SECURITY OPERATIONS FUNDAMENTALS

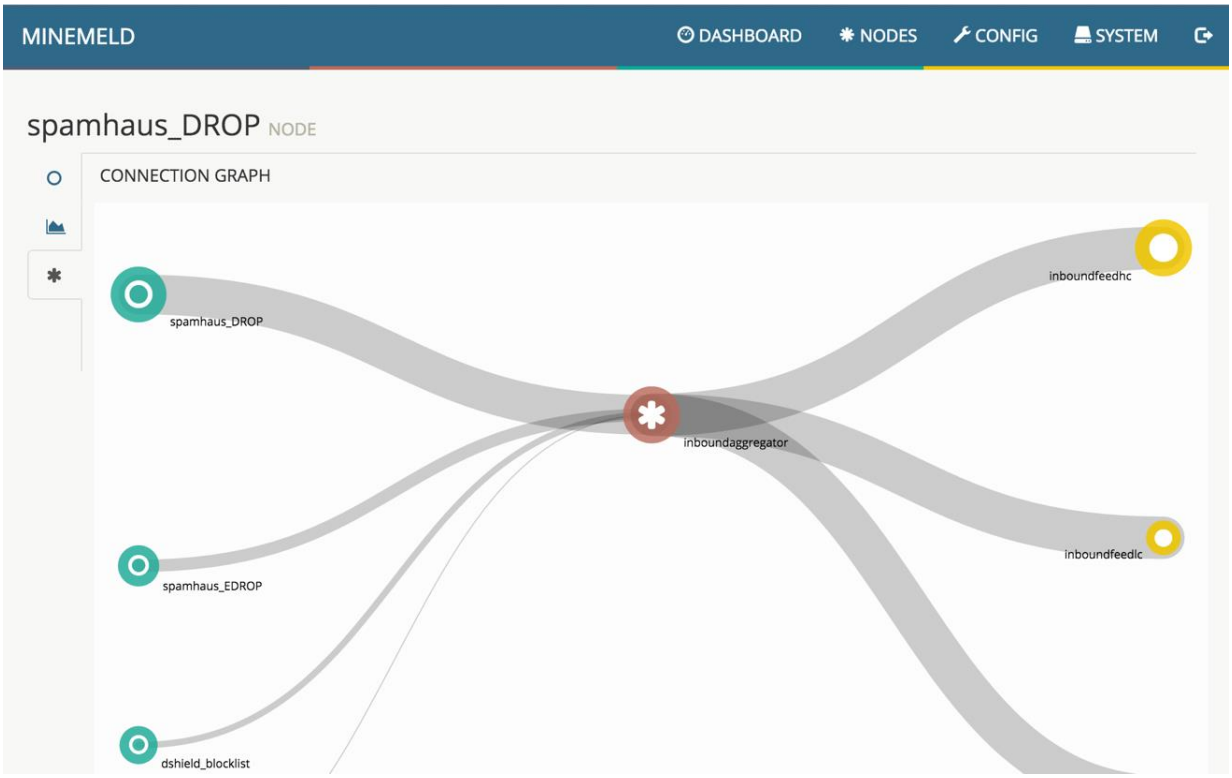
Lab 7: Threat Intelligence

Document Version: 2021-01-29

Contents

Introduction

In this lab, you will analyze data from the Palo Alto Networks Firewall. The data will be coming from the logs on the Palo Alto Networks Firewall. To effectively utilize the information, you will become familiar with a variety of logs and how to search the logs.

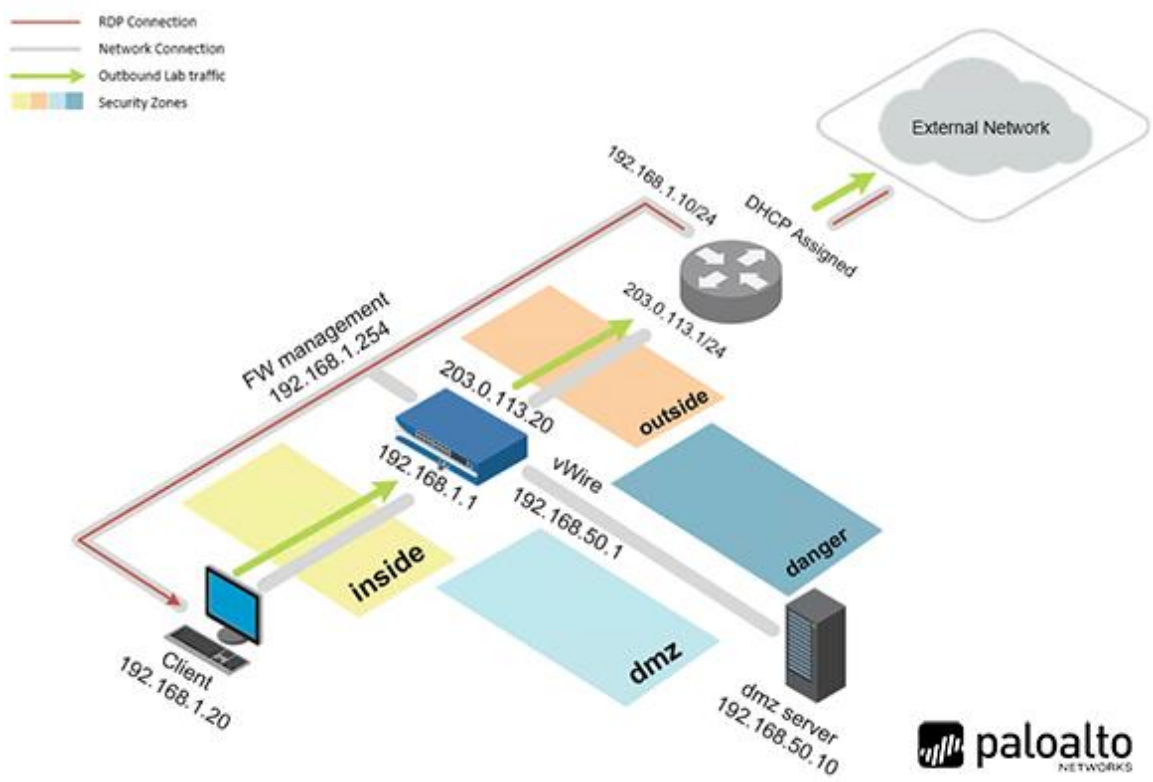


Objective

In this lab, you will perform the following tasks:

- Create Docker volumes to store MineMeld container data on client
- Deploy a MineMeld container image using Docker Compose
- Log on to the MineMeld Web UI and observe default configurations
- On the firewall appliance configure an External Dynamic List (EDL) to use MineMeld's default threat intelligence IP block list feeds
- Create a custom MineMeld intelligence feed and use it to configure another EDL block list on the firewall appliance

Lab Topology



Lab Settings

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

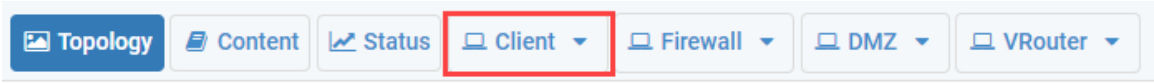
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

7 Threat Intelligence

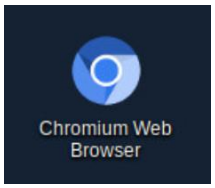
7.0 Load Lab Configuration

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

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

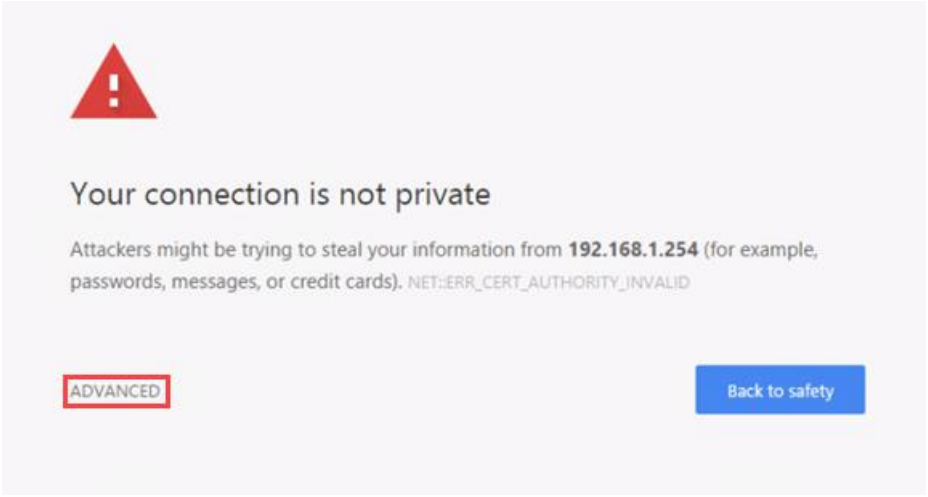


2. Log in to the client PC with the username `lab-user` and password `Train1ng$`.
3. Double-click the **Chromium** icon located on the desktop.



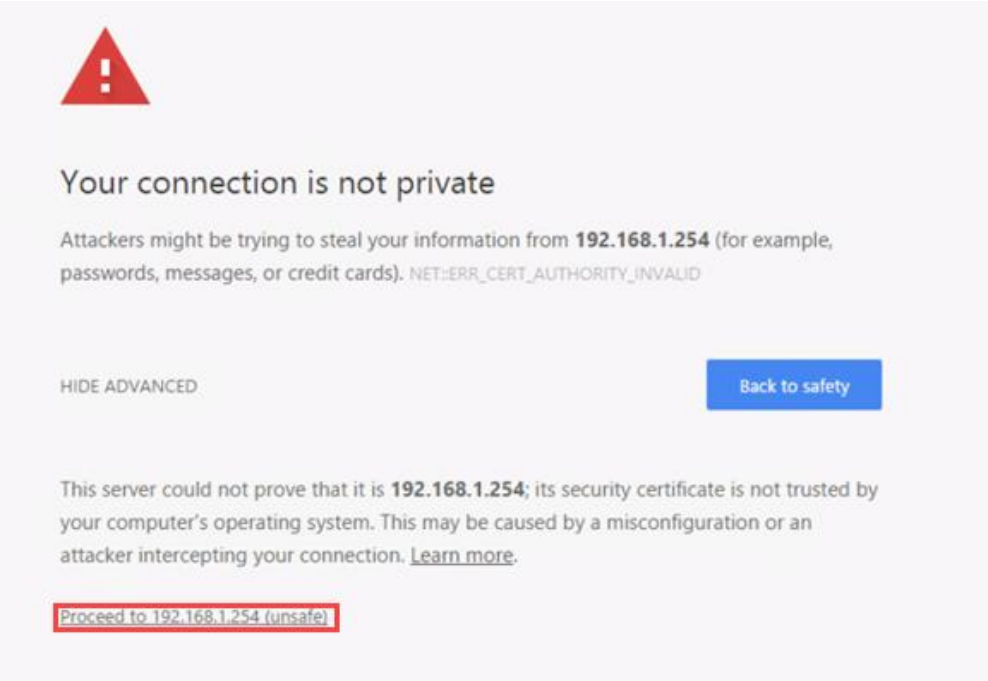
4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.

5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



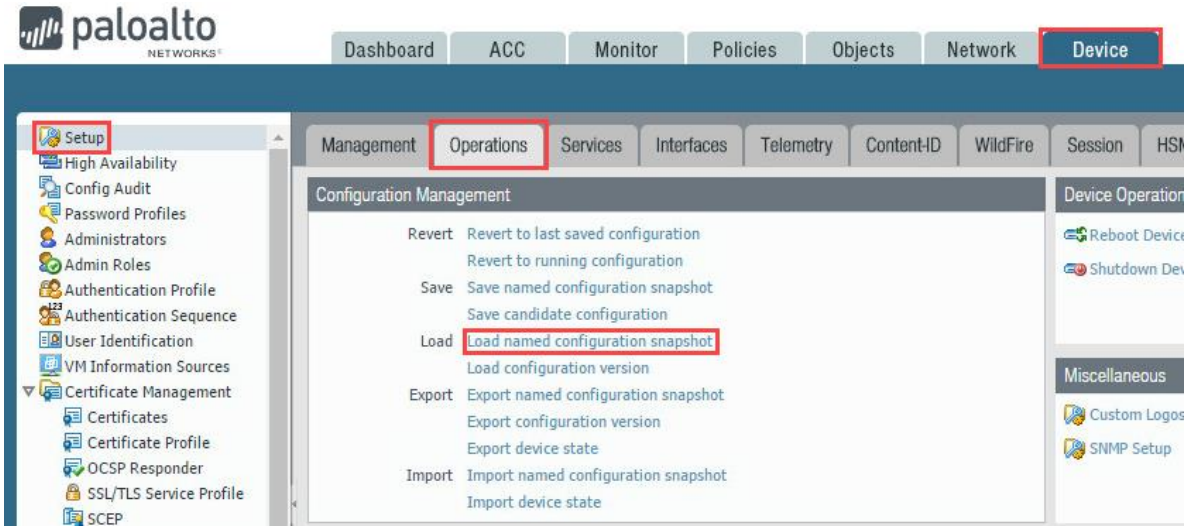
If you encounter the *"Unable to connect"* or *"502 Bad Gateway"* message while attempting to connect to the IP specified above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

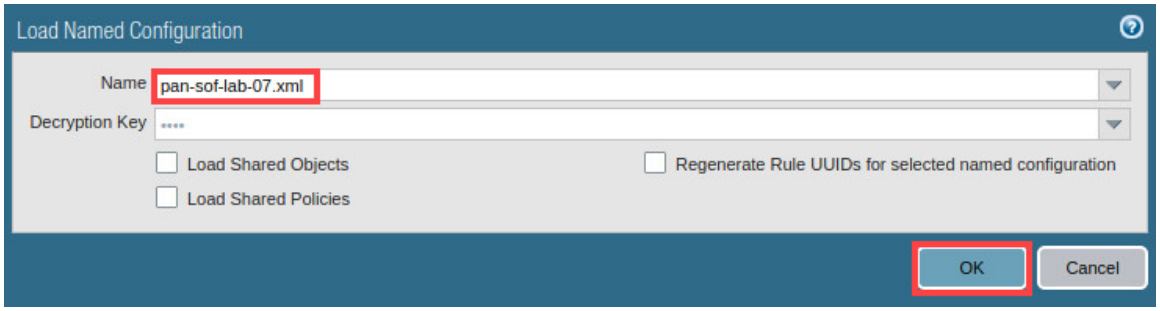


7. Log in to the Firewall web interface as username **`admin`**, password **`Train1ng$.`**

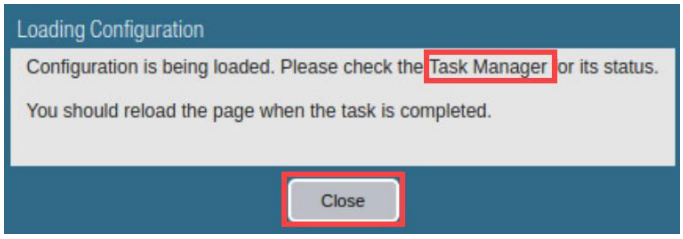
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** in the *Configuration Management* section.



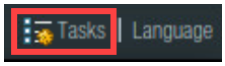
9. In the *Load Named Configuration* window, select **pan-sof-lab-07.xml** from the *Name* dropdown list and click **OK**.



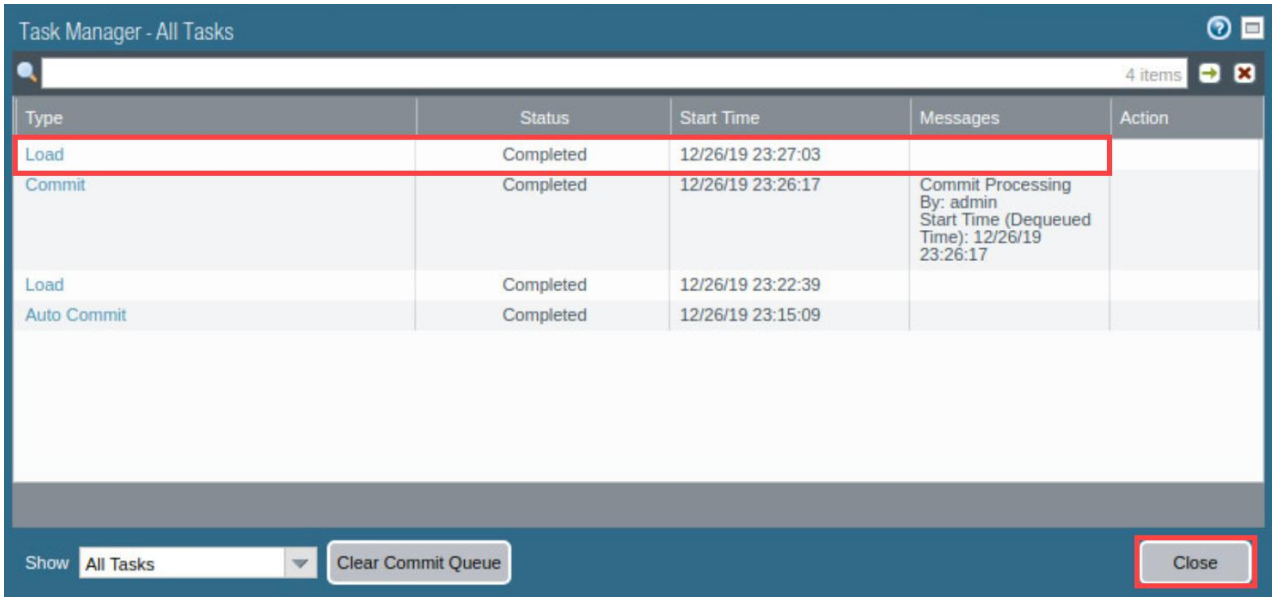
10. In the *Loading Configuration* window, a message will say *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

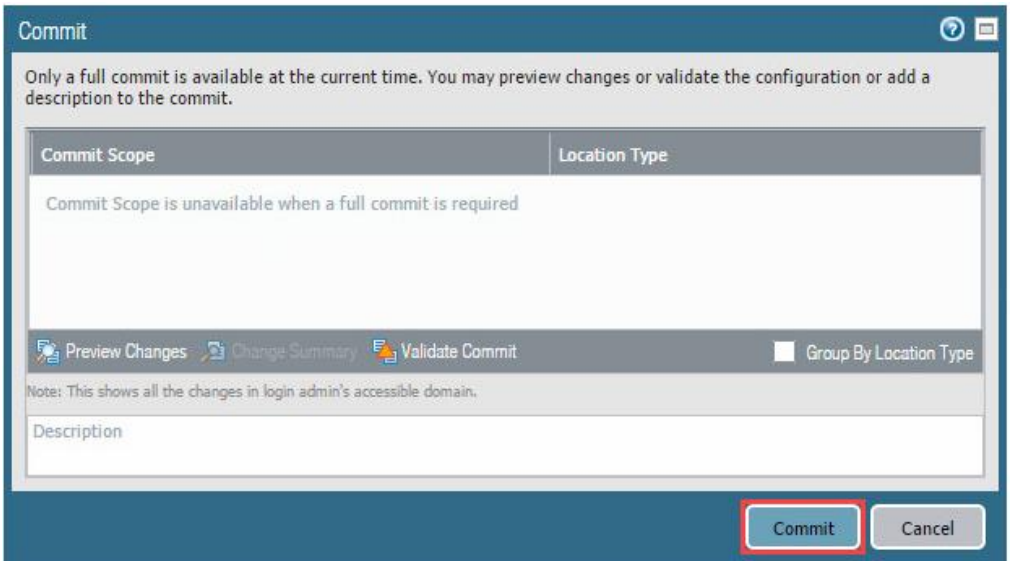


12. In the *Task Manager – All Tasks* window, verify that the *Load* type has successfully completed. Click **Close**.

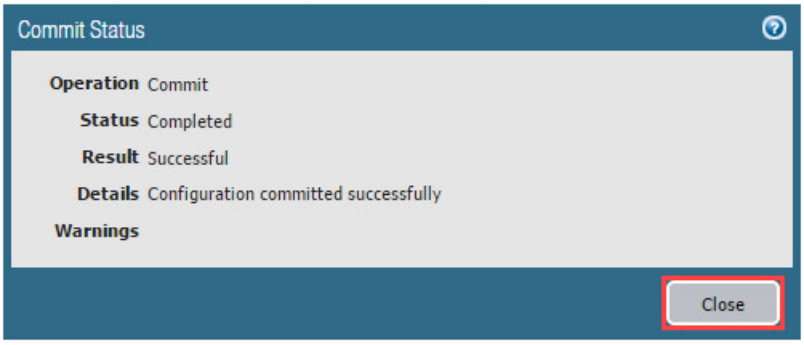


13. Click the **Commit** link located at the top-right of the web interface.

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



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. Close *Chromium* by clicking on the **X** icon located at the top-right corner.

17. Continue to the next task.

7.1 Create a Docker Volume on the Client for a MineMeld Container

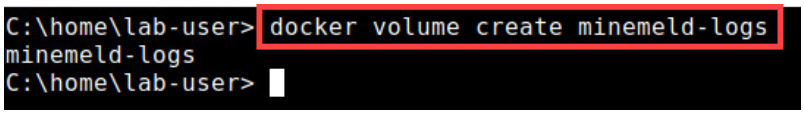
In this section, you will create a Docker volume for a MineMeld container.

When you create a Docker volume, a directory is created in the host's */var/lib/docker/volumes* directory for containers to use. You can then map the Docker volume on a host to a container's directory in either a Docker run command or by using a docker-compose.yml file. The container's data can then persist if the container stops running.

1. On the student desktop, open an *Xfce Terminal* window by clicking on the **Terminal** icon.

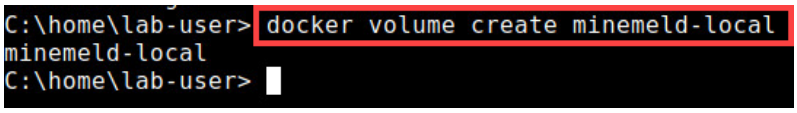
2. Create a Docker volume called **minemeld-logs** by typing the command below.

```
C:\home\lab-user> docker volume create minemeld-logs
```



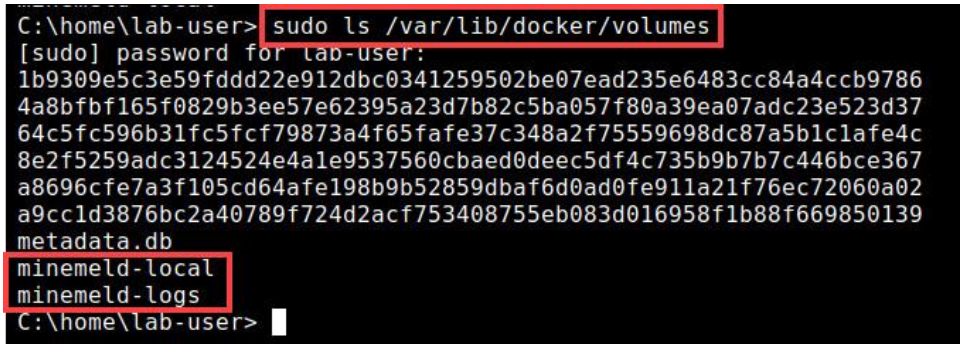
3. Create a Docker volume called **minemeld-local** by typing the command below.

```
C:\home\lab-user> docker volume create minemeld-local
```



4. View the Docker volumes created by typing the command below. When prompted for the password, type **Train1ng$** and press **Enter**.

```
C:\home\lab-user> sudo ls /var/lib/docker/volumes
```



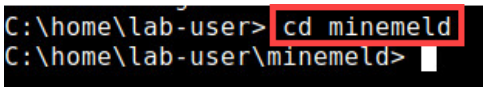
5. Leave the *terminal* window open and continue to the next task.

7.2 Launch a MineMeld Container using Docker Compose

In this section, you will create a MineMeld container and view the **docker-compose.yml** file using *vi editor*.

1. Navigate to the **minemeld** directory by typing the command below.

```
C:\home\lab-user> cd minemeld
```

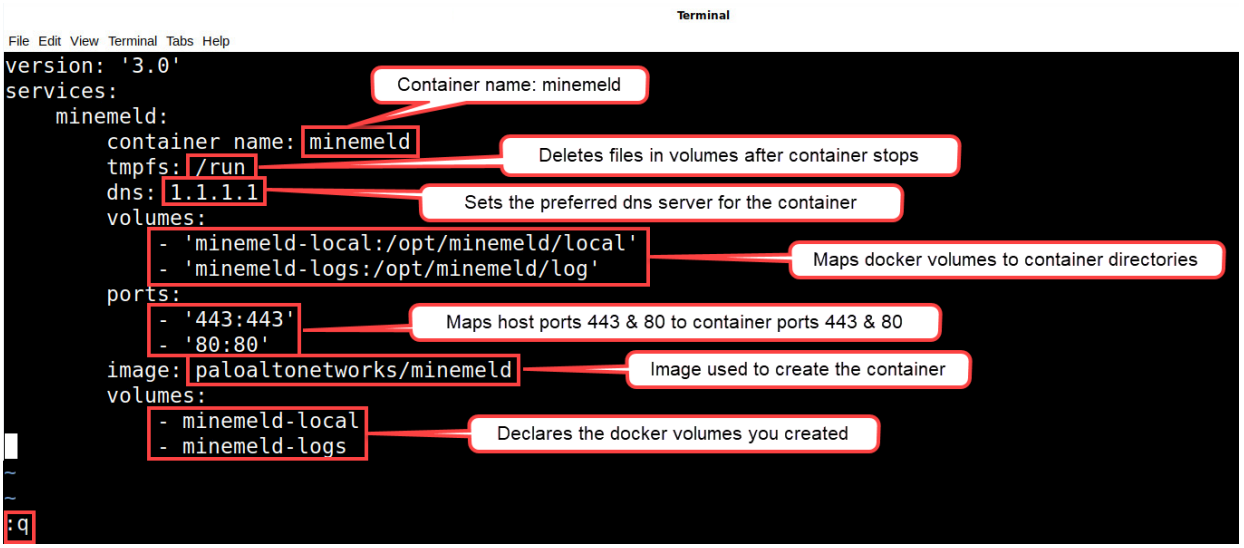


2. Observe the contents of the **docker-compose.yml** file by entering the command below.

```
[root@pod-dmz ~]# vi docker-compose.yml
```

```
C:\home\lab-user\minemeld> vi docker-compose.yml
```

3. Examine the contents of the **docker-compose.yml** file. Lastly, type `:q` and press **Enter** to exit the *vi editor* and return to the *terminal* shell.



4. Launch the MineMeld container by typing the command below.

```
[root@pod-dmz ~]# docker-compose up -d
```

```
C:\home\lab-user\minemeld> docker-compose up -d
Creating network "minemeld_default" with the default driver
Creating minemeld ... done
C:\home\lab-user\minemeld>
```

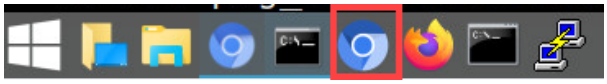

5. View the **minemeld-logs** volume by typing the command below. When prompted for the password, type **Train1ng$** and press **Enter**.

```
[root@pod-dmz ~]# sudo docker logs minemeld
```

```
C:\home\lab-user\minemeld> sudo docker logs minemeld
[sudo] password for lab-user:
*** Running /etc/rc.local...
*** Booting runit daemon...
*** Runit started as PID 7
minemeld: checking if dependencies are running...
run: redis: (pid 20) 0s
run: collectd: (pid 21) 0s
Copying constraints
Starting redis-server...
Regenarating CA bundle
2021-01-04T04:23:48 (34)cacert_merge.main INFO: config: {'cafile': ['/opt/minemeld/local/certs/site/'], 'dst': '/opt/m
inemeld/local/certs/bundle.crt', 'config': '/opt/minemeld/local/certs/cacert-merge-config.yml', 'no_merge_certifi': Fa
lse}
0
Starting minemeld...
/opt/minemeld/engine/0.9.70.post1/local/lib/python2.7/site-packages/supervisor/options.py:383: PkgResourcesDeprecation
Warning: Parameters to load are deprecated.  Call .resolve and .require separately.
  return pkg_resources.EntryPoint.parse("x="+spec).load(False)
```

6. Minimize the *terminal* window by clicking the **Minimize** icon in the top-right of the *terminal* window.

7. Open a new *Chromium* web browser by clicking on the **Chromium** icon in the lower-left of the student desktop.



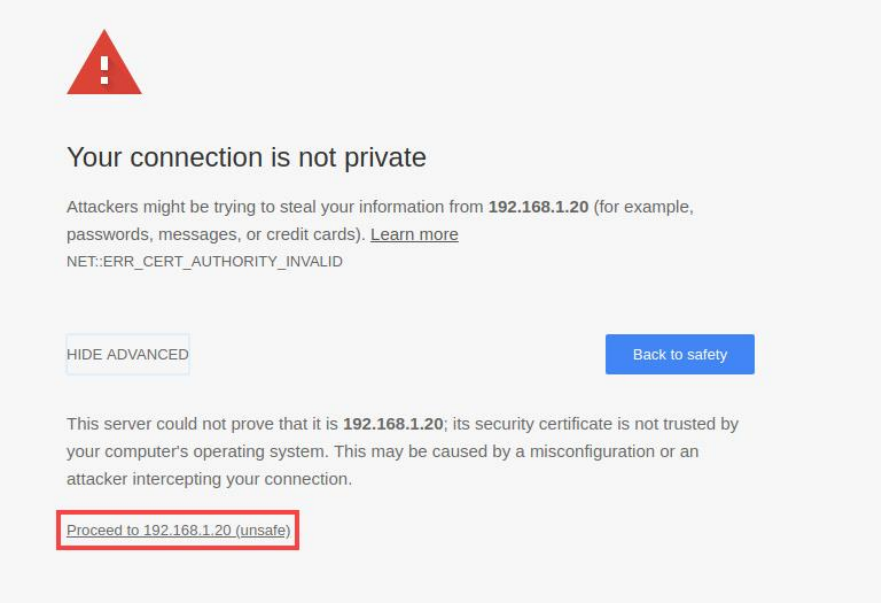
8. Leave *Chromium* open and continue to the next task.

7.3 Access the MineMeld Web UI to View the Default Configurations

In this section, you will access MineMeld to aggregate threat intelligence feeds across public, private and commercial intelligence sources that include government and commercial organizations.

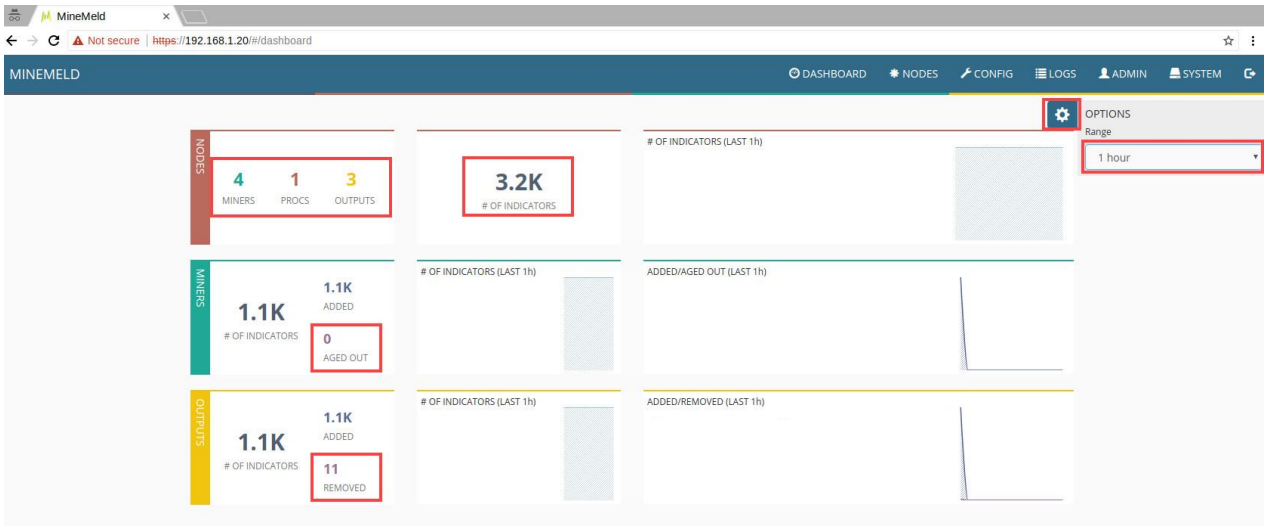
1. In the *Chromium* web browser, enter **https://192.168.1.20** in the address bar and press **Enter**.

2. In the *Your connection is not private* window, advance through the security warning and click **Proceed to 192.168.1.20 (unsafe).**



3. Log on to the *MineMeld Web UI* by typing **`admin`** for the username and **`minemeld`** for the password. Click **Login**.

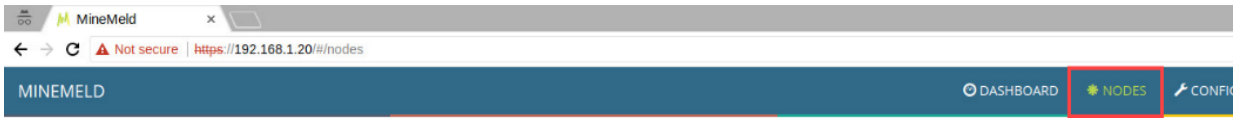
4. In the *MineMeld Web UI's* dashboard, click the settings **gear** icon on the far-right and change the range to **1 hour**. In the **Nodes** widget, note you have 4 Miners, 1 Processor and 3 Outputs. The **Miners** collect and serve the intelligence feed indicators containing block lists to the **Processors**. The **Processors** deduplicate and process the intelligence feeds for the **Outputs**. The **Outputs** can send the intelligence indicators to downstream MineMeld instances, to firewall/IPS devices, and/or to endpoint protection software.



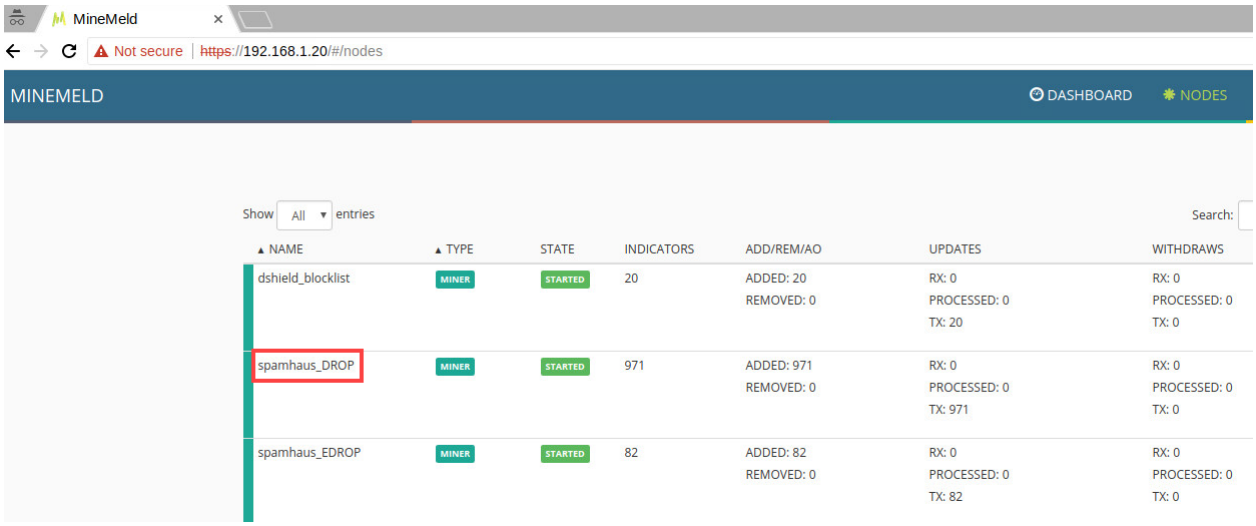
Please Note

Note that there are 3.2K block list indicators and the intelligence feed indicators are constantly being updated. The number of indicators may vary.

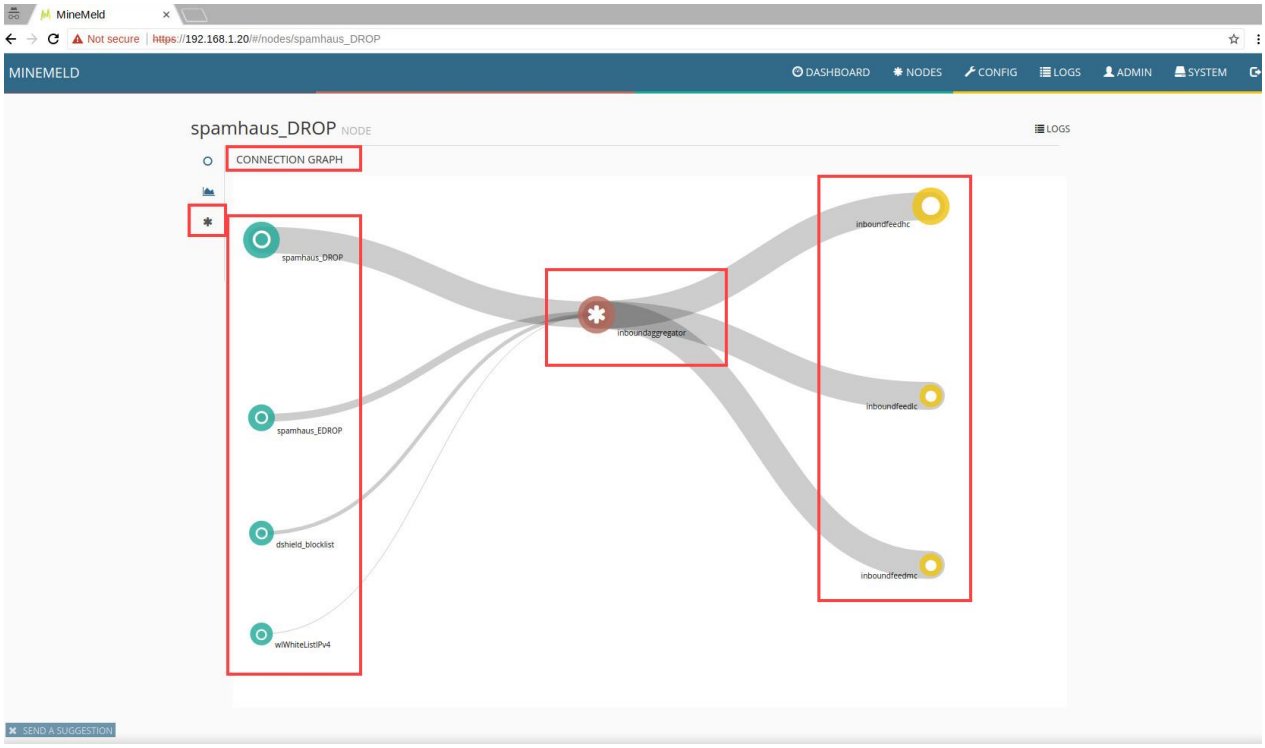
5. In the *MineMeld UI*, navigate to the *Nodes* webpage by clicking on the **NODES** link.



6. On the *nodes* webpage, select the **spamhaus_Drop** Miner.



7. On the **spamhaus_DROP** node, select the **graph** icon. In the *CONNECTION GRAPH*, you should see 4 Miners (which collect the block list indicators) connect to the **inboundaggregator** Processor**.** This Processor feeds the processed indicators to 3 Output nodes: **inboundfeedhc** (hc=high confidence), **inboundfeedlc** (lc=low confidence), and **inboundfeedmc** (mc = medium confidence).

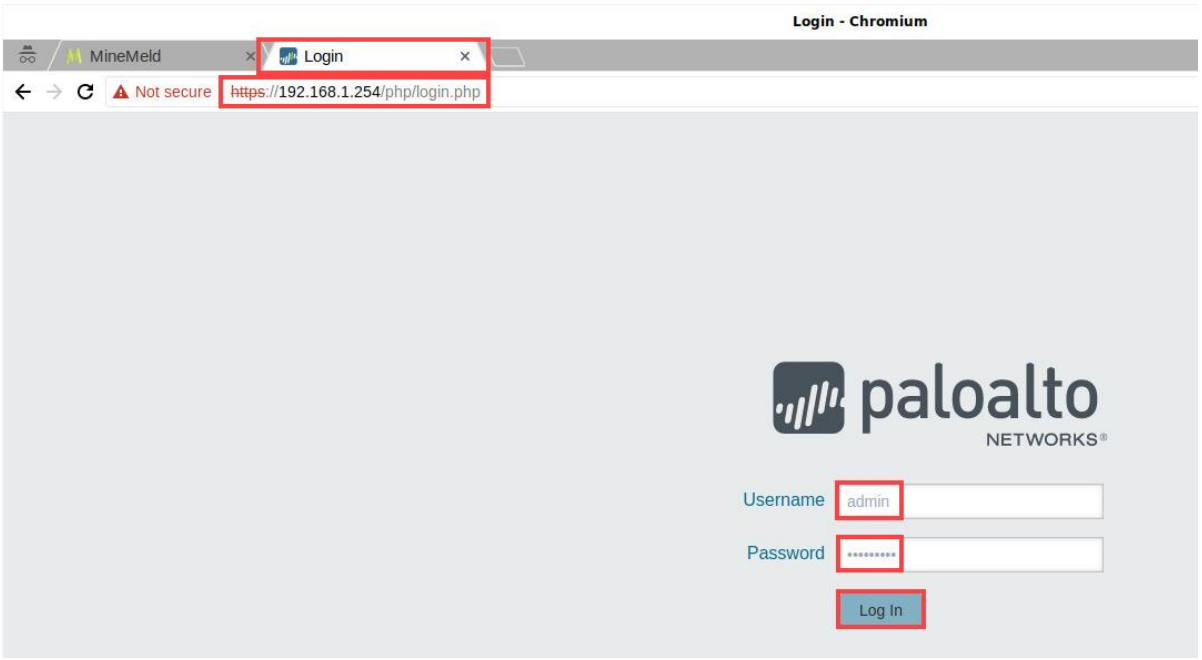


8. Leave the *Chromium* web browser open and continue to the next task.

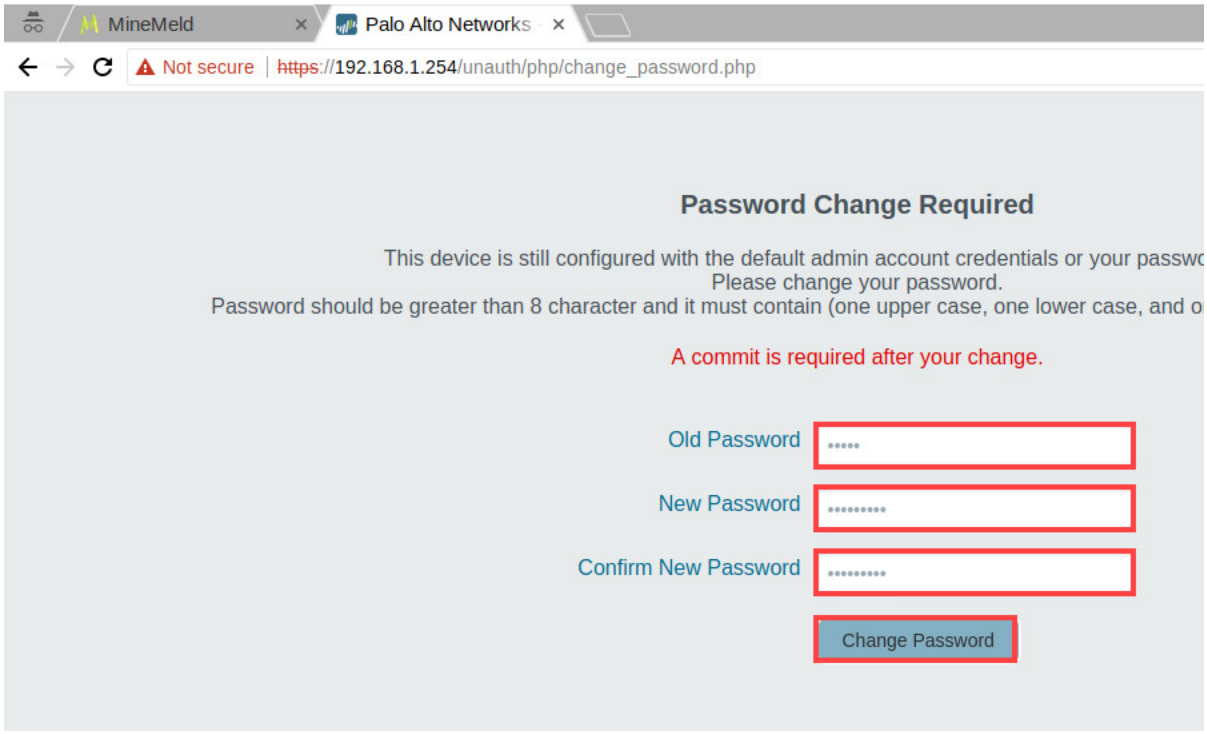
7.4 Configure an External Dynamic List (EDL) on the Firewall Appliance Using a MineMeld Output Feed

In this section, you will configure an External Dynamic List (EDL) on the Firewall to use the *inboundfeedhc* Output node feed and then use the EDL in a Security Policy rule to block incoming traffic.

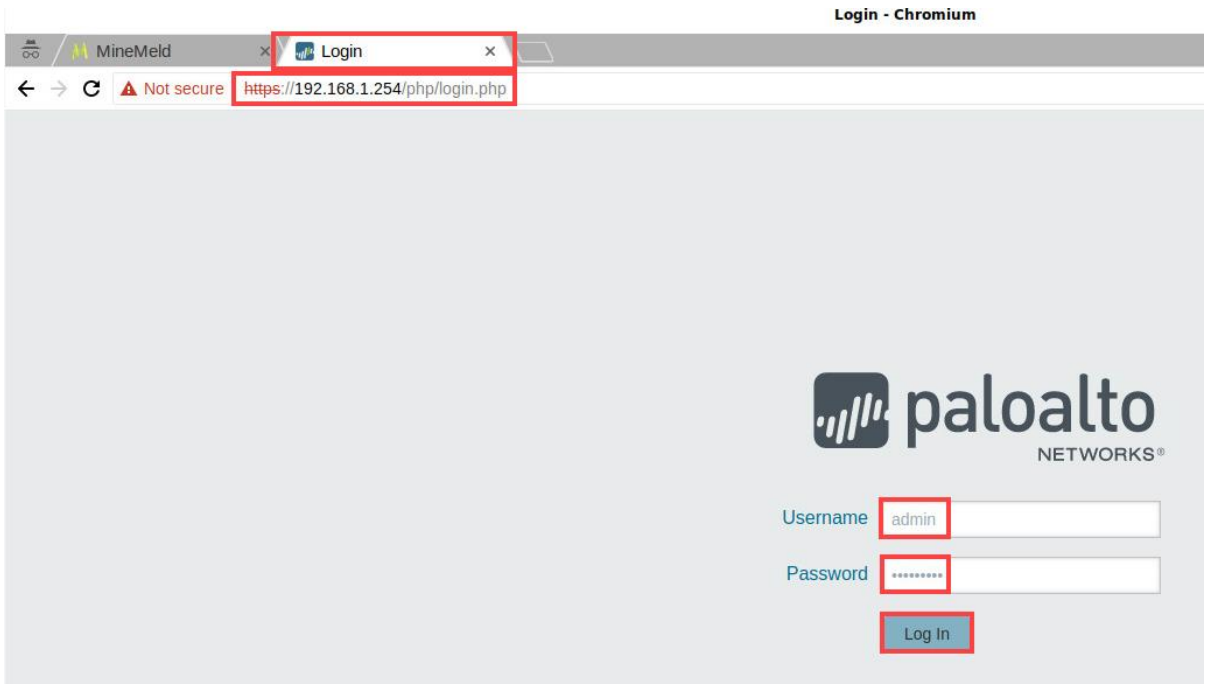
1. In the *Chromium* web browser, open a new tab and enter **`https://192.168.1.254`** in the address bar and press **Enter**. For the username, enter **`admin`** and for the password enter **`Train1ng$.`** If successful, continue to *step* **4**. If you cannot log in, enter **`admin`** for the username and **`admin`** for the password. Click **Log In**.



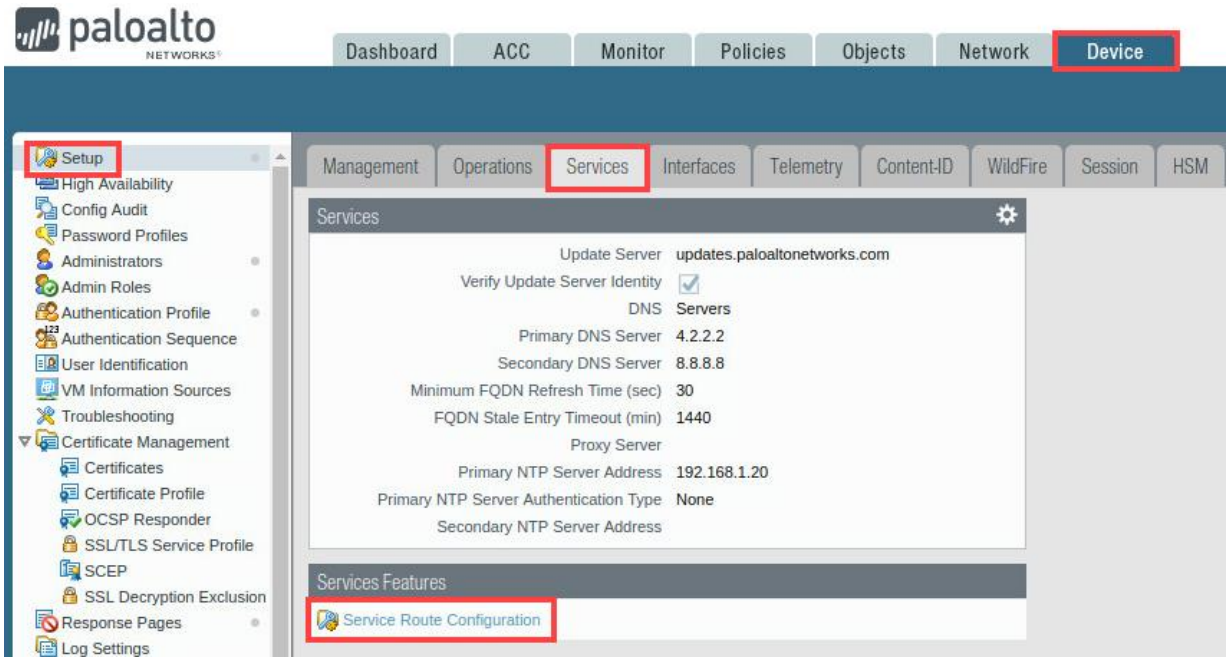
2. If the *Password Change Required* window appears, type **admin** for the *Old Password*, and **Train1ng$** for the *New Password* and *Confirm Password* fields. Click **Change Password**.



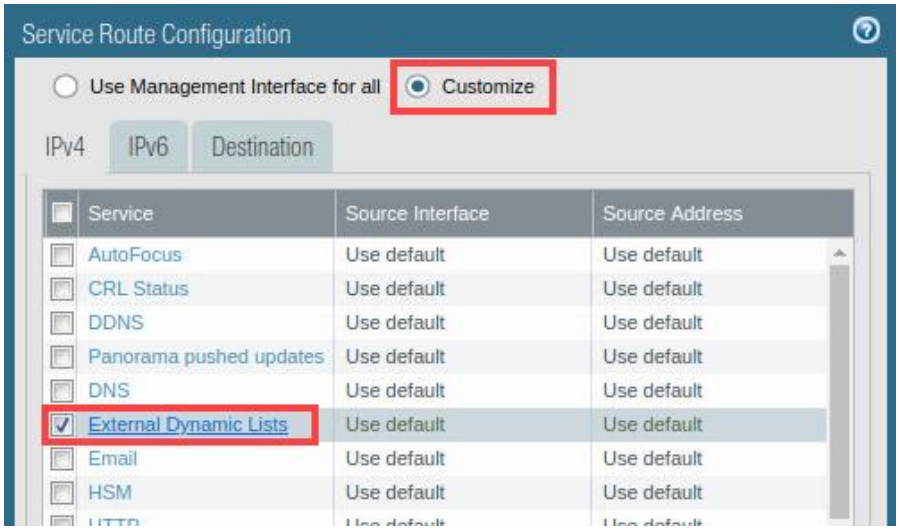
3. When prompted to log back in, enter **admin** for the username and **Train1ng$** for the password. Click **Log In**.



4. Navigate to **Device > Setup > Services** and select **Service Route Configuration**.

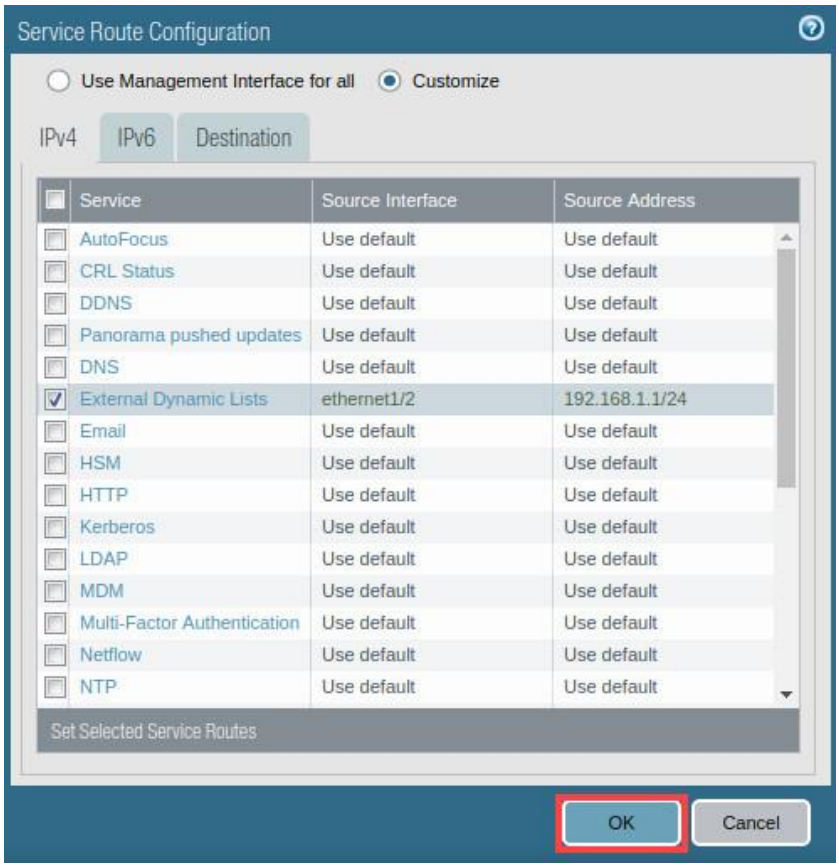


5. In the *Service Route Configuration* dialog box, select **Customize**. Select and click **External Dynamic Lists**.

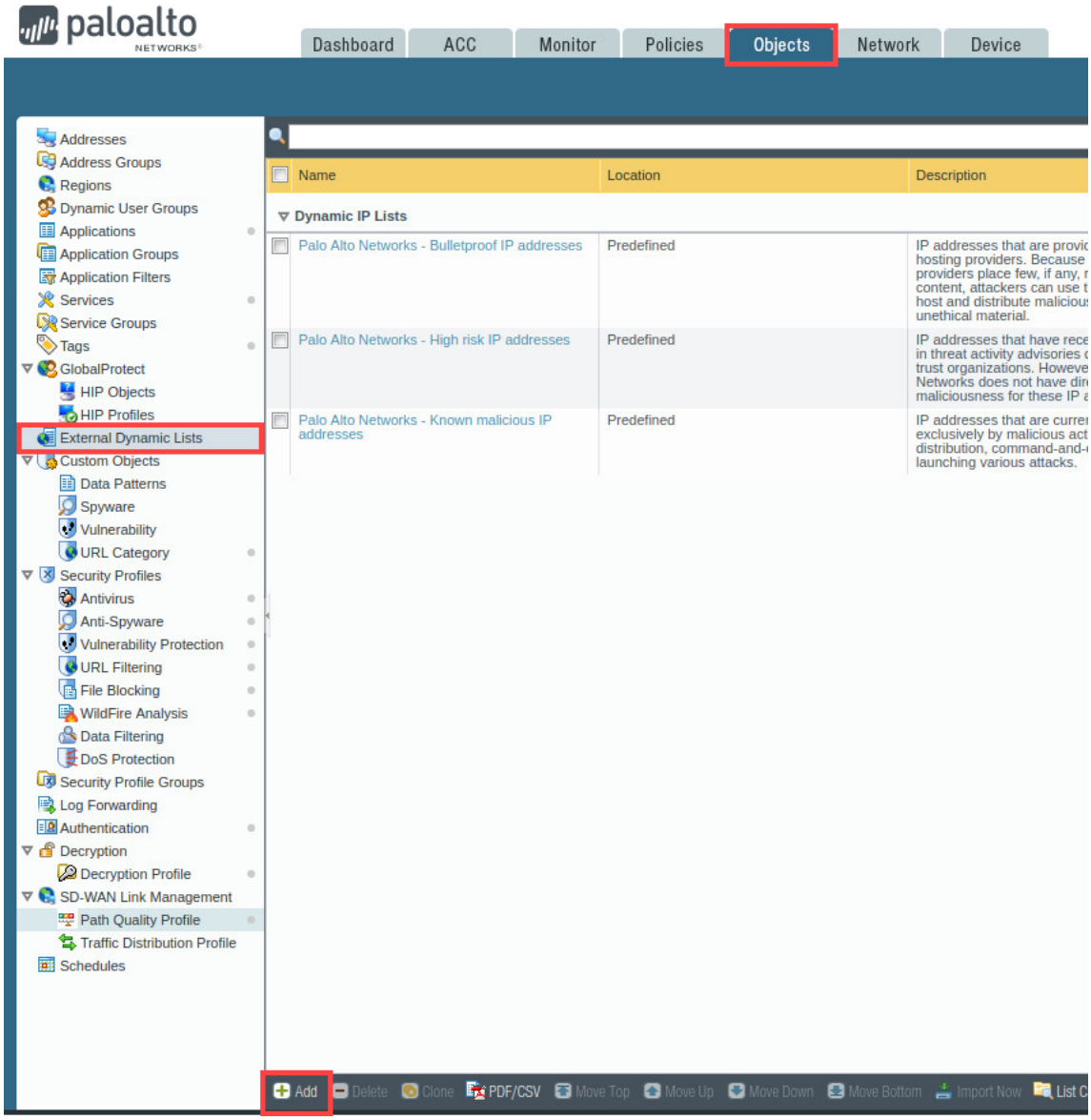


6. In the *Service Route Source* dialog box, select **ethernet1/2** for the *Source Interface* and verify **192.168.1.1/24** for the *Source Address*. Click **OK**.

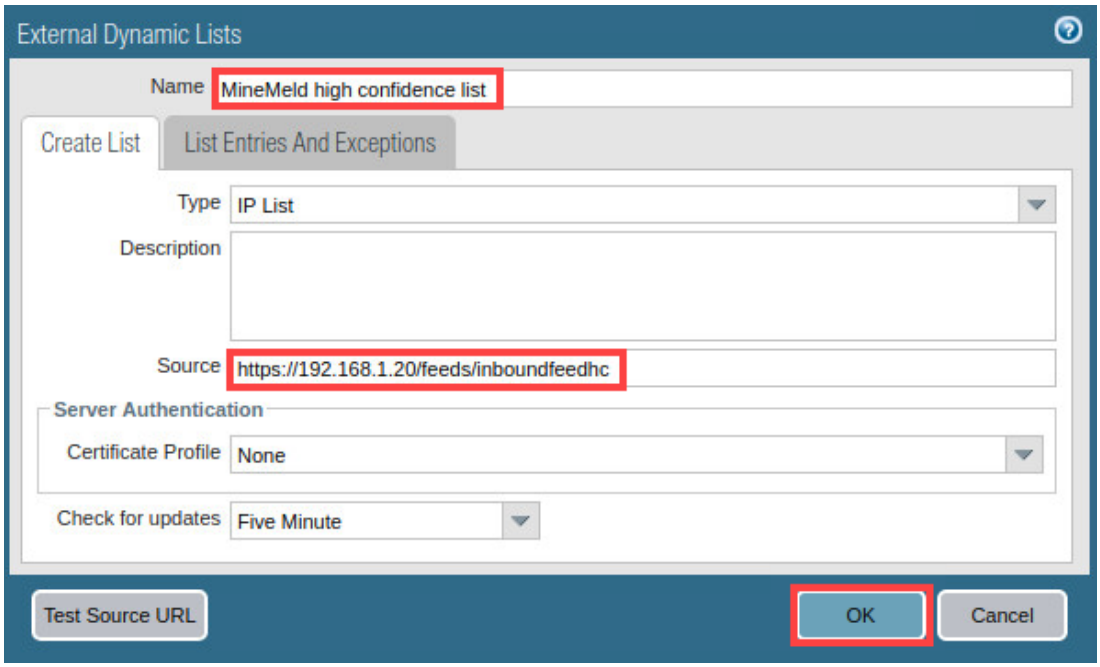
7. In the *Service Route Configuration* window, click **OK**.



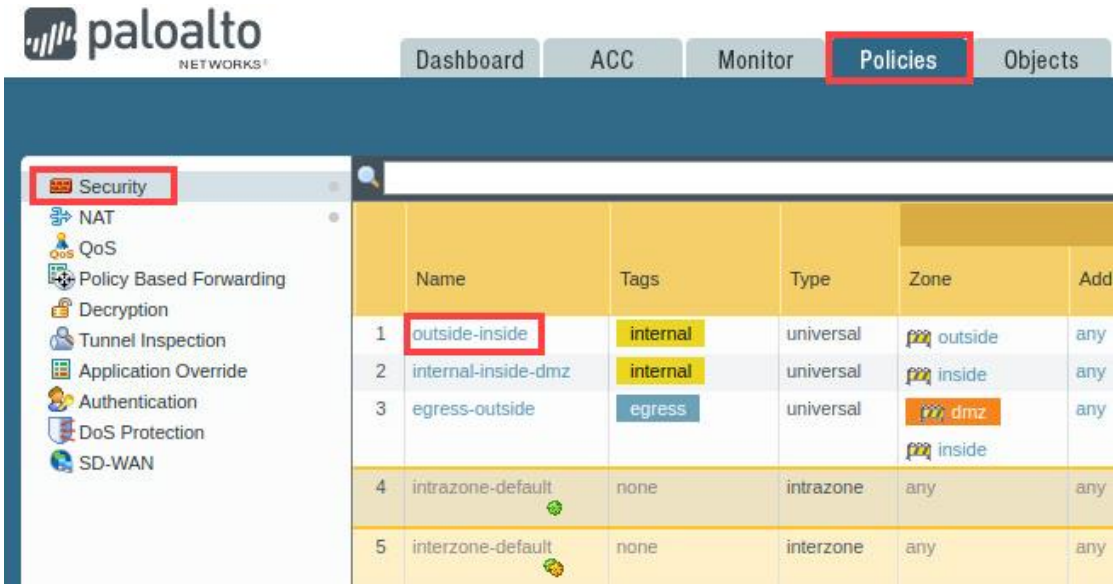
8. Navigate to **Objects > External Dynamic Lists** and select **Add**.



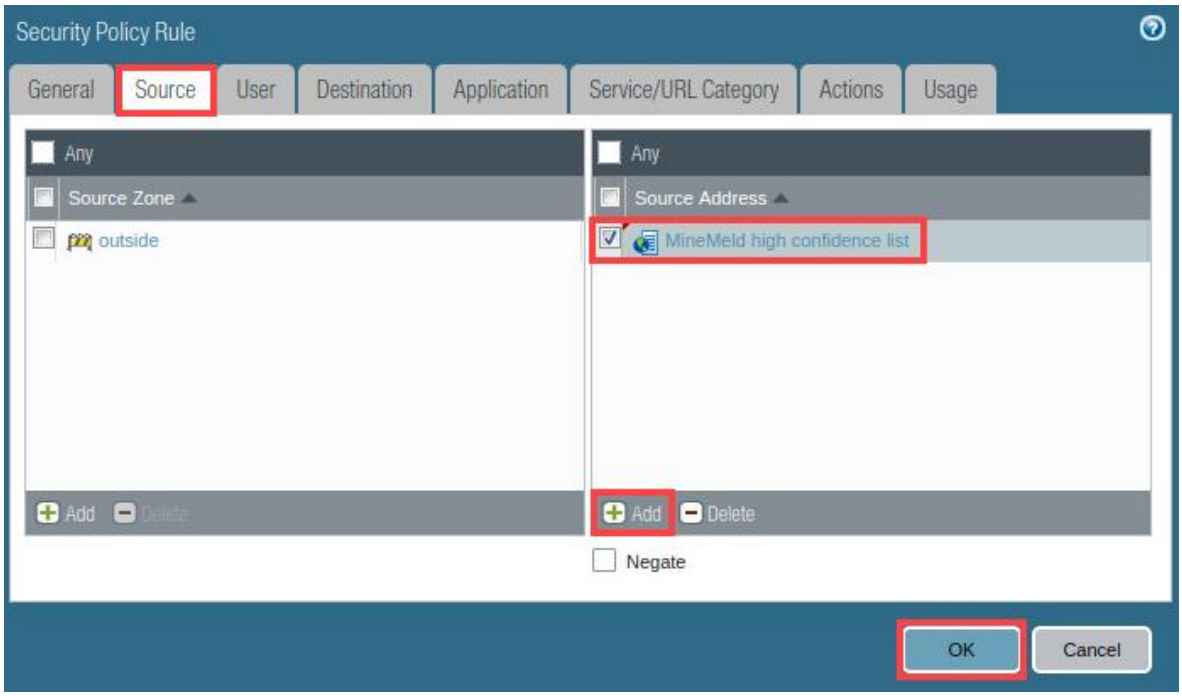
9. In the *External Dynamic Lists* window, type **`MineMeld high confidence list`** in the *Name* field, and enter **`https://192.168.1.20/feeds/inboundfeedhc`** for the *Source*. Click **OK**.



10. Navigate to **Policies > Security** and select the **outside-inside** policy.

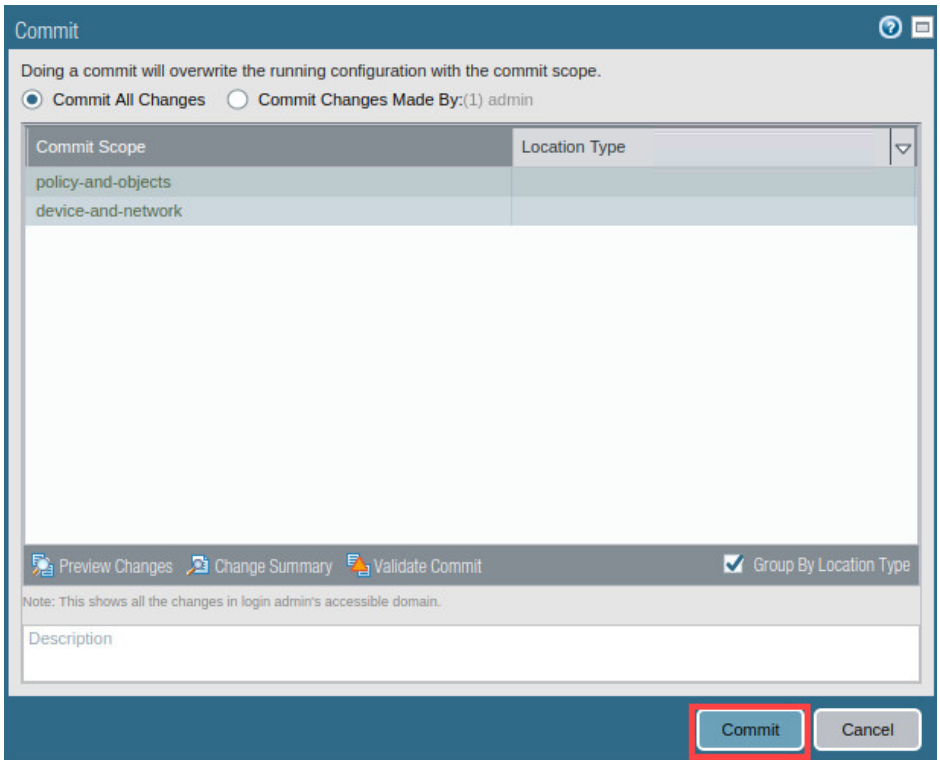


11. In the *Security Policy Rule* window, select the **Source** tab. In the *Source Address* box, click **Add**. Select the **MineMeld high confidence list** from the dropdown menu. Click **OK** to close the *Security Policy Rule* window.

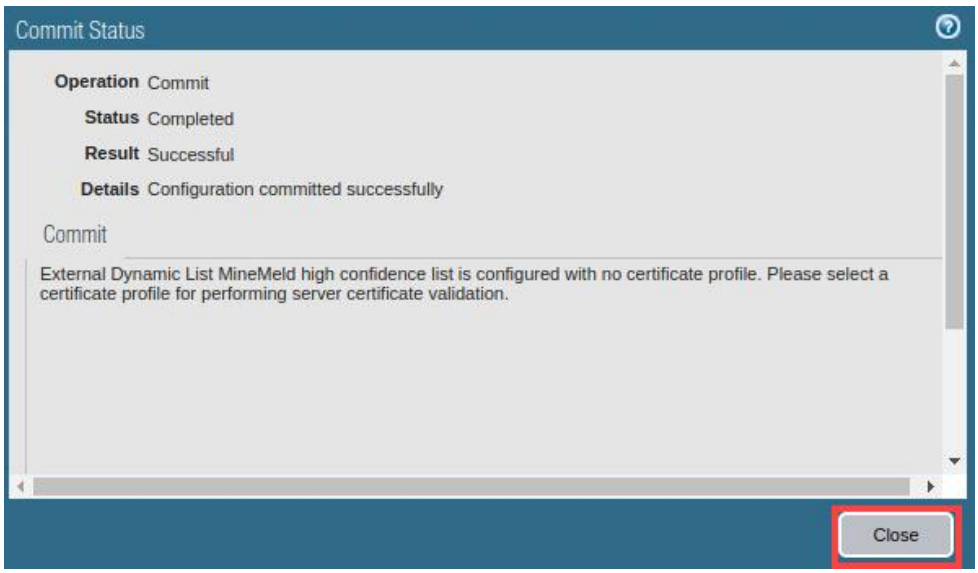


12. Click the **Commit** link located at the top-right of the web interface.

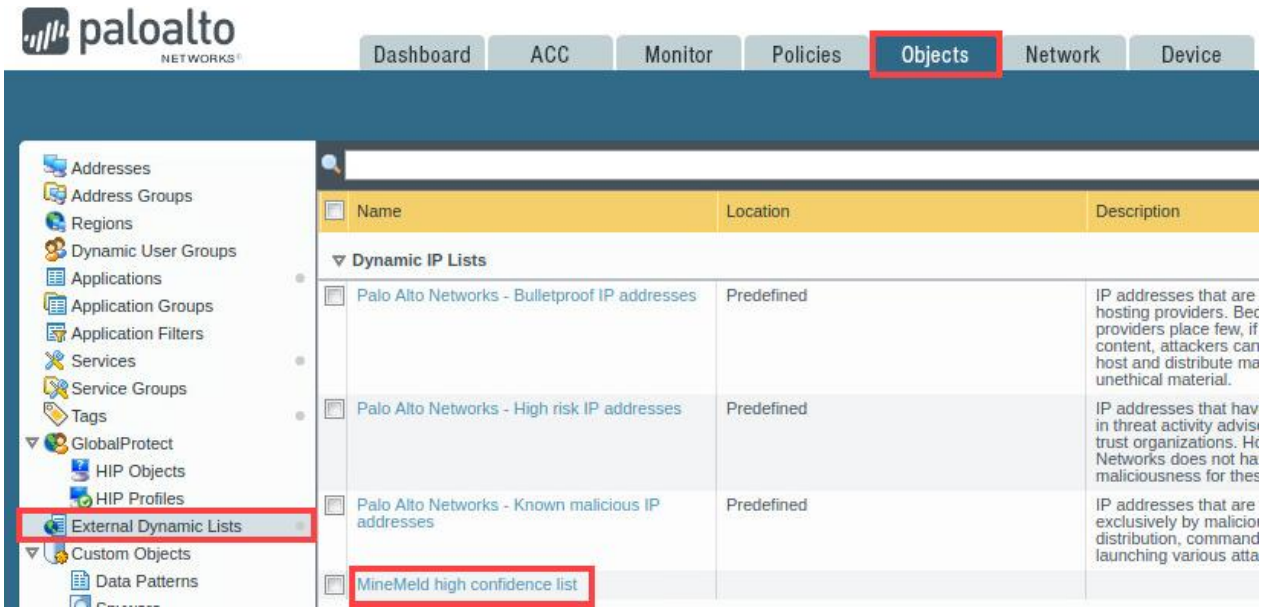
13. In the *Commit* window, click **Commit**.



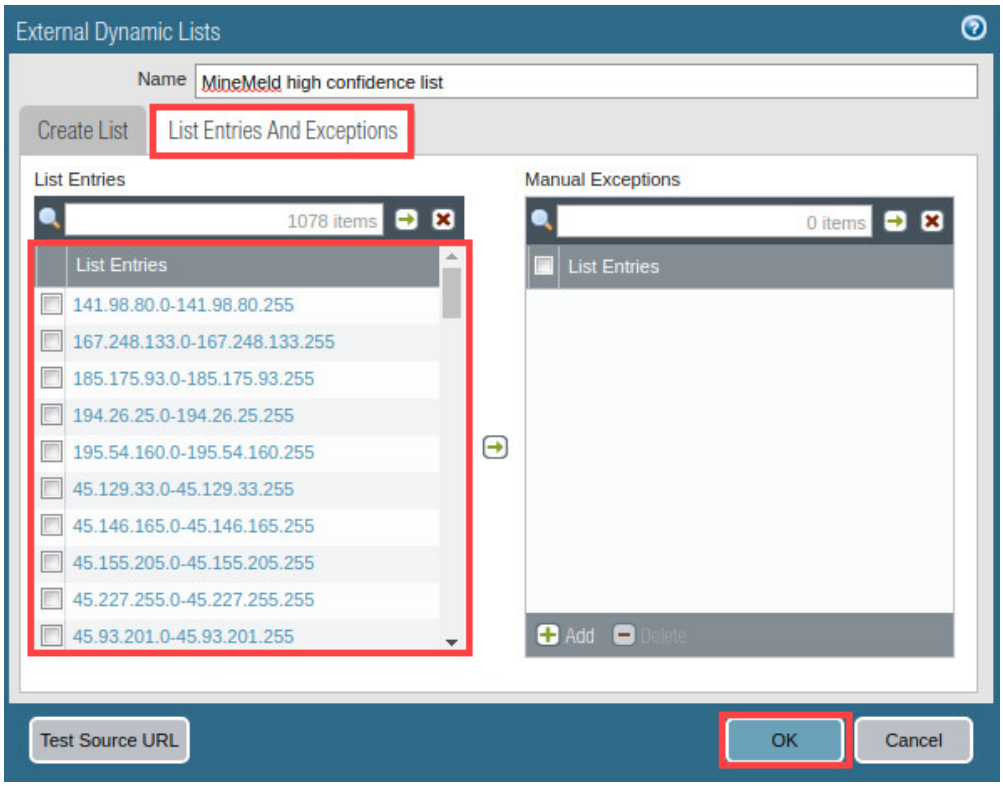
14. Once the commit finishes, click **Close**.



15. Navigate to **Objects > External Dynamic Lists** and click the **MineMeld high confidence list**.



16. In the *External Dynamic Lists* window, select **List Entries and Exceptions** and observe the *IP block list indicators* that MineMeld is feeding the Palo Alto Networks Firewall. Click **OK**.

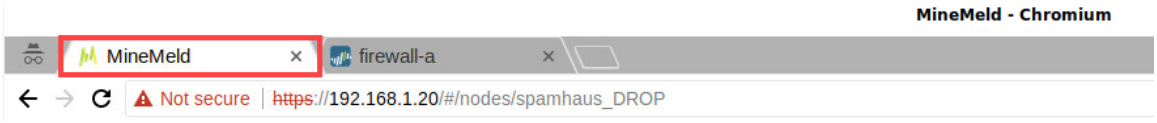


17. Leave *Chromium* open and continue to the next task.

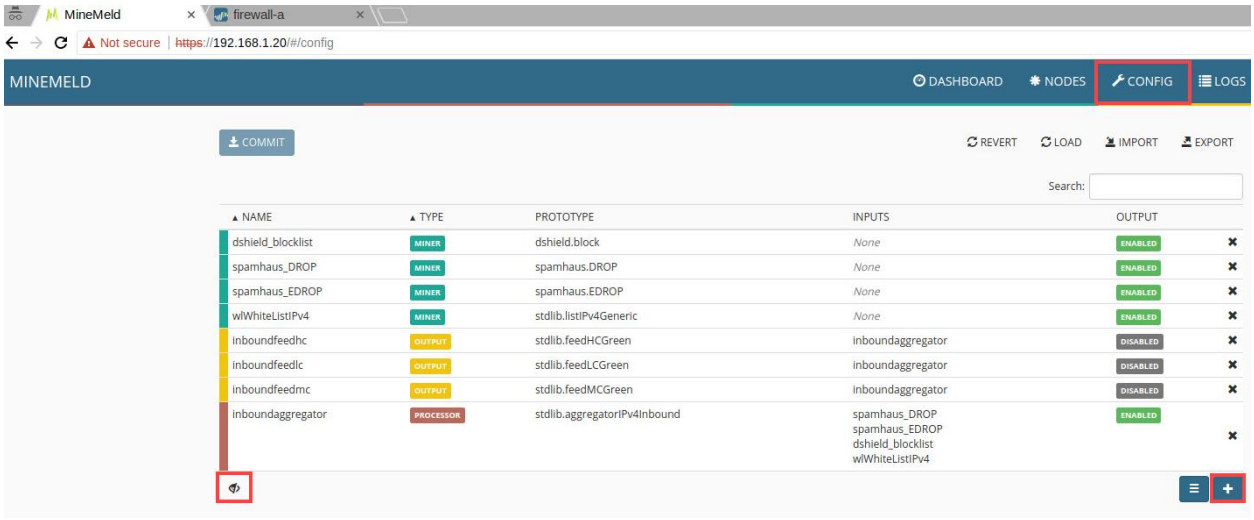
7.5 Configure Custom MineMeld Miner, Processor and Output Nodes, and Configure an EDL to use the Custom Output Node

In this section, you will configure custom MineMeld Miner, Processor and Output nodes. You will also configure an EDL to use the custom Output node.

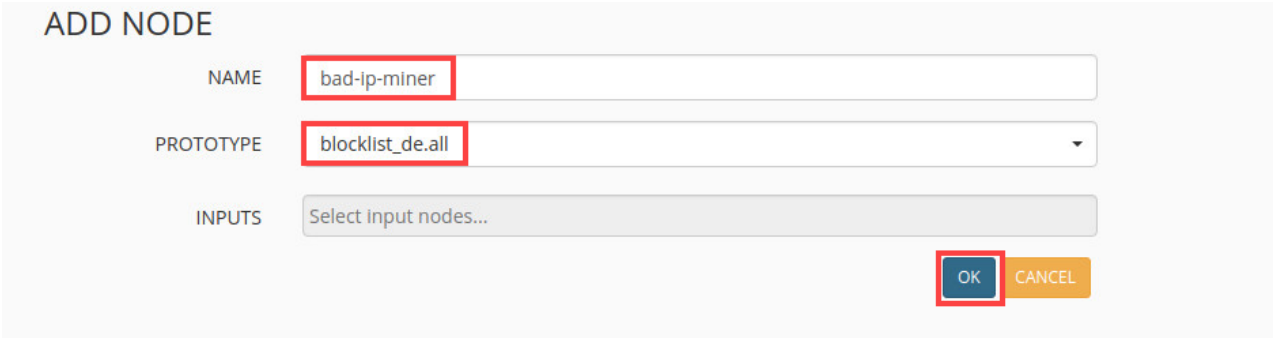
1. Change focus back to MineMeld by clicking on the **MindMeld** tab.



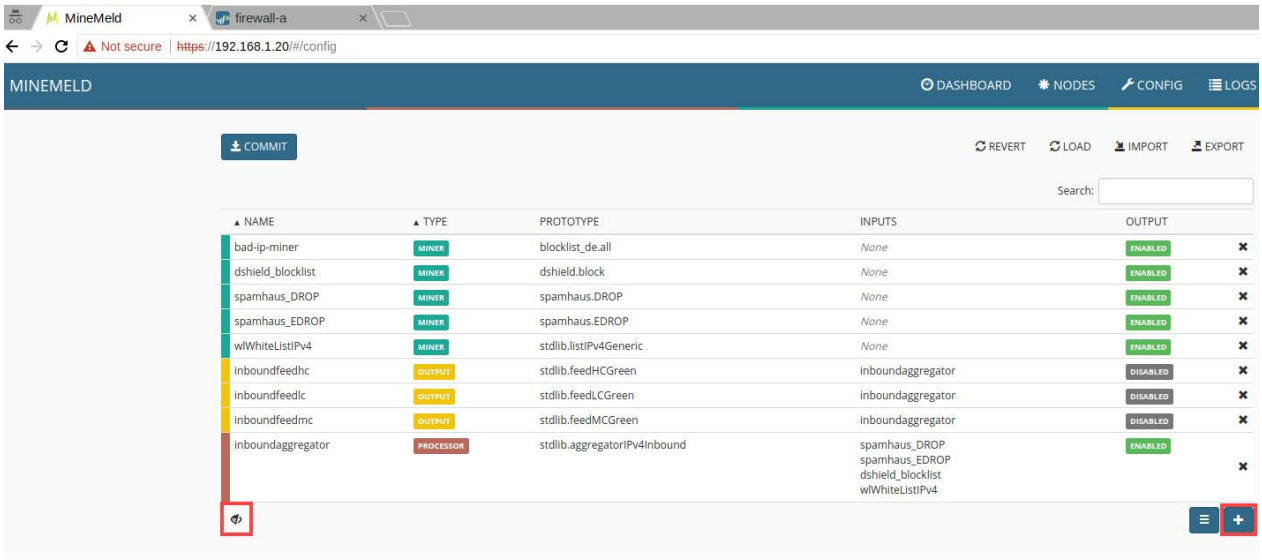
2. In the *MineMeld Web UI*, browse to the **CONFIG** tab. On the *config* webpage, click the **eye** icon in the lower-left corner and then click the **+** icon that appears at the far-right bottom.



3. On the *ADD NODE* webpage, enter **`bad-ip-miner`** for the *NAME*. Select **blocklist_de.all** for the *PROTOTYPE*. Leave all other defaults and click **OK**.

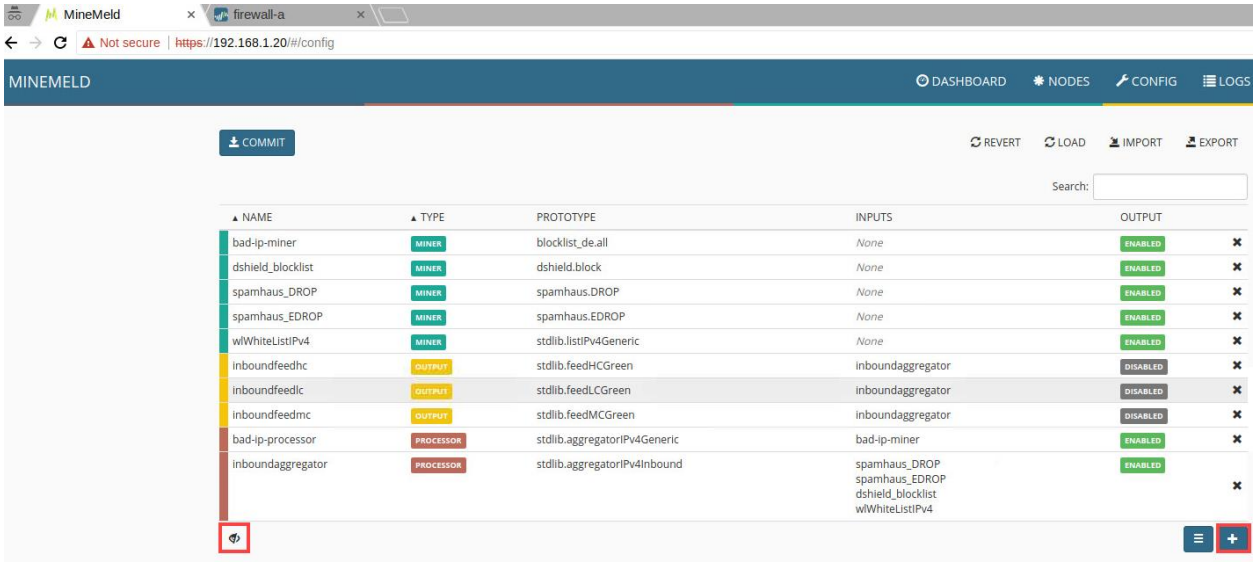


4. On the **CONFIG** tab, on the *config* webpage, click the **eye** icon in the lower-left corner and then click the **+** icon that appears at the far-right bottom.



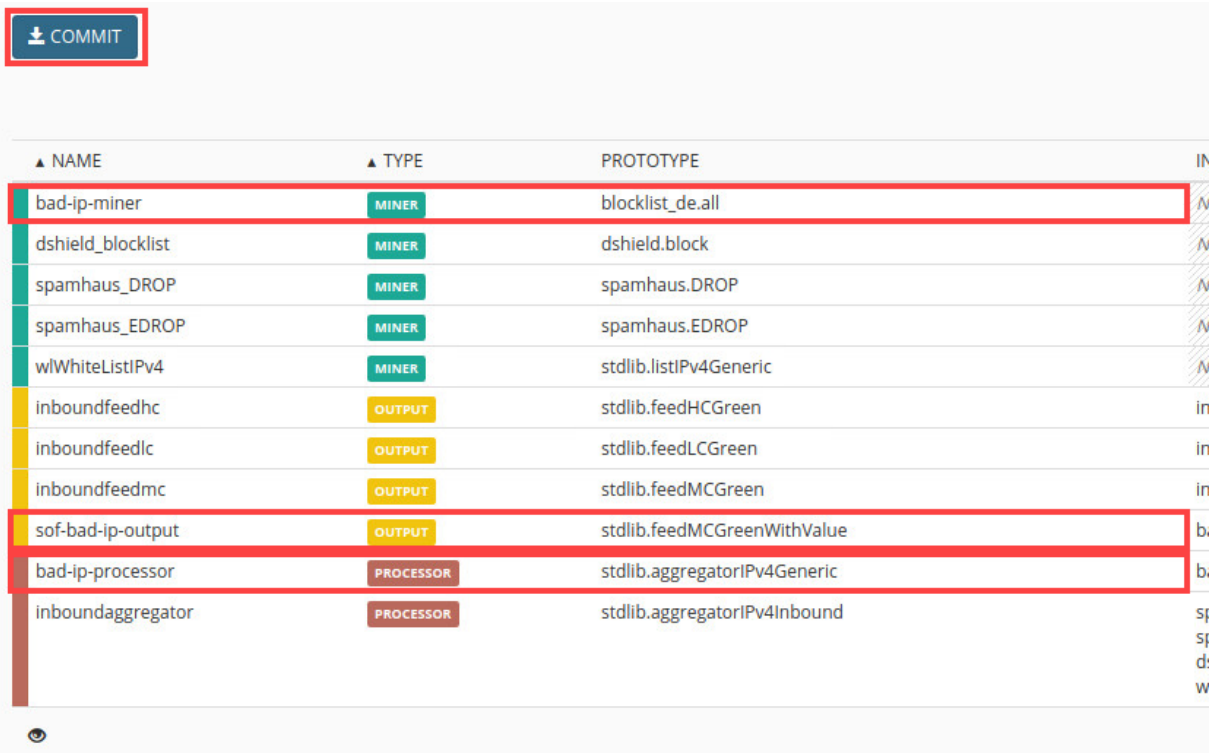
5. On the *ADD NODE* webpage, enter **`bad-ip-processor`** for the *NAME*. Select **stdlib.aggregatorIPv4Generic** for the *PROTOTYPE*. For the *INPUTS*, select **bad-ip-miner** and click **OK**.

6. On the **CONFIG** tab, on the *config* webpage, click the **eye** icon in the lower-left corner and then click the **+** icon that appears at the far-right bottom.

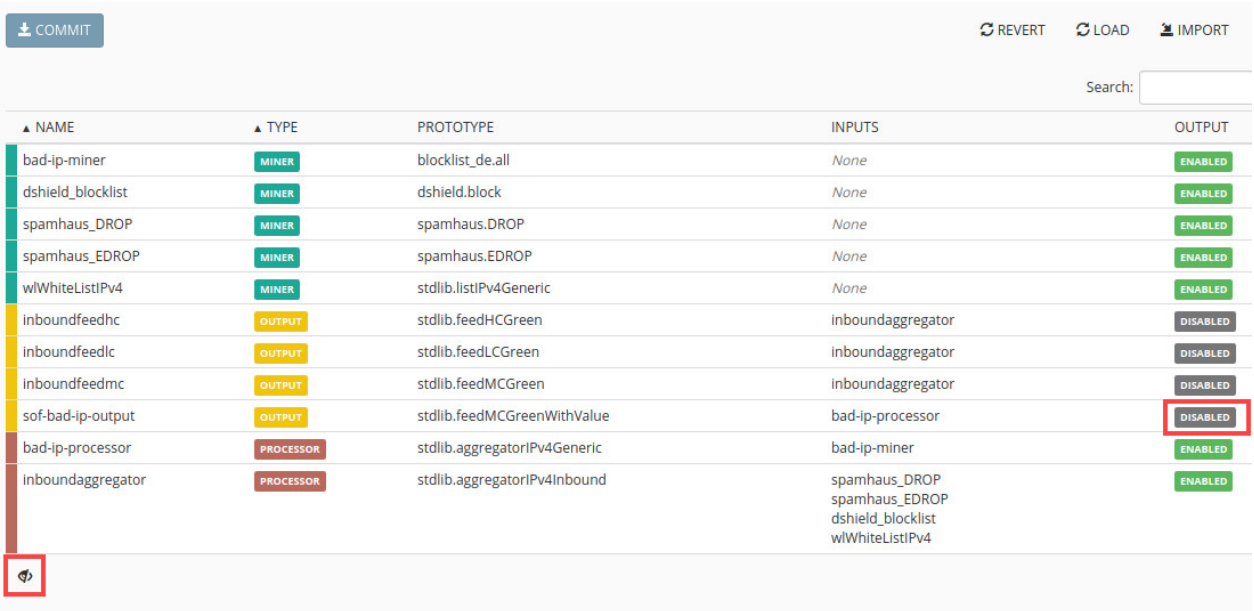


7. On the *ADD NODE* webpage, enter **`sof-bad-ip-output`** for the *NAME*. Select **stdlib.feedMCGreenWithValue** for the *PROTOTYPE*. For the INPUTS, select **bad-ip-processor** and click **OK**.

8. On the *config* webpage, verify that **bad-ip-miner**, **bad-ip-processor** and **sof-bad-ip-output** are showing. Click **COMMIT** to save your changes.



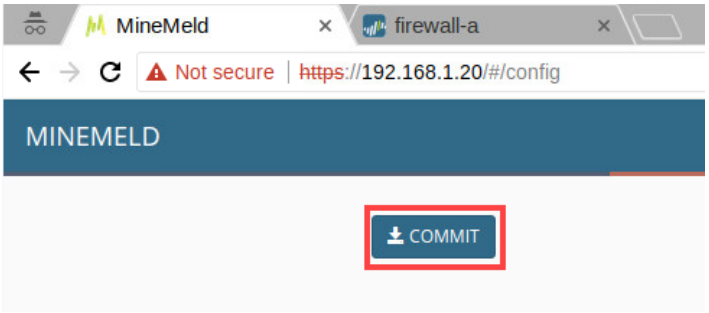
9. On the *config* webpage, click the **eye** icon. For **sof-bad-ip-output** click the **DISABLED** to the far right.



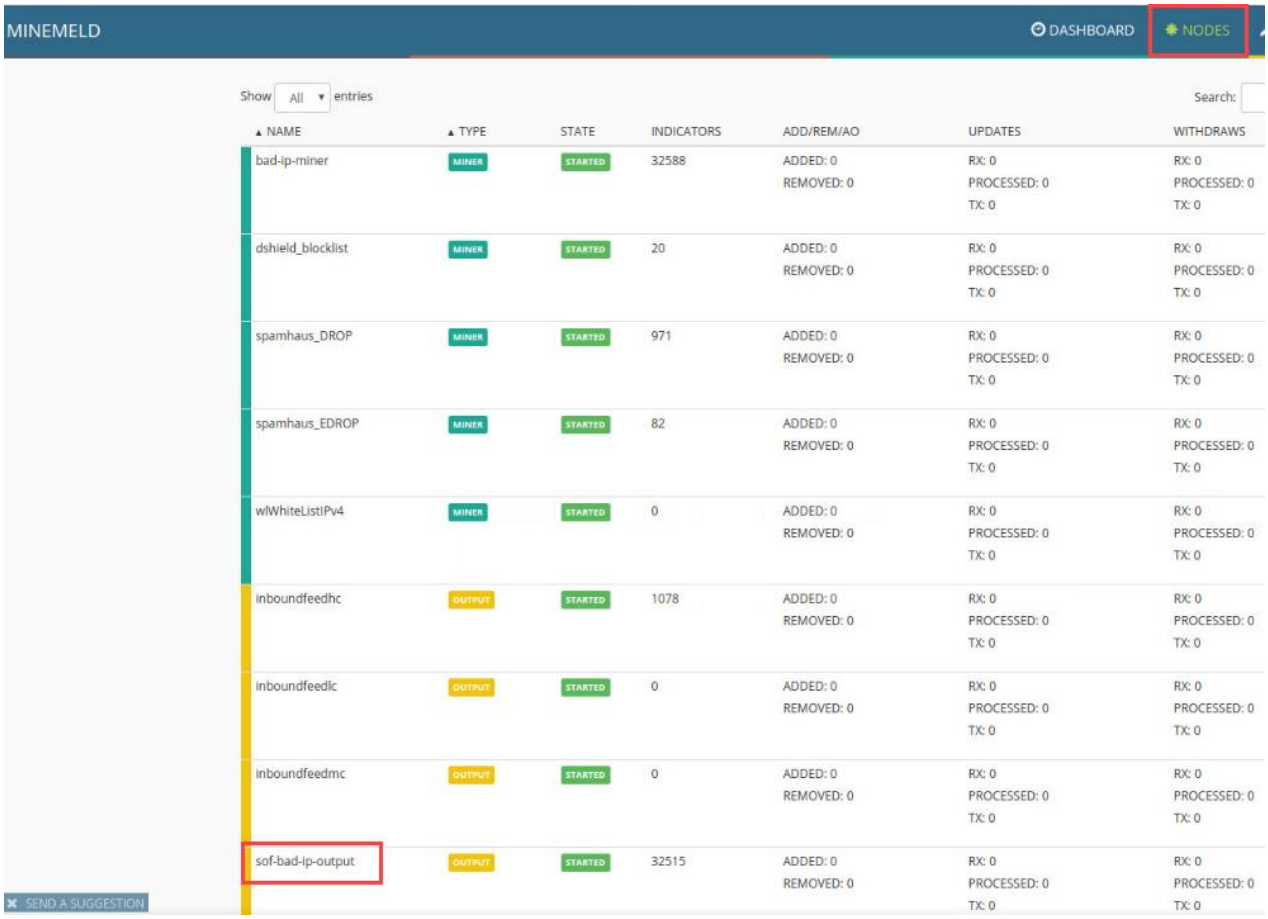
10. In the *sof-bad-ip-output* window dialog box, click **DISABALED**.

11. In the *sof-bad-ip-output* window dialog box, the output should now be **ENABLED**. Click **OK**.

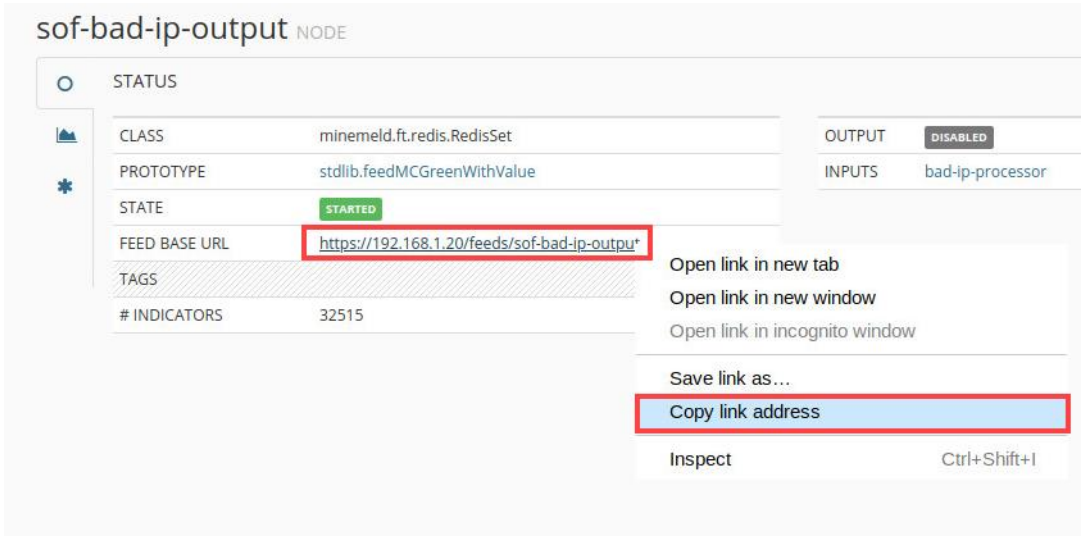
12. On the *config* webpage, click **COMMIT** to save your changes.



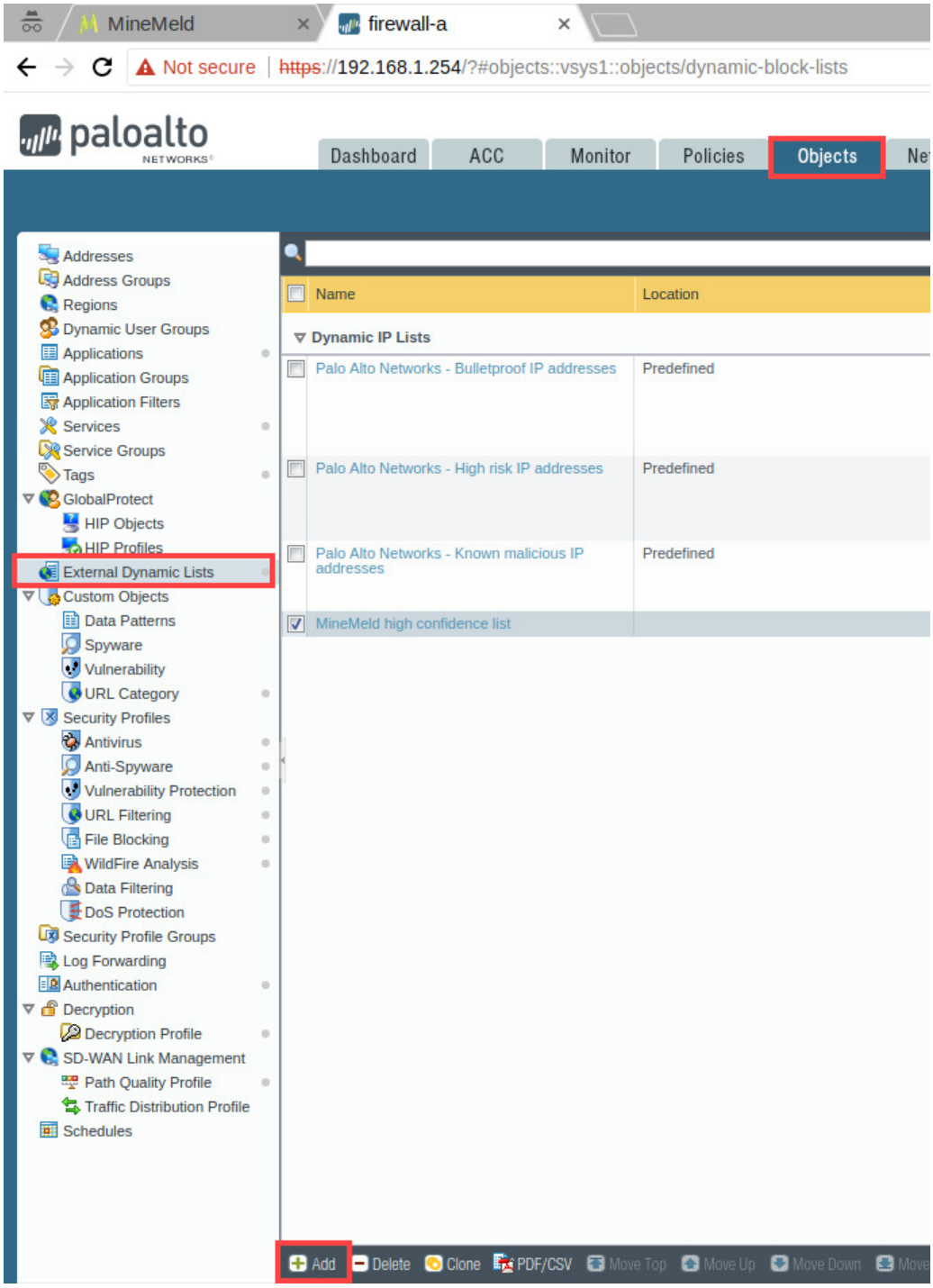
13. On the *MineMeld* webpage, click the **NODES** tab and select **sof-bad-ip-output**.



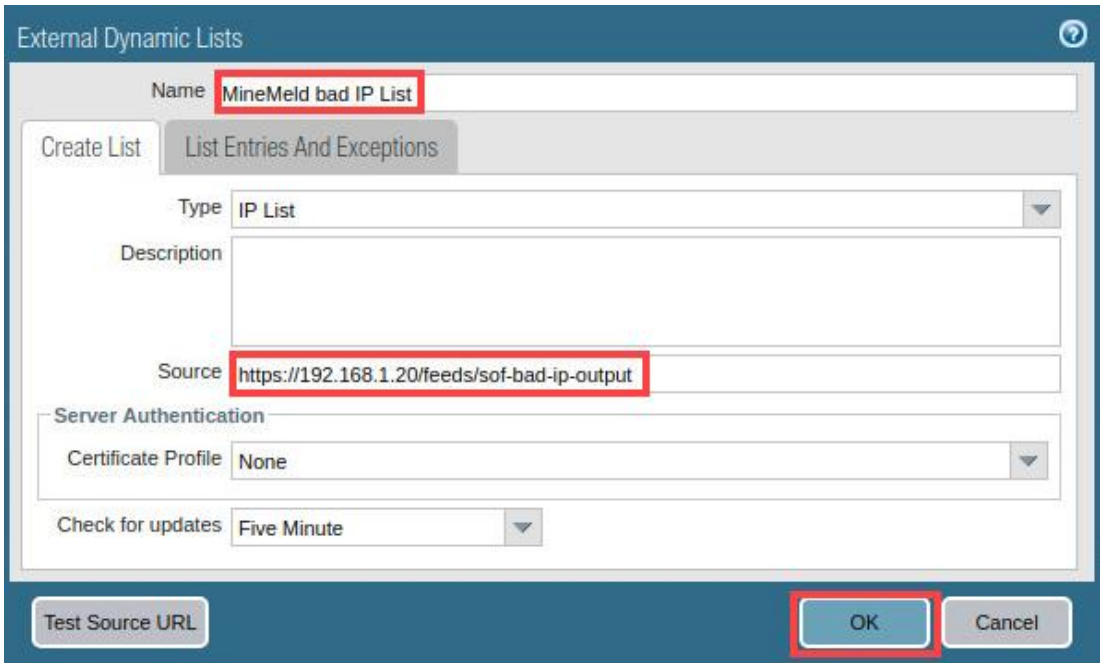
14. In the *sof-bad-ip-output* window, right-click *FEED BASE URL* and click **Copy link address**. You will use the URL to create another External Dynamic List on your Palo Alto Networks Firewall.



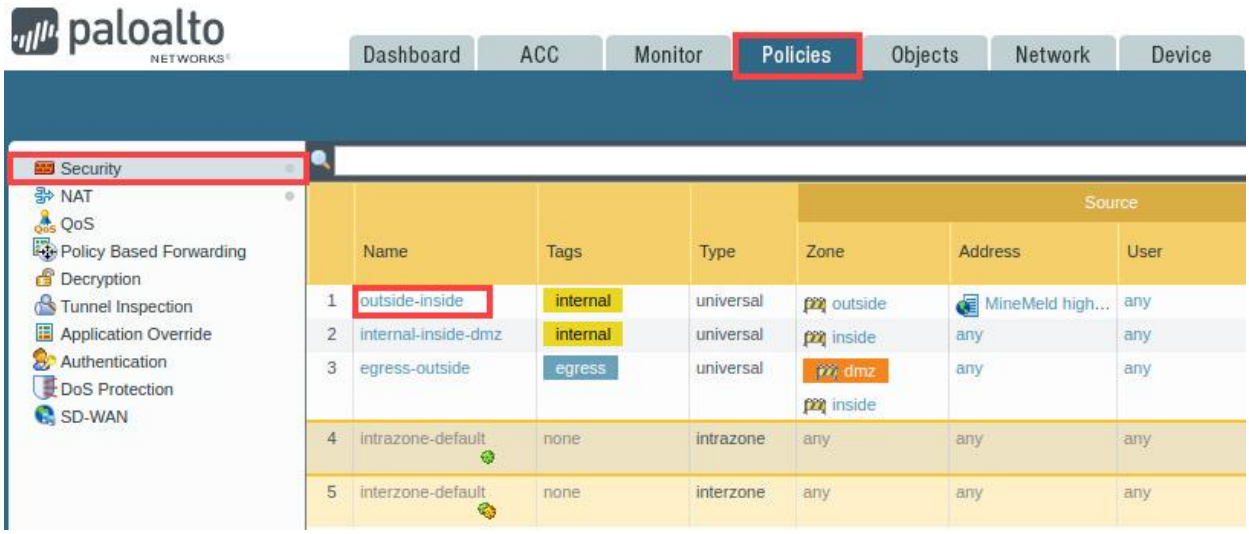
15. Change focus back to the **firewall-a** tab in the *Chromium* web browser. Navigate to **Objects > External Dynamic Lists** and click **Add**.



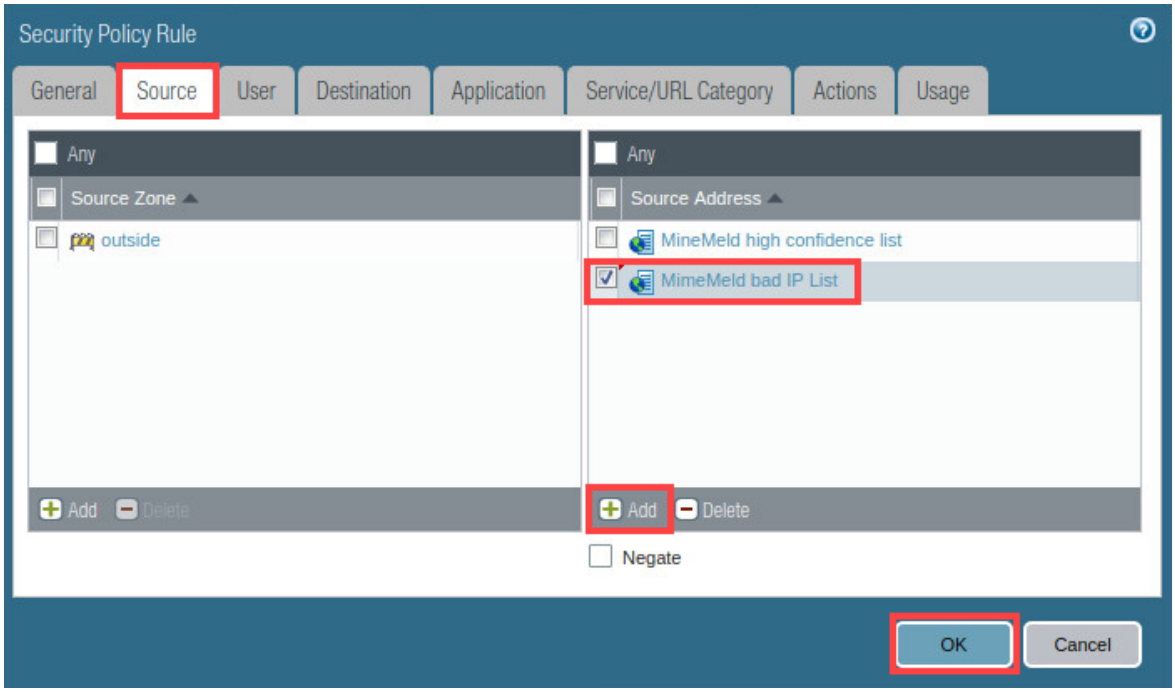
16. In the *External Dynamic Lists* dialog box, enter `MineMeld bad IP List` for the *Name*. Paste the *MineMeld output node URL* you copied from *step* **14** for the *Source*. Click **OK**.



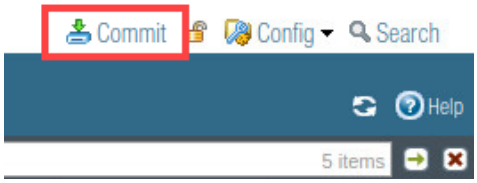
17. Navigate to **Policies > Security** and click the **outside-inside** security policy to open it.



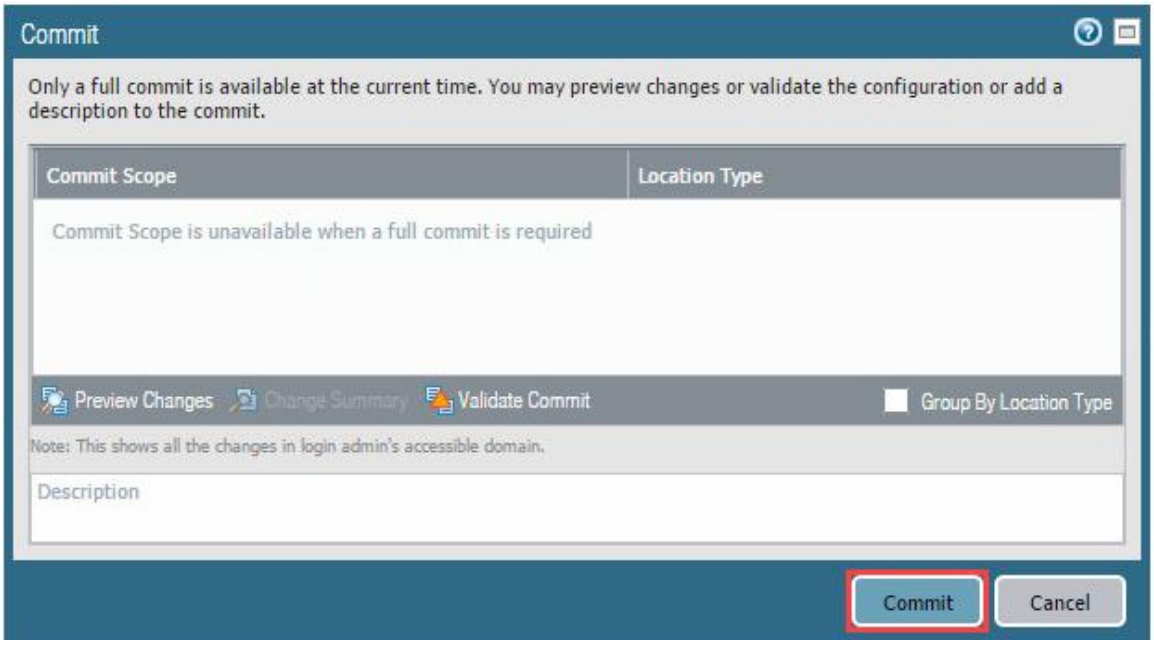
18. In the *Security Policy Rule* window, select the **Source** tab. In the *Source Address* window, click **Add** and select the **MineMeld bad IP List** EDL. Click **OK**.



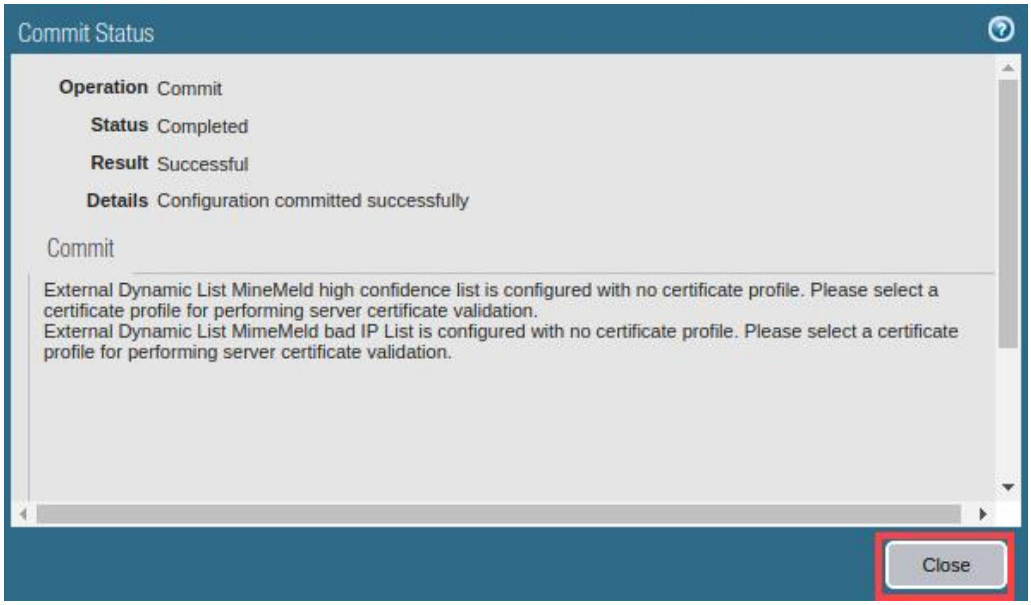
19. Click **Commit** on the Palo Alto Networks Firewall.



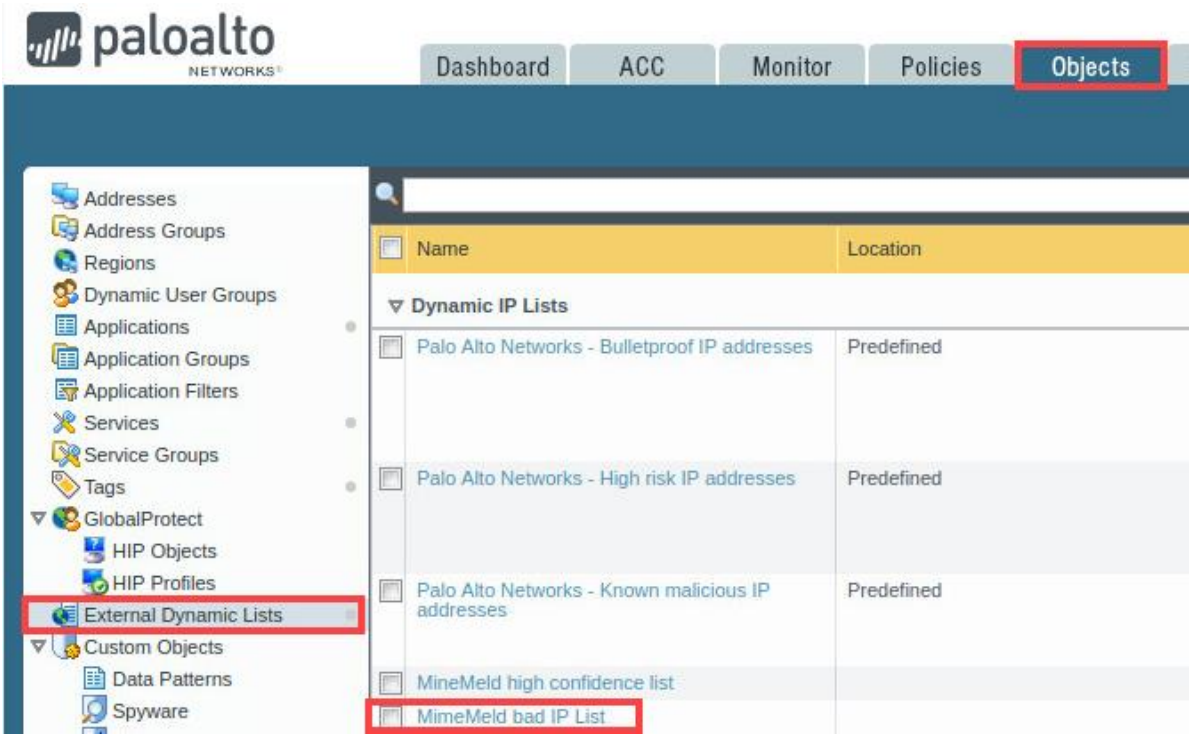
20. In the *Commit* window, click **Commit**.



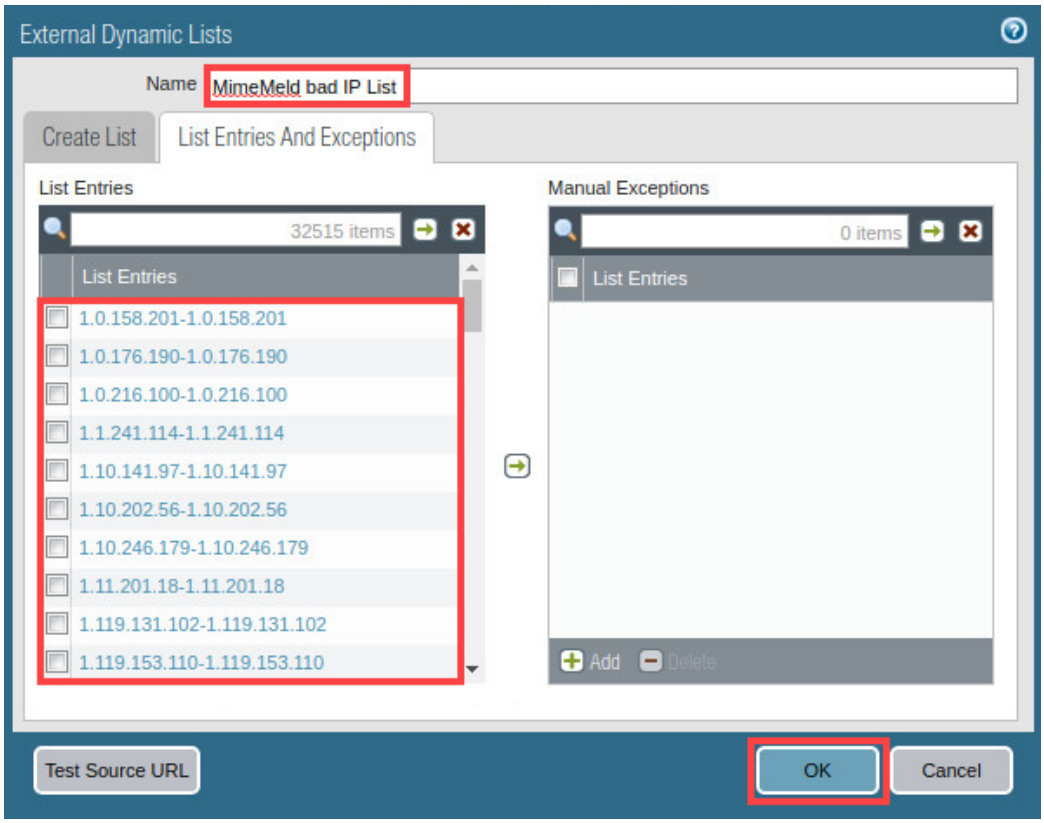
21. In the *Commit Status* window, click **Close**. You may ignore the warnings.



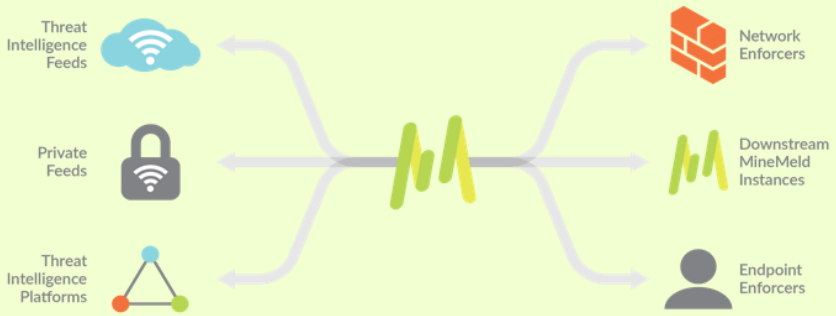
22. Navigate to **Objects > External Dynamic Lists**. Open the **MineMeld bad IP List**.



23. In the *External Dynamic Lists* window, select **List Entries And Exceptions**. View the *IP Address block list indicators* that MineMeld is now feeding the Palo Alto Networks Firewall.



MineMeld simplifies the collection and correlation of intelligence across commercial threat intelligence feeds, open-source intelligence (OSINT) providers, threat intelligence platforms, ISACs, CERTs and other *MineMeld* users.



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

