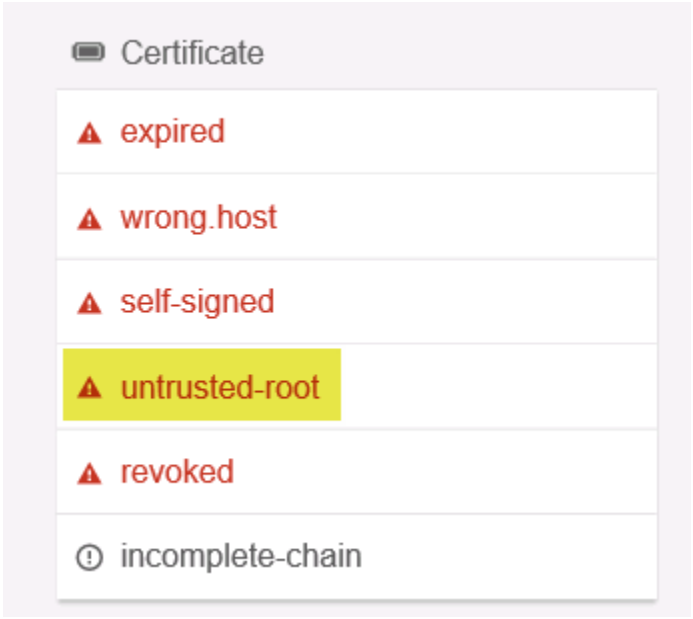
The Eicar Test File is detected and the connection gets reset.



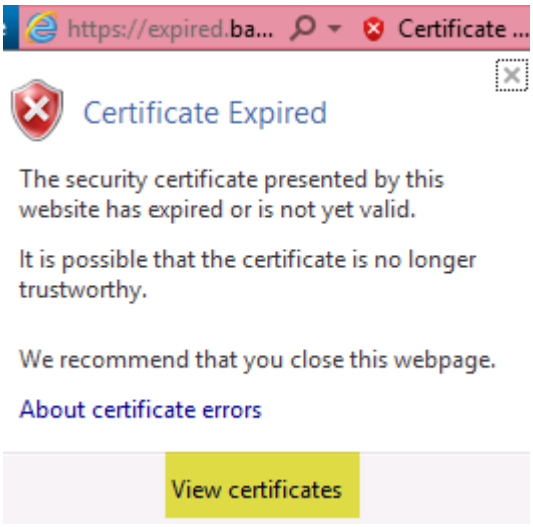
5. In the same browser, browse to `https://www.paloaltonetworks.com`. There is no certificate warning and the page is displayed correctly.
6. Click the **lock** icon next to the URL in the browser (Internet Explorer).
7. Notice that the signer is the firewall 192.168.1.1:



8. Close all browser windows except for the firewall WebUI.
9. Open a new browser and browse to `https://www.badssl.com`.
10. Click **untrusted-root**:



11. Notice that a certificate warning is now displayed. Choose to continue to the website.
12. Click the  icon near the URL and then click **View Certificates**:

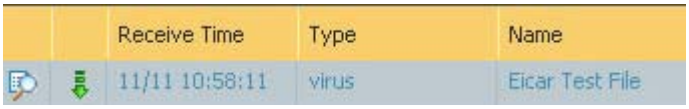


Notice that the certificate is still signed by the firewall. However, it was signed with the untrusted certificate.

7.9 Review Logs

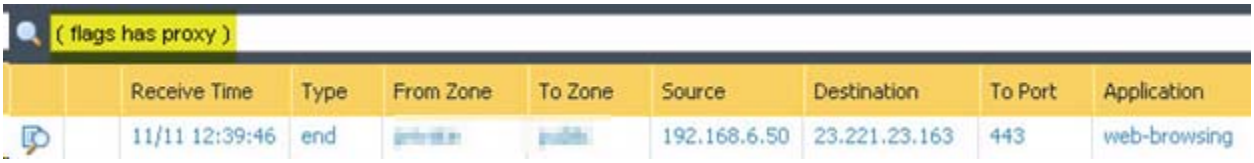
1. Select **Monitor > Logs > Threat**. 

Notice that there is an entry for when the connection was reset in the browser:



2. Select **Monitor > Logs > Traffic**. 

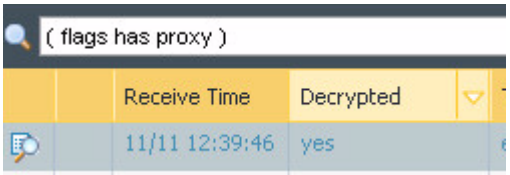
3. Type `( flags has proxy )` in the filter text box. This filter flags only traffic entries that were decrypted.



4. Hover over **Receive Time** and click the **down-arrow**.
5. Add the 

column.

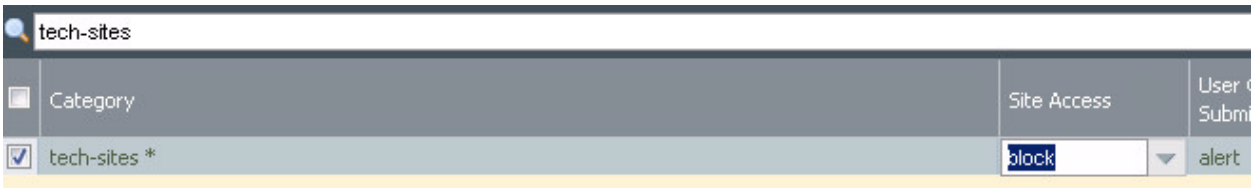
Notice the newly added column:



7.10 Test URL Filtering with Decryption

1. In the WebUI select **Objects > Security Profiles > URL Filtering**. 

2. Click to open the **lab-url-filtering** object.
3. Click the **Categories** tab and type a search for `tech-sites`.
4. Change **Site Access** to **block**:



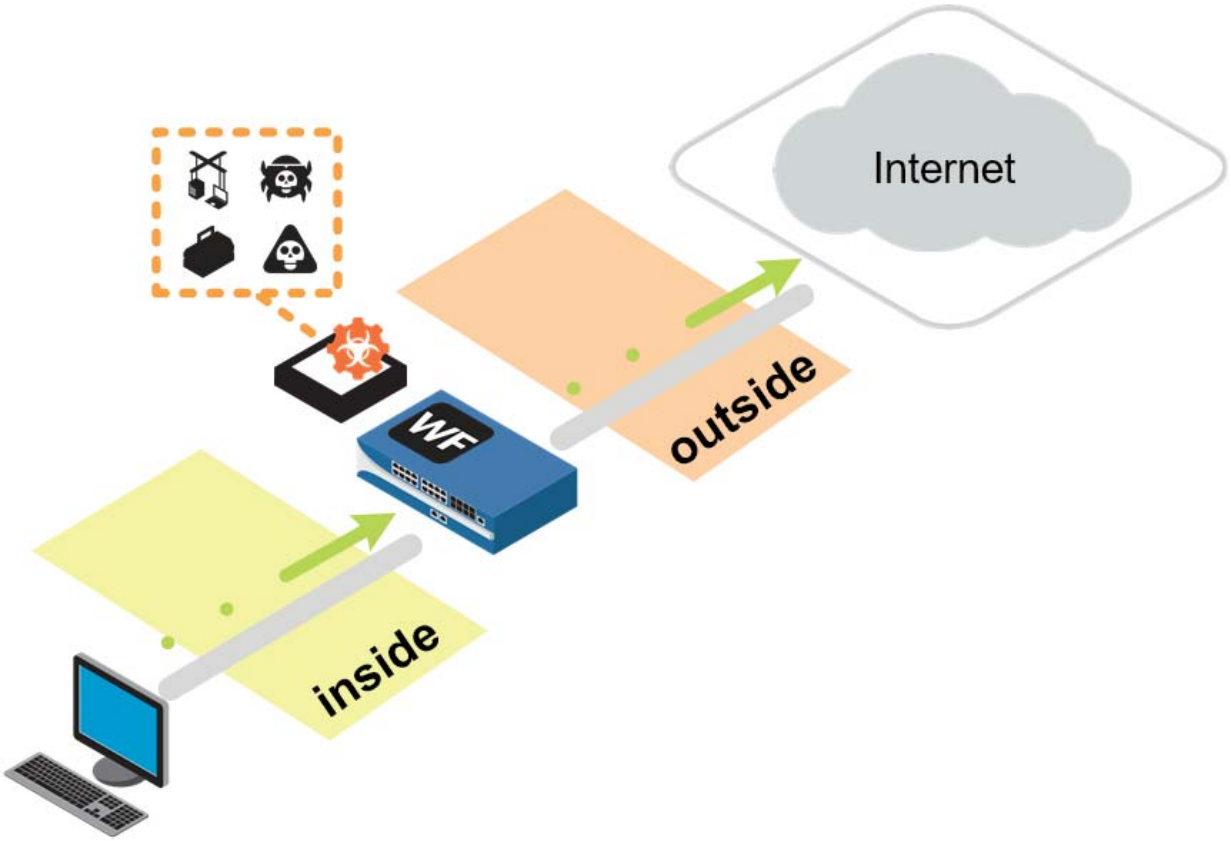
5. Click **OK**.
6. 

all changes.
7. Open Internet Explorer in private mode and browse to `https://engadget.com`.

   Engadget is now blocked.

Stop. This is the end of the Decryption lab.

8. Lab: WildFire

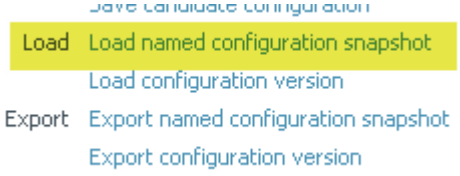


Lab Objectives

- Configure and test WildFire Analysis Security Profile.

8.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-08** and click **OK**.
4. Click **Close**.
5. Commit all changes.

8.1 Create a WildFire Analysis Profile

1. In the WebUI select **Objects > Security Profiles > WildFire Analysis**. 

2. Click 

to open the WildFire Analysis Profile configuration window.
3. Configure the following:

Parameter	Value#
Name	`lab-wildfire`

4. Click 

and configure the following:

Parameter	Value#
Name	`pe`
Applications	**any**
File Types	**pe**
Direction	**both**
Analysis	**public-cloud**

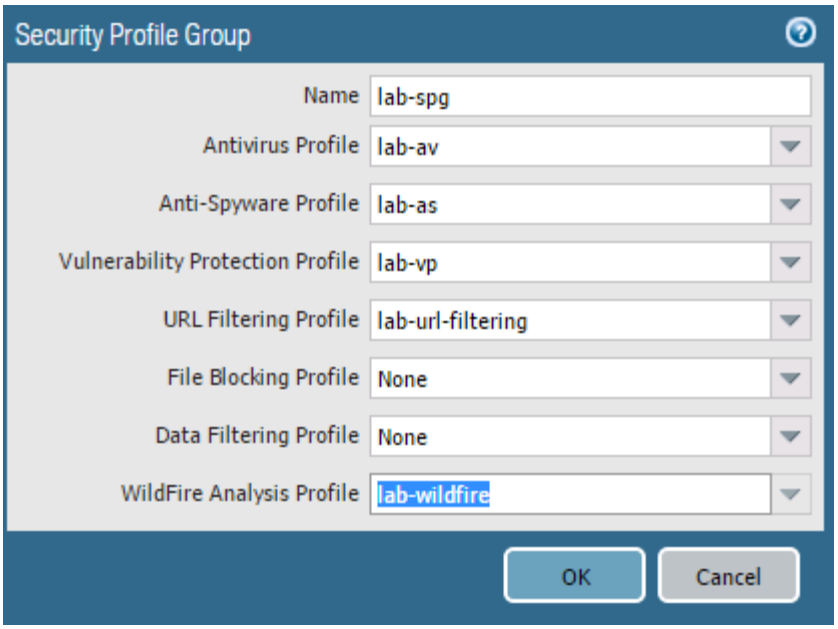
Note: The file type pe includes both .exe and .dll file types.

5. Click **OK** to close the WildFire Analysis Profile configuration window.

8.2 Modify Security Profile Group

1. In the WebUI select **Objects > Security Profile Groups**. 

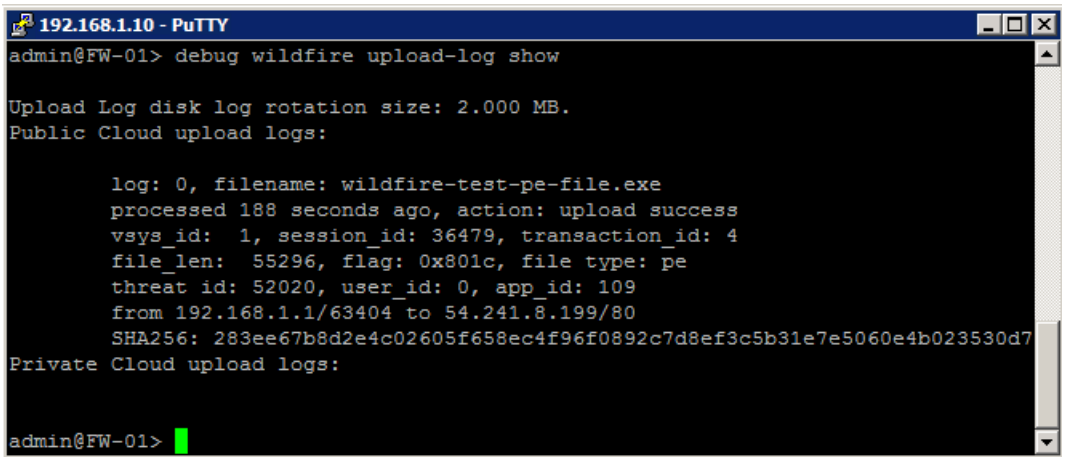
2. Click to open the **lab-spg** Security Profile Group.
3. Add the newly created **lab-wildfire** WildFire Analysis Profile:



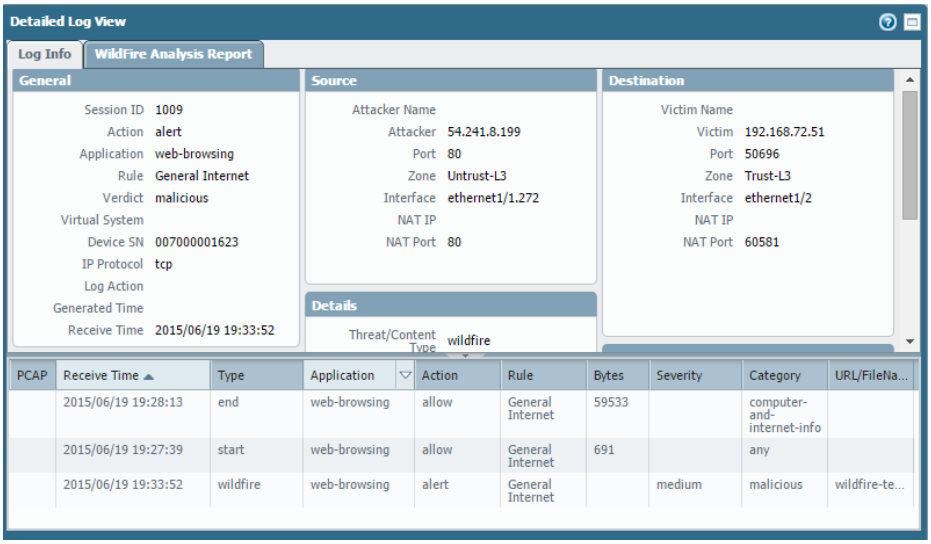
4. Click **OK**.
5. Commit all changes.

8.3 Test the WildFire Analysis Profile

1. Open a new browser in private/incognito mode and browse to `http://wildfire.paloaltonetworks.com/publicapi/test/pe`. This site generates an attack file with a unique signature, which simulates a zero-day attack.
2. Without opening the file, save it to the **Downloads** directory.
3. To verify that the file was uploaded to the public WildFire cloud, open **PuTTY** and double-click **firewall-management** to log in to the firewall with admin/admin.
4. When you are logged in, enter the `debug wildfire upload-log show` command to display the output `log: 0, filename: wildfire-test-pe-file.exe processed`.... This output verifies that the file was uploaded to the WildFire public cloud. The message might take a minute or two to appear:



5. Select **Monitor > Logs > WildFire Submissions**. After five minutes have passed, find the entry for **wildfire-test-pe-file.exe** that has been submitted to WildFire and identified as malicious.
6. Click the **magnifying glass** icon next to the entry to see the Detailed Log View of the WildFire entry:



7. On the **Log Info** tab, check the information within the **General**, **Details**, and **Destination** panels. Then look at the information in the **WildFire Analysis Report** tab.
8. Log out and close the **PuTTY** session.

8.4 Disable Security Policy Rule

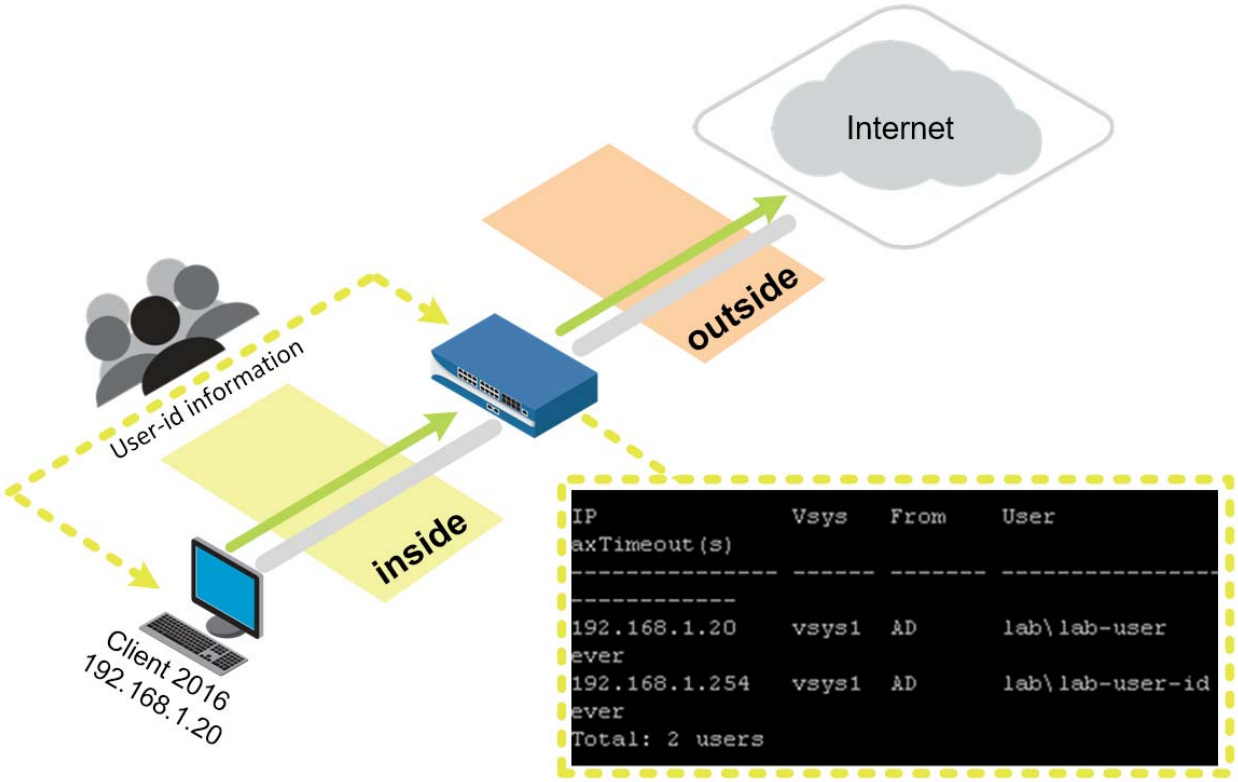
1. Select **Policies > Security**. 

2. Select but do not open **egress-outside-content-id**.
3. Click 
.
4. Select but do not open **egress-outside**.

5. Click Enable.
6. Commit all changes.

Stop. This is the end of the WildFire lab.

9. Lab: User-ID

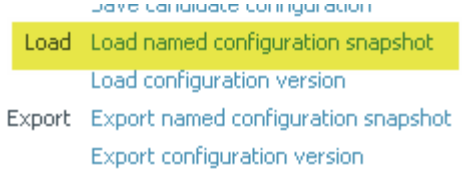


Lab Objectives

- Enable User-ID technology on the inside zone.
- Configure the LDAP Server Profile to be used in group mapping.
- Configure group mapping for User-ID.
- Configure and test the PAN-OS® integrated User-ID agent.
- Leverage User-ID information in a Security policy rule.

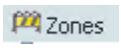
9.0 Load Lab Configuration

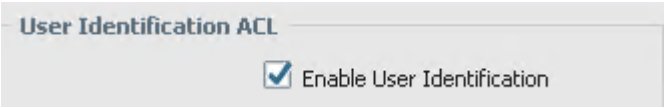
1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-09** and click **OK**.
4. Click **Close**.
5. Commit all changes.

9.1 Enable User-ID on the Inside Zone

1. In the WebUI select **Network > Zones**. 

2. Click to open the **inside** zone.
3. Enable User-ID by selecting the **Enable User Identification** check box:


4. Click **OK**.

9.2 Configure the LDAP Server Profile

Create a Server profile so that the firewall can pull group and user information from Active Directory.

1. In the WebUI select **Device > Server Profiles > LDAP**. 

2. Click 

and configure the following:

Parameter	Value#
Profile Name	`lab-active-directory`

3. Locate the server list on the left side of the window and click 

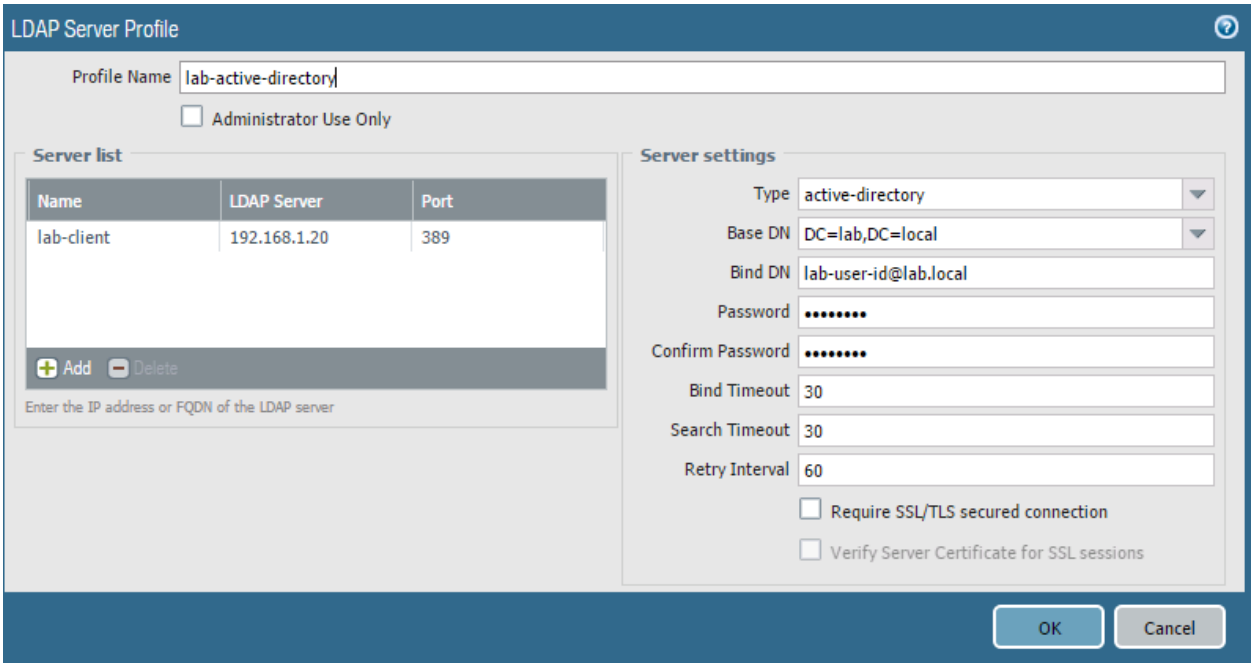
.
4. Configure the following:

Parameter	Value#
Name	`lab-client`
LDAP Server	`192.168.1.20`
Port	`389`

5. Locate **Server Settings** on the right side of the window and configure the following:

Parameter	Value#
Require SSL/TLS secured connection (*make sure to do this first*)	Deselect the check box
Type	**active-directory**
Base DN	`DC=lab,DC=local`

Parameter	Value#
Bind DN	`lab-user-id@lab.local`
Password	`Pal0Alt0`



6. Click **OK** to close the LDAP Server Profile configuration window.

9.3 Configure User-ID Group Mapping

Define which users and groups will be available when creating policy rules.

1. In the WebUI select **Device > User Identification > Group Mapping Settings**.
2. Click 

to open the Group Mapping configuration window.
3. Configure the following:

Parameter	Value#
Name	`lab-group-mapping`
Server Profile	**lab-active-directory** (all other fields will autopopulate)

4. Click the **Group Include List** tab and configure the following:

Parameter	Value#
Search box	`lab users`

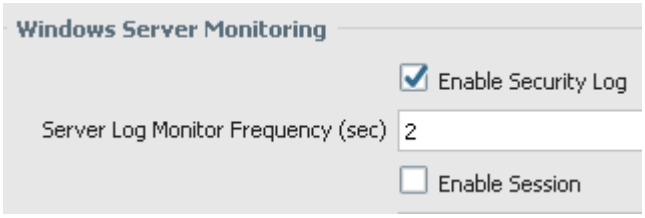
5. Click **OK**.

9.4 Configure Integrated Firewall Agent

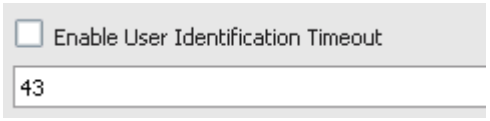
1. Select **Device > User Identification > User Mapping**.
2. Click the icon in the top-left of the **Palo Alto Networks User-ID Agent Setup** pane.
3. Configure the following:

Parameter	Value#
User Name	`lab.local\lab-user-id`
Password	`Pal0Alt0`

4. Click the **Server Monitor** tab and verify the following:

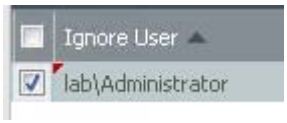
Parameter	Value#
Windows Server Monitoring	

5. Click the **Client Probing** tab.
6. Verify that the **Enable Probing** check box is deselected.
7. Click the **Cache** tab and configure the following:

Parameter	Value#
Enable User Identification Timeout	

Note: Ensure that the timeout option is *not* enabled. You do not need to time out the IP address associated with the lab-user-id because the IP never changes. In a production environment the timeout is recommended to be half the DHCP lease time.

8. Click the **Ignore User List** tab.
9. Click  and configure the following:

Parameter	Value#
Ignore User	 Prevents the firewall from assuming that Administrator is associated with 192.168.1.20

10. Click **OK**.
11. Scroll down to the **Server Monitoring** pane.
12. Click  and configure the following:

Parameter	Value#
Name	`lab-client`
Enabled	
Type	**Microsoft Active Diretory**

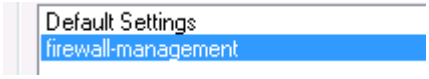
Parameter	Value#
Network Address	`192.168.1.20`

13. Click **OK**.
14. Commit all changes.

9.5 Verify User-ID Configuration

1. Under the **Server Monitoring** section, the status should be Connected:

2. On the Windows desktop, double-click the **lab** folder and then double-click the **bat files** folder.
3. Double-click the **user-id.bat** file  icon.
   Note: This action will force a login event for the firewall to parse.
4. On the Windows desktop, double-click the **PuTTY**  icon.
5. Double-click **firewall-management**:



6. Log in to the firewall with admin/admin.
7. Type the CLI command `show user group-mapping state all`.
   The output should be similar to the following:

```
admin@firewall-panos> show user group-mapping state all


Group Mapping(vsys1, type: active-directory): lab-group-mapping
        Bind DN    : CN=lab-user-id,CN=Managed Service Accounts,DC=lab,DC=local
        Base       : DC=lab,DC=local
        Group Filter: (None)
        User Filter: (None)
        Servers    : configured 1 servers
                192.168.1.20(389)
                        Last Action Time: 1536 secs ago(took 0 secs)
                        Next Action Time: In 2064 secs
        Number of Groups: 1
        cn=lab users,cn=users,dc=lab,dc=local
```

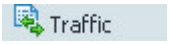
8. Type the CLI command `show user ip-user-mapping all`.
   The output should be similar to the following:

```
IP              Vsys    From    User                                IdleTimeout(s)
axTimeout(s)
--------------- ------ ------- ---------------------------------- --------------
------------
192.168.1.20    vsys1   AD      lab\lab-user                        Never
ever
192.168.1.254   vsys1   AD      lab\lab-user-id                     Never
ever
Total: 2 users
```

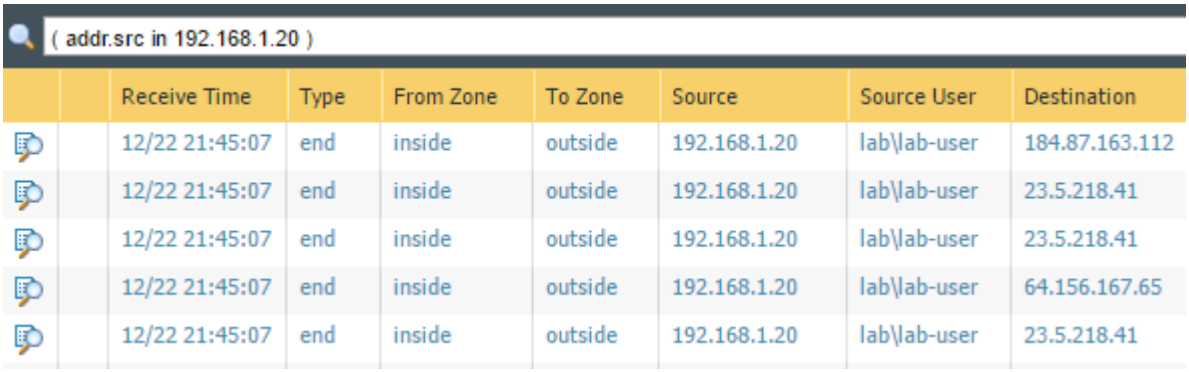
Note: lab\lab-user must have the IP address of 192.168.1.20. If that IP address is not listed, *do not* proceed. Contact your instructor or lab partner for assistance.

9. Open a browser and browse to `shutterfly.com` and `google.com` in order to generate some traffic.

9.6 Review Logs

1. Select **Monitor > Logs > Traffic**. 

2. Type the filter `(addr.src in 192.168.1.20 )` in the filter text box.
3. Notice that the **Source User** column now shows the lab-user. **Note:** This user-id references could take up to three minutes. Click  refresh to update the log entries:



9.7 Create Security Policy Rule

1. Select **Policies > Security**. 

2. Click 

to open the Security Policy Rule configuration window.
3. Configure the following:

Parameter	Value#
Name	`egress-outside-user-id`

4. Click the **Source** tab and configure the following:

Parameter	Value#
Source Zone	

5. Click the **User** tab and configure the following:

Parameter	Value#
Source User	 You must start typing before usernames become available on the drop-down list.

6. Click the **Destination** tab and configure the following:

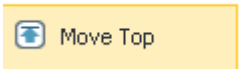
Parameter	Value#
Destination Zone	

7. Click the **Application** tab and configure the following:

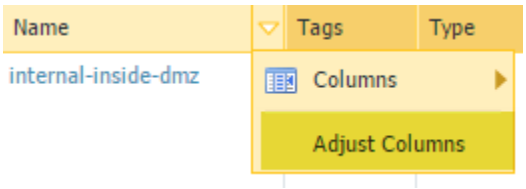
Parameter	Value#
Applications	`facebook-base`

8. Click the **Actions** tab and configure the following:

Parameter	Value#
Action	**Deny**

9. Click **OK** to close the Security Policy Rule configuration window.
10. Select but do not open the **egress-outside-user-id** Security policy rule.
11. Click  and select  .

12. You might need to Adjust columns.

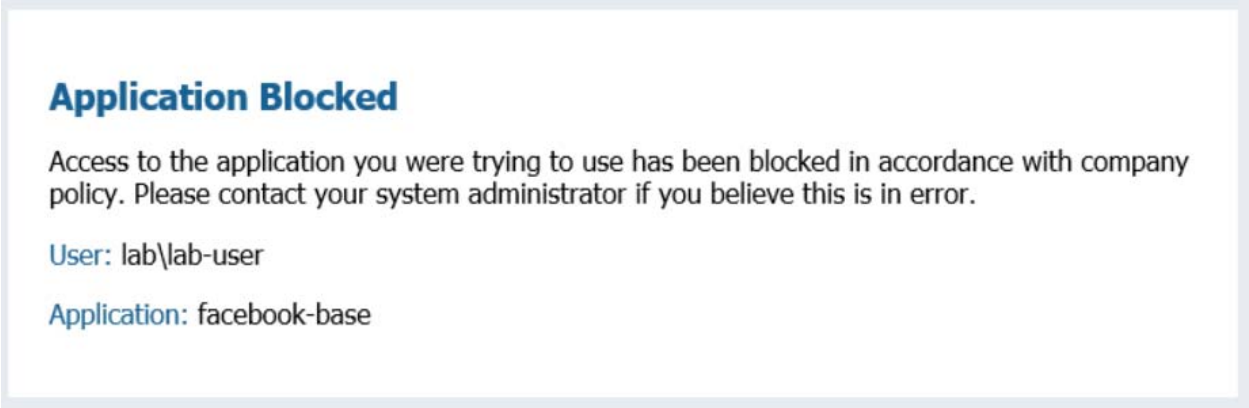


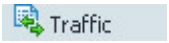
13.  all changes.

9.8 Review Logs

1. Open a new browser in private/incognito mode and browse to `www.facebook.com`.

The connection is denied based on the egress-outside-user-id Security policy rule:



2. Select **Monitor > Logs > Traffic**. 

3. Type the filter `(rule eq 'egress-outside-user-id')` in the filter text box.
4. Notice that the Source User column shows the **lab-user** and the Action is **reset-both**:

Source User	Destination	To Port	Application	Action	Rule	Session End Reason
lab\lab-user	157.240.8.35	443	facebook-base	reset-both	egress-outside-user-id	policy-deny
lab\lab-user	157.240.8.35	443	facebook-base	reset-both	egress-outside-user-id	policy-deny

9.9 Disable Integrated Firewall Agent

1. Select **Device > User Identification > User Mapping**.
2. Click to open the **lab-client** item under Server Monitoring:

3. Deselect the **Enabled** check box. 

4. Click **OK**.
5. Select **Policies > Security**. 

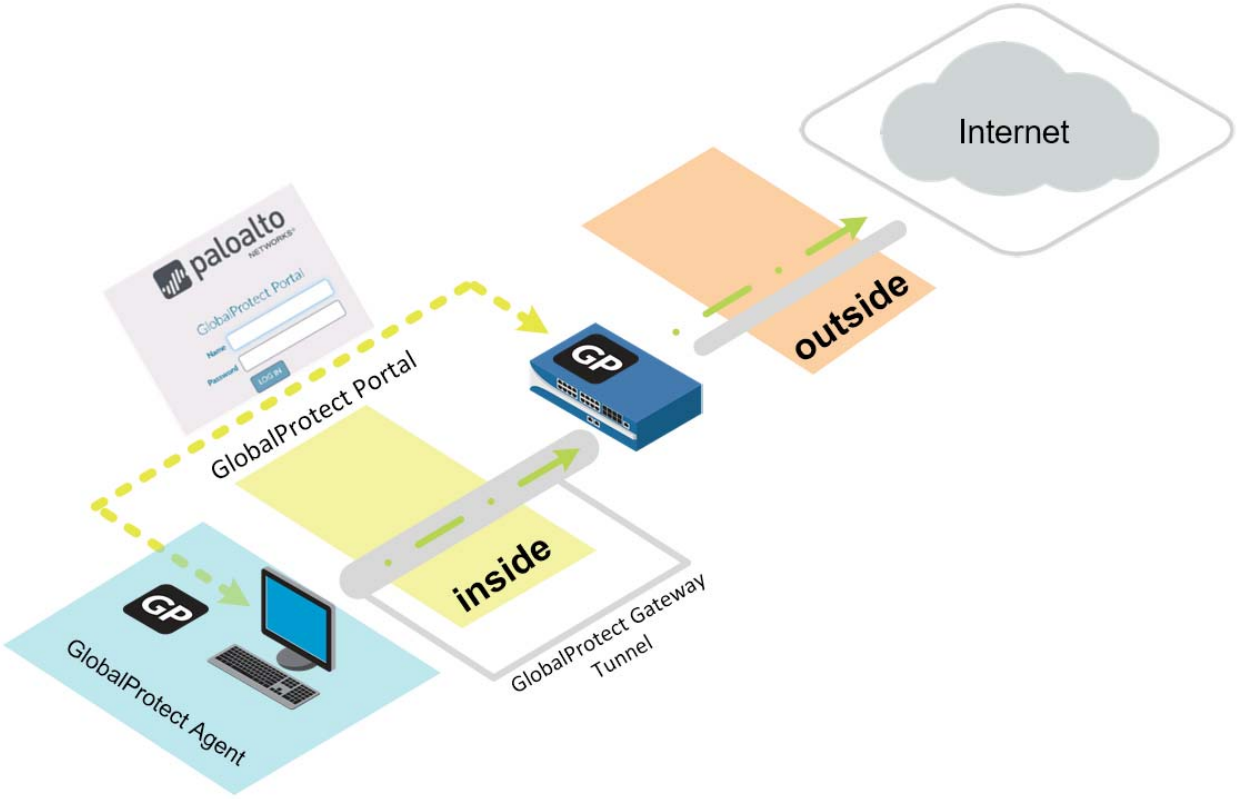
6. Select but do not open the Security policy rule named **egress-outside-user-id**.
7. Click 

.
8. Click **Yes**.
9. 

all changes.

Stop. This is the end of the User-ID lab.

10. Lab: GlobalProtect

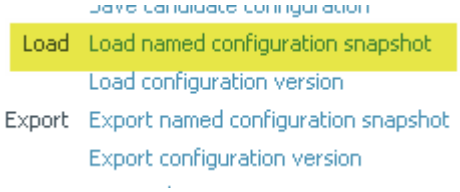


Lab Objectives

- Create and configure a subinterface.
- Create certificates for the GlobalProtect Portal, internal gateway, and external gateway.
- Attach certificates to a SSL-TLS Service Profile.
- Configure the Server Profile and Authentication Profile to be used when authenticating users.
- Create and configure the tunnel interface to be used with the external gateway.
- Configure the internal gateway, external gateway, and portal.
- Host the GlobalProtect agent on the portal for download.
- Create a No-NAT policy rule to ensure that portal traffic is not subjected to network address translation.
- Test the external gateway and internal gateway.

10.0 Load Lab Configuration

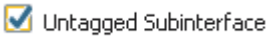
1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-10** and click **OK**.
4. Click **Close**.
5. Commit all changes.

10.1 Configure a Subinterface

Subinterfaces enable logical interfaces to be associated with a physical interface. By default, VLAN tags are required for subinterfaces. However, untagged interfaces can be used to isolate traffic via zones on the same physical interface. A subinterface is created in the lab to provide experience using a subinterface. Traffic will not be isolated using zones.

1. Select **Network > Interfaces > Ethernet**.
2. Click to open **ethernet1/2**.
3. Click the **Advanced** tab.
4. Select the **Untagged Subinterface** check box. 

5. Click **OK**.
6. Verify that **ethernet1/2** is still selected and click 
.
7. Configure the following:

Parameter	Value#
Interface Name	 ethernet1/2 . 2 #
Comment	`internal gateway`
Virtual Router	**lab-vr**
Security Zone	**inside**

8. Click the **IPv4** tab and configure the following:

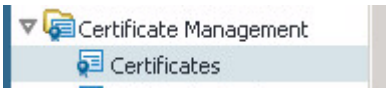
Parameter	Value#
IP	`192.168.2.1/24#`

9. Click the **Advanced** tab and select **ping** for the Management Profile.
10. Click **OK**.

10.2 Generate Self-Signed Certificates

GlobalProtect needs three certificates, one each for the portal, external gateway, and internal gateway. These certificates typically are signed by a common CA certificate. This lab creates a CA certificate and Internal Gateway certificate, but combines the Portal and External Gateway certificates because these GlobalProtect functions are combined on the same IP address.

1. In the WebUI select **Device > Certificate Management > Certificates**.



2. Click 

and create a certificate:

Parameter	Value#
Certificate Name	`GlobalProtect#`
Common Name	`GlobalProtect`
Signed By	Leave blank
Certificate Authority	Select the check box

3. Click 

.
4. Click **OK** to dismiss the successful status window.
5. Click 

and create another certificate:

Parameter	Value#
Certificate Name	`external-gw-portal#`
Common Name	`203.0.113.20`
Signed By	**GlobalProtect**

6. Click 

.
7. Click **OK** to dismiss the successful status window.
8. Click 

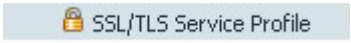
and create another certificate:

Parameter	Value#
Certificate Name	`internal-gw#`
Common Name	`192.168.2.1`
Signed By	**GlobalProtect**

9. Click 

.
10. Click **OK** to dismiss the successful status window.

10.3 Configure the SSL-TLS Service Profile

1. Select **Device > Certificate Management > SSL/TLS Service Profile**.


2. Click 

and create an SSL/TLS Service Profile:

Parameter	Value#
Name	`external-gw-portal`
Certificate	**external-gw-portal**

3. Click **OK**.
4. Click 

and create an SSL/TLS Service Profile:

Parameter	Value#
Name	`internal-gw`
Certificate	**internal-gw**

5. Click **OK**.

10.4 Configure the LDAP Server Profile

Do not perform this task if an LDAP Server Profile exists.

1. In the WebUI select **Device > Server Profiles > LDAP**. 

2. Click 

and configure the following:

Parameter	Value#
Profile Name	`lab-active-directory`

3. Locate the **Server list** on the left side of the window and click 

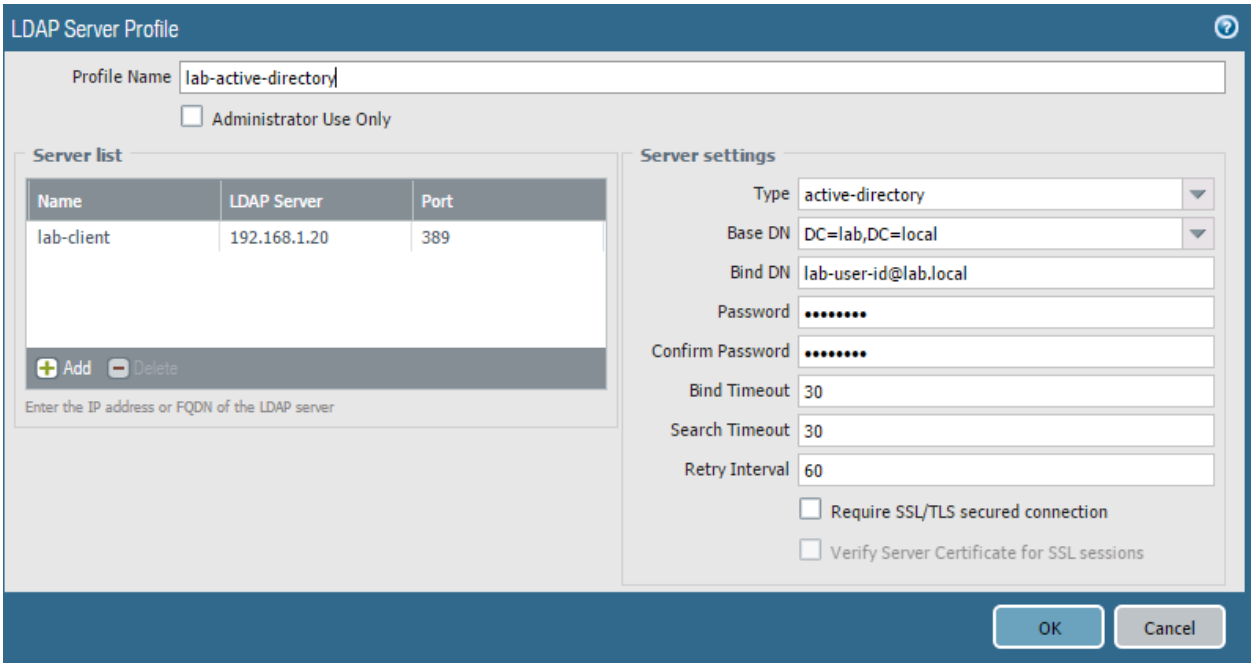
.
4. Configure the following:

Parameter	Value#
Name	`lab-client`
LDAP Server	`192.168.1.20`

Parameter	Value#
Port	389

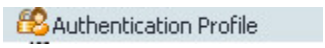
5. Locate **Server settings** on the right-side of the window and configure the following:

Parameter	Value#
Type	**active-directory**
Require SSL/TLS secured connection *(Make sure to do this before proceeding)*	Deselect the check box
Base DN	DC=lab,DC=local
Bind DN	lab-user-id@lab.local
Password	Pal0Alt0



6. Click **OK** to close the LDAP Server Profile configuration window.

10.5 Configure the Authentication Profile

1. Select **Device > Authentication Profile**. 

2. Click 

and configure the following:

Parameter	Value#
Name	`auth-gp`
Type	**LDAP**
Server Profile	**lab-active-directory**
User Domain	`lab.local`

3. Click the **Advanced** tab.
4. Configure the following:

Parameter	Value#
Allow List	**all**

5. Click **OK**.

10.6 Configure the Tunnel Interface

1. Select **Network > Interfaces > Tunnel**.
2. Click 

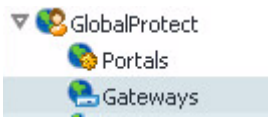
and create a new tunnel interface:

Parameter	Value#
Interface Name	
Virtual Router	**lab-vr**
Security Zone	**inside**

3. Click **OK** to close the Tunnel Interface configuration window.

10.7 Configure the Internal Gateway

Internal gateways are used for User-ID deployment and Host Information Profile (HIP) enforcement.

1. In the WebUI select **Network > GlobalProtect > Gateways**. 

2. Click 

to create a gateway. The GlobalProtect Gateway Configuration window opens.
3. Configure the following:

Parameter	Value#
Name	`gp-int-gateway`
Interface	**ethernet1/2.2**
IPv4 Address	**192.168.2.1**

4. Select the **Authentication** tab and configure the following:

Parameter	Value#
SSL/TLS Service Profile	**internal-gw**

5. Locate the **Client Authentication** list box. Click 

and configure the following:

Parameter	Value#
Name	`lab-ad`
OS	**Any**
Authentication Profile	**auth-gp**

6. Click **OK**.

10.8 Configure the External Gateway

1. Click 

to create a gateway. The GlobalProtect Gateway configuration window opens.
2. Configure the following:

Parameter	Value#
Name	`gp-ext-gateway`
Interface	**ethernet1/1**
IPv4 Address	**203.0.113.20/24**

3. Select the **Authentication** tab and configure the following:

Parameter	Value#
SSL/TLS Service Profile	**external-gw-portal**

4. Locate the **Client Authentication** list box. Click 

and configure the following:

Parameter	Value#
Name	`lab-ad`

Parameter	Value#
OS	**Any**
Authentication Profile	**auth-gp**

5. Click the **Agent** tab and configure the following:

Parameter	Value#
Tunnel Mode	Select the check box
Tunnel Interface	**tunnel.11**
Enable IPSec	Verify that the check box is selected

6. Click the **Client Settings** subtab.
7. Click 

and configure the following:

Parameter	Value#
Name	`gp-client-config`

8. Click the **IP Pools** tab and configure the following:

Parameter	Value#
IP Pool	Click  and type `192.168.100.200-192.168.100.210`

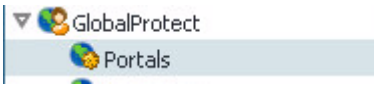
9. Click **OK** to close the Configs window.
   The GlobalProtect Gateway configuration window should still be open.
10. Click the **Network Services** subtab and configure the following:

Parameter	Value#
Primary DNS	`4.2.2.2`
Secondary DNS	`8.8.8.8`

11. Click **OK** to close the GlobalProtect Gateway configuration window.

10.9 Configure the Portal

The GlobalProtect Portal provides the management functions for the GlobalProtect infrastructure. Every endpoint that participates in the GlobalProtect network receives its configuration from the portal, including information about the available GlobalProtect gateways and any client certificates that might be necessary for the client to connect to a gateway.

1. Select **Network > GlobalProtect > Portals**. 

2. Click 

to create a portal. The GlobalProtect Portal configuration window opens.
3. Configure the following:

Parameter	Value#
Name	`gp-portal`
Interface	**ethernet1/1**
IPv4 Address	**203.0.113.20/24**

4. Click the **Authentication** tab and configure the following:

Parameter	Value#
SSL/TLS Service Profile	**external-gw-portal**

5. Locate the **Client Authentication** list box. Click 

and configure the following:

Parameter	Value#
Name	`lab-ad`
OS	**Any**
Authentication Profile	**auth-gp**

6. Click the **Agent** tab.
7. Locate the **Agent** list box and click 

to open the Configs window and configure the following:

Parameter	Value#
Name	`portal-agent-config`

8. Click the **Internal** tab.
9. Select the **Internal Host Detection IPv4** check box.
10. Configure the following:

Parameter	Value#
IP Address	`192.168.2.1`
Hostname	`gp-int-gw.lab.local`

11. Locate the **Internal Gateways** list box and click 

to open the Internal Gateway configuration window.

12. Configure the following:

Parameter	Value#
Name	`int-gw-1`
Address	**IP**
IPv4	`192.168.2.1`

13. Click **OK** to close the Internal Gateway configuration window.
14. Click the **External** tab.
15. Locate the **External Gateways** list box and click 

to open the External Gateway configuration window.
16. Configure the following:

Parameter	Value#
Name	`ext-gw-1`
Address	**IP**
IPv4	`203.0.113.20`

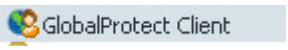
17. Locate the **Source Region** list box and click 

and configure the following:

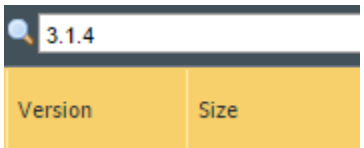
Parameter	Value#
Source Region	**Any**
Priority	**Highest**

18. Click **OK** three times to close the External Gateway, Configs, and GlobalProtect Portal configuration windows.

10.10 Host the GlobalProtect Agent on the Portal

1. In the WebUI select **Device > GlobalProtect Client**. 

2. Click **Check Now**. The Palo Alto Networks firewall checks for the latest version of the GlobalProtect agent.
3. Search for 3.14.



4. Click **Download** next to the latest version of the GlobalProtect *that does not have a, b, or c in its name.*
5. **Activate** the GlobalProtect agent that you have just downloaded:

10.11 Create Security Policy Rule

1. Select **Policies > Security**. 

2. Select the **egress-outside** Security policy rule without opening it.
3. Click 

. The Clone configuration window opens.
4. Select **Move top** from the **Rule Order** drop-down list.
5. Click **OK** to close the Clone configuration window.
6. Click to open the cloned Security policy rule named **egress-outside-1**.
7. Configure the following:

Parameter	Value#
Name	`inside-portal`
Tags	**internal**

8. Click the **Destination** tab and configure the following:

Parameter	Value#
Destination Address	`203.0.113.20`

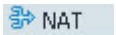
9. Click the **Service/URL Category** tab and configure the following:

Parameter	Value#
Service	

10. Click **OK** to close the Security Policy Rule configuration window.

10.12 Create a No-NAT Rule

All traffic from the inside zone to the outside zone uses source NAT. You will create a new NAT policy rule so that internal requests for the GlobalProtect Portal will not get their address translated by the source-egress-public rule. The new NAT policy rule must be matched before the source-egress-outside rule.

1. Select **Policies > NAT**. 

2. Click 

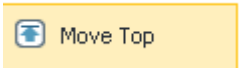
to define a new source NAT policy rule.
3. Configure the following:

Parameter	Value#
Name	gp-portal-no-nat#
Tags	**internal**

4. Click the **Original Packet** tab and configure the following:

Parameter	Value#
Source Zone	**inside**
Destination Zone	**outside**
Destination Interface	**ethernet1/1**
Destination Address	203.0.113.20

5. Click **OK** to close the NAT Policy Rule configuration window.
6. Select but do not open the **gp-portal-no-nat** NAT Policy rule.
7. Click 

and select 

.
8. 

all changes.

   Note: A warning might appear about IPv6. It can be safely ignored.

10.13 Download the GlobalProtect Agent

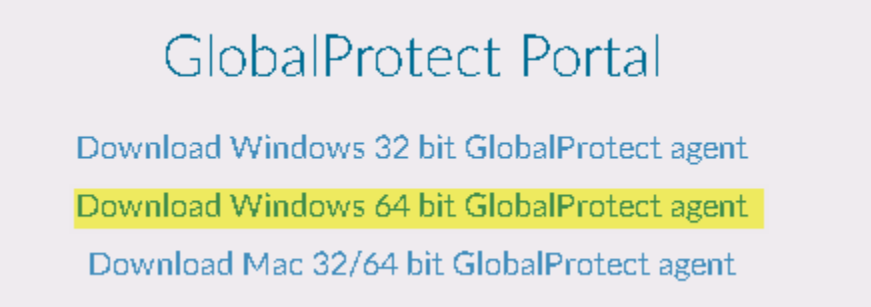
1. Open a new browser window in private/incognito mode and browse to https://203.0.113.20. Proceed past the certificate error.

The GlobalProtect Portal login page is presented.

2. Log in with the following:

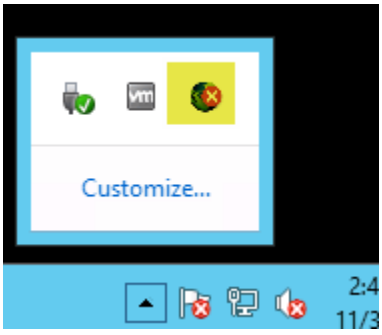
Parameter	Value#
Name	lab-user
Password	Pal0Alt0

3. Download the Windows 64-bit MSI install file and use it to install the 64-bit GlobalProtect agent:



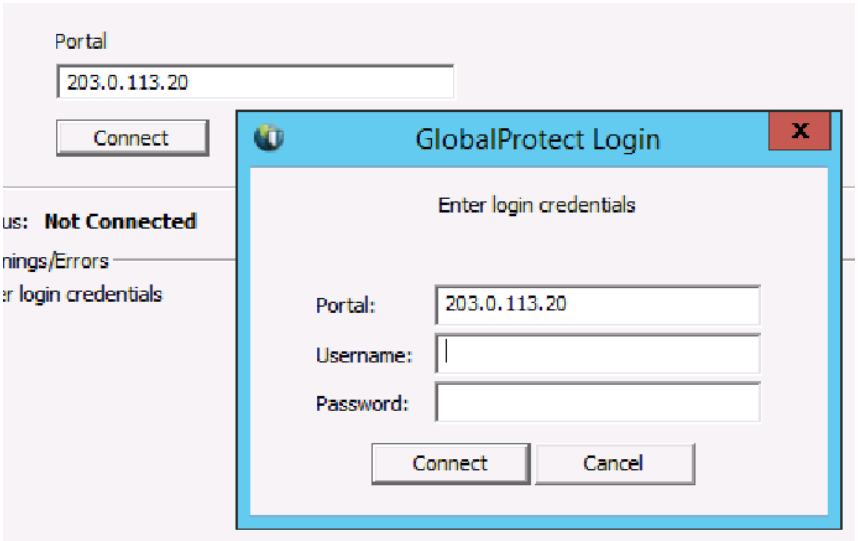
10.14 Connect to the External Gateway

1. Double-click the GlobalProtect agent in the Windows desktop system tray:



Note: This action might take a minute.

2. Type `203.0.113.20` for the portal name.
3. Click **Connect**. Connecting can take a moment.
4. Click **Continue** when presented with a certificate warning:

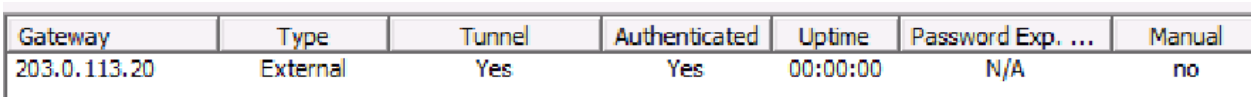


5. Log in using the following information, and then click **Connect**. Click **Continue** if you receive another certificate warning:

Parameter	Value#
Name	`lab-user`
Password	`Pal0Alt0`

6. After a moment the status should update to **Connected**:

7. The system tray icon should update to  .
8. Click the **Details** tab in the GlobalProtect window.
   Notice that at the bottom of the window the gateway is listed as 203.0.113.20, the gateway type is External, and a tunnel is established:



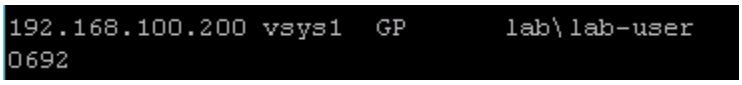
Gateway	Type	Tunnel	Authenticated	Uptime	Password Exp. ...	Manual
203.0.113.20	External	Yes	Yes	00:00:00	N/A	no

9. Click the **Troubleshooting** tab and select **Network Configurations**.
10. Notice that the IP assigned is the first in the IP Pool specified on the external gateway:

10.15 View User-ID Information

1. On the Windows desktop, double-click the **PuTTY**  icon.
2. Double-click **firewall-management** and log in to the firewall.
3. Type the command `show user ip-user-mapping all`.

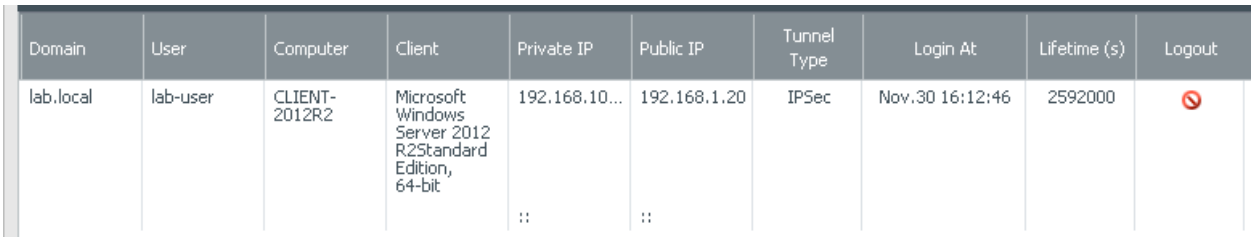
The IP addresses for lab-user have been updated to include the tunnel IP address. Notice that the **From** column lists GP (GlobalProtect):



10.16 Disconnect the Connected User

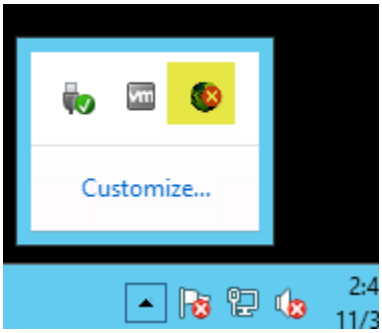
1. In the WebUI select **Network > GlobalProtect > Gateways**. 

2. Click  to the far right of the gp-ext-gateway:



Domain	User	Computer	Client	Private IP	Public IP	Tunnel Type	Login At	Lifetime (s)	Logout
lab.local	lab-user	CLIENT-2012R2	Microsoft Windows Server 2012 R2Standard Edition, 64-bit	192.168.10... ::	192.168.1.20 ::	IPSec	Nov.30 16:12:46	2592000	

3. Click to disconnect the lab-user.
4. Click **Close**.
5. Right-click the GlobalProtect agent in the Windows desktop system tray and click **Disable**:



10.17 Configure DNS Proxy

DNS servers perform the service of resolving a domain name to an IP address and vice versa. When you configure the firewall as a DNS proxy, it acts as an intermediary between DNS clients and DNS servers, and as a DNS server by resolving queries from its DNS cache or forwarding queries to other DNS servers. Configuration of the firewall to be a DNS proxy is required so that GlobalProtect internal host detection works correctly.

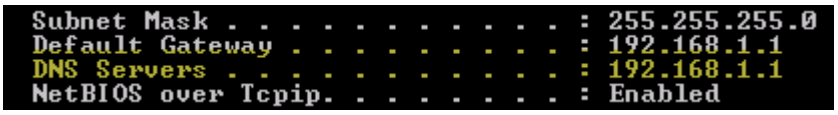
1. In the WebUI select **Network > DNS Proxy**. DNS Proxy
2. Click Add to open the DNS Proxy configuration window.
3. Configure the following:

Parameter	Value#
Name	`gp-dns-proxy`
Interface	Add **ethernet1/2**
Primary	`4.2.2.2`
Secondary	`8.8.8.8`

4. Click the **Static Entries** tab.
5. Click Add and configure the following:

Parameter	Value#
Name	`Internal Host Detection`
FQDN	`gp-int-gw.lab.local`
Address	`192.168.2.1`

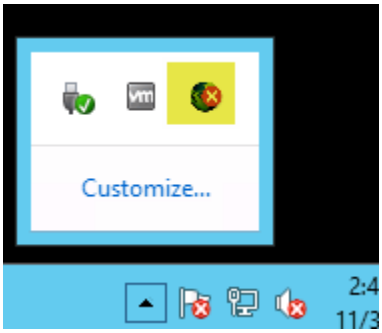
6. Click **OK** twice.
7. Commit all changes.
8. On the Windows desktop, double-click the **lab** folder and then the **bat files** folder.
9. Right-click the **set-dns-proxy.bat** batch file and select **Run as administrator**.
10. On the Windows desktop, right-click the CMD  icon and select **Run as administrator**.
11. Type the command `ipconfig /all`.
12. Verify that the current DNS server is 192.168.1.1:



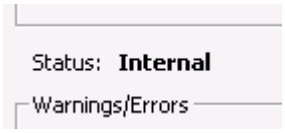
Note: Do *not* continue if the DNS server is otherwise. Contact the instructor.

10.18 Connect to the Internal Gateway

1. Right-click the **GlobalProtect** agent in the Windows desktop system tray and select **Enable**.
2. Double-click the **GlobalProtect** agent in the Windows desktop system tray. Click **Continue** if warned about the certificate:



After a moment the status should update to Internal:



3. The system tray icon should update to  .
4. Click the **Details** tab in the GlobalProtect window and notice at the bottom of the window that the gateway is listed as 192.168.2.1, the gateway type is Internal, and a tunnel is not established:

Gateway	Type	Tunnel	Authenticated
192.168.2.1	Internal	No	No

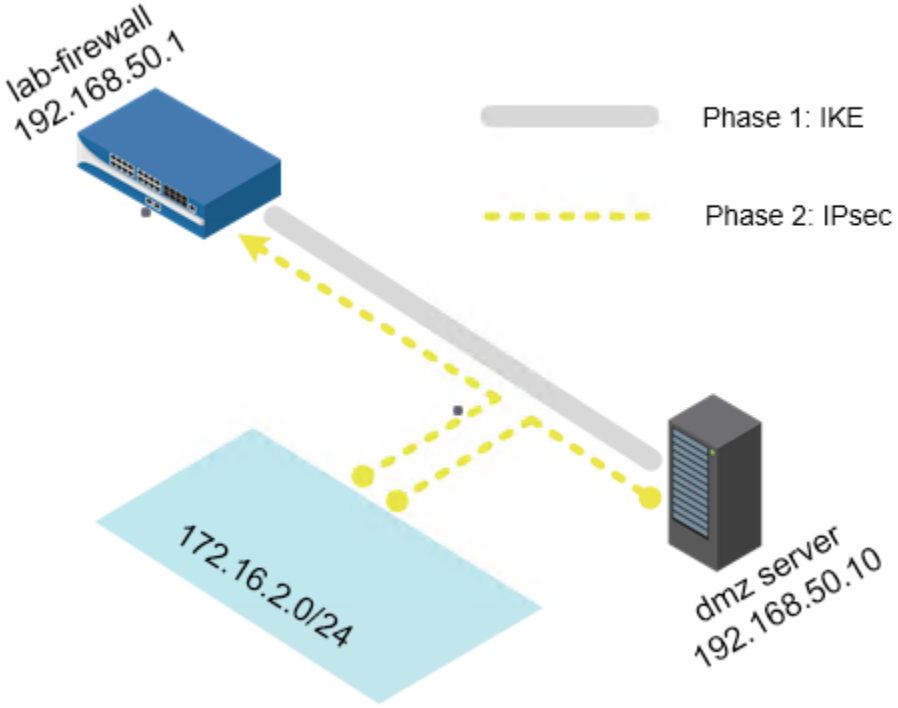
10.19 Reset DNS

1. On the Windows desktop, double-click the **lab** folder and then the **bat files** folder.
2. Right-click the **remove-dns-proxy.bat** batch file and select **Run as administrator**.
3. Use the Windows tools to uninstall the GlobalProtect Agent.
4. On the Windows desktop, right-click the **CMD**  icon, and select **Run as administrator**.
5. Type the command `ipconfig /all`.
6. Verify that the current DNS server is 127.0.0.1:

Note: Do *not* continue if the DNS server is otherwise. Contact the instructor.

Stop. This is the end of the GlobalProtect lab.

11. Lab: Site-to-Site VPN

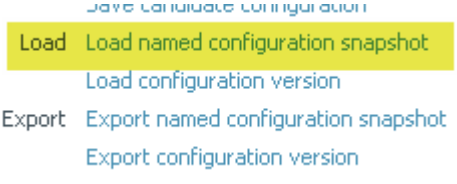


Lab Objectives

- Create and configure a tunnel interface to use in the site-to-site VPN connection.
- Configure the IKE gateway and IKE Crypto Profile.
- Configure the IPSec Crypto Profile and IPsec tunnel.
- Test connectivity.

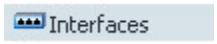
11.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-11** and click **OK**.
4. Click **Close**.
5. Commit all changes.

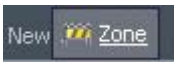
11.1 Configure the Tunnel Interface

1. In the WebUI select **Network > Interfaces**. 

2. Click the **Tunnel** tab. 

3. Click 

to configure a tunnel interface:

Parameter	Value#
Interface Name	In the text box to the right of tunnel, enter `12`
Comment	`Tunnel to DMZ`
Virtual Router	**lab-vr**
Security Zone	Create and assign a new Layer 3 zone named `VPN` 

4. Click the **IPv4** tab and configure the following:

Parameter	Value#
IP	`172.16.2.10/24`

5. Click the **Advanced** tab and configure the following:

Parameter	Value#
Management Profile	**ping**

6. Click **OK** to close the Tunnel Interface configuration window.

11.2 Configure the IKE Gateway

1. Select **Network > Network Profiles > IKE Gateways**. 

2. Click 

to create the IKE gateway and configure the following:

Parameter	Value#
Name	`dmz-ike-gateway#`
Version	**IKEv1 only mode**
Interface	**ethernet1/3**

Parameter	Value#
Local IP Address	Select **192.168.50.1/24**
Peer Type	**static**
Peer IP Address	`192.168.50.10`
Pre-shared Key	`paloalto#`

3. Click the **Advanced Options** tab.
4. On the **IKEv1** subtab configure the following:

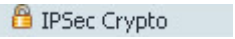
Parameter	Value#
IKE Crypto Profile	Select 

5. Configure the following:

Parameter	Value#
Name	`AES256-DH2-SHA2`
DH Group	Add **Group 2**
Authentication	Add **sha256**
Encryption	Add **aes-256-cbc**

6. Click **OK** twice to close the IKE Crypto Profile and the IKE Gateway window.

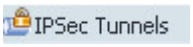
11.3 Create an IPSec Crypto Profile

1. In the WebUI select **Network > Network Profiles > IPSec Crypto**. 
2. Click  to open the IPSec Crypto Profile configuration window.
3. Configure the following:

Parameter	Value#
Name	AES256-SHA256#
IPSec Protocol	**ESP**
Encryption	Add **aes-256-cbc**
Authentication	Add **sha256**
DH Groups	Select **group2**

4. Click **OK** to close the IPSec Crypto Profile configuration window.

11.4 Configure the IPsec Tunnel

1. In the WebUI select **Network > IPSec Tunnels**. 

2. Click 

to define the IPsec tunnel.
3. On the **General** tab:

Parameter	Value#
Name	`dmz-tunnel#`
Tunnel Interface	**tunnel.12**
Type	**Auto Key**
IKE Gateway	**dmz-ike-gateway**
IPSec Crypto Profile	**AES256-SHA256**
Show Advanced Options	Select the check box
Tunnel Monitor	Select the check box
Destination IP	`172.16.2.11`

4. Click the **Proxy IDs** tab.
5. Click **Add** and configure the following:

Parameter	Value#
Proxy ID	`dmz–tunnel-network#`
Local	`172.16.2.0/24`
Remote	`172.16.2.0/24`

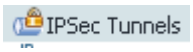
6. Click **OK** twice to close the Proxy IDs and IPsec Tunnel windows:

Name	Status	Type	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
dmz-tunnel	Tunnel Info	Auto Key	etherne...	192.16...	192.16...	IKE Info	tunnel.12	lab-vr (Show Routes)	vsys1	VPN	

7. 

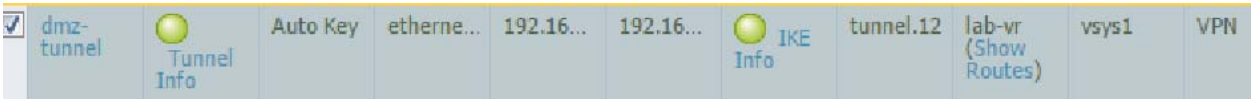
all changes.

11.5 Test Connectivity

1. Select **Network > IPSec Tunnels**. 

Notice that the Status column indicator on the VPN tunnel might be red.

2. Refresh the **Network > IPSec Tunnels** page. The Status column indicator is now green:



3. Select **Monitor > Logs > System**. System
4. Review the VPN log entries:

12/27 21:46:41	vpn	informational	ipsec-key-install	dmz-tunnel:dmz-network	IPSec key installed. Installed SA: 192.168.50.1[500]-192.168.50.10[500] SPI:0xA7B29CF3/0xFD87733D lifetime 3600 Sec lifesize unlimited.
12/27 21:46:41	vpn	informational	ike-nego-p2-succ	dmz-tunnel:dmz-network	IKE phase-2 negotiation is succeeded as initiator, quick mode. Established SA: 192.168.50.1[500]-192.168.50.10[500] message id:0x81ED59A0, SPI:0xA7B29CF3/0xFD87733D.
12/27 21:46:41	vpn	informational	ike-nego-p2-start	dmz-tunnel:dmz-network	IKE phase-2 negotiation is started as initiator, quick mode. Initiated SA: 192.168.50.1[500]-192.168.50.10[500] message id:0x81ED59A0.

5. On the Windows desktop, launch **PuTTY**, double-click **firewall-management**, and log in to the firewall.
6. After the VPN tunnel is connected, type the following CLI commands and observe the output:

```
show vpn ike-sa
show vpn ipsec-sa tunnel dmz-tunnel-network
show vpn flow name dmz-tunnel
show running tunnel flow
```

Stop. This is the end of the Site-to-Site VPN lab.

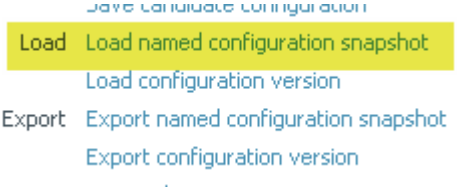
12. Lab: Monitoring and Reporting

Lab Objectives

- Explore the Session Browser, App-Scope, and Application Command Center (ACC).
- Investigate traffic via the ACC and logs.
- Generate a User Activity report.
- Create a Custom report.
- Create a Report Group.
- Configure an email schedule.

12.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-12** and click **OK**.
4. Click **Close**.
5. Commit all changes.

12.1 Generate Traffic

Note: The metrics displayed in the lab screenshots and the metrics displayed on your lab firewall might be different.

Pre-populate the firewall with log entries and usernames that you can observe and investigate in this lab.

1. On the Windows desktop, open **PuTTY** and double-click **traffic-generator**.
2. Enter the following information when prompted:

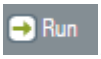
Parameter	Value#
Password	`Pal0Alt0`

3. While in the PuTTY window, type the command `sh /tg/traffic.sh`.
   Note: After you execute the command, it can take up to 10 minutes to complete. Wait until it is finished before proceeding.

12.2 Explore the Session Browser

The Session Browser enables you to browse and filter current running sessions on the firewall.

1. Select **Monitor > Session Browser** 

to see any current sessions. You might be able to see simulated sessions from the generated traffic. Notice that there is no Source User column.
2. Click the  icon at the top-right of the window to open the Filters pane.
3. Type `lab\jamie` in the From User field.
4. Click 

.
5. Notice that, even though there is not a Source User column, there is an ability to search for the **From User**. **Note:** You can also search for a **To User**.

From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application
danger	danger	192.168.3.131	65.54.95.142	55973	80	6	web-browsing
danger	danger	192.168.3.131	204.14.234.85	57245	8443	6	salesforce-base
danger	danger	192.168.3.131	204.14.234.85	57248	8443	6	salesforce-base

6. Locate a **salesforce-base** entry and click the **Plus** icon on the left to expand the display. Notice the three sections labeled Detail, Flow 1, and Flow 2.
7. In the Detail section, you can see various items of information.
   Important items that can help when troubleshooting are Session ID, Application, Security Rule, QoS Rule, and Class:

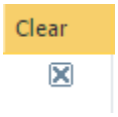
Detail	
Session ID	25167
Timeout	600
Time To Live	600
Virtual System	vsys1
Application	salesforce-base
Protocol	6
Security Rule	intrazone-default
QoS Rule	N/A
QoS Class	4
Created By Syn Cookie	False
To Host Session	False
Traverse Tunnel	False
Captive Portal	False
Session End Log	False
Session In Ager	True
Session From HA	False

Notice **c2s** (Client to Server) and **s2c** (Server to Client) in Flow 1 and Flow 2:

Flow 1		Flow 2	
Direction	c2s	Direction	s2c
From Zone	danger	From Zone	danger
Source	192.168.3.131	Source	204.14.234.85
Destination	204.14.234.85	Destination	192.168.3.131
From Port	57248	From Port	8443
To Port	8443	To Port	57248
From User	lab\jamie	From User	unknown
To User	unknown	To User	lab\jamie
State	ACTIVE	State	ACTIVE
Type	FLOW	Type	FLOW

These flows provide information about both the request and response traffic.

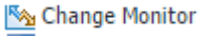
8. You can end an active session by clicking the **X** icon at the far right of a session row:



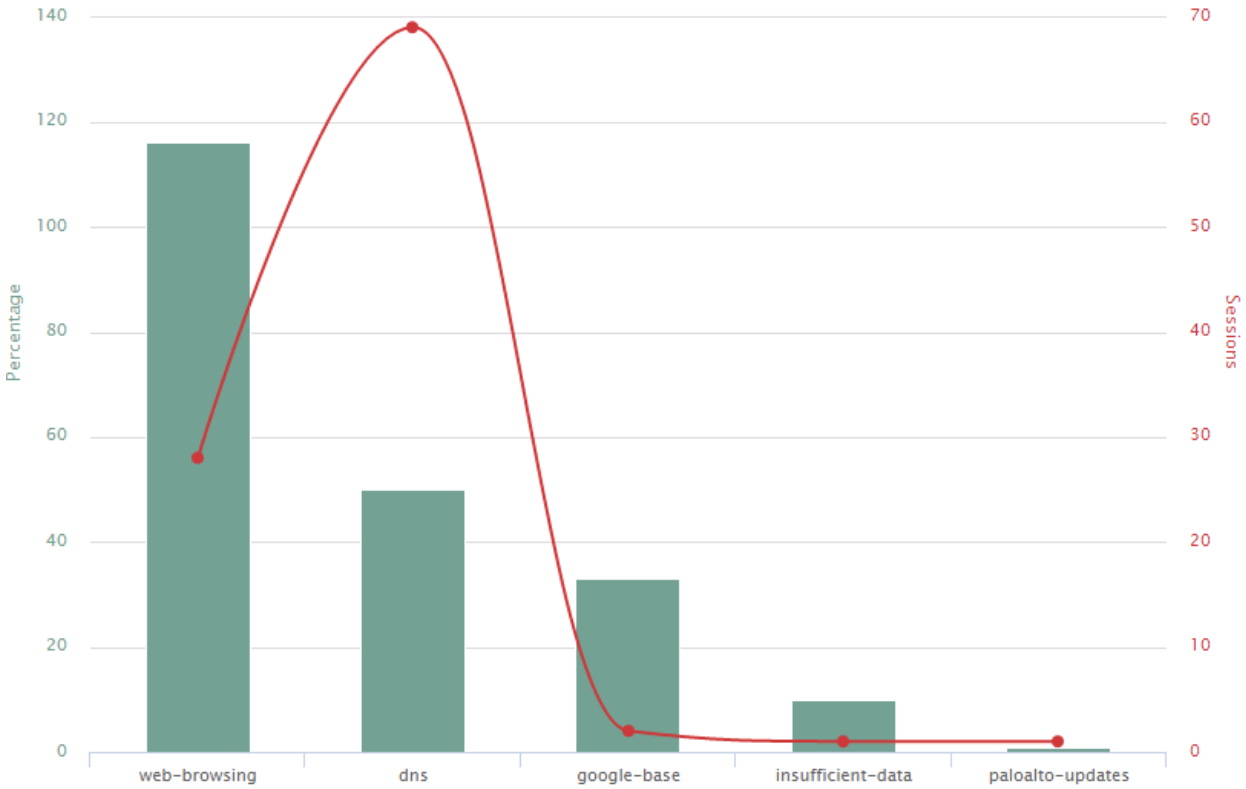
12.3 Explore App-Scope

With the App-Scope reports, you can quickly see if any behavior is unusual or unexpected, which helps identify problematic behavior. Each report provides a dynamic, user-customizable window into the network. Long-term trends are difficult to represent in a lab environment. However, knowing where to look is key to finding potential issues.

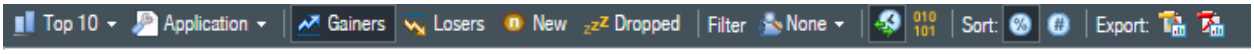
1. Select **Monitor > App Scope > Summary**. 

The Summary report displays charts for the top five gainers, losers, and bandwidth-consuming applications, application categories, users, and sources.
2. Select **Monitor > App Scope > Change Monitor**. 

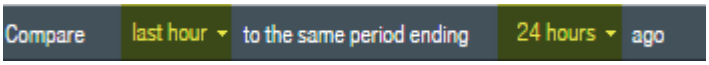
The Change Monitor report displays changes over a specified time period. For example, the following figure displays the top applications that gained in use over the last hour as compared with the last 24-hour period. The top applications are determined by session count and are sorted by percentage.

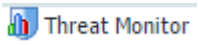


3. The type of information displayed can be controlled at the top. The displayed Graph can be exported as a PDF or PNG:

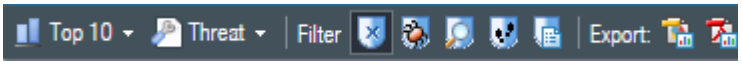


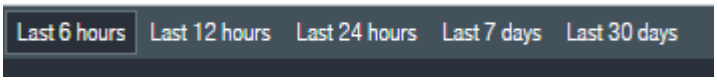
4. The time period also can be changed at the bottom:

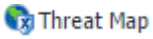


5. Select **Monitor > App Scope > Threat Monitor**. 

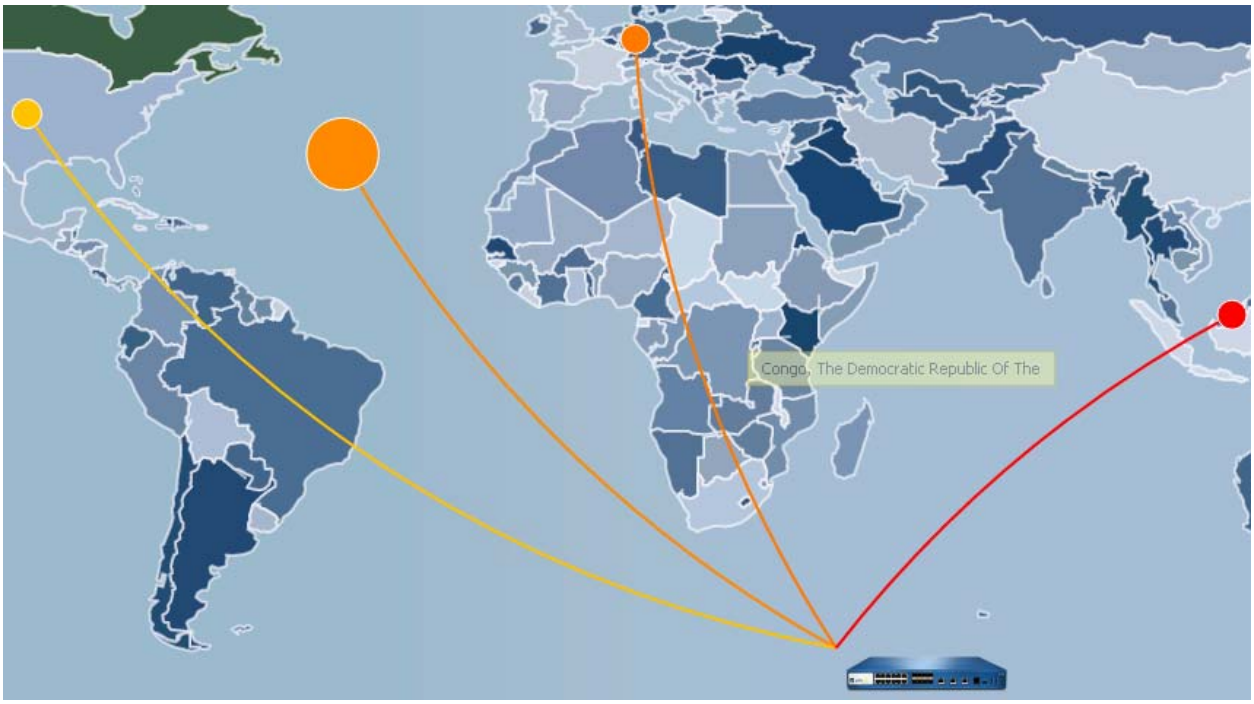
The Threat Monitor report displays a count of the top threats over the selected time period. By default, the figure shows the top 10 threat types for the past six hours.
6. The type of threat also can be filtered at the top:



7. The time period can be changed to the Last 6 hours, 12 hours, 24 hours, 7 days, or 30 days. 

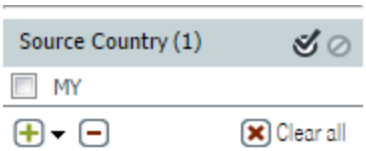
8. Select **Monitor > App Scope > Threat Map**. 

The Threat Map report shows a geographical view of threats, including severity.
9. Click **Last 30 Days**:

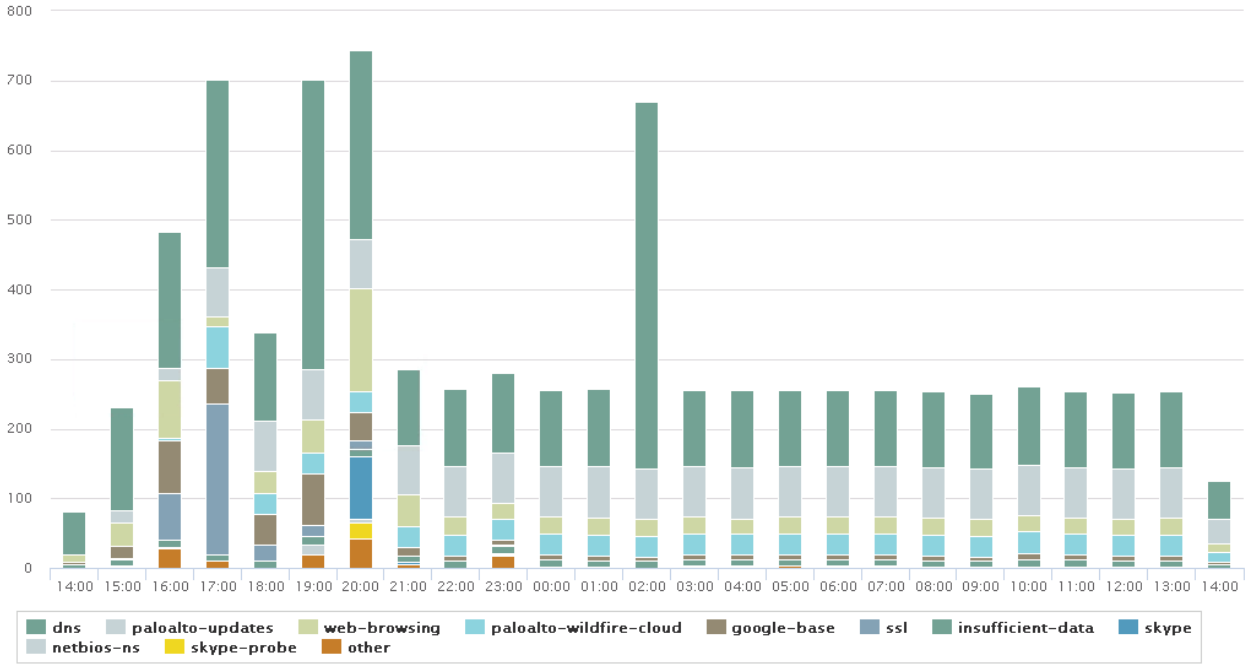


10. Click **Malaysia**:

The ACC opens with a global filter referencing Malaysia (MY):



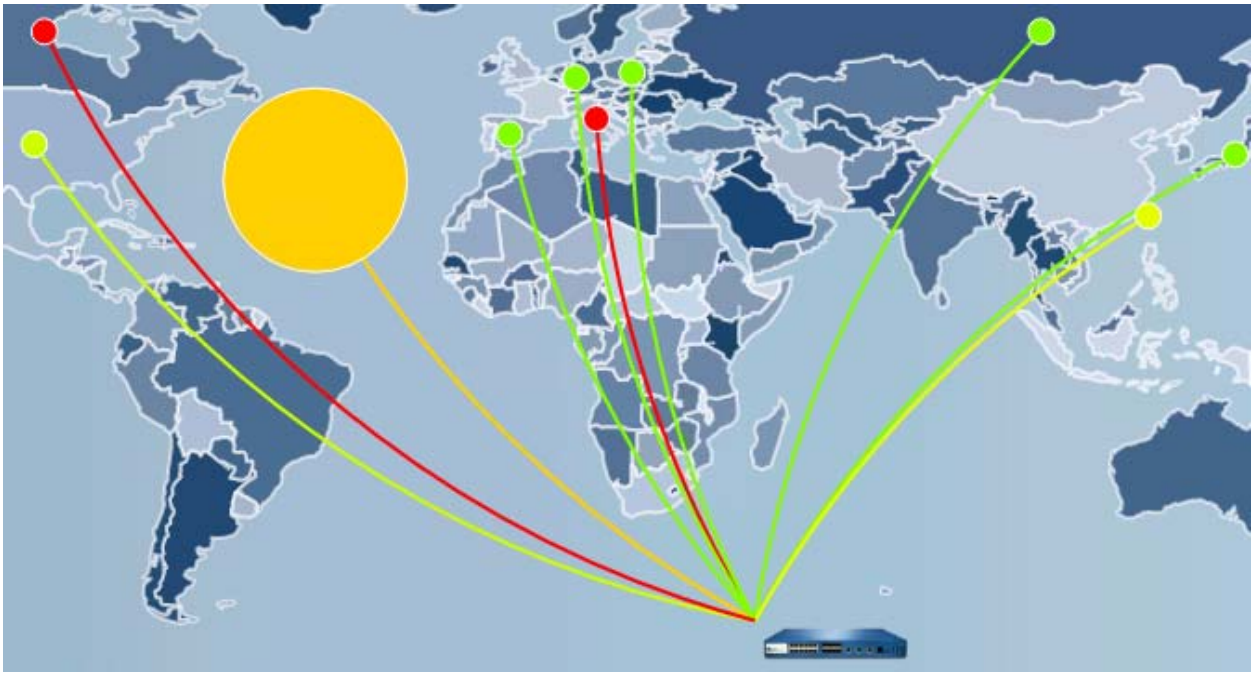
11. Click Clear all to clear the Global Filter.
12. Select **Monitor > App Scope > Network Monitor**. Network Monitor
    The Network Monitor report displays the bandwidth dedicated to different network functions over the specified period of time. Each network function is color-coded, as indicated in the legend below the chart. For example, the following diagram shows application bandwidth for the past six hours based on session information.
13. Click the  icon to display the information by Session Count and not Bytes:



Note: As is standard in all App-Scope graph items, you can click an application color, which switches your view in the WebUI to the ACC tab.

14. Select **Monitor > App Scope > Traffic Map**. Traffic Map

The Traffic Map report shows a geographical view of traffic flows according to sessions or flows:

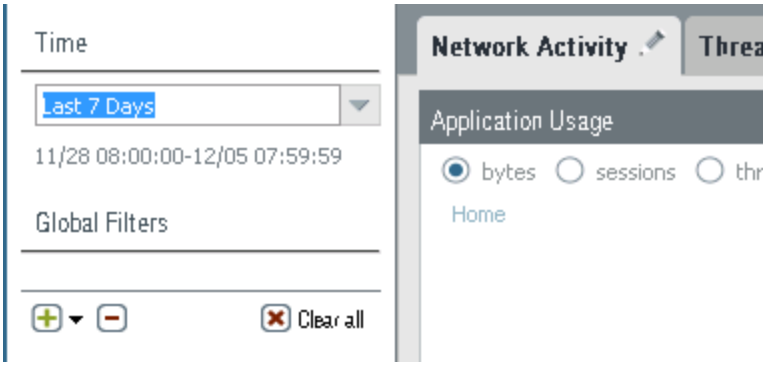


12.4 Explore the ACC

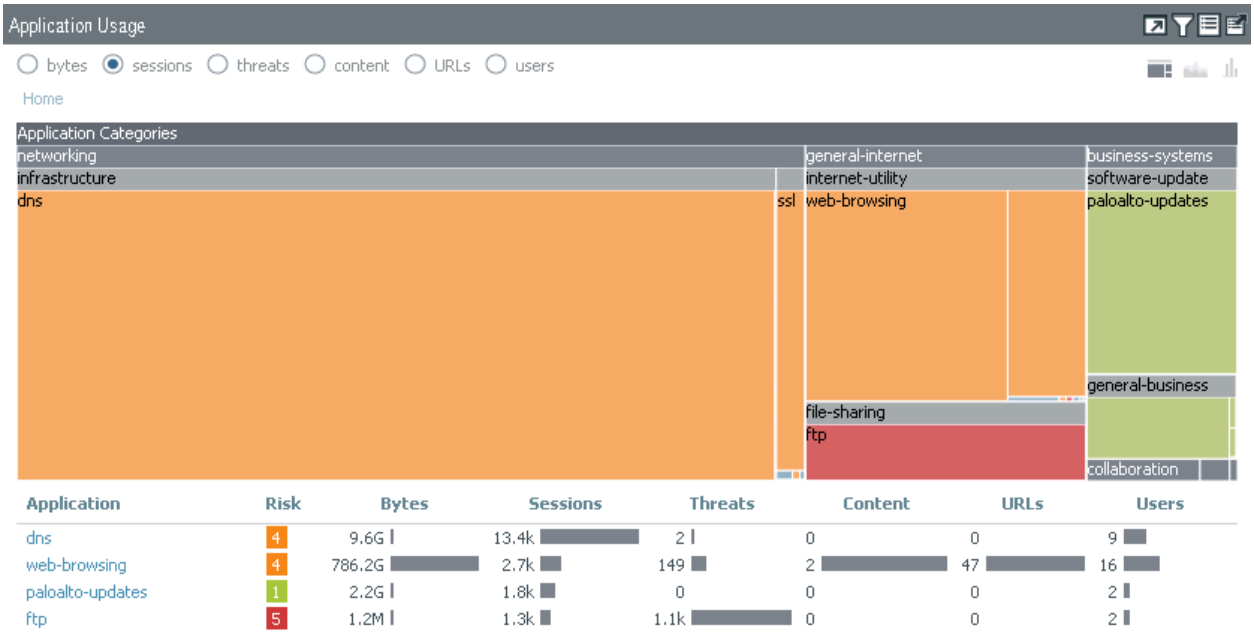
The ACC is an analytical tool that provides actionable intelligence about the activity within your network. The ACC uses the firewall logs to graphically depict traffic trends on your network.

1. Click the **ACC** tab. 

2. Click the **Time** drop-down list and select **Last 7 Days**:



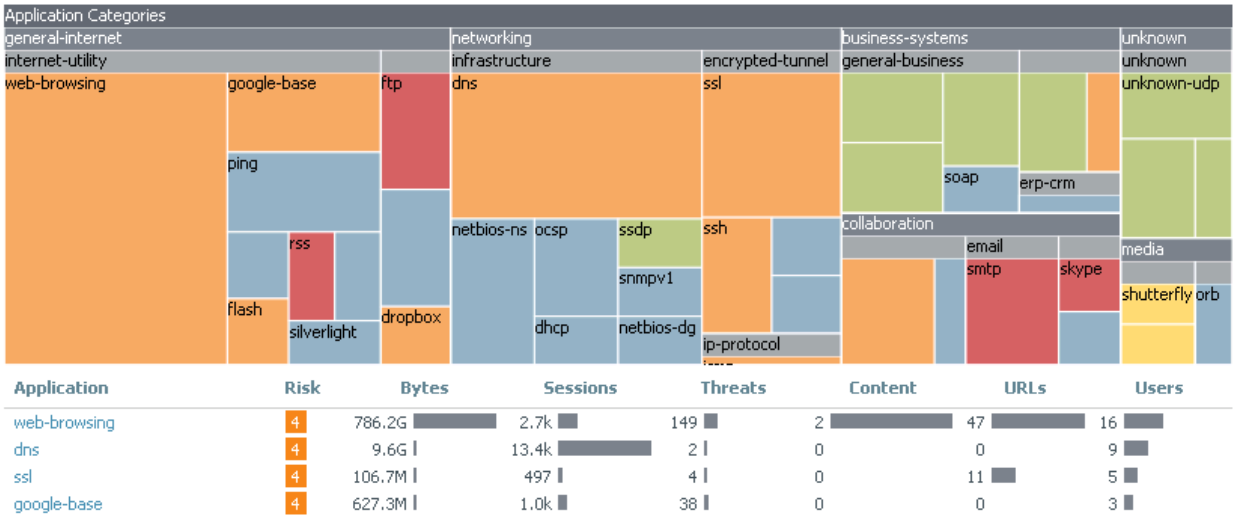
3. Explore the information available on the **Network Activity** tab. This tab displays an overview of traffic and user activity on your network. It focuses on the top applications being used; the top users who generate traffic with detailed information about the bytes, content, threats, or URLs accessed by the user; and the most used security rules against which traffic matches occur.



Notice that in every pane you can display data by bytes, sessions, threats, content, URLs, and users:

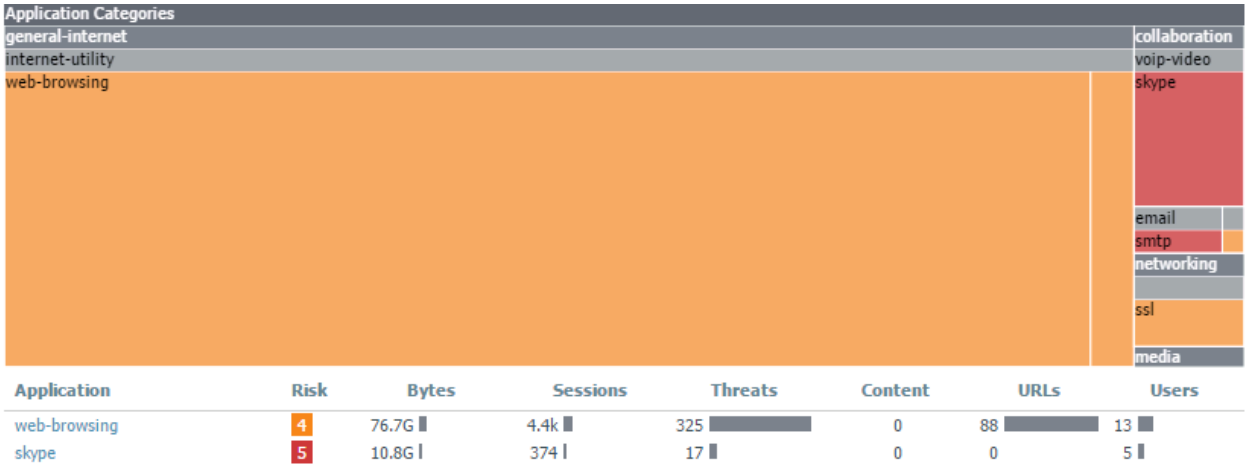
4. Select the **users** option.

Notice how the application use seems more consistent across all colors versus bytes:



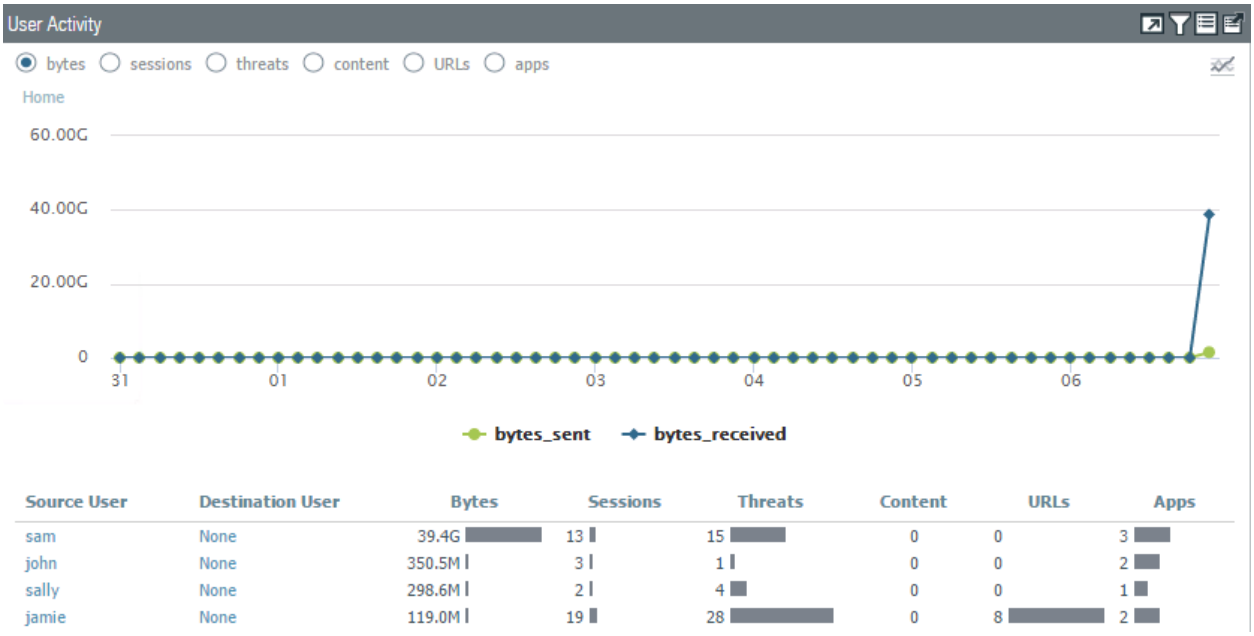
This information indicates that one application does not supersede any other application in overall use by users.

5. Select **threats** in the Application Usage pane:



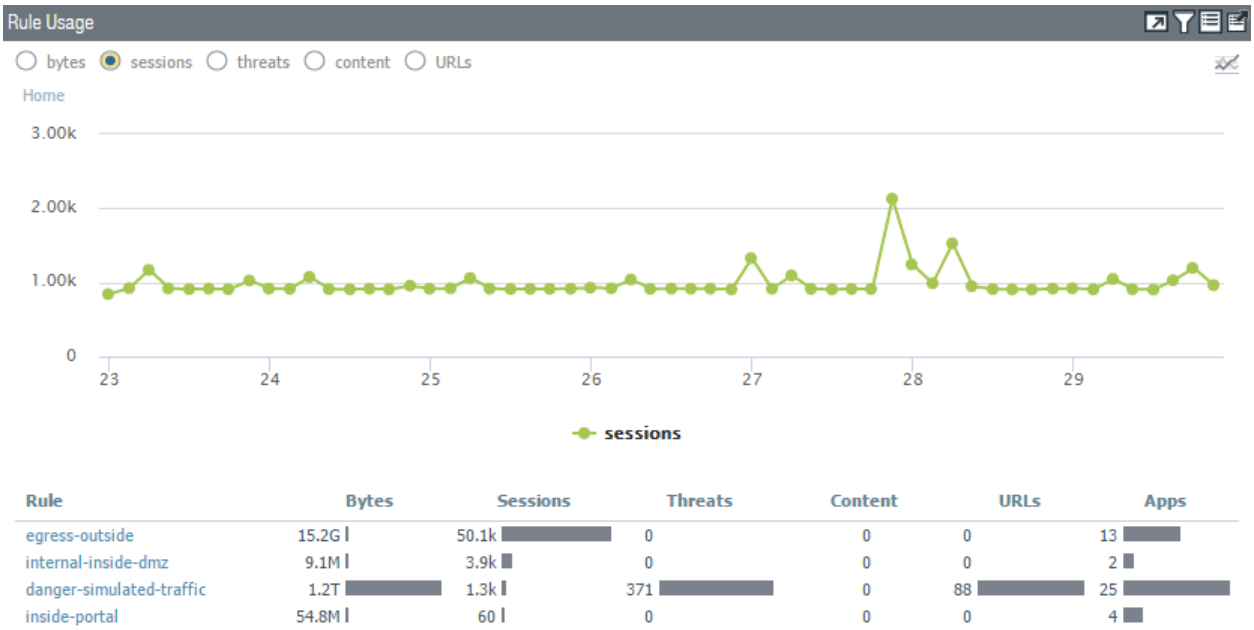
Given the displayed information you can see that web-browsing is the primary source of threats in this environment.

6. Focus your attention on the **User Activity** pane. Which user consumed the most bandwidth in the past seven days?



From the graph in the example, you can see that Jamie has consumed the most bandwidth. Your user might be different.

7. Focus your attention on the bottom-right **Rule Usage** pane.
8. Select **sessions**. Which Security policy rule has been used the most?

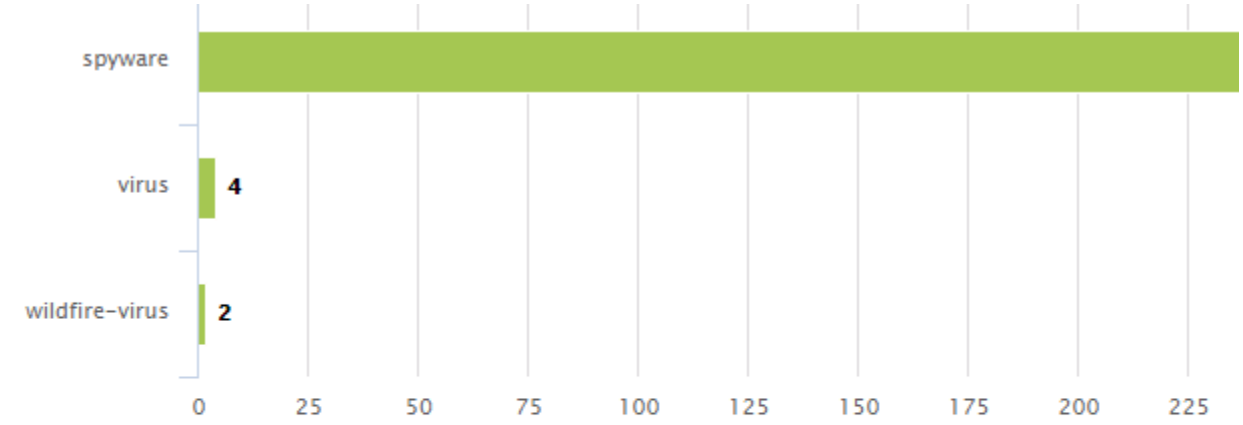


Rule	Bytes	Sessions	Threats	Content	URLs	Apps
egress-outside	15.2G	50.1k	0	0	0	13
internal-inside-dmz	9.1M	3.9k	0	0	0	2
danger-simulated-traffic	1.2T	1.3k	371	0	88	25
inside-portal	54.8M	60	0	0	0	4

From the displayed information, you can see that the most active rule based on session count is egress-outside.

9. Click the **Threat Activity** tab:

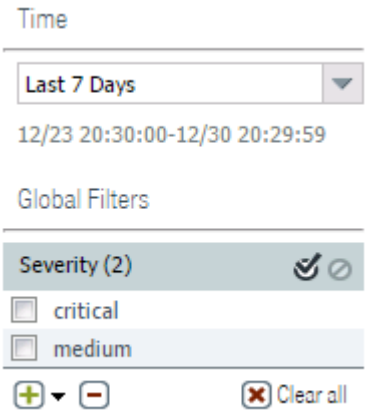
This tab displays an overview of the threats on the network. It focuses on the top threats: vulnerabilities, spyware, viruses, hosts visiting malicious domains or URLs, top WildFire submissions by file type and application, and applications that use non-standard ports:



Threat Name	ID	Severity	Threat Type
Suspicious HTTP Evasion Found	14984	informational	spyware
Suspicious TLS Evasion Found	14978	informational	spyware
Virus/Win32.generic.jqxdj	41110866	medium	virus
Bredolab.Gen Command and Control Traffic	13024	critical	spyware
Ransom/Win32.locky.fo	122670184	medium	wildfire-virus
Trojan/Win32.swrort.dfap	124503378	medium	wildfire-virus

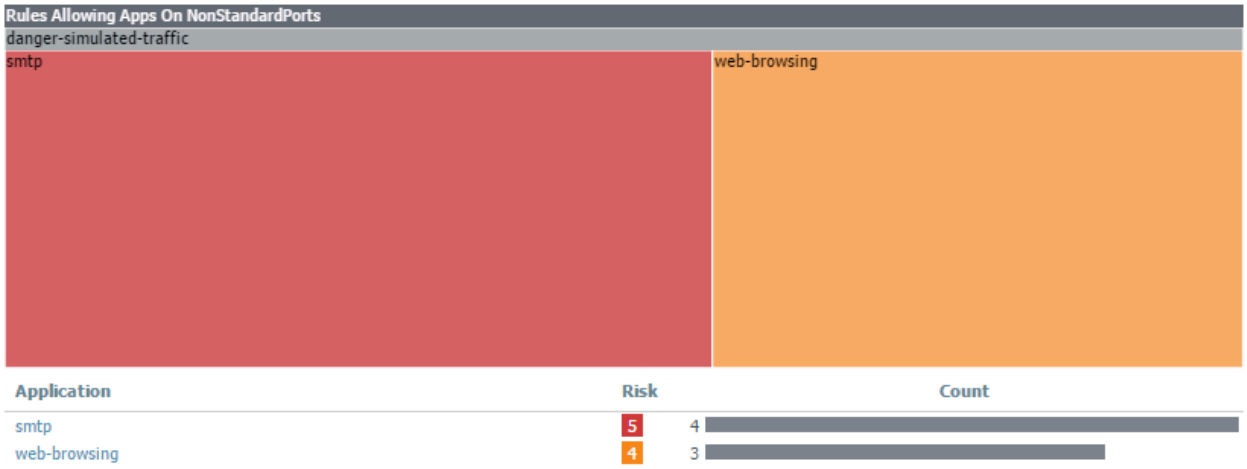
Notice that there are informational entries that might not be useful.

10. Create a global filter for only medium and critical severities:



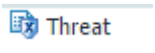
Notice that the graph updates to display only critical and medium severities.

11. Scroll down to the bottom-right and notice the **Rules Allowing Apps On Non Standard Ports** pane.

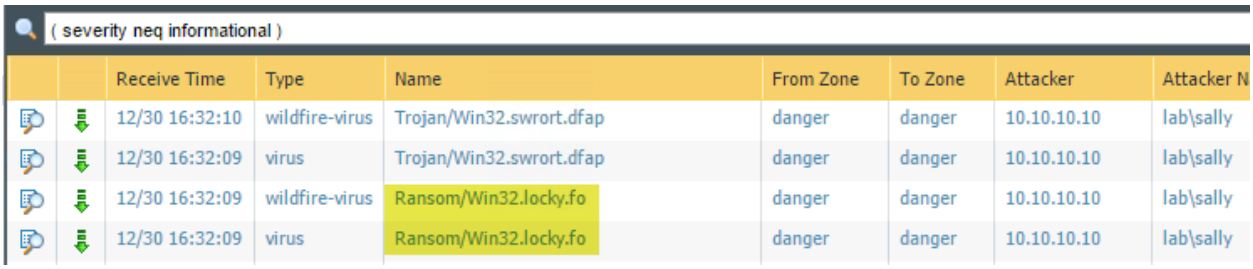


This pane is good for identifying rules that need to enforce the application-default service setting.

12.5 Investigate Traffic

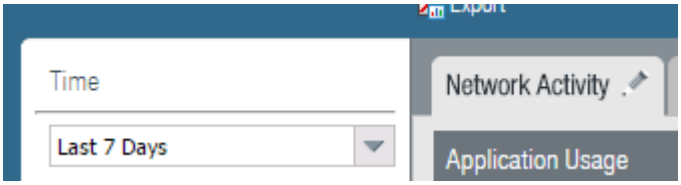
1. In the WebUI select **Monitor > Logs > Threat**. 

2. Type the filter `(severity neq informational )` into the log filter text box and press **Enter.**
3. Locate the first entry referencing **locky** and notice that the user sally is associated with it:

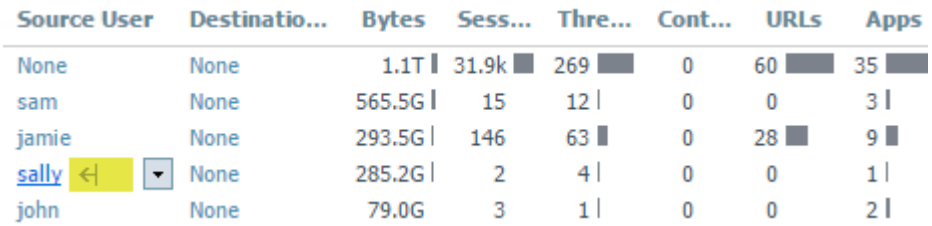


4. Click the **ACC** tab. 

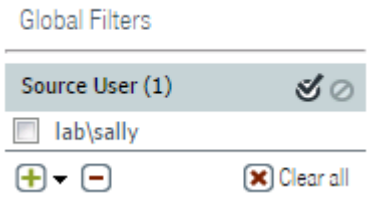
5. Ensure that the **Time** drop-down list is **Last 7 Days** and the **Network Activity** tab is selected:



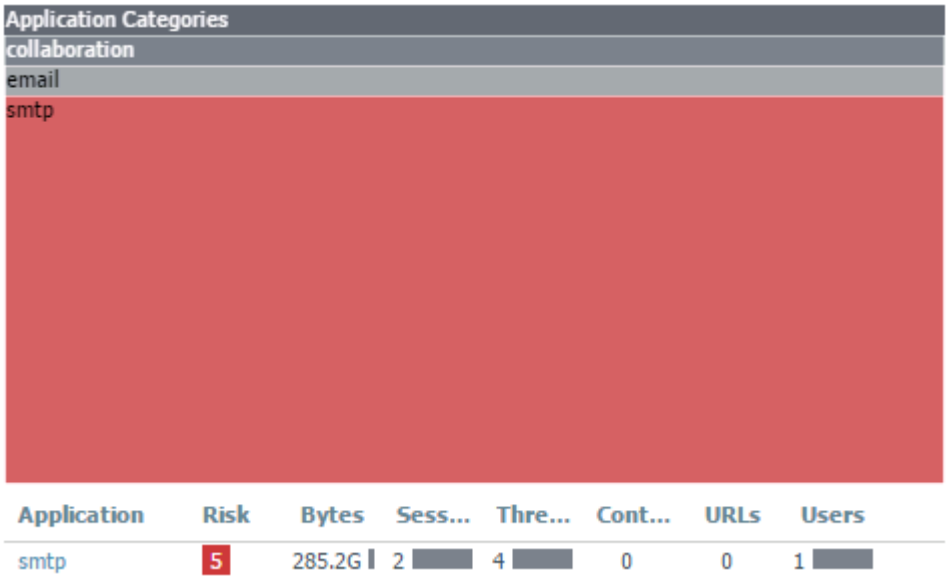
6. Move to the **User Activity** pane.
7. Use the left-arrow to promote **sally** to a Global Filter:



8. Ensure that sally was promoted to a Global Filter:

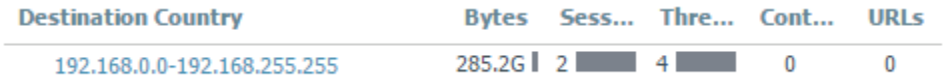


Notice that all window panes have updated to show only information based on *sally*:



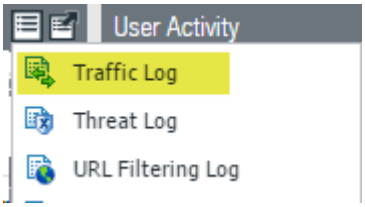
From the displayed information, you can see that sally is associated only with smtp traffic, which could indicate a possible infection and lateral movement.

9. Scroll down and locate the **Destination Regions** pane.
   Notice that this is an internal network, which could indicate that sally is using corporate e-mail and not an external source or that there might be a rogue SMTP relay.



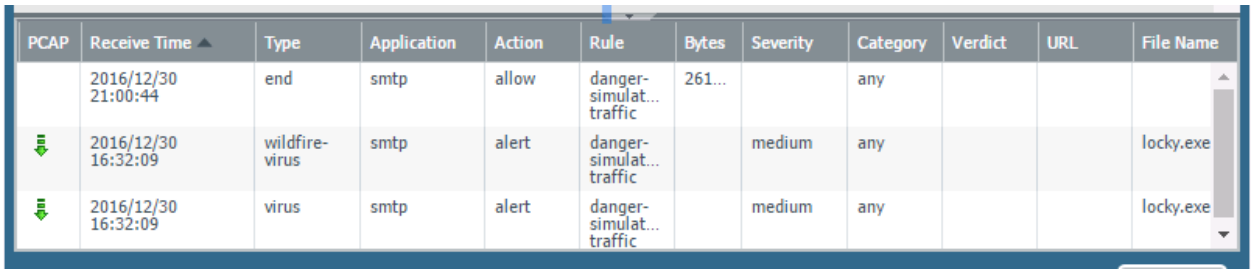
10. Scroll down to the **Rule Usage** pane. Notice that only one rule allowed this traffic. If this were a production environment, inspection should be done to ensure that this rule is operating effectively. For example, should the rule allow SMTP? If not, is this a rogue SMTP relay?

11. Scroll to the top-left **Application Usage** pane.
12. Click the  icon and select **Traffic Log**:



Notice that the WebUI switched views to the Traffic log with a predefined filter.

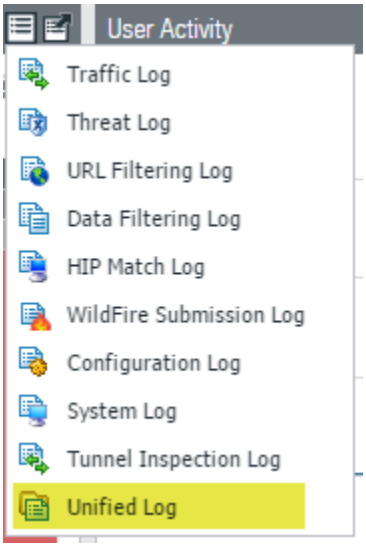
13. Select the  icon. Notice at the bottom you can see the associated threat entries:



PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	Verdict	URL	File Name
	2016/12/30 21:00:44	end	smtp	allow	danger-simulat... traffic	261...		any			
	2016/12/30 16:32:09	wildfire-virus	smtp	alert	danger-simulat... traffic		medium	any			locky.exe
	2016/12/30 16:32:09	virus	smtp	alert	danger-simulat... traffic		medium	any			locky.exe

14. Click the **ACC** tab. 

15. Click the **Jump to Logs** icon and select the **Unified Log**:



Notice that you now see both Traffic and Threat logs in one unified display, which can help with correlation.

12.6 User Activity Report

The firewall can generate reports that summarize the activity of individual users or user groups.

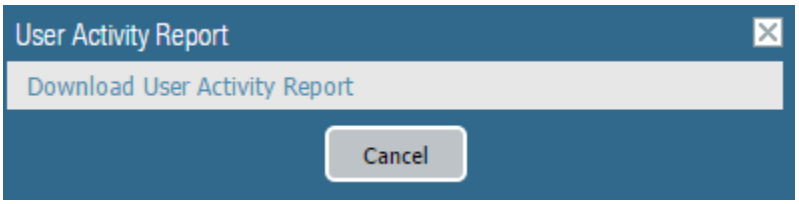
1. Select **Monitor > PDF Reports > User Activity Report**. 

2. Click 

to define a new user activity report:

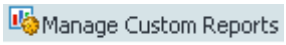
Parameter	Value#
Name	`mark#`
Type	**User**
Username / IP Address	`lab\mark`
Time Period	**Last 7 days**

3. Click **Run Now**.
4. Download and open the report when it finishes:

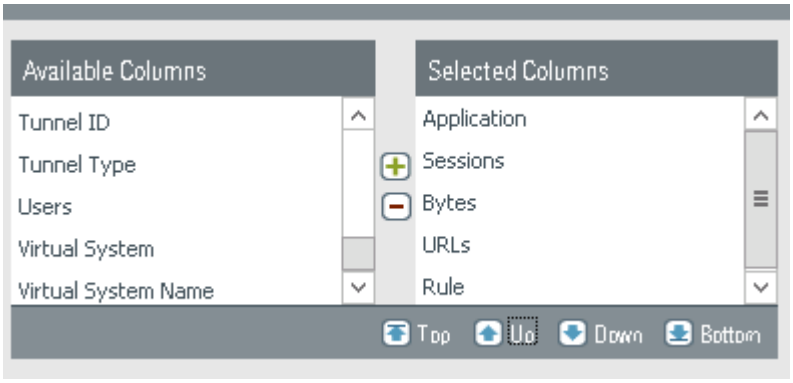


5. Browse through the report to get familiar with the presented information. You can also include detailed browsing history that will include an approximate time a user spends on a website (not available when specifying a group).

12.7 Create a Custom Report

1. Select **Monitor > Manage Custom Reports**. 

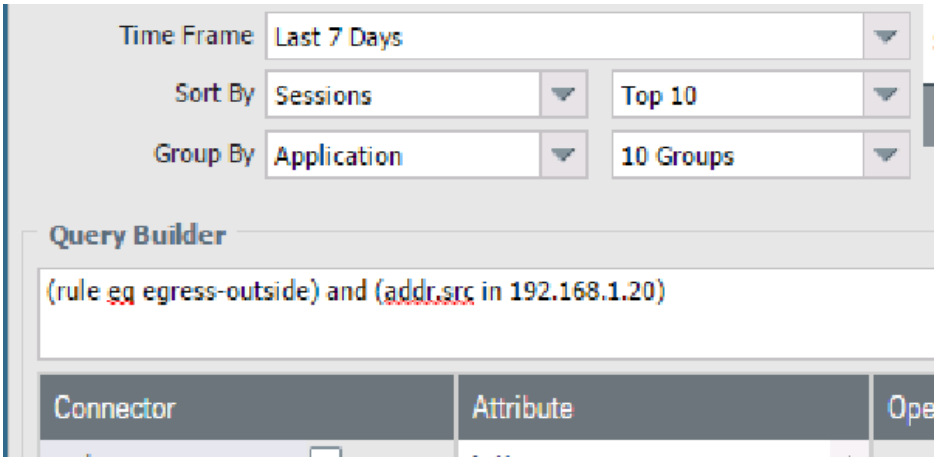
2. Click  to define a new custom report:

Parameter	Value#
Name	`top-applications#`
Database	Select **Summary Databases > Traffic**
Time Frame	**Last 7 Days**
Sort By	**Sessions** and **Top 10**
Group By	**Application** and **10 Groups**
Selected Columns	

3. Click **OK** to save the Custom Report window.
4. Click the **top-applications** report to reopen the Custom Report window.
5. Click **Run Now** to generate the report. The report will appear in a new tab in the browser window:

	Application	Rule	Sessions	Bytes	URLs
1	dns	egress-outside	26.6k	11.2M	0
2		danger-simulated-traffic	111	26.9G	0
3	paloalto-updates	egress-outside	12.1k	15.0G	0
4	paloalto-wildfire-cloud	egress-outside	10.0k	139.6M	0
5	web-browsing	internal-inside-dmz	3.9k	4.0M	0
6		danger-simulated-traffic	424	704.5G	88
7		egress-outside	34	29.4k	0

6. Close the **top-applications** tab containing the report.
7. On the **Report Setting** tab, create the following query using the Query Builder: `(rule eq egress-outside) and (addr.src in 192.168.1.20)`



8. Click **Run Now** to run the report again, this time with the query:

Custom Report

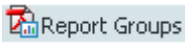
Report Setting | top applications (100%)

	Application	Rule	Sessions	Bytes
1	dns	egress-outside	1.6k	373.1k
2	google-base	egress-outside	1.2k	26.6M
3	web-browsing	egress-outside	225	11.4M
4	ssl	egress-outside	217	4.4M
5	windows-azure-base	egress-outside	126	1.5M
6	ms-update	egress-outside	19	22.6k

9. Click 

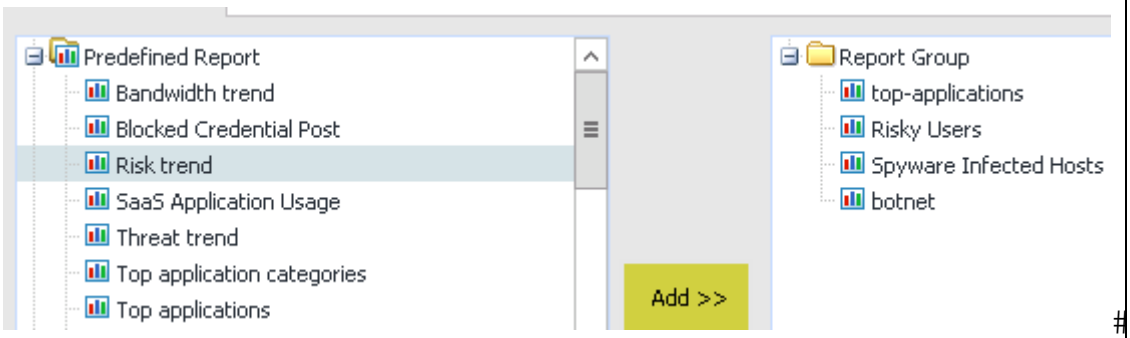
to save the report as a PDF. (You might need to disable your browser's popup blocker.)
10. Click **OK** to close the Custom Report window.

12.8 Create a Report Group

1. In the WebUI select **Monitor > PDF Reports > Report Groups**. 

2. Click 

to define a new Report Group:

Parameter	Value#
Name	`lab-report-group#`
Reports	

3. Click **OK**.

12.9 Schedule Report Group Email

1. In the WebUI select **Monitor > PDF Reports > Email Scheduler**. 

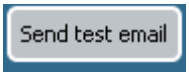
2. Click 

to define a new email schedule:

Parameter	Value#
Name	`lab-email-schedule#`
Report Group	**lab-report-group**
Recurrence	**Daily**
Email Profile	Select **New Email Profile** 

3. The Email Server Profile window is now displayed. Configure the following:

Parameter	Value#
Name	lab-smtp#
Email Display Name	PANW EDU Admin
From	edu-lab-admin@paloaltonetworks.com
To	<your e-mail address>
Email Gateway	192.168.1.20

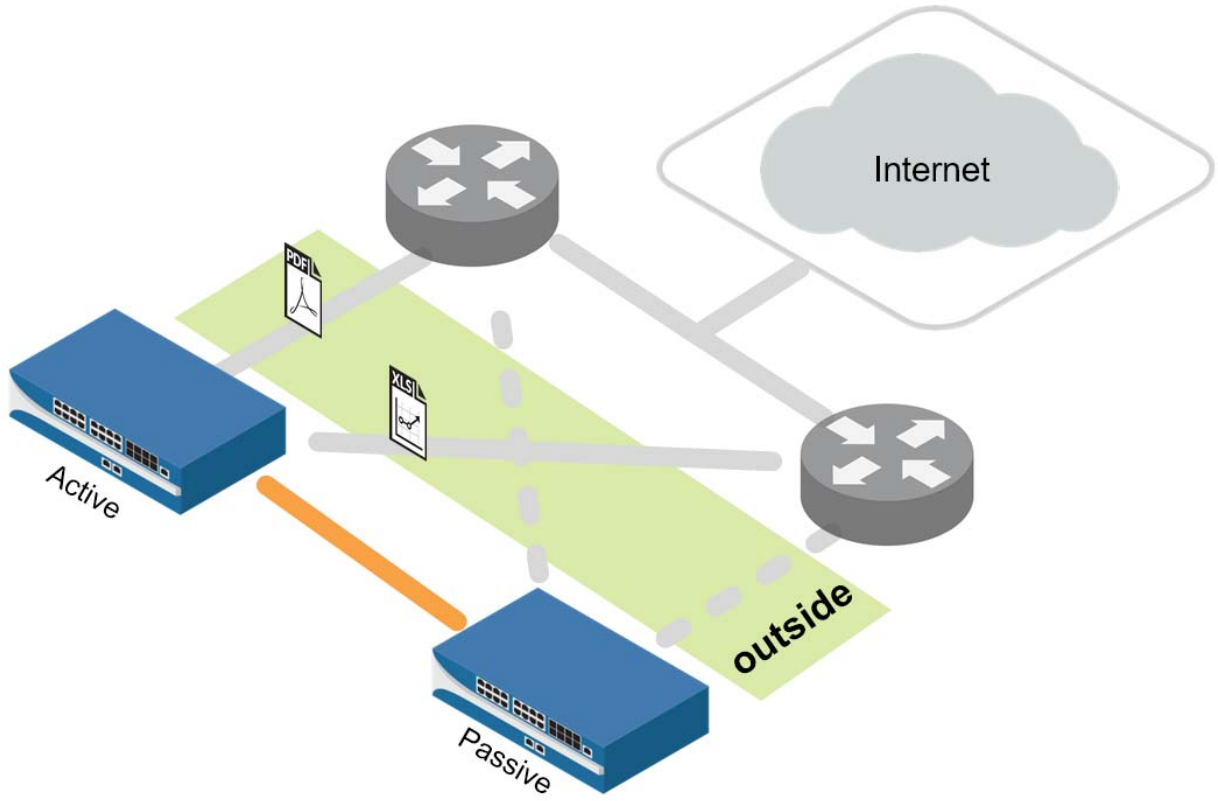
4. Click **OK** twice to close the Email Server Profile and Email Scheduler windows.
5. Click 

. A test email will be sent to the address you provided. Wait for and confirm its arrival.
   Note: Check your SPAM folder.
6. Click **OK** twice.

Stop. This is the end of the Monitoring and Reporting lab.

13. Lab: Active/Passive High Availability

This is a configuration lab only.

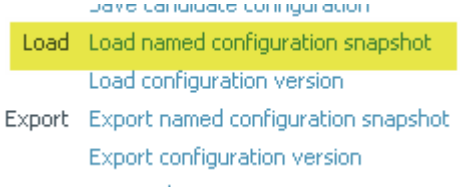


Lab Objectives

- Display the Dashboard HA widget.
- Configure a dedicated HA interface.
- Configure active/passive HA.
- Configure HA monitoring.
- Observe the HA widget.

13.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:

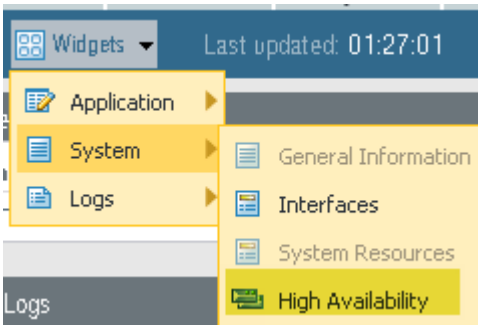


3. Select **edu-210-lab-13** and click **OK**.
4. Click **Close**.
5. Commit all changes.

13.1 Display the HA Widget

If high availability (HA) is enabled, the High Availability widget on the Dashboard indicates the HA status.

1. In the WebUI click the **Dashboard** tab to display current firewall information.
2. If the High Availability panel is not displayed, select **Widgets > System > High Availability** to enable the display:

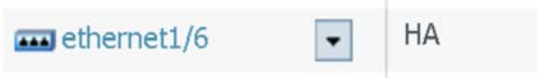


The High Availability Widget now displays on the Dashboard:

13.2 Configure the HA Interface

Each HA interface has a specific function: One interface is for configuration synchronization and heartbeats, and the other interface is for state synchronization (not configured in this lab).

1. In the WebUI select **Network > Interfaces > Ethernet**.
2. Click **ethernet1/6** to open the configuration window for that interface.
3. Select **HA** on the Interface Type drop-down list and click **OK**:



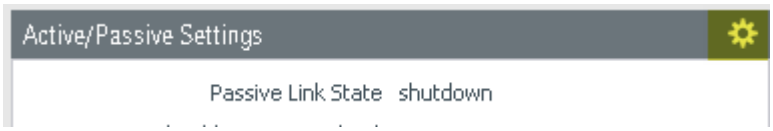
13.3 Configure Active/Passive HA

In this deployment, the active firewall continuously synchronizes its configuration and session information with the passive firewall over two dedicated interfaces. In the event of a hardware or software disruption on the active firewall, the passive firewall becomes active automatically without loss of service. Active/passive HA deployments are supported by the interface modes Virtual Wire, Layer 2, and Layer 3.

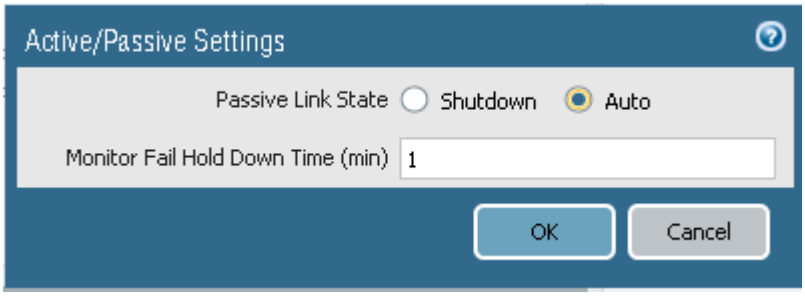
1. In the WebUI select **Device > High Availability > General**.
2. Click the  icon of the Setup panel to open the Setup configuration window.
3. Configure the following:

Parameter	Value#
Enable HA	
Group ID	**60** (This field is required, and must be unique, if multiple HA pairs reside on the same broadcast domain.)
Mode	**Active Passive**
Enable Config Sync	 (Select this option to enable synchronization of configuration settings between the peers.)
Peer HA1 IP Address	`172.16.3.11`

4. Click **OK** to close the Setup configuration window.
5. Click the  icon of the Active/Passive Settings panel:



6. Select the **Auto** radio button. When Auto is selected, the links that have physical connectivity remain physically up but in a disabled state. They do not participate in ARP or packet forwarding. This configuration helps reduce convergence times during failover because no time is required to activate the links. To avoid network loops, do not select this option if the firewall has any Layer 2 interfaces configured.



7. Click **OK** to close the Active/Passive Settings configuration window.
8. Click the  icon of the Election Settings panel to configure failover behavior:

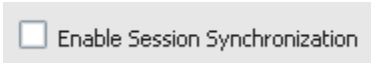
Parameter	Value#
Device Priority	`80` Enter a priority value (range is 0–255) to identify the active firewall. The firewall with the lower value (higher priority)

Parameter	Value#
	becomes the active firewall when the preemptive capability is enabled on both firewalls in the pair.)
Preemptive	Preemptive # Enables the higher priority firewall to resume active operation after recovering from a failure. This parameter must be enabled on both firewalls but is not always a recommended practice.#
Heartbeat Backup	Heartbeat Backup # Uses the management ports on the HA firewalls to provide a backup path for heartbeat and hello messages#

9. Click **OK** to close the Election Settings configuration window.
10. Click the  icon of the Control Link (HA1) panel to configure the HA1 link. The firewalls in an HA pair use HA links to synchronize data and maintain state information:

Parameter	Value#
Port	**ethernet1/6**
IP address	`172.16.3.10`
Netmask	`255.255.255.0`

11. Click **OK** to close the Control Link (HA1) configuration window.
12. Click the  icon of the Data Link (HA2) configuration window.
13. Deselect the **Enable Session Synchronization** check box:

14. Click **OK** to close the Data Link (HA2) configuration window.

13.4 Configure HA Monitoring

1. In the WebUI select **Device > High Availability > Link and Path Monitoring**.
2. Click the  icon of the Link Monitoring panel to configure link failure detection. Link monitoring enables failover to be triggered when a physical link or group of physical links fails.

Parameter	Value#
Enabled	Enabled #
Failure Condition	**Any**

3. Click **OK** to close the Link Monitoring configuration window.
4. Click Add in the Link Group panel to configure the traffic links to monitor:

Parameter	Value#
Name	`traffic-links`
Enabled	Enabled #
Failure Condition	**Any**
Interface	**ethernet1/1** **ethernet1/2**

5. Click **OK** to close the Link Group configuration window.
6. Click the icon of the Path Monitoring panel to configure the Path Failure detection. Path monitoring enables the firewall to monitor specified destination IP addresses by sending ICMP ping messages to ensure that they are responsive.

Parameter	Value#
Enabled	Enabled
Failure Condition	**Any**

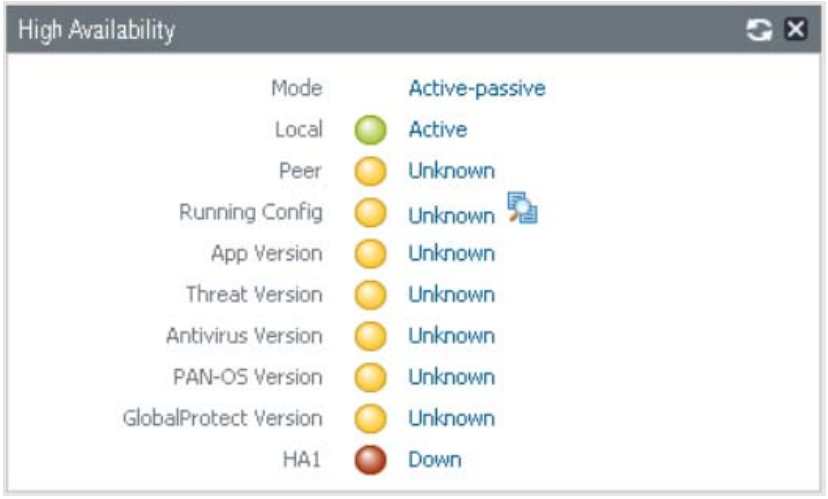
7. Click **OK** to close the Path Monitoring configuration window.
8. Find the Path Group panel and click **Add Virtual Router Path** to configure the path failure condition:

Parameter	Value#
Name	`lab-vr`
Enabled	Enabled #
Failure Condition	**Any**
Destination IP	`8.8.8.8`

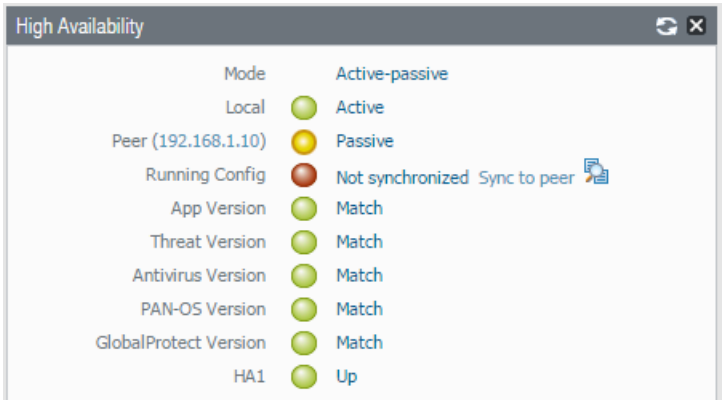
9. Click **OK** to close the HA Path Group Virtual Router configuration window.
10. Commit all changes.

13.5 Observe the HA Widget

1. In the WebUI click the **Dashboard** tab and view the High Availability status widget for the firewall. Active-passive mode should be enabled and the local firewall should be active (green). However, because there is no peer firewall, the status of most monitored items is unknown (yellow). Because HA1 has no peer, its state is down (red):



2. If a peer was configured and was operating in passive mode, the High Availability widget on the Dashboard would appear as follows. In order to avoid overwriting the wrong firewall configuration, the firewalls are not automatically synchronized. You must manually synchronize a firewall to the firewall with the "valid" configuration by clicking **Sync to peer**.



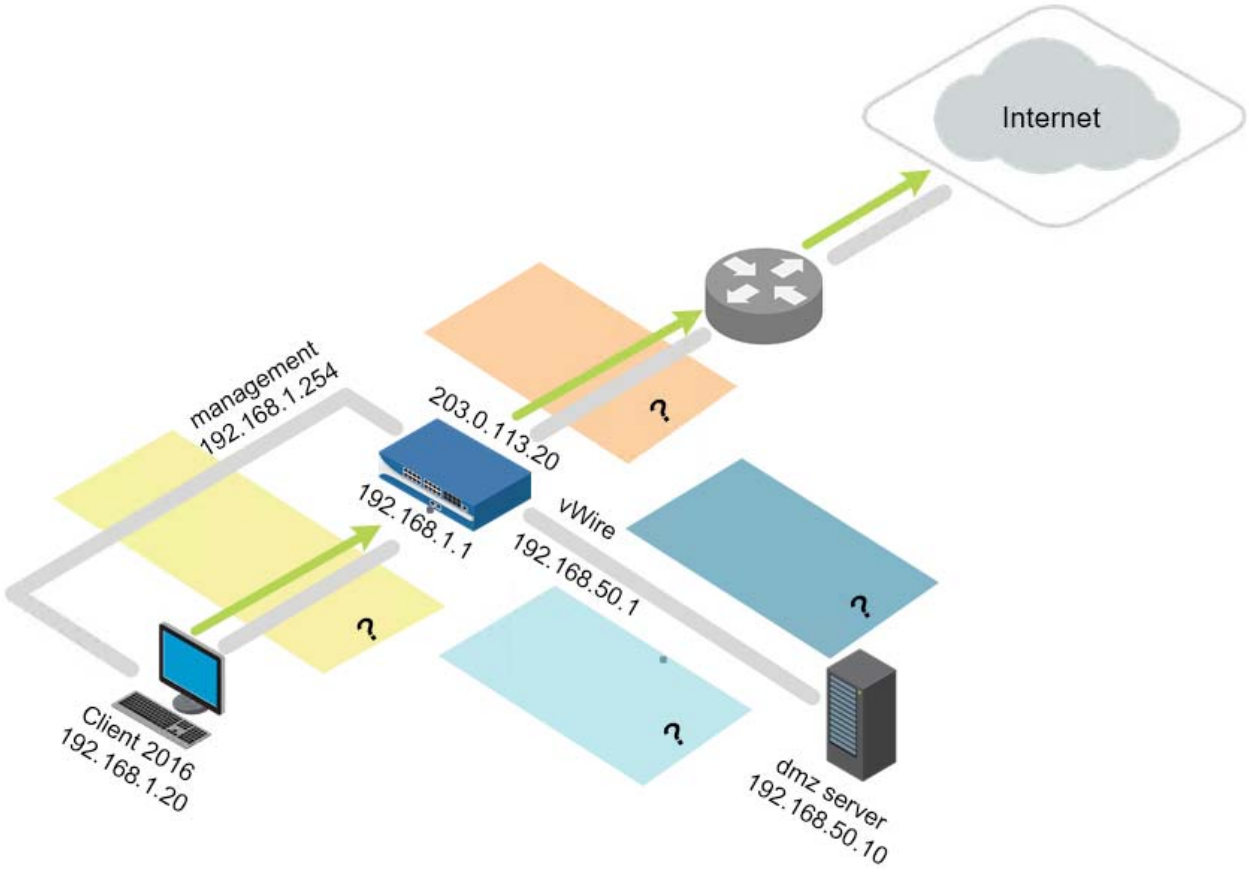
Stop. This is the end of the Active/Passive High Availability lab.

14. Lab: Capstone

This comprehensive lab is meant to provide you with additional hands-on firewall experience and to enable you to test your new knowledge and skills. You can to refer to your student guide and previous lab exercises.

In this scenario you are a network administrator and recently received a new Palo Alto Networks VM-Series firewall. The firewall's management IP address is 192.168.1.254. You can log in with the default username and password. You also have been given permission to use your own naming conventions for firewall objects such as Security zones, Security Profiles, Address Groups, and Tags.

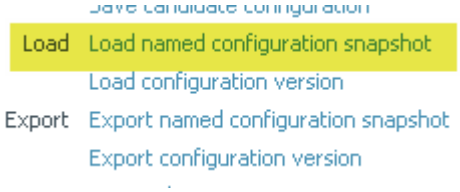
You are being asked to meet multiple configuration objectives. These objectives are listed in the lab exercise sections that follow.



14.0 Load Lab Configuration

Reset your lab environment before you begin to work through the scenario.

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-14** and click **OK**.
4. Click **Close**.
5. Commit all changes.

14.1 Configure Interfaces and Zones

Complete the following objectives:

- Configure three firewall interfaces using the following values:
  - Ethernet 1/1: 203.0.113.20/24 - Layer 3: Public network facing interface
  - Ethernet 1/2: 192.168.1.1/24 - Layer 3: Internal network facing interface
  - Ethernet 1/3: 192.168.50.1/24 – Layer 3: DMX network facing interface
- Create Security zones for each network area of interest: DMZ, internal, and public. You can name these zones whatever you like.
- Create a virtual router for all configured firewall interfaces.
- Create and assign an Interface Management Profile that enables 192.168.1.1 to respond to ping requests.
- Create and assign unique tags to important zones.

You can consider this objective complete when the following tests are successful:

- Your internal host can ping 192.168.1.1
- From the firewall CLI the following commands are successful:
  - `ping source 203.0.113.20 host 203.0.113.1`
  - `ping source 203.0.113.20 host 8.8.8.8`
  - `ping source 192.168.1.1 host 192.168.1.10`
  - `ping source 192.168.50.1 host 192.168.50.10`

14.2 Configure Security and NAT Policy Rules

Create or modify the Security and NAT policy rules to address the following objectives:
Note: *Optional tags can be helpful for identifying important rules.*

- IP addresses 192.168.1.1 and 192.168.1.254 require access to the internet.
- A separate Security policy rule is required that allows the 192.168.1.0/24 network to access the internet.
- Only the DMZ host 192.168.50.10 requires access to the internet.
- Facebook, Twitter, and Reddit applications must be blocked for users on the 192.168.1.0/24 network.

- The URL categories web-advertisements, phishing, malware, and unknown must be blocked by a Security policy rule match criterion.
- Internal hosts 192.168.1.20 and 192.168.1.254 need to access the DMZ host for the following applications: SSH, SSL, web-browsing, FTP, and ping. Access must be limited to the applications' default ports.
- Traffic matching the interzone default Security policy rule must log all traffic at session end.

You can consider this objective complete when the following tests are successful:

- The internal host can ping 8.8.8.8 and google.com.
- The internal host cannot access twitter.com, youtube.com, reddit.com, and 2600.org.
- The internal host can access http://192.168.50.10/block-list.txt.
- The internal host can use FTP to access the DMZ host at 192.168.50.10 using the login name `lab-user` and the password `paloalto`.
- The internal host can use SSH to access the DMZ host at 192.168.1.20 using the login name `lab-user` and the password `paloalto`.
- The DMZ host can ping 8.8.8.8 and google.com.

14.3 Create and Apply Security Profiles

Create Security Profile Groups and apply them to the applicable Security policy rules to meet the following objectives:

- A three-tiered URL filtering scheme is required:
  - Tier 1: Allow access to only URL categories government, financial-services, reference-and-research, and search-engines
  - Tier 2: Allow access to only the URL category online-storage-and-backup
  - Tier 3: Allow access to all URL categories
- The Tier 3 URL filtering must apply to the internal host.
- The Tier 2 URL filtering must apply to the DMZ host.
- The Tier 1 URL filtering must apply to the network 192.168.1.0/24.
- **Note:** The Security policy rule specifically matching 192.168.1.20 must be evaluated before the entire network segment.
- The Facebook, Twitter, YouTube, and Reddit applications must be blocked for everyone.
- All Security policy rules allowing internet access must leverage Antivirus, Anti-Spyware, and Vulnerability Protection Profiles.
- The firewall must reset both the client and server when a virus is detected in HTTP traffic.
- The firewall must reset both the client and server when medium-, high-, or critical-level spyware is detected.

- The Anti-Spyware Security Profile must use the DNS Sinkhole feature for Palo Alto Networks DNS Signatures and consult a custom External Dynamic List that references http://192.168.50.10/dns-sinkhole.txt.
- The dns-sinkhole.txt file must contain the domain name phproxy.org.
- The firewall must reset both the client and server when high or critical level vulnerabilities are detected.
- WildFire analysis must be enabled on all Security policy rules that allow internet access.
- The File Blocking feature must block PE file types and any multi-level-encoded files for access between the internet and the 192.168.1.0/24 network segment.

You can consider this objective complete when the following tests are successful:

- Three URL Filtering configurations have been created and applied to the appropriate Security policy rule(s).
- The DMZ host can ping box.net.
- The internal host can access box.net.
- The internal host cannot download an Eicar test virus using HTTP.
- A WildFire test file gets reported to the WildFire cloud when downloaded to the internal host.
- A DNS request to phproxy.org initiated by an `nslookup` command on the internal host results in a sinkhole event recorded in the Threat log.

14.4 GlobalProtect

Configure GlobalProtect to meet the requirements listed in the following objectives:

- User access is provided through an external gateway.
- The GlobalProtect Portal and external gateway can authenticate users using either LDAP or a local user group configured on the firewall.
- The external gateway provides an IP address pool in the range 172.16.5.200 to 172.16.5.250.
- The Tunnel interface must be assigned to a new and separate Security zone.
- A Security policy rule must allow internet access for hosts using the external gateway IP pool.
- The external gateway requires the use of IPsec.
- One or more certificates are required for the portal and external gateway.
- Create a Security policy rule to allow the internal host access to the portal and external gateway. This access might require the use of a no-NAT rule.

You can consider this objective complete when the following tests are successful:

- The internal host can successfully connect to the portal and external gateway.
- The internal host receives an IP pool address when connected to the external gateway.

- The internal host can access paloaltonetworks.com when connected to the external gateway.

Stop. This is the end of the Capstone lab.