5 - Configuring Security Policy Rules and NAT Rules

1. Create a Security Policy Rule
    1. In the web interface, select Policies > Security. Click Add.
    2. In the Security Policy Rule window, on the General tab. Type Users-to-Extranet for the Name. 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.
    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.
2. 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.
3. 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.
4. Choose Columns and note the available columns that you can hide or display in this table.
5. In the Columns, uncheck Type, Source Device, Destination Device, and Options.
6. At the top of the Name column, click the dropdown icon again and choose Adjust Columns

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

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.
   - `ping 192.168.50.80
3. You should see a webpage displayed by the server. If you are seeing Hello World !, you have properly configured the security policy.
4. Close the Firefox browser. Click the close icon in the upper-right.
5. Reopen the PA-VM firewall interface by clicking the Chromium icon in the taskbar.
6. Leave the terminal and firewall 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

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.
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.
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.
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
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.
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
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.
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.
16. Verify the Extranet-to-Internet security policy rule appears in the Security policies window.
17. Commit all changes

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).

1. In the web interface, navigate to Policies > NAT. Click Add to define a new source NAT policy
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
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
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
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.
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.
11. From the terminal window on the desktop, ping an address on the internet by issuing the following command.
    - `ping 8.8.8.8
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.
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.
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.

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

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
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)
5. Verify that the Dest_NAT_To_Webserver NAT policy is showing.
6. Commit all changes