SLASHNEXT

USER GUIDE V1.0.0

SlashNext Threat Intelligence Integration Guide PAN-OS Firewall

TABLE OF CONTENTS

1 | EXTERNAL DYNAMIC LISTS (EDL)

An External Dynamic list is a text type of file hosted on an external web server. A firewall can import objects such as IP Addresses, Domain names and URLs from the EDL and enforce the required policies on the incoming traffic. The EDL can be modified in real-time and the firewall is able update its policies correspondingly. In case the EDL becomes unreachable due to network issues, the firewall uses the most recently imported EDL. Thus EDLs provide a convenient way to enforce network policies on a firewall without manual labor. The Palo Alto Networks Firewall supports four different types of EDLs:

1. **IP Address:** The policy can be applied for a source or destination IP address present as a static object in the EDL.
2. **Predefined IP Address:** A predefined IP address list is referred to the Palo Alto Networks Malicious IP Address Feeds. These feeds can be used to enforce policies on the network traffic if you have an active Threat Prevention license.
3. **Domain:** An EDL of domain type can be used to import custom domain names to enforce a network policy based on an Anti-Spyware profile.
4. **URL:** An external dynamic list of URL type can be used to filter the network traffic from malicious URLs.

2 | EDLS IN PAN-OS FIREWALL

Below we elaborate on how to create EDLs of all the above mentioned types.

2.1 | CREATING AN EDL OF TYPE IP ADDRESSES

Log into Palo Alto Networks Firewall by typing your username and password.

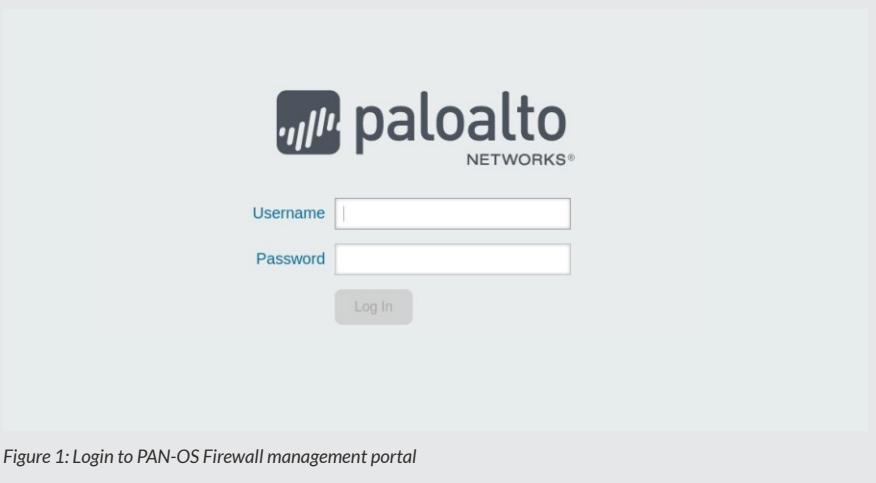


Figure 1: Login to PAN-OS Firewall management portal

Click on **Objects** from the top menu-bar and **External Dynamic Lists** option from the left menu. Click on **Add** button from the bottom menu-bar to create a new EDL.

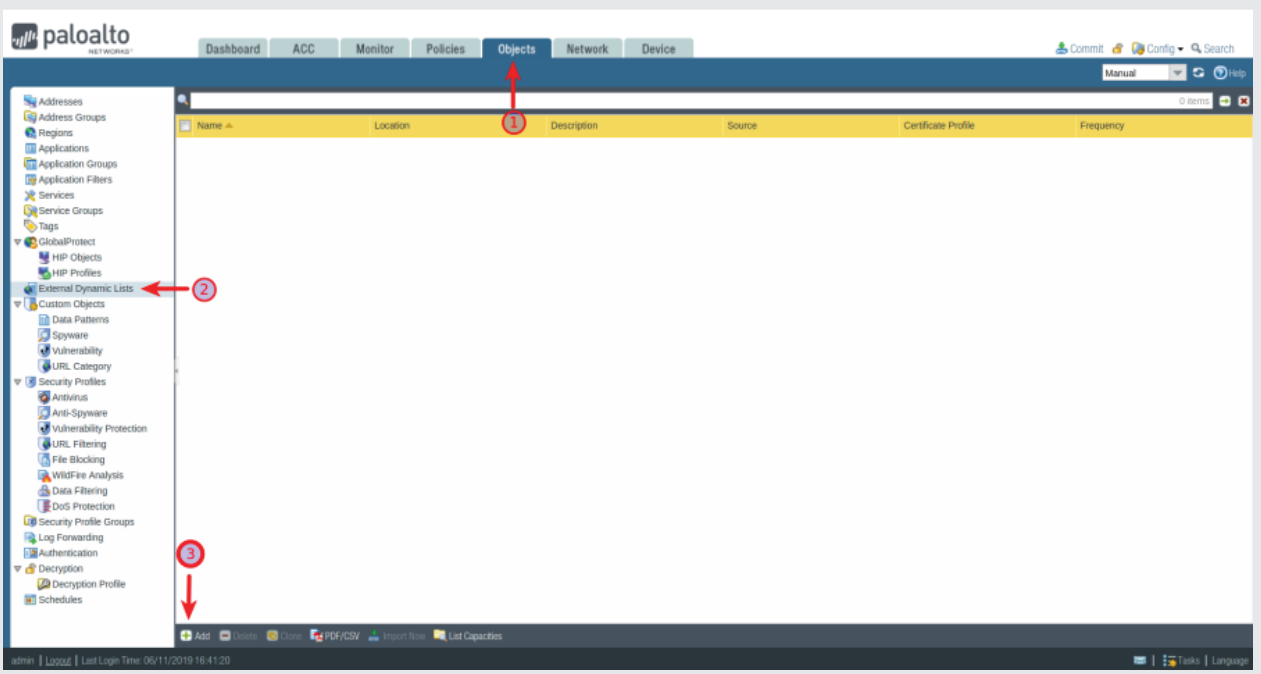


Figure 2: Steps to create a new EDL in PAN-OS Firewall

A new dialog box to create the EDL will open up. Type the desired **Name** and **Description**. Select **IP List** as the type of the new EDL from the Type drop-down menu. Use the SlashNext Plaintext type feed for Phishing IPs pointed to by:

```
https://intel.slashnext.cloud/api/intel/ips?authkey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Important Note

Please note that if the user wants to use MineMeld output for the EDL, use the FEED BASE URL from output node for IP intel here instead of the above SlashNext threat intelligence API here.

Finally select **Hourly** option from the Repeat drop-down menu which refers to the update interval at which the EDL retrieves the feed from SlashNext endpoint and updates itself. You can also click on **Test Source URL** to verify the status of the source used for the new EDL.

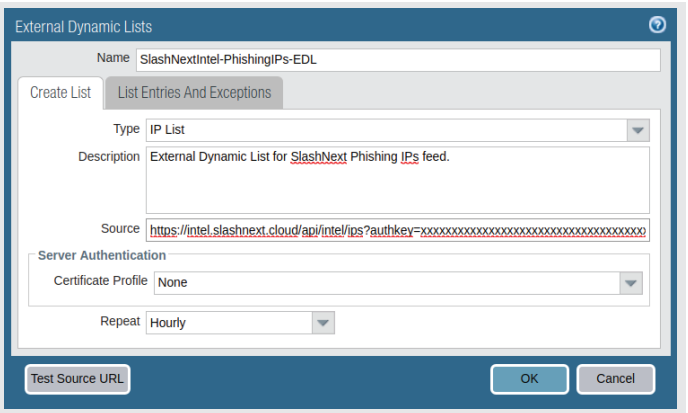


Figure 3: Configuration settings for SlashNext Phishing IPs EDL

Click on the **List Entries And Exceptions** menu from the top menu-bar to see all the entries of the EDL fetched from the selected feed source. Please note that at this point, the List Entries will be empty and an EDL in PAN-OS Firewall is only updated if it is used in at-least one Policy so, you have to create a new policy using this newly created EDL. Click on **OK** to finish the creation of EDL. In section 3, we explain how to create policies based on different types of EDLs created in this section.

2.2 | CREATING AN EDL OF TYPE DOMAINS

Similarly we create an EDL for malicious domains provided by SlashNext domains feed according to the settings shown in Figure 4.

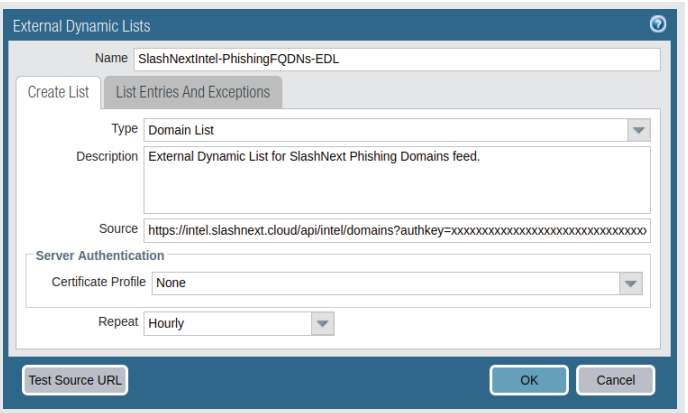


Figure 4: Configuration settings for SlashNext Phishing Domains EDL

The Type of the EDL in this case is selected to be **Domain List** and the Source URL is given as:

https://intel.slashnext.cloud/api/intel/domains?authkey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Important Note

Please note that if the user wants to use MineMeld output for the EDL, use the **FEED BASE URL** from output node for FQDN intel here instead of the above SlashNext threat intelligence API here.

2.3 | CREATING AN EDL OF TYPE WILDCARD URLS

Finally, we create an EDL to cater Widlcard URLs from SlashNext Wildcard URLs feed. The source of the EDL is given to be as:

https://intel.slashnext.cloud/api/intel/wildcardurls?authkey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Important Note

Please note that if the user wants to use MineMeld output for the EDL, use the **FEED BASE URL** from output node for wildcard URL intel here instead of the above SlashNext threat intelligence API here.

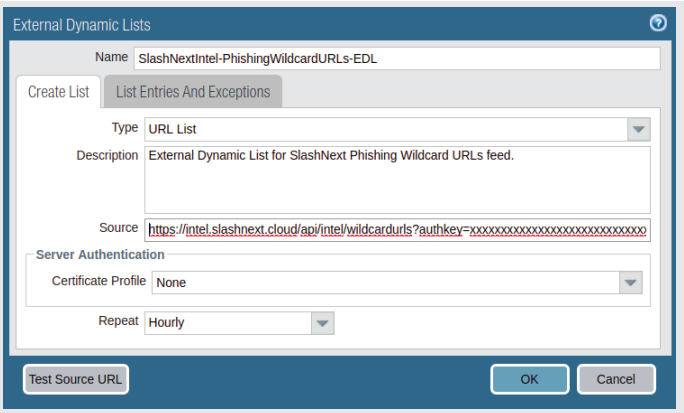


Figure 5: Configuration settings for SlashNext Phishing Wildcard URLs EDL

3 | POLICIES IN PAN-OS FIREWALL

In this section we explain the procedure to create different policies to block malicious traffic, based on the EDLs created in the previous section.

3.1 | CREATING A POLICY BASED ON IPS EDL

Click on **Policies** from the top menu-bar and select **Security** from the left menu then, click on the **Add** button from the bottom menu-bar to create a new policy based on IPs EDL.

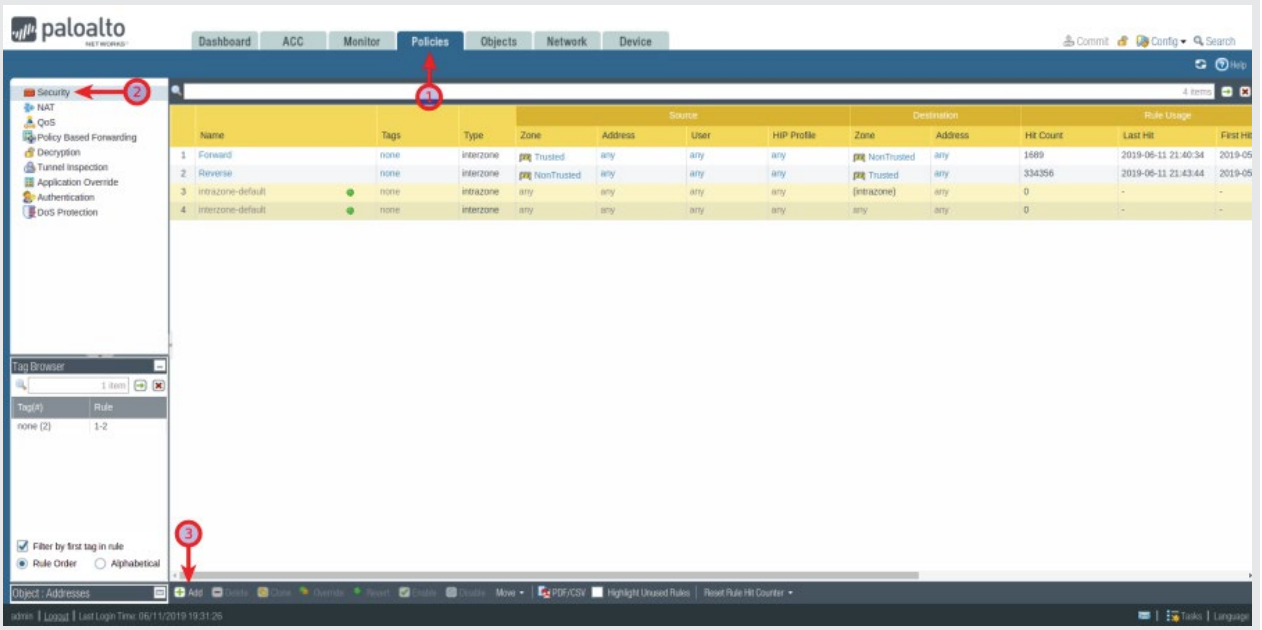
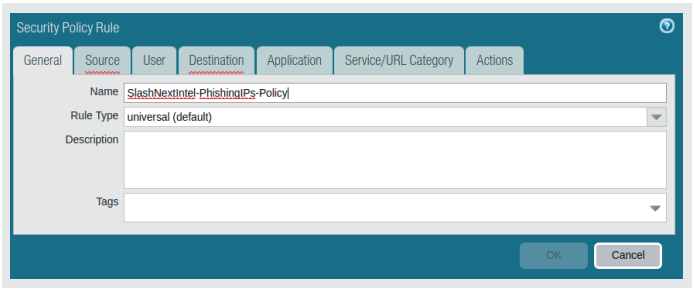
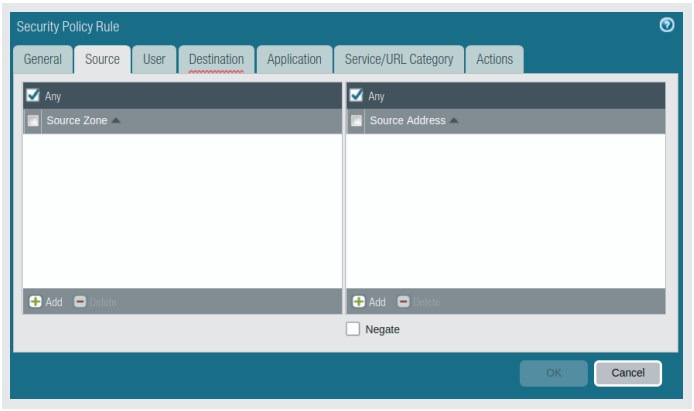


Figure 6: Steps to create a new policy in PAN-OS Firewall

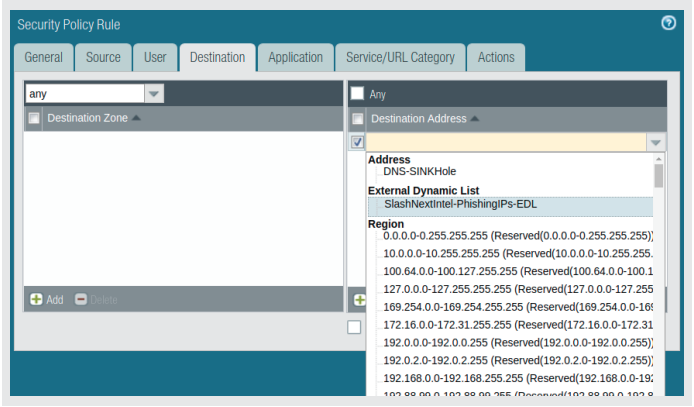
A new dialog box by the name **Security Policy Rule** will open up. In the **General** tab, select a suitable name for your policy.



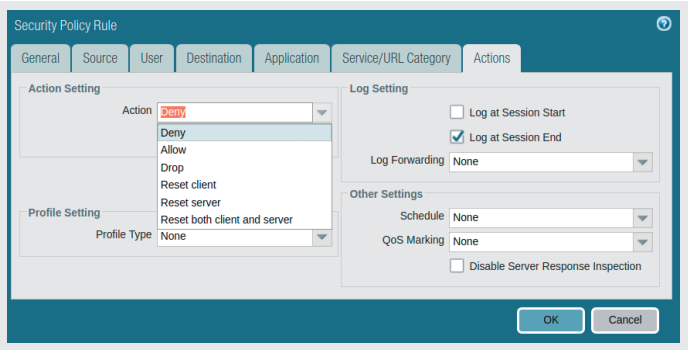
Then go to the **Source** tab and check **Any** checkbox for **Source Zone** and **Source Address** panel. This means that you are applying no filter on outgoing traffic from your network.



Now go to the **Destination** tab and select **any** option from the drop-down list in the **Destination Zone**. In the **Destination Address** panel, select the Phishing IPs EDL created in the previous sections. By doing so, you are restricting the users on your network to access anything on the internet that is malicious and present on our Phishing IPs EDL.



Finally, go to the **Actions** tab to select the desired action in case the firewall detects any packet that is coming from a source marked as malicious in our IPs EDL. In our case we want to deny any such traffic so select **Deny** from the **Action** drop-down list. For a complete understanding of different actions, please refer to Security Policy Actions. Click **OK** to save our newly created policy.



3.2 | CREATING A POLICY BASED ON DOMAINS EDL

To blocks access to malicious domains, first we need to create an Anti-Spyware profile based on our previously create EDL. This profile can then be attached in a security policy to enforce the necessary restrictions. PAN-OS Firewall also allows DNS Sinkholing for malicious domains to a Palo Alto Networks' or a user defined sinkhole server.

Let us first create an Anti-Spyware profile based on malicious domains EDL. Go to the **Objects** tab and select **Anti-Spyware** from the **Security Profiles** sub menu on the left as shows in Figure 7.

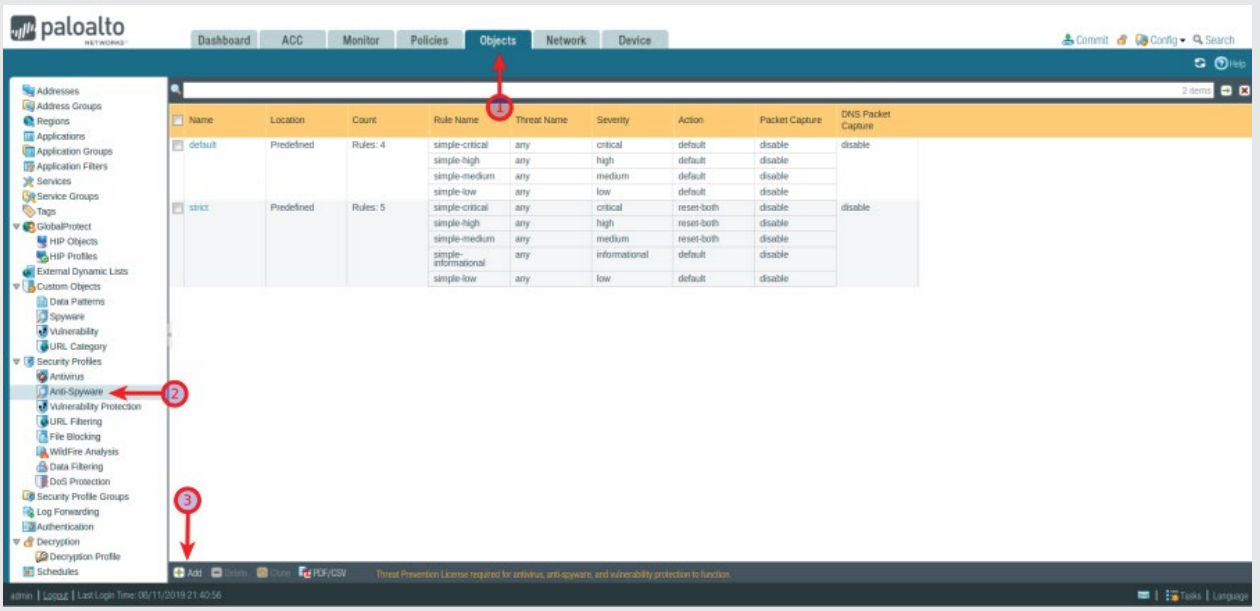
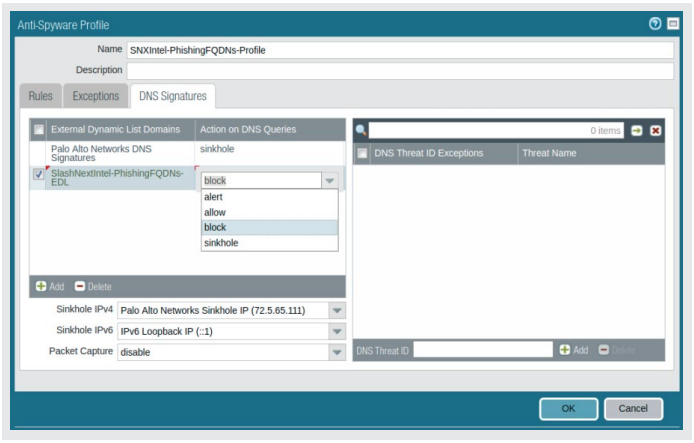
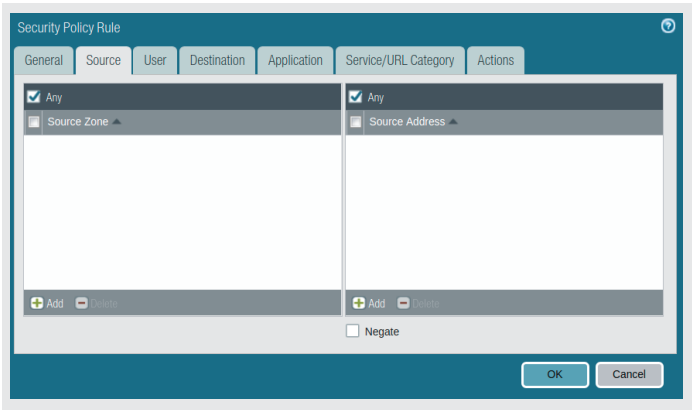


Figure 7: Steps to create a new Anti-Spyware profile

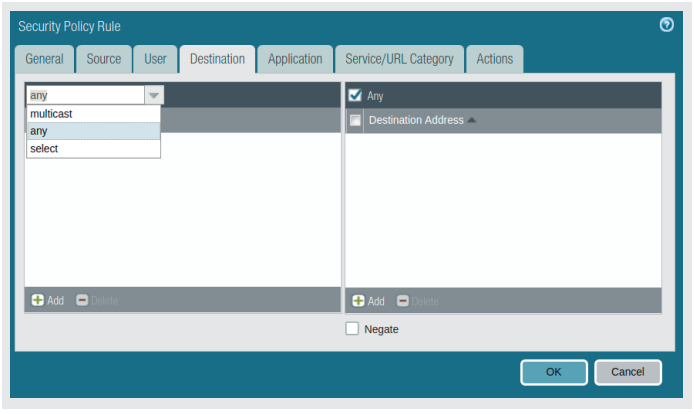
A new dialog box by the name of Anti-Spyware Profile will open up. Add a friendly name for the profile and then click on the **DNS Signatures** tab. Click on the **Add** button to select our Phishing Domains EDL from the drop-down list. Select the appropriate **Action on DNS Queries** option according to your own need. In this case, we can simply block the malicious domains. Click on **OK** to finally save the new profile.



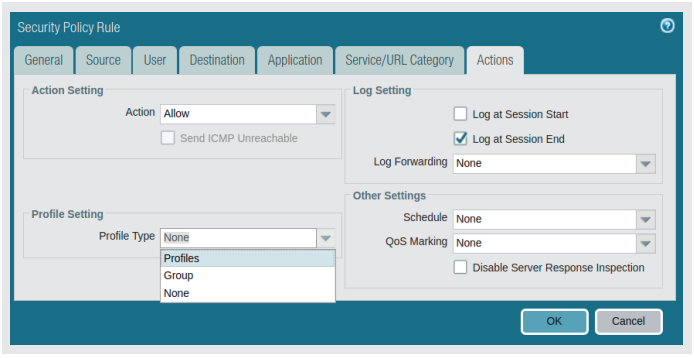
Next, we go the **Policies** tab to create a new policy for malicious domains. After selecting a suitable name for your policy in the **General** tab, go to the **Source** tab and check the **Any** checkbox for both **Source Zone** and **Source Address**.



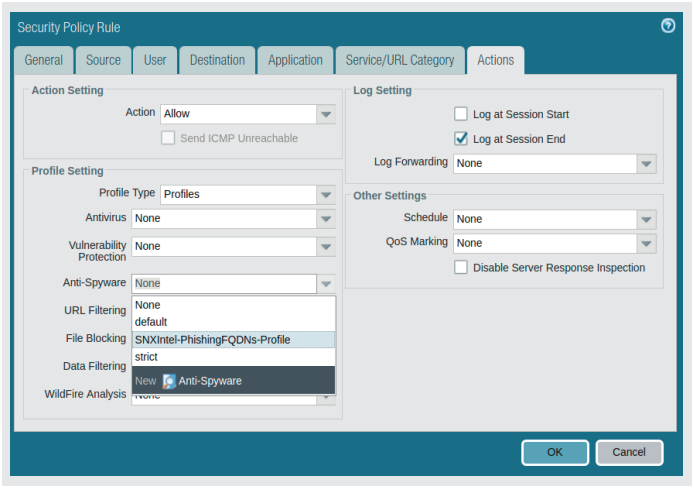
Similarly, for the **Destination** we select the **Any** option for both **Destination Zone** and **Destination Address**.



Finally, go to the **Actions** tab and from the **Profile Setting** pane, choose **Profiles** as the **Profile Type** from the drop-down list.



Some further options will appear in the **Profile Setting** pane. Select the recently created Anti-Spyware profile from the **Anti-Spyware** drop-down list. Finally, click on OK to save the malicious domains policy.



3.3 | CREATING A POLICY BASED ON WILDCARD URLS EDL

PAN-OS firewall also supports direct protection against malicious URL via a URL Filtering profile based on our URL EDLs. These URL Filtering profiles can then be used to create a new policy to block malicious traffic. Therefore, let us first create profiles Wildcard URL EDLs to be later used in creating policies.

Go to **Objects** → **Security Profiles** → **URL Filtering** and click on the **Add** button present at the bottom as demonstrated by Figure 8.

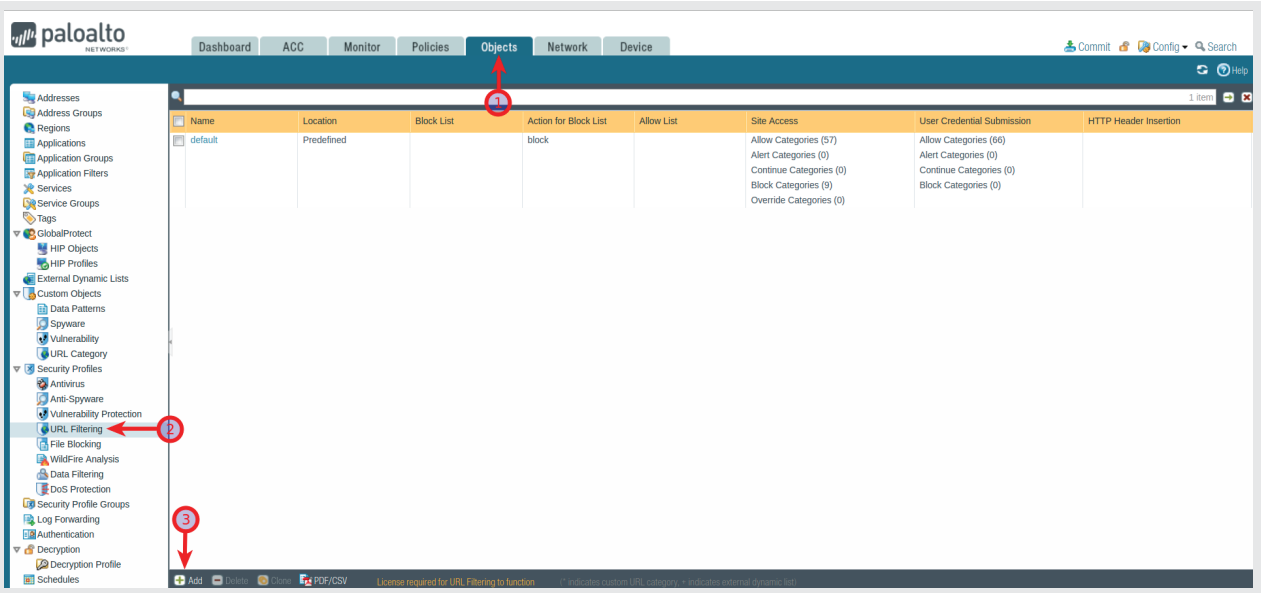


Figure 8: Steps to create a new URL Filtering profile

Use a suitable name for the Profile and select our Phishing Wildcard URLs EDL from **Category** list in the **Categories** tab. Finally, select suitable action for the firewall to take from the drop-down list under **Site Access** as show in Figure 9.

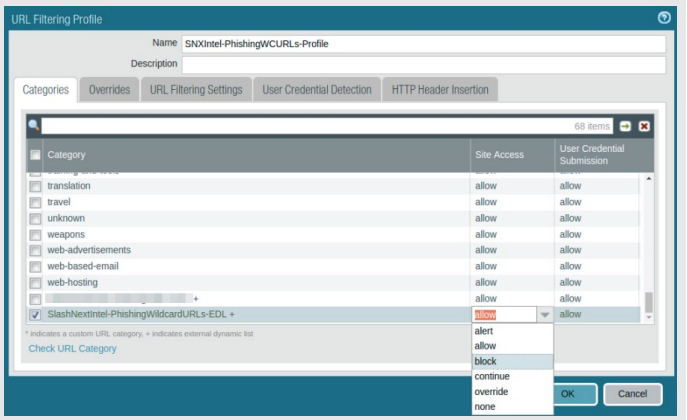
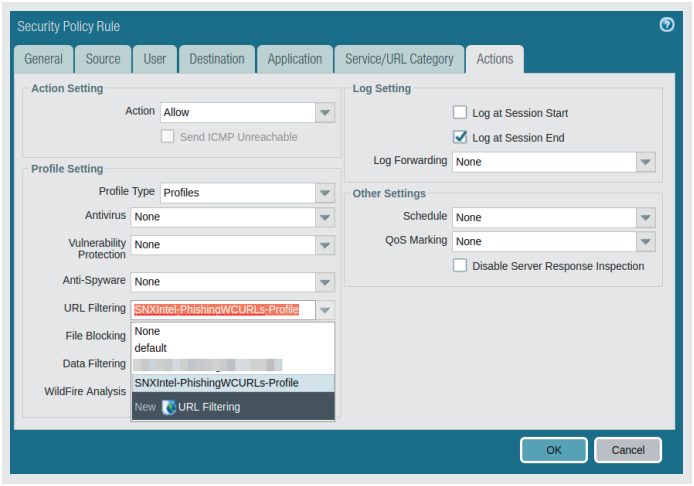
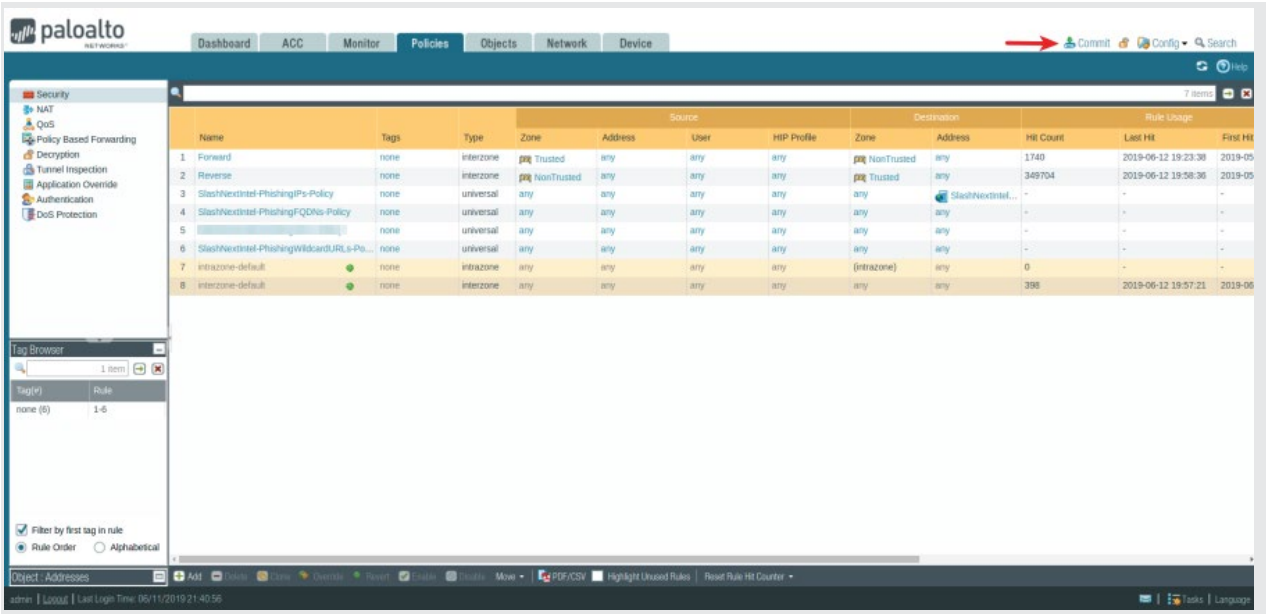


Figure 9: Configuration Settings for Wildcard URLs Profile

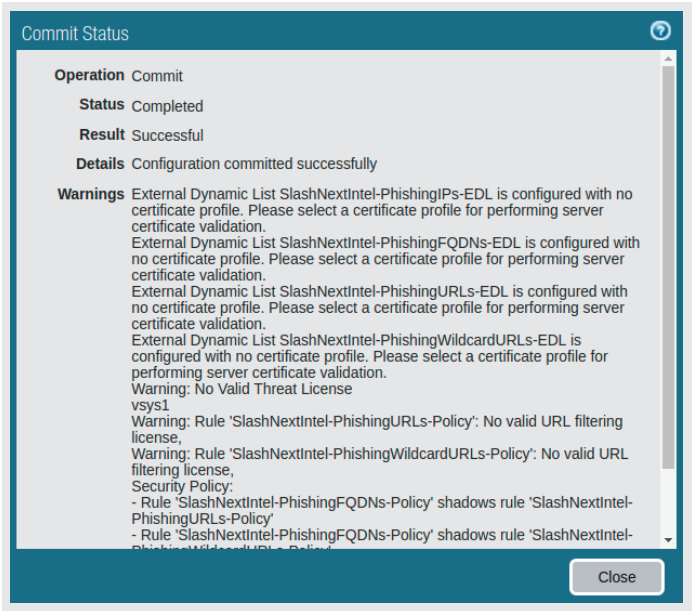
Finally, we can use our recently created URL Filtering Profiles in creating a new policy. Go to **Policies** → **Security** and click on **Add** to create a new policy.
Select a suitable name and use the **Any** option for both **Source** and **Destination** as done in Section 3.2 Next, select **Profiles** from the **Profile Type** drop-down list in **Profile Setting** pane. In the URL Filtering option, select the recently created URL Filtering Profile and click on **OK** to create the new policy.



Once you are done creating all the policies and objects, click on the **Commit** button to deploy all the changes on the firewall as shown in Figure (Please note that it is recommended to commit after making any substantial change in your firewall configurations. To maintain the continuity of this document, we committed the configurations in the end only).



A dialog bar showing the progress and Status of your commit will appear on the screen. Once the configurations are successfully committed, the dialog box will look something like this (Ignore all the warnings at the moment).



4 | RESULTS

Once the policies are deployed, you can see the EDLs getting updated as they fetch data from SlashNext Threat Intelligence Platform feeds. These List entries will keep on updating as new items are fetches.

Go to **Objects** → **External Dynamic Lists** and click on one of the EDLs. Then go to **List Entries And Exceptions** tab to see the **List Entries** as shown in Figure 10, 11, and 12.

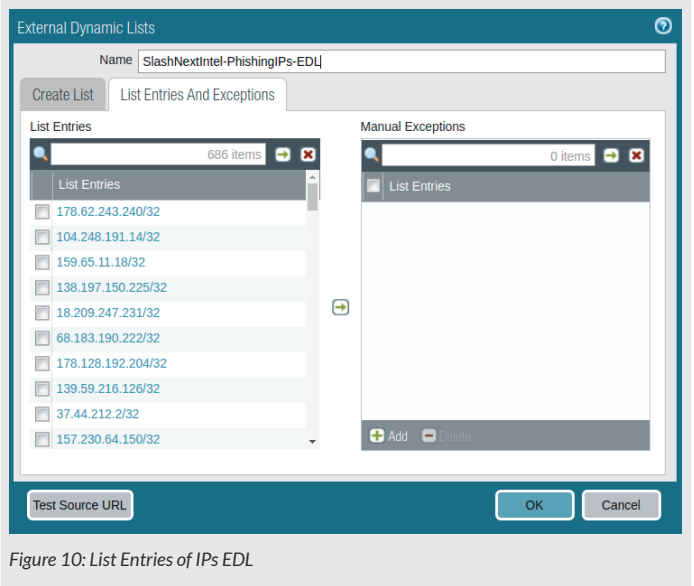


Figure 10: List Entries of IPs EDL

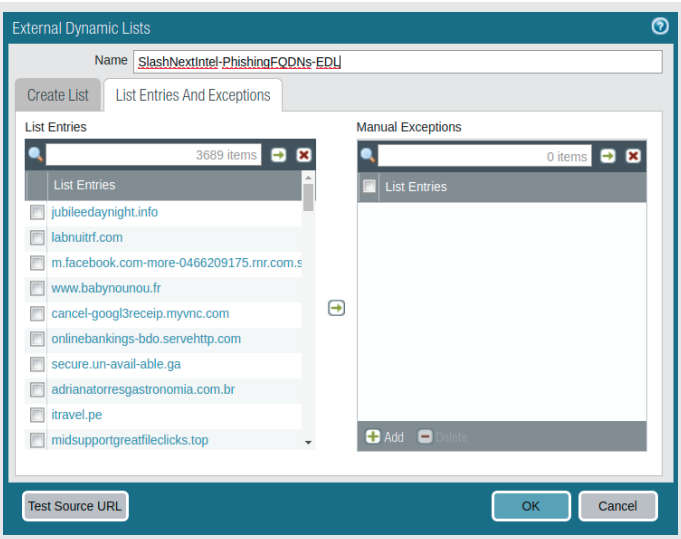


Figure 11: List Entries of Domains EDL

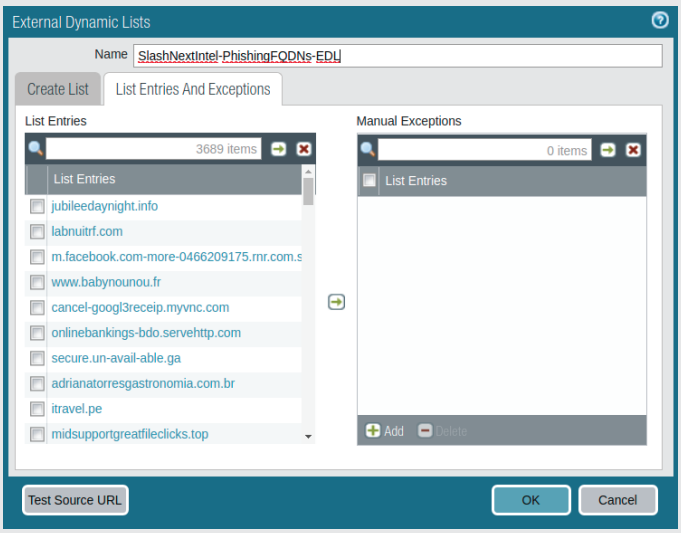


Figure 12: List Entries for Wildcard URLs EDL

5 | TROUBLESHOOTING

You might face an error while committing your changes to the firewall as shows in Figure 13.

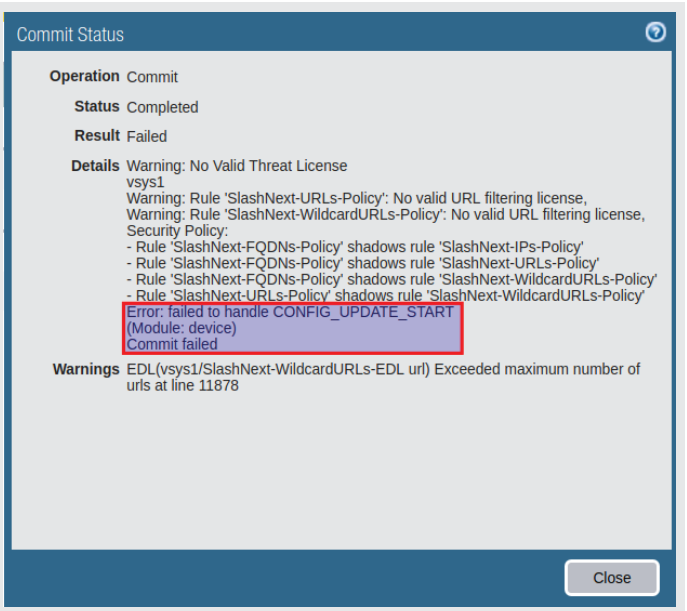


Figure 13: Frequently occurring Commit Error

This can be circumvented by rebooting the firewall device (Please note that all your changes which are not yet committed will be gone. To save and load a snapshot of the firewall, refer to Save and Export Firewall configurations). To reboot the firewall, Go to **Device** → **Setup** → **Reboot Device** as shown in Figure 14.

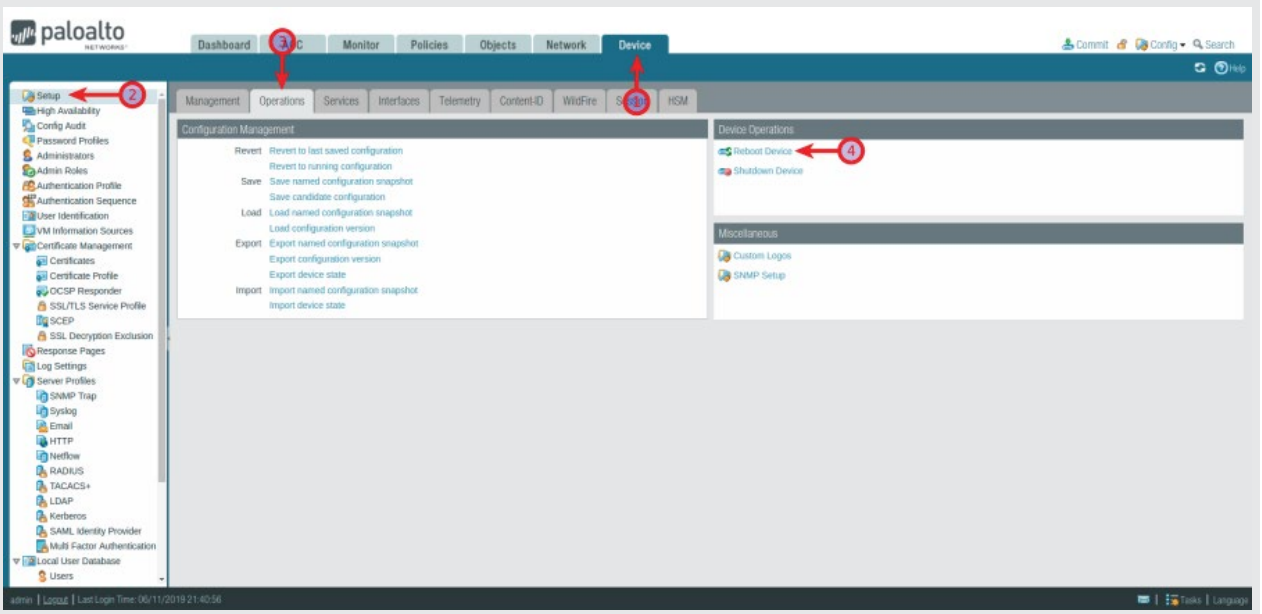


Figure 14: Steps to restart PAN Firewall