PALO ALTO NETWORKS – EDU 210

Lab 1: Connect to the Management Network

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Connect to the Management Network 6
1.1 Load Lab Configuration 6
1.2 Configure the Update Server and DNS Server 11
1.3 Configure General Settings of the Firewall 13
1.4 Modify the Management Interface 14
1.5 Check for New PAN-OS Software 16

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Your organization has just received a new Palo Alto Networks firewall, and you have been tasked with deploying it. The first steps will be to connect to the firewall's management interface address and configure basic settings to provide the firewall with network access.

In this lab, you will connect to the Palo Alto Networks firewall management interface and configure basic settings to provide the firewall with network access.

Objective

In this lab, you will perform the following tasks:

- Connect to the firewall web interface
- Load a starting lab configuration
- Set DNS servers for the firewall
- Set NTP servers for the firewall
- Configure a login banner for the firewall
- Configure permitted IP addresses for the firewall management
- Check for new PAN-OS software

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Connect to the Management Network

1.1 Load Lab Configuration

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-01.xml** from the *Name* dropdown box and click **OK**.

9. In *the Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.2 Configure the Update Server and DNS Server

In this section, you will configure the DNS and Update Server settings. 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. In the web interface, select **Device > Setup > Services**. Click the **Services gear** icon to open the *Services* window.

2. In the *Services* window, verify that the *Update Server* is set to **`updates.paloaltonetworks.com`**. Set the *Primary DNS Server* to **`8.8.8.8`** and the *Secondary DNS Server* to **`192.168.50.53`**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Select the **NTP** tab. Set the *Primary NTP Server* to **`0.pool.ntp.org`** and the *Secondary NTP Server* to **`1.pool.ntp.org`**. Click **OK**.

4. Verify the settings have been updated in the *Services* window.

5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Configure General Settings of the Firewall

In this section, you will configure the general settings of the Palo Alto Networks Firewall. You will verify the Domain, set your location's time zone, and set a login banner.

1. Navigate **Device > Setup > Management**. Click on the **General Settings gear** icon to open the *General Settings* window.

2. In the *General Settings* window, verify the *Domain* listed is **lab.local**. For the *Login Banner*, enter **`Authorized Access Only`**. Choose the *Time Zone* of your location. For this lab, we chose to use **Etc/UTC** as the *Time Zone*. Click **OK**.

3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.4 Modify the Management Interface

In this section, you will modify the management interface of the firewall.

1. Navigate to **Device > Setup > Interfaces** and click on interface name **Management**.

2. In the *Management Interface Settings* window, verify **`192.168.1.254`** for the *IP Address*, **`255.255.255.0`** for the *Netmask*, and **`192.168.1.1`** for the *Default Gateway*. At the bottom of the *Permitted IP Addresses* area, click **Add.**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the *Permitted IP Addresses*, type **`192.168.1.20/24`** for the *IP Address* and **`MGT access from this host only`** for the *description*. Click **OK**.

4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Check for New PAN-OS Software

In this section, you will check for new PAN-OS software and commit your changes.

1. In the *PA-VM* web interface, navigate to **Device > Software**. If needed, use the scroll bar to find Software.

2. In the *Software* window, click **Check Now** in the bottom-left corner.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. The Palo Alto Networks Firewall will complete a *software check*. Monitor the *software check,* and when the process is complete, the firewall will display an updated list of available software.

VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
10.1.1	297 MB	2021/07/21 09:33:46			Download
10.1.0	917 MB	2021/06/02 08:16:22			Download
10.0.6	441 MB	2021/05/12 09:48:56			Download
10.0.5	440 MB	2021/03/25 10:41:47			Download
10.0.4	431 MB	2021/02/01 17:09:54			Download
10.0.3	431 MB	2020/12/09 19:38:09			Download
10.0.2	430 MB	2020/10/28 11:33:33			Download
10.0.1	332 MB	2020/09/03 09:32:34			Download
10.0.0	806 MB	2020/07/16 20:15:10	✓	✓	Reinstall
9.1.10	398 MB	2021/06/10 11:28:23			Download

The list you see will vary from this example. Also, newer versions of PAN-OS software may be available at the time you carry out these steps. Do not upgrade your firewall.

4. Commit your changes to the firewall by clicking the **Commit** button at the upper-right of the *PA-VM* web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Commit* window, view the commit scope. Click **Commit**.

6. Wait until the *Commit* process is complete. Click **Close**.

7. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 2: Working with Firewall Configurations and Log Files

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Working with Firewall Configurations and Log Files 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Save a Named Configuration Snapshot 11
1.3 Export a Named Configuration Snapshot 12
1.4 Revert Ongoing Configuration Changes 14
1.5 Preview Configuration Changes 17
1.6 Examine Log Files 21
1.7 Create a Log File Filter 24
1.8 Use the Filter Builder 28

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Now that you have set up the firewall to allow management access, you need to make certain that you can save, load, and restore configurations to the device. You also need to familiarize yourself with the log files available and with searching through the logs to find specific events.

In this lab, you will work with snapshots, revert and preview configuration changes, examine log files, and create and use the filter builder.

Objective

In this lab, you will perform the following tasks:

- Load a starting lab configuration
- Save a named configuration snapshot
- Export a named configuration snapshot
- Save ongoing configuration changes before a commit
- Revert ongoing configuration changes
- Preview configuration changes
- Examine log files
- Create a log file filter
- Use the Filter Builder

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Working with Firewall Configurations and Log Files

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-02.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.2 Save a Named Configuration Snapshot

In this section, you will save the firewall configuration with a specific filename.

1. In the web interface, select **Device > Setup > Operations**. Click **Save named configuration snapshot**.

2. In the *Save Named Configuration* window, enter **`firewall-a-lab2`**. Click **OK**.

3. In the *Confirmation* window, click **Close**.

> Note that this process saved the configuration file to a location on the firewall itself.

4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Export a Named Configuration Snapshot

In this section, you will export the saved configuration file firewall-a-lab2 from the firewall to your workstation.

1. Under **Device > Setup > Operations > Configuration Management,** click the link for **Export named configuration snapshot**.

2. In the *Export Named Configuration* window, use the dropdown list and select the **firewall-a-lab2** configuration file. Click **OK**.

3. On the client taskbar, click the **Minimize all open windows and show the desktop** icon.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. On the *client desktop*, open the **Downloads** folder. Verify the saved file **firewall-a-lab2** appears in the folder. Close the *Downloads* folder by clicking the **X** icon.

5. Reopen the firewall web interface by clicking on the **Chromium** icon in the taskbar.

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.4 Revert Ongoing Configuration Changes

As you work on a firewall configuration, it is theoretically possible to make a mistake. In such a situation, you may not remember exactly which changes you have made or where the mistake exists in the configuration, particularly if you have made multiple changes (or multiple mistakes). Fortunately, you can revert the firewall to the current running configuration. This process essentially erases any of the changes you had made to the working configuration and puts the firewall back at the starting point before you made changes.

In this section, you will change the IP address for one of the firewall's DNS servers. You will then use Revert Changes to reset the firewall to the running configuration and remove the mistake.

1. In the firewall web interface, select **Device > Setup > Services**. Edit the *Services* section by clicking the **Services gear** icon.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Services* window, change the value for the *Primary DNS Server* to **`88.8.8.8`** (an easy mistake to make)**.** Click **OK.**

3. Verify the mistake is showing in the *Services* window for the **Primary DNS Server**.

4. In the upper-right corner of the *PA-VM* web interface, click the **Changes** button and select **Revert Changes.**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Revert Changes* window, leave the settings unchanged. Click **Revert**.

The Revert Changes window allows you to select specific elements of the configuration that you can revert. In this case, because you only made a single change, the Revert Scope shows device-and-network (which is the portion of the configuration that contains the changes to the DNS server).

6. In the *Message* window, click **Close**.

7. In the *Services* window, notice that the **Primary DNS Server** has been reset to the original value before you mistakenly changed it.

8. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Preview Configuration Changes

Before you commit changes to the firewall, you can compare the impending changes with the current configuration settings. This process can be useful to make certain you have the right changes in place before they are implemented on the firewall.

In this section, you will make a minor modification to the firewall and use **Preview Changes** to compare the candidate config to the running config.

1. Modify the SNMP configuration by going to **Device > Setup > Operations** and clicking **SNMP Setup** under the *Miscellaneous* section.

2. In the *SNMP Setup* window, change the *Physical Location* to **`Santa Clara, CA, USA`** for *Contact*, enter **`Unit 42`**, for *SNMP Community String*, enter **`paloalto42`**. Click **`OK`**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Commit your changes to the firewall by clicking the **Commit** button at the upper-right of the *PA-VM* web interface.

4. In the *Commit* window, click **Preview Changes**.

5. In the *Preview Changes* window, leave the *Lines of Context* set to **10**. Click **OK**.

The Lines of Context setting determines how many lines are displayed before a change and after a change in the configuration file.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. A new browser window named *Device Config Audit* will appear that displays a side-by-side comparison of the current *running configuration* (on the left) and the proposed changes in the *candidate configuration* (on the right). Review the snmp settings that were changed.

Changes are color coded. Green indicates new elements that have been added. Yellow indicates existing elements that have been modified. Red indicates existing elements that have been deleted.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Close the *Device Config Audit* window by clicking the **X** in the upper right corner.

8. Click **Cancel** in the *Commit* window.

9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 Examine Log Files

Although the information in log files varies, the process of examining and searching log files on the firewall is the same.

In this section, you will examine and navigate the firewall System log. You can later apply the same tasks and techniques while examining any other log file on the firewall, such as the Traffic or Threat logs.

1. In the *PA-VM* firewall interface, select **Monitor > Logs > System**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *System Logs* windows, hide the **Object** column by clicking the small **dropdown arrow** in the right portion of any column header. Notice that before unchecking **Object**, it appears in the *System Logs* window.

3. Uncheck **Object** and notice the *Object* column is now hidden.

Hiding and displaying log columns is optional but quite useful. Each log file contains different columns, some of which you may not need so you can hide them. There may be columns in certain log tables that are not shown by default, and you can use this process to display hidden columns that you want to view.

4. Drag and drop the **Severity** column to the left-most position in the table by holding down the *left mouse* button.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. The table now displays **Severity** as the first column.

Reordering columns is also optional; however, you may discover that the information in a specific log file is easier for you to analyze after you customize the columns.

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.7 Create a Log File Filter

Scanning through log files row-by-row is tedious. If you are looking for specific information, you can create filters quickly to display only entries that match certain criteria. All log files support filters.

In this section, you will examine and navigate the firewall System **l**og. You can later apply the same tasks and techniques while examining any other log file on the firewall, such as the Traffic or Threat logs.

1. In the PA-VM firewall interface, select **Monitor > Logs > System**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *System log* file, notice the filter **(subtype eq vpn)**. Delete the filter by clicking on the **X** *(Clear Filter)* button.

3. In the *System log* file, click any entry under the *Severity* column that contains **informational**. Click **informational**.

4. The web interface will automatically build a filter statement with the appropriate syntax to search for all entries that contain **informational** in the *Severity* field. Click the **Apply Filter** button in the upper-right of the window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. The System log display will update to show only those entries that contain **informational** as the *Severity* level.

6. Under the *Event* column, click any entry that contains the word **general**. Click **general**.

7. Notice the interface will update the syntax to create a combined filter.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Click the **Apply Filter** button. The interface will update the log file to display only those entries that match both conditions.

9. Remove the filter by clicking the **Clear Filter** button in the upper-right corner of the window.

A good practice is to clear any filters from log file displays before you move to other portions of the web interface. The next time you examine the same log, it will display all results instead of only ones you have previously filtered.

10. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.8 Use the Filter Builder

Clicking the link for a specific entry in a log file will automatically create a simple filter. You can create more complex filters by clicking multiple conditions; however, there are some situations in which this process will not provide you with the kind of criteria you need to complete a search. For long or sophisticated searches, you can use the Filter Builder.

In this section, you will use the Filter Builder to search the System log for all entries that have occurred in the last 60 minutes.

1. In the *PA-VM* web interface, select the **Dashboard** tab. Under the *General Information* section, scroll to the bottom and locate the **Time.** Make a note of the date and time displayed (you will need this information in a later step).

Please Note

For this lab, notice the time of 03:22:17. The times you see will vary.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Select **Monitor > Logs > System.** Verify you do not have any filters present. If you have a filter present, click the **Clear Filter** button in the upper-right corner of the *System Logs* window.

3. Click the **Add Filter** button in the upper-right corner of the *System Logs* window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Add Log Filter* window, fill in the following information below.

   A. Under the *Connector* column, click **and.**
   B. Under the *Attribute* column, click **Severity.**
   C. Under the *Operator* column, click **equal.**
   D. Under the *Value* column, click **informational.**
   E. Click **Add.**
   F. Note that the filter field at the top of the window updates to display the correct syntax for this filter

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. With the *Add Log Filter* window open, build the second part of the filter.

   A. Under the *Connector* column, select **and.**
   B. Under the *Attribute* column, select **Time Generated.**
   C. Under *Operator*, select **greater than or equal to.**
   D. Under the *Value* column, use the first dropdown list to select the date you recorded in step 1.
   E. Under the *Value* column, use the second dropdown list to select a time approximately sixty minutes prior to the time you recorded in step 1 (round up or down if you need to).
   F. Click **Add.**
   G. Note that the filter is updated to reflect the additional syntax.

Please Note

For this lab example, you notice the time that was recorded will be 03:22:17. When you round down, the value to record will be 02:30:00. The time and date for your filter will differ from the example shown here.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. In the *Add Log Filter* window, click **Apply**.

7. Your filter will appear in the System log syntax field. Remember, your *time* will be different than this lab example.

8. Click the **Apply Filter** button in the upper-right corner of the window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. The *System log* display will update to show you only entries that have been generated after the time you specified for this lab. For this lab, we waited some time and went to the very last page, which was page 10. Page 10 shows you the first entry after the time that was specified in the filter creation.

Please Note

Although you used the System log as the basis for this exercise, the process of creating filters is the same throughout all Palo Alto Networks firewall log files. The Filter Builder also is available to use in all log file tables.

The number of pages you will see may vary based on the amount of time you allow. For this step, you will notice we waited to allow for 10 pages of logs to show.

10. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 3: Working with Firewall Administrator Accounts

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Working with Firewall Configurations and Log Files 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Create a Local Database Authentication Profile 11
1.3 Create a Local User Database Account 13
1.4 Create an Administrator Account 14
1.5 Configure LDAP Authentication 21
1.6 Configure RADIUS Authentication 32
1.7 Configure and Authentication Sequence 41

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

When you deploy the firewall into your production network, you need to make sure that other members of your team have administrative access to the device. You want to leverage an existing LDAP server that maintains account and password information for members of your team. However, your organization recently merged with another company whose administrative accounts are maintained in a RADIUS database.

No one has had time yet to migrate all the accounts from RADIUS into LDAP, so you need to configure the firewall to check both LDAP and RADIUS to authenticate an account when an administrator logs in.

In this lab, you will provide management with those types of reports and to be able to restrict the applications.

Objective

In this lab, you will perform the following tasks:

- Create a local firewall administrator account
- Configure an LDAP Server Profile
- Configure a RADIUS Server Profile
- Configure an LDAP Authentication Profile
- Configure a RADIUS Authentication Profile
- Configure an Authentication Sequence
- Create non-local firewall administrator accounts

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Working with Firewall Configurations and Log Files

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-03.xml** from the *Name* dropdown box and click **OK**.

9. In the Loading Configuration window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.2 Create a Local Database Authentication Profile

In this section, you will create a local database authentication profile. Local database profiles allow the firewall to authenticate administrators who need access to the firewall web interface through Captive Portal or GlobalProtect.

1. In the *PA-VM* web interface, navigate to **Device > Authentication Profile**. Click **Add** at the bottom of the window.

2. In the *Authentication Profile* window, under the *Authentication* tab, enter **`Local-Database`** for the *Name***,** for *Type*, use the dropdown list to select **Local Database,** select the tab for **Advanced.**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. On the *Advanced* tab, in the *Allow List* section, click **Add**. Select **All** and click **OK**.

4. Leave the firewall web interface open to continue with the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Create a Local User Database Account

In this section, you will create a new entry in the Local User Database on the firewall. This entry will be for a new team member, **adminBob**.

1. In the web interface, select **Device > Local Users Database > Users**. In the bottom-left corner of the window, click **Add**. You may need to use the scroll bar to locate the Local User Database dropdown.

2. In the *Local User* window, type **`adminBob`** for the *Name* field. Enter **`Pal0Alt0!`** for *Password* and *Confirm Password*. Click **OK**.

3. Leave the firewall web interface open to continue with the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.4 Create an Administrator Account

In this task, you will create an administrator account for adminBob. The adminBob account will use the Local-Database Authentication Profile.

1. In the web interface, select **Device > Administrators**. Click **Add** at the bottom of the window.

2. In the *Administrator* window, enter **`adminBob`** for the *Name*. For the *Authentication Profile*, select **Local-Database**. Click **OK**.

Please Note

Note that when you select Local-database for the Authentication Profile, there is no option to enter a Password for the administrator. The password information for this account is maintained in the Local-database on the firewall.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **Commit** button at the upper-right of the *PA-VM* web interface.

4. In the *Commit* window, click **Commit** to proceed with committing the changes.

5. In the *Commit Status* window, click **Close**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Log out of the firewall web interface by clicking the **Logout** button in the bottom-left corner of the window.

7. In the *Log In* window, click **Log In**.

8. Log back into the firewall as username **`adminBob`**, password **`Pal0Alt0!`**. Click **Log In**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. In the *Welcome* window, click **Close**.

10. In the *Telemetry Data Collection* window, click **Remind Me Later**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. Select **Monitor > System**. Look for an entry with **Type > Auth**. You may need to scroll through the logs to find the auth type.

Note that the entry in the firewall system log indicates that adminBob was successfully authenticated against the **Local-Database.**

If you do not see an entry in the System log indicating a successful authentication for adminBob, you can use a filter (subtype eq auth) as the syntax.

12. Log out of the firewall.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. In the *Log In* window, click **Log In**.

14. Log back into the firewall with the **`admin/Pal0Alt0!`** credentials.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

15. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.

16. Leave the firewall web interface open to continue with the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Configure LDAP Authentication

Your organization uses an LDAP server to maintain a database of users, including network administrators. Your team of security personnel is growing each month, and you want to leverage the existing LDAP server to authenticate administrators when they attempt to log into the firewall.

The first step in this process is to define an LDAP server profile that contains specific information that the firewall can use when sending queries for authentication.

1. Minimize the PA-VM web interface.

2. On the client desktop, open the **Lab-Files** folder.

3. In the *Lab-Files* folder, open the **Class-Scripts**.

4. In the *Class-Scripts* folder, open the **EDU-210** folder.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Execute the *User-ID Data* script by **double-clicking** it.

6. Notice the *Terminal* window will pop up. **Minimize** the terminal window and let it run for the remainder of the lab.

7. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the taskbar.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the web interface, select **Device > Server Profiles > LDAP**. At the bottom of the window, click **Add**.

9. In the *LDAP Server Profile* window, enter **`LDAP Server Profile`** for the *Profile Name*. Under the *Server List*, click **Add**. Enter **`ldap.panw.lab`** for the *Name*, **`192.168.50.89`** for the *LDAP Server*, and confirm **389** populates or the *Port* number.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. In the *Server Settings* section, Enter **`dc=panw,dc=lab`** for *Base DN*, enter **`cn=admin,dc=panw,dc=lab`** for *Bind DN*, enter **`Pal0Alt0!`** for *Password* and *Confirm Password* and uncheck **Require SSL/TLS secured connection**. Click **OK**.

Please Note

With your LDAP Server Profile in place, you will now create an Authentication Profile and reference the LDAP Server Profile you just created.

11. Verify the *LDAP Server Profile* is now showing in the *LDAP Profile* list.

NAME	LOCATION	SERVERS	OTHERS
LDAP Server Profile		Name: ldap.panw.lab LDAP Server: 192.168.50.89 Port: 389	Base: dc=panw,dc=lab Bind DN: cn=admin,dc=panw,dc=lab

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Select **Device > Authentication Profile**. Click **Add**.

13. In the *Authentication Profile* window, type **`LDAP Auth Profile`** for the *Name*. Select **LDAP** for the *Type* and **LDAP Server Profile** for the *Server Profile*. Click **Advanced**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. On the *Advanced* tab, in the *Allow List,* click **Add**. Select **all** and click **OK**.

15. Navigate to **Device > Administrators** and click **Add**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

16. In the *Administrator* window, type **`adminSally`** for the *Name*. Select **LDAP Auth Profile** for the *Authentication Profile*. Click **OK**.

Please Note

The adminSally account is one which exists in the LDAP server.

17. Click the **Commit** link located at the top-right of the web interface.

18. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

19. When the *Commit* operation successfully completes, click **Close** to continue.

20. Log out of the firewall web interface by clicking the **Logout** button in the bottom-left corner of the window.

21. In the *Log In* window, click **Log In**.

22. Log back into the firewall as username **`adminSally`**, password **`Pal0Alt0!`**. Click **Log In**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

23. In the *Welcome* window, click **Close**.

24. In the *Telemetry Data Collection* window, click **Remind Me Later**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

25. Select **Monitor > System**. Look for an entry with **Type > Auth**. You may need to scroll through the logs to find the *auth* type.

Please Note

Note that the entry in the firewall system log indicates that adminSally was successfully authenticated against the **LDAP Server.**

If you do not see an entry in the System log indicating a successful authentication for adminSally, you can use a filter (subtype eq auth) as the syntax.

26. Log out of the firewall.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

27. In the *Log In* window, click **Log In**.

28. Log back into the firewall with the **`admin/Pal0Alt0!`** credentials.

29. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.

30. Leave the firewall web interface open to continue with the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 Configure RADIUS Authentication

Your organization has recently acquired another company. The newly acquired company maintains all network administrator accounts in a RADIUS server. You need to incorporate RADIUS authentication for the firewall so the new network administrators who have joined your team can access the firewall for management purposes.

For this section, you will configure RADIUS Authentication and test that the user adminHelga can log in.

1. Navigate to **Device > Server Profiles > RADIUS.** Click **Add.**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *RADIUS Server Profile* window, enter **`RADIUS Server Profile`** for the *Profile Name*. For the *Authentication Protocol*, select **CHAP**. Under the *Servers* section, click **Add.** For the server *Name* field, enter **`radius.panw.lab`.** For the *RADIUS Server* field, enter **`192.168.50.150`.** Enter **`Pal0Alt0!`** for *Secret* and *Confirm Secret***.** Leave the *Port* set to **1812.** Click **OK.**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Navigate to **Device > Authentication** Profile. Click **Add**.

4. In the *Authentication Profile* window, enter **`RADIUS Auth Profile`** for the *Profile Name*. For the *Type*, select **RADIUS**. For the *Server Profile*, select **RADIUS Server Profile**. Click the **Advanced** tab.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Under the *Allow List,* click **Add**. Select **all** and click **OK**.

6. To test *RADIUS Authentication*, create an *administrator* account named **adminHelga** by selecting **Device > Administrators**. Click **Add**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the *Administrator* window, enter **`adminHelga`** for the *Name*. For the *Authentication Profile*, select **RADIUS Auth Profile**. Click **OK**.

8. Click the **Commit** link located at the top-right of the web interface.

9. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. When the *Commit* operation successfully completes, click **Close** to continue.

11. Log out of the firewall web interface by clicking the **Logout** button in the bottom-left corner of the window.

12. In the *Log In* window, click **Log In**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. Log back into the firewall as username **`adminHelga`**, password **`Pal0Alt0!`**. Click **Log In**.

14. In the *Welcome* window, click **Close**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

15. In the *Telemetry Data Collection* window, click **Remind Me Later**.

16. Select **Monitor > System**. Look for an entry with **Type > Auth**. You may need to scroll through the logs to find the *auth* type.

Please Note

Note that the entry in the firewall system log indicates that adminHelga was successfully authenticated against the **RADIUS Profile.**

If you do not see an entry in the System log indicating a successful authentication for adminHelga, you can use a filter (subtype eq auth)

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

17. Log out of the firewall.

18. In the *Log In* window, click **Log In**.

19. Log back into the firewall with the **`admin/Pal0Alt0!`** credentials.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

20. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.

21. Leave the firewall web interface open to continue with the next task.

1.7 Configure and Authentication Sequence

Since the acquisition, some administrator accounts exist in LDAP, and other accounts exist in RADIUS. With administrator accounts in these two different systems, you need to configure the firewall so that it can check both external databases when an administrator attempts to log in.

In this section, you will accomplish this by creating an Authentication Sequence. The sequence will instruct the firewall to check an account against LDAP first and then against RADIUS if the account does not exist in LDAP (or if the LDAP server is unavailable).

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Navigate to **Device > Authentication Sequence.** Click **Add**.

2. In the *Authentication Sequence* window, type **`LDAP then RADIUS`** for the *Name*. Under the *Authentication Profiles*, click **Add**. Select **LDAP Auth Profile**. Click **Add** again and select **RADIUS Auth Profile**. Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Note the Move Up and Move Down buttons. These allow you to change the order of the Authentication Profiles, if necessary. In this example, the firewall will use the LDAP-Auth-Profile first when an administrator logs in to attempt authentication; if the user account does not exist in LDAP (or if the LDAP server is unavailable), the firewall will use the RADIUS-Auth-Profile to attempt authentication.

3. Click the **Commit** link located at the top-right of the web interface.

4. In the *Commit* window, click **Commit** to proceed with committing the changes.

5. When the *Commit* operation successfully completes, click **Close** to continue.

6. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 4: Connecting the Firewall to Production Networks

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Working with Firewall Configurations and Log Files 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Create Layer 3 Network Interfaces 10
1.3 Create a Virtual Router 16
1.4 Segment Your Production Network Using Security Zones 19
1.5 Test Connectivity to Each Zone 24
1.6 Test Interface Access before Management Profiles 28
1.7 Define Interface Management Profiles 29
1.8 Test Interface Access after Management Profiles 38

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

In preparation for deployment, you need to connect the firewall to the appropriate production networks. You already have cabled the firewall interfaces to the appropriate switch ports in the data center. You will configure the firewall with Layer 3 IP addresses and a virtual router. You also will create security zones that divide your network into separate logical areas so that you have more control over traffic from one segment to another.

When you have the configuration in place on the firewall, you will use ping from different devices to verify connectivity between all the segments.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Create Layer 3 interfaces
- Create a virtual router
- Segment your production network using security zones
- Test connectivity from firewall to hosts in each security zone
- Create Interface Management Profiles

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Working with Firewall Configurations and Log Files

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-04.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Create Layer 3 Network Interfaces

In this section, you will create Layer 3 interfaces on the firewall that will provide basic network connectivity to your production networks. You have a network with users (192.168.1.0/24), a network with production servers (192.168.50.0/24) and a network connecting the firewall to an upstream internet router (203.0.113.0/24).

1. In the web interface, select **Network > Interfaces > Ethernet**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Click **ethernet1/1** to configure the interface.

3. Notice the *Ethernet Interface* window appears. Configure the following:

Parameter	Value
Comment	`Internet Connection`
Interface Type	**Layer3**
Virtual Router	**None**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Select the tab for **IPv4**. Leave the *Type* set to **Static,** Under the *IP* heading, click **Add.** Enter **`203.0.113.20/24`.** Click **OK**.

5. Click **ethernet1/2** to configure the interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Notice the *Ethernet Interface* window appears. Configure the following:

Parameter	Value
Comment	**`Users network connection`**
Interface Type	**Layer3**
Virtual Router	**None**

7. Select the tab for **IPv4**. Leave the *Type* set to **Static,** Under the *IP* heading, click **Add.** Enter **`192.168.1.1/24`.** Click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Click **ethernet1/3** to configure the interface.

9. Notice the *Ethernet Interface* window appears. Configure the following:

Parameter	Value
Comment	**`Extranet servers connection`**
Interface Type	**Layer3**
Virtual Router	**None**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. Select the tab for **IPv4**. Leave the *Type* set to **Static,** Under the *IP* heading, click **Add.** Enter **`192.168.50.1/24`.** Click **OK**.

11. When complete, your *Ethernet* table will have three entries. Confirm that *Ethernets 1/1, 1/2,* and *1/3* are showing as seen below.

12. Leave the web interface open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Create a Virtual Router

In this section, you will create a virtual router and connect your Layer 3 interfaces to it. You also will define a default gateway for the virtual router itself.

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. The firewall has a predefined virtual router named default.

A virtual router is a separate routing instance that allows the firewall to route traffic from one network to another through its Layer 3 interfaces. In this environment, we have three networks - 192.168.1.0/24, 192.168.50.0/24, and 203.0.113.0/24. You will modify the default virtual router and add the firewall's interfaces from each of these networks to the virtual router.

Because we are using Layer 3 interfaces, the firewall must have a way to route traffic from one network to another; this process is done with a virtual router. However, because each interface is in a different security zone, the Security rules will prevent traffic in one network from going to another network through the firewall

1. In the web interface, select **Network > Virtual Routers**.

2. Click **default** to open the default router.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the *Virtual Router - default* window, rename the default router to **`lab-vr`**. Click **Add** to add the following interfaces: **ethernet1/1**, **ethernet1/2**, and **ethernet1/3**.

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

Please Note

The order in which you add these interfaces to the list is not important. You could start by adding ethernet1/3 and the result will be the same. You are simply adding the appropriate interfaces to this virtual router.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Virtual Router - default* window, click the link on the side for **Static Routes**. Under the tab for **IPv4**, click **Add** at the bottom of the window.

5. In the *Virtual Router – Static Route - IPv4* window, for *Name*, enter **`Firewall Default Gateway`**, for *Destination*, enter **`0.0.0.0/0`**, for *Interface*, select **ethernet1/1,** for the *Next Hop* address, enter **`203.0.113.1`**. Leave the remaining settings unchanged. Click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

This entry is the default route for the firewall. Like all other network hosts, the firewall needs a default gateway to send traffic to unknown networks. The firewall has local connections to 192.168.1.0, 192.168.50.0 and 203.0.113.0 networks, so it can forward packets to hosts on those networks directly. However, for any other destination IP addresses (such as 8.8.8.8 for DNS), this route statement instructs the firewall to forward packets to 203.0.113.1, which is the internet.

6. In the *Virtual Router – default* window, click **OK.**

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Segment Your Production Network Using Security Zones

Security zones are a logical way to group physical and virtual interfaces on the firewall 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.

With your network interfaces and virtual router in place, you can now create security zones. You will create three security zones.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, select **Network > Zones**.

2. Click **Add** to create a new zone**.**

3. In the *Zone* window, enter **`Internet`** for the *Name*, for *Type*, select **Layer3**. Under the *Interfaces* section, click **Add**. Select **Ethernet 1/1** and leave all other settings unchanged. Click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Click **Add** to create a new zone**.**

5. In the *Zone* window, enter **Users Net** for the *Name*, for *Type*, select **Layer3**. Under the *Interfaces* section, click **Add**. Select **Ethernet 1/2** and leave all other settings unchanged. Click **OK**.

6. Click **Add** to create a new zone**.**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the *Zone* window, enter **`Extra Net`** for the *Name*, for *Type*, select **Layer3**. Under the *Interfaces* section, click **Add**. Select **Ethernet 1/3** and leave all other settings unchanged. Click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. You should now have three security zones.

9. Click the **Commit** button at the upper right of the *PA-VM* web interface.

10. In the *Commit* window, click **Commit**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Commit Status* window, click **Close**.

12. Minimize the *PA-VM* firewall by clicking the **minimize** icon in the upper right of the web interface and continue to the next task.

1.5 Test Connectivity to Each Zone

In this section, you will verify network connectivity from the firewall to hosts in each zone. You will use an SSH connection and ping hosts on each network.

1. On the *client desktop*, open the **Remmina** application.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Double-click the entry for **Firewall-A.**

3. If you are presented the *Connecting to 'Firewall-A'…* window, click **OK**.

Please Note

The Firewall-A connection in Remmina has been pre-configured to provide login credentials to the firewall so that you do not have to log in each time. This is for convenience in the lab only.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the CLI connection to the firewall, use the **ping** command to check network connectivity to a host in the *User_Net Security Zone* by using the following command at the **admin@firewall-a>** prompt.

```
admin@firewall-a> ping source 192.168.1.1 host 192.168.1.20
```

> **Please Note**
>
> Note the syntax for this command. 192.168.1.1 is the IP address of ethernet1/2 on the firewall. The command instructs the firewall to use that IP address on ethernet1/2 to ping the host 192.168.1.20. If you do not use the source option, the firewall uses its management interface address as the source IP.

5. Allow the *ping* to continue for three or four seconds and then use **Ctrl+C** to interrupt the command. Notice the *pings* are successful.

6. Use the *ping* command to check connectivity to a host in the Extranet zone by using the following command at the **admin@firewall-a>** prompt.

```
admin@firewall-a> ping source 192.168.50.1 host 192.168.50.150
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> 192.168.50.1 is the IP address on ethernet1/3 which is assigned to the Extranet security zone. 192.168.50.150 is a server in the Extranet zone.

7. Allow the *ping* to continue for three or four seconds and then use **Ctrl+C** to interrupt the command. Notice the *pings* are successful.

```
admin@firewall-a> ping source 192.168.50.1 host 192.168.50.150
PING 192.168.50.150 (192.168.50.150) from 192.168.50.1 : 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=1.60 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=0.957 ms
64 bytes from 192.168.50.150: icmp_seq=3 ttl=64 time=1.02 ms
^C
--- 192.168.50.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.957/1.193/1.602/0.291 ms
```

8. Use the *ping* command to check connectivity to a host on the Internet by using the following command at the **admin@firewall-a>** prompt.

```
admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8
```

```
admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8
```

> **Please Note**
> 203.0.113.20 is the IP address on ethernet1/1 which is assigned to the Internet security zone. 8.8.8.8 is a DNS server on the Internet zone.

9. Allow the *ping* to continue for three or four seconds and then use **Ctrl+C** to interrupt the command. Notice the *pings* are successful.

```
admin@firewall-a> 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=113 time=8.68 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=9.14 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=8.82 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 8.681/8.885/9.147/0.222 ms
```

10. Close the *Firewall-A Remmina* terminal console by clicking on the **close** icon in the upper-right.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. Close the *Remmina Remote Desktop Client* by clicking on the **close** icon in the upper-right.

12. Stay on the *client desktop* and continue to the next task.

1.6 Test Interface Access before Management Profiles

Management interface profiles allow you to enable specific network services on individual firewall interfaces.

To illustrate the default behavior of firewall interfaces, you will ping 192.168.1.1 from the client workstation. You will also attempt to access the firewall CLI by SSH through 192.168.1.1. Without any Interface Management Profiles in place, both ping and SSH will fail.

1. Open the **Terminal Emulator** on the *client desktop*.

2. Issue the following command below.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1 <Enter>
```

3. Wait a few seconds and use **Ctrl+C** to stop the command. You will not get a response because *Management profiles* have not been configured.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Attempt to open an *SSH* connection to the firewall through **192.168.1.1** by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ssh admin@192.168.1.1 <Enter>
```

5. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.

6. Leave the *Terminal* window open on the *client* because you will perform these same tests after applying an *Interface Management profile* to *ethernet1/1* and continue to the next task.

1.7 Define Interface Management Profiles

Often, your team members need to manage the firewall but do not always have network connectivity to the management network. In this exercise, you will define two management interface profiles. One profile will allow ping. You will apply this allow-ping profile to the Internet interface so that your SecOps team members can ping the external firewall interface for troubleshooting from outside your organization's network.

You will create a second management interface profile that allows ping and secure management traffic, including SSH and HTTPS. You will apply this Allow-mgt profile to the User_Net interface and to the Extranet interface. This profile will allow your SecOps team to manage the firewall from those networks if they need to.

1. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Select **Network > Network Profiles > Interface Management**. Click **Add** at the bottom of the window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the *Interface Management Profile* window, enter **`Allow-ping`** for the *Name*. Under the *Network Services* section, **check** the box for **Ping**. Click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Interface Management* section, click **Add** again to create another entry. In the *Interface Management Profile* window, enter **`Allow-mgt`** for the *Name*. Under the *Administrative Management Services* section, **check** the boxes for **HTTPS** and **SSH**. Under the section for *Network Services*, check **Ping**, **SNMP**, **Response Pages** and **User-ID**. Click **OK**.

5. Select **Network > Interfaces > Ethernet**. Click **Ethernet 1/1**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. In the *Ethernet 1/1* window, click **Advanced**. Under the *Other Info* section, use the dropdown list for *Management Profile* and select **Allow-ping**. Click **OK**.

Please Note

This action applies the Allow-ping interface management profile to ethernet1/1. As a result, ethernet1/1 will answer ping requests.
Note that in a production environment, you may not want an internet-facing interface to reply to any type of traffic. Applying this profile in the lab allows you to see how different profiles can be applied to different interfaces.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Click **Ethernet 1/2**.

8. In the *Ethernet Interface* window, click **Advanced**. Under the *Other Info* section, use the dropdown list for *Management Profile* and select **Allow-mgt**. Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Read the *Warning* message and click **Yes**.

Please Note

Because this interface is connected to one of your internal networks (Users_Net), the risk of applying this profile is acceptable.

10. Click **Ethernet 1/3**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Ethernet 1/3* window, click **Advanced**. Under the *Other Info* section, use the dropdown list for *Management Profile* and select **Allow-mgt**. Click **OK**.

12. Read the *Warning* message and click **Yes**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. When you complete steps *5 - 12*, your interface table should have an entry under the management profile column for each interface.

14. Click the **Commit** button at the upper-right of the web interface.

15. In the *Commit* window, click **Commit**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

16. Wait until the *Commit* process is complete. Click **Close**.

17. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.8 Test Interface Access after Management Profiles

In this section, you will use the ping command to test the management profiles that you defined. Both ping and SSH will succeed.

1. Return to the *Terminal* window used previously or reopen the **Terminal Emulator** on the *client desktop*.

2. Issue the following command below.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1 <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Wait a few seconds and use **Ctrl+C** to stop the command. You will get a response because *Management* profiles have been configured.

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.45 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.883 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.58 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.883/1.641/2.457/0.645 ms
```

4. Elevate to *super user* by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> sudo su
```

```
C:\home\lab-user\Desktop\Lab-Files> sudo su
```

5. Attempt to open an *SSH connection* to the firewall through **192.168.1.1** by issuing the following command.

```
root@client-a:/home/lab-user/Desktop/Lab-Files# ssh admin@192.168.1.1 <Enter>
```

```
root@client-a:/home/lab-user/Desktop/Lab-Files# ssh admin@192.168.1.1
```

6. When prompted to accept the *RSA key fingerprint*, type **yes** and press **Enter**.

```
RSA key fingerprint is SHA256:NLIJBMoViMy4a3acVKjvdDQnx0cyOa2814qfVOgD13c.
Are you sure you want to continue connecting (yes/no)? yes
```

7. For password, type **`Pal0Alt0!`** and press **Enter**.

```
Authorized Access Only
Password:
```

8. The *firewall* will present the *CLI interface*.

```
root@client-a:/home/lab-user/Desktop/Lab-Files# ssh admin@192.168.1.1
Authorized Access Only
Password:
Last login: Fri Aug  6 05:33:35 2021 from 192.168.1.20


Number of failed attempts since last successful login: 0


admin@firewall-a>
```

9. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 5: Configuring Security Policy Rules and NAT Rules

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Configuring Security Policy and NAT Rules 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Create a Security Policy Rule 10
1.3 Modify Security Policy Table Columns 15
1.4 Test New Security Policy Rule 17
1.5 Examine and Reset the Rule Hit Count 19
1.6 Examine the Traffic Log 22
1.7 Create Security Rules for Internet Access 27
1.8 Ping Internet Host from Client 36
1.9 Create a Source NAT Policy 37
1.10 Create a Destination NAT Policy 44

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

In this lab, you will allow network traffic from the Users_Net security zone to the Extranet security zone so that employees can access various business applications. You will create, modify, and test a security policy rule to allow access between these two zones. Once your rule is successfully in place, you will examine hit counters in the security policy rule table and examine the Traffic Log. Next, you will create security policy rules to allow hosts in your network to access the internet. You will then create source and destination NAT policy rules.

Objective

In this lab, you will perform the following tasks:

- Apply a baseline configuration to the firewall
- Create and test a security policy rule
- Modify security policy table columns
- Examine and reset the Rule Hit Count
- Examine the Traffic Log
- Create security rules for internet access
- Ping the internet host from the client
- Create source and destination NAT Policies

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Configuring Security Policy and NAT Rules

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-05.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Create a Security Policy Rule

You need to allow network traffic from the Users_Net security zone to the Extranet security zone so that employees can access various business applications. In this section, you will create a security policy rule to allow access between these two zones

1. In the web interface, select **Policies > Security**. Click **Add**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Security Policy Rule* window, on the *General* tab. Type **`Users-to-Extranet`** for the N*ame*. For *Description*, enter **`Allows hosts in Users_Net zone to access servers in Extranet zone`**.

3. Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Users_Net**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Select the **Destination** tab. Under the *Destination Zone* section, click **Add** and select **Extranet**.

5. Select the **Application** tab. Verify **Any** is selected for *Applications*.

6. Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service,* and **Any** is selected for *URL Category.*

The application-default setting instructs the firewall to allow an application such as web-browsing as long as that application is using the predefined service (or destination port). For an application like web-browsing, the application default service is TCP 80; for an application such as SSL, the application default service is TCP 443.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Select the **Actions** tab. Do not make any changes in this section but notice that the *Action* is set to **Allow** by default**.** Click **OK**.

> **Please Note**
> When you create a new security policy rule, the Action is automatically set to Allow. If you are creating a rule to block traffic, make sure you select the Actions tab and change the Action before you commit the rule.

8. Verify the *Users to Extranet* security policy rule appears in the *Security Policies* window.

> **Please Note**
> The rule appears above the two preconfigured entries intrazone-default and interzone-default. These two rules always appear at the bottom of the ruleset.

9. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. In the *Commit* window, click **Commit**.

11. Wait until the *Commit* process is complete. Click **Close**.

12. Leave the web interface open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Modify Security Policy Table Columns

You can customize the information presented in the Security Policy table to fit your needs. In this section, you will hide some of the columns and display others that may be of more interest. You will also move columns around and use the Adjust Column feature.

1. In the *Security Policy* window, click the **small dropdown** icon next to the *Name* column in the *Security Policy* table. You may need to hover your pointer over the icon for it to appear.

> **Please Note** This icon is available next to all column headers.

2. Choose **Columns** and note the available columns that you can hide or display in this table.

> **Please Note** Note that the column list in this image has been cropped and wrapped to make it clearer in the lab guide.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the *Columns*, uncheck **Type**, **Source Device**, **Destination Device,** and **Options**.

Please Note

These changes are optional. You do not have to show or hide columns or rearrange items in any of the firewall tables. However, you may find that there are certain columns in certain tables that you never use, and you can hide them to provide more room in the table. You may also find that there are certain columns that you scan frequently, and you can move those to locations that are easier to see. You can use these same steps to show, hide or move columns in all firewall tables.

4. At the top of the *Name* column, click the **dropdown** icon again and choose **Adjust Columns**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. This action will resize the displayed columns to best fit in the browser window**.**

6. Minimize the *PA-VM* firewall by clicking the **minimize** icon in the upper-right of the web interface and continue to the next task.

1.4 Test New Security Policy Rule

In this section, you will test the new security policy rule you created in a previous task.

1. Open the **Terminal Emulator** on the *client desktop*.

2. Issue the following command below to ensure your security policy rule is functioning correctly.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.80 <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Wait a few seconds and use **Ctrl+C** to stop the command. If you see a reply from 192.168.50.80, then your security policy rule is configured correctly! If not, review the previous steps and try this test again.

```
PING 192.168.50.80 (192.168.50.80) 56(84) bytes of data.
64 bytes from 192.168.50.80: icmp_seq=2 ttl=63 time=0.691 ms
64 bytes from 192.168.50.80: icmp_seq=3 ttl=63 time=0.703 ms
64 bytes from 192.168.50.80: icmp_seq=4 ttl=63 time=0.583 ms
^C
--- 192.168.50.80 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.583/0.659/0.703/0.053 ms
C:\home\lab-user\Desktop\Lab-Files>
```

4. On the *client desktop*, double-click the **Firefox** browser to open it.

5. Use the *Bookmark* bar and select **Extranet > Extranet**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. You should see a *webpage* displayed by the server. If you are seeing **Hello World !**, you have properly configured the security policy.

7. Close the *Firefox* browser. Click the **close** icon in the upper-right.

8. Reopen the *PA-VM firewall* interface by clicking the **Chromium** icon in the taskbar.

9. Leave the terminal and firewall web interface open and continue to the next task.

1.5 Examine and Reset the Rule Hit Count

With your rule successfully in place, you can now examine hit counters in the security policy rule table. These counters can be useful for troubleshooting. If a rule is not being hit, you may need to modify it.

Rule hit counts are very useful to track whether a rule is configured correctly. You can reset the counters for all security policy rules or for a single rule.

In this section, you will examine and reset the counters for the **Users_to_Extranet** rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the firewall interface, select **Policies > Security**.

2. In the *Security Policies* window, scroll to the right and locate the column for **Hit Count.** Note the number of hits on the Users to Extranet Rule. For this lab, there were **1166** hits. You may get different results, but the conclusion will be the same.

3. Return to the terminal window by clicking on the **terminal** icon in the taskbar of your *client desktop*.

4. In the CLI connection to the firewall, use the **ping** command to check network connectivity to the panw.lab server. Notice the ping was successful. Wait a few seconds and use **Ctrl+C** to stop the command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.80 <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Return to the *PA-VM firewall* interface and update the security policy rules table by clicking the **Refresh** button in the upper-right corner of the window. Notice the increase in the *Hit Count* for the **Users to Extranet** security policy rule has increased.

	NAME	TAGS	ZONE	ACTION	PROFILE	Rule Usage HIT COUNT	LAST HIT	FIRST HIT
1	Users-to-Extranet	none	Users	Allow	none	1757	2021-08-06 23:28:...	2021-08-06 22:49:...
2	intrazone-default	none	any	Allow	none	2724	2021-08-06 23:23:...	2020-02-27 02:30:...
3	interzone-default	none	any	Deny	none	11260	2021-08-06 23:29:...	2020-02-27 19:18:...

6. Highlight the **Users to Extranet** security policy rule. But do not open it.

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ADDRESS	Destination ZONE	APPLICATI...
1	Users-to-Extranet	none	Users_Net	any	any	any	Extranet	any
2	intrazone-default	none	any	any	any	any	(intrazone)	any
3	interzone-default	none	any	any	any	any	any	any

7. At the bottom of the *security policy* rules window, select **Reset Rule Hit Counter > Selected rules**.

8. Notice the *Hit Count* for *Users to Extranet* has been reset to **0**.

	NAME	TAGS	ZONE	ACTION	PROFILE	Rule Usage HIT COUNT	LAST HIT	FIRST HIT
1	Users-to-Extranet	none	Users_Ne	Allow	none	0	-	-
2	intrazone-default	none	any	Allow	none	2724	2021-08-06 23:23:...	2020-02-27 02:30:...
3	interzone-default	none	any	Deny	none	11260	2021-08-06 23:29:...	2020-02-27 19:18:...

9. Leave the firewall interface open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 Examine the Traffic Log

The Traffic Log contains information about sessions that the firewall allows or blocks. In this section, you will examine the Traffic Log to locate entries for sessions between the Users_Net zone and the Extranet zone.

1. In the *firewall* interface, select **Monitor > Logs > Traffic**.

2. Click the dropdown icon next to **Receive Time** and choose **Columns**.

3. Uncheck **Type**, **Source Dynamic Address Group**, **Destination Dynamic Address Group,** and **Dynamic User Group** to hide their columns.

Please Note This is not a requirement, but we will not be using information from these columns in any lab for this course.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Return to the terminal window by clicking on the terminal icon in the taskbar of your *client desktop*.

5. From the *terminal* window on the *desktop*, ping an address on the internet by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

6. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.

7. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.

8. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Ensure you are still viewing the *traffic logs*. In the filter field, enter **(addr.dst eq 8.8.8.8) and (zone.src eq Users_Net).** Click the **Apply Filter** button in the upper-right corner of the window. You will notice the firewall did not log your ping session to an external address. Notice the last successful log was on 09/02 from the *Users_net* to *Internet*. You should not see any entries on the date you complete this lab in this step.

Please Note

Filters are case sensitive so be precise! Also, note that there is a space after the first parentheses mark and right before the last parentheses mark.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

There are two reasons why the firewall did not log the ping session.

First, you do not have a security policy rule in place to allow traffic from the Users_Net zone to the internet zone. As the firewall examines the ping session, the only rule that matches is the interzone-default, which denies any traffic from one zone to another. The ping session matches this rule; however, there are no entries in the Traffic log indicating the match.

Second, remember that traffic that hits the interzone-default rule is not automatically logged. You must manually change a setting on this rule to see entries in the Traffic log. You will enable this setting now and perform the test again.

9. For the firewall to see the entries in the Traffic log, enable *Log at Session End* in the *interzone-default* rule. Navigate to **Policies > Security**. Highlight the **interzone-default** rule but do not open it.

10. Click the **Override** button at the bottom of the window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Security Policy Rule – predefined* window, click the **Actions** tab. Select **Log at Session End** and click **OK**.

12. Click the **Commit** button at the upper-right of the web interface.

13. In the *Commit* window, click **Commit**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. Wait until the *Commit* process is complete. Click **Close**.

15. Return to the terminal window by clicking on the *terminal* icon in the taskbar of your *client desktop*.

16. From the *terminal* window on the *desktop*, ping an address on the internet by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

17. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.

18. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

19. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter **`( addr.dst eq 8.8.8.8 ) and ( zone.src eq Users_Net ).`** Click the **Apply Filter** button in the upper right corner of the window. You will notice the firewall is now logging entries on the date you complete this step matching your filter.

20. Leave the web interface open and continue to the next task.

1.7 Create Security Rules for Internet Access

In this section, you will create security policy rules to allow hosts in your network to access the internet. You need to create a rule for hosts in the Users_Net security zone to access hosts in the internet security zone. You also need to create a rule to allow hosts in the Extranet security zone to access hosts in the internet security zone.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the *PA-VM firewall* web interface, navigate to **Policies > Security**. Click **Add** at the bottom of the window.

2. In the *Security Policy Rule* window, on the *General* tab. Type **`Users-to-Internet`** for the *Name*. For *Description*, enter **`Allows hosts in Users_Net zone to access Internet zone`**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Users_Net**.

4. Select the **Destination** tab. Under the *Destination Zone* section, click **Add,** and select **Internet**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Select the **Application** tab. Verify **Any** is selected for *Applications*.

6. Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service,* and **Any** is selected for *URL Category.*

The application-default setting instructs the firewall to allow an application such as web-browsing as long as that application is using the predefined service (or destination port). For an application like web-browsing, the application default service is TCP 80; for an application such as SSL, the application default service is TCP 443.

7. Select the **Actions** tab. Do not make any changes in this section but notice that the *Action* is set to **Allow** by default**.** Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
>
> When you create a new security policy rule, the Action is automatically set to Allow. If you are creating a rule to block traffic, make sure you select the Actions tab and change the Action before you commit the rule.

8. Verify the *Users-to-Internet* security policy rule appears in the *Security Policies* window.

9. Click **Add** at the bottom of the *Security Policies* window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. In the *Security Policy Rule* window, on the *General* tab. Type **`Extranet-to-Internet`** for the *Name*. For *Description*, enter **`Allows hosts in Extranet zone to access Internet zone`**.

11. Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Extranet**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Select the **Destination** tab. Under the *Destination Zone* section, click **Add,** and select **Internet**.

13. Select the **Application** tab. Verify **Any** is selected for *Applications*.

14. Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service,* and **Any** is selected for *URL Category.*

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

The application-default setting instructs the firewall to allow an application such as web-browsing as long as that application is using the predefined service (or destination port). For an application like web-browsing, the application default service is TCP 80; for an application such as SSL, the application default service is TCP 443.

15. Select the **Actions** tab. Do not make any changes in this section but notice that the *Action* is set to **Allow** by default**.** Click **OK**.

Please Note

When you create a new security policy rule, the Action is automatically set to Allow. If you are creating a rule to block traffic, make sure you select the Actions tab and change the Action before you commit the rule.

16. Verify the *Extranet-to-Internet* security policy rule appears in the Security policies window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

17. Click the **Commit** button at the upper right of the web interface.

18. In the *Commit* window, click **Commit**.

19. Wait until the Commit process is complete. Click **Close**.

20. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.8 Ping Internet Host from Client

In this section, you verify that your Security Policy rule is allowing traffic; you will ping an internet host from the client workstation and examine the Traffic log to see the results.

1. Return to the *terminal* window by clicking on the **terminal** icon in the taskbar of your *client desktop*.

2. From the *terminal* window on the *desktop*, ping an address on the internet by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

3. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.

4. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Reopen the firewall interface if you minimized it. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter **`( addr.dst eq 8.8.8.8 ) and ( app eq ping ).`** Click the **Apply Filter** button in the upper right corner of the window. You will notice the firewall is now logging entries hitting the **Users-to-Internet** rule. You may need to refresh the Traffic logs every one to two minutes for the Traffic logs to update.

Notice the ping failed. It failed because your ping session from the client to the Internet host did not get a reply even though the firewall is allowing the traffic. For the ping to be successful, you will need to create a NAT policy.

6. Leave the firewall open and continue to the next task.

1.9 Create a Source NAT Policy

You must create entries in the firewall's NAT Policy table to translate traffic from internal hosts (often on private networks) to a public, routable address (often an interface on the firewall itself). NAT rules provide address translation and are different from security policy rules, which allow and deny packets. You can configure a NAT policy rule to match a packet's source and destination zone, destination interface, source and destination address, and service.

In your previous ping test to an internet host, the ping traffic from your client is allowed by the Security Policy rule, but the packets leave the firewall with a non-routable source IP address from the private network of 192.168.1.0/24.

In this section, you will create a NAT policy rule to translate traffic from the private networks in the Users_Net and Extranet security zones to a routable address. You will use the same interface IP address on the firewall (203.0.113.20) as the source IP for outbound traffic from both Users_Net and Extranet hosts.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, navigate to **Policies > NAT**. Click **Add** to define a new *source NAT policy*.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *NAT Policy Rule* window, configure the following on the *General* tab:

Parameter	Value
Name	**`Inside_Nets_to_Internet`**
NAT Type	Verify **ipv4** is selected
Description	**`Translates traffic from Users_Net and Extranet to 203.0.113.20 outbound to Internet`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **Original Packet** tab and configure the following.

Parameter	Value
Source Zone	Click **Add** and select the **Users_Net** zone Click **Add** and select the **Extranet** zone
Destination Zone	Select **Internet** from the dropdown list
Destination Interface	Select **ethernet1/1** from the dropdown list
Service	Verify that the **any** is selected
Source Address	Verify that the **Any** check box is selected
Destination Address	Verify that the **Any** check box is selected

Please Note

This section defines what the packet will look like when it reaches the firewall. Note that we are using a single NAT rule to translate both source zones to the same interface on the firewall. You could accomplish this same task by creating two separate rules – one for each source zone – and using the same external firewall interface.

4. Click the **Translated Packet** tab and configure the following under the section for **Source Address Translation**. Click **OK**.

Parameter	Value
Translation Type	Select **Dynamic IP And Port** from the dropdown list
Address Type	Select **Interface Address** from the dropdown list
Interface	Select **ethernet1/1** from the dropdown list

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Parameter	Value
IP Address	Select **203.0.113.20/24** from the dropdown list. (Make sure that you **select** the interface IP address from the dropdown list and ***do not type it***.)

Please Note

This section defines how the firewall will translate the packet.

You are configuring *only* the **Source Address Translation** part of this window. Leave the destination address translation **Translation Type** set to **None**.

5. Verify that the **Inside_Nets_to_Internet** *NAT* policy is showing.

6. Click the **Commit** button at the upper right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the *Commit* window, click **Commit**.

8. Wait until the *Commit* process is complete. Click **Close**.

9. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

10. Return to the terminal window by clicking on the terminal icon in the taskbar of your *client desktop*.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. From the *terminal* window on the *desktop*, ping an address on the internet by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

12. After a few seconds, use **Ctrl+C** to stop the connection. You should now receive a successful reply.

13. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.

14. Open a new tab on the *Chromium* web browser. Type **`www.paloaltonetworks.com`** and verify connectivity. Close the newly opened tab by clicking the **X** icon.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

15. Examine the firewall Traffic log by ensuring you are at **Monitor > Logs > Traffic**. Clear any filters you have in place by clicking the **Clear** Filter button in the upper right corner of the window. Verify that there is allowed traffic that matches the security policy rule **Users_to_Internet.**

Please Note

Traffic log entries should be present based on the internet test. A minute or two may elapse for the log files to be updated. If the entries are not present, click the **refresh** icon

16. Leave the firewall open and continue to the next task.

1.10 Create a Destination NAT Policy

In this section, you will create a NAT address on the firewall using an IP address on the Users_Net network. The firewall will translate traffic that hits this address to the destination IP address of the web server in the Extranet Zone.

You will connect from the client host (192.168.1.20) to the NAT IP address on the firewall (192.168.1.80). The firewall will translate this connection to the DMZ server at 192.168.50.10.

This exercise will help you see how to configure Destination NAT rules.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, navigate to **Policies > NAT**. Click **Add** to define a new source NAT policy.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In *the NAT Policy Rule* window, configure the following on the **General** tab:

Parameter	Value
Name	`Dest_NAT_To_Webserver`
NAT Type	Verify that **ipv4** is selected
Description	`Translates traffic to web server at 192.168.50.80`

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **Original Packet** tab and configure the following.

Parameter	Value
Source Zone	Click **Add** and select the **Users_Net** zone
Destination Zone	Select **Users_Net** from the dropdown list
Destination Interface	Select **ethernet1/2** from the dropdown list
Service	Verify that **Any** is selected
Source Address	Verify that the **Any** check box is selected
Destination Address	Click **Add** and manually enter **`192.168.1.80`**

Please Note

The **Original Packet** tab defines how the packet will look when it reaches the firewall. When selecting the Destination Zone, remember that the IP address we are using (192.168.1.80) is one that resides on the firewall in the Users_Net security zone.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Click the **Translated Packet** tab and configure the following under the section for *Source Address Translation*. Click **OK**.

Parameter	Value
Translation Type	Select **Static IP** from the dropdown list
Translated Address	**`192.168.50.80`** (address of the Extranet web server)

> **Please Note**
>
> The **Translated Packet** tab defines how the firewall will translate a matching packet. Leave the **Source Address Translation** section set to **None** because we are performing only destination translation in this exercise.

5. Verify that the **Dest_NAT_To_Webserver** *NAT* policy is showing.

6. Click the **Commit** button at the upper right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the *Commit* window, click **Commit**.

8. Wait until the *Commit* process is complete. Click **Close**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Open a new tab on the *Chromium* web browser. Type **`http://192.168.1.80`** and verify connectivity to the *Extranet Server*. Close the newly opened tab by clicking the **X** icon.

10. Examine the firewall Traffic log by ensuring you are at **Monitor > Logs > Traffic**. Use a filter to locate the entry for Destination IP 192.168.1.80 **`( addr.dst in 192.168.1.80 ).`** Verify that there is allowed traffic that matches the security policy rule **Users_to_Internet.**

Please Note

Note the security policy rule that was matched: **Users_to_Extranet**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. As an alternate method to access the Traffic log in the web interface, select **Policies > Security**. Hover to the right of *Users-to-Extranet* to utilize the **dropdown** icon below the *Name* column, select **Log Viewer**.

When you use the Log Viewer option on a security policy, it opens the Traffic log and applies a filter automatically to display only those entries that match the security policy rule “Users_to_Extranet” that was selected.

12. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 6: Blocking Packet and Protocol Based Attacks

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Blocking Packet and Protocol Based Attacks 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Generate SYN Flood Traffic 10
1.3 Configure and Test TCP SYN Flood Zone Protection 14
1.4 Reconnaissance Protection 19
1.5 Concurrent Sessions on a Target Host and DoS Protection 30

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

You want to make certain that the Palo Alto Networks firewall provides protection against Layer 3 and Layer 4 attacks and network probes such as port scans.

You will create a Zone Protection Profile that you can assign to security zones. You will also create a DoS Protection Profile and DoS policy rules to ensure that you are taking advantage of all the tools that the firewall has available to block packet-based floods and probes.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Configure a Zone Protection Profile to detect and control SYN floods
- Configure a Zone Protection Profile to detect and control reconnaissance scans
- Configure a Zone Protection Profile to detect and control specific IP header options
- Configure a Zone Protection Profile to perform spoofed IP address checking
- Configure a DoS Protection Profile to protect firewall and node resource consumption
- Configure a DoS Protection Profile to detect and control SYN floods

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Packet and Protocol Based Attacks

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-06.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Generate SYN Flood Traffic

You will use a script on the client host in the Users_Net zone to send numerous TCP SYN packets to a target server in the Extranet zone.

1. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

2. On the *client desktop*, double-click the folder for **Class-Scripts**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Open the **EDU-210** folder.

4. Double-click the icon for **Clear Firewall Logs.**

5. Press **Enter** to start the *Clear Firewall Logs* script. Allow the script to complete. Once the *Clear Firewall Logs* script completes, press **Enter**. Leave the *EDU-210 – File Manager* window open.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Double-click the icon for **SYN Flood**.

Please Note

This script uses the nmap tool to send multiple SYN packets to a server in the Extranet zone.
nping --tcp-connect -p 80 --rate 10000 -c 50 -1 192.168.50.80

7. Press **Enter** to start the *SYN Flood* script. Allow the script to complete. Once the SYN Flood script completes, press **Enter**. Leave the *EDU-210 – File Manager* window open.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Open the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*

9. Navigate to **Monitor > Logs > Traffic**. Type **`( addr.src in 192.168.1.20 ) and ( app eq incomplete )`** in the filter builder. Press **Enter** or click the **Apply Filter** icon, and you should see incomplete connection attempts from *192.168.1.20* to *192.168.50.80* and port *80* in the Traffic log.

> **Please Note**
>
> Note that in the previous example image, several default columns have been moved or hidden. You may also find that there are certain columns that you scan frequently, and you can move those to locations by dragging and dropping to make easier to see.

10. Navigate to **Monitor > Logs > Threat**. Click the **X** icon to clear any filters. Nothing should be logged to the Threat log because no threat protections have been configured on the firewall.

11. Leave the web interface open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Configure and Test TCP SYN Flood Zone Protection

A Zone Protection Profile can detect and block flood attacks, including a TCP SYN flood. You will configure a very low SYN flood protection threshold that quickly will trigger flood events, even with a limited amount of traffic. You will see how flood protection operates.

After you define the settings for a Zone Protection Profile, you must apply it to the security zone.

Lastly, you will Generate TCP SYN flood traffic again to determine how the flood threshold settings in the Zone Protection Profile operate. The flood packets will arrive at the firewall's inside zone, which is protected by the Zone Protection Profile.

1. In the web interface, select **Network > Network Profiles > Zone Protection**. Click **Add** to create a new Zone Protection Profile.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. On the *Flood Protection* tab, configure the following. Click **OK**.

Parameter	Value
Name	`User_Net_Profiles`
SYN	Select **check box**
Action	**SYN Cookies**
Alarm Rate	**5**
Activate	**10**
Maximum	**20**

Please Note

These settings are artificially low so that the firewall will implement Zone Protection during the testing part of the lab.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the web interface, select **Network > Zones**. Click **Users_net**.

4. In the *Zone* window, in the bottom-left corner, select **User_Net_Profiles** under the *Zone Protection Profile* dropdown list. Verify **Enable Packet Buffer Protection** is checked. Click **OK**.

5. Click the **Commit** button at the upper-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. In the *Commit* window, click **Commit**.

7. Wait until the *Commit* process is complete. Click **Close**.

8. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

9. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. Double-click the icon for **SYN Flood**.

Please Note

This script uses the nmap tool to send multiple SYN packets to a server in the Extranet zone.
nping --tcp-connect -p 80 --rate 10000 -c 50 -1 192.168.50.80

11. Press **Enter** to start the *SYN Flood* script. Allow the script to complete. Once the *SYN Flood* script completes, press **Enter**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Open the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*

13. Navigate to **Monitor > Logs > Threat**. Click the **X** icon to clear any filters. You should see entries for **TCP Flood** threat recorded in the log.

Note that in the previous example image, the Severity column has been moved and several other default columns have been hidden. You may also find that there are certain columns that you scan frequently, and you can move those to locations by dragging and dropping to make it easier to see.

14. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Reconnaissance Protection

In this section, you will modify the existing Zone Protection Profile to include protection against port scans and ping sweeps. An attacker often will use these techniques against hosts to determine open ports, the version of the services running on the open ports, or the host's operating system. The attacker can use this information to plan further attacks.

An attacker often will probe a host to determine its open ports, the version of the services running on the open ports, or the host's operating system. The attacker can use this information to plan attacks. Once you add reconnaissance to a zone protection profile, you will generate a reconnaissance port scan.

Lastly, a Zone Protection Profile can detect and block packet-based attacks, including the use of specific IP header options such as *Record Route.* An attacker sometimes can use specific IP header options to perform reconnaissance as a precursor to an attack. The firewall can be configured to detect and drop IP packets with specific header options. You will update a zone protection profile to include traceroute protection and test the zone protection profile by generating Traceroute traffic.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Navigate to **Network > Network Profiles > Zone Protection**. Select **User_Net_Profiles**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Select the tab for **Reconnaissance Protection.** Modify the **TCP Port Scan** with the following settings. Click **OK**.

Parameter	Value
Enable	Select **check box**
Action	Select **Block-IP** Note that when you select block-IP as the action, you will see an overlay menu that allows you to select Track By and Duration. For **Track By**, select **source** For **Duration**, type **2**
Interval (sec)	**2**
Threshold (events)	**2**

3. Click the **Commit** button at the upper-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Commit* window, click **Commit**.

5. Wait until the *Commit* process is complete. Click **Close**.

6. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

7. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Double-click the icon for **TCP Scan**.

Please Note

This script runs the nmap command to scan 192.168.50.80 for open ports.
The exact syntax for the command is:
`nmap -v1 -Pn -T4 --max-retries 1 192.168.50.80`

9. Press **Enter** to start the *TCP Scan*. This script runs the nmap command to scan **192.168.50.80** for open ports. After 30 seconds, use **Ctrl+C** to stop the scan script.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. Open the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*

11. Select **Monitor > Logs > Threat**. You should see several **SCAN: TCP Port Scan** records populated. If you do not, wait about **30** seconds and refresh the threat logs by clicking the **Refresh** icon.

12. Select **Network > Network Profiles > Zone Protection**. Click the **User_Net_Profiles** to open the profile.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. Click the **Packet Based Attack Protection** tab. If necessary, you may need to click the **IP Drop** tab. Select the **Record Route** option on the *IP Option Drop* panel. Click **OK**.

14. Click the **Commit** button at the upper-right of the web interface.

15. In the *Commit* window, click **Commit**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

16. Wait until the *Commit* process is complete. Click **Close**.

17. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next step.

18. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

19. Double-click the icon for **IP Record Route Ping**.

Please Note

This option in the IP header records the network path from the source host to the destination host. The Record Route option is not commonly used, and an attacker could use such information for network reconnaissance.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

20. Press **Enter** to start the *IP Record Route Ping* script. Allow the script to complete. Once the *IP Record Route Ping* script completes, press **Enter**. The script will stall with **100%** packet loss.

```
Terminal
    ##########################################
    ##          Record Route Pings          ##
    ##########################################

    This script sends pings to target server with record route flag set.

    Press ENTER to start or CTRL+C to quit.

    nmap -sP --ip-options R 192.168.50.80 --max-retries 3

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-07 00:36 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.00 seconds

    ##############################################
    ##             Process Complete             ##
    ##############################################

    Press ENTER to close this window.
```

21. In the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*

22. Select **Monitor > Logs > Threat**. You should now see an informational message with a threat named *IP Option Record Route*.

Please Note

To move forward in this lab, you will need to remove your Zone Protection Profile configuration to ensure that it does not interfere while you test a DoS Protection policy and profile

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

23. Select **Network > Zones**. Click **Users_Net** to edit the zone.

24. In the *Zone* window, select **None** for the *Zone Protection Profile*. Click **OK**.

25. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

26. In the *Commit* window, click **Commit**.

27. Wait until the *Commit* process is complete. Click **Close**.

28. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Concurrent Sessions on a Target Host and DoS Protection

In this section, you will run a script that uses **nmap** to open multiple concurrent sessions from the client host in the Users_Net zone to a target server in the Extranet zone. The script will test whether the firewall will allow 10 concurrent sessions to the target host. You will monitor the results using the Traffic and Threat logs.

A DoS Protection policy and profile can detect when the number of concurrent sessions to a host has exceeded a specified limit. You will configure a maximum concurrent session limit for a host in the Extranet zone.

You will use the **Concurrent Connections** script again to generate multiple concurrent sessions to the Linux host in the dmz zone. The host is protected by a DoS Protection policy rule and profile that should drop any connection requests that exceed the configured maximum number of nine concurrent sessions to the Linux host.

A DoS Protection Profile can detect and block flood attacks to a zone, to a subset of hosts in a zone, or to a specific host in a zone. You will configure flood protection in both a Zone Protection Profile and a DoS Protection Profile so that you can see how they interact. You will configure a higher TCP SYN flood protection threshold in a Zone Protection Profile and a lower TCP SYN flood protection threshold in the DoS Protection Profile.

Lastly, you will use the **Concurrent Connections** script to generate multiple concurrent sessions to the target server in the Extranet zone. The host is protected by both a Zone Protection Profile and a DoS Protection Profile that should drop any connection requests that exceed the lowest configured flood threshold settings. The lower DoS Protection Profile thresholds should be reached first.

1. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

2. Double-click the icon for **Clear Firewall Logs**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> This script uses the XML API to clear the Threat, Traffic and URL Filtering log files. We are clearing the log files to make it easier to identify traffic and threats blocked by DoS Protection.

3. Press **Enter** to start the *Clear Firewall Logs* script. Allow the script to complete. Once the *Clear Firewall Logs* script completes, press **Enter**.

4. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop*.

5. Navigate to **Monitor > Logs > Threat** and verify the logs have been cleared.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

7. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

8. Double-click the icon for **Concurrent Connections**.

Please Note

The exact syntax for this command is:
nmap --script http-slowloris --max-parallelism 10 192.168.50.80

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Press **Enter** to start the *Concurrent Connections* script. The command can take 30 minutes to complete. You do not need to wait for the script to complete. Allow the command to run for at least 3 minutes and then press **Ctrl+C** to stop command execution**.**

10. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the client desktop.

11. Select **Monitor >Logs > Traffic**. Clear any filters you have in place by clicking the **Clear Filter** button.

Please Note

As the command execution progressed, you should see multiple web-browsing log entries for traffic to multiple ports, but especially to port 80 and 443. The traffic was not blocked by any Security Profiles or Security policy rules.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Navigate to **Monitor > Logs > Threat**. Notice there are no logs present.

> **Please Note**
> There should be *no* Threat log entries because nothing has been configured to monitor traffic for the number of concurrent sessions to a specific target host

13. Configure maximum concurrent sessions with DoS protection by selecting **Objects > Security Profiles > DoS Protection**. Click **Add** in the lower-left of the window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. In the *DoS Protection Profile* window, configure the following. Click **OK**.

Parameter	Value
Name	**`protect-session-max`**
Classified	Select it
Resources Protection tab	Click it
Sessions	Select **check box**
Maximum Concurrent Sessions	**9**

15. Navigate to **Polices > DoS Protection**. Click **Add**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

16. In the *DoS Rule* window, configure the following. Click **OK**.

Parameter	Value
General tab	Click it, if necessary
Name	`internal-protection`
Source tab	Click it
Zone	Select **Users_Net**
Destination tab	Click it
Zone	Select **Extranet**
Option/Protection tab	Click it
Action	Select **Protect**
Classified	Select **check box**
Profile	Select **protect-session-max**
Address	Select **destination-ip-only**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

17. Verify the *internal-protection* rule is present in the DoS Protection policies.

	NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection	
			ZONE/INTERFA...	ADDRESS	USER	ZONE/INTERFA...	ADDRESS			AGGREGATE	CLASSIFIED
1	internal-protection	none	Users_Net	any	any	Extranet	any	any	protect	none	profile: protect-session-max destination-ip-only

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

18. Click the **Commit** button at the upper-right of the web interface.

19. In the *Commit* window, click **Commit**.

20. Wait until the *Commit* process is complete. Click **Close**.

21. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

22. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

23. Double-click the icon for **Concurrent Connections**.

> **Please Note**
> The exact syntax for this command is:
> **nmap --script http-slowloris --max-parallelism 10 192.168.50.80**

24. Press **Enter** to start the *Concurrent Connections* script. The command can take *30* minutes to complete. You do not need to wait for the script to complete. Allow the command to run for at least *3* minutes and then press **Ctrl+C** to stop command execution**.**

25. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

26. Navigate to **Monitor > Logs > Threat**. Notice the new *Threats*.

Please Note

Several columns have been hidden in this example.

You should see **Session Limit Event** entries in the Threat log because the number of concurrent connection requests to the protected host has exceeded the configured session maximum limit.

27. Navigate to **Objects > Security Profiles > DoS Protection**. Click **protect-session-max** to edit the profile.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

28. In the *DoS Protection Profile* window, click the **Resources Protection** tab. **Deselect** *Sessions*. Click **OK**.

29. Navigate to **Network > Network Profiles > Zone Protection**. Click **User_Net_Profile**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

30. On the *Flood Protection* tab, configure the following.

Parameter	Value
SYN	**Verify the check box is selected**
Action	**SYN Cookies**
Alarm Rate	**1000**
Activate	**1100**
Maximum	**1300**

Please Note

The threshold values here are configured with high values to ensure that the lower DoS Protection Profile thresholds are reached first during testing in a later lab section.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

31. Click the **Reconnaissance Protection** tab. For *TCP Port Scan*, deselect the **Enable** checkbox. Click **OK**.

32. Select **Network > Zones**. Click the **Users_Net** zone.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

33. In the *Zone* window**,** *Zone Protection Profile* menu, select **User_Net_Profiles**. Click **OK**.

34. Navigate to **Objects > Security Profiles > DoS Protection**. Click **protect-session-max**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

35. In the *DoS Protection Profile* window, configure the following. Click **OK**.

Parameter	Value
Flood Protection tab	**Verify that the tab is selected**
SYN Flood	**Select check box**
Action	**SYN Cookies**
Alarm Rate	**5**
Activate Rate	**10**
Max Rate	**20**

36. Click the **Commit** button at the upper-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

37. In the *Commit* window, click **Commit**.

38. Wait until the *Commit* process is complete. Click **Close**.

39. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

40. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

41. Double-click the icon for **Concurrent Connections**.

> **Please Note**
> The exact syntax for this command is:
> **nmap --script http-slowloris --max-parallelism 10 192.168.50.80**

42. Press **Enter** to start the *Concurrent Connections* script. The command can take *30* minutes to complete. You do not need to wait for the script to complete. Allow the command to run for at least *3* minutes and then press **Ctrl+C** to stop command execution**.**

43. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

44. Navigate to **Monitor > Logs > Threat**. Notice the new *Threats*.

Please Note

Several columns have been hidden in this example.

You should see **TCP Flood** Threat log entries because the number of connection requests to the target host has exceeded the configured flood threshold maximum in the DoS Protection Profile. The flood threshold in the DoS Protection Profile is lower than the Zone Protection Profile, so it should have been triggered first.

45. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 7: Blocking Threats from Known-Bad Sources

Document Version: 2022-08-29

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
7 Block Threats from Known-Bad Sources 6
7.1 Apply a Baseline Configuration to the Firewall 6
7.2 Test Access to Know Malicious IP Addresses 11
7.3 Block Access to Malicious IP Addresses Using Address Objects 14
7.4 Block Access to Malicious IP Addresses Using Address Groups 23
7.5 Block Access to Malicious IP Addresses by Geographic Region 29
7.6 Block Access to Malicious IP Addresses Using EDLs 33
7.7 Block Access to Malicious Domains Using an EDL 44
7.8 Add the Domain List EDL to an Anti-Spyware Profile 48
7.9 Add the Anti-Spyware Profile to a Security Policy Rule 51
7.10 Block Access to Malicious URLs Using the Security Policy 55
7.11 Create a Custom URL Category 64
7.12 Create an EDL to Block Malicious URL Access 70
7.13 Block Access to a Malicious URL Using a URL Filtering Profile 78

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

You need to make certain that the firewall blocks traffic, both to and from known malicious IP addresses, hostnames, and domain names. There are numerous external blocklists that you may want to implement on the Palo Alto Networks firewall. You also need to implement your own custom lists of IP addresses, hostnames, and domain names to block traffic based on various corporate policies. Upper management is also concerned that some users have been accessing inappropriate web content from their corporate devices. You need to configure the firewall to block browsing to certain categories of web traffic, including adult and nudity.

You are concerned about users accessing websites that are often the source of malicious files and content, such as viruses and spyware.

In this section, you will explore the options available on the firewall that allow you to block individual addresses, groups of addresses, and lists of addresses. You will also configure the firewall to block certain categories of websites.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Block access to malicious IP addresses using address objects
- Block access to malicious IP addresses using address Groups
- Block access to malicious IP addresses using geographic regions
- Block access to malicious IP addresses using an External Dynamic List (EDL)
- Block access to malicious domains using an EDL
- Block access to malicious URLs using the security policy
- Block access to a malicious URL using a URL filtering profile

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7 Block Threats from Known-Bad Sources

7.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the *Client PC*.

2. Double-click the **Chromium Web Browser** icon located on the *desktop*.

3. In the *Chromium* address field, type **`https://192.168.1.254`** and press **Enter**.

4. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.

If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.

> **Please Note**
> Before you can enable Telemetry Data Collection, you would need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. In the *Load Named Configuration* window, select **edu-210-lab-07.xml** from the *Name* dropdown box and click **OK**.

10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

11. Click the **Tasks** icon located at the bottom-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

13. Click the **Commit** link located at the top-right of the web interface.

14. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

15. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

7.2 Test Access to Known Malicious IP Addresses

You can use security policy rules to block access to known malicious IP addresses. Because the list of malicious IP addresses can quickly change, you will treat two legitimate IP addresses as though they are malicious and block access to them.

Please Note

Although you can block access to specific IP addresses, Palo Alto Networks recommends that you use a positive enforcement model whenever possible. Use of a positive enforcement model means that you configure a security policy to pass what is allowed rather than what should be blocked, with the assumption that anything not specifically allowed is blocked by default.

1. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

2. On the *client desktop*, open a *terminal* window by double-clicking **Terminal Emulator**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Enter the command below to obtain the IP Address of 2600.org. Write down the **IP address** or **copy** and paste it into a text document on the *desktop*.

```
C:\home\lab-user\Desktop\Lab-Files> nslookup 2600.org
```

4. In the same **CMD** window, enter the command below. Write down the **IP address** or **copy** and paste it into a text document on the *desktop*.

```
C:\home\lab-user\Desktop\Lab-Files> nslookup www.breakthesecurity.com
```

5. In the same **CMD** window, verify connectivity to the websites by entering the commands below. You will **ping** two IP Addresses. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=1 ttl=46 time=120 ms
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=2 ttl=46 time=124 ms
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=3 ttl=46 time=133 ms
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=4 ttl=46 time=128 ms
^C
--- www.breakthesecurity.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 120.138/126.615/133.107/4.823 ms
C:\home\lab-user\Desktop\Lab-Files>
```

Please Note

Here, pinging *2600.org* and *breakthesecurity.com* will be successful. Access will be blocked in the next tasks.

6. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.

7. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7.3 Block Access to Malicious IP Addresses Using Address Objects

Be aware that the list of malicious IP addresses quickly changes, so keeping your Address objects current could be problematic. For this reason, later lab exercises will illustrate more automated methods to block the current list of malicious IP addresses.

In this section, you will create an Address object that contains a list of malicious IP addresses. You will use this Address object in the security policy to block access to the malicious IP addresses.

Lastly, you will test access to the IP Addresses contained in the Address Objects.

1. In the *PA-VM* interface, select **Objects > Addresses**. Click **Add**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Address* window, configure the following. Click **OK**.

Parameter	Value
Name	`malicious-ip-address-1`
Description	`2600.org IP address`
Type	**IP Netmask**
(address text box)	`<IP_address_of_2600.org>`

Please Note

Note that the IP address you enter may be different from the previous example.

3. In the *Addresses* window, click **Add**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Address* window, configure the following. Click **Resolve**.

Parameter	Value
Name	`malicious-fqdn-1`
Description	`www.breakthesecurity.com`
Type	**FQDN**
(FQDN text box)	`www.breakthesecurity.com`

5. Once you click **Resolve,** you will be prompted to select **Use this Address**.

6. In the *Address* window, click **OK**.

7. Confirm the *address* objects appear in the *Addresses* window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Select **Policies > Security**. Click **Add** to create a new security policy rule.

9. In the *Security Policy Rule* window, on the *General* tab, type **`Block-Known-Bad-IPs`** as the *Name*. For *Description*, enter **`Blocks traffic to malicious address objects`**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	Add **Users_Net** and **Extranet**
Source Address	**Any**

11. Click the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	Add **Internet**
Destination Address	Add **malicious-fqdn-1** and **malicious-ip-address-1**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Click the **Application** tab and verify that **Any** is selected.

13. Click the **Service/URL Category** tab and verify that **application-default** and **Any** are selected.

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

Parameter	Value
Action	**Deny**
Log Setting	**Log at Session End**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

15. Select, but do not open, the **Block-Known-Bad-IPs** rule in the security policy.

	NAME	TAGS	TYPE	Sou ZONE	ADDRESS
1	Users_to_Extranet	none	universal	Users_Net	any
2	Users_to_Internet	none	universal	Users_Net	any
3	Extranet_to_Internet	none	universal	Extranet	any
4	Block-known-Bad-IPs	none	universal	Extranet Users_Net	any
5	intrazone-default	none	intrazone	any	any
6	interzone-default	none	interzone	any	any

16. At the bottom of the window, select **Move > Move Top** to move the rule to the top of the security policy.

17. Verify that the **Block-Known-Bad-IPs** rule is rule number *1*.

	NAME	TAGS	TYPE	Sour ZONE	ADDRESS
1	Block-known-Bad-IPs	none	universal	Extranet Users_Net	any
2	Users_to_Extranet	none	universal	Users_Net	any
3	Users_to_Internet	none	universal	Users_Net	any
4	Extranet_to_Internet	none	universal	Extranet	any
5	intrazone-default	none	intrazone	any	any
6	interzone-default	none	interzone	any	any

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

18. Click the **Commit** button at the upper-right of the web interface.

19. In the *Commit* window, click **Commit**.

20. Wait until the *Commit* process is complete. Click **Close**.

21. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

22. Return to the *terminal* window by clicking on the **Terminal** icon in the taskbar of your *client desktop.*

23. From the *terminal* window on the *desktop*, enter the following commands. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org <Enter>
```

Please Note

Pinging 2600.org will fail.

```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com <Enter>
```

Please Note

Pinging www.breakthesecurity will fail because access to the IP addresses was blocked by the Address objects in the Security policy.

24. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.

25. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

26. Navigate to **Monitor > Logs > Traffic**. Enter the filter **(action eq deny)** in the *Filter builder* to look for traffic that has been denied. You should see entries indicating that your **Block-Known-Bad-IPs** security policy rule has denied traffic to each host.

> **Please Note**
> Note some columns have been adjusted to view the information shown in the screen shot.

27. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

7.4 Block Access to Malicious IP Addresses Using Address Groups

You can use Address Groups in security policy rules to control access to IP addresses. You can group multiple Address objects in an Address Group and then use just the Address Group in your security policy rules. Address Groups are used to shorten and simplify a policy or a policy rule.

You will create a static Address Group, add two Address objects to the group, and then modify the security policy to use the Address Group.

Lastly, you will test access to the IP addresses contained in the Address objects.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the *firewall* interface, select **Objects > Address Groups**. Click **Add**.

2. In the *Address Group* window, configure the following. Click **OK**.

Parameter	Value
Name	`Malicious-IP-Group`
Description	`Contains malicious IP address objects`
Type	**Static**
Addresses	Add **malicious-fqdn-1** and **malicious-ip-address-1**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Select **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.

4. In the *Security Policy Rule* window, **Destination** tab, select the **malicious-fqdn-1** and **malicious-ip-address-1** checkboxes. Click **Delete**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Destination Address* window, click **Add**. Select **Malicious-IP-Group**. Click **OK**.

6. Click the **Commit** button at the upper-right of the web interface.

7. In the *Commit* window, click **Commit**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Wait until the *Commit* process is complete. Click **Close**.

9. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

10. Return to the *terminal* window by clicking on the **terminal** icon in the taskbar of your *client desktop*.

11. From the *terminal* window on the *desktop*, enter the commands below. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org <Enter>
```

Please Note

Pinging 2600.org will fail.

```
C:\home\lab-user\
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
^C
--- www.breakthesecurity.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

C:\home\lab-user\Desktop\Lab-Files>
```

Please Note

Pinging www.breakthesecurity will fail because access to the IP addresses was blocked by the address objects in the security policy.

12. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.

13. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.

14. Navigate to **Monitor > Logs > Traffic**. Enter the filter **(action eq deny)** in the *filter builder* to look for traffic that has been denied. You should see *additional* entries indicating that your **Block-Known-Bad-IPs** security policy rule has denied traffic to each host.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7.5 Block Access to Malicious IP Addresses by Geographic Region

You can block access to IP addresses associated with specific geographic regions. This ability is useful for reducing your attack surface by prohibiting traffic from countries where you have no legitimate business contacts.

In this section, you will configure and test access to the blocked geographic region. After you have tested access, you will restore access to the blocked region.

1. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

2. Return to the *terminal* window by clicking on the **Terminal** icon in the taskbar of your client desktop.

3. From the *terminal* window on the *desktop*, enter the command below to obtain the IP Address of 2600.org. Write down the **IP address** or **copy** and paste it into a text document on the *desktop*.

```
C:\home\lab-user\Desktop\Lab-Files> nslookup nic.ir <Enter>
```

Please Note

The nic.ir domain is in Iran.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the same **CMD** window, verify connectivity *to nic.ir* by entering the command below. Use **Ctrl+C** to stop the ping after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping nic.ir <Enter>
```

Please Note

You may not get a response to the ping but that will not affect this lab.

5. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.

6. If you minimized the *Firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.

7. In the web interface, select **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the *Security Policy Rule* window, click the **Destination** tab and Add **IR** to the *Destination Address* list. Click **OK**.

> **Please Note** You will need to scroll down the list of available addresses to locate the entry for IR.

16. Click the **Commit** button at the upper-right of the web interface.

17. In the *Commit* window, click **Commit**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

18. Wait until the *Commit* process is complete. Click **Close**.

19. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

20. Return to the *terminal* window by clicking on the **Terminal** icon in the taskbar of your *client desktop*.

21. From the *terminal* window on the *desktop*, verify connectivity *to nic.ir* by entering the command below. Use **Ctrl+C** to stop the ping after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping nic.ir <Enter>
```

Please Note

The ping will fail because you blocked the region of IR.

22. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

23. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.

24. Navigate to **Monitor > Logs > Traffic**. Enter the filter **`( addr.dst in 194.225.70.16 )`** in the *filter builder* to look for traffic that has been denied. You should see entries indicating that your **Block-Known-Bad-IPs** security policy rule has denied traffic to each host.

25. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

7.6 Block Access to Malicious IP Addresses Using EDLs

You can add a list of malicious IP addresses to a file on an external web server and configure the firewall to access the list as an EDL. The advantage of this approach is that the malicious IP address list can be regularly updated without the need to recommit the firewall configuration, as you would have to do if you updated an Address object or Address Group. EDLs simplify the maintenance of a current list of IP addresses.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the *firewall* interface, select **Objects > External Dynamic Lists.** Note the three predefined EDLs contain known malicious and high-risk IP address lists. Click **Palo Alto Networks – High risk IP addresses**.

Please Note

Palo Alto Networks maintains and provides these lists.

2. Read the description of the list.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **List Entries And Exceptions** tab. Write down *three IP addresses* on the current list of IP addresses. You will try to **ping** these addresses later in this lab exercise. Click **Cancel**.

Please Note

For this step, we chose the first three IP Addresses on the list. You may choose any IP Addresses you would like however, it is important to write down the IP Address to complete this task.

Note that you can also copy and paste these addresses into a text file on the client desktop.

4. At the bottom of the *External Dynamic Lists* window, click **Add**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *External Dynamic Lists* window, create another **EDL** and configure the following. Click **Test Source URL**.

Parameter	Value
Name	**`custom-malicious-ips-edl`**
Type	**IP List**
Description	**`Contains manually entered IP address list on web server.`**
Source	**`http://192.168.50.80/malicious-ips.txt`** (The EDL contains only the IP address 192.168.50.11.)
Check for updates	**Five Minute**

6. The firewall should present a *Test Source URL* window indicating that it can access the URL. Click **Close**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Click **OK** in the *External Dynamic Lists* window.

8. Update the security policy to include *External Dynamic Lists*. Navigate to **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Click the **Destination** tab and configure the following. Click **OK**.

Parameter	Value
Destination Zone	**Internet**
Destination Address	Add the following to the list: **Palo Alto Networks – Bulletproof IP addresses** **Palo Alto Networks – High risk IP addresses** **Palo Alto Networks – Known malicious IP addresses**

Please Note

The "Block-Known-Bad-IPs" rule now is configured to block access to the three IP addresses you wrote down in lab Step 3.

10. Click **Users_to_Extranet** to edit the rule.

	NAME	TAGS	TYPE	ZONE	ADDRESS
1	Block-known-Bad-IPs	none	universal	Extranet Users_Net	any
2	Users_to_Extranet	none	universal	Users_Net	any
3	Users_to_Internet	none	universal	Users_Net	any
4	Extranet_to_Internet	none	universal	Extranet	any

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Security Policy Rule* window, click the **Destination** tab and configure the following. Click **OK**.

Parameter	Value
Destination Zone	**Extranet**
Destination Address	**custom-malicious-ips-edl**
Negate	Select **check box**

> **Please Note**
> The malicious-ips-edl EDL contains the IP address of a host in the Extranet zone (192.168.50.11). When the destination address is used in conjunction with the Negate option, the rule matches and allows any address in the Extranet zone except the address listed in the EDL.

12. Notice in the *Users_to_Extranet* rule that *custom-malicious-ips-edl* has a line through it. This line indicates that the **Negate** option has been employed for addresses in the list.

13. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. In the *Commit* window, click **Commit**.

15. Wait until the *Commit* process is complete. Click **Close**.

16. Return to the *terminal* window by clicking on the **Terminal** icon in the taskbar of your *client desktop*.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

17. From the *terminal* window on the *desktop*, ping an address on the internet by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.11 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.11
```

18. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.11
PING 192.168.50.11 (192.168.50.11) 56(84) bytes of data.
^C
--- 192.168.50.11 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3065ms

C:\home\lab-user\Desktop\Lab-Files>
```

Please Note

The **ping** should fail because the IP address is listed in the custom EDL.

19. From the *terminal* window, use **ping** again, but this time try one of the three IP addresses that you wrote down earlier in lab step 3.

```
C:\home\lab-user\Desktop\Lab-Files> ping 89.37.192.194 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 89.37.192.194
```

20. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.

```
C:\home\lab-user\Desktop\Lab-Files> ping 89.37.192.194
PING 89.37.192.194 (89.37.192.194) 56(84) bytes of data.
^C
--- 89.37.192.194 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2036ms

C:\home\lab-user\Desktop\Lab-Files>
```

Please Note

These IP addresses were in one of the EDLs predefined by Palo Alto Networks.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

21. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.

22. If you minimized the *Firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.

23. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter **`( action neq allow ) and ( app eq ping )`.** Click the **Apply Filter** button in the upper-right corner of the window. You will notice the firewall is now logging entries matching your filter.

Please Note

Note that ping to 192.168.50.11 hit the **interzone-default** rule and not the **Users_to_Extranet** rule. The Users_to_Extranet rule is set to allow traffic (with the exception of the IP address 192.168.50.11). Traffic to the 192.168.50.11 address does not match the rule because of the negate setting you applied in the Destination Address section. However, that traffic does match the interzone-default rule which denies traffic.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

24. In the firewall web interface, select **Policies > Security**. Click **Users_to_Extranet** to edit the rule.

25. In the *Security Policy Rule* window, click the **Destination** tab and configure the following. Click **OK**.

Parameter	Value
Destination Zone	**Extranet**
Destination Address	Delete **custom-malicious-ips-edl**
Negate check box	**Deselect it**

26. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

27. In the *Commit* window, click **Commit**.

28. Wait until the *Commit* process is complete. Click **Close**.

29. Leave the web interface open and continue to the next task.

7.7 Block Access to Malicious Domains Using an EDL

You can add a list of malicious domains to a file on an external web server and then configure the firewall to access the list as an EDL. The advantage of this approach is that the malicious domain list can be updated regularly without the need to recommit the firewall configuration.

In this section, you will block access to malicious domains using an External Dynamic List.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the *PA-VM firewall* web interface, navigate to **Objects > External Dynamic Lists**. Click **Add** at the bottom of the window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *External Dynamic Lists* window, configure the following. Click **OK**.

Parameter	Value
Name	**`malicious-domains-edl`**
Type	**`Domain List`**
Source	**`http://192.168.50.80/malicious-domains.txt`** (The EDL contains the domains quora.com and producthunt.com.)
Automatically expand to include subdomains	Select it
Check for updates	**Five Minute**

Please Note

This EDL will be used to block access to the quora.com and producthunt.com domains.

3. Click to reopen the **malicious-domains-edl**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *External Dynamic Lists* window, click **Test Source URL**.

5. The firewall should present a **Test Source URL** window indicating that it can access the URL. Click **Close**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Click **OK** in the *External Dynamic Lists* window.

7. Leave the firewall open and continue to the next task.

7.8 Add the Domain List EDL to an Anti-Spyware Profile

You can add an EDL containing a domain list to an Anti-Spyware Profile to block access to malicious domains. You must attach the Anti-Spyware Profile to a security policy rule that allows network access. Although the security policy rule might allow the traffic, the attached Anti-Spyware Profile will block access to any domains listed in the EDL.

In this section, you will add a domain list EDL to an anti-spyware profile.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, select **Objects > Security Profiles > Anti-Spyware**. Select the checkbox next to the **strict** *Anti-Spyware Profile*. Click **Clone**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Clone* window, click **OK**.

3. A new **strict-1** Anti-Spyware Profile should have been created. Click **strict-1** to edit the profile.

4. Rename the profile **outbound-as.** Click the **DNS Policies** tab. Under the *External Dynamic Lists* section, change the **Policy Action** dropdown list to **block.** Click **OK.**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> Palo Alto Networks typically recommends the “sinkhole” action, which will be discussed and used in another lab exercise.

5. Leave the firewall open and continue to the next task.

7.9 Add the Anti-Spyware Profile to a Security Policy Rule

In this section, you will add the **outbound-as** Anti-Spyware Profile to the security policy. The configuration of the profile will enable the firewall to use malicious domain signatures to block access to malicious domains.

1. In the web interface, navigate to **Policies > Security**. Click **Users_to_Internet** to edit the rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Security Policy Rule* window, configure the following on the **Actions** tab. Click **OK**.

Parameter	Value
Profile Type	**Profiles**
Anti-Spyware	**outbound-as**

3. Click the **Commit** button at the upper-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Commit* window, click **Commit**.

5. Wait until the *Commit* process is complete. Click **Close**.

6. Minimize the *Chromium* browser by clicking the **minimize** icon.

7. Return to the *terminal* window by clicking on the **terminal** icon in the taskbar of your *client desktop*.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. From the *terminal* window on the *desktop*, ping two addresses on the internet by issuing the following commands. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping quora.com <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping producthunt.com <Enter>
```

> **Please Note**
> The ping commands should fail because the domains are listed in the custom EDL and the custom EDL was added to the outbound-as Anti-Spyware Profile and configured with the "block" action.

9. Minimize the *Terminal* window.

10. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.

11. Examine the firewall traffic log by ensuring you are at **Monitor > Logs > Threat**. Clear any *filters* in filter builder. You should see several entries indicating that the firewall has blocked DNS queries for the hosts listed in the **malicious-domains-edl.**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note** The order of columns has been rearranged and several columns have been hidden in the example above.

12. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

7.10 Block Access to Malicious URLs Using the Security Policy

In this section, you will block access to known-malicious URLs by configuring the firewall's URL Filtering feature. You will add URL categories to a security policy rule configured to block traffic.

> **Please Note** Although you can configure the security policy to control access to URLs, the URL Filtering Profile more commonly is used to configure the action that a firewall should take when it detects a URL. You will configure a URL Filtering Profile in a later lab section.

1. On the *client desktop*, double-click the folder for **Class-Scripts**.

2. Open the **EDU-210** folder.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Double-click the icon for **Clear Firewall Logs**.

> **Please Note**
> This script uses the XML API to clear the Threat, Traffic and URL Filtering log files. We are clearing the log files to make it easier to identify traffic and threats blocked by DoS Protection.

4. Press **Enter** to start the *Clear Firewall Logs* script. Allow the script to complete. Once the *Clear Firewall Logs* script completes, press **Enter**.

5. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Open a new tab in **Chromium**.

7. Type **`hacker9.com`** which belongs to the *URL category hacking* in the address bar, and press **Enter**.

8. Close the *hacker9.com* tab by clicking the **X** icon.

9. In the web interface, select **Policies > Security**. If the **URL Category** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **down-arrow**) and select **Columns > URL Category.**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> You may need to scroll through the Security Policies to find the URL Category once you have selected to display it.

10. In the *Security Policies* window, click **Add** to create a new security policy rule.

11. In the *Security Policy Rule* window, on the *General* tab, type **`block-known-bad-urls`** as the *Name*. For *Description*, enter **`Blocks bad URL categories.`**

12. Click the **Source** tab and for the *Source Zone*, select **Users_Net**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. Click the **Destination** tab, and for the *Destination Zone*, select **Internet**.

14. Click the **Application** tab and verify that **Any** is selected.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

Parameter	Value
Service	**application-default**
URL Category	Add the following: **adult** **command-and-control** **extremism** **hacking** **high-risk** **malware** **nudity** **parked** **peer-to-peer** **phishing** **proxy-avoidance-and-anonymizers** **questionable**

Please Note

You can type in the first few letters of each category to locate each one more quickly.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

16. Click the **Actions** tab and for the action, select **Deny**. Verify *Log at Session End* is checked. Click **OK**.

17. Select, but do not open, the **block-known-bad-urls** rule in the security policy. Select **Move > Move Top** to move the *block-known-bad-urls* rule to the top of the security policy.

18. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

19. In the *Commit* window, click **Commit**.

20. Wait until the *Commit* process is complete. Click **Close**.

21. Open a new tab in **Chromium**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

22. Type **`hacker9.com`** which belongs to the *URL category hacking* in the address bar, and press **Enter**.

Please Note

The browser should display an error message similar to the following example because the URL category *hacking* is blocked in the security policy. If you get a browser window, it was likely a version cached locally by the browser. Refresh the browser window and access should be blocked.

23. Close the *hacker9.com* tab by clicking the **X** icon.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

24. In the web interface, select **Monitor > Logs > URL Filtering**. If the **URL Category List** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **down-arrow**) and select **Columns > URL Category List**.

Please Note

You should see multiple entries that have been blocked. Several default columns have been hidden in the example URL Filtering log file shown here.

25. Leave the firewall open and continue to the next task.

7.11 Create a Custom URL Category

In this section, you will add your Custom URL Category to a security policy rule that has a "deny" action.

1. Open a new tab in **Chromium**.

2. Type **`www.nbcnews.com`** and press **Enter**. The browser should display a valid webpage.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Close the *nbcnews.com* tab by clicking the **X** icon.

4. In the web interface, select **Objects > Custom Objects > URL Category.** Click **Add**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Custom URL Category* window, configure the following. Click **OK.**

Parameter	Value
Name	`block-per-company-policy`
Description	`URLs that are blocked by company policy.`

Sites	Add the following:
	`*.nbcnews.com`
	`*.theguardian.com`

6. Confirm the *block-per-company-policy* Custom URL is showing in the *URL Category* window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Add your *Custom URL Category* to a security policy rule that has a **deny** action. Select **Policies > Security**. Click **block-known-bad-urls** to edit the rule.

8. Select the **Service/URL Category** tab and click **Add**. Add **block-per-company-policy** to the list. Click **OK**.

9. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. In the *Commit* window, click **Commit**.

11. Wait until the *Commit* process is complete. Click **Close**.

12. Test access to URLs that belong to the *Custom URL Category* that you added to a security policy *deny* rule. Open two new tabs in **Chromium**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. Type **`www.nbcnews.com`** on the first tab and press **Enter**. Type **`www.theguardian.com`** on the second tab and press **Enter**.

> **Please Note** The browser should display an error message because the Custom URL Category in the security policy blocks access to the webpage.

14. Close the *nbcnews* and *theguardian* tabs by clicking the **X** icon.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

15. In the web interface, select **Monitor > Logs > URL Filtering**. If the **URL Category** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **down-arrow**) and select **Columns > URL Category.**

Please Note

You should see multiple entries for sessions to www.nbcnews.com and www.theguardian.com that the firewall has blocked.

16. Leave the firewall open and continue to the next task.

7.12 Create an EDL to Block Malicious URL Access

You can add a list of malicious URLs to a file on an external web server and then configure the firewall to access the list as an EDL. The advantage of this approach is that you can regularly update the malicious URL list without the need to recommit the firewall configuration each time, as you would have to do if you updated a security policy rule with a new URL.

In this section, you will create an EDL to block malicious URL access.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, select **Objects > External Dynamic Lists.** Click **Add**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *External Dynamic Lists* window, configure the following. Click **OK.**

Parameter	Value
Name	**`malicious-urls-edl`**
Type	**URL List**
Source	**`http://192.168.50.80/malicious-urls.txt`** (The EDL contains only the URL www.popurls.com)
Check for updates	**Five Minute**

Please Note

The malicious-urls.txt file contains an entry for popurls.com.

3. In the *External Dynamic Lists* window, click **malicious-urls-edl**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Click **Test Source URL** and verify the firewall can access the *EDL URL*.

5. In the *Test Source URL* window, verify the *Source URL* is accessible. Click **Close**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. In the *External Dynamic List* window, click **OK**.

7. Add the *EDL* containing the malicious URL list to a security policy rule with a *deny* action. In the web interface, select **Policies > Security.** Click **block-known-bad-urls** to edit the rule**.**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the *Security Policy Rule* window, click the **Service/URL Category** tab. Add **malicious-urls-edl** to the list. Click **OK.**

9. Click the **Commit** button at the upper-right of the web interface.

10. In the *Commit* window, click **Commit**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. Wait until the *Commit* process is complete. Click **Close**.

12. Test access to a URL contained in the EDL that you added to the *block-known-bad-urls* security policy. Open a new tab in **Chromium**.

13. Type **`http://www.popurls.com`** in the address bar.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. The browser displays a block page because the EDL in the security policy blocks access to the *popurls.com* webpage.

> **Please Note** The browser should display an error message because the Custom URL Category in the security policy blocks access to the webpage.

15. Close the *popurls.com* tab by clicking the **X** icon.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

16. In the web interface, select **Monitor > Logs > URL Filtering**. Type **`( action eq block-url )`** in the filter builder. You should see multiple entries for sessions to *www.popurls.com* that the firewall has blocked.

17. Leave the firewall open and continue to the next task.

7.13 Block Access to a Malicious URL Using a URL Filtering Profile

Now you will configure a URL Filtering Profile to control access to URLs. You must add the URL Filtering Profile to a security policy rule with an “allow” action. The use of a URL Filtering Profile to block access to URLs typically is easier to maintain over time compared to the addition of URLs to a security policy block rule. You will also enable the Application Block Page, which instructs the firewall to present a warning page to users when they access websites that have been purposely blocked.

In this section, you will block access to a Malicious URL with a URL Filtering Profile and test the URL Filtering Profile.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, select **Device > Response Pages.** Locate the entry for **Application Block Page** and click the link for **Disabled** under the *Action* column.

2. In the *Application Block Page* window, place a **check** in the box for **Enable Application Block Page**. Click **OK.**

3. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Commit* window, click **Commit**.

5. Wait until the *Commit* process is complete. Click **Close**.

6. Test the *Application Block Page* response. Open a new tab in **Chromium**.

7. Type **`www.evilzone.org`** in the address bar, press **Enter**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. The browser displays a block page because the EDL in the security policy blocks access to the *evilzone.org* webpage.

> **Please Note**
> The browser should display a block page because the URL belongs to the URL category *hacking*, which is blocked by a security policy rule. You will continue to block access to this website but will use another method.

9. Close the *evilzone.org* tab by clicking the **X** icon.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. In the web interface, select **Objects > Security Profiles > URL Filtering**. Click **Add** to create a new profile.

11. In the *URL Filtering Profile*, type **`Corp-URL-Profile`** as the *Name* of the profile. For *Description*, enter **`Company URL Filtering profile`**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. On the **Categories** tab, configure the following. You will need to scroll through each *Category* for the value to set it to block the site access.

Parameter	Value
Site Access	Configure the **block** action for the following URL categories: **block-per-company-policy*** (your Custom URL Category) **malicious-urls-edl+** (your custom URL list) **adult** **command-and-control** **extremism** **hacking** **high-risk** **malware** **nudity** **parked** **peer-to-peer** **phishing** **proxy-avoidance-and-anonymizers** **questionable**

Please Note

These categories are the same ones you set to **block** earlier using the URL Category as part of the security policy rule. In this configuration, the firewall will use the URL Filtering profile to block these categories.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. Select the tab for **Inline ML**. For **Phishing Detection** and **Javascript Exploit Detection**, set the **Policy Action** to **block**. Click **OK**.

14. In the web interface, select **Policies > Security.** Click **Users_to_Internet** to edit the rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

15. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. Click **OK**.

Parameter	Value
Action	**Allow**
Log Setting	**Log at Session End**
Profile Type	**Profiles**
URL Filtering	**Corp-URL-Profile**

16. Select, but do not open the *block-known-bad-urls* security policy rule. Click **Delete** to remove the *block-known-bad-urls* rule.

Please Note

This rule no longer will be used to block access to the URLs. Instead, the “Users_to_Internet” rule with its attached URL Filtering Profile will control URL access.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

17. In the *Security Rule* window, click **Yes** to confirm the deletion.

18. Click the **Commit** button at the upper-right of the web interface.

19. In the *Commit* window, click **Commit**.

20. Wait until the *Commit* process is complete. Click **Close**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

21. Test the *Application Block Page* response. Open a new tab in **Chromium**.

22. Type **`www.evilzone.org`** and press **Enter**.

23. The browser displays a block page because the EDL in the security policy blocks access to the *evilzone.org* webpage. If the *Web Page Blocked* message does not appear, allow 1 to 3 minutes for the firewall to process the changes, then refresh the *evilzone.org* tab.

Please Note

The browser should display a block page because the URL belongs to the URL category *hacking*, which is blocked by a security policy rule. You will continue to block access to this website but will use another method.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

24. Close the *evilzone.com* tab by clicking the **X** icon.

25. Examine the URL Filtering Log under **Monitor > Logs > URL Filtering**.

26. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 8: Blocking Threats using App-ID

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Blocking Threats Using App-ID 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Create an FTP Service Object and Port-Based Security Policy Rule 10
1.3 Generate Application Traffic 19
1.4 Configure an Application Group 21
1.5 Configure a Security Policy to Allow Update Traffic 22
1.6 Test the Allow-PANW-Apps Security Policy Rule 27
1.7 Examine the Tasks Lists to See Shadowed Message 28
1.8 Modify the Security Policy to Function Properly 30
1.9 Test the Modified Security Policy Rule 33

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

The old firewalls in your network only allowed you to block or allow traffic using Layer 3 and Layer 4 characteristics. With the deployment of the new Palo Alto Networks firewall, your control over traffic now includes which applications are allowed or blocked into and out of your network.

Some skeptics on your security team still do not fully believe that the Palo Alto Networks firewall can recognize applications beyond their Layer 4 characteristics.

To illustrate application awareness, you will create a Layer 4 object for FTP and use that in a security policy rule. In a later lab, you will convert this security policy rule to use the FTP application instead of the Layer 4 port-based object.

The list of applications that Palo Alto Networks maintains is long, but you already know some of the applications you must allow from and to your security zones. You will create an Application Group and include individual applications that the Palo Alto Networks devices use. You will then use this Application Group as part of a security policy rule. This process will give you practice in creating security policy rules that take advantage of applications instead of simply Layer 3 and Layer 4 traffic characteristics.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Create an FTP Service object and an FTP port-based security policy rule
- Test the port-based security policy
- Generate application traffic
- Configure an application group
- Configure a Security policy to allow updated traffic
- Test the Allow-PANW-Apps security policy rule
- Examine the tasks list to see shadowed message
- Modify the security policy to function properly
- Test the modified security policy rule

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Threats Using App-ID

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-08.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Create an FTP Service Object and Port-Based Security Policy Rule

In this section, you will start by creating an FTP Service object that defines the FTP port. Once you create the FTP Service object, you will create and test a port-based security policy rule that will enable you to simulate part of the process of migrating from a legacy, port-based security policy to a next-generation, application-based security policy.

Lastly, you will generate FTP traffic from the client host to an FTP server in the Extranet zone. Then you will examine the Traffic log to view how the firewall processed the FTP traffic. After you complete this section, you will move on to other tasks related to App-ID. At the end of this lab, you will return to the task of migrating the FTP port-based rule to an application-based rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Navigate to **Objects > Services**. Click **Add** at the bottom of the *Services* window.

2. In the *Service* window, configure the following. Click **OK**.

Parameter	Value
Name	`service-ftp`
Protocol	**TCP**
Destination Port	**21**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the web interface, select **Policies > Security**. Click **Add** at the bottom of the *Security policy* window.

4. On the *General* tab, type **`migrated-ftp-port-based`** as the *Name*. For *Description*, enter **`Migrated from legacy firewall`**.

Please Note

You are creating a rule that simulates a port-based rule that was migrated from another vendor's firewall.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**

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

Parameter	Value
Destination Zone	**Extranet**
Destination Address	**Any**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

Parameter	Value
Applications	**Any**

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

Parameter	Value
Service	**service-ftp**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Click the **Actions** tab and verify the following. Click **OK**.

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

10. Verify the *migrated-ftp-port-based* security policy is visible.

	NAME	TAGS	TYPE	Sour ZONE	ADDRESS
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any
2	Users_to_Extranet	none	universal	Users_Net	any
3	Users_to_Internet	none	universal	Users_Net	any
4	Extranet_to_Internet	none	universal	Extranet	any
5	migrated-ftp-port-ba...	none	universal	Users_Net	any
6	intrazone-default	none	intrazone	any	any
7	interzone-default	none	interzone	any	any

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. Use your mouse pointer to drag-and-drop the **migrated-ftp-port-based** rule to just above the **Users_to_Extranet** rule.

	NAME	TAGS	TYPE	Source		
				ZONE	ADDRESS	USER
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any	any
2	migrated-ftp-port-ba...	none	universal	Users_Net	any	any
3	Users_to_Extranet	none	universal	Users_Net	any	any

12. Click the **Commit** button at the upper-right of the web interface.

13. In the *Commit* window, click **Commit**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. Wait until the *Commit* process is complete. Click **Close**.

15. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

16. On the *client desktop*, open **Terminal Emulator**.

17. Enter the command below to connect to the ftp server at 192.168.50.21.

```
C:\home\lab-user\Desktop\Lab-Files> ftp 192.168.50.21 <Enter>
```

18. Log in with the username **`paloalto42`** and **`Pal0Alt0!`** as the password.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

19. Type **bye** at the FTP command prompt.

```
ftp> bye
```

> **Please Note**
> This command should end the FTP session. An FTP session will be logged on the firewall even though no file was transferred.

20. Close the *terminal* window by typing **`exit`**.

```
C:\home\lab-user\Desktop\Lab-Files> exit <Enter>
```

21. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.

22. In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following filter **`( addr.src in 192.168.1.20 ) and ( app eq ftp )`** in the filter builder.

> **Please Note**
> Some columns have been hidden to provide all the information needed for this step. If you do not hide or move columns, you can use the scroll bar to view the entire traffic log for the FTP session.

23. Minimize the *Chromium* browser by clicking the minimize icon and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Generate Application Traffic

In this section, you will run a short script that generates application traffic from your client workstation to hosts against the Internet and Extranet security zones.

1. On the *client desktop*, double-click the folder for **Class-Scripts**.

2. Open the **EDU-210** folder.

3. Double-click the icon for **App Generator**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Press **Enter** to start the *App Generator* script. Allow the script to complete. Once the *App Generator* script completes, press **Enter**. Allow the script *30* seconds to *1* minute to complete before proceeding to the next step.

5. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.

6. In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following new filter **`( addr.src in 192.168.1.20 )`** in the filter builder. Note the entries in the *Application* column.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
>
> You may need to scroll the pages in the traffic window to see all the entries.
>
> You should see entries for ftp, dns, google-base, ssl, web-browsing, facebook-base and ping. Use the refresh button to update the entries if necessary.

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Configure an Application Group

In this section, you will configure an application group called **paloalto-apps** that includes some Palo Alto Networks applications. These applications are used to label and control access to the content update network and other Palo Alto Networks products and features. You will add the application group to a security policy rule later in this lab exercise.

1. Navigate to **Objects > Application Groups**. Click **Add**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Application Group* window, configure the following. Click **OK**.

Parameter	Value
Name	**`paloalto-apps`**
Applications	**paloalto-dns-security** **paloalto-updates** **paloalto-userid-agent** **paloalto-wildfire-cloud** **pan-db-cloud**

3. Leave the firewall open and continue to the next task.

1.5 Configure a Security Policy to Allow Update Traffic

In this section, you will create a specific security policy rule to enable access to Palo Alto Networks content updates. This configuration is an example of the positive enforcement model where you configure what the firewall should allow rather than only specifying what should be blocked.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, navigate to **Policies > Security.** Click **Add** to configure a new security policy.

2. On the *General* tab, type **`Allow-PANW-Apps`** as the *Name*. For *Description*, enter **`Allows PANW apps for firewall`**.

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

Parameter	Value
Source Zone	**Users_Net**
Source Address	**192.168.1.254**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

Parameter	Value
Destination Zone	**Internet**
Destination Address	**Any**

5. Click the **Application** tab and configure the following.

Parameter	Value
Applications	**paloalto-apps**

Please Note

To locate your **paloalto-apps** Application Group, start typing in the first few letters of the group name, and the interface will display only those entries which match. Application Groups appear at the very end of the Application list.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Click the **Service/URL Category** tab and verify that **application-default** and **Any** are selected.

7. Click the **Actions** tab and verify the following. Click **OK**.

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

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. The **Allow PANW-Apps** rule should be listed just above the *intrazone-default* rule in the security policy rule list.

	NAME	TAGS	TYPE	Sour ZONE	ADDRESS
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any
2	migrated-ftp-port-ba...	none	universal	Users_Net	any
3	Users_to_Extranet	none	universal	Users_Net	any
4	Users_to_Internet	none	universal	Users_Net	any
5	Extranet_to_Internet	none	universal	Extranet	any
6	Allow-PANW-Apps	none	universal	Users_Net	192.168.1.254
7	intrazone-default	none	intrazone	any	any
8	interzone-default	none	interzone	any	any

9. Click the **Commit** button at the upper-right of the web interface.

10. In the *Commit* window, click **Commit**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. When the *Commit* process completes, notice that there is an additional tab available for *Rule Shadow.* Click **Close**.

12. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.6 Test the Allow-PANW-Apps Security Policy Rule

In this section, you will test the new security policy rule for **Allow-PANW-Apps** to see how it is working.

1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
>
> This action instructs the firewall to check for Dynamic Content updates. The application used by the firewall is called *paloalto-updates* and is one that you included in the Application Group called paloalto-apps.

2. Select **Monitor > Logs > Traffic**. Clear any filters you have in place. Create and apply the following filter **`( app eq paloalto-updates )`** in the filter builder.

> Notice the **Users_to_Internet** rule allowed application traffic to pass through the firewall. The firewall traffic did not his the Allow-PANW-Apps rule because the **Users_to_Internet** rule 'shadows' the **Allow-PANW-Apps** rule. Traffic matched the **Users_to_Internet** rule and the firewall carried out the allow action. There is no reason for the firewall to continue comparing packet characteristics to any following rules after it has found a match. Remember: Rule order is important!

3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.7 Examine the Tasks Lists to See Shadowed Message

The firewall provides notification when you have a rule shadowing one or more other rules. The **Rule Shadow** tab appears at the end of the Commit process.

However, you might not always notice the **Rule Shadow** tab, so in this section, you will use the **Task** list to examine your earlier Commit messages.

1. In the bottom-right corner of the *PA-VM firewall* interface, click the **Tasks** button.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Task Manager – All Tasks* window, scroll down and locate the most recent entry for **Commit** under *Type*. Click the link for **Commit**.

3. In the *Job Status – Commit* window, select the **Rule Shadow** tab. The interface shows you which rule is shadowing other rules. **Click** the number under the *Count* (in this example, the value is **1**). Click **Close**.

Please Note

The value under the **Count** column indicates the number of rules that are shadowed. The **Shadowed Rule** column shows you details about which rule is shadowed.
You can use this detailed information to modify your security policy rule order to make certain traffic hits rules in the correct manner

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Task Manager – All Tasks* window, click **Close**.

5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.8 Modify the Security Policy to Function Properly

In this section, you will modify your security policy to ensure that only the Allow-PANW-Apps rule allows Palo Alto Networks content update traffic. This configuration is another example of the positive enforcement model where you configure what the firewall should allow rather than only specifying what should be blocked.

You will also modify the security policy rule that allows traffic from the Users_Net to the Internet. Instead of allowing any application, the modified rule will allow only a few applications.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, navigate to **Policies > Security.** Click **Users_to_Internet** to edit the rule.

2. In the *Security Policy Rule* window, click the **Application** tab and configure the following. Click **OK**.

Parameter	Value
Applications	**dns** **ping** **ssl** **web-browsing**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **Commit** button at the upper-right of the web interface.

4. In the *Commit* window, click **Commit**.

5. Wait until the *Commit* process is complete. Click **Close**.

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.9 Test the Modified Security Policy Rule

In this section, you will test the modified security policy to verify that it is working as expected. You want to verify that Dynamic Update traffic from the firewall uses the **Allow-PANW-Apps** rule.

1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.

2. Select **Monitor > Logs > Traffic**. Apply the following filter **`( app eq paloalto-updates )`** in the filter builder. Look for the log entries for the application *paloalto-updates*. It should be the **Allow-PANW_Apps** rule.

3. Open a new tab in **Chromium**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Type **`www.paloaltonetworks.com`** in the address bar and press **Enter**. Once you have verified the website will open, close the *Chromium* tab by clicking on the **X** icon.

5. Select **Monitor > Logs > Traffic**. Clear any filters you have in place. Create and apply the following filter **`( addr.src eq 192.168.1.20 ) and ( rule eq Users_to_Internet )`** in the filter builder.

Please Note

Notice the App-ID identified the traffic as dns and ssl. The rule "Users_to_Internet" allowed the traffic for both applications.

6. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 9: Maintaining Application-Based Policies

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Maintaining Application-Based Policies 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Create a Custom Service Object for HTTP 11
1.3 Add the New Service to the Security Policy 12
1.4 Test Access to the Web Server on Port 8080 17
1.5 Revert the Web Server to Port 80 20
1.6 Create an FTP Application-Based Security Policy Rule with Policy Optimizer 23
1.7 Manually Create FTP Application-Based Security Policy 30
1.8 Test the Application-Based Security Policy 34
1.9 Remove the FTP Rules 38
1.10 Scheduling App-ID Updates 39

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Your organization runs several common application servers on non-standard ports. For example, there are several web servers in your network that use TCP port 8080 instead of the default TCP port 80. You need to make certain that you configure the firewall to allow web-browsing traffic even when that traffic is using TCP port 8080. To accomplish this task, you will configure a new service object and incorporate it into a security policy rule for web-browsing.

You will also use the Policy Optimizer utility on the firewall to migrate the port-based FTP rule to an application-based rule.

In the last section, you will make certain that your firewall is consistently up to date with the latest signatures and information from Palo Alto Networks. You need to make sure that the firewall downloads and incorporates these updates automatically, so you will schedule the process.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Create a custom Service object for HTTP
- Add the new service to the security policy
- Test Access to the web server on port 8080
- Revert the web server to port 80
- Create an FTP application-based security policy rule
- Test the application-based security policy
- Remove the FTP rules
- Scheduling App-ID updates

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Maintaining Application-Based Policies

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

In this lab, *Task 1.6* is optional. This task includes a step that only updates the Policy Optimizer statistics on the firewall every hour, on the hour. To complete Task 9.6, you will want to be closer to the top of the hour. If you start at the bottom of the hour, please note that the lab will possibly take about two hours to complete due to waiting for the top of the hour.

If you plan on completing *Task 1.6*, it is recommended that you start this lab 30 minutes before the top of the hour to minimize your wait time to complete this lab.

If you choose to skip *Task 1.6*, without using the Policy Optimizer, and manually adding the FTP Application based policy, please continue to start this lab at *Task 1.1*, skip *Task 1.6* and continue on with *Task 1.7* and onwards.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Log in to the firewall web interface as username **admin**, password **Pal0Alt0!.**

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-09.xml** from the *Name* dropdown box and click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.2 Create a Custom Service Object for HTTP

In some networks, servers run common applications on non-standard ports: for example, running a web server on TCP port 8080 instead of TCP port 80. Palo Alto firewalls expect to see HTTP traffic running on the standard TCP port 80 and will block HTTP traffic that is not running on the application default port. To allow this type of non-standard port traffic, you can create a service object and use it as part of your Security policy rule definition.

In this section, you will create a custom service for TCP port 8080. You will add this custom service to the Security policy later in this lab exercise.

1. Navigate to **Objects > Services**. Click **Add** at the bottom of the *Services* window.

2. In the *Service* window, configure the following. Click **OK**.

Parameter	Value
Name	`service-http8080`
Description	`Alternate web service port.`
Protocol	**TCP**
Destination Port	**8080**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Leave the firewall open and continue to the next task.

1.3 Add the New Service to the Security Policy

In this section, you will add a security policy rule to enable the firewall to match and pass web-browsing traffic using the non-standard TCP port 8080.

1. In the web interface, select **Policies > Security**. Click **Add** at the bottom of the security policy window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. On the *General* tab, type **`allow-non-standard-web`** as the *Name*. For *Description*, enter **`Allows web traffic on 8080.`**

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

Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**

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

Parameter	Value
Destination Zone	**Extranet**
Destination Address	**`192.168.50.80`**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click the **Application** tab and verify the following:

Parameter	Value
Applications	**Web-Browsing**

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

Parameter	Value
Service	**service-http8080**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Click the **Actions** tab and verify the following. Click **OK**.

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

8. Select, but do not open, the **allow-non-standard-web** rule in the security policy.

9. Use your mouse pointer to drag-and-drop the **allow-non-standard-web** rule to just above the **Users_to_Extranet** rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. Click the **Commit** button at the upper-right of the web interface.

11. In the *Commit* window, click **Commit**.

12. Wait until the *Commit* process is complete. Click **Close**.

13. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.4 Test Access to the Web Server on Port 8080

In this section, you will test whether the security policy allows access to the web server running on the non-standard TCP port 8080.

1. Open a new tab in **Chromium**.

2. Type **`http://192.168.50.80:8080`** and press **Enter**. The connection will fail because the web server is not using port **8080**. Close the *Chromium* tab after the connection fails.

3. Minimize the *Palo Alto Networks Firewall*.

4. On the *client desktop*, open the **Remmina** application.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Double-click the entry for **Server-Extranet**.

Please Note

This script will connect you to the Extranet lab server using SSH.

6. Run the following command to change the HTTP service port from 80 to 8080.

```
paloalto42@extranet1:~$ /tg/http8080.sh <Enter>
```

7. Leave the **Remmina** connection to the *Extranet* server open.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

9. Open a new tab in **Chromium**.

10. Type **`http://192.168.50.80:8080`** and press **Enter**. You should be connected to the server now that the service port has been changed to *8080*. Close the **Chromium** tab.

11. In the firewall web interface, select **Monitor > Logs > Traffic.** Clear any filters you have in place. Find the log entries for the web traffic to port *8080*. You can use the filter **`( port.dst eq 8080 )`** to find the log entry.

12. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Revert the Web Server to Port 80

In this section, you will run a script on the Extranet host to configure the web server to listen on its standard TCP port 80. You also will remove the Security policy rule that enabled web server access on the non-standard port.

1. Reopen *Remmina* by clicking on the **Remmina** icon in the taskbar.

2. Run the following command to change the *HTTP service port* from **8080** to **80**.

```
paloalto42@extranet1:~$ /tg/http80.sh <Enter>
```

3. Close your *Remmina* connection to the **Extranet server** by entering the command below.

```
paloalto42@extranet1:~$ exit <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In firewall web interface, select **Policies > Security**. Select, but do not open, the **allow-non-standard-web** rule in the security policy.

5. At the bottom of the window, click **Delete** to remove the rule.

6. In the *Security Rule* window, click **Yes** to delete the allow-non-standard-web security policy.

7. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the *Commit* window, click **Commit**.

9. Wait until the *Commit* process is complete, click **Close**.

10. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 Create an FTP Application-Based Security Policy Rule with Policy Optimizer

The goal of this exercise is to simulate the process of migrating from a port-based rule to an application-based rule. In the previous lab, you created a port-based rule that allowed FTP traffic from the Users_Net zone to the Extranet zone and then opened a session to the FTP server.

By now, the beginning of the hour should have passed, so the Policy Optimizer tool should have recorded the FTP traffic through the port-based FTP rule, which will enable you to use the Policy Optimizer tool to migrate from the port-based rule to an application-based rule.

In this section, you will use the Policy Optimizer tool's cloning method to create an application-based rule to match and allow FTP traffic from the Users_Net zone to the Extranet zone.

To complete this task, you will want to be closer to the top of the hour. If you start at the bottom of the hour, please note that the lab will possibly take about two hours to complete due to waiting for the top of the hour.

It is recommended that you start this lab 30 minutes before the top of the hour to minimize your wait time to complete this lab.

If you would like to skip this task without using the Policy Optimizer, and manually add the FTP Application based policy, please skip to task 9.7.

1. On the *client desktop*, double-click the folder for **Class-Scripts**.

2. Open the **EDU-210** folder.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Double-click the icon for **App Generator**.

4. Press **Enter** to start the *App Generator* script. Allow the script to complete. Once the *App Generator* script completes, press **Enter**.

5. Reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.

6. In the *firewall* interface, select **Policies > Security**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. If necessary, open the **Policy Optimizer** panel by clicking the **Up arrow** beneath the list of policies on the left side of the web interface.

8. Select **Policy Optimizer > No App Specified**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. View the *No App Specified* window. If you do not see an entry for **migrated-ftp-port-based** in the list, wait until the top of the hour has passed. The firewall updates these statistics every hour, on the hour.

10. In the *migrated-ftp-port-based* rule, notice the number **1** in the Apps Seen column indicates that only a single application has been seen by this port-based rule. However, this window does not tell you which application. Click **Compare**.

11. In the *Applications & Usage – migrated-ftp-port-based* window, notice the application **ftp** has been seen. Select the **ftp** checkbox to select the application and click **Create Cloned Rule** to create an application-based FTP rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. In the *Clone* window, type **`ftp-application-based`** as the *Name* of the new rule. Click **OK**.

13. In the **No App Specified** window, the **`migrated-ftp-port-based`** rule is removed.

Please Note

The firewall has moved the ftp application from the "migrated-ftp-port-based" rule to the new "ftp-application-based" rule.

14. Select **Policies > Security**. The new **ftp-application-based** rule has been added to your security policy.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
>
> Notice the *Policy Optimizer* moved the new **ftp-application-based** rule to precede the **migrated-ftp-port-based** security rule and match *FTP traffic* before the **migrated-ftp-port-based** rule. Take note of the service listed in the service column. It is **service-ftp**.

15. On the *ftp-application-based* rule, click **service-ftp** in the *Service* column.

16. In the *Service* window, select the **service-ftp** checkbox and then click **Delete** to delete the service.

17. After deleting *service-ftp*, notice the service changed to **application-default**. Click **OK**.

18. Click the **Commit** button at the upper-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

19. In the *Commit* window, click **Commit**.

20. Wait until the *Commit* process is complete, click **Close**.

21. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.7 Manually Create FTP Application-Based Security Policy

> **STOP** If you completed task 9.6 using the Policy Optimizer, skip this task and continue to task 9.8.

In this section, you will manually create an FTP Application-Based Security Policy.

1. In the web interface, select **Policies > Security**. Click **Add** at the bottom of the security policy window.

2. On the *General* tab, type **`ftp-application-based`** as the *Name*. For *Description*, enter **`FTP traffic`**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**

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

Parameter	Value
Destination Zone	**Extranet**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click the **Application** tab and add the following:

Parameter	Value
Applications	**ftp**

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

Parameter	Value
Service	**service-ftp**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Click the **Actions** tab and verify the following. Click **OK**.

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

8. Use your mouse pointer to drag-and-drop the **ftp-application-based** security policy above the **migrated-ftp-port-based** rule.

9. Click the **Commit** button at the upper-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. In the *Commit* window, click **Commit**.

11. Wait until the *Commit* process is complete. Click **Close**.

12. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.8 Test the Application-Based Security Policy

In this section, you will generate FTP traffic from your client host to the FTP server in the Extranet zone. Then you will examine the Traffic log to view how the firewall processed the FTP traffic. The FTP traffic should match the application-based rule and not the port-based rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Ensure you are still viewing the *Security policies*. In the **ftp-application-based** rule, note that the *Hit Count* is **0**.

2. Highlight the entry for the **migrated-ftp-port-based** rule. At the bottom of the window, click **Reset Rule Hit Counter > Selected rules** if it shows a hit count. This number may vary and will not hinder the completion of this task.

3. The *counter* has been reset to **zero** for the *migrated-ftp-port-based* rule. This will allow you to determine whether traffic is hitting the migrated-ftp-port-based rule during a test.

4. Minimize the *Palo Alto Networks Firewall*.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Open the **Terminal Emulator** on the *client desktop*.

6. Issue the following command below.

```
C:\home\lab-user\Desktop\Lab-Files> ftp 192.168.50.21 <Enter>
```

7. Log in with the username **paloalto42** and the password **Pal0Alt0!**.

8. Type **bye** <Enter> at the FTP command prompt. Click the **X** to close the *terminal.*

```
C:\home\lab-user\Desktop\Lab-Files> bye <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Reopen the *Pa-VM firewall* by clicking on the **Chromium** icon in the taskbar.

10. In the web interface, select **Monitor > Logs > Traffic.** Clear any filters you have in place. Apply the filter **`(app eq ftp)`** to help you locate the log entry for the FTP session.

11. Select **Policies > Security**. Examine the **Hit Count** values for the *ftp-application-based* rule and the *migrated-ftp-port-based* rule. The hit count is now reversed because the order of the security rule was to hit the *ftp-application-based* security rule first.

> **Please Note**
>
> In a real migration, you would disable the port-based rule for a while and wait to see if any FTP sessions are affected. After you are confident that the new application-based rule is matching all required FTP traffic, you would delete the port-based rule.

12. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.9 Remove the FTP Rules

In this section, you will remove the application-based and port-based FTP rules from the Security policy.

1. Ensure you are at **Policies > Security**. Use your **Shift-key** and mouse pointer to select both the **ftp-application-based** and **migrated-ftp-port-based** rules.

2. Click **Delete** to remove the rules.

3. In the *Security Rule* window, click **Yes** to confirm the removal.

4. Click the **Commit** link located at the top-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Commit* window, click **Commit**.

6. Wait until the *Commit* process is complete**.** Click **Close**.

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.10 Scheduling App-ID Updates

Keeping the firewall updated with new signatures for threats, viruses, and applications is critical. You can perform the update tasks manually, but a far more efficient method is to schedule the process.

In this section, you will configure the firewall to check for and retrieve any new content updates for Anti-Virus, Vulnerabilities, Threats, and Applications.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.

2. In the row for **Antivirus**, click the link for **None** beside **Schedule**.

3. In the *Antivirus Update Schedule* window, set the *Recurrence* to **Weekly**, select **Sunday** for the *Day*, set the *time* to **03:00,** and set the *Action* to **download-only**. Click **OK**.

Please Note

For this lab, you are setting the Action to download-only. This action means that the firewall will check for new signatures and download them but will not install them. In a production environment, you should use download-and-install for the Action.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Locate the section for **Applications and Threats**. Click the link for the *existing schedule*.

5. In the *Applications and Threats Update Schedule* window, preview the settings. Click **OK**.

6. Scroll down and locate the section for **WildFire**. Click **None** next to *Schedule***.**

7. In the *Wildfire Update Schedule* window, set the *recurrence* to **Every Minute** and set the A*ction* to **download-only**. Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Click the **Commit** link located at the top-right of the web interface.

9. In the *Commit* window, click **Commit** to proceed with committing the changes.

10. When the *Commit* operation successfully completes, click **Close** to continue.

11. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 10: Blocking Threats Using Custom Applications

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Blocking Threats Using Custom Applications 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Gather Custom Application Information 10
1.3 Configure a Packet Capture 12
1.4 Packet Capture Application Traffic 15
1.5 Analyze the Packet Capture 18
1.6 Create a Custom Application with a Signature 20
1.7 Add the Custom Application to the Security Policy 25
1.8 Test the Custom Application 28

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Your company uses a very old application written long ago that provides critical information to the accounting department. This application has not been upgraded yet. There are plans to have a new version developed, but no one seems to have the time to take on the task. You must isolate and secure this application so that the firewall can identify it. However, the application developer (who no longer works for the company) designed the application to run on TCP port 80 and use the HTTP protocol. Because the application is so like general web-browsing, you need to identify unique characteristics of this application traffic so that you can create a custom signature for it.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Gather custom application information
- Configure a packet capture
- Capture application traffic
- Analyze the packet capture
- Create a custom application with a signature
- Add the custom application to the security policy
- Test the custom application signature

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Threats Using Custom Applications

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-10.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.2 Gather Custom Application Information

You will gather information about the traffic that this application uses so that you can create a custom application signature.

1. On the *client desktop*, double-click the folder for **Class-Scripts**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Open the **EDU-210** folder.

3. Double-click the icon for **Custom-App-1**.

4. Press **Enter** to start the *Custom-App-1* script. Allow the script to complete. Once the *Custom-App-1* script completes, press **Enter**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.

6. In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following new filter **`( addr.dst eq 192.168.50.22 )`** in the filter builder. Write down the *Source IP address*, Destination *IP address*, *Port number*, and the *IP protocol*. If the *IP Protocol* column is not displayed, place your mouse pointer over any column header and select **Columns > IP Protocol**.

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 Configure a Packet Capture

In this section, you will configure a packet capture on the firewall's data plane. The goal of the packet capture is to identify a unique bit pattern that can be used to create a custom application signature.

1. In the web interface, select **Monitor > Packet Capture**. Click **Clear All Settings**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Clear All Settings* window, click **Yes**.

3. In the *PCAP settings cleared* window, click **OK**.

4. In the *Configure Filtering* window, click **Manage Filters**.

5. In the *Packet Capture Filter* window, click **Add**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. In the *Packet Capture Stage* window, configure the following. Click **OK**.

Parameter	Value
Id	**1**
Ingress Interface	**ethernet1/2**
Source	**192.168.1.20**
Destination	**192.168.50.22**
Dest Port	**80**
Proto	**6** (This number is assigned to TCP.)
Non-IP	**exclude**

In Internet Protocol v4, there is a value called protocol to associate the next level protocol. 6 is the number assigned to TCP.

7. Toggle the *Filtering* button to **ON**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Under the section for *Configure Capturing*, click **Add** to configure a file for the receive stage on the firewall.

9. In the *Packet Capture Stage* window, configure the following. Click **OK**.

Parameter	Value
Stage	**receive**
File	**`receive-file.pcap`**

10. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Packet Capture Application Traffic

In this section, you will take a packet capture on the firewall while using the Custom Application on the client host.

1. Ensure you are still located at **Monitor > Packet Capture**. Toggle *Packet Capture* to **ON**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Packet Capture Warning* window, click **OK**.

Please Note

The firewall is now actively capturing packets that match the filter you created. The packets are being stored on the firewall in the receive-file.pcap you designated.

3. Minimize the *Palo Alto Networks Firewall*.

4. Open the **EDU-210** folder by clicking on the **File Manager** tab in the taskbar if necessary. Double-click the icon for **Custom-App-1**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Press **Enter** to start the *Custom-App-1* script. Allow the script to complete. Once the *Custom-App-1* script completes, press **Enter**.

6. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.

7. Ensure you are still located at **Monitor > Packet Capture**. Toggle *Packet Capture* to **OFF.**

8. Refresh the web interface display to view the **receive-file** listed in the *Captured Files* panel. Click **receive-file.pcap** to open it in Wireshark and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Analyze the Packet Capture

In this section, you will use Wireshark to analyze the packet capture to discover a unique bit pattern that identifies traffic to the Custom Application.

1. In the *Wireshark* window, find and highlight the first entry for **GET**.

1	0.000000	192.168.1.20	192.168.50.22	TCP	74 56904 → 80 [SYN] Seq=0 Win=2
2	0.000582	192.168.50.22	192.168.1.20	TCP	74 80 → 56904 [SYN, ACK] Seq=0
3	0.000642	192.168.1.20	192.168.50.22	TCP	66 56904 → 80 [ACK] Seq=1 Ack=1
4	0.000681	192.168.1.20	192.168.50.22	HTTP	156 GET /customapp.txt HTTP/1.1
5	0.000717	192.168.50.22	192.168.1.20	TCP	66 80 → 56904 [ACK] Seq=1 Ack=9

2. In the Wireshark window, click **Hypertext Transfer Protocol** to expand the display and notice that the HTTP request header included a **GET /custom-app.txt** entry and the Host **192.168.50.22**.

```
▸ Frame 4: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
▸ Ethernet II, Src: Vmware_99:a0:42 (00:50:56:99:a0:42), Dst: Vmware_8a:91:c4 (00:50:56:8a:91:c4)
▸ Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.50.22
▸ Transmission Control Protocol, Src Port: 56904, Dst Port: 80, Seq: 1, Ack: 1, Len: 90
▾ Hypertext Transfer Protocol
  ▸ GET /customapp.txt HTTP/1.1\r\n
    Host: 192.168.50.22\r\n
    User-Agent: curl/7.58.0\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://192.168.50.22/customapp.txt]
    [HTTP request 1/1]
    [Response in frame: 6]
```

> **Please Note**
> You will use the HTTP GET method, and the URI path customapp.txt to build a custom application signature for the Custom Application

3. Close the **Wireshark** window.

4. Ensure you are still located at **Monitor > Packet Capture**. Click **Clear All Settings**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Clear All Settings* window, click **Yes**.

6. In the *PCAP settings clear* window, click **OK**.

7. In the *Captured Files* window, select the checkbox next to **receive-file-pcap**. Click **Delete**.

8. In the *Packet Capture File* window, click **Yes**.

9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 Create a Custom Application with a Signature

In this section, you will use the information discovered in the packet capture to create a unique signature that can identify HTTP traffic to the Internal Company Custom Application.

1. In the web interface, select **Objects > Applications**. Click **Add**.

2. In the *Application* window, on the **Configuration** tab. Configure the following.

Parameter	Value
Name	**`Custom-App-1`**
Category	**business-systems**
Subcategory	**office-programs**
Technology	**client-server**
Parent App	**None**
Risk	**1**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **Advanced** tab and configure the following.

Parameter	Value
Port	Select **radio button**
Port	Click **Add** and type **`tcp/80`**

4. Click the **Signatures** tab. Click **Add**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Signature* window, configure the following. Click **Add or Condition**.

Parameter	Value
Signature Name	**`Signature-1`**
Scope	**Transaction**
Ordered Condition Match	**Leave selected (Neither choice affects the signature.)**

6. In the *New and Condition – Or Condition* window, configure the following. Click **Add**.

Parameter	Value custom
Operator	**Patten Match**
Context	**http-req-uri-path**
Pattern	**`customapp.txt`**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the *Qualifier* window, configure the following and then click **OK**.

Parameter	Value
Qualifier	**http-method**
Value	**GET**

8. Click **OK** to close the *New And Condition – Or Condition* window.

9. Click **OK** to close the *Signature* window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. Click **OK** to close the *Application* window.

11. To display only custom applications, select **Custom applications** on the filter dropdown menu. A new entry for **Custom-App-1** appears at the top of the *Application* list.

12. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.7 Add the Custom Application to the Security Policy

In this section, you will create a security policy rule that allows hosts in the Users_Net to access the Custom Application in the Extranet zone.

1. Select **Policies > Security**. Click **Add**.

2. In the *Security Policy Rule* window, under the **General** tab, enter **`Allow_Custom_App`** for the *Name*. For *Description*, enter **`Allows users to access custom application in Extranet zone`**.

3. Select the tab for **Source,** under the *Source Zone* section**,** click **Add** and select **Users_Net**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Select the tab for **Destination,** under the *Destination Zone* section, click **Add** and select **Extranet**.

5. Select the **Application** tab, click **Add** and enter the first few letters of the **`Custom-App-1`** name to locate the entry.

6. Select the **Actions** tab and verify that the *Action Setting* is set to **Allow**. Click **OK**.

7. Highlight the **Allow_Custom_App** entry without opening it.

5	Extranet_to_Internet	none	universal	Extranet	any	any	any	Internet
6	Allow-PANW-Apps	none	universal	Users_Net	any	any	any	Internet
7	Allow_Custom_App	none	universal	Users_Net	any	any	any	Extranet

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Use the **Move > Move up** button at the bottom of the window to relocate this rule just above **Users_to_Extranet**.

9. Click the **Commit** link located at the top-right of the web interface.

10. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. When the *Commit* operation successfully completes, click **Close** to continue.

12. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.8 Test the Custom Application

In this section, you will run the Custom Application to determine whether the firewall correctly identifies the traffic.

1. Open the **EDU-210** folder by clicking on the **File Manager** tab in the taskbar if necessary. Double-click the icon for **Custom-App-1**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Press **Enter** to start the *Custom-App-1* script. Allow the script to complete. Once the *Custom-App-1* script completes, press **Enter**.

3. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.

4. In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following new filter **`( addr.dst eq 192.168.50.22 )`** in the filter builder. Notice the *Application* label is **Custom-App-1** and how the custom application enables more granular logging of application traffic. The traffic no longer was generically identified as web-browsing

> **Please Note**
> Note that you may need to use the refresh button several times to see the new entry in the Traffic Log. The sessions must end before the firewall writes an entry to the Traffic log

5. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 11: Blocking Threats with User-ID

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Blocking Threats with User-ID 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Examine Firewall Configuration 10
1.3 Generate Traffic from the Acquisition Zone 13
1.4 Enable User-ID on the Acquisition Zone 16
1.5 Modify the Allow-All-Acquisition Zone 17
1.6 Create Marketing Apps Rule 18
1.7 Create Deny Rule 21
1.8 Generate Traffic from the Acquisition Zone 24
1.9 Exam User-ID Logs 26
1.10 Examine Firewall Traffic Log 28

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Your organization recently acquired another company, and you have been tasked to create appropriate security policy rules for traffic generated by these new users.

Your firewall has been configured with a vWire that allows traffic to the internet from the users in the newly acquired company. The firewall also has a new security zone in place called Acquisition that contains all new users.

The firewall has an existing security policy rule that allows all users in the Acquisition zone to access any application on the internet. Your task is to restrict users in this new organization to approved corporate applications only.

The approved corporate applications include DNS, web-browsing, and SSL.

You also need to ensure that only users in the marketing group are allowed to use social media applications such as Facebook, Instagram, and others.

Another firewall administrator has created the appropriate Application Groups for you.

The firewall receives User-ID and Group membership information about users in this new company from an XML upload sent by network authentication devices. (Note that this is simulated in this lab and outside the scope of this course.)

In this lab, you will create a security policy rule that explicitly denies any other traffic generated by users in the Acquisition zone. Although the interzone-default rule will deny any traffic not expressly allowed, the creation of an explicit deny rule will allow you to examine the kinds of applications users in the Acquisition zone are attempting to access.

Objective

In this lab, you will perform the following tasks:

- Examine current configuration
- Enable User-ID technology on the acquisition zone
- Generate traffic
- Modify security policy to meet requirements

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Threats with User-ID

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-11.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Examine Firewall Configuration

In this section, you will review the settings that another administrator has configured for Application Groups and Security policy rules.

1. Select **Policies > Security**. Click the **Allow-All-Acquisition** policy.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Security Policy Rule*, select the **Source** tab. Note that the *Source Zone* is set to **Acquisition**.

3. Select the **Destination** tab. Note that the *Destination Zone* is set to **any**.

4. Select the **Application** tab. Note that the *Application* is set to **Any**.

5. Select the **Actions** tab. Note that the **Action** is set to **Allow**. Click **OK**.

Please Note

This Security policy rule allows any host in the Acquisition security zone to access any application anywhere.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Clear the counters for all Security policy rules by clicking **Reset Rule Hit Counter > All rules** at the bottom of the window.

7. In the *Reset* window, click **Yes**.

8. Select **Objects > Application Groups** and note the two new **Application Groups.**

Please Note

You will configure the firewall to allow all users in the Acquisition zone to use the Allowed-Corp-Apps. However, only users in the Marketing group will be able to use applications in the Allowed-Mktg-Apps group.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Minimize the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 Generate Traffic from the Acquisition Zone

In this section, you will configure a packet capture on the firewall's data plane. The goal of the packet capture is to identify a unique bit pattern that can be used to create a custom application signature.

1. On the *client desktop*, open the **Remmina** application.

2. Double-click the entry for **Server-Extranet**.

3. In the CLI connection, enter the following command.

```
paloalto42@extranet1:~$ cd /home/paloalto42/pcaps92019/app.pcaps <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the CLI connection, enter the following command.

```
paloalto42@extranet1:~/pcaps92019/app.pcaps$ ./Appgenerator-2.sh <Enter>
```

5. Verify the **Appgenerator-2** script is running.

STOP

Allow the Appgenerator-2 script to complete before continuing to the next step.

6. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Select **Monitor > Logs > Traffic**. Clear any filters in place. Note that almost all traffic is hitting the **Allow-All-Acquisition Rule**. Please allow the firewall 3 to 6 minutes for the traffic logs to update.

Please Note

Some columns have been hidden to show what is presented in the above screen shot. You may hide and show columns as needed for the duration of this lab.

8. Add the **Source User** column, if necessary, to the table by clicking the small triangle in any header and choosing **Columns > Source User**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Drag and drop the **Source User** column between the **Receive Time** and **Source** columns.

RECEIVE TIME	SOURCE USER	SOURCE
08/10 23:46:51		192.168.1.20
08/10 23:46:51		192.168.1.20

> **Please Note** This action will make it easier for you to locate Source User information later in this lab.

10. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Enable User-ID on the Acquisition Zone

In this section, you will enable User-ID on the Acquisition security zone as part of the process of enabling User-ID on a firewall.

1. Select **Network > Zones**. Click **Acquisition** to open the zone.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Zone* window, select the **Enable User Identification** check box. Click **OK**.

3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.5 Modify the Allow-All-Acquisition Zone

In this section, you will now change the set of applications that Acquisition users are allowed to access by modifying the existing **Allow-All-Acquisition** rule.

1. Select **Policies > Security**. Click **Allow-All-Acquisition**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Security Policy Rule* window, under the *General* tab, change the name of this rule to **`Allow-Corp-Apps`**. For *Description*, type **`Allows only approved apps for Acquisition users`**.

3. Select the **Application** tab, uncheck the option for *Any*. Click **Add** and enter the first few letters of the **Allowed-Corp-Apps** to display the *Application Groups* available. Click **OK**.

4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.6 Create Marketing Apps Rule

In this section, you will create a new security policy rule to allow only Marketing users to access the Allowed-Mktg-Applications.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Policies > Security**. Click **Add**.

2. In the *Security Policy Rule* window, under the *General* tab, enter **`Allow-Mktg-Apps`** for the *Name*. For *Description*, enter **`Allows only users of marketing group to access Mktg apps`**.

3. Select the **Source** tab, under *Source Zone*, click **Add.** Select **Acquisition**. Under the *Source User* column, click **Add** and enter **`marketing`**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Select the **Destination** tab. Use the dropdown list at the top to select **any** in the *Destination Zone*.

5. Select the **Application** tab and u*ncheck* the option for **Any**. Click **Add** and enter the first few letters of the **Allowed-Mktg-App**s to display the *Application Groups* available. Select **Allowed-Mktg-Apps**. On the right side of the *Application* window, place a **check** in the checkbox beside **DEPENDS ON.** Click **Add to Current Rule**.

Please Note This action will select all the individual applications under the DEPENDS ON column.

6. Notice the *Applications* have now been added to the *Applications* window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Select the **Actions** tab and verify the *Action* is set to **Allow**. Click **OK**.

Please Note

When you create a new Security policy rule, the default setting for Action is Allow. However, it is always a good practice to verify this setting before closing the window.

8. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.7 Create Deny Rule

In this section, you will create a security policy rule that allows hosts in the Users_Net to access the Custom Application in the Extranet zone.

1. Select **Policies > Security**. Click **Add**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Security Policy Rule* window, under the *General* tab, enter **`Deny-All-Others`** for the *Name*. For *Description*, enter **`Denies non-approved applications for users in Acquisition zone`**.

3. Select the tab for **Source,** click **Add,** and select **Acquisition**.

> **Please Note**
> Note that you do not need to specify any users or user groups under the Source User column. Because the dropdown list is set to any, this rule will deny traffic to any user, regardless of group membership.

4. Select the tab for **Destination,** use the dropdown list at the top to select **any**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Select the tab for **Application** and verify that **Any** is checked.

6. Select the **Actions** tab and change the *Action Setting* to **Deny**. Click **OK**.

7. Verify that the **Deny-All-Others** rule appears at the bottom of the security policy.

If the "Deny-All-Others" rule does not appear at the bottom of the ruleset, use the Move Down button to place the rule just above the "intrazone-default" rule.

8. Click the **Commit** link located at the top-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. In the *Commit* window, click **Commit** to proceed with committing the changes.

10. When the *Commit* operation successfully completes, click **Close** to continue.

11. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.8 Generate Traffic from the Acquisition Zone

In this section, you will generate traffic from the Acquisition zone using the Extranet-Server.

1. Open the **Remmina** application by clicking on the *Server-Extranet* tab in the taskbar if necessary.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Ensure you are still in the **app.pcaps** directory. In the CLI connection, enter the following command.

```
paloalto42@extranet1:~/pcaps92019/app.pcaps$ ./Appgenerator-2.sh
```

3. Verify the **Appgenerator-2** script is running.

STOP

Allow the Appgenerator-2 script to complete before continuing to the next task.

4. Close the **Server-Extranet** connection by clicking the **X** icon.

5. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.9 Exam User-ID Logs

You can see information about User-ID through the firewall CLI or in the web interface. In this section, you will use both tools to examine User-ID entries.

1. Select **Monitor > Logs > User-ID**. The firewall should have numerous entries with *username-to-ip-address* mappings. If the *User* mappings are not showing, repeat **Task 11.8**.

2. Minimize the PA-VM firewall by clicking minimize in the upper-right of the web interface and continue to the next task.

3. On the *client desktop*, in the taskbar, reopen the **Remmina** application.

4. Double-click the entry for **Firewall-A**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. If you get *Connecting to 'Firewall-A'…* window, click **OK**.

> **Please Note**
> The Firewall-A connection in Remmina has been pre-configured to provide login credentials to the firewall so that you do not have to log in each time. This is for convenience in the lab only.

6. In the *firewall CLI*, enter the following command to display entries for *User-ID*. Examine the *User-ID* information.

```
admin@firewall-a> show user ip-user-mapping all <Enter>
```

```
admin@firewall-a> show user ip-user-mapping all

IP                                      Vsys            From    User                            IdleTimeout(s) MaxTimeout(
s)
---------------------------------------- ---------------- ------- ------------------------------- -------------- -----------
10.10.24.102                            vsys1           XMLAPI  chicago\jcaesar                 2078           2078
192.168.1.9                             vsys1           XMLAPI  chicago\nnickleby               2078           2078
10.4.5.101                              vsys1           XMLAPI  chicago\tsawyer                 2078           2078
192.168.1.104                           vsys1           XMLAPI  chicago\mrhyde                  2078           2078
192.168.1.22                            vsys1           XMLAPI  chicago\hpoirot                 2078           2078
192.168.1.43                            vsys1           XMLAPI  chicago\jringo                  2078           2078
192.168.1.36                            vsys1           XMLAPI  chicago\bbill                   2078           2078
192.168.1.41                            vsys1           XMLAPI  chicago\gronimo                 2078           2078
lines 1-11...skipping...
```

7. Close the *Firewall-A* window by clicking the **close** icon.

8. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.10 Examine Firewall Traffic Log

Create and apply filters to view rules and users.

1. Select **Monitor > Logs > Traffic.** In the filter builder, type **`( app eq youtube-base ).`** Click **Apply Filter**.

2. Clear the filter, and in the filter builder, type **`( app eq dns ).`** Click **Apply Filter**.

3. Clear the filter, and in the filter builder, type **`( app eq facebook-base ).`** Click **Apply Filter**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the filter builder, type **`( app eq facebook-base ) and (action eq allow ).`** Click **Apply Filter**.

RECEIVE TIME	SOURCE USER	SOURCE	TYPE	FROM ZONE	TO ZONE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
08/10 23:46:43		192.168.1.35	end	Acquisition	Acquisition	31.13.70.36	443	facebook-base	allow	Allow-All-Acquisition
12/02 04:35:18		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1
12/02 04:35:18		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1
12/02 04:32:04		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1
12/02 04:06:33		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1

5. Clear the filter and in the filter builder, type **`( app eq instagram-base ) and ( user.src eq 'chicago\bbart' ).`** Click **Apply Filter**.

RECEIVE TIME	SOURCE USER	SOURCE	TYPE	FROM ZONE	TO ZONE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
08/11 01:49:10	chicago\bbart	192.168.1.35	deny	Acquisition	Acquisition	31.13.70.174	443	instagram-base	reset-both	Deny-All-Others
08/11 01:47:15	chicago\bbart	192.168.1.35	deny	Acquisition	Acquisition	31.13.70.174	443	instagram-base	reset-both	Deny-All-Others

6. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 12: Blocking Unknown Malware with Wildfire

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Blocking Threats with User-ID 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Create a WildFire Analysis Profile 10
1.3 Apply WildFire Profile to Security Rules 12
1.4 Update WildFire Settings 14
1.5 Test the WildFire Analysis Profile 16
1.6 Examine WildFire Analysis Details 19

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Your company has recently seen an increase in malicious files being downloaded by users. You have sent out informational emails explaining how much damage these types of files can do, and you have told people not to download files from “sketchy” sources.

Fortunately, you have deployed the Palo Alto Networks firewall, and you can set up a Security Profile that will send any unknown files to the WildFire cloud for analysis.

To test the Security Profile after you have configured it, you will download a test file from Palo Alto Networks. This test file is not actually malicious, but WildFire will identify it as such.

You will then examine a detailed report from WildFire with information about the file that was analyzed.

Objective

In this lab, you will perform the following tasks:

- Create a WildFire Analysis Profile
- Apply Wildfire Profile to security rules
- Test the Wildfire Analysis Profile
- Examine Wildfire analysis details

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Threats with User-ID

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-12.xml** from the *Name* dropdown box and click **OK**.

9. In the Loading Configuration window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the commit operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Create a WildFire Analysis Profile

In this section, you will create a WildFire Analysis Security Profile that you can attach to Security policy rules to test files and URLs for malware.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, select **Objects > Security Profiles > WildFire Analysis**. Click **Add**.

2. In the *WildFire Analysis Profile window*, configure the following.

Parameter	Value
Name	`Corp-WF`
Description	`WildFire profile for Corp security rules.`

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click **Add** and configure the following. Click **OK** to close the *WildFire Analysis Profile* window.

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

4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 Apply WildFire Profile to Security Rules

In this section, you will apply the *WildFire Analysis* profile to a security rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Policies > Security**. Click on the **Users_to_Internet** rule.

2. In the *Security Policy Rule* window, select the **Actions** tab. Under *Profile Settings*, use the dropdown list to select **Profiles.** For *WildFire Analysis***,** select **Corp-WF**. Click **OK**.

3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.4 Update WildFire Settings

In this section, you will update the WildFire settings.

1. Select **Device > Setup > WildFire.** Click the **gear** icon to edit the **General Settings**.

2. In the *General Settings* window, check the boxes for **Report Benign Files** and **Report Grayware Files**. Leave the remaining settings unchanged and click **OK**.

3. Click the **Commit** link located at the top-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Commit* window, click **Commit** to proceed with committing the changes.

5. When the *Commit* operation successfully completes, click **Close** to continue.

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Test the WildFire Analysis Profile

In this section, you will test the Wildfire Analysis profile that you added to a security rule.

1. Open a new tab in **Chromium**.

2.
3. Type **`http://wildfire.paloaltonetworks.com/publicapi/test/pe`** and press **Enter**.

> **Please Note** This site generates an attack file with a unique signature that simulates a zero-day attack. A wildfire-test-pe-file.exe file automatically is downloaded to the Downloads directory.

4. Verify the *wildfire-test-pe-file.exe* file successfully downloaded at the bottom of the *Chromium* window.

> **Please Note** You can also verify the wildfire-test-pe-file.exe was successfully downloaded by viewing the downloads folder.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Close the new *chromium* tab that you opened by clicking the **X** icon.

6. Minimize the *Palo Alto Networks Firewall*.

7. On the *client desktop*, open the **Remmina** application.

8. Double-click the entry for **Firewall-A**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. If you get *Connecting to 'Firewall-A'…* window, click **OK**.

10. In the CLI connection to the firewall, enter the command below.

```
admin@firewall-a> debug wildfire upload-log show <Enter>
```

Please Note

The command should 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 display.

The details of the entry you see will differ from the example shown here.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. Type **Exit** to close the SSH session to the firewall.

```
admin@firewall-a> exit <Enter>
```

12. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

13. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.6 Examine WildFire Analysis Details

In this section, you will examine the WildFire Analysis details in the Palo Alto Networks firewall and view a PDF of the Detailed Log view.

1. Select **Monitor > Logs > Wildfire Submissions**. Verify the **wildfire-test-pe-file.exe** is visible.

> **Please Note** Note that in this example several default columns have been hidden, and the details of the entry you see will differ.

> **STOP** Analysis can take 5 to 15 minutes, and the table will remain empty until WildFire has reached a verdict about the file. Do not continue to the next step until the WildFire Submissions is showing.

2. Click the **magnifying glass** icon next to the entry to open the **Detailed Log View** of the entry.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the *Detailed Log View* window, under the *General* section, note the **Verdict**.

4. Click the tab labeled **Wildfire Analysis Report** at the top of the *Detailed Log View*.

5. In the *WildFire Analysis Summary* window, click **Download PDF**. This action will open a PDF version of the *Wildfire Analysis Report* in another tab of the Chromium browser.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Scroll through the report and view the detailed information about the WildFire analysis of the file.

3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

3.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
This is a WildFire test sample WildFire test samples exercise the capabilities of the WildFire analysis engine for purposes of testing.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	

3.1.2. Network Activity

Please Note

For example, section 3.1 provides of the report details about the kind of environment that WildFire used to test the file along with specific actions that the malware file carried out.

7. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 13: Blocking Threats in Encrypted Traffic

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Blocking Threats in Encrypted Traffic 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Test the Firewall Behavior Without Decryption 10
1.3 Create a Self-Signed Certificate for Trusted Connections 13
1.4 Create a Self-Signed Certificate for Untrusted Connections 16
1.5 Create Decryption Policy for Outbound Traffic 18
1.6 Test Outbound Decryption Policy 23
1.7 Export the Firewall Certificate 25
1.8 Import the Firewall Certificate 26
1.9 Test Outbound Decryption Policy Again 30
1.10 Review Firewall Logs 31
1.11 Exclude URL Categories from Decryption 34
1.12 Test the No-Decryption Rule 39

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

As a network security professional, you have noticed a dramatic increase in HTTPS secure traffic over the past few years. Correspondingly, you have noticed that very few websites even use unencrypted HTTP traffic any more. Virtually all network traffic is now encrypted.

You know that HTTPS protects privacy and sensitive data in transit between hosts, but you have begun to realize that HTTPS also hides potentially damaging data as well. Encrypted traffic into and out of your network might contain viruses, spyware, vulnerability exploits, and other damaging types of data.

You need to make certain that the Palo Alto Networks firewall can inspect even encrypted traffic, so you have decided to implement decryption. This process will allow the firewall to decrypt HTTPS traffic, inspect it, and then block any sessions that contain malicious content.

Right now, you do not have budget funds available to request a decryption certificate from a CA (certificate authority). However, you can generate a self-signed certificate on the Palo Alto Networks firewall and deploy that for decryption.

HR has also told you that there are certain types of traffic from employees that should not be decrypted because those transactions might contain personally identifiable information (PII). You need to exclude certain categories of websites (such as finance and healthcare) from decryption. You will create a No-Decrypt rule to prevent the firewall from decrypting traffic to and from these kinds of websites.

Objective

In this lab, you will perform the following tasks:

- Load a lab configuration
- Test the firewall without decryption
- Create a self-signed certificate for trusted connections
- Create a self-signed certificate for untrusted connections
- Create and test a decryption policy rule for outbound traffic
- Test outbound decryption policy rule
- Export the firewall certificate and import to Firefox
- Test outbound decryption policy again
- Review firewall logs
- Exclude URL categories from decryption using a no-decrypt rule
- Test the no-decrypt rule

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

Theoretical Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Threats in Encrypted Traffic

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-13.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Test the Firewall Behavior Without Decryption

In this section, you will test the firewall behavior without decryption by downloading a virus.

1. Open a new tab in **Chromium**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Type **`http://192.168.50.80/eicar.com`** and press **Enter**. You should get a blocked page.

Please Note

Because the connection between the client and the server is not encrypted, the firewall is able to examine the traffic and block malicious content.

In the configuration you loaded to begin this lab, there is an *Antivirus Security profile* applied to security policy rules. The *Antivirus profile* is preconfigured and pre-applied for this exercise so that you can focus on how to configure the firewall to perform decryption. We will examine *Security profiles* (including *Antivirus*) in more detail in later sections of this course.

3. In the new tab, type **`www.eicar.org`**. Press **Enter**.

4. **Click** the *link* for **Download Anti Malware Testfile**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Scroll down and locate the section *Download* area. Right-click the link for the **eicar.com** file and select **Save link as**.

6. In the *Save File* window, save to the *~/Downloads* directory and click **Save**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Notice at the bottom of the *Chromium* window that the download is not blocked because the connection is encrypted, and the virus is hidden. This exercise proves that without decryption, the firewall is unable to examine the contents of an encrypted connection to scan for malicious content.

> **Please Note**
> You can also verify the eicar.com file was successfully downloaded by viewing the downloads folder.

8. Close the two *Chromium* tabs that you just opened.

9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 Create a Self-Signed Certificate for Trusted Connections

In this section, you will generate a certificate on the firewall that will be used when clients connect to HTTPS websites that have certificates issued by trusted certificate authorities.

The firewall will use this certificate as part of the decryption process between clients and trusted HTTPS websites.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Device > Certificate Management > Certificates**. Click **Generate** to create a new *CA Certificate*.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`trusted-cert`
Common Name	`192.168.1.1`
Certificate Authority	**Certificate Authority**

Please Note A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

3. In the *Generate Certificate* window, click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. You should have a new entry in the *Device Certificates* table. Click **trusted-cert**.

5. In the *Certificate information* window, place a **check** in the box for **Forward Trust Certificate**. Click **OK**.

Please Note

This action instructs the firewall to use this certificate to decrypt traffic between clients and trusted HTTPS sites.

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Create a Self-Signed Certificate for Untrusted Connections

In this section, you will generate a certificate on the firewall that will be used when clients connect to HTTPS websites that DO NOT have certificates issued by trusted certificate authorities - for example, sites that use self-signed certificates or certificates that have expired.

The firewall will use this certificate as part of the decryption process between clients and untrusted HTTPS websites.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Click **Generate** to create a new *CA Certificate*.

2. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`untrusted-cert`
Common Name	`untrusted`
Certificate Authority	**Certificate Authority**

Please Note A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

3. In the *Generate Certificate* window, click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. You should have a new entry in the *Device Certificates* table. Click **untrusted-cert**.

5. In the *Certificate information* window, place a **check** in the box for **Forward untrust Certificate**. Click **OK**.

Please Note

This action instructs the firewall to use this certificate to decrypt traffic between clients and HTTPS sites that are not trustworthy (expired certificates, self-signed certificates, etc.).

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.5 Create Decryption Policy for Outbound Traffic

In this section, you will create a Decryption Policy to decrypt HTTPS traffic from the Users_Net security zone to the Internet security zone.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Policies > Decryption**. Click **Add**.

2. In the *Decryption Policy Rule* window, under the **General** tab, configure the following.

Parameter	Value
Name	`Decrypt_User_Traffic`
Description	`Decrypts web traffic from Users_Net.`

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**
Source User	**any**

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

Parameter	Value
Destination Zone	**Internet** **Extranet**
Destination Address	**Any**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click the **Service/URL Category** tab and verify that the *Service* is set to **Any** and that the box for **Any** above *URL Category* is **checked**.

Please Note

Note that the Any setting for URL category instructs the firewall to decrypt all HTTPS traffic, regardless of the type of website users are accessing. Decrypting traffic from users to website categories such as Health and Medicine, Shopping or Government can expose Personally Identifiable Information (PII). In a production environment, you will need to make sure you only decrypt traffic which is appropriate.

Later in this lab, you will exclude several categories of websites as an illustration.

6. Click the **Options** tab and configure the following. Click **OK**.

Parameter	Value
Action	**Decrypt**
Type	**SSL Forward Proxy**
Decryption Profile	**None**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Verify the *Decryption* policy is visible, and the configuration matches the following.

		Source	Destination				
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

8. Click the **Commit** link located at the top-right of the web interface.

9. In the *Commit* window, click **Commit** to proceed with committing the changes.

10. When the *Commit* operation successfully completes, click **Close** to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 Test Outbound Decryption Policy

In this section, you will test the outbound decryption policy.

1. On the client desktop, open the **Firefox Web Browser** application.

2. Type **`https://www.eicar.org`** and press **Enter**. The browser presents a warning message. Click **Advanced**.

> **Please Note**
> The endpoint (client workstation) does not trust the certificate generated by the firewall (192.168.1.1).

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the link for **View Certificate**.

4. Under the section for *www.eicar.org*, note the *Issuer Name* section contains **192.168.1.1**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> This certificate has been issued on behalf of www.eicar.org by the firewall (192.168.1.1) using the Trusted Certificate you created earlier. The client browser does not trust this certificate because it is "self-signed" by the firewall. In the next section, you will fix this issue so that the Firefox browser trusts certificates issued by the firewall.

5. **Minimize** the *Firefox Web Browser*.

6. If you minimized the *firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.

1.7 Export the Firewall Certificate

In this section, you will export the trusted certificate from the firewall.

1. Select **Device > Certificate Management > Certificates**. **Highlight** but do not open *trusted-cert*.

2. At the bottom of the window, click **Export Certificate** to open the *Export Certificate* configuration window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the *Export Certificate – trusted-cert* window, leave all settings unchanged. Click **OK** to export the *trusted-cert* certificate.

> **Please Note** The file will be saved to the workstation's Downloads folder.

4. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.8 Import the Firewall Certificate

In this section, you will import the trusted-cert certificate from the workstation to the Firefox Web Browser.

1. On the client desktop, reopen the Firebox Web Browser by clicking the **Firefox** icon in the taskbar.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the upper-right corner of the window, click the "**hamburger**" button and choose **Preferences**.

3. On the left side of the *Preferences* screen, select **Privacy & Security**.

4. Scroll to the bottom of the screen and locate the *Certificates* section. Click **View Certificates**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Certificate Manager* window, select the **Authorities** tab. Click **Import**.

6. In the *Select File containing CA certificate(s) to import* window, click **Downloads**. Select **cert_trusted-cert.crt** and click **Open**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the *Downloading Certificate* window, place **checks** in both boxes for **Trust this CA**. Click **OK**.

8. The firewall **trusted-cert** entry appears in the list of certificate authorities. Click **OK**.

Please Note

The Firefox browser will trust any certificate issued by the entities in this Authorities list. By adding the firewall certificate to this list, the Firefox browser will trust any certificates issued by the firewall. Note that the process of importing certificates to client workstations varies based on the browser type and the operating system.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. Open a new Firefox tab and continue to the next task.

1.9 Test Outbound Decryption Policy Again

With the firewall trusted-cert certificate imported to Firefox on the client workstation, try downloading the virus file using HTTPS again.

10. In the new *Firefox* tab, type **`https://www.eicar.org`**. Press **Enter**.

11. **Click** the *link* for **Download Anti Malware Testfile**.

12. Scroll down and locate the section *Download area*. Click the link for the **eicar.com** file download.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. You will receive a warning pane from the firewall indicating that it has detected and blocked the malicious file download.

> **Please Note** The kind of message a client receives will vary depending on the browser.

14. Close the *Firefox Web Browser* by clicking the **close** icon.

15. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar and continue to the next task.

1.10 Review Firewall Logs

In this section, you will examine information in the firewall logs to see more details about the decryption process.

1. Select **Monitor > Logs > Traffic.** In the filter builder, type **`( app eq youtube-base ).`** Click **Apply Filter**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Add the **Decrypted** column to the table by selecting **Columns > Decrypted**.

3. Drag and drop the **Session End Reason** column from the right side of the table to the beginning of the table. You may need to *scroll* the *Traffic* window to find the *Session End Reason*.

SESSION END REASON	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED
aged-out	08/11 05:24:05	end	Users_Net	Internet	192.168.1.20	no
aged-out	08/11 05:24:05	end	Users_Net	Extranet	192.168.1.20	no
policy-deny	08/11 05:24:04	deny	Users_Net	Internet	192.168.1.20	no

Please Note

This is not a requirement, but placing this column at the beginning of the table will make it easier for you to locate entries that have ended because of unusual actions taken by the firewall (such as detecting a threat).

4. In the filter builder, type **`( flags has proxy ) and ( session_end_reason eq threat ).`** Click **Apply Filter**. This will display entries that have been decrypted from the client workstation and that have been terminated because of a detected threat in the traffic. If the traffic log is not showing, allow one to two minutes for it to populate.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
>
> The filter syntax “flags has proxy” displays entries which have been decrypted (the value will show as **yes** in the **Decrypted** column). Entries that match the filter indicate that the firewall carried out a proxy connection for decryption.

5. Click the **magnifying glass** next to the entry listed to see details about the session.

		SESSION END REASON	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED
		threat	08/11 05:21:03	end	Users_Net	Internet	192.168.1.20	yes

6. In the *Detailed Log View* window, you should see similar information indicating that the firewall detected the **eicar.com** file and used **reset-server** to terminate the session. Note that several columns have been hidden in the lower section of this example window. Click **Close**.

Detailed Log View

General		Source		Destination	
Session ID	15574	Source User		Destination User	
Action	allow	Source	192.168.1.20	Destination	89.238.73.97
Action Source	from-policy	Source DAG		Destination DAG	
Host ID		Country	192.168.0.0-192.168.255.255	Country	Germany
Application	web-browsing	Port	33806	Port	443
Rule	Users_to_Internet	Zone	Users_Net	Zone	Internet
Rule UUID	2309069a-3647-4c56-be4d-be31f2e85a47	Interface	ethernet1/2	Interface	ethernet1/1
Session End Reason	threat	NAT IP	203.0.113.20	NAT IP	89.238.73.97
		NAT Port	42603	NAT Port	443

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2021/08/11 05:21:03	end	web-browsing	allow	Users_...	23090...	7993		any				
	2021/08/11 05:19:38	virus	web-browsing	reset-server	Users_...	23090...		medium	any				eicar.c...

Close

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Select **Monitor > Logs > Threat**.

8. Delete any filters in place. Notice the entry for virus indicates that the firewall detected and blocked the **eicar.com** file.

		RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	TO ZONE	APPLICATION
		08/11 05:19:38	medium	virus	Eicar Test File	Internet	web-browsing

TO PORT	FROM ZONE	DESTINATION ADDRESS	ACTION	SOURCE ADDRESS	FILE NAME
443	Users_Net	89.238.73.97	reset-server	192.168.1.20	eicar.com

9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.11 Exclude URL Categories from Decryption

The existing decryption policy rule you created instructs the firewall to decrypt all traffic, regardless of the URL category. In this section, you will configure a no-decrypt rule that instructs the firewall to exclude sensitive categories of web traffic from decryption in order to avoid exposing PII (Personally Identifiable Information).

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the firewall web browser, select **Policies > Decryption**. Click **Add**.

2. In the *Decryption Policy Rule* under the *General* tab, enter **`No-Decryption`** for *Name*. For *Description*, enter **`Do not decrypt URLs in gov, shopping and finance`**.

3. Select the tab for **Source.** Under the *Source Zone* section, click **Add** and select **Users_Net**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Select the **Destination** tab. Under the *Destination Zone* section, click **Add** and select **Internet**.

5. Select the tab for **Service/URL Category.** Leave the **Service** set to **any**.

6. Under the *URL Category*, use the **Add** button to add **government, financial-services,** and **shopping**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Select the tab for **Options.** Verify that the *Action* is set to **No Decrypt**. Click **OK**.

8. You should have two entries in the *Decryption* policy. Do you notice what is wrong with the Decryption Policies? The answer is yes. They are in the wrong order. All traffic will match the first rule Decrypt_Users_Traffic because the URL category is set to **any**. The firewall will therefore never proceed beyond that first rule to implement the second rule, which instructs the firewall to exclude financial-services, government, and shopping websites from decryption

		Source	Destination			
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt
2	No-Decryption	Users_Net	Internet	financial-services government shopping	any	no-decrypt

9. Drag and drop the **No-Decryption** rule entry above the **Decrypt_User_Traffic**.

		Source	Destination				
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	No-Decryption	Users_Net	Internet	financial-services government shopping	any	no-decrypt	ssl-forward-proxy
2	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> Always place no-decrypt rules at the beginning of the decryption policy table so that specified packets don't get decrypted when the firewall evaluates rules from top-to-bottom.

10. Click the **Commit** link located at the top-right of the web interface.

11. In the *Commit* window, click **Commit** to proceed with committing the changes.

12. When the *Commit* operation successfully completes, click **Close** to continue.

13. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.12 Test the No-Decryption Rule

With your No-Decryption rule in place, you will test the No-Decryption rule by browsing to a website that falls into one of the excluded categories.

1. On the client desktop, open the **Firefox Web Browser** application.

2. Type **`https://www.texas.gov`** and press **Enter**.

3. Click the **padlock** icon to view the site information window for *texas.gov*. Click the **arrow** next to *Connection secure*.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Connection Security for www.texas.gov* window, click **More Information**.

5. In the *Page Info – https://www.texas.gov* window, click **View Certificate**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Note that the *Issuer Name* is *not* **192.168.1.1**.

Please Note

If the firewall had decrypted this website, the Issuer Name would be displayed as 192.168.1.1. Because you excluded government websites from Decryption, the firewall has not decrypted this site. The issuer name you see may be different from the example shown here.

7. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 14: Preventing Use of Stolen Credentials

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Preventing Use of Stolen Credentials 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Prepare the Lab Environment 10
1.3 Test the Firewall Behavior Without Credential Detection 24
1.4 Apply the Corp-URL-Profile to Security Policy 29
1.5 Provide the Firewall with User-ID Information 32
1.6 Test the Firewall Behavior with Credential Detection 34

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Recently, numerous users in your organization have received phishing emails. Most employees have wisely ignored and deleted emails from unrecognized senders; however, an alarming number of people continue to open suspicious emails and click included links.

You suspect that several users have supplied their work credentials to phishing websites, so you will implement Credential Protection on the Palo Alto Networks firewall.

With Credential Protection in place, the firewall will block employees' attempts to enter work usernames into external websites.

Objective

In this lab, you will perform the following tasks:

- Create a self-signed certificate for trusted connections
- Create a self-signed certificate for untrusted connections
- Export the firewall certificate and import to Firefox
- Test the firewall behavior without credential detection
- Provide the firewall with User-ID information
- Test the firewall behavior with credential detection

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Preventing Use of Stolen Credentials

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-14.xml** from the *Name* dropdown box and click **OK**.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Prepare the Lab Environment

To start this lab exercise, you will continue from the configuration you completed in the previous lab on Decryption. This action will allow you to reconfigure the certificate needed for the firewall and import it to the Firefox browser.

You will re-generate a certificate on the firewall that will be used when clients connect to HTTPS websites that DO NOT have certificates issued by trusted certificate authorities - for example, sites that use self-signed certificates or certificates that have expired. You will also create a Decryption Policy to decrypt HTTPS traffic from the Users_Net security zone to the Internet security zone.

Remember that certificates are very important to help keep integrity between the client and the Palo Alto Networks Firewall. The firewall will use this certificate as part of the decryption process between clients and untrusted HTTPS websites.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Device > Certificate Management > Certificates**. Click **Generate** to create a new *CA Certificate*.

2. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`trusted-cert`
Common Name	`192.168.1.1`
Certificate Authority	**Certificate Authority**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note** A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

3. In the *Generate Certificate* window, click **OK**.

4. You should have a new entry in the *Device Certificates* table. Click **trusted-cert**.

5. In the *Certificate information* window, place a **check** in the box for **Forward Trust Certificate**. Click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> This action instructs the firewall to use this certificate to decrypt traffic between clients and trusted HTTPS sites.

6. Click **Generate** to create a new *CA Certificate*.

7. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`untrusted-cert`
Common Name	`untrusted`
Certificate Authority	**Certificate Authority**

> **Please Note**
> A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the *Generate Certificate* window, click **OK**.

9. You should have a new entry in the *Device Certificates* table. Click **untrusted-cert**.

10. In the *Certificate information* window, place a **check** in the box for **Forward untrust Certificate**. Click **OK**.

Please Note

This action instructs the firewall to use this certificate to decrypt traffic between clients and HTTPS sites that are not trustworthy (expired certificates, self-signed certificates, etc.).

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. Select **Device > Certificate Management > Certificates**. **Highlight** but do not open *trusted-cert*.

12. At the bottom of the window, click **Export Certificate** to open the *Export Certificate* configuration window.

13. In the *Export Certificate – trusted-cert* window, leave all settings unchanged. Click **OK** to export the *trusted-cert* certificate.

Please Note The file will be saved to the workstation's Downloads folder.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. Select **Policies > Decryption**. Click **Add**.

15. In the *Decryption Policy Rule* window, under the *General* tab, configure the following.

Parameter	Value
Name	`Decrypt_User_Traffic`
Description	`Decrypts web traffic from Users_Net.`

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

16. Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**
Source User	**any**

17. Click the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	**Internet** **Extranet**
Destination Address	**Any**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

18. Click the **Service/URL Category** tab and verify that the **Service** is set to **any** and that the box for **Any** above *URL Category* is **checked**.

Please Note

Note that the Any setting for URL category instructs the firewall to decrypt all HTTPS traffic, regardless of the type of website users are accessing. Decrypting traffic from users to website categories such as Health and Medicine, Shopping or Government can expose Personally Identifiable Information (PII). In a production environment, you will need to make sure you only decrypt traffic which is appropriate.

Later in this lab, you will exclude several categories of websites as an illustration.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

19. Click the **Options** tab and configure the following. Click **OK**.

Parameter	Value
Action	**Decrypt**
Type	**SSL Forward Proxy**
Decryption Profile	**None**

20. Verify the Decryption policy is visible, and the configuration matches the following.

	NAME	Source ZONE	Destination ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

21. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

22. On the *client desktop*, open the **Firefox Web Browser** application.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

23. In the upper-right corner of the window, click the "**hamburger**" button and choose **Preferences**.

24. On the left side of the *Preferences* screen, select **Privacy & Security**.

25. Scroll to the bottom of the screen and locate the *Certificates* section. Click **View Certificates**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

26. In the *Certificate Manager* window, select the **Authorities** tab. Click **Import**.

27. In the *Select File containing CA certificate(s) to import* window, click **Downloads**. Select **cert_trusted-cert.crt** and click **Open**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

28. In the *Downloading Certificate* window, place **checks** in both boxes for **Trust this CA**. Click **OK**.

29. The firewall **trusted-cert** entry appears in the list of certificate authorities. Click **OK**.

Please Note

The Firefox browser will trust any certificate issued by the entities in this Authorities list. By adding the firewall certificate to this list, the Firefox browser will trust any certificates issued by the firewall. Note that the process of importing certificates to client workstations varies based on the browser type and the operating system.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

30. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

31. Click the **Commit** link located at the top-right of the web interface.

32. In the *Commit* window, click **Commit** to proceed with committing the changes.

33. When the commit operation successfully completes, click **Close** to continue.

34. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Test the Firewall Behavior Without Credential Detection

In this section, you will connect to an internet website and enter a fictitious user's domain credentials. This action will allow you to see how the firewall behaves without Credential Detection configured.

1. Open a new tab in **Chromium**.

2. Type **`https://login.paloaltonetworks.com`** and press **Enter**. Click **Advanced** and **Proceed to login.paloaltonetworks.com (unsafe)**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. For *Username*, enter **`sholmes`.** Click **Next.**

4. In the *Sign In* window, enter **1234** as the *password*. Click **Sign In**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Because there is no account for **sholmes**, the site will present you with the *Username or password provided is incorrect* message.

6. Close the *Chromium tab* for the *Palo Alto Networks SSO* by clicking the **X** icon.

7. In the firewall web interface, select **Network > Zones**. Click the entry for the **Users_Net** to edit it.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the *Zone* window, click **Enable User Identification**. Click **OK**.

9. Select **Objects > Security Profiles > URL Filtering**. Click the entry for **Corp-URL-Profile**.

10. Select the tab for **User Credential Detection**. Select **Use IP User Mapping** for *User Credential Detection***.** Change the dropdown for *Valid Username Detected Log Severity* to **critical**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *URL Filtering Profile*, select **Categories**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Select set all **Credential Submission** actions to **block**. Click the small triangle next to the column header for *User Credential Submission***.** Hover your mouse over **Set All Credential Submission Actions** and select **block**. Click **OK**.

Please Note

Note that setting all URL categories to block credential submissions is not a good idea in a production environment because no users would be able to submit any credentials to any website. In this lab, you will use this setting so that you do not have to select individual categories and change the option.

13. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Apply the Corp-URL-Profile to Security Policy

In this section, you will apply the Corp-URL-Profile to the security policy rule, which allows user traffic to reach the internet.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Policies > Security**. Click the **Users_to_Internet** security policy.

2. In the *Security Policy Rule* window, click the **Actions** tab. Under *Profile Settings*, use the dropdown list to select **Profiles**. For *URL Filtering*, select **Corp-URL-Profile**. Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **Commit** link located at the top-right of the web interface.

4. In the *Commit* window, click **Commit** to proceed with committing the changes.

5. When the commit operation successfully completes, click **Close** to continue.

6. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

7. Close the *Preferences – Mozilla Firefox* window by clicking the **X** icon.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Provide the Firewall with User-ID Information

In this section, you will run a short script that generates application traffic from your client workstation to hosts in the internet and Extranet security zones.

1. On the *client* desktop, double-click the folder for **Class-Scripts**.

2. Open the **EDU-210** folder.

3. Execute the **User-ID Data** script by double-clicking it.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Notice the *Terminal* window will pop up. Allow the *User-ID Data* script to finish before moving to the next step. Press **Enter**.

Please Note

This script uses the XML API to send a list of users, IP addresses and groups to the firewall.

5. Close the *EDU-210 - File Manager* window by clicking the **X** icon.

6. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the taskbar.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Select **Monitor > User-ID**. You should see numerous entries indicating that the firewall has User-to-IP mappings.

8. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.6 Test the Firewall Behavior with Credential Detection

In this section, you will test the firewall behavior with credential detection.

1. On the *client desktop*, open the **Firefox Web Browser** application.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Type **`https://login.paloaltonetworks.com`** and press **Enter**. For *Username*, enter **`sholmes`**. Click **Next.**

3. The firewall will present a window indicating that you have submitted your credentials to a blocked site. Close the *Firefox browser* using the **X** icon.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
>
> Recall that before configuring Credential Detection, the firewall allowed you to submit the username and even a password to the website. With Credential Detection enabled, the firewall blocks the session when you submit a username which belongs to the domain.

4. Reopen the *firewall* web interface by clicking on the **Chromium** icon in the taskbar.

5. Select **Monitor > URL Filtering**. Modify the URL Filtering table by adding the **Credential Detected** and **Decrypted** columns.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Clear any filters you may have in place. In the *filter* field, enter the following filter **`( action eq block-url )`** to display only entries that have been blocked. Press **Enter** to apply the filter.

7. Note the information displayed under the *Credential Detected* column. Click the **magnifying glass** icon to see more detailed information about this entry.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the *Detailed Log View* window, scroll down and locate the *Flags* section. Note the checkbox for **Decrypted,** which indicates that the firewall decrypted this traffic and was able to detect an attempted credential submission.

9. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 15: Implementing Day-One Best Practice Configuration

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Blocking Threats in Encrypted Traffic 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Generate Traffic Without Security Profiles 10
1.3 Modify Existing Security Policies 15
1.4 Create A Corporate Vulnerability Security Profile 17
1.5 Create A Corporate File Blocking Profile 20
1.6 Create Data Filtering Profiles 22
1.7 Create a Security Profile Group 25
1.8 Apply the Corp-Profiles-Group to a Security Policy 27
1.9 Generate Attack Traffic with Security Profiles 29
1.10 Create Tags 34
1.11 Apply Tags to Security Policy Rule 35
1.12 Enforce Rule Tags and Description Requirements 38
1.13 Test Rule Requirements 42

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

You intend to cut over, all production networks to use the Palo Alto Networks firewall this weekend during a maintenance window. Before the change, you want to implement as many of the best practices from Palo Alto Networks as you can before the firewall cut over. You realize that maintaining a secure network is a continuous process and that you will need to review logs, alerts, and reports each day to help you fine-tune the configuration.

Nevertheless, there are several tasks that you can complete before the firewall goes into production so that you start with a solid, secure network.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Generate traffic without profiles and examine logs
- Create security profiles
- Create a security group
- Apply the security group to existing security policy rules
- Generate traffic with profiles and examine logs
- Create tags
- Enable policy rulebase settings and observe behavior

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Threats in Encrypted Traffic

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-15.xml** from the *Name* dropdown box and click **OK**.

9. In the Loading Configuration window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the *Commit* operation successfully completes, click **Close** to continue.

The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.2 Generate Traffic Without Security Profiles

In this section, you will create a new security policy rule and attempt to leave out the description. This will let you see what happens when an administrator does not provide adequate information when creating a rule.

1. On the *client desktop*, open the **Remmina** application.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Double-click the entry for **Server-Extranet**.

> **Please Note** This action will open an SSH connection to the server and automatically log you in with appropriate credentials.

3. In the CLI connection, enter the following command to change the working directory.

```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcaps/ <Enter>
```

4. In the CLI connection, enter the following command to run the simulated attacks.

```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>
```

> **Please Note** This script takes about 6 minutes to complete. Allow the **malwareattacks** script to run uninterrupted.

5. Minimize the *Remmina* connection window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. On the *client desktop*, open the **Firefox Web Browser** application.

7. Type **`http://192.168.50.80/badtarfile.tar`** and press **Enter**.

8. In the *Opening badtarfile.tar* window, select **Save File**. Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

9. In the *Firefox Web Browser*, open a new tab. Type **`http://192.168.50.80/companyssns.txt`** and press **Enter.** The browser will display a file with *fictitious names* and *social security numbers.*

10. Close the *Firefox browser*.

11. On the *client desktop*, open **Terminal Emulator**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Enter the following command to generate a DNS query using **dig** to resolve a URL to an IP address. The command returns a public IP address, indicating that the URL is accessible.

```
C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com
```

Please Note

Quora.com is one of the entries included in the malicious domains external dynamic list you configured in an earlier lab.

Also note that you may see a different IP address than what the screen shot shows.

13. Leave the Terminal Emulator window open because you will use it again later in this lab.
14. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the taskbar.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Modify Existing Security Policies

In previous labs, you created Security Profiles to inspect traffic for spyware and virus signatures. You created a Security Profile for WildFire that forwards unknown executable files to the WildFire cloud for inspection. And you created a URL Filtering Profile to prevent users from browsing to potentially harmful categories of websites.

In this section, you will review these profiles.

1. Select **Objects > Security Profiles > Antivirus**. Click **Corp-AV.**

2. In the *Antivirus Profile* window, for *Description*, enter **`Standard antivirus profile for all security policy rules`**. Check the box for **Enable Packet Capture**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> Enabling Packet Capture instructs the firewall to take very small packet captures (more like packet snippets) that contains patterns in traffic which match the signatures used in the profile.

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

4. Select **Objects > Security Profiles > Anti-Spyware**. Click **outbound-as**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. In the *Anti-Spyware Profile* window, change the *Name* to **Corp-AS**. Select the tab for **DNS Policies.**

6. On the *DNS Policies* tab, for the **malicious-domains-edl** entry, change the *Policy Action* to **sinkhole**. Change the *Packet Capture* to **single-packet.** Click **OK.**

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Create A Corporate Vulnerability Security Profile

In this section, you will create a vulnerability Security Profile. Palo Alto Networks provides two vulnerability profiles which you can use as the basis for your own – strict and default.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Objects > Security Profiles > Vulnerability Protection**. Place a check in the box beside **strict.** Click **Clone.**

2. In the *Clone* window, click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the entry for **strict-1** to open it.

4. In the *Vulnerability Protection Profile* window, change the *Name* to **`Corp-Vuln`**. For *Description*, enter **`Standard vulnerability profile for all security policy rules`**. Click **OK**.

5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.5 Create A Corporate File Blocking Profile

In this section, you will configure a File Blocking Security Profile that the firewall will use to help detect, report, and block attempts to download potentially harmful filetypes. Palo Alto Networks provides two file blocking profiles that you can use as the basis for your own – basic file blocking and strict file blocking.

You will clone the strict file blocking profile and modify it to function as your Corp-FileBlock profile.

1. Select **Objects > Security Profiles > File Blocking**. Place a check beside the entry for **strict file blocking**. Click **Clone**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Clone* window, click **OK**.

3. Click the entry for **strict file blocking-1** to open it.

4. Change the *Name* to **`Corp-FileBlock`**. For *Description*, enter **`Standard file blocking profile for all security policy rules`**. Click **OK**.

5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 Create Data Filtering Profiles

Create a data filtering profile to detect and block the transfer of files that contain more than three US social security numbers. Data Filtering Profiles are based on one or more Data Patterns, so you will need to first configure a Data Pattern that matches variations of US social security numbers.

1. Select **Objects > Custom Objects > Data Patterns**. Click **Add**.

2. In the *Data Patterns* window, for *Name*, enter **US-SSNs**. For *Description*, enter **`US Social Security Numbers`**. Change the *Pattern Type* to **Predefined Pattern**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click **Add** and scroll down the available list and select **Social Security Numbers**. Click **Add** again and select **Social Security Numbers (without dash separator)**. Click **OK**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Select **Objects > Security Profiles > Data Filtering**. Click **Add**.

5. In the *Data Filtering Profiles* window, for *Name*, enter **`Corp-DataFilter`**. For *Description*, enter **`Standard data filtering profile for all security rules.`**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Click **Add** and select the **US-SSNs** data pattern that you defined. Click in the **Alert Threshold** field and change the value to **1.** Click in the **Block Threshold** field and change the value to **3.** Change the **Log Severity** to **critical.** Click **OK.**

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.7 Create a Security Profile Group

To simplify the process of applying Security Profiles to Security policy rules, you can create a Security Profile Group which contains individual Security Profiles.

You can then apply the Security Profile Group to a Security policy rule, rather than individually selecting each profile for each rule.

In this section, you will create a Security Profile Group called Corp-Profiles-Group. You will add each of your Corp-* Security Profiles to the group.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

2. In the *Security Profile Group* window, enter **`Corp-Profiles-Group`** for the *Name*. For each of the available **Profiles**, use the dropdown list to select the **Corp-*** entry you have created. Click **OK**.

3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.8 Apply the Corp-Profiles-Group to a Security Policy

In this section, you will apply the Corp-Profiles-Group to a security policy. With the Security Profiles in place, you can modify your security policy rules to use these protections.

1. Select **Policies > Security**.

2. Individually edit each security policy rule which allows traffic and change the **Profile Setting** under the **Action** tab to use the **Corp-Profiles-Group**. Be sure to edit and modify each of these rules.

   - **Users_to_Extranet –** Click **OK.**
   - **Users_to_Internet –** Click **OK**
   - **Extranet_to_Internet –** Click **OK**
   - **Extranet_to_Users_Net –** Click **OK**
   - **Allow-PANW-Apps –** Click **OK**
   - **Acquisition-Allow-All –** Click **OK**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Verify each of the rules you modified is showing the *Corp-Profiles-Group* by hovering over the **Profile** icon for each rule.

4. Click the **Commit** link located at the top-right of the web interface.

5. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. When the *Commit* operation successfully completes, click **Close** to continue.

7. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.9 Generate Attack Traffic with Security Profiles

In this section, you will generate attack traffic with security policies.

1. Reopen the **Remmina** application by clicking the icon in the taskbar.

2. In the CLI connection, enter the following command to change the working directory. If you are already in the *attack.pcaps* directory, please proceed to the next step.

```
paloalto42@extranet1:~$ cd pcaps92019/attack.pcap/ <Enter>
```

3. In the CLI connection, enter the following command to run the simulated attacks.

```
paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>
```

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> This script takes about 6 minutes to complete. Allow the **malwareattacks** script to run uninterrupted.

4. Minimize the *Remmina* connection window.

5. On the *client desktop*, open the **Firefox Web Browser** application.

6. Type **`http://192.168.50.80/badtarfile.tar`** and press **Enter**.

7. You should receive a **File Transfer Blocked** page from the firewall.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In *Firefox*, open a new tab. Type **`http://192.168.50.80/companyssns.txt`** and press **Enter.**

9. You should receive a **Data Transfer Blocked** page from the firewall.

This page indicates that the firewall has blocked the transfer using the Data Filtering Profile and Data Pattern you defined for Social Security Numbers.

10. Close the *Firefox Web Browser* by clicking the **close** icon.

11. On the client workstation, locate the open Terminal Emulator window you used earlier in this lab. You can maximize by clicking the **Terminal** icon in the taskbar.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

12. Enter the following command to generate a DNS query using **dig** to resolve a URL to an IP address. The command returns a public IP address, indicating that the URL is accessible. It will now show the **www.quora.com** *DNS query* is now in the **sinkhole.paloaltonetworks.com**.

```
C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com
```

Please Note

This indicates that the firewall has intercepted and sinkholed the DNS query using the DNS Sinkholing function in your Anti-Spyware profile.

13. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the *taskbar*.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. In the firewall web interface, select **Monitor > Logs > Threat**. Clear any filters in place and press **Enter**. The Threat Log should contain numerous entries for *Spyware* and *Vulnerabilities*.

Please Note

These entries indicate that the firewall has blocked malicious traffic using the Vulnerability and Anti-Spyware profiles that you defined. Note that the entries you see in the Threat Log may differ from the example shown here. The table may not contain very many entries until the malwareattacks script is finished. Use the refresh button periodically to update the table. Also, several Threat Log columns have been hidden in this example.

15. Select **Monitor > Logs > URL Filtering**. Note the numerous entries for blocked URLs.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> These entries indicate that the firewall has blocked access to dangerous URL categories using the URL Filtering profile you defined. Note that several default columns have been hidden in this example.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.10 Create Tags

You can create color-coded labels for use in various places within the firewall web configuration. These labels can be visual aids that help you more quickly locate information. In this section, you will create Tags to use with your security policy rules.

1. Select **Objects > Tags.** Click **Add.**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. In the *Tag* window, Enter **`Allow`** for the *Name*. For *Color*, select **Lime**. For *comments,* type **`Tag for allowed traffic`**. Click **OK**.

3. In the *Tags* window, click **Add** again.

4. In the *Tag* window, Enter **Block** for the Name. For *Color*, select **Red**. For *Comments,* type **`Tag for blocked traffic`**. Click **OK**.

5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.11 Apply Tags to Security Policy Rule

With the Tags defined, you can assign them to your security rules. You will assign the Allow tag to all rules which have an action of Allow. You will assign the Blocked tag to all rules which have an action of Deny.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the firewall web browser, select **Policies > Security**.

2. If the *Tags* column is not showing, add the **Tags** column to the display. Click the small triangle in the column header for *Name*. Select **Columns** and **check** the box for **Tags**.

> **Please Note** Note that if you have already displayed the Tags column in the Security Policy Rule table, you can drag and drop it beside the Name column.

3. In the row for *Block-Known-Bad-IPs*, click the link for **none** under the *Tags* column. In the *Tagging window*, select **Block** from the dropdown box. Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Repeat this process for each remaining rule in the list, applying the appropriate **Allow** or **Blocked** tag, depending on the rule action.

   - **Users_to_Extranet –** Click **OK.**
   - **Users_to_Internet –** Click **OK**
   - **Extranet_to_Internet –** Click **OK**
   - **Extranet_to_Users_Net –** Click **OK**
   - **Allow-PANW-Apps –** Click **OK**
   - **Acquisition-Allow-All –** Click **OK**

5. When complete, your rules should match the following example.

	NAME	TAGS	TYPE
1	Block-Known-Bad-IPs	Block	universal
2	Users_to_Extranet	Allow	universal
3	Users_to_Internet	Allow	universal
4	Extranet_to_Internet	Allow	universal
5	Extranet_to_Users_N...	Allow	universal
6	Allow-PANW-Apps	Allow	universal
7	Acquisition-Allow-All	Allow	universal

Please Note

Note that this is a simple illustration of how to create and apply Tags to your security policy rules. You can also apply more than one Tag to your rules.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Click the **Commit** link located at the top-right of the web interface.

7. In the *Commit* window, click **Commit** to proceed with committing the changes.

8. When the *Commit* operation successfully completes, click **Close** to continue.

9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.12 Enforce Rule Tags and Description Requirements

You can force firewall administrators to supply information in the *Description* field of security policy rules and to apply a **Tag** as well. This additional information can help you determine why a rule has been created and what it was meant to accomplish.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Device > Setup > Management**. Scroll down and locate the section for *Policy Rulebase Settings***.** Click the **gear** icon to edit these settings.

2. In the *Policy Rulebase Settings* window, check the boxes for **Require description on policies** and **Fail commit if policies have no tags or description**. Click **OK**.

Please Note If you check the option for Require Tag on policies, you will need to modify your NAT Policy rules and assign a Tag to each of them.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. Click the **Commit** link located at the top-right of the web interface.

4. In the *Commit* window, click **Commit** to proceed with committing the changes.

5. You should see a message indicating that one of the rules does not have a **Description**. When the commit operation successfully completes, click **Close** to continue.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Select **Policies > Security**. Click the **Acquisition-Allow-All** rule to open it.

7. In the *Security Policy Rule* window, on the *General* tab, enter **Allows traffic from acquisition zone** for the *Description*. Click **OK**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Click the **Commit** link located at the top-right of the web interface.

9. In the *Commit* window, click **Commit** to proceed with committing the changes.

10. When the *Commit* operation successfully completes, click **Close** to continue.

11. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.13 Test Rule Requirements

In this section, you will create a new security policy rule and attempt to leave out the description. This will let you see what happens when an administrator does not provide adequate information when creating a rule.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Ensure you are at **Policies > Security**. Click **Add**.

2. In the *Security Policy Rule* window, enter **`Test-Policy`** for the *Name*. Click inside the **Description** field and note the pop-up indicator. Click **Cancel**.

3. The lab is now complete; you may end your reservation.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 16: Viewing Threat and Application Information

Document Version: 2022-07-19

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Blocking Threats in Encrypted Traffic 6
1.1 Apply a Baseline Configuration to the Firewall 6
1.2 Generate Traffic 10
1.3 Display Recent Threat Information in the Dashboard 13
1.4 Display Recent Application Information in the Dashboard 16
1.5 View Threat Information in the ACC 18
1.6 View Application Information in the ACC 22
1.7 View Threat Information in the Threat Log 26
1.8 View Application Information in the Traffic Log 31
1.9 View Threats Using App Scope Reports 36

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

Having worked with the new Palo Alto Networks firewall, you have discovered how much information the device provides about traffic that it processes. You have already worked with the Traffic, Threat, URL, and System log files and learned how to create filters to locate specific information. But before you roll the firewall into production, you want to spend some time looking at some of the other resources, graphs, reports, and tools that are available.

You will also need to show your colleagues where to find different kinds of information in the firewall web interface so that they can assist you in keeping your network as secure as possible.

Objective

In this lab, you will perform the following tasks:

- View threat information using the Dashboard
- View application information using the Dashboard
- View threat information using the ACC
- View application information using the ACC
- View threat information using the Threat log
- View application information using the Traffic log
- View threat information using App Scope reports

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Blocking Threats in Encrypted Traffic

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-lab-16.xml** from the *Name* dropdown box and click **OK**.

9. In the Loading Configuration window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

10. Click the **Tasks** icon located at the bottom-right of the web interface.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

12. Click the **Commit** link located at the top-right of the web interface.

13. In the *Commit* window, click **Commit** to proceed with committing the changes.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

14. When the commit operation successfully completes, click **Close** to continue.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.2 Generate Traffic

In this section, you will create a new Security policy rule and attempt to leave out the Description. This will let you see what happens when an administrator does not provide adequate information when creating a rule.

1. On the client desktop, open the **Remmina** application.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Double-click the entry for **Server-Extranet**.

> **Please Note**
> This action will open an SSH connection to the server and automatically log you in with appropriate credentials.

3. In the CLI connection, enter the following command to generate traffic for logging.

```
paloalto42@extranet1:~$ ./UsingLogs-V1.sh <Enter>
```

4. Press **Enter** to start the *UsingLogsV1.sh* script.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Allow 5 to 7 minutes for the script to run uninterrupted. Once the **UsingLogsV1** script completes, minimize the *Remmina* connection window.

Do not continue until the **UsingLogsV1** script completes.

6. Re-open the *PA-VM firewall* by clicking on the **Chromium** icon in the *Taskbar*.

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.3 Display Recent Threat Information in the Dashboard

You will use the Dashboard to view threats detected by the firewall in the last hour. Because you can configure the Dashboard to periodically refresh, the displayed threats will change, depending on the most recent information available. The Dashboard information is sourced from the Threat, URL Filtering, and Data Filtering logs.

1. In the web interface, click the **Dashboard** tab**.** Click **Widgets** and select **Logs > Threat Logs.**

Please Note

Note that if Threat Logs is greyed-out, it means that the widget is already displayed on the Dashboard.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. The *Threat* Logs window will display the 10 most recent threats detected by the firewall in the last hour.

Threat Logs

Name	Severity	Time
generic:31.smokemenowhhalala.bit	high	08/12 06:06:31
generic:31.smokemenowhhalala.bit	high	08/12 06:06:28
generic:31.smokemenowhhalala.bit	high	08/12 06:06:23
generic:31.smokemenowhhalala.bit	high	08/12 06:06:21
Trojan-Banker.neutrinopos:gdiscoun.org	high	08/12 06:06:19
generic:transmercasa.com	medium	08/12 06:06:19
generic:poperitte.host	high	08/12 06:05:50
generic:annamount.pw	medium	08/12 06:05:36
generic:against on.pw	medium	08/12 06:05:36
generic:packals.pw	medium	08/12 06:05:35

Please Note

Depending on activity in your lab environment in the last hour, you might not see threat entries. This widget is useful for viewing only the most recent threats detected by the firewall.

3. Click **Widgets** and select **Logs > URL Filtering Logs**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. The *URL Filtering Logs* window will display the 10 most recent threats detected by the firewall in the last hour.

URL Filtering Logs

URL	Category	Time
aplatmesse.com/images/aiXIa28QV6duat/PF_2BY9stc2V0NdiiPtOK/Lsb7S_2BfaOIiDlf/WGVj1o4_2FOYves/9xJ_2FDB1nwuG2_2FQ/OyxKYJEL6/vLpbY5jgEX999CYMCfS6/Al4ZqesjAl9QBegDyJg/jjxapq6x5O3DBHsTEJOzpJ/tVm_2FeF.avi	command-and-control	08/12 06:07:30
n31.smokemenowhhalala.bit/newfiz31/logout.php	command-and-control	08/12 06:06:26
n31.smokemenowhhalala.bit/newfiz31/logout.php	command-and-control	08/12 06:06:23
poperitte.host/data2.php?79504E1137D96CED	command-and-control	08/12 06:05:38
82.146.42.174/sin.png	malware	08/12 06:05:33
against on.pw/	malware	08/12 06:05:31
46.249.62.199/Tinx86_14.exe	malware	08/12 06:05:31
wodjfdhhen2dsads.info/	adult	08/12 06:05:25
wodjfdhhen1ndhd.online/	command-and-control	08/12 06:05:23
wodjfdhhen1ndhd.online/	command-and-control	08/12 06:05:22

Please Note

Depending on activity in your lab environment in the last hour, you might not see threat entries. This widget is useful for viewing only the most recent threats detected by the firewall.

5. Click **Widgets** and select **Logs > Data Filtering Logs** if it is not already selected.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. The *Data Logs* window will display the 10 most recent threats detected by the firewall in the last hour**.** For this step, you may not see the file entries in the *Data Logs* window. This is due to no activity being logged in the last hour in *Data*.

When logs are present, you will be presented with the following below.

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Display Recent Application Information in the Dashboard

In this section, you will display the Dashboard and view applications identified by the firewall in the last hour. Because you can configure the Dashboard to periodically refresh, the displayed applications will change depending on the most recent information available. You also will use the Dashboard to display those applications identified by the firewall in the last hour that have the most risk associated with them.

1. In the web interface, verify you are still located on the **Dashboard** tab. Click **Widgets** and select **Application > Top Applications.**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. Look at the applications displayed in the **Top Applications** widget. It displays the applications seen by the firewall in the last hour.

Please Note

Some applications should be listed because some "housekeeping" traffic nearly always traverses the network, even in the lab environment. This widget is useful for viewing only the recent application traffic seen in the last hour by the firewall.

3. Click **Widgets** and select **Application** > **Top High Risk Applications**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. Notice the applications displayed in the **Top High Risk Applications** widget. It displays the high-risk applications seen by the firewall in the last hour.

Please Note

Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks. If the Top High Risk and Top Applications have not updated, please allow 3 to 5 minutes for the widgets to update.

5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.5 View Threat Information in the ACC

In this section, you will view a few ACC widgets on the Threat Activity tab to become familiar with widgets that display threats against your environment. Spend time examining each widget so that you can determine which information is presented that might be most useful to you back in your environment.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. In the web interface, click the **ACC** tab. On the left side of the *ACC* page, look at **Global Filters** for any configured global filters. If there are filters, click **Clear all**.

2. Click the **Threat Activity** tab. On the left side of the **ACC** window, click the **Time** dropdown menu and select **Last 7 Days**. This value configures all the widgets to display threat information for the last seven days.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **Please Note**
> You should see some combination of flood, scan, spyware, packet, vulnerability, and virus threats displayed in a graph. Next to each entry should be the number of occurrences of these threat types that the firewall has seen in the last seven days. More detail about the threats should be displayed in a table below the graph.

3. In the **Threat Activity** widget's table below the graph, click the small arrow icon next to one of the *Severity* level entries. For this step, we chose to use the **high** *Severity* level.

THREAT NAME	ID	SEVERITY	THREAT TYPE
Trojan.yakes:afroamericanec.bit	209627145	medium	spyware
generic:31.smokemenowhhalala.bit	188290431	high	spyware
Suspicious HTTP Evasion Found	14984	informational	spyware
Trojan.yakes:hellobro.bit	187048410	medium	spyware
generic:crypto-pool.fr	367598334	medium	spyware
generic:poperitte.host	217645464	high	spyware
DGA:wodjfdhhen1ndhd.online	109000001	high	spyware
Suspicious TLS Evasion Found	14978	informational	spyware
generic:mustardcafeonline.com	318388689	medium	spyware
generic:toptoptop1.online	262789992	medium	spyware

> **Please Note**
> Based on the Severity level you choose, this action adds the severity level as a Global filter for the ACC. Global filters are applied to every widget on the ACC. Global filters are useful for quickly pivoting your search on a specific piece of information, thus causing all widgets to display only information that is relevant to a specific object or threat.

4. Find the global filter on the left side of the *ACC* window. Notice **high** was added as a global filter condition.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. Note that the *Threat Activity* graph and the table of *Threat Names* are updated to reflect only items with a *Severity* level of **high**.

6. In the *Global Filters* area, click **Clear all** to remove the global filter.

7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.6 View Application Information in the ACC

In this section, you will view two widgets on the Network Activity tab. The goal is for you to gain familiarity with some of the widgets available for viewing application and traffic information.

1. In the web interface, click the **ACC** tab and then the **Network Activity** tab. Hide the sidebar to make more room for the widgets by clicking the very small arrow shown.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

2. The top section of the **Application Usage** widget is a graph that illustrates how much of the traffic a specific application represents. Select the **sessions** radio button.

3. Hover your pointer over the section for **dns**. This action displays a summary window with information about that application.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the table below the graph, hover your pointer over the **dns** application until the global filter **left arrow** appears. Then click the **Left arrow** to promote the **dns** application to a global filter.

5. Unhide the sidebar by clicking the *tiny* arrow again**.** Notice the *Application Usage* chart has been upgraded to show the **dns** application.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

6. Scroll down in the **Network Activity** tab until you reach the **Rule Usage** widget**.** Select the radio button at the top for **Bytes.** In the *Time* column, select **Last Hour**.

7. In the upper-right corner of the *Rule Usage* widget, click the **Jump to Logs** button and select **Traffic Log** icon to open the *Logs* menu.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Notice it navigated you to **Monitor > Logs > Traffic**. There should be a time range filter and an application filter for web browsing. The time range filter is derived from the time specified in the ACC. Note that the entries displayed in the Traffic log match the filter

9. Clear the filter in the Traffic log.

10. Click the **ACC** tab. In the *Global Filters* area, click **Clear all** to remove the global filter.

11. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.7 View Threat Information in the Threat Log

In this section, you will apply different filters to the Threat log. You will use the filters to determine whether all critical-severity and high-severity threats detected by the firewall have been blocked. You also will use a log filter to determine which threats have been detected that come from a specific security zone.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1. Select **Monitor > Logs > Threat.** In the upper-right corner of the window, click the **X** icon in the filter area to remove any existing log filter.

2. Click the **+** icon in the filter area to open the *Add Log Filter* window.

3. In the *Add Log Filter* window, select the following. Click **Add**.

Parameter	Value
Connector	**and**
Attribute	**Severity**
Operator	**greater than or equal**
Value	**high**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

4. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.

5. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.

6. Notice the Threat log has been filtered to display only threats of high severity or greater. Some columns have been adjusted to reflect the *Severity* column.

7. Click the **X** icon in the filter area to remove any existing log filter.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. Click the **+** icon in the filter area to re-open the **Add Log Filter** window.

9. In the *Add Log Filter* window, select the following. Click **Add**.

Parameter	Value
Connector	**and**
Attribute	**Source User**
Operator	**equal**
Value	**chicago\escrooge**

10. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

11. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.

12. Notice the Threat log has been filtered to display only threats from the Source User **Chicago\escrooge**. Some columns have been adjusted to reflect the *Severity* column.

13. Click the **X** icon to clear the filter from the log filter text box.

> **Please Note**
> URL Filtering, WildFire Submissions, and Data Filtering logs are available to display traffic and threats detected by the firewall but are not shown in this section. You also can use filters to view these logs.

14. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.8 View Application Information in the Traffic Log

In this section, you will apply different filters to the Traffic log. You will use a filter to determine which applications are being seen in a specific zone.

1. Select **Monitor > Logs > Traffic.** Click the **X** icon in the filter area to remove any existing log filter.

2. Click the **+** icon in the filter area to open the *Add Log Filter* window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. In the *Add Log Filter* window, select the following. Click **Add**.

Parameter	Value
Connector	**and**
Attribute	**Source Zone**
Operator	**equal**
Value	**`Acquisition`**

Please Note

This configuration filters the log to display only application traffic that is sourced from the Acquisition zone. You could use this information, for example, to help you to determine how to configure your Security policy rules. You easily could modify the filter to display application traffic sourced from any zone and use that information to help you improve your Security policy configuration.

4. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

5. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.

6. Notice the Traffic log has been filtered to display only threats from the *From Zone* **Acquisition**. Some columns have been adjusted to reflect the *Severity* column.

(zone.src eq Acquisition)

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER
		08/12 15:37:16	end	Acquisition	Acquisition	192.168.1.104	chicago\mrhyde
		08/12 15:37:16	end	Acquisition	Acquisition	192.168.1.20	chicago\sholmes
		08/12 15:35:43	end	Acquisition	Acquisition	192.168.1.104	chicago\mrhyde
		08/12 15:35:00	end	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot

Please Note

You could use this information to help you determine the Security policy rules required to control legitimate traffic sourced from devices in the dmz zone.

7. Click the **+** icon in the filter area to again open the *Add Log Filter* window.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

8. In the *Add Log Filter* window in the top pane, modify the existing source zone filter to filter on the *User_Net* zone instead of the *Acquisition* zone. The completed filter should read **`(zone.src eq Users_Net)`**. Click **Apply**.

9. Click the **+** icon in the filter area to again open the *Add Log Filter* window.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

10. In the *Add Log Filter* window, select the following. Click **Add**.

Parameter	Value
Connector	**and**
Attribute	**Application**
Operator	**equal**
Value	**google-base**

11. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.

12. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

13. Notice the Traffic log has been filtered to display only threats from the *From Zone* **Users_Net** and the *Application* **google-base**. Some columns have been adjusted to reflect the *Application* column.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION
08/12 16:13:53	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
08/12 16:13:53	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
08/12 16:13:52	deny	Users_Net	Internet	192.168.1.20	142.250.188.46	80	google-base
08/12 16:13:52	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
08/12 16:13:52	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base

14. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.9 View Threats Using App Scope Reports

In this section, you will view threat information using App Scope's Threat Monitor and Threat Map reports.

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

2. At the bottom of the window, click **Last 7 days**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

3. The window should update to display the *top 10 threats* detected by the firewall in the last seven days. At the top of the window, click **Top 10** and select **Top 25** from the menu.

4. At the top of the window, click **Threat** and choose **Source User**.

5. At the top of the window, hover your pointer over each **Filter** icon to see how to display specific types of threats.

6. Select **Show all threat types**.

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

7. Hover your pointer over the top section of any bar on the bar chart**.** You should see a pop-up window that shows the threat name and number of detections**.**

Please Note The information you see may differ from the example here.

8. The lab is now complete; you may end your reservation.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

PALO ALTO NETWORKS EDU 210

Lab 17: Capstone

Document Version: 2022-07-18

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Capstone 6
1.1 Load Lab Configuration 6
1.2 Configure Networking 6
1.3 Configure Security Zones 6
1.4 Configure NAT Policies 7
1.5 Configure Security Policy Rules 7
1.6 Create and Apply Security Profiles 8

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Introduction

This comprehensive lab is intended to provide you with additional hands-on firewall experience and to enable you to test your new knowledge and skills. You can 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 username **`admin`** and **`Pal0Alt0!`** as the password. Take special care to use the exact spelling and capitalization for the items you are asked to configure.

You are being asked to meet multiple configuration objectives. These objectives are listed in the lab exercise sections that follow.

Objective

You are being asked to meet multiple configuration objectives. These objectives are listed in the lab exercise sections that follow.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Capstone

1.1 Load Lab Configuration

- In the web interface, select **Device > Setup > Operations**.
- Click **Load named configuration snapshot.**
- Select **edu-210-lab-17a-start.xml** and click **OK**.
- Click **Close**.
- **Commit** all changes.

1.2 Configure Networking

Complete the following objectives:

- Configure three firewall interfaces using the following values:
  - **Ethernet 1/1**: **203.0.113.20/24 - Layer 3**
  - **Ethernet 1/2**: **192.168.1.1/24 - Layer 3**
  - **Ethernet 1/3**: **192.168.50.1/24 - Layer 3**
- Create a virtual router called **VR-1** for all configured firewall interfaces.
- Create a default route for the firewall called **Default-Route**
- Create an **Interface Management Profile** called **Allow-ping** that allows **ping**
- Assign the **Allow-ping** Interface Management Profile to **ethernet1/2**

Verify network connectivity from the firewall to other hosts.

- Your internal host can ping **192.168.1.1** and receive a response
- 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 192.168.1.20**

1.3 Configure Security Zones

Complete the following objectives:

- Create a **Security Zone** called **Internet** and assign **ethernet1/1** to the zone
- Create a **Security Zone** called **Users** and assign **ethernet1/2** to the zone:
  - Configure the **Users Zone** for User-ID
- Create a **Security Zone** called **Extranet** and assign **ethernet1/3** to the zone
- Create **Tags** for each **Security Zone** using the following names and colors:
  - **Extranet** – orange
  - **Internet** – black
  - **Users** – green

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.4 Configure NAT Policies

Create Source NAT rules to meet the following requirements:

- Rule Name = **Users_to_Internet**
  - From Source Zone **Users** to Destination Zone **Internet**
  - Use **ethernet1/1** on the firewall as the source translation address
  - **Tag** = **Users**
- Rule Name = **Extranet_to_Internet**
  - From Source Zone **Extranet** to Destination Zone **Internet**
  - Use **ethernet1/1** on the firewall as the source translation address
  - Tag = **Extranet**
- All NAT rules must include a helpful Description

1.5 Configure Security Policy Rules

Create security policy rules to meet the following requirements:

- For all security policy rules, enter a helpful **Description**.
- Create and apply the following **Tags** to the Security policy rules as appropriate:
  - **Allow** – Lime
  - **Block** – Red
- Modify the **interzone-default** security policy rule so that traffic is logged at session end.
- Create a security policy rule called **Block_Bad_URLs** with the following characteristics:
  - For all outbound traffic, the URL categories **hacking**, **phishing**, **malware**, and **unknown** must be **blocked** by a security policy rule match criterion.
- From the User zone to the Extranet zone, create a security policy rule called **Users_to_Extranet** to allow the following applications:
  - **ping**
  - **ssl**
  - **ssh**
  - **dns**
  - **web-browsing**
- From the User zone to the Internet zone, create a security policy rule called **Users_to_Internet** to allow the following applications:
  - **ping**
  - **dns**
  - **web-browsing**
  - **ssl**

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

- From the Extranet zone to the Internet zone, create a security policy rule called **Extranet_to_Internet** to allow the following applications:
    - **ping**
    - **dns**
    - **web-browsing**
    - **ssl**

You can consider this objective complete when the following tests are successful:

- The client host can **ping 8.8.8.8** and **google.com**
- The client host can access **www.paloaltonetworks.com**
- The client host can browse to the Extranet web server at **http://192.168.50.80**
- The client host can use **SSH** to access the Extranet host at **192.168.50.150** using the login name **paloalto42** and the password **Pal0Alt0!**
- The Extranet host can **ping 8.8.8.8** and **google.com**
- The internal host cannot access **hacker9.com**

1.6 Create and Apply Security Profiles

Create Security Profiles and a Security Profile Group to meet the following requirements:

- A Corporate **URL Filtering Security Profile** called **Corp-URL** to log access to all web categories

  You can use the existing default profile as the basis for your own.

- A Corporate **File Blocking Security Profile** called **Corp-FB** to block dangerous file types

  You can use the existing strict profile as the basis for your own.

- A Corporate **Antivirus Security Profile** called **Corp-AV** to block viruses

  You can use the existing default profile as the basis for your own.

- A Corporate **Anti-Spyware Security Profile** called **Corp-AS** to block viruses

  You can use the existing strict profile as the basis for your own.

- A Corporate **Vulnerability Protection Security Profile** called **Corp-Vuln** to block viruses

  You can use the existing strict profile as the basis for your own.

- A Corporate **WildFire Profile** called **Corp-WF** to send all file types to the public cloud for inspection

  You can use the existing default profile as the basis for your own.

The lab is now complete; you may end your reservation.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com