



SECURITY OPERATIONS FUNDAMENTALS

Lab 7: Threat Intelligence

Document Version: **2021-01-29**

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

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

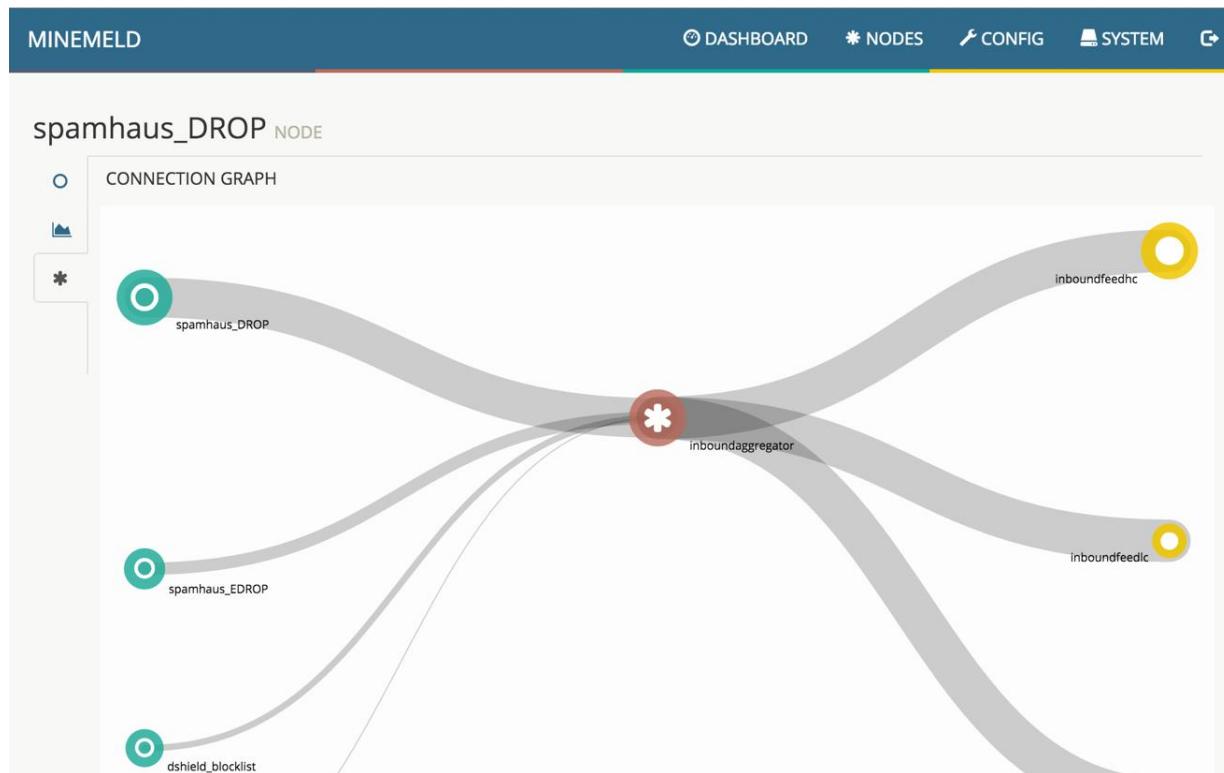
Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
7 Threat Intelligence.....	6
7.0 Load Lab Configuration.....	6
7.1 Create a Docker Volume on the Client for a MineMeld Container.....	10
7.2 Launch a MineMeld Container using Docker Compose	11
7.3 Access the MineMeld Web UI to View the Default Configurations	13
7.4 Configure an External Dynamic List (EDL) on the Firewall Appliance Using a MineMeld Output Feed.....	17
7.5 Configure Custom MineMeld Miner, Processor and Output Nodes, and Configure an EDL to use the Custom Output Node	26

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.

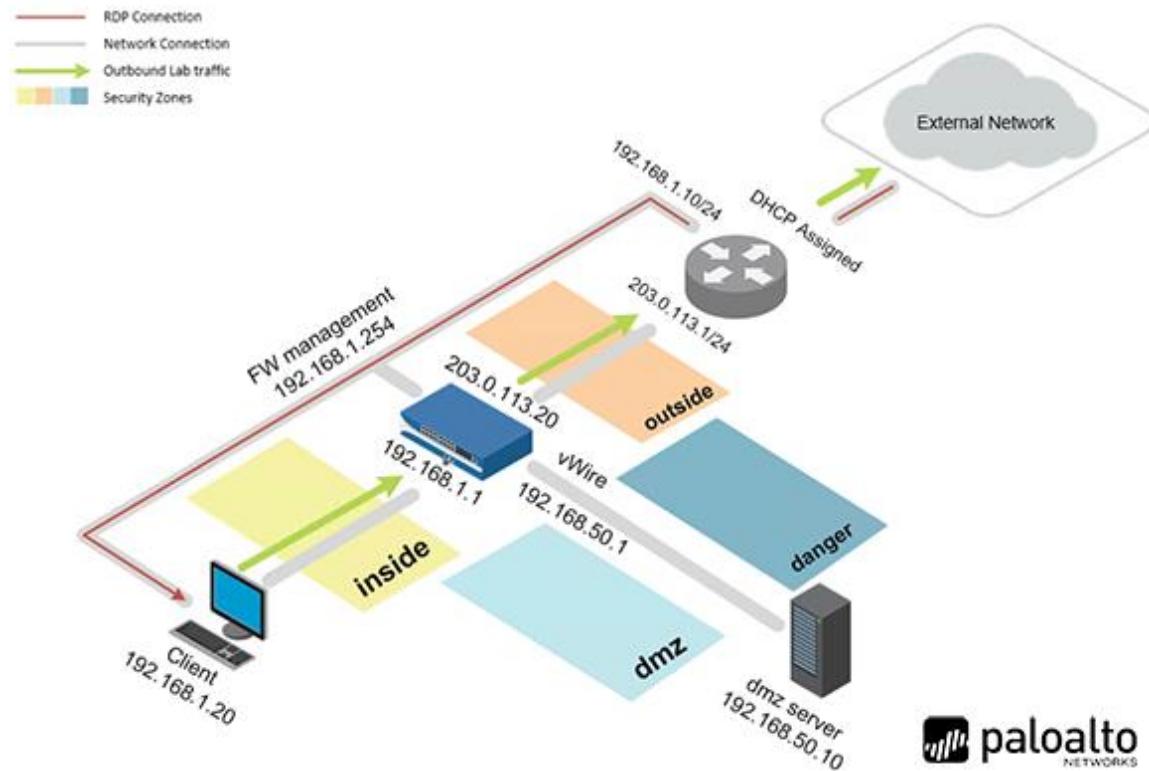


Objective

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

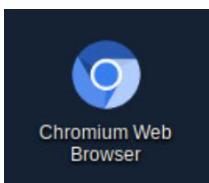
7.0 Load Lab Configuration

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

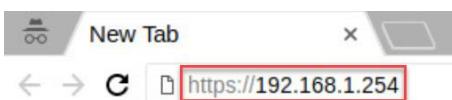
1. Click on the **Client** tab to access the client PC.



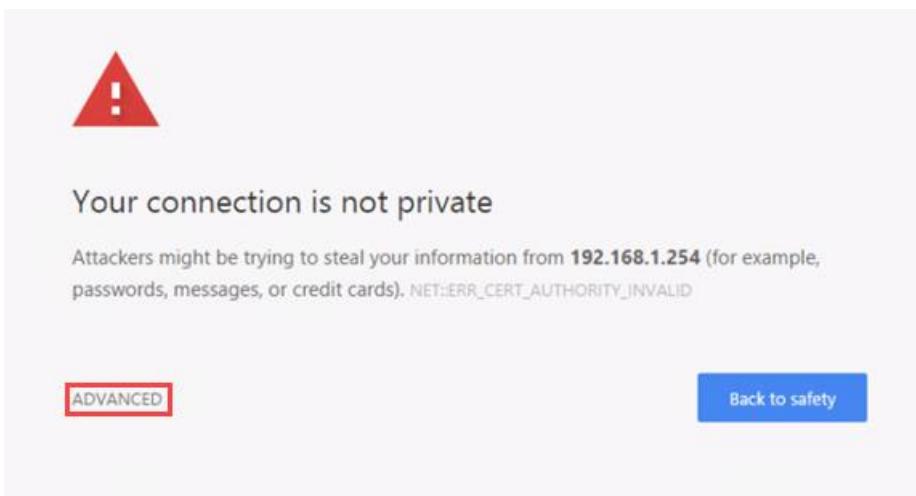
2. Log in to the client PC with the username **Lab-user** and password **Training\$**.
3. Double-click the **Chromium** icon located on the desktop.



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

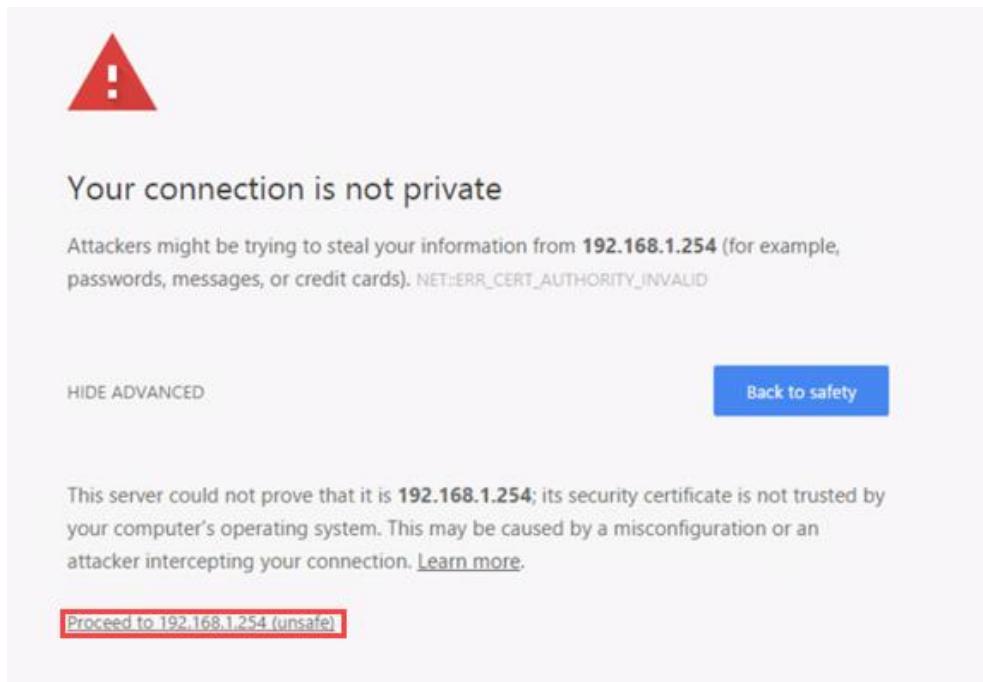


5. You will see a “*Your connection is not private*” message. Click on the **ADVANCED** link.



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)**.

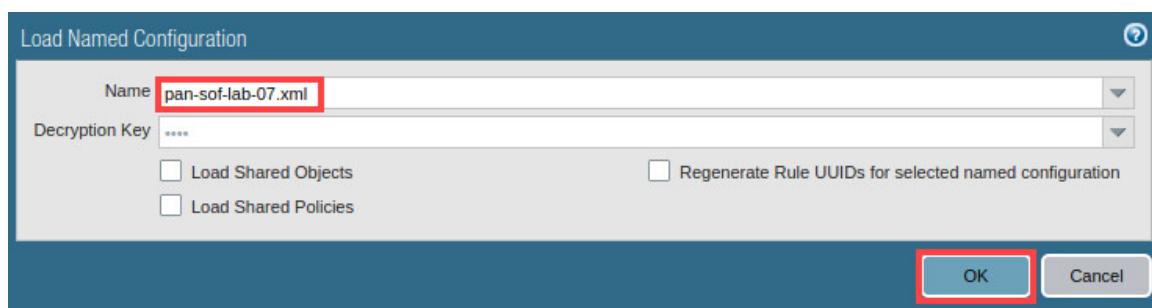


7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.

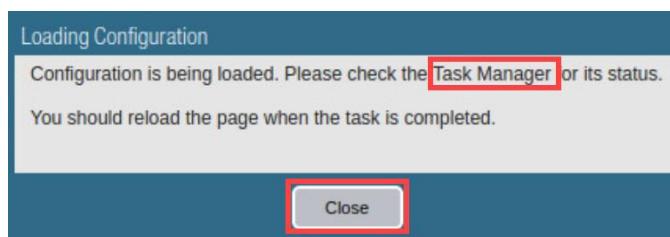


8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** in the *Configuration Management* section.

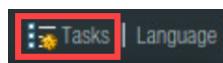
9. In the *Load Named Configuration* window, select **pan-sof-lab-07.xml** from the *Name* dropdown list and click **OK**.



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**.

Type	Status	Start Time	Messages	Action
Load	Completed	12/26/19 23:27:03		
Commit	Completed	12/26/19 23:26:17	Commit Processing By: admin Start Time (Dequeued Time): 12/26/19 23:26:17	
Load	Completed	12/26/19 23:22:39		
Auto Commit	Completed	12/26/19 23:15:09		

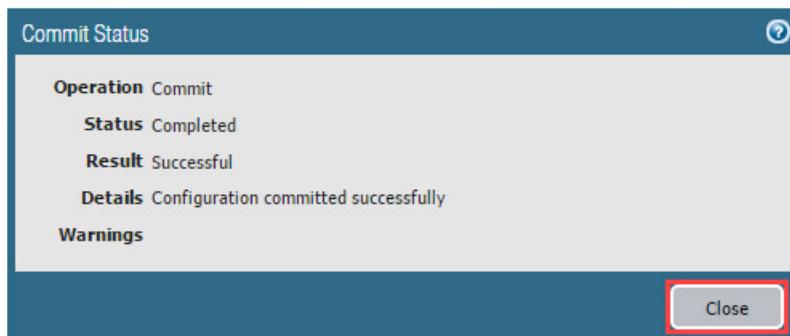
13. Click the **Commit** link located at the top-right of the web interface.



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

Commit	
Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.	
Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	
Preview Changes Change Summary Validate Commit	<input type="checkbox"/> Group By Location Type
Note: This shows all the changes in login admin's accessible domain.	
Description	
<input style="background-color: #0070C0; color: white; border: 1px solid #006699; padding: 5px; margin-right: 10px;" type="button" value="Commit"/> <input style="border: 1px solid #006699; padding: 5px;" type="button" value="Cancel"/>	

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
```

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

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

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

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

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
```

```
C:\home\lab-user> sudo ls /var/lib/docker/volumes
[sudo] password for lab-user:
1b9309e5c3e59fddd22e912dbc0341259502be07ead235e6483cc84a4ccb9786
4a8bfbf165f0829b3ee57e62395a23d7b82c5ba057f80a39ea07adc23e523d37
64c5fc596b31fc5fcf79873a4f65fafe37c348a2f75559698dc87a5b1c1afe4c
8e2f5259adc3124524e4ale9537560cbaed0deec5df4c735b9b7b7c446bce367
a8696cfe7a3f105cd64afe198b9b52859dbaf6d0ad0fe911a21f76ec72060a02
a9cc1d3876bc2a40789f724d2acf753408755eb083d016958f1b88f669850139
metadata.db
minemeld-local
minemeld-logs
C:\home\lab-user>
```

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
```

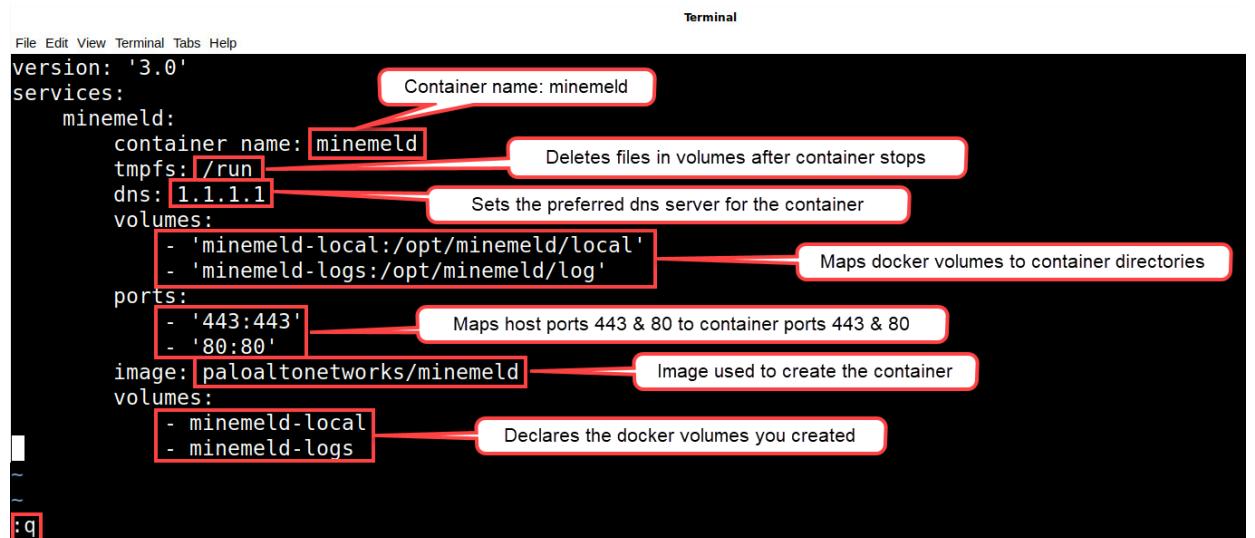
```
C:\home\lab-user> cd minemeld
C:\home\lab-user\minemeld>
```

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.



```
version: '3.0'
services:
  minemeld:
    container_name: minemeld
    tmpfs: /run
    dns: 1.1.1.1
    volumes:
      - 'minemeld-local:/opt/minemeld/local'
      - 'minemeld-logs:/opt/minemeld/log'
    ports:
      - '443:443'
      - '80:80'
    image: paloaltonetworks/minemeld
    volumes:
      - minemeld-local
      - minemeld-logs
```

The terminal window shows the **File Edit View Terminal Tabs Help** menu bar at the top. The **Terminal** tab is selected. The command **:q** is visible at the bottom left. The configuration file is displayed with several annotations:

- Container name: minemeld**
- Deletes files in volumes after container stops**
- Sets the preferred dns server for the container**
- Maps docker volumes to container directories**
- Maps host ports 443 & 80 to container ports 443 & 80**
- Image used to create the container**
- Declares the docker volumes you created**

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 **Training\$** and press **Enter**.

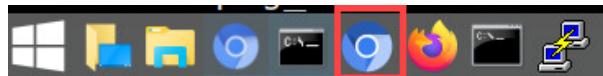
```
[root@pod-dmz ~]# sudo docker logs minemeld
```

```
C:\home\lab-user\minemeld> sudo docker logs minemeld
[sudo] password for lab-user: [REDACTED]
*** 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...
Regenerating CA bundle
2021-01-04T04:23:48 (34)cacert_merge.main INFO: config: {'cafile': ['/opt/minemeld/local/certs/site/'], 'dst': '/opt/minemeld/local/certs/bundle.crt', 'config': '/opt/minemeld/local/certs/cacert-merge-config.yml', 'no_merge_certificate': False}
0
Starting minemeld...
/opt/minemeld/engine/0.9.70.post1/local/lib/python2.7/site-packages/supervisor/options.py:383: PkgResourcesDeprecationWarning: 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.

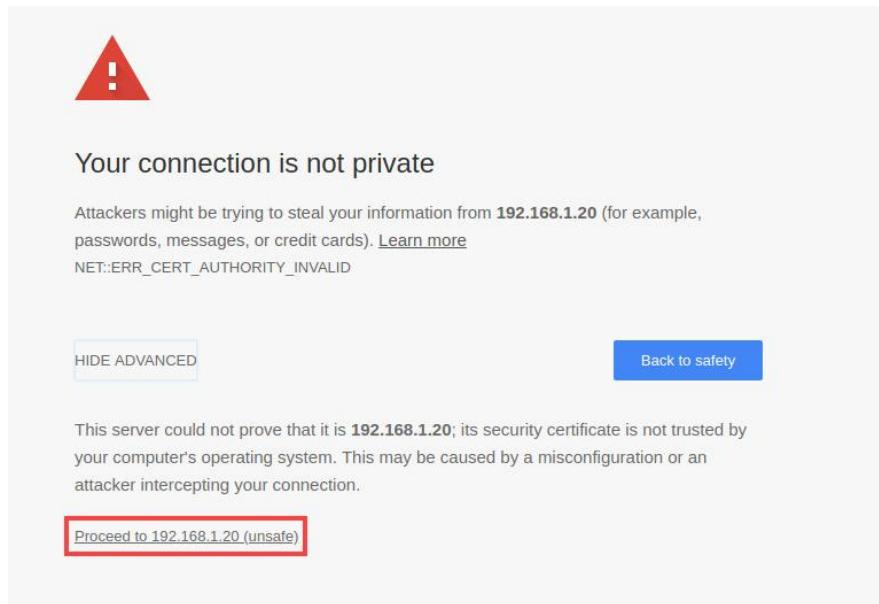
7.3 Access the MineMeld Web UI to View the Default Configurations

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**.



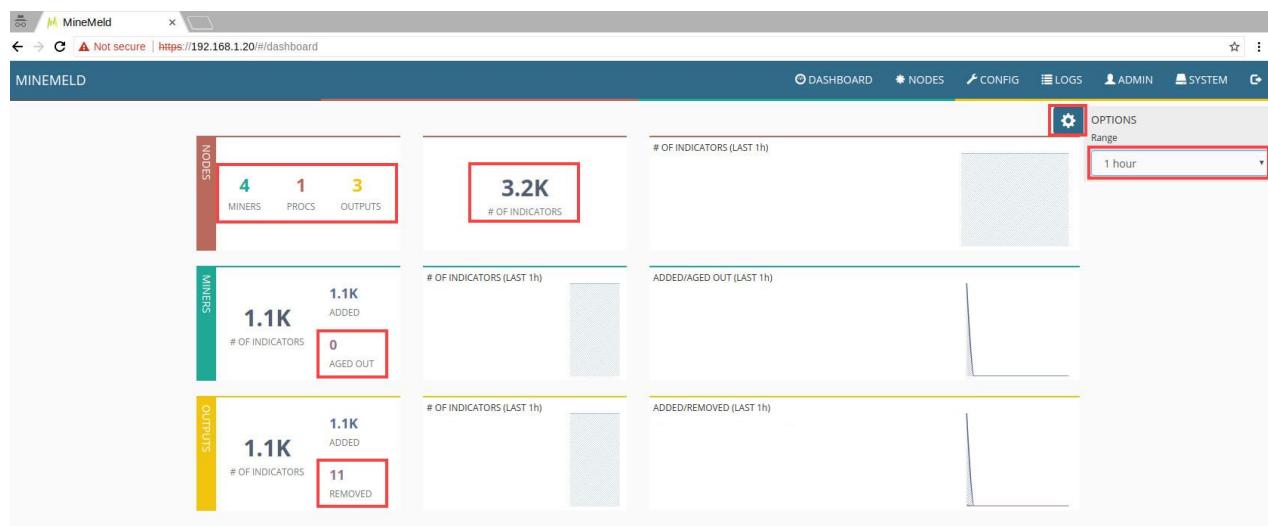
2. In the *Your connection is not private* window, advance through the security warning and click **Proceed to 192.168.1.20 (unsafe)**.



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.

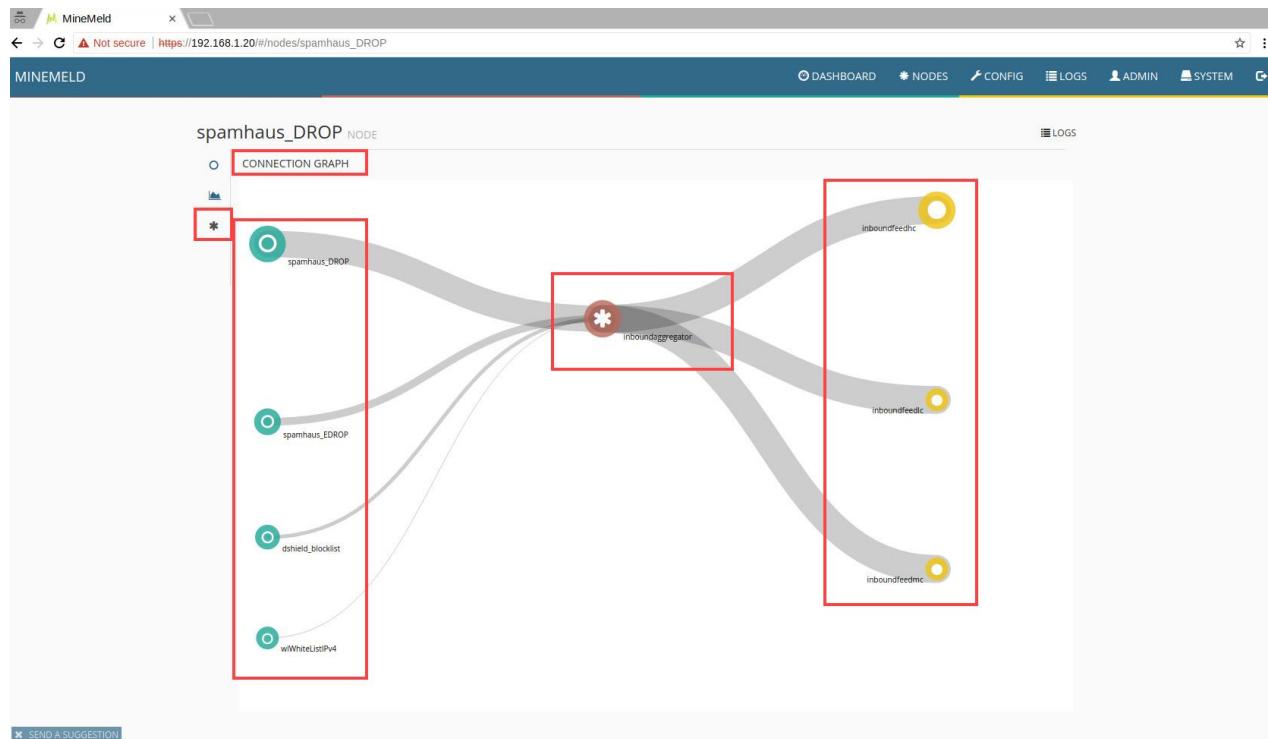
5. In the *MineMeld UI*, navigate to the *Nodes* webpage by clicking on the **NODES** link.



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

NAME	TYPE	STATE	INDICATORS	ADD/REM/AO	UPDATES	WITHDRAWS
dshield_blocklist	MINER	STARTED	20	ADDED: 20 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 20	RX: 0 PROCESSED: 0 TX: 0
spamhaus_DROP	MINER	STARTED	971	ADDED: 971 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 971	RX: 0 PROCESSED: 0 TX: 0
spamhaus_EDROP	MINER	STARTED	82	ADDED: 82 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 82	RX: 0 PROCESSED: 0 TX: 0

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).

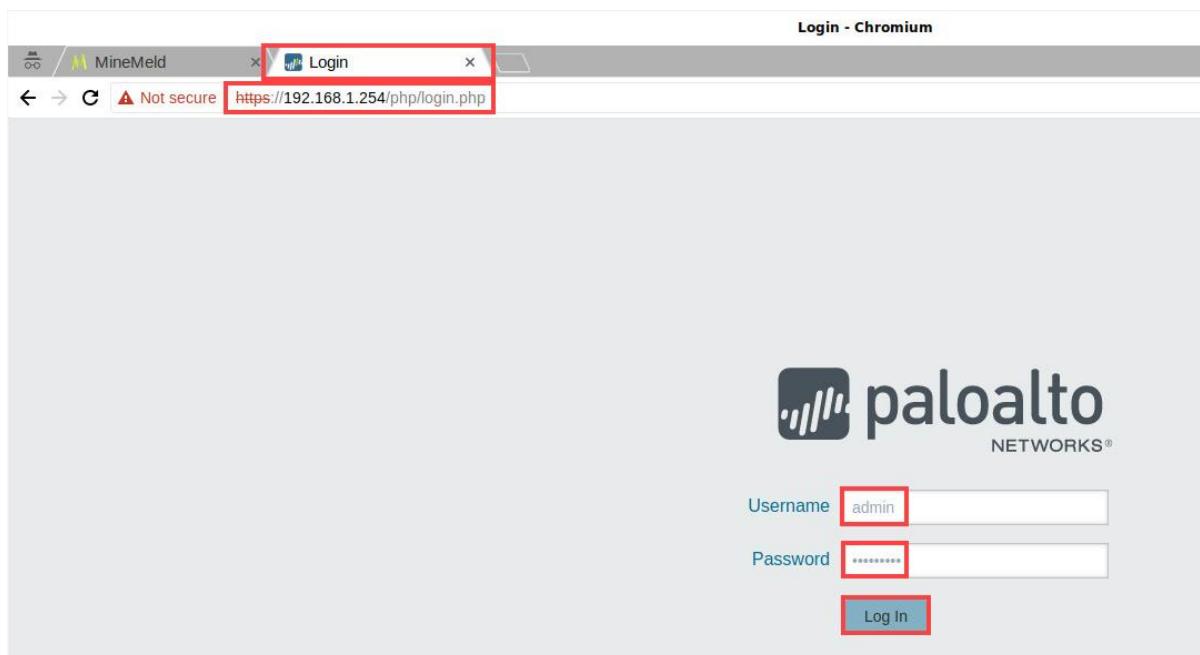


8. Leave the *Chromium* web browser open and continue to the next task.

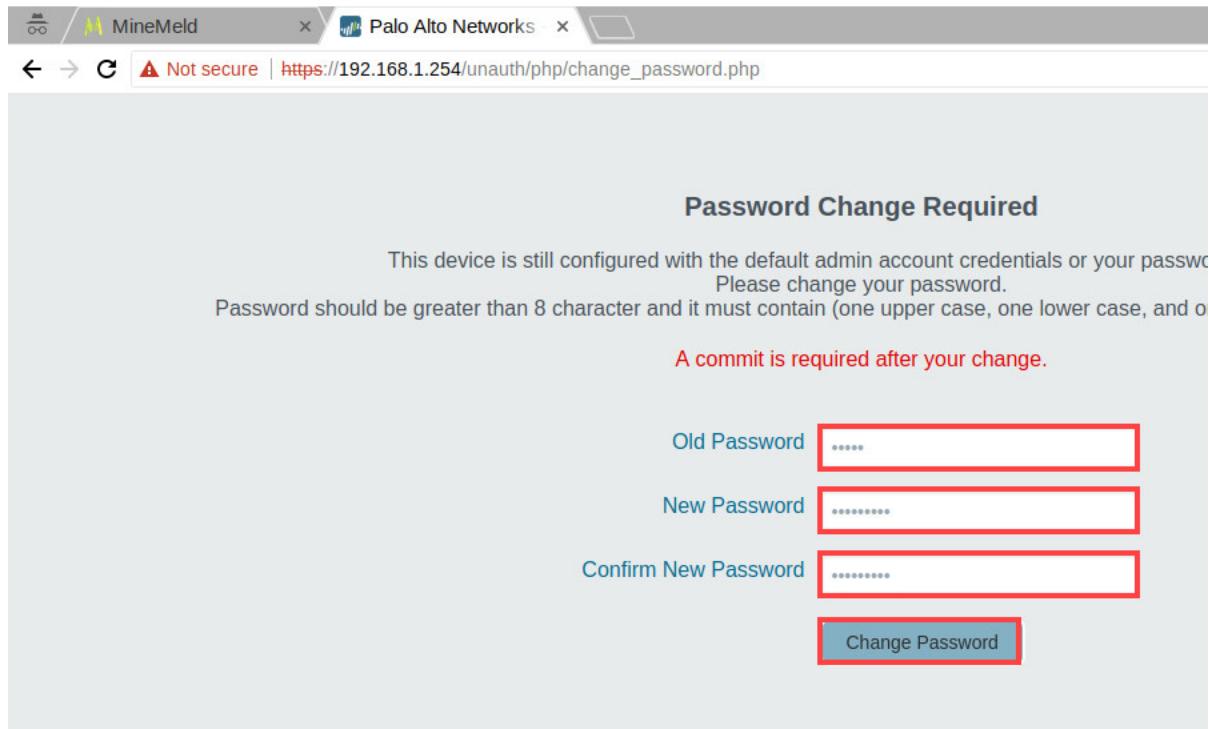
7.4 Configure an External Dynamic List (EDL) on the Firewall Appliance Using a MineMeld Output Feed

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**.

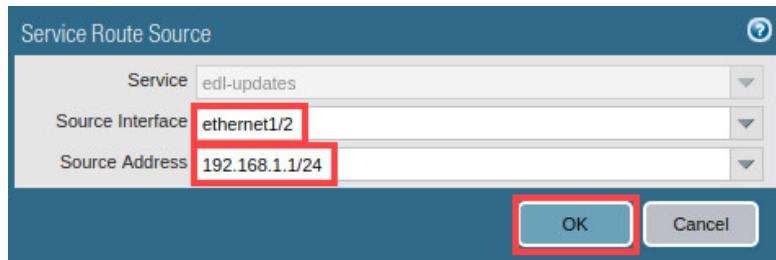
The screenshot shows the Palo Alto Networks Device setup interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The Device tab is highlighted with a red box. On the left, a sidebar under the Setup heading lists various configuration options like High Availability, Config Audit, and Certificate Management. The main content area is titled 'Services' and contains settings for Update Server, Verify Update Server Identity, DNS Servers, Primary DNS Server, Secondary DNS Server, Minimum FQDN Refresh Time, FQDN Stale Entry Timeout, Proxy Server, Primary NTP Server Address, Primary NTP Server Authentication Type, and Secondary NTP Server Address. At the bottom of the Services section, there is a 'Service Features' section with a link labeled 'Service Route Configuration'.

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

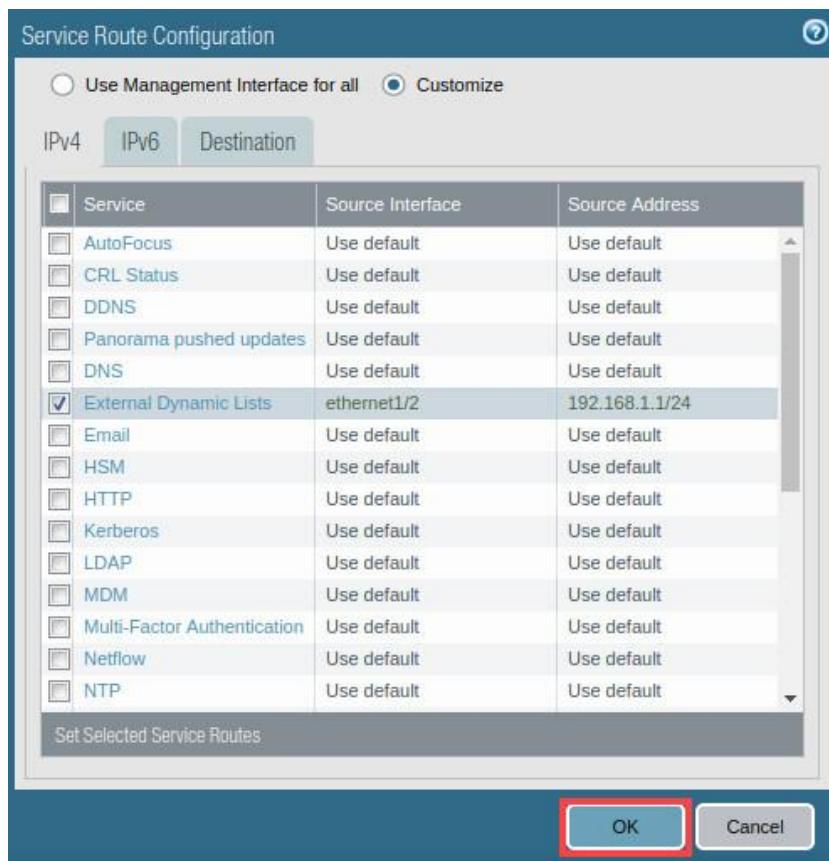
The screenshot shows the 'Service Route Configuration' dialog box. At the top, there are two radio buttons: 'Use Management Interface for all' and 'Customize', with 'Customize' selected and highlighted with a red box. Below this are tabs for 'IPv4', 'IPv6', and 'Destination'. The main area is a table with columns 'Service', 'Source Interface', and 'Source Address'. A row for 'External Dynamic Lists' is highlighted with a red box and has a checked checkbox in the 'Service' column. Other rows in the table include AutoFocus, CRL Status, DDNS, Panorama pushed updates, DNS, Email, HSM, and HTTPS.

Service	Source Interface	Source Address
AutoFocus	Use default	Use default
CRL Status	Use default	Use default
DDNS	Use default	Use default
Panorama pushed updates	Use default	Use default
DNS	Use default	Use default
External Dynamic Lists	Use default	Use default
Email	Use default	Use default
HSM	Use default	Use default
HTTPS	Use default	Use default

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**.



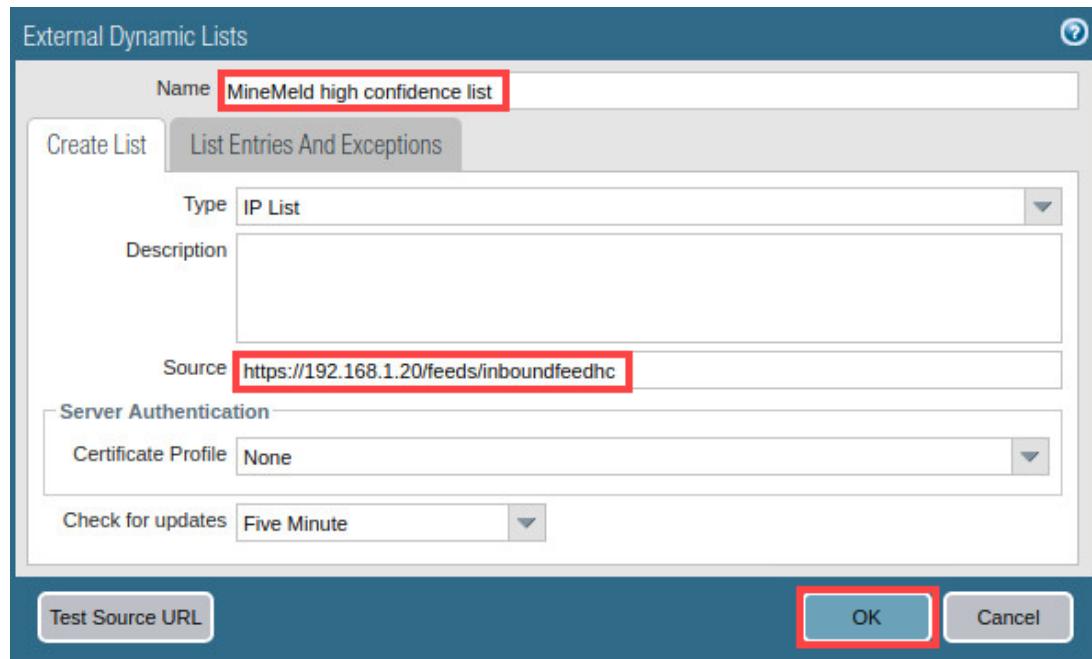
7. In the *Service Route Configuration* window, click **OK**.



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

Name	Location	Description
Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by hosting providers. Because providers place few, if any, restrictions on content, attackers can use them to host and distribute malicious or unethical material.
Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have received threat activity advisories from trust organizations. However, Palo Alto Networks does not have definitive maliciousness for these IP addresses.
Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used exclusively by malicious actors for distribution, command-and-control, launching various attacks.

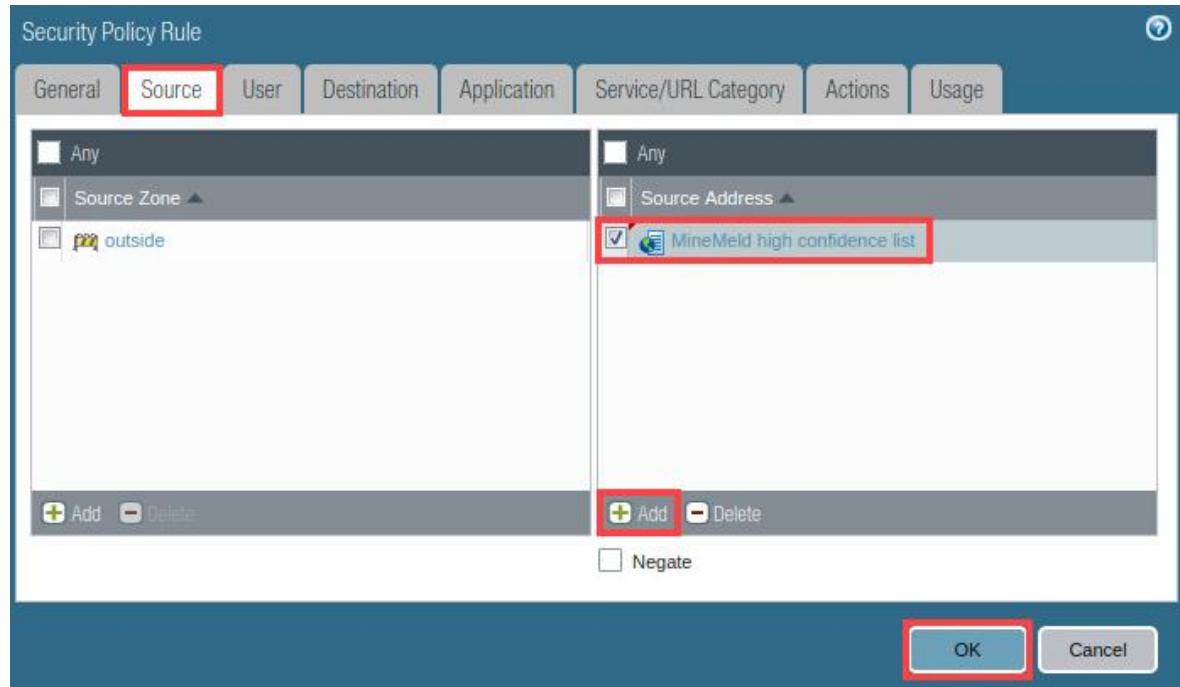
9. In the *External Dynamic Lists* window, type **MineMeld high confidence list** in the *Name* field, and enter <https://192.168.1.20/feeds/inboundfeedhc> for the *Source*. Click **OK**.



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

	Name	Tags	Type	Zone	Add
1	outside-inside	internal	universal	outside	any
2	internal-inside-dmz	internal	universal	inside	any
3	egress-outside	egress	universal	dmz	any
4	intrazone-default	none	intrazone	any	any
5	interzone-default	none	interzone	any	any

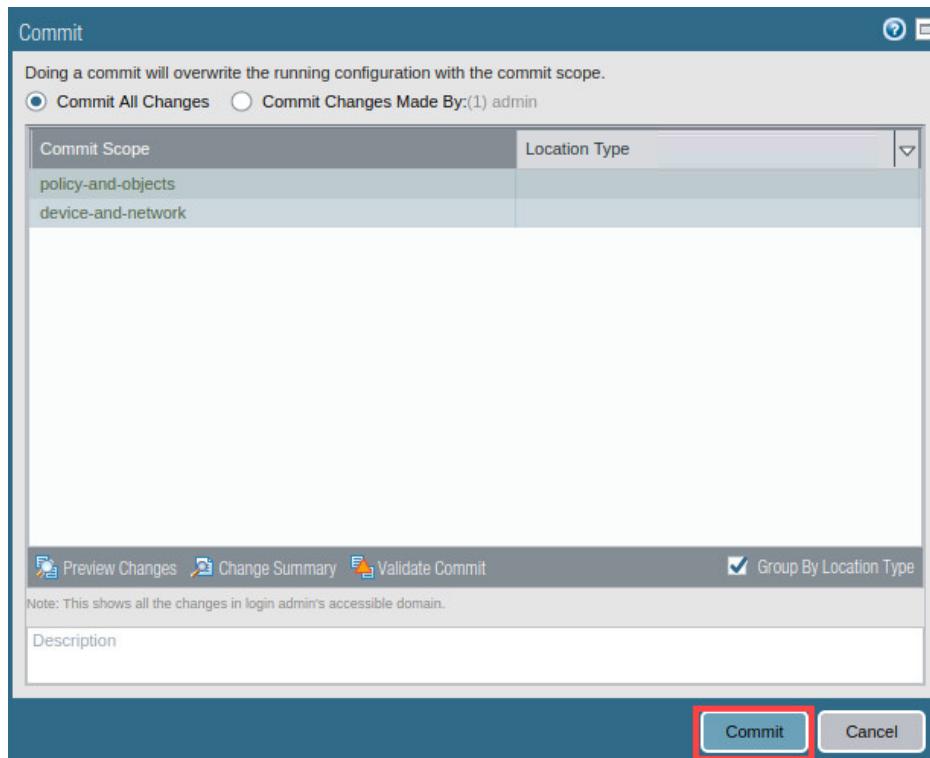
11. In the *Security Policy Rule* window, select the **Source** tab. In the *Source Address* box, click **Add**. Select the **MineMeld high confidence list** from the dropdown menu. Click **OK** to close the *Security Policy Rule* window.



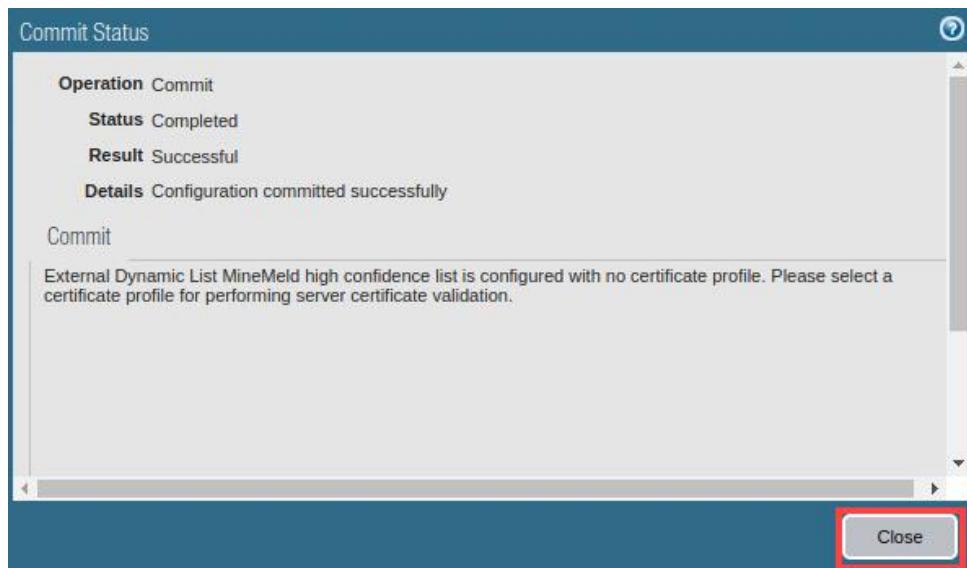
12. Click the **Commit** link located at the top-right of the web interface.



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**.

The screenshot shows the Palo Alto Networks interface. The top navigation bar has tabs: Dashboard, ACC, Monitor, Policies, **Objects**, Network, and Device. The 'Objects' tab is selected. On the left, a sidebar lists various object types: Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, GlobalProtect (with HIP Objects and HIP Profiles), External Dynamic Lists, Custom Objects, Data Patterns, and others. The 'External Dynamic Lists' item is highlighted with a red box. The main pane displays a table titled 'Dynamic IP Lists'. The table has columns: Name, Location, and Description. It lists three predefined entries: 'Palo Alto Networks - Bulletproof IP addresses', 'Palo Alto Networks - High risk IP addresses', and 'Palo Alto Networks - Known malicious IP addresses'. Below these, a new entry 'MineMeld high confidence list' is listed, also with a red box around it.

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**.

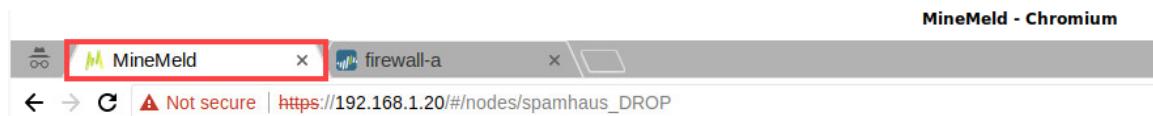
The screenshot shows the 'External Dynamic Lists' dialog box. At the top, there's a 'Name' field containing 'MineMeld high confidence list'. Below it are two tabs: 'Create List' and 'List Entries And Exceptions', with 'List Entries And Exceptions' being the active tab and highlighted with a red box. The main area is divided into two sections: 'List Entries' and 'Manual Exceptions'. The 'List Entries' section contains a list of IP ranges, such as '141.98.80.0-141.98.80.255', '167.248.133.0-167.248.133.255', etc., with many entries highlighted in red. The 'Manual Exceptions' section is empty, showing a list box with '0 items'. At the bottom, there are 'Test Source URL', 'OK' (highlighted with a red box), and 'Cancel' buttons.

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 **MineMeld** 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.

A screenshot of the MineMeld Web UI. The top navigation bar has tabs for DASHBOARD, NODES, CONFIG (selected), and LOGS. Below the navigation is a search bar and a "COMMIT" button. The main area displays a table of nodes:

NAME	TYPE	PROTOTYPE	INPUTS	OUTPUT
dshield_blocklist	MINER	dshield.block	None	ENABLED
spamhaus_DROP	MINER	spamhaus.DROP	None	ENABLED
spamhaus_EDROP	MINER	spamhaus.EDROP	None	ENABLED
wlWhiteListIPv4	MINER	stdlib.lstIPv4Generic	None	ENABLED
inboundfeeddh	OUTPUT	stdlib.feedHCGreen	inboundaggregator	DISABLED
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	DISABLED
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	DISABLED
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wlWhiteListIPv4	ENABLED

At the bottom right of the table, there is a red box around a small eye icon and a red box around a plus sign icon.

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**.

A screenshot of the "ADD NODE" configuration form. It has fields for NAME, PROTOTYPE, INPUTS, and buttons for OK and CANCEL. The NAME field contains "bad-ip-miner" and the PROTOTYPE field contains "blocklist_de.all", both highlighted with red boxes. The OK button is highlighted with a red box.

NAME	bad-ip-miner
PROTOTYPE	blocklist_de.all
INPUTS	Select input nodes...
<input type="button" value="OK"/> <input type="button" value="CANCEL"/>	

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.

NAME	TYPE	PROTOTYPE	INPUTS	OUTPUT
bad-ip-miner	MINER	blocklist_de.all	None	ENABLED
dshield_blocklist	MINER	dshield.block	None	ENABLED
spamhaus_DROP	MINER	spamhaus.DROP	None	ENABLED
spamhaus_EDROP	MINER	spamhaus.EDROP	None	ENABLED
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic	None	ENABLED
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	DISABLED
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	DISABLED
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	DISABLED
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wlWhiteListIPv4	ENABLED

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**.

ADD NODE

NAME	bad-ip-processor
PROTOTYPE	stdlib.aggregatorIPv4Generic
INPUTS	bad-ip-miner

OK **CANCEL**

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.

NAME	TYPE	PROTOTYPE	INPUTS	OUTPUT
bad-ip-miner	MINER	blocklist_de.all	None	ENABLED
dshield_blocklist	MINER	dshield.block	None	ENABLED
spamhaus_DROP	MINER	spamhaus.DROP	None	ENABLED
spamhaus_EDROP	MINER	spamhaus.EDROP	None	ENABLED
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic	None	ENABLED
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	DISABLED
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	DISABLED
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	DISABLED
bad-ip-processor	PROCESSOR	stdlib.aggregatorIPv4Generic	bad-ip-miner	ENABLED
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wlWhiteListIPv4	ENABLED

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**.

ADD NODE

NAME	<input type="text" value="sof-bad-ip-output"/>
PROTOTYPE	<input type="text" value="stdlib.feedMCGreenWithValue"/>
INPUTS	<input type="text" value="bad-ip-processor"/>
	<input type="button" value="OK"/> <input type="button" value="CANCEL"/>

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.

NAME	TYPE	PROTOTYPE
bad-ip-miner	MINER	blocklist_de.all
dshield_blocklist	MINER	dshield.block
spamhaus_DROP	MINER	spamhaus.DROP
spamhaus_EDROP	MINER	spamhaus.EDROP
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic
inboundfeedhc	OUTPUT	stdlib.feedHCGreen
inboundfeedlc	OUTPUT	stdlib.feedLCGreen
inboundfeedmc	OUTPUT	stdlib.feedMCGreen
sof-bad-ip-output	OUTPUT	stdlib.feedMCGreenWithValue
bad-ip-processor	PROCESSOR	stdlib.aggregatorIPv4Generic
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound

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

NAME	TYPE	PROTOTYPE	INPUTS	OUTPUT
bad-ip-miner	MINER	blocklist_de.all	None	ENABLED
dshield_blocklist	MINER	dshield.block	None	ENABLED
spamhaus_DROP	MINER	spamhaus.DROP	None	ENABLED
spamhaus_EDROP	MINER	spamhaus.EDROP	None	ENABLED
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic	None	ENABLED
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	DISABLED
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	DISABLED
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	DISABLED
sof-bad-ip-output	OUTPUT	stdlib.feedMCGreenWithValue	bad-ip-processor	DISABLED
bad-ip-processor	PROCESSOR	stdlib.aggregatorIPv4Generic	bad-ip-miner	ENABLED
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wlWhiteListIPv4	ENABLED

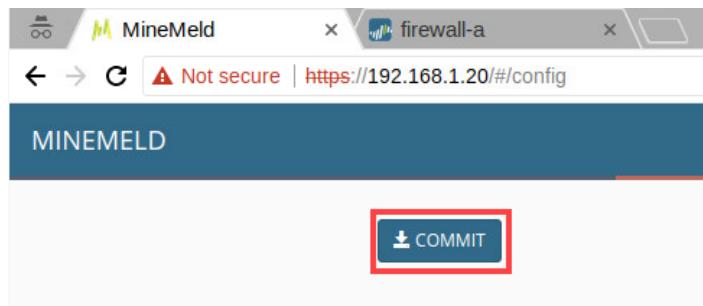
10. In the *sof-bad-ip-output* window dialog box, click **DISABLED**.



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**.

NAME	TYPE	STATE	INDICATORS	ADD/REM/AO	UPDATES	WITHDRAWS
bad-ip-miner	MINER	STARTED	32588	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
dshield_blocklist	MINER	STARTED	20	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
spamhaus_DROP	MINER	STARTED	971	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
spamhaus_EDROP	MINER	STARTED	82	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
wlWhiteListIPv4	MINER	STARTED	0	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
inboundfeedhc	OUTPUT	STARTED	1078	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
inboundfeedlc	OUTPUT	STARTED	0	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
inboundfeedmc	OUTPUT	STARTED	0	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
sof-bad-ip-output	OUTPUT	STARTED	32515	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0

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.

sof-bad-ip-output NODE	
	STATUS
	CLASS: minemeld.ft.redis.RedisSet
	PROTOTYPE: stdlib.feedMCGreenWithValue
	STATE: STARTED
	TAGS
# INDICATORS	32515
FEED BASE URL	https://192.168.1.20/feeds/sof-bad-ip-output

[Open link in new tab](#)
[Open link in new window](#)
[Open link in incognito window](#)

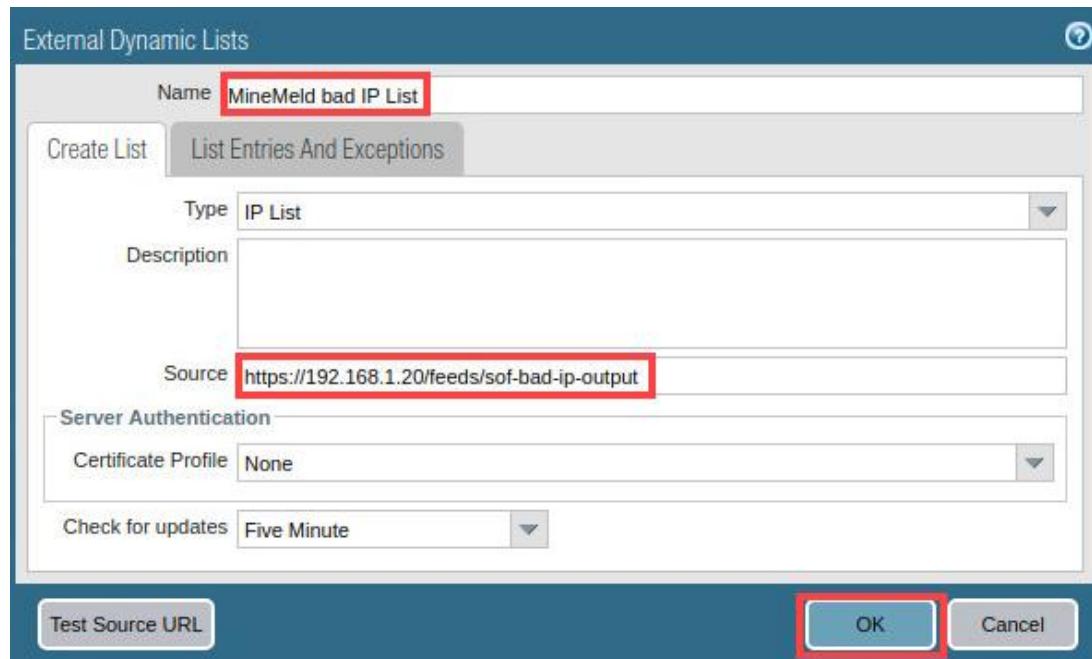
[Save link as...](#)
[Copy link address](#)

Inspect
Ctrl+Shift+I

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

The screenshot shows the Palo Alto Networks UI in a web browser. The title bar indicates the browser is 'Not secure' and the URL is <https://192.168.1.254/#objects::vsys1::objects/dynamic-block-lists>. The navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, and Objects, with the Objects tab highlighted by a red box. The left sidebar contains a tree view of objects: Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, GlobalProtect (with HIP Objects and HIP Profiles), External Dynamic Lists (which is also highlighted by a red box), Custom Objects (with Data Patterns, Spyware, Vulnerability, and URL Category), Security Profiles (with Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, WildFire Analysis, Data Filtering, and DoS Protection), Security Profile Groups, Log Forwarding, Authentication, Decryption (with Decryption Profile), SD-WAN Link Management (with Path Quality Profile and Traffic Distribution Profile), and Schedules. The main content area displays a table titled 'Dynamic IP Lists' with three entries: 'Palo Alto Networks - Bulletproof IP addresses' (Predefined), 'Palo Alto Networks - High risk IP addresses' (Predefined), and 'Palo Alto Networks - Known malicious IP addresses'. Below this table, a list item 'MineMeld high confidence list' is selected, indicated by a checked checkbox. At the bottom of the main content area, there is a toolbar with icons for Add, Delete, Clone, PDF/CSV, Move Top, Move Up, Move Down, and Move.

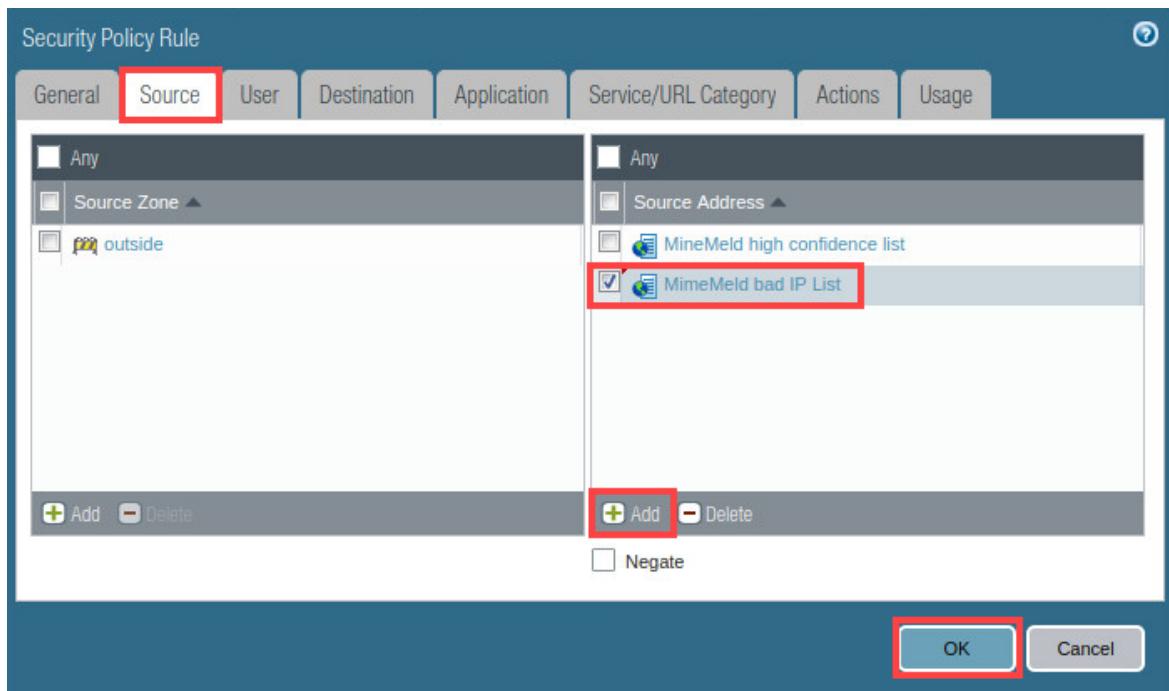
16. In the *External Dynamic Lists* dialog box, enter **MineMeld bad IP List** for the **Name**. Paste the *MineMeld output node URL* you copied from step 14 for the **Source**. Click **OK**.



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

Name	Tags	Type	Source		
			Zone	Address	User
1 outside-inside	internal	universal	outside	MineMeld high...	any
2 internal-inside-dmz	internal	universal	inside	any	any
3 egress-outside	egress	universal	dmz	any	any
4 intrazone-default	none	intrazone	any	any	any
5 interzone-default	none	interzone	any	any	any

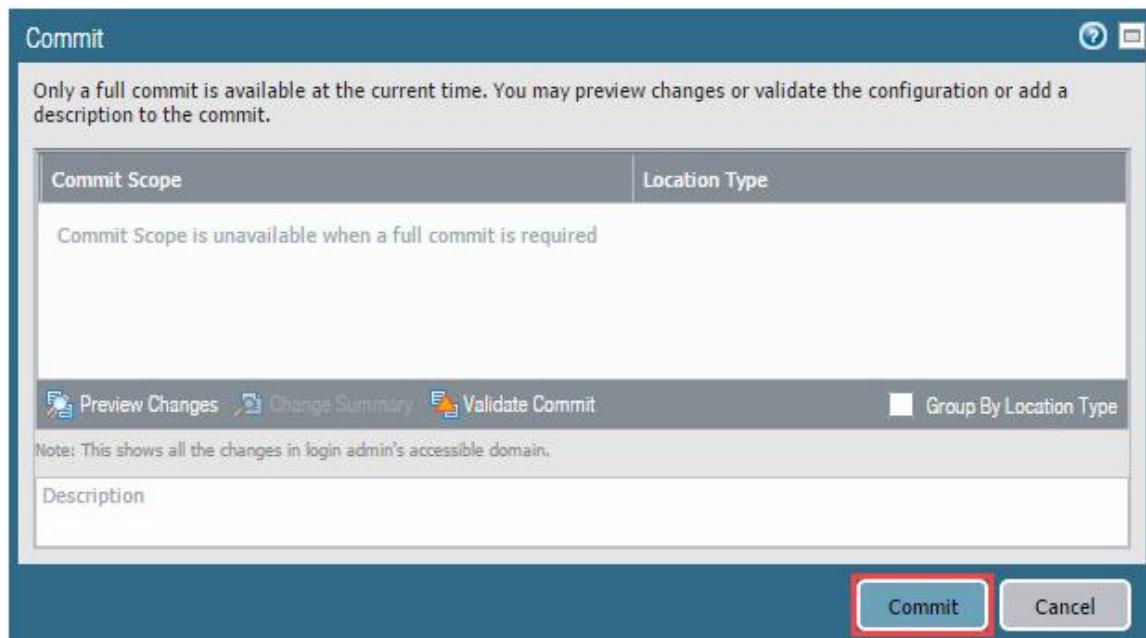
18. In the *Security Policy Rule* window, select the **Source** tab. In the *Source Address* window, click **Add** and select the **MineMeld bad IP List** EDL. Click **OK**.



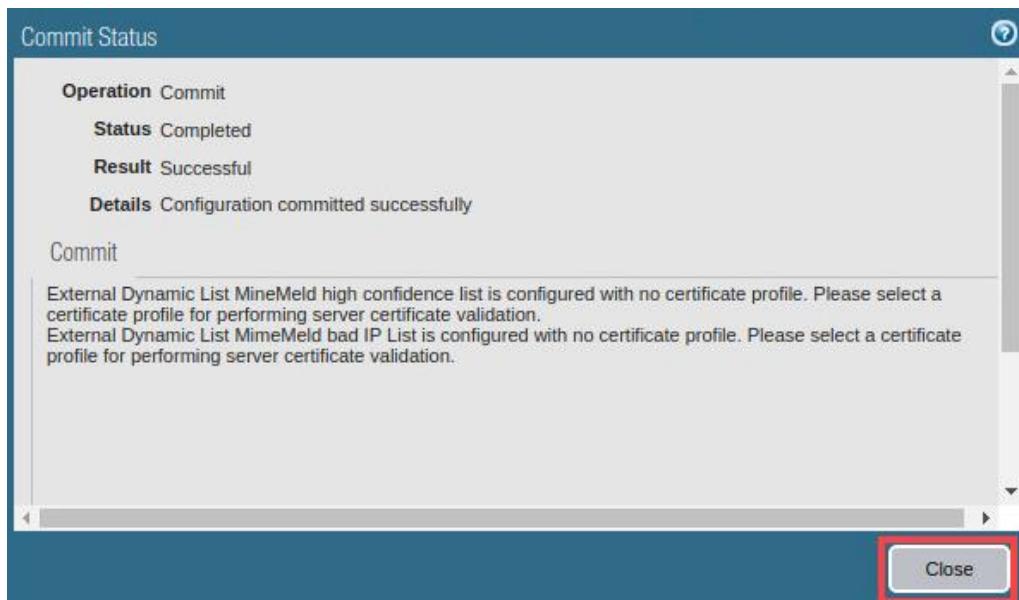
19. Click **Commit** on the Palo Alto Networks Firewall.



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**.

The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', and 'Objects'. The 'Objects' tab is selected and highlighted with a red box. On the left, a sidebar lists various object types: Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, GlobalProtect (with HIP Objects and HIP Profiles), External Dynamic Lists (which is also highlighted with a red box), Custom Objects, Data Patterns, and Spyware. The main pane displays a table titled 'Dynamic IP Lists' with the following entries:

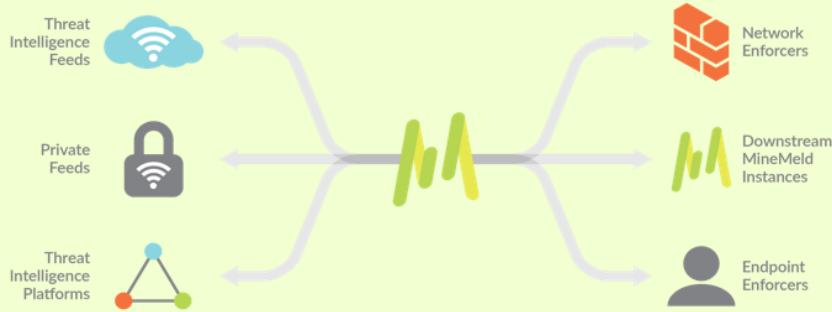
Name	Location
Palo Alto Networks - Bulletproof IP addresses	Predefined
Palo Alto Networks - High risk IP addresses	Predefined
Palo Alto Networks - Known malicious IP addresses	Predefined
MineMeld high confidence list	
MineMeld bad IP List	

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.

The screenshot shows the 'External Dynamic Lists' configuration window. The title bar says 'External Dynamic Lists'. The 'Name' field is set to 'MineMeld bad IP List'. Below the title bar are two tabs: 'Create List' and 'List Entries And Exceptions'. The 'List Entries And Exceptions' tab is selected. The main area has two sections: 'List Entries' and 'Manual Exceptions'. The 'List Entries' section contains a list of IP address ranges, such as '1.0.158.201-1.0.158.201', '1.0.176.190-1.0.176.190', etc., with a total count of 32515 items. Many of these entries are highlighted with red boxes. The 'Manual Exceptions' section is empty, showing '0 items'. At the bottom are 'Test Source URL', 'OK' (which is highlighted with a red box), and 'Cancel' buttons.



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.