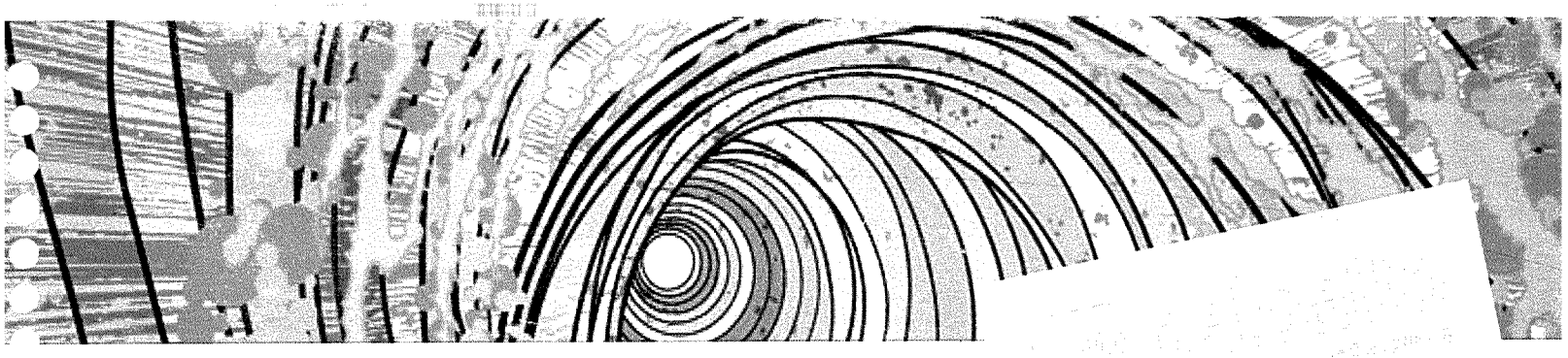


LAB GUIDE | PAN-OS® 7.1

Palo Alto Networks

Firewall 7.1

Install, Configure, and Manage

May 2016

EDU-201

Courseware Version A

education@paloaltonetworks.com

http://education.paloaltonetworks.com

Table of Contents

Typographical Conventions 7

How to Use This Lab Guide 7

Lab Guide Objectives 8

Lab Scenario: Initial Configuration 9

Lab Solution: Initial Configuration 10

- Connect to Your Student Firewall 10
- Apply a Baseline Configuration to the Firewall (Optional) 10
- Change the Default admin User Password 10
- Add an Administrator Role 11
- Add an Administrator Account 11
- Test the ip-admin User 12
- Take a Transaction Lock and Test the Lock 13
- Confirm the Update and DNS Servers 14

Lab Scenario: Basic Interface Configuration 16

Lab Solution: Basic Interface Configuration 17

- Create New Security Zones 17
- Create Interface Management Profiles 17
- Configure Ethernet Interfaces with Layer 3 Information 18
- Create a Virtual Router 19
- Configure DHCP 20
- Test Connectivity to the Trust Interface 21

Lab Scenarios: NAT and Security Policies 23

- *Scenario 1* *23*
- *Scenario 2* *23*

Lab Solution: NAT and Security Policies 25

- Create a Source NAT Policy 25
- Create the Allow All Out Policy 26
- Verify Internet Connectivity 27
- Enable the FTP Server 27
- Create a Destination NAT Policy 28
- Create a Security Policy Rule 29

Test the Connection 30
Lab Scenario: Basic App-ID 31
Lab Solution: Basic App-ID 32
Create the General Internet Policy 32
Enable Interzone Logging 33
Enable the Application Block Page 34
Verify Internet Connectivity and Application Blocking 34
Lab Scenario: Basic Content-ID 36
Lab Solution: Basic Content-ID 38
Configure a Custom URL Filtering Category 38
Configure a URL Filtering Profile 38
Configure an Antivirus Profile 39
Configure an Anti-Spyware Profile 40
Assign Profiles to a Policy 41
Test the Antivirus Profile 41
Test the URL Filtering Profile 43
Configure a Security Profile Group 44
Assign the Security Profile Group to a Policy 44
Lab Scenario: File Blocking and WildFire 46
Lab Solution: File Blocking and WildFire 47
Create a File Blocking Profile 47
Create a WildFire Analysis Profile 47
Assign the File Blocking and WildFire Profiles to the Profile Group 48
Test the File Blocking Profile 48
Test the WildFire Analysis Profile 48
Lab Scenario: Decryption 51
Lab Solution: Decryption 53
Verify Firewall Behavior Without Decryption 53
Create Two SSL Self-Signed Certificates 53
Create SSL Decryption Policies 54
Modify the Security Policy Rules 56
Test the SSL Decryption Policy 57
Test the SSL No-Decryption Policy 57

Import the CA Certificate into Windows Trusted Certificates 59
Exclude a Site from Decryption 60
Lab Scenario: Basic User-ID 62
Lab Solution: Basic User-ID 63
Enable User-ID on Trust Zone 63
Configure the LDAP Server Profile and Authentication Profile 63
Configure User-ID Group Mapping 64
Install the Software User-ID Agent 65
Configure the User-ID Agent Service 66
Configure the Software User-ID Agent 67
Configure Palo Alto Networks Firewall to Connect to User-ID Agent 68
Test User-ID 69
Lab Scenario: Site-to-Site VPN 70
Lab Solution: Site-to-Site VPN 71
Prepare for the Lab 71
Configure the Tunnel Interface 71
Configure the IKE Gateway 71
Create an IPSec Crypto Profile 72
Configure the IPsec Tunnel 73
Define the Route to the Network 73
Create a Security Policy Rule 74
Test Connectivity 75
Lab Scenario: Management and Reporting 77
Lab Solution: Management and Reporting 78
Explore the Dashboard, ACC, App Scope, and Session Browser 78
Explore the Logs 78
Create a Custom Report 78
Lab Scenario: Active/Passive High Availability 81
Lab Solution: Active/Passive High Availability 82
Lab Preparation 82
Save the Configuration 82
Display the HA Widget 82
Configure the Firewall for HA Setup 82

Configure Active/Passive HA 82
Configure HA Monitoring 84
Verify the HA Configuration 85

Typographical Conventions

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

Convention	Meaning	Example
Boldface	Names of selectable items in the web interface	Click **Security** to open the Security Rule Page
Italics	Name of Uniform Resource Locators (URLs)	The address of the Palo Alto Networks home page is *http://www.paloaltonetworks.com*.

`Courier` font	Coding examples and text that you enter	Enter the following command:
		`a:\setup`
		The `show arp all` command yields this output:
		`username@hostname> show arp all maximum of entries supported: 8192 default timeout: 1800 seconds total ARP entries in table: 0`

Click	Click the left mouse button	Click **Administrators** under the Device tab.
Right-click	Click the right mouse button	Right-click on 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 a scenario and a solution.

The scenario describes the lab exercise in terms of objectives and customer requirements.

The solution provides step-by-step instructions to solve the problem presented in the scenario.

Lab Guide Objectives

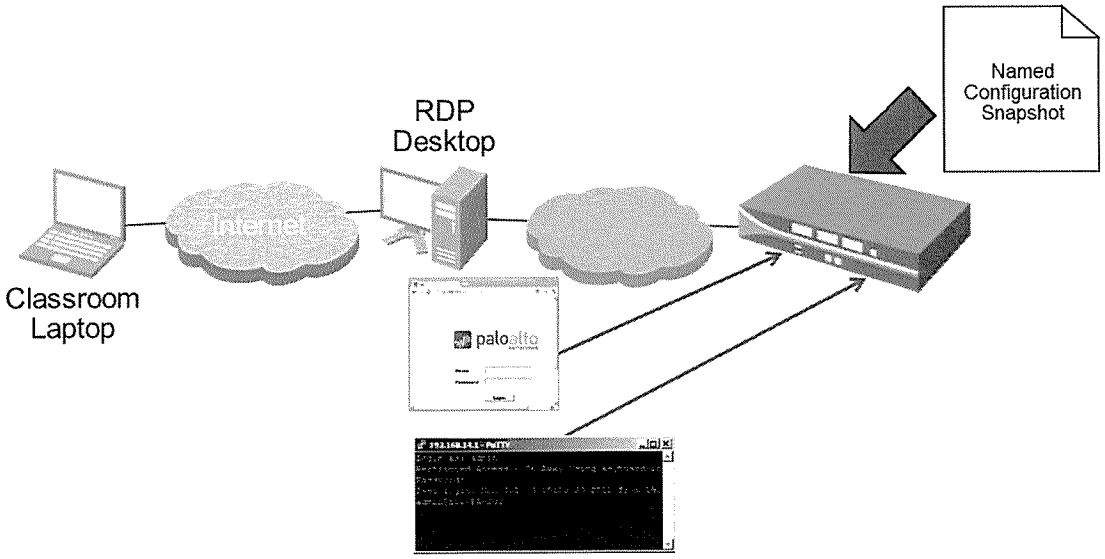
When you have finished these labs, you will be able to complete these tasks:

- Configure the basic components of the firewall, including interfaces, security zones, and security policies.
- Configure basic Layer 3 settings, such as IP addressing and a NAT policy.
- Configure basic Content-ID functionality, including antivirus protection and URL filtering.
- Configure extended firewall features, including IPSec VPNs, SSL decryption, and high availability.

Lab Scenario: Initial Configuration

In this lab, you will:

- Apply a baseline configuration to build successive labs
- Create a new admin account and test the config locks



You have been tasked with integrating a new firewall into your environment:

- Apply a saved configuration to the firewall so that it is in a known state.
- Create a new admin account.
- Create a role for a policy administrator that allows access to all firewall functionality through the WebUI, excluding the Monitor, Network, Privacy, and Device tabs. The account should have no access to the XML API or to the CLI.
- Use the newly created account and your administrator account to test the locking features of the WebUI. Verify that you cannot configure anything if the configuration is locked by the other. Be sure to remove the locks when you finish this exercise.

Lab Solution: Initial Configuration

Note: In all instructions, substitute X with your pod number. Whenever you see a parameter surrounded by <brackets>, refer to your Lab Settings Handout for the value of the specific parameter.

Connect to Your Student Firewall

1. Get your login credentials, IP information, and other information from your instructor.
2. Connect to the Windows desktop for your lab PC.
3. Launch a browser and connect to `https://<Mgt IP Address>`.
4. Log in to the Palo Alto Networks firewall with the username and password provided by your instructor.

Apply a Baseline Configuration to the Firewall (Optional)

5. Ask your instructor if this section is necessary.
6. In the Palo Alto Networks firewall WebUI, select **Device > Setup > Operations**.
7. Click **Load named configuration snapshot**.
8. Click the drop-down list next to the Name text box and select **<Named Configuration Snapshot>**, using the name of the Configuration Snapshot from your Lab Settings Handout.
9. Click **OK**. After some time, a confirmation that the configuration has been loaded appears.
10. Click **Close**.
11. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the commit process is complete, and click **Close** to continue.

Change the Default admin User Password

12. Select **Device > Administrators**.
13. Open the **admin** user account.
14. Change the password to `paloalto`.

Add an Administrator Role

15. Select **Device > Admin Roles**.

16. Click **Add** in the lower left of the panel and create a new administrator role.

Name	Enter `Policy Admins`
WebUI tab	Click these major categories to disable them: • **Monitor** • **Network** • **Device** • **Privacy** The remaining major categories (Dashboard, ACC, Policies, Objects, Validate, Commit, and Global) should remain enabled.
XML API tab	Verify that the categories are disabled.
Command Line tab	Keep the default of **None**.

17. Click **OK** to continue.

Add an Administrator Account

18. Select **Device > Administrators.**

19. Click **Add** in the lower left corner of the panel.

20. Configure a new administrator account.

Name	Enter `ip-admin`
Authentication Profile	Select **None**

Password/Confirm Password	Enter `paloalto`
Administrator Type	Select **Role Based**
Profile	Select **Policy Admins**
Password Profile	Select **None**

21. Click **OK**.

22. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the commit process is complete, and click **Close** to continue.

Test the ip-admin User

23. Open **PuTTY**.

24. Open an SSH connection to `< Mgt IP Address>`. You are prompted for a username.

25. Enter the username `admin` and the `paloalto` password. (When you type the password, it is invisible.) The role assigned to this account is allowed CLI access, so the connection should succeed.

26. Close the session, and open PuTTY again.

27. Attempt to open an SSH connection to `<Mgt IP Address>`. You are prompted for a username.

28. Enter the username `ip-admin` and the password `paloalto`. The role assigned to this account was denied CLI access, so the connection resets and PuTTY closes.

29. Open a new browser. Use a different brand of browser than the one you already have open.

30. Go to `https://<Mgt IP Address>`. A Certificate Warning appears.

31. Click through the Certificate Warning. The Palo Alto login page opens.

32. Log in to the WebUI as `ip-admin` with the password `paloalto`.

33. Explore the available functionality of the WebUI. Notice that several tabs and functions are excluded from the interface.

Take a Transaction Lock and Test the Lock

34. From the WebUI where you are logged in as ip-admin, click the **transaction lock** icon to the right of the Commit link. A Locks window opens.

35. Click **Take Lock**. A Take Lock window opens.

36. Set the Type to **Commit**, and click **OK**. The ip-admin lock is listed.

37. Click **Close** to close the Transaction Lock window.

38. Return to the WebUI where you logged in with the admin account.

39. Click the **Device > Administrators** link. The WebUI refreshes. Notice the lock in the upper right corner of the WebUI.

40. Click **Add** to add another user.

41. Configure a new administrator account:

Name	Enter `TestLock`
Authentication Profile	Select **None**
Password/Confirm Password	Enter `paloalto`
Administrator Type	Select **Role Based**
Profile	Select **Policy Admins**
Password Profile	Select **None**

42. Click **OK**. The new user is listed.

43. Click **Commit.** A Commit prompt appears.

44. Click **Commit**. An Error window opens. You are not allowed to commit the changes because of the lock set by the ip-admin user.

45. Click **Close**.

46. Click the **Lock** icon in the upper right corner. The Transaction Lock window opens.

47. Select the ip-admin lock and click **Remove Lock**.

48. Click **OK** and then **Close**. The lock is removed.

49. **Delete** the TestLock user.

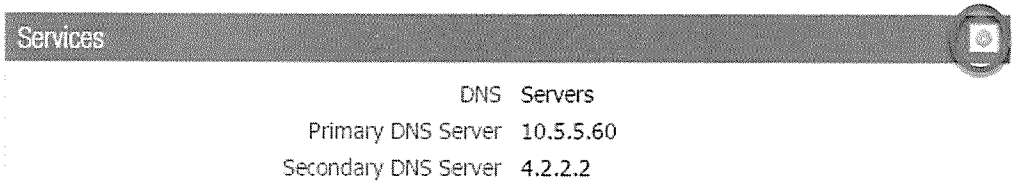
50. In the ip-admin browser, select the **logout** button on the bottom left of the WebUI.

51. Close the browser.

Confirm the Update and DNS Servers

52. Select **Device > Setup > Services**.

53. Open the **Services** panel by clicking the gear icon in the upper-right corner of the Settings panel.

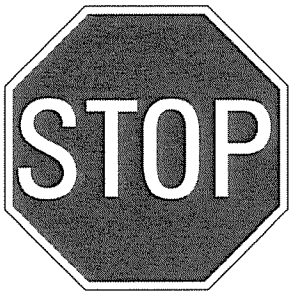


54. Confirm that `<DNS Server>` is the Primary DNS Server.

55. Confirm that `<Update Server Address>` is the Update Server.

56. Click **OK**.

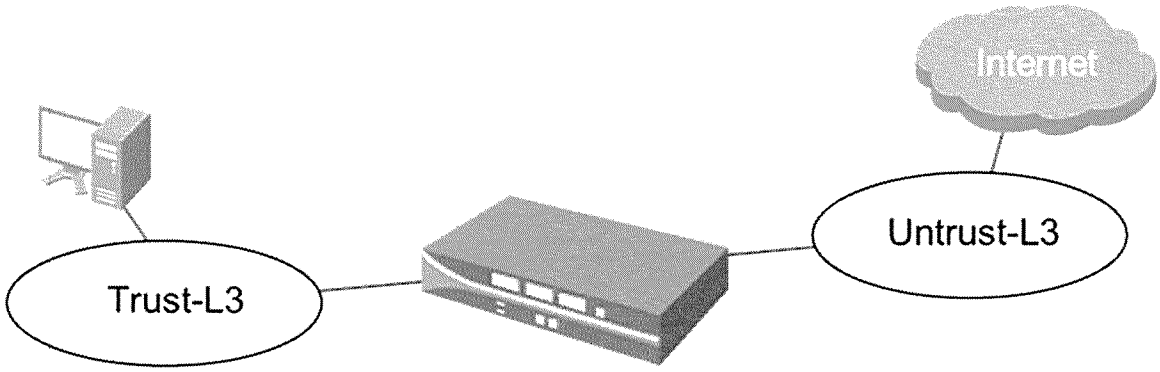
57. **Commit** your changes. You may need to reconnect to the WebUI afterward.


STOP

Lab Scenario: Basic Interface Configuration

In this lab, you will:

- Create interface management profiles
- Configure Ethernet interfaces and subinterfaces with Layer 3 information
- Create a virtual router



You are to create two zones, Trust-L3 and Untrust-L3. The internal clients will connect to the interface assigned to the Trust-L3 Zone.

The external-facing interface will be in the Untrust-L3 zone. By default, all interfaces on the firewall must route traffic through the external-facing interface.

The interface in Untrust-L3 must be configured to respond to pings, and the interface in Trust-L3 must be able to provide all management services.

Lab Solution: Basic Interface Configuration

Create New Security Zones

1. Go to the Palo Alto Networks firewall WebUI and select **Network > Zones**.

2. Click **Add** and create an Untrust-L3 zone:

Name	Enter `Untrust-L3`
Type	Select **Layer 3**

3. Click **OK** to close the Zone Creation window.

4. Click **Add** and create the Trust-L3 zone:

Name	Enter `Trust-L3`
Type	Select **Layer 3**

5. Click **OK** to close the Zone Creation window.

Create Interface Management Profiles

6. Select **Network > Network Profiles > Interface Mgmt**.

7. Click **Add** and create an interface management profile:

Name	Enter `allow-mgt`
Permitted Services	Check the boxes for **Ping**, **SSH**, **HTTPS**, and **Response Pages**
Permitted IP Addresses	Do not add any addresses

8. Click **OK** to close the Interface Management Profile Creation window.

9. Click **Add** and create another interface management profile:

Name	Enter `allow-ping`
Permitted Services	Check only the **Ping** check box
Permitted IP Addresses	Do not add any addresses

10. Click **OK** to close the Interface Management Profile Creation window.

Configure Ethernet Interfaces with Layer 3 Information

11. Select **Network > Interfaces > Ethernet**.

12. Click the interface **<Internal interface>** and configure the interface.

Interface Type	Select **Layer 3**
Config tab	
Virtual Router	Keep **None**
Security Zone	Select **Trust-L3**
IPv4 tab	
Type	Keep **Static**
IP	Click **Add** and then enter `<Internal IP Address with mask>`
Advanced > Other Info tab	
Management Profile	Select **allow-mgt**

13. Click **OK** to close the Interface Configuration window.

14. Click the interface name **<External interface>**.

Interface Type	Select **Layer 3**
Config tab	
Virtual Router	Keep **None**
Security Zone	Select **Untrust-L3**
IPv4 tab	
Type	Keep **Static**
IP	Click **Add** and then enter `<External IP Address with mask>`
Advanced tab	
Management Profile	Select **allow-ping**

15. Click **OK** to close the Interface Configuration window.

Create a Virtual Router

16. Select **Network > Virtual Routers**.

17. Click **Add** to define a new virtual router:

Router Settings	
Name	Enter `Student-VR`
General subtab	

Interfaces	Click **Add** and then select **<External interface>** Click **Add** again and select **<Internal interface>**
Static Routes > IPv4 tab	Click **Add** and create an entry with these values.
Name	Enter `default`
Interface	Select **<External interface>**
Destination	Enter `0.0.0.0/0`
Next Hop	Select **IP Address**
Next Hop IP Address	Enter `<Next Hop IP Address>`

18. Click **OK** to add the static route and then click **OK** again to close the Virtual Router Configuration window.

Configure DHCP

19. Select **Network > DHCP > DHCP Server**.

20. Click **Add** to define a new DHCP server.

Interface Name	Select **<Internal interface>**
Mode	Select **enabled**
Lease tab	
Ping IP when allocating new IP	Check

Lease	Select **Timeout** 2 Days 0 Hours 0 Minutes
IP Pools	Click **Add** then enter `<DHCP address range>`
Options tab	
Gateway	Enter `<Internal IP Address>`
Subnet Mask	`255.255.255.0`
Primary DNS	Enter `<DNS Server>`

21. Click **OK** to close the DHCP Server Configuration window.

22. Click the **Commit** link at the top right of the WebUI. Click **Commit** again and wait until the Commit process completes before clicking **Close** to continue.

Test Connectivity to the Trust Interface

23. On the Windows Desktop, open a command prompt, as an administrator if necessary.

24. **NOTE**: Please do not release the IP address. If the management port of your PC is using DHCP, you will lose connectivity to the PC.

25. Renew the IP configuration with the command: `> ipconfig /renew`. The received IP address should be in the range you created on the firewall DHCP configuration. If a pop-up screen asks you to assign a network location, choose "Work" and close the pop-up.

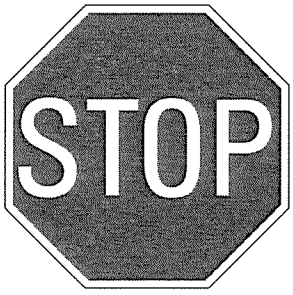
26. Verify that you have connectivity between your PC and the firewall by opening a command prompt on the Windows desktop and entering `ping <Internal IP Address>`.

27. Close the command prompt window.

28. In the WebUI, click **Network > DHCP > DHCP Server**.

29. For the DHCP server on <Internal interface>, click **View Allocation**. You should see the leased IP address being used by the Windows station. (You may see multiple IP addresses assigned to multiple hosts because of the setup of the lab network).

30. Click **Close**.

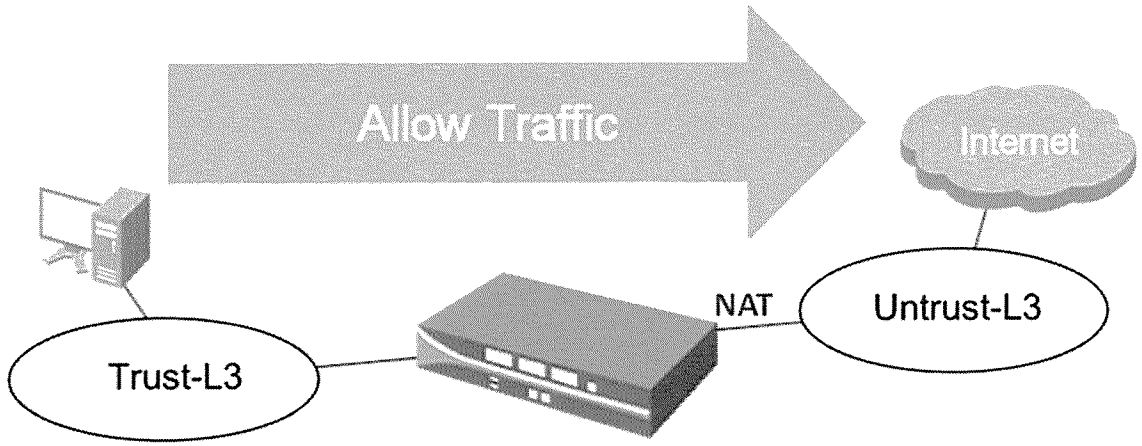


Lab Scenarios: NAT and Security Policies

In this lab, you will:

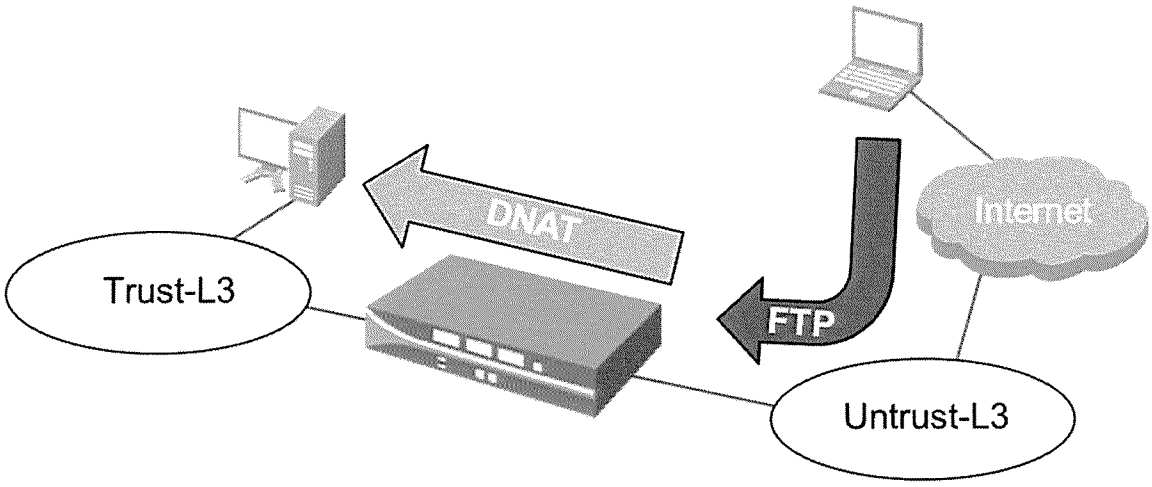
- Create a Source NAT policy
- Create a Security policy to allow connectivity from the Trust-L3 to the Untrust-L3 zone
- Configure destination NAT to allow FTP traffic to your student desktop

Scenario 1



At this point, the firewall is configured but it is unable to pass traffic between zones. NAT and Security policies must be defined before traffic will flow between zones. In this lab, you will create a source NAT policy using the Untrust-L3 IP address as the source address for all outgoing traffic. Then you will create a Security policy to allow traffic from the Trust-L3 zone to the Untrust-L3 zone so that your workstation can access the outside world.

Scenario 2



To enable you to share files with remote users, you have been instructed to set up an FTP server on your student desktop. Configure the firewall to accept FTP traffic on its publicly facing interface and then redirect the traffic to your PC using destination NAT.

Partner with another student to test your FTP configurations. Enable the FTP server on your student desktop. From another student's desktop, have your partner launch FTP using a command prompt, and verify that you can connect to the external IP address.

Lab Solution: NAT and Security Policies

Scenario 1

Create a Source NAT Policy

1. Select **Policies > NAT**.

2. Click **Add** to define a new source NAT policy:

General tab	
Name	Enter `Student Source NAT`
Original Packet tab	
Source Zone	Click **Add** and select **Trust-L3**
Destination Zone	Select **Untrust-L3**
Destination Interface	Select **<External interface>**
Translated Packet > Source Address Translation tab	
Translation Type	Select **Dynamic IP and Port**
Address Type	Select **Interface Address**
Interface	Select **<External interface>**
IP Address	Select **<External IP Address with mask>**

3. Click **OK** to close the NAT Policy Configuration window.

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

Create the Allow All Out Policy

4. Select **Policies > Security**.

5. Click **Add** to define a Security Policy rule:

General tab	
Name	Enter `Allow All Out`
Rule Type	**universal (default)**
Source tab	
Source Zone	Click **Add** and select **Trust-L3**
Source Address	Select **Any**
Destination tab	
Destination Zone	Click **Add** and select **Untrust-L3**
Destination Address	Select **Any**
Application tab	
Applications	Make sure that **Any** is checked
Service/URL Category tab	
Service	Select **application-default** from the drop-down list
Actions tab	

Action Setting	Select **Allow**
Log Setting	Check **Log at Session End**

6. Click **OK** to close the Security Policy Configuration window.

7. **Commit** your changes. You may need to reconnect to the WebUI afterward.

Verify Internet Connectivity

8. Test Internet connectivity by browsing websites from your desktop. You should be able to browse common sites on the Internet such as Google and Yahoo.

9. In the WebUI, select **Monitor > Logs > Traffic** to display the traffic logs. You should be able to see Web traffic and other sorts of traffic passing through the Allow All Out Security policy.

Scenario 2

Enable the FTP Server

10. On the desktop, double-click the **3CDaemon** icon.

11. Click the **FTP Server** tab in the left-hand column.

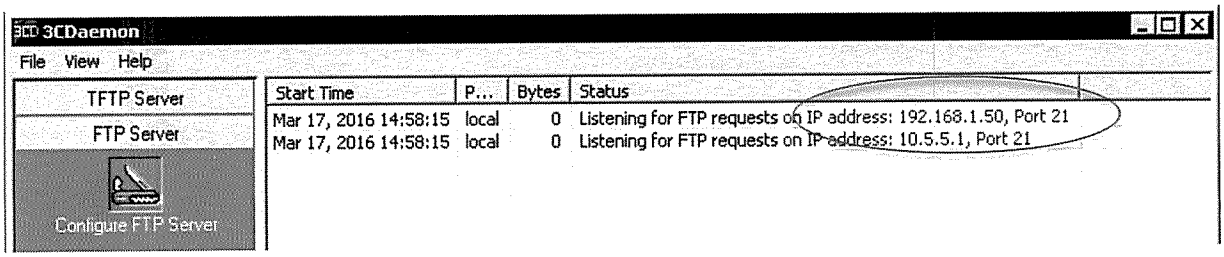
12. Click the **Configure FTP Server** icon.

13. Change the User Directory to the Desktop.

14. Click **OK**, then **Yes**, then **OK**.

15. If there is a green **GO** button listed, click it to start the FTP server.

16. Notice that the FTP server is listening on the IP address assigned by the firewall DHCP Server on the Trust interface for the PC.



Create a Destination NAT Policy

17. In the WebUI, select **Objects > Services**.

18. Click **Add** to create a new service:

General tab	
Name	Enter `service-ftp`
Destination Port	Enter `20-21`

19. Click **OK** to close the Service window.

20. In the WebUI, select **Policies > NAT**.

21. Click **Add** to define a new destination NAT policy.

General tab	
Name	Enter `Inbound-FTP-NAT`
Original Packet tab	
Source Zone	Click **Add** and select **Untrust-L3**
Destination Zone	Select **Untrust-L3** (*not* Trust-L3)
Service	Select **service-ftp**
Destination Address	Click **Add** and enter `<External IP Address>`
Translated Packet tab	

Destination Address Translation	Check the box
Translated Address	<PC Trust Interface IP Address>

22. Click **OK** to close the NAT Policy Configuration window.

Create a Security Policy Rule

23. Select **Policies > Security**.

24. Click **Add** to define a new Security Policy rule:

General tab	
Name	Enter Inbound-FTP-Rule
Source tab	
Source Zone	Click **Add** and select **Untrust-L3**
Destination tab	
Destination Zone	Click **Add** and select **Trust-L3**
Destination Address	Click **Add** and enter <External IP Address>
Application tab	
Applications	Click **Add** and select **ftp**
Service/URL Category tab	

Service	Select **application-default**
Action	
Action Setting	**Allow**

25. Click **OK** to close the Security Policy Configuration window.

26. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the process is complete, and click **Close** to continue.

Test the Connection

27. From your partner's desktop, open a command prompt and enter `ping <External IP Address>`. Your ping should be successful.

28. From the partner's desktop, enter `ftp <External IP Address>`.

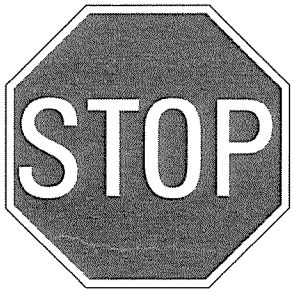
29. You are prompted for a username, which indicates that FTP was successfully passed through the firewall using destination NAT.

30. Close the command prompt.

31. In the WebUI, select **Monitor > Logs > Traffic** and find the entries where the application ftp has been allowed by rule Inbound-FTP-Policy.

32. In the FTP app, deactivate the FTP server by clicking the **STOP** button.

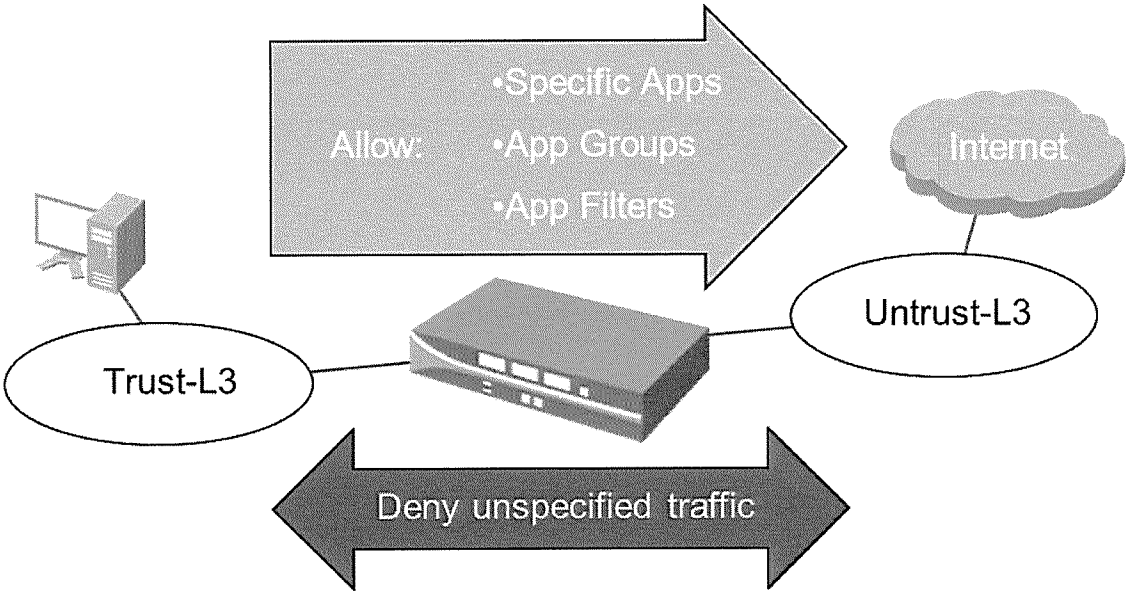
33. Close the 3CDaemon application.



Lab Scenario: Basic App-ID

In this lab, you will:

- Create a new Security policy to allow Internet connectivity
- Enable application block pages



Now that you have confirmed that your workstation has connectivity to the Internet, you will delete the Allow All Out Security policy rule and replace it with a more restrictive security rule. By default, the Palo Alto Networks firewall will block any traffic between different security zones. You will create a Security policy rule to selectively enable specific applications to pass from the Trust-L3 to the Untrust-L3 zone. All other applications will be blocked.

Create a rule named General Internet that allows users in the Trust-L3 zone to use a set of commonly used applications such as dns, google-base, flash, ftp, ping, ssl, and Web-browsing. The applications should be permitted only on an application's default port. All other traffic (inbound and outbound) between zones will be blocked and logged so that you can identify which other applications are being used.

Next, you will configure the firewall to notify users when applications are blocked by a rule.

Then you will test your connectivity by connecting to http://www.depositfiles.com. You have not specified depositfiles as an allowed application, so the firewall should block the application, even if you attempt to use a proxy like avoidr.com or php-proxy.net.

Lab Solution: Basic App-ID

Create the General Internet Policy

1. Go to the WebUI and select **Policies > Security.**

2. Select the Allow All Out Security policy rule without opening it, and click **Disable**.

3. Click **Add** to define a new Security policy rule:

General tab	
Name	Enter `General Internet`
Rule Type	**universal (default)**
Source tab	
Source Zone	Click **Add** and select **Trust-L3**
Source Address	Select **Any**
Destination tab	
Destination Zone	Click **Add** and select **Untrust-L3**
Destination Address	Select **Any**
Application tab	

Applications	Click **Add** and select each of these values: **dns** **google-base** **flash** **ftp** **ping** **ssl** **web-browsing**
Service/URL Category tab	
Service	Select **application-default**
Actions tab	
Action Setting	Select **Allow**
Log Setting	Check **Log at Session Start** Check **Log at Session End** (Logging at Session Start will allow you to see application shifts. In the rest of the labs, we will use only Log at Session End.)

4. Click **OK** to close the Security Policy Configuration window.

Enable Interzone Logging

5. Open the **interzone-default** policy.

6. Click the **Actions** tab. Note that Log at Session Start and Log at Session End are unchecked, and cannot be edited.

7. Click **Cancel**.

8. Select the **interzone-default** policy row, without opening the policy, and click **Override**. The Security Policy Rule – predefined window opens.

9. Click the **Actions** tab.

10. Check **Log at Session End**.

11. Click **OK**.

Enable the Application Block Page

12. Select **Device > Response Pages**.

13. Make sure that the Application Block Page line is **Enabled**.

14. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the commit process is complete, and continue.

Verify Internet Connectivity and Application Blocking

15. Test Internet connectivity by browsing websites from your desktop. You should be able to surf common sites on the Internet such as Google and Yahoo.

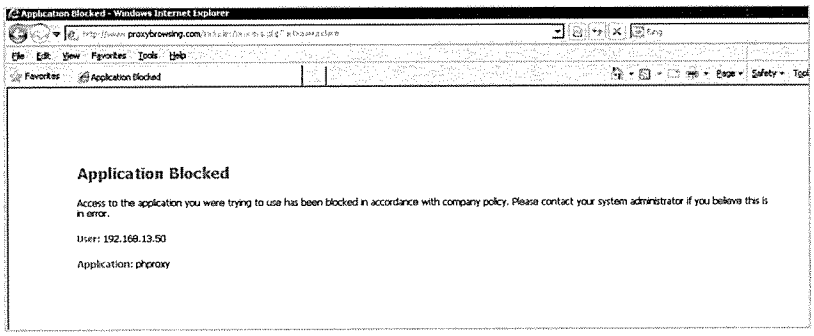
16. Use a browser to connect to the site `http://www.depositfiles.com`. An Application Blocked page opens, indicating that the depositfiles application has been blocked.

17. Select **Monitor > Logs > Traffic** to review the traffic logs. After the session has expired, you can find the entry where the depositfiles application has been blocked. You may want to put `( app eq depositfiles )` in the filter text box.

    The site has been blocked because the depositfiles application is not listed in the allowed applications in the General Internet policy.

18. Now try to work around the application block by using a proxy. From the desktop, go to the proxy site `http://www.avoidr.com`. (If avoidr is down, use another proxy like `php-proxy.net`.)

19. Enter `www.depositfiles.com` in the text box near the bottom of the page and click **Go**. An Application Blocked page opens showing that the phproxy application was blocked.



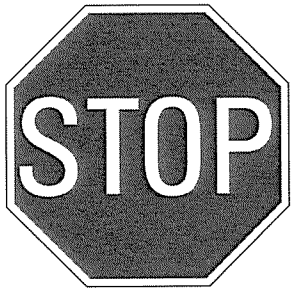
20. Select **Monitor > Logs > Traffic** to find the corresponding entry in the Traffic Logs. It indicates that the phproxy application has been blocked. You may want to put `( app eq phproxy )` in the filter text box.

21. Click the **ACC** tab to access the Application Command Center. 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.

22. On the **Network Activity** tab, maximize the **Application Usage** tab to see the application traffic you have generated so far (15 minutes may be needed before the ACC shows all application because of log aggregation).

23. Explore the other information available in the Network Activity tab.

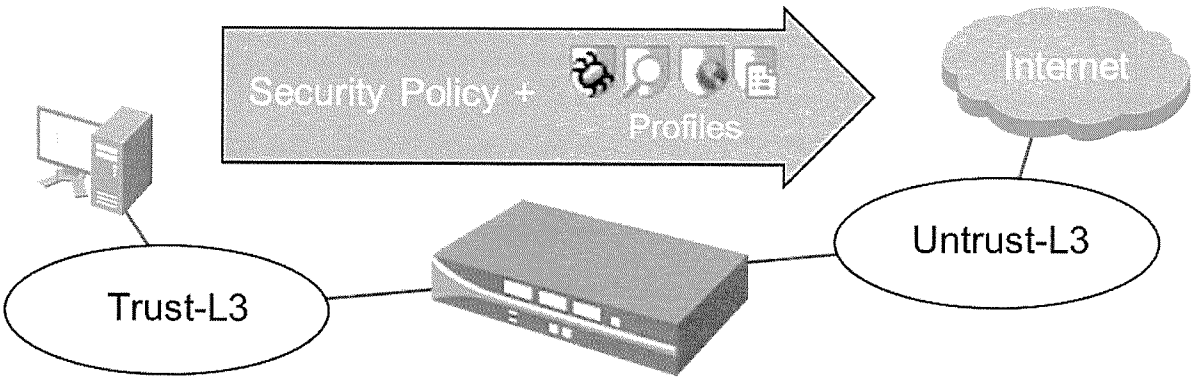
24. Notice that the **Threat Activity** tab contains no matching records yet.



Lab Scenario: Basic Content-ID

In this lab, you will:

- Configure Security Profiles
- Create a Security Profile group
- Associate the Security Profile group to a Security policy rule



Now that traffic is passing through the firewall, you decide to further protect the environment with Security Profiles. The specific security requirements for general Internet traffic are:

- Configure a custom URL filtering category TechSites specifying newegg, cnet, and zdnet
- Log all URLs accessed by users in the Trust-L3 zone
- Block these URL categories:
  - adult (or adult-and-pornography)
  - government
  - hacking
  - questionable
  - TechSites
  - unknown (set to continue)
- Log, but do not block, all viruses detected and maintain packet captures of these events for analysis
- Log spyware of severity levels medium, critical, and high. Ignore all other spyware
- After all of these profiles are configured, assign them to a Security Profile group, and assign the profile group to the Security policy rule.
- Then send test traffic to verify that the protection behaves as expected. Test the antivirus profile by downloading a file over HTTP from eicar.org. Test the URL Filtering Profile by trying to browse sites that have been prohibited.

After the initial testing is complete, you will be asked to change the antivirus protection to block viruses. Make the changes and verify the difference in behavior.

Lab Notes

Test the antivirus profile using HTTP and *not* HTTPS because decryption has not been configured on the firewall yet. HTTPS connections will prevent the firewall from seeing the packet contents, so the viruses contained will not be detected by the profile.

Lab Solution: Basic Content-ID

Configure a Custom URL Filtering Category

1. Go to the WebUI and select **Objects > Custom Objects > URL Category**.

2. Click **Add** to create a custom URL category:

Name	Enter `TechSites`
Sites	Click **Add** and add each of these URLs: ▪ `www.newegg.com` ▪ `www.cnet.com` ▪ `www.zdnet.com`

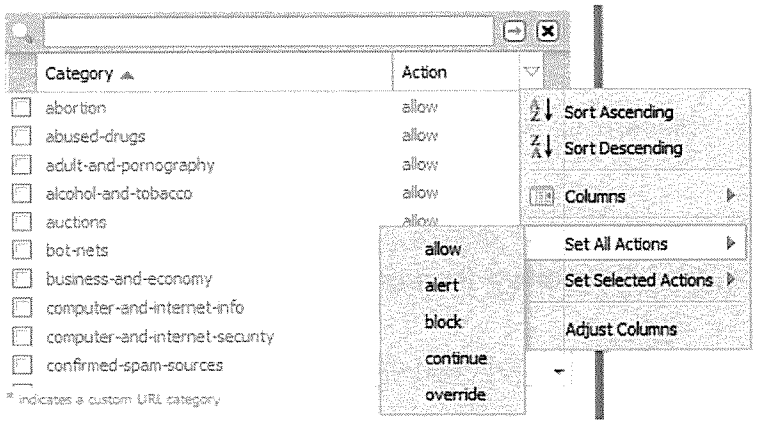
3. Click **OK** to close the Custom URL Category window.

Configure a URL Filtering Profile

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

5. Click **Add** to define a URL Filtering Profile:

Name	Enter `student-url-filtering`
Category/Action	Click the right side of the Action header to access the drop-down list. Click **Set All Actions > alert**.

	 Search the Category field for these six categories and set the Action to **block** for each except for the unknown category. Set the unknown category to **continue**. adult (or adult-and-pornography): [Action = **block**] government: [Action = **block**] hacking: [Action = **block**] questionable: [Action = **block**] unknown: [Action = **continue**] TechSites: [Action = **block**]

6. Click **OK** to close the URL Filtering profile Profile window.

Configure an Antivirus Profile

7. Select **Objects > Security Profiles > Antivirus**.

8. Click **Add** to create an antivirus profile:

Name	Enter `student-antivirus`
Antivirus tab	
Packet Capture	Check the **Packet Capture** box.

Decoders	Set the Action column to **Alert** for all decoders.

9. Click **OK** to close the Antivirus Profile window.

Configure an Anti-Spyware Profile

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

11. Click **Add** to create an anti-spyware profile:

Name	Enter `student-antispyware`
Rules tab	Click **Add** and create a rule with these parameters: ▪ Rule Name: Enter `AllowMLI` ▪ Action: Select **Allow**. ▪ Severity: Select **Medium**, **Low**, and **Informational**. Click **OK** to save the rule. Click **Add** and create another rule with these parameters: ▪ Rule Name: Enter `AlertCH` ▪ Action: Select **Alert**. ▪ Severity: Check the boxes for **Critical** and **High** only. Click **OK** to save the rule.
DNS Signatures tab	Confirm that Action on DNS Queries is set to **sinkhole** Sinkhole IPv4: **Palo Alto Networks Sinkhole IP (71.19.152.112)** Sinkhole IPv6: **IPv6 Loopback IP (::1)**

12. Click **OK** to close the Anti-Spyware Profile window.

Assign Profiles to a Policy

13. Select **Policies > Security**.

14. Click **General Internet** in the list of policy names. In the Actions tab, edit the policy rule to include the newly created profiles:

Actions tab	
Profile Type	Select **Profiles**
Antivirus	Select **student-antivirus**
Anti-Spyware	Select **student-antispyware**
URL Filtering	Select **student-url-filtering**

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

16. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the commit process is complete, then continue.

Test the Antivirus Profile

17. On your desktop, open a browser to `http://www.eicar.org`.

18. Click the **Download Anti-Malware Testfile** link.

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

20. 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 protocol http. (Do *not* use the SSL-encrypted downloads. The firewall will not be able to detect the viruses in an https connection until decryption is configured.)

21. If prompted, **Save** the file. Do *not* open or run the file. (The firewall is set to alert but not block the virus, but you may find that the browser blocks the file.)

22. Close the browser.

23. In the WebUI, select **Monitor > Logs > Threat** to display the threat log.

24. Find the log message that detected the Eicar file. Notice that the action for the file is Alert.

25. Click the **green down arrow** at on the left side of the line for the Eicar file detection to display the packet capture (pcap). Here is an example of what a pcap might look like:

```
00:06:21.000000 00:1b:17:00:64:1a > 00:1b:17:0c:e5:10, ethertype IPv4 (0x0800),
length 122: truncated-ip - 387 bytes missing! (tos 0x0, ttl  48, id 65353, offset
0, flags [DF], proto: TCP (6), length: 495) 188.40.238.250.80 > 192.168.16.50.3108:
P, cksum 0xe9cc (incorrect (-> 0x8f1c), 2964771028:2964771483(455) ack 1330196269
win 7504
        0x0000:  001b 170c e510 001b 1700 641a 0800 4500  ..........d...E.
        0x0010:  01ef ff49 4000 3006 cdc1 bc28 eefa c0a8  ...I@.0....(....
        0x0020:  1032 0050 0c24 16fb ae05 6644 dd32 5018  .2.P.$....fD.2P.
        0x0030:  1d50 e9cc 0000 5835 4f21 5025 4041 505b  .P....X5O!P%@AP[
        0x0040:  345c 505a 5835 3428 505e 2937 4343 2937  4\PZX54(P^)7CC)7
        0x0050:  7d24 4549 4341 522d 5354 414e 4441 5244  }$EICAR-STANDARD
        0x0060:  2d41 4e54 4956 4952 5553 2d54 4553 542d  -ANTIVIRUS-TEST-
        0x0070:  4649 4c45 2124 482b 482a 0000 0000 0000  FILE!$H+H*......
```

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

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

27. Select **Objects > Security Profiles > Antivirus**.

28. Open the **student-antivirus** profile.

29. Change the Action column for the ftp, http, and smb decoders to **default (reset-both)**.

30. Click **OK**.

31. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the commit process is complete, then continue.

32. Open a new browser window to `www.eicar.org/85-0-Download.html`.

33. Attempt to download a virus file using HTTP again. The Antivirus profile is now set to Block, so a response page should appear.

34. Select **Monitor > Logs > Threat** and note that the log entries stating that the Eicar virus was detected and denied.

35. After 15 minutes, the threats that you just generated will appear on the ACC tab under the Threat Activity and the Blocked Activity tabs.

Test the URL Filtering Profile

36. Select **Device > Licenses**.

37. Under the PAN-DB URL Filtering header, click **Download Now** (or **Re-Download**). A warning appears.

38. Click **Yes**.

39. Select the region nearest the location of your firewall.

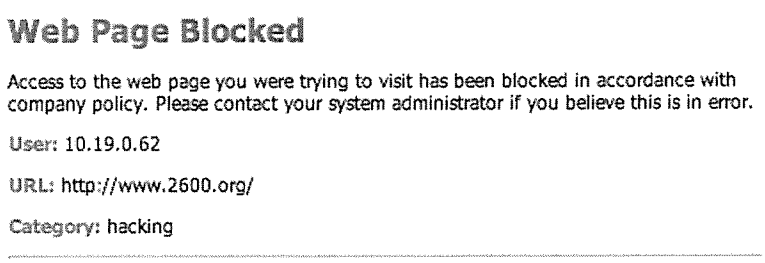
40. Click **OK**. When the download completes, a Download Successful window appears.

41. Click **OK** to close the open windows.

42. Open a browser and browse to various websites such as Google, Yahoo, or Bing. The URL Filtering Profile records each website that you visit.

43. In the WebUI, select **Monitor > Logs > URL Filtering**. Verify that the log entries track the sites that you visited during your tests.

44. Now test the block condition that you created by visiting a site that is part of the hacking, government, or TechSites category. Open a browser and attempt to browse to a government site such as `http://www.ca.gov`, hacking sites such as `http://www.2600.org`, or to the sites that you listed in the TechSites group. The profile will block these actions and you will see a block page similar to this one:



45. Select **Monitor > Logs > URL Filtering**. Find the sites that were blocked in the log.

Configure a Security Profile Group

46. In the WebUI, select **Objects > Security Profile Groups**.

47. Click **Add** to define a Security Profile group:

Name	Enter `student-profile-group`
Antivirus Profile	Select **student-antivirus**
Anti-Spyware Profile	Select **student-antispyware**
URL Filtering Profile	Select **student-url-filtering**

48. Click **OK** to close the Security Profile Group window.

Assign the Security Profile Group to a Policy

49. Select **Policies > Security**.

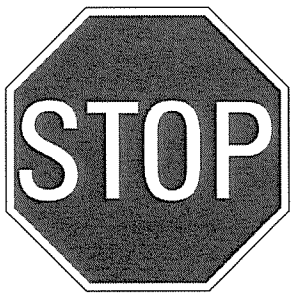
50. Click **General Internet** in the list of policy names.

51. Edit the policy rule to replace the profiles with the profile group:

Actions tab	
Profile Type	Select **Group**
Group Profile	Select **student-profile-group**

52. Click **OK** to close the Policy window.

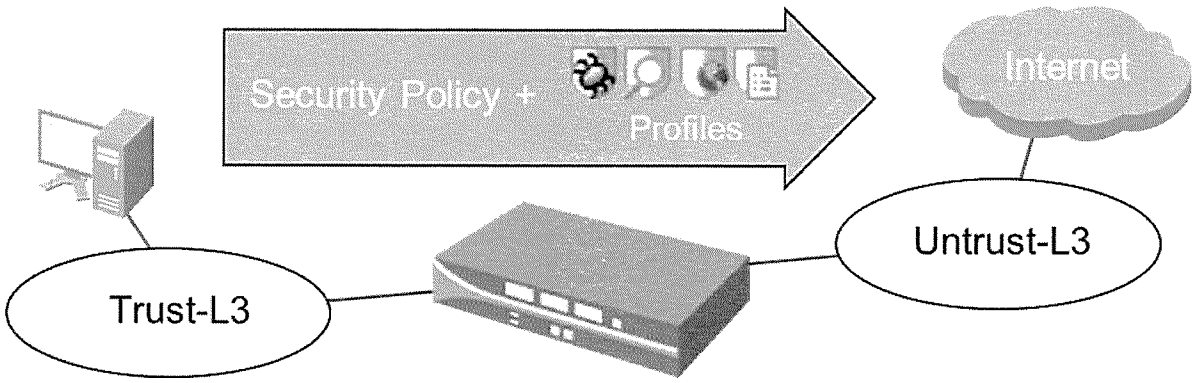
53. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the commit process is complete, then continue.



Lab Scenario: File Blocking and WildFire

In this lab, you will:

- Configure Security Profiles for file blocking and WildFire analysis
- Add these Security Profiles to the Security Profile groups associated with the Security policy rule



Now that traffic is passing through the firewall, you decide to further protect the environment with some more Security Profiles. The addictional security requirements for general Internet traffic are:

- Configure downloaded pdf files to be automatically blocked
- Test file blocking by trying to download a PDF file
- Configure WildFire and confirm that executable files are sent to WildFire for analysis

Lab Solution: File Blocking and WildFire

Create a File Blocking Profile

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

2. Click **Add** to create a File Blocking Profile:

Name	Enter `student-file-blocking`
Rules list	Click **Add** and create a rule with these parameters: ▪ Rule Name: Enter `BlockPDF` ▪ Applications: **any** ▪ File Types: **pdf** ▪ Direction: **both** ▪ Action: **block**

3. Click **OK** to close the File Blocking Profile window.

Create a WildFire Analysis Profile

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

5. Click **Add** to create a WildFire Analysis profile:

Name	Enter `student-wildfire`
Rules list	Click **Add** and create a rule with these parameters: ▪ Name: `AnalyzeEXE` ▪ Applications: **any** ▪ File Types: **pe** ▪ Direction: **both**

	▪ Analysis: **public-cloud**

6. Click **OK**.

Assign the File Blocking and WildFire Profiles to the Profile Group

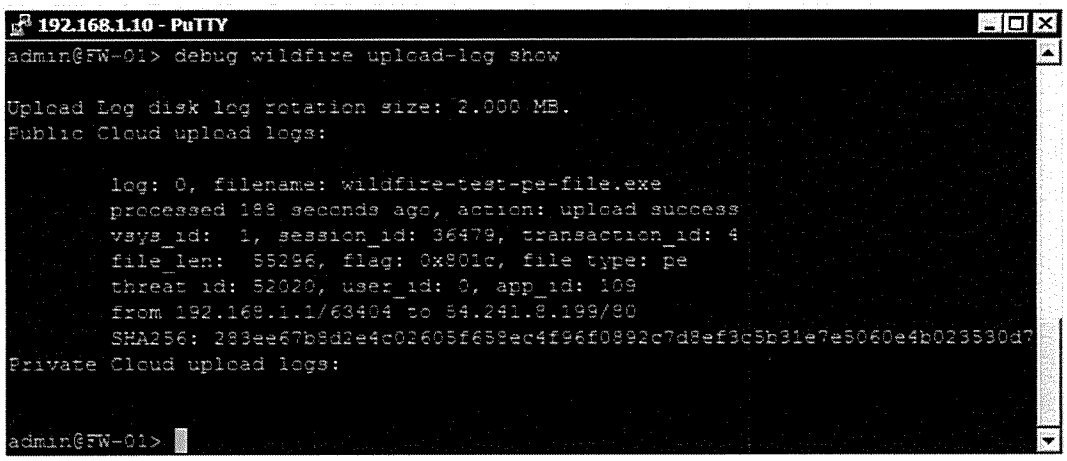
7. In the WebUI, select **Objects > Security Profile Groups**.
8. Open **student-profile-group**.
9. Choose **student-file-blocking** as the File Blocking Profile.
10. Choose **student-wildfire** as the WildFire Analysis Profile.
11. Click **OK**.
12. **Commit** the changes.

Test the File Blocking Profile

13. Open a new browser window to `http://www.panedufiles.com/`. The site opens.
14. Click the **Panorama_AdminGuide70.pdf** link. The download fails.
15. Select **Monitor > Logs > Data Filtering** and find the entry for the PDF file that has been blocked.

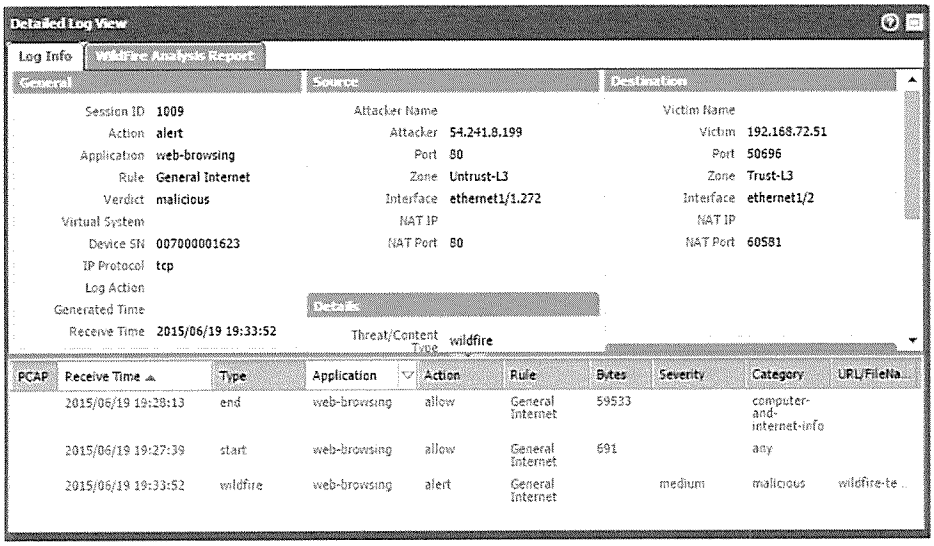
Test the WildFire Analysis Profile

16. Open a new browser window to: `http://wildfire.paloaltonetworks.com/publicapi/test/pe`. This site generates an attack file with a unique signature, which simulates a zero-day attack.
17. Save the file, without opening it, to the Downloads directory.
18. To verify that the file was uploaded to the Public WildFire Cloud, use PuTTY to open an SSH connection into the firewall using the `<Firewall Mgt Address>`.
19. When you are logged in via SSH, enter the `debug wildfire upload-log show` command to display the output showing "log: 0, filename: wildire-test-pe-file.exe processed….". This output verifies that the file was uploaded to the WildFire Public Cloud. It may take some time for the message to appear.



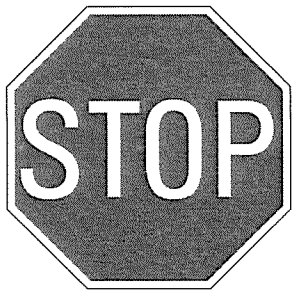
20. Select **Monitor > Logs > WildFire Submissions.** After some time has passed (may be as long as 5 minutes), find the entry for wildfire-test-pe-file.exe that has been submitted to WildFire and identified as malicious.

21. Click the **magnifying glass icon** next to the entry to see the Detailed Log View of the WildFire entry:



22. 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.

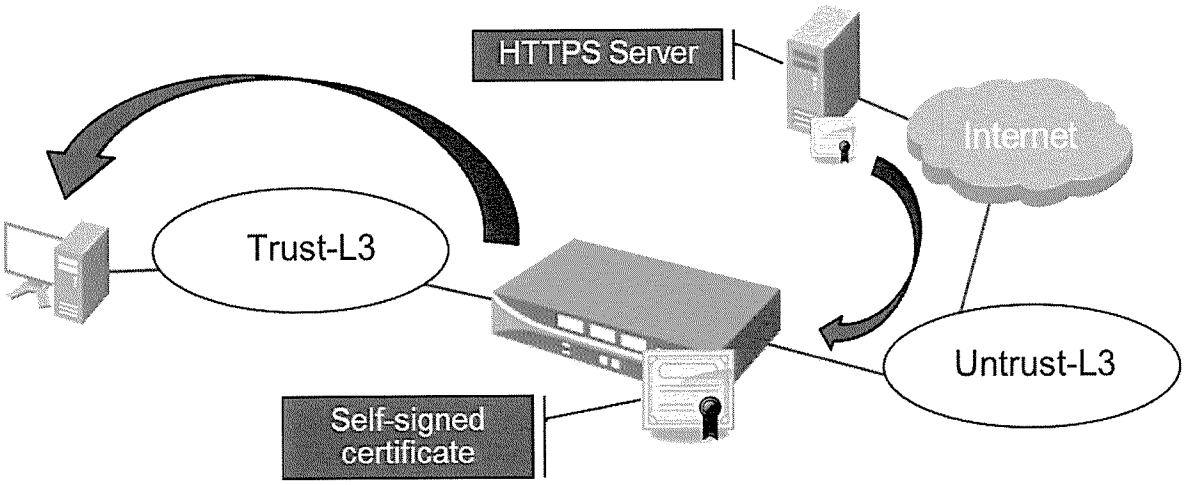
23. Log out and close the SSH putty.exe session.



Lab Scenario: Decryption

In this lab, you will:

- Create a self-signed SSL certificate
- Configure the firewall as a forward proxy using decryption rules
- Import the firewall forward trust certificate into the Windows desktop.



The security team observed that the Antivirus Profile identified only viruses that were not SSL-encrypted. The team is concerned that files transferred from encrypted sources (e.g., https://www.facebook.com) can escape detection and cause issues. Verify that HTTPS downloads of virus files from www.eicar.org are not detected by the Antivirus Profile.

Create a forward-proxy configuration on the Palo Alto Networks firewall. Only traffic from Trust-L3 to Untrust-L3 must be decrypted. Use self-signed SSL certificates generated on the firewall.

The Legal department has advised you that certain traffic should not be decrypted for liability reasons. Specifically, you may not decrypt traffic from health-related, shopping, or financial websites.

After an application is decrypted and identified by the Palo Alto Networks firewall, it may be denied if you have set the Security policy to only allow applications that arrive on their standard default ports. You may find that when you are using decryption, you will need to set your security rule to allow any port instead of using application-default. Create a new security policy rule specifically for web browsing, and move any applications related to web browsing to that policy. Then allow traffic for services http and https in the policy rule.

Test the decryption in two ways:

1. Attempt to download test files from www.eicar.org using HTTPS in Internet Explorer and verify that they are detected by the firewall

2. Connect to various websites using HTTPS in Internet Explorer and use the traffic logs to verify that the traffic from the correct URL categories is being decrypted

You will receive certificate errors when browsing after decryption is enabled. This behavior is expected because the self-signed certificates have not been added to the trusted certificates of the client browser. Resolve this issue by adding the firewall certificate to the clients as a trusted root certificate.

After your initial testing of the forward proxy, the penetration testing team calls you to request an exception to the decryption rules. The team asks that www.eicar.org be excluded from decryption so that it still will be able to download the files that it needs to perform its evaluations. Change the implementation to allow this exception.

Lab Notes

- Sequence order matters with policies. Make sure that the decrypt and no-decrypt rules are evaluated in the correct order.

- To find URLs to test the no-decrypt rule, go to https://urlfiltering.paloaltonetworks.com/testASite.aspx and enter various URLs that you think will fall into the categories that you are testing.

Lab Solution: Decryption

Verify 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. From the desktop, open an Internet Explorer browser and browse to `www.eicar.org/85-0-Download.html`.

2. Scroll to the bottom of the page and use HTTP to download one of the test files. The file is blocked and a warning page opens.

3. Click the **Back** button and use HTTPS to download one of the files. The file will download (but may be deleted by the browser).

4. Select **Monitor > Logs > Threat** to display the log. Only the non-encrypted download should appear in the log. SSL decryption has hidden the contents of the second test file and so it is not detected as a threat.

Create Two SSL Self-Signed Certificates

5. In the Web UI, select **Device > Certificate Management > Certificates**.

6. Click **Generate** at the bottom of the page to create a new CA certificate:

Certificate Name	Enter `TrustCA`
Common Name	Enter `<Internal IP Address>`
Certificate Authority	Check the box

7. Click **Generate** to create the certificate.

8. Click **OK** to close the Generate Certificate Success window.

9. Click **Generate** at the bottom of the page to create a new CA certificate:

Certificate Name	Enter `UntrustCA`

Common Name	Enter `<Internal IP Address>`
Certificate Authority	Check the box

10. Click **Generate** to create the certificate.

11. Click **OK** to dismiss the Generate Certificate Success window.

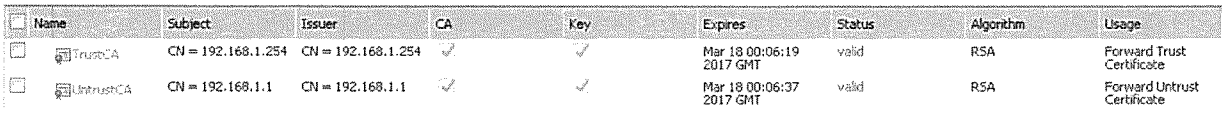
12. Click **TrustCA** in the list of certificates to edit the Certificate Information.

13. Check the box for **Forward Trust Certificate**. Click **OK**.

14. Click **UntrustCA** in the list of certificates to edit the Certificate Information.

15. Check the box for **Forward Untrust Certificate**. Click **OK**.

16. Your certificates should look like this:



Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
TrustCA	CN = 192.168.1.254	CN = 192.168.1.254	✓	✓	Mar 18 00:06:19 2017 GMT	valid	RSA	Forward Trust Certificate
UntrustCA	CN = 192.168.1.1	CN = 192.168.1.1	✓	✓	Mar 18 00:06:37 2017 GMT	valid	RSA	Forward Untrust Certificate

Create SSL Decryption Policies

17. In the WebUI, select **Policies > Decryption**.

18. Click **Add** to create an SSL decryption rule for the exception categories:

General tab	
Name	Enter `no-decrypt-traffic`
Source tab	
Source Zone	Select **Trust-L3**.
Destination tab	

Destination Zone	Select **Untrust-L3**.
Service/URL Category tab	
URL Category	Click **Add** and add each of these URL categories: ▪ **financial-services** ▪ **health-and-medicine** ▪ **shopping**
Options tab	
Action	Select **no-decrypt**

19. Click **OK** to close the Decryption Policy Rule window.

20. Click **Add** to create the SSL Decryption Rule for general decryption:

General tab	
Name	Enter `decrypt-all-traffic`
Source tab	
Source Zone	Select **Trust-L3**
Destination tab	
Destination Zone	Select **Untrust-L3**
Service/URL Category tab	
URL Category	Verify that the **any** box is checked

Options tab	
Action	Select **Decrypt**
Type	Select **SSL Forward Proxy**

21. Click **OK** to close the Decryption Policy Rule window.

22. In the **Policies > Decryption** window, confirm that the no-decrypt-traffic policy rule is above the decrypt-all-traffic policy rule.

Modify the Security Policy Rules

23. In the WebUI, select **Policies > Security**.

24. Select the **General Internet** policy rule without opening it.

25. Click **Clone**. A new General Internet-1 policy rule is created.

26. Click **OK**.

27. Open the **General Internet** policy rule.

28. In the **Application** tab, delete the **flash**, **google-base**, **ssl**, and **web-browsing** applications.

29. Select **OK** to close the General Internet security policy rule.

30. Open the **General Internet-1** security policy rule.

31. In the **General** tab, rename the policy rule to `Web Traffic`.

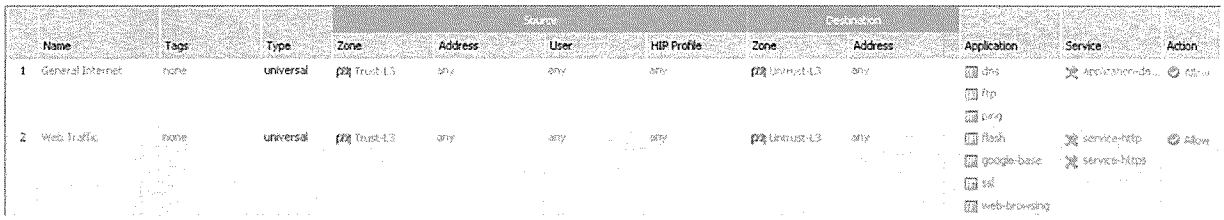
32. Select the **Application** tab.

33. Delete the **dns**, **ftp**, and **ping** applications.

34. Select the **Service/URL Category** tab.

35. Add the services **service-http** and **service-https**.

36. Click **OK** to close. Your security policy rule list should now look like this:



37. **Commit** the changes. Ignore the duplicate certificate warning.

Test the SSL Decryption Policy

38. Open a new Internet Explorer browser and go to `www.eicar.org/85-0-Download.html`.

39. Try to download a test file using HTTPS. A certificate error appears.

40. Click through the certificate error. The test file is blocked.

41. Close the browser window.

42. In the WebUI, examine the **Monitor > Logs > Threat** logs. The virus should have been detected because the SSL connection was decrypted.

43. Click the **magnifying glass icon** at the beginning of the line to display the Detailed Log View, maximize the view, and then examine the **Flags** panel to verify that the Decrypted box is checked:

Test the SSL No-Decryption Policy

44. Open a browser to the Palo Alto Networks Test A Site page at `https://urlfiltering.paloaltonetworks.com/testASite.aspx`.

45. Click through the certificate error.

46. Enter `www.bankofthewest.com` in the URL Lookup field, enter the required Captcha Code, and click **Search**. The financial-services category appears.

47. Test other URLs that you believe are in the categories for financial-services, health-and-medicine, and shopping. For example:

    - Category: financial-services

      `www.wellsfargo.com, www.chase.com`

    - Category: health-and-medicine

      `www.deltadental.com, www.kp.org`

- Category: shopping

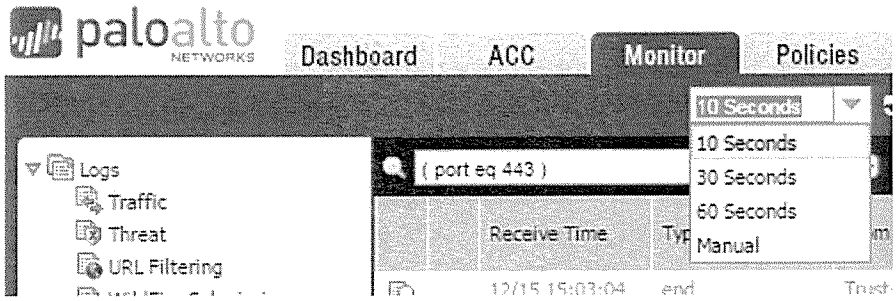
  `www.macys.com, www.costco.com`

48. In the WebUI, select **Monitor > Logs > Traffic**.

49. Set the traffic log to display only port 443 traffic by entering `( port.dst eq 443 )` in the filter field and clicking the **right-facing green arrow**.

50. If the Decrypted column is not displayed, display it by clicking the arrow next to one of the column titles, selecting **Columns**, and then selecting **Decrypted**.

51. Select **10 Seconds** from the drop-down list so that the display will refresh automatically. Leave this window open so that you can monitor the traffic.



52. In a new browser, use SSL (https://) to navigate to the websites that you found in the excluded URL categories. Notice that there are no certificate errors displayed.

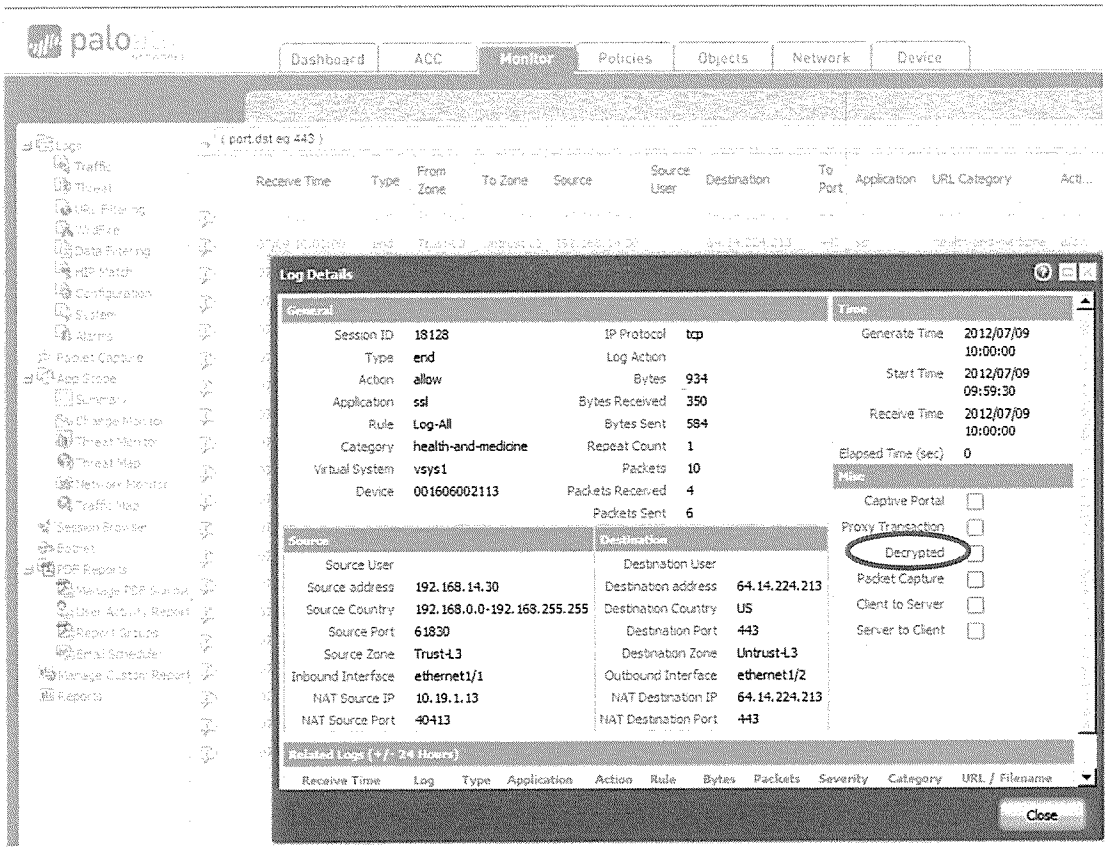
53. Navigate to websites that will be decrypted (e.g., `https://www.paloaltonetworks.com`, `https://www.bing.com`) for comparison purposes. Click through any certificate errors.

54. Select **Monitor > Logs > Traffic**.

55. Find an entry for one of the excluded categories by looking for an entry where Decrypted is listed as no.

56. Click **the magnifying glass icon** at the beginning of the line, and maximize the window to show the Log Details window.

57. Verify that the Decrypted check box in the Flags panel is unchecked.



Import the CA Certificate into Windows Trusted Certificates

58. In the Web UI, select **Device > Certificate Management > Certificates**.

59. Check the checkbox for the TrustCA certificate, without opening it.

60. Click **Export**. The Export Certification window opens.

61. Leave the file format at Base64 Encoded Certificate (PEM), and leave the Export private key check box unchecked.

62. Click **OK** and download the .crt file. (If your browser saves the file as a .txt file, change the extension to .crt.)

63. Find the downloaded.crt file in the Windows file system, and double-click the certificate. A security warning appears.

64. Click **Open**. The certificate opens.

65. Click **Install Certificate…** The Certificate Import Wizard opens.

66. Click **Next**.

67. Select **Place all certificates in the following store** and click **Browse**. The Select Certificate Store window opens.

68. Select **Trusted Root Certification Authorities** and click **OK**. The window closes.

69. Click **Next**. The Completing the Certificate Import Wizard window opens.

70. Click **Finish**. After a short delay, a security warning appears.

71. Click **Yes**. A box indicates that the import was successful.

72. Click **OK**.

73. Close the certificate by clicking **OK**.

74. Double-click the certificate and click **Open** to open it.

75. In the certificate, click the **Certification Path** tab. Notice that the Certificate Status says "This certificate is OK".

76. Click **OK** to close the certificate.

77. Open a new browser window using Chrome or Internet Explorer (*not* Firefox, which uses its own certificate store). Restart the browser if it is already open.

78. Browse some HTTPS sites such as `https://www.paloaltonetworks.com` or `https://www.bing.com`. Notice that you no longer receive the certificate errors.

Exclude a Site from Decryption

79. Use PuTTY to open an SSH session to the `<Firewall MgtAddress>`.

80. Issue these commands:

```
> configure
# set shared ssl-decrypt ssl-exclude-cert *.eicar.org
# show shared ssl-decrypt
# commit
# exit
```

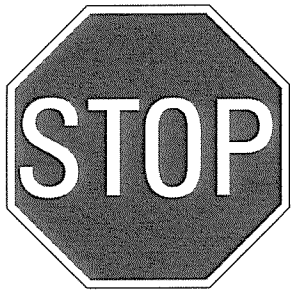
```
10.5.5.11 - PuTTY
admin@FW-01# set shared ssl-decrypt ssl-exclude-cert *.eicar.org

[edit]
admin@FW-01# show shared ssl-decrypt
ssl-decrypt {
  forward-untrust-certificate UntrustCA;
  forward-trust-certificate TrustCA;
  ssl-exclude-cert *.eicar.org;
}
[edit]
```

81. After the commit has completed, open a new Internet Explorer window to `http://www.eicar.org/85-0-Download.html`.

82. Scroll to the bottom of the page and download a virus file encrypted by HTTPS. You should see that now the file downloads without being blocked (though the browser may detect the virus and delete the file) because files from eicar are now excluded from encryption.

83. Enter `show system setting ssl-decrypt exclude-cache`. The exclude cache is displayed. You should see an address in the 188.40.238.0/24 range, which is the IP address for eicar.org.

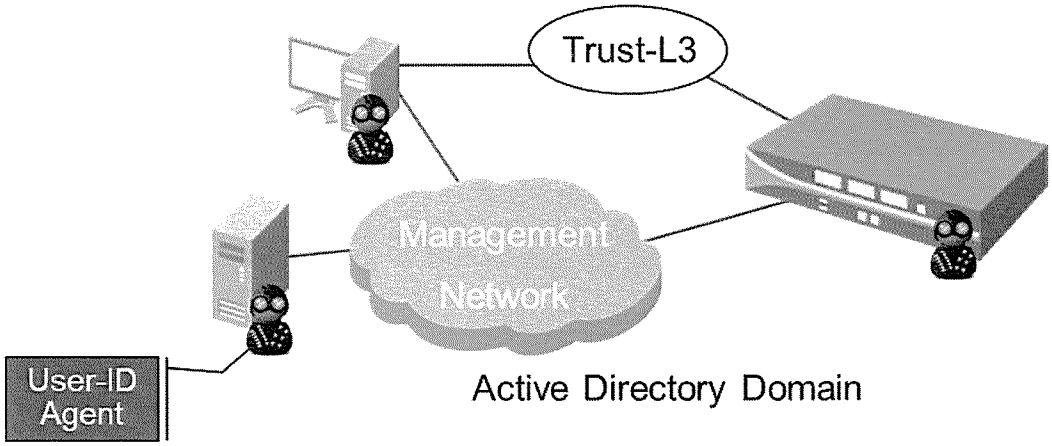
```
admin@FW-01> show system setting ssl-decrypt exclude-cache

VSYS  SERVER                  APP          TIMEOUT  REASON            DECRYPTED_APP  PROFILE
1     188.40.238.252:443      ssl          43086    CERT_UNSUPPORTED   undecided
```



Lab Scenario: Basic User-ID

In this lab, you will:

- Enable User-ID for a zone
- Configure User-ID group mapping
- Install a software User-ID agent on a Windows host
- Connect your firewall to the User-ID agent



Management wants to evaluate the benefits of monitoring traffic on a more granular level, such as allowing or denying access on a per-user basis. Your firewall is already configured as part of the Active Directory (AD) domain, as is the desktop.

Install a User-ID software agent on your desktop. A user account has been configured in AD with the appropriate permissions to read the system logs. On the system hosting the agent, the account must have specific permissions:

- Local Security policy must allow the account to log on as a service.
- The account must have modify permissions on the User-ID agent folder.
- The account must have full control for the Palo Alto Networks registry entry.

The firewall must also be configured to communicate with the agent.

Lab Solution: Basic User-ID

Enable User-ID on Trust Zone

1. Go to the WebUI and select **Network > Zones.**

2. Open the **Trust-L3** zone.

3. Enable User-ID by checking the **Enable User Identification** check box. Click **OK**.

Configure the LDAP Server Profile and Authentication Profile

4. In the WebUI, select **Device > Server Profiles > LDAP**.

5. Select **Add**.

Profile Name	PAN-Training-AD
Server List	Select **Add**
Name	DC1
LDAP Server	<Domain Controller Address>
Port	636
Server Settings	
Type	**active-directory**
Base DN	<Base DN>
Bind DN	<Bind DN>
Password	<LDAP password>

Require SSL/TLS secured connection	Check

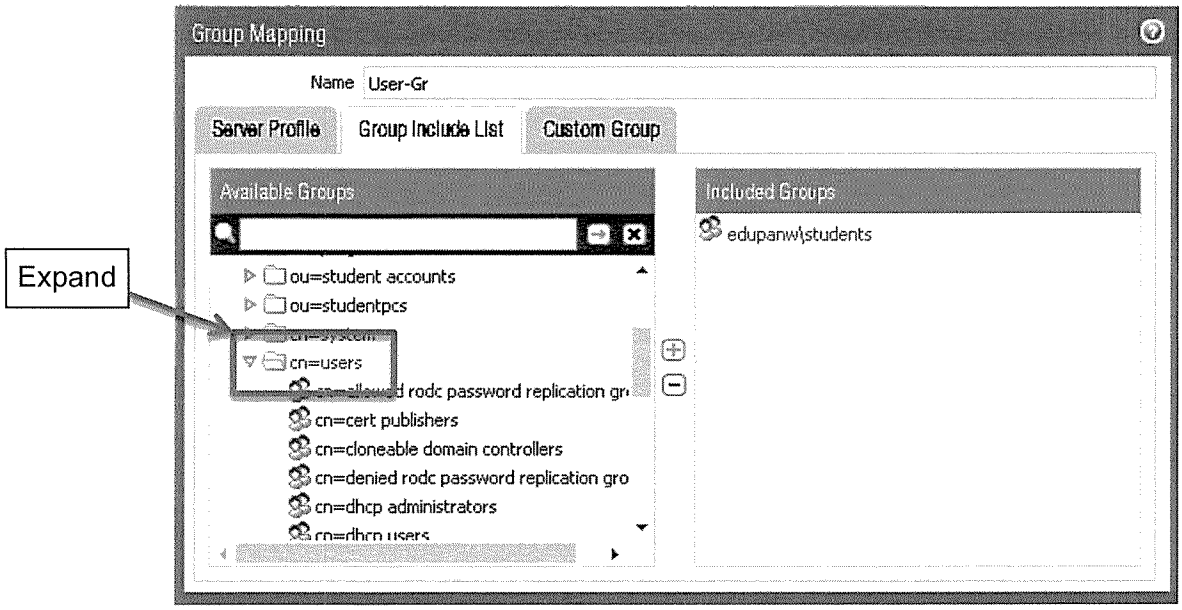
6. Close the LDAP Server Profile window.

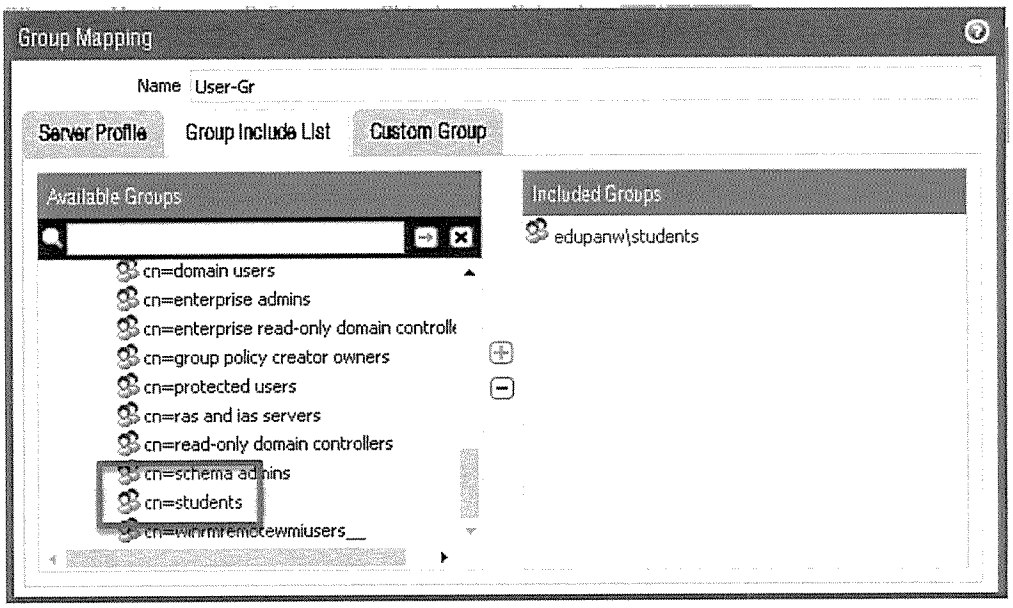
Configure User-ID Group Mapping

7. In the WebUI, select **Device > User Identification > Group Mapping Settings**.

8. Click **Add**:

Name	Enter `User-Gr`
Server Profile tab	
Server Profile	**PAN-Training-AD**
Group Include List tab	
Included Groups	Add **<LDAP Group>** to the Included Groups column





9. Click **OK.**

10. **Commit** the changes.

11. Open a PuTTY session to the `<Firewall Mgt Address>`.

12. Enter the command `show user group-mapping state all`. The output should confirm that the students group has been mapped.

```
10.5.5.11 - PuTTY

admin@FW-01>
admin@FW-01> show user group-mapping state all


Group Mapping(vsys1, type: active-directory): LDAP
        Bind DN     : CN=pwldap,CN=Users,DC=edupanw,DC=com
        Base        : DC=edupanw,DC=com
        Group Filter: (None)
        User Filter: (None)
        Servers     : configured 1 servers
                10.5.5.60(636)
                        Last Action Time: 180 secs ago(took 0 secs)
                        Next Action Time: In 3420 secs
        Number of Groups: 1
        cn=students,cn=users,dc=edupanw,dc=com
```

Install the Software User-ID Agent

13. On the Windows desktop, open the network share `<Network Drive>`. (There may be a shortcut named **Students** on your desktop. See your instructor if you need assistance.)

14. Copy the latest available version of the UaInstall msi file to your desktop.

15. Close Windows Explorer.

16. Double-click the **UaInstall** msi file on your desktop.

17. Click **Run**, then click **Next** three times to complete the installation. Wait for the installation to complete, then click **Close** to continue.

Configure the User-ID Agent Service

18. Enter `services.msc` in a command prompt on the Windows desktop. The Services panel opens.

19. Find the User-ID Agent service in the list of services.

20. Right-click the **User-ID Agent** service, and select **Properties**.The User-ID Agent Properties window opens.

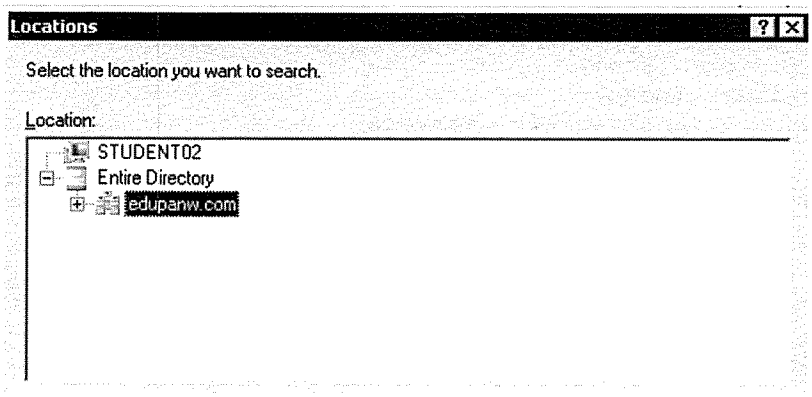
21. Select the **Log On** tab.

22. Select the **This account** radio button.

23. Select **Browse...** The Select User window opens.

24. Select **Locations...** The Locations window opens.

25. Expand the Entire Directory tree, and then select the domain name immediately under the Entire Directory branch.



26. Click **OK**.

27. Enter the <User-ID account name> in the text box and click **Check Names**. The full name of the user is populated.
28. Click **OK**.
29. Enter the <User-ID account password>.
30. Click **OK**. A warning appears instructing you to stop and restart the service.
31. Click **OK**.
32. Select the User-ID Agent service in the list of services without opening it, and then select the **Restart the service** link in the upper left corner of the window. The service restarts.
33. Close the Services window.

Configure the Software User-ID Agent

34. Using Windows Explorer, open the folder **C:\Program Files\Palo Alto Networks\User-ID Agent**.
35. Right-click the file **UaController** application and choose **Run as administrator**. (Use Shift+click if the Run as administrator option does not appear.) The User-ID agent program starts.
36. Click **Yes** if prompted. The program opens.
37. Click **Setup** in the tree diagram.
38. Click the **Edit** button under the Setup panel to configure the agent:

Authentication tab	
User name for Active Directory	<User-ID account name with FQDN> For example, useridagent@EDUPANW.COM
Password	<User-ID account password>
Client Probing tab	
Enable WMI Probing	Keep the box checked

Enable NetBIOS Probing	Uncheck the box
Agent Service tab	
User-ID Service TCP Port	Verify that the port is 5007

39. Click **OK** to close the setup window.

40. Click **Discovery** in the tree diagram.

41. Click the **Auto Discover** button under the Servers panel. A list of Domain Controller server names and IP addresses populates.

42. Click **Commit** in the User-ID agent to activate your changes.

43. Click **Logs** in the tree diagram to verify that the service has started. There may be a short wait.

44. Select the **Monitoring** tab. The existing user-to-IP mappings are listed. NOTE: The student PC's have been authenticated to the Domain Controller through the Mgt port of the PC. Notice that the userids have been mapped to addresses in the Mgt subnet.

Configure Palo Alto Networks Firewall to Connect to User-ID Agent

45. Go to the WebUI and select **Device > User Identification > User-ID Agents**.

46. Click **Add** to define a connection to the newly installed User-ID agent:

Name	Enter `software-UIA`
Host	`<Desktop Mgt IP Address>`
Port	Enter `5007`
Enabled	Verify that the box is checked

47. Click **OK** to close the User Identification Agent window.

48. Click the **Commit** link at the top right of the WebUI. Click Commit again, wait until the commit process is complete, and click **Close** to continue.

Test User-ID

49. To verify connectivity between the firewall and the agent, from the WebUI, select **Device > User Identification > User-ID Agents.** The round indicator in the **Connected** column should turn green.

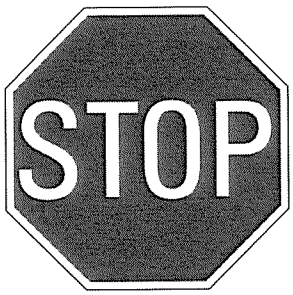
50. In the User-ID agent program, select **User Identification** in the tree. The firewall's Mgt address is listed in the Connected Devices list.

51. From the desktop, use PuTTY to open an SSH session to the `<Firewall Mgt Address>`.

52. From the CLI, issue this command: `show user user-id-agent statistics`. The software-UIA agent should be in the list.

53. From PuTTY, verify that the User-ID agent is mapping users to the Management IP address on your PC with the `show user ip-user-mapping all` command.

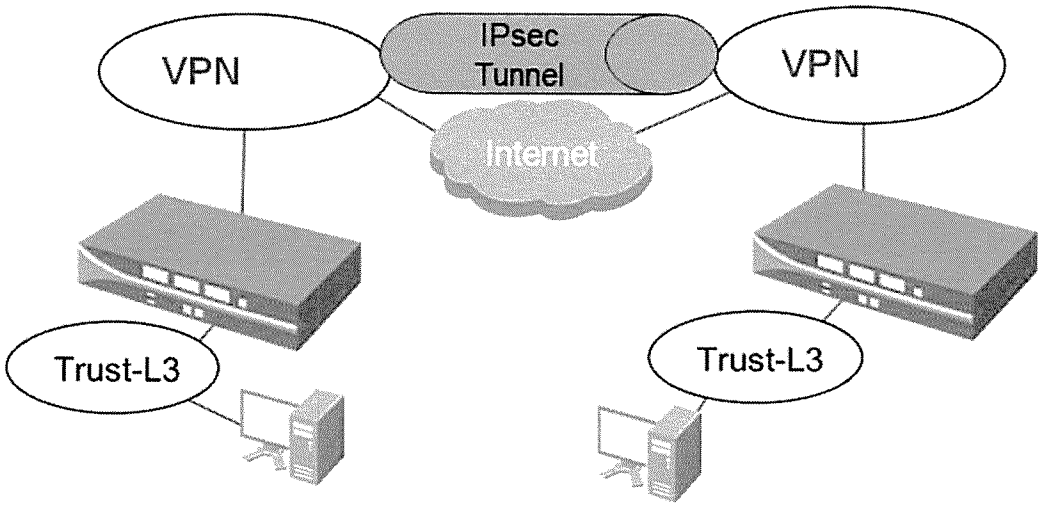
54. Close the PuTTY CLI.



Lab Scenario: Site-to-Site VPN

In this lab, you will:

- Configure an IPSec tunnel to another student firewall.



Your environment spans two physical locations. Management wants users at each site to be able to access both networks easily and securely. An IPSec VPN has been chosen for the connection between the two sites. Use a new VPN zone on the firewalls to create the connection. The tunnel endpoints must be in the VPN zone so that traffic passing through to the Trust-L3 zone can be examined and protected by the firewall. Clients in the Trust-L3 zone on either firewall must be able to initiate sessions to the other network. However, in-bound traffic from the VPN to the Trust-L3 zone should be allowed only from the other trusted network.

Lab Notes

Make sure that all traffic going to your partner's trusted network goes through the VPN and not just through the default gateway.

Lab Solution: Site-to-Site VPN

Prepare for the Lab

1. Find a partner and get their pod number. In the lab, use your partner's pod number any time you see a <Y>. You and your partner will work independently to configure each end of the VPN tunnel. Wait until both partners are finished before testing the connection.

Configure the Tunnel Interface

2. Go to the WebUI and select **Network > Interfaces**.

3. Click the **Tunnel** tab.

4. Click **Add** to configure a tunnel interface:

Interface Name	In the text box to the right of "tunnel:", enter `<Y>`
Comment	`Tunnel to <Y>`
Config tab	
Virtual Router	Select **Student-VR**
Security Zone	Create and assign a new Layer 3 Zone called `VPN`

5. Click **OK** to close the Tunnel Interface window.

Configure the IKE Gateway

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

7. Click **Add** to create the IKE gateway.

Name	Enter `pod-<Y>-IKE-GW`

Interface	Select **<Your External interface>**
Local IP Address	Select **<Your External IP Address with mask>**
Peer Type	Select **Static**
Peer IP Address	Enter **<Your partner's External IP address>**
Pre-shared Key	Enter `paloalto`
Confirm Pre-shared Key	Enter `paloalto`

8. Click **OK** to close the IKE Gateway window.

Create an IPSec Crypto Profile

9. Select **Network > Network Profiles > IPSec Crypto**.

10. Click **Add**. An IPSec Crypto Profile window opens.

Name	Enter `aes128sha256grp5`
IPSec Protocol	**ESP**
Encryption	**aes-256-gcm** **aes-192-cbc** **aes-128-cbc**
Authentication	**sha512** **sha384** **sha256**

DH Groups	**group 5**

11. Click **OK** to close the IPSec Crypto Profile window.

Configure the IPsec Tunnel

12. Select **Network > IPSec Tunnels**.

13. Click **Add** to define the IPSec tunnel:

Name	Enter `tunnel-to-<Y>`
Tunnel Interface	Select **tunnel.<Y>**
Type	Select **Auto Key**
IKE Gateway	Select **pod-<Y>-IKE-GW**
IPSec Crypto Profile	Select **aes128sha256grp5**

14. Click **OK** to close the IPSec Tunnel window.

Define the Route to the Network

15. Select **Network > Virtual Routers**.

16. Click **Student-VR** to open the Virtual Router window.

17. Click **Static Routes > IPv4**, then **Add** to add a new route:

Name	Enter `Route-to-<Y>`
Destination	Enter `<Your Partner's Internal network>` **NOTE**: This is the internal network behind your partner's firewall

Interface	Select **tunnel.Y**
Next Hop	**None**

18. Click **OK** twice to close the configuration windows.

Create a Security Policy Rule

19. Select **Policies > Security**.

20. Click **Add** to add a new Security policy rule.

General tab	
Name	Enter `VPN-traffic`
Rule Type	**universal**
Source tab	
Source Zone	Select **Add** and select **Trust-L3** Select **Add** and select **VPN**
Source Address	Click **Add** and enter `<Your partner's Internal network>` Click **Add** and enter `<Your Internal network>`
Destination tab	
Destination Zone	Click **Add** and select **Trust-L3** Click **Add** and select **VPN**.

Destination Address	Click **Add** and enter `<Your partner's Internal network>` Click **Add** and enter `<Your Internal network>`
Application tab	
Applications	Check the **Any** check box
Service/URL Category tab	
Service	Select **any** from the drop-down list
Actions tab	
Action Setting	Select **Allow**
Log Setting	Select **Log at Session End**

21. Click **OK** to close the Security Policy Configuration window.

22. Click the **Commit** link at the top right of the WebUI. Click **Commit** again. wait until the commit process is complete, then continue.

23. Wait for your partner to complete this lab to this point before proceeding.

Test Connectivity

24. In the WebUI, select **Network > IPSec Tunnels**. Notice that the Status lights on the VPN tunnel are red.

25. On the Windows desktop, open a command prompt and ping the internal interface of your partner's firewall. The ping should succeed.

```
ping <Your Partner's Internal IP address> -t
```

26. Refresh the **Network > IPSec Tunnels** page. The status lights are now green.

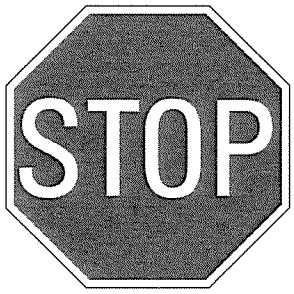
27. Select **Monitor > Traffic Logs**.

28. Filter for the ping application to see the logs for the ping traffic crossing the VPN.

29. Open PuTTy on the desktop and connect to the firewall.

30. In the PuTTy CLI, enter the following commands to display the status of the VPN tunnel. Note that the VPN tunnel will not be active until you send traffic over it.

```
show vpn ike-sa
show vpn ipsec-sa tunnel tunnel-to-<Y>
show vpn flow name tunnel-to-<Y>
show running tunnel flow
```



Lab Scenario: Management and Reporting

In this lab, you will:

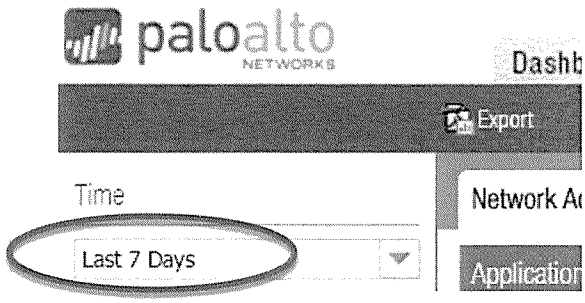
- Explore the Palo Alto Networks firewall dashboard
- Explore the logs
- Generate reports

Your manager wants to see daily reports that detail the threats encountered by the firewall. Configure a custom report to show a threat summary for all traffic allowed in the past seven days. It should include the threat name, the application (including technology and subcategory for reference), and the number of times that threat was encountered. Export the file as a PDF.

Lab Solution: Management and Reporting

Explore the Dashboard, ACC, App Scope, and Session Browser

1. In the WebUI, go to the **Dashboard**.
2. Review the contents of the available widgets. What information is available?
3. Go the **ACC** tab.
4. Change the Time period to the **Last 7 Days**.



5. Explore the information available on the **Network Activity** tab.
6. Explore the information available on the **Threat Activity** tab.
7. Explore the information available on the **Blocked Activity** tab.
8. Select **Monitor > App Scope > Summary**.
9. Explore the other branches underneath the App Scope tree. What information is available?
10. Click the **Session Browser** to see any current sessions.

Explore the Logs

11. Select **Monitor > Logs**, click each type of log, and examine the log activity.
12. Experiment with the filters to limit the log entries shown in the log files.

Create a Custom Report

13. Select **Monitor > Manage Custom Reports**.
14. Click **Add** to define a new custom threat report:

Name	Enter `Top Applications`
Database	Select **Summary Databases - Traffic**
Time Frame	Select **Last 7 Days**
Sort by	Select **Sessions** and **Top 10**
Group by	Select **Application** and **10 Groups**
Selected Columns	Populate the **Selected Columns** field with these values, in this order: ▪ **Application** ▪ **Sessions** ▪ **Bytes** ▪ **URLs** ▪ **Rule**

15. Click **OK** to save the Custom Report window.

16. Click the **Top Applications** report to reopen the Custom Report window.

17. Click **Run Now** to generate the report. The report will appear in a new tab in the window.

18. Close the small tab containing the report.

19. Click the **Report Setting** tab.

20. Create a query using the Query Builder:

Query Builder	Build a query using these parameters: ▪ Connector: Select **and**

	▪ Attribute: Select **Rule** ▪ Operator: Select **equal** ▪ Value: Enter `General Internet` ▪ Click **Add**. The text "(rule eq 'General Internet')" appears in the Query Builder box.

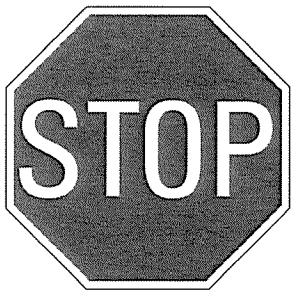
21. Extend the query using the Query Builder:

Query Builder	Build a query using these parameters: ▪ Connector: Select **or** ▪ Attribute: Select **Rule** ▪ Operator: Select **equal** ▪ Value: Enter `Web Traffic` ▪ Click **Add**. The text "or (rule eq 'Web Traffic')" is added to the query.

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

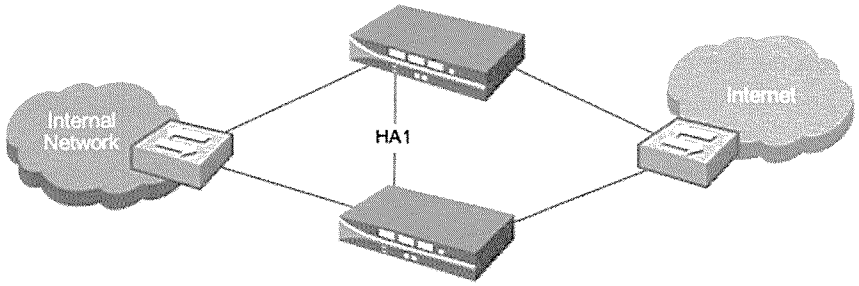
23. Click **Export to PDF** to save the report as a PDF. (You may need to disable your browser's pop-up blocker.)

24. Click **OK** to close the Custom Report window.



Lab Scenario: Active/Passive High Availability

In this lab, you will set up an active/passive high availability (HA) configuration.



To enable redundancy for the mission-critical connections provided by the firewall, you decide to implement active/passive HA. You will pair up with another firewall administrator to provide access for your users. The HA configuration should provide protection against upstream and downstream link failures. For example, the external network is considered down if the default gateway cannot be reached.

After HA is configured, test failover by suspending the primary device and verify that the other firewall becomes primary. Re-enable the suspended device and observe the results.

Lab Notes

The node with the lower priority number is designated as primary.

Lab Solution: Active/Passive High Availability

Lab Preparation

1. Confer with your partner and get their pod number. In the lab, replace the letter Y with your partner's pod number. The pod with the higher pod number (H) will be the passive firewall in the active/passive configuration. You and your partner will work independently to configure each firewall. Wait until both partners are finished before testing the configuration.

Save the Configuration

2. In the WebUI, select **Device > Setup > Operations**.

3. Click **Save named configuration** snapshot. A prompt opens.

4. Enter `pod<X>b4HA` and click **OK**.

5. Click **Close**.

Display the HA Widget

6. Click the **Dashboard** tab to display current firewall information.

7. If the High Availability panel is not displayed, select **Widgets > System > High Availability** to enable the display.

Configure the Firewall for HA Setup

8. Go the WebUI and select **Network > Interfaces > Ethernet**.

9. Select **<Control Link HA1>** to open the configuration window for that interface.

10. Set the Interface Type to **HA** and click **OK**.

Configure Active/Passive HA

11. Select **Device > High Availability > General**.

12. Click **the button in the upper-right corner** of the Setup panel to configure HA:

Enable HA	Check the check box

Group ID	`<Group ID Number>`
Mode	Verify that **Active Passive** is selected
Enable Config Sync	Verify that the check box is checked
Peer HA1 IP Address	Enter `<Your Partner's HA1 IP address>`
Backup Peer HA1 IP Address	Enter `<Your Partner's Mgt IP address>`

13. Click **OK** to close the Setup window.

14. Open the Active/Passive Settings window.

15. Select the **Auto radio button**, and click **OK**.

16. Open the Election Settings panel to configure failover behavior:

Device Priority	`X`
Preemptive	Check the check box
Heartbeat Backup	Uncheck the check box

17. Click **OK** to close the Setup window.

18. Click the **button in the upper-right corner** of the Control Link (HA1) panel to configure the HA1 link:

Port	Select **<Control Link HA1>**
IP address	Enter **<Your HA1 IP address>**
Netmask	Enter `255.255.255.0`

19. Click **OK** to close the window.

20. Open the Control Link (HA1 Backup) window

21. Under Port, select **management (Dedicated management port as HA1 interface)**.

22. Click **OK**.

23. You are not using a dedicated HA2 interface, so open the **Data Link (HA2)** window and make sure that Enable Session Synchronization is unchecked.

24. Click **OK** to close the window.

Configure HA Monitoring

25. Select **Device > High Availability > Link and Path Monitoring**.

26. Click the **button in the upper-right corner** of the Link Monitoring panel to configure link failure detection:

Enabled	Checked
Failure Condition	Select **any**

27. Click **OK** to close the window.

28. Click **Add** in the Link Group panel to configure the traffic links to monitor:

Name	Enter `Traffic-links`
Enabled	Checked
Failure Condition	Select **any**
Interface	Click **Add** and select **<Traffic Link 1>** Click **Add** and select **<Traffic Link 2>**

29. Click **OK** to close the window.

30. Open the **Path Monitoring** panel to configure the Path Failure detection.

Enabled	Checked
Failure Condition	Select **any**

31. Click **OK** to close the window.

32. Find the Path Group panel and click **Add Virtual Router Path** to configure the path failure condition:

Name	Select **Student-VR**
Enabled	Checked
Failure Condition	Select **any**
Destination IP	Click **Add** and enter `<Destination IP>`

33. Click **OK** to close the window.

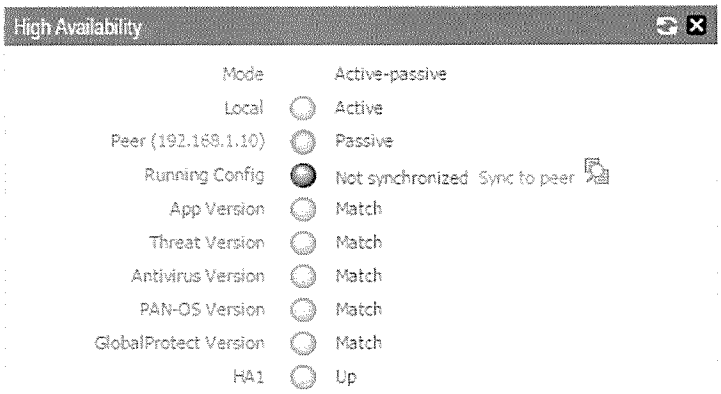
34. Click the **Commit** link at the top right of the WebUI. Click **Commit** again, wait until the commit process is complete, then continue.

Verify the HA Configuration

Note: Both partners must have completed all preceding steps before continuing.

35. Click the **Dashboard** tab and display the **High Availability** status widget on the WebUIs for both firewalls.

36. In the High Availability widget, the Mode should be Active/Passive. A local and peer machine should be listed, with a green status indicator next to the Active machine and a yellow status indicator next to the Passive machine.



37. Determine which of your team's firewalls is the primary device. The lower number pod firewall should be the primary device because you set the device priority on the firewalls to match the pod numbers.

38. The HA1 status indicator should be green. If not, refresh the HA widget to update the display.

39. The Running Config status indicator should not be green. As a safety precaution, HA does not sync the configurations, which allows the administrator to ensure that the correct configurations are pushed and overwritten by selecting which peer to sync.

40. Do *not* sync the configurations at this time, unless your instructor asks you to.

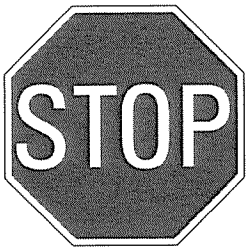
41. To verify that the secondary device will assume primary status in a failure, on the primary device select **Device > High Availability > Operational Commands > Suspend Local Device**.

42. Click **OK**.

43. Return to the **Dashboard** tab on both firewalls and verify that the status has updated for each firewall. You may need to refresh the display by clicking the circular arrow button next to the Help icon in the upper-right corner of the WebUI.

44. To re-enable the suspended firewall, on the lower numbered device select **Device > High Availability > Operational Commands** and make the local device functional.

45. Return to the **Dashboard** tab on both firewalls. After some time, the lower-numbered firewall becomes the primary firewall again.


STOP