



## **CLOUD SECURITY FUNDAMENTALS V2**

### **Lab 04: Denying International Attackers**

Document Version: **2022-12-22**

Copyright © 2022 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

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

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

## Contents

Introduction .....	3
Objective .....	3
Lab Topology .....	4
Lab Settings .....	5
1 Denying International Attackers .....	6
1.0 Load Lab Configuration .....	6
1.1 Clone a Security Policy .....	11
1.2 Modify a Security Policy and Commit .....	12

## Introduction

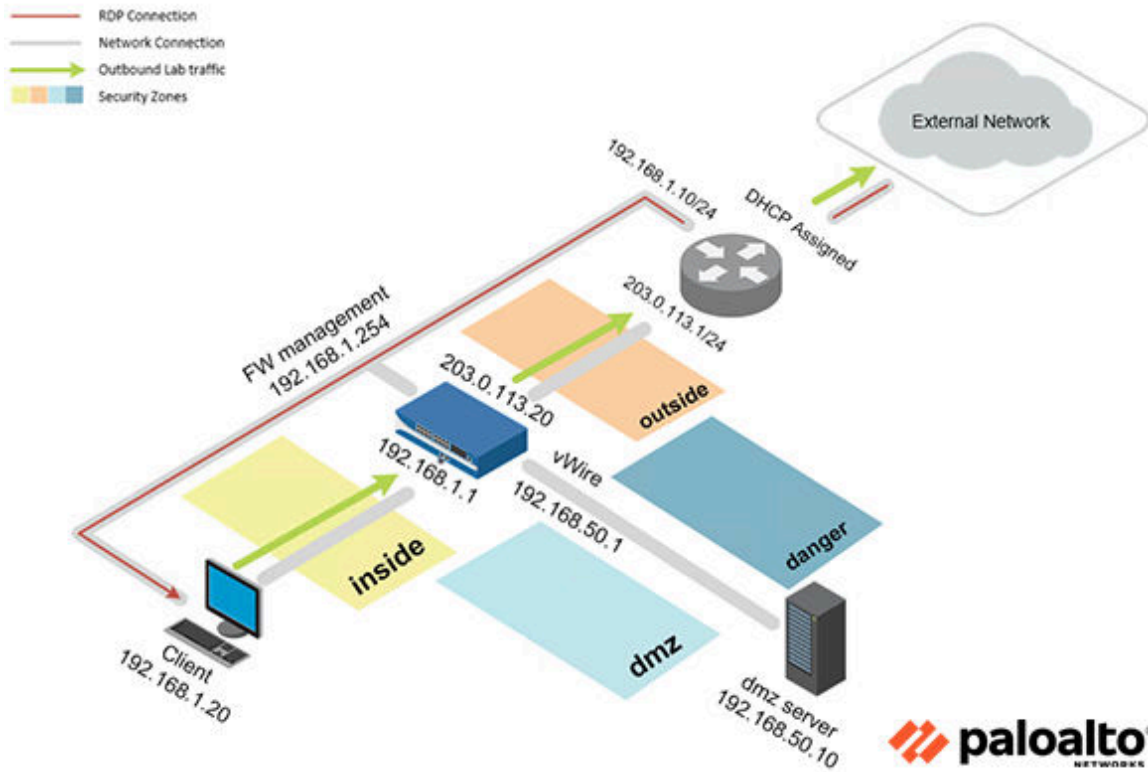
In this lab, you will configure a security policy to block malicious incoming traffic originating from three international locations of your choice.

## Objective

In this lab, you will perform the following tasks:

- Clone a Security Policy
- Modify a Security Policy and Commit

## 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.

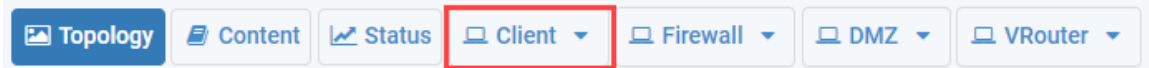
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

## 1 Denying International Attackers

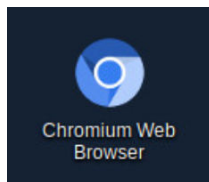
### 1.0 Load Lab Configuration

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

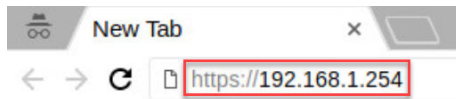
1. Click on the **Client** tab to access the Client PC.



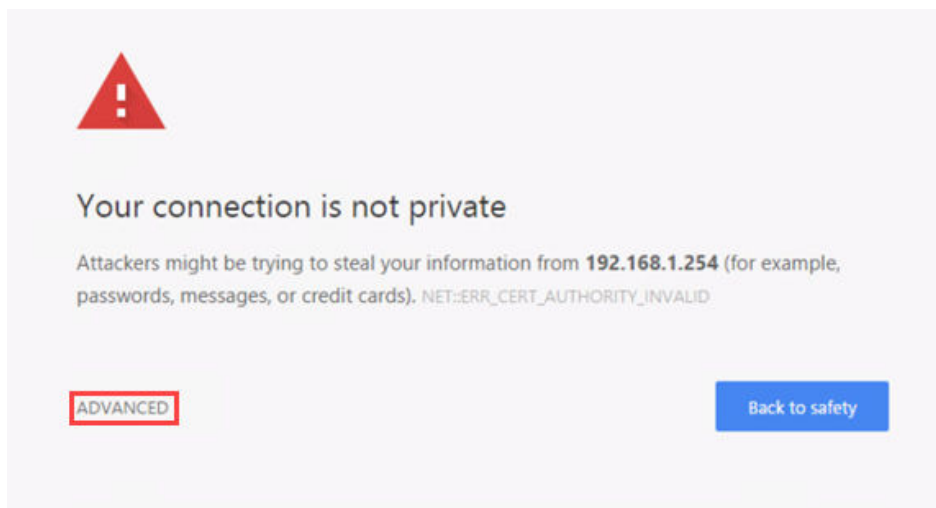
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

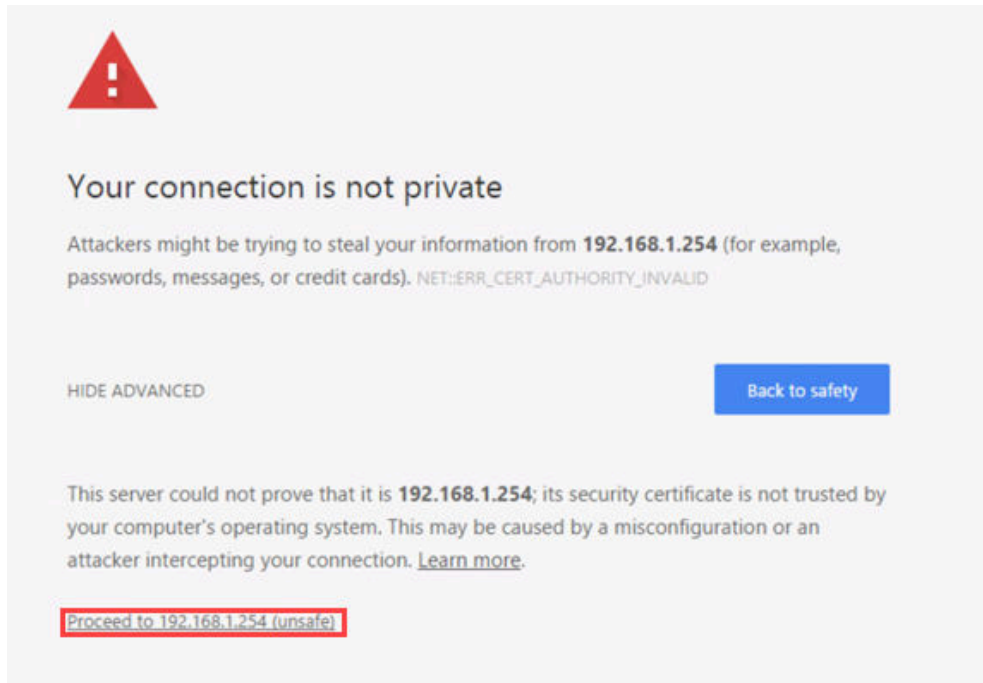


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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

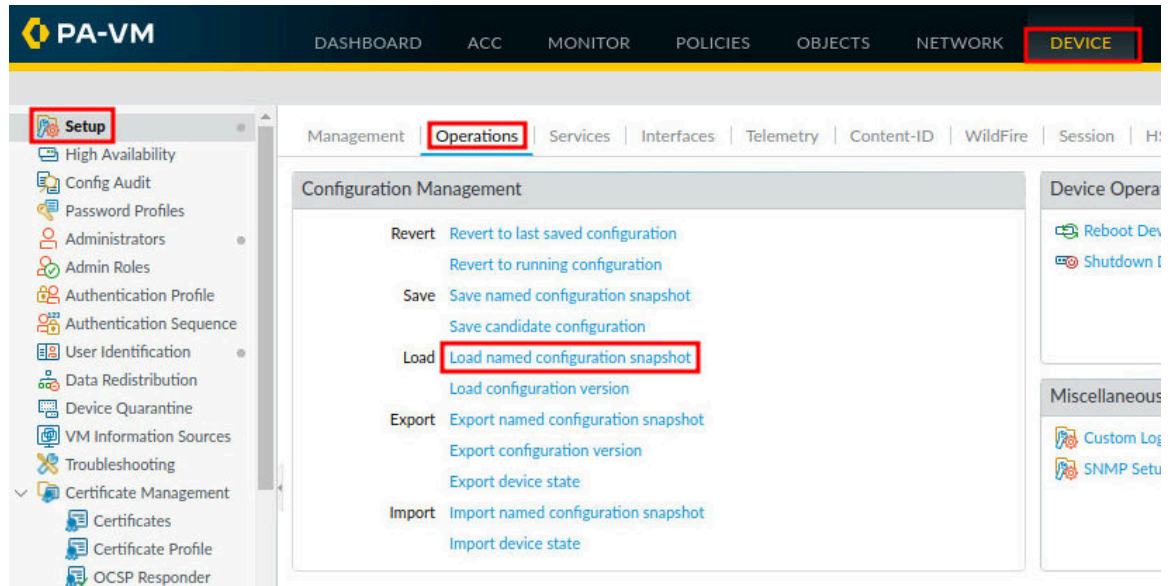
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



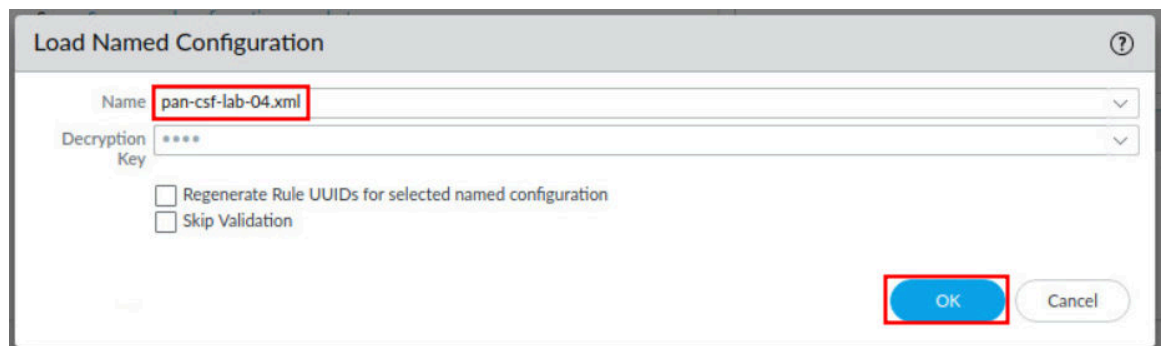
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



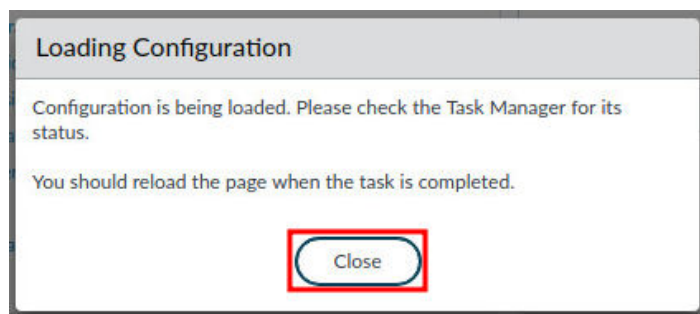
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-csf-lab-04.xml** from the *Name* dropdown box and click **OK**.

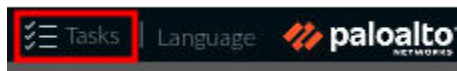


10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the Task Manager for its status. You should reload the page when the task is completed. Click **Close** to continue.

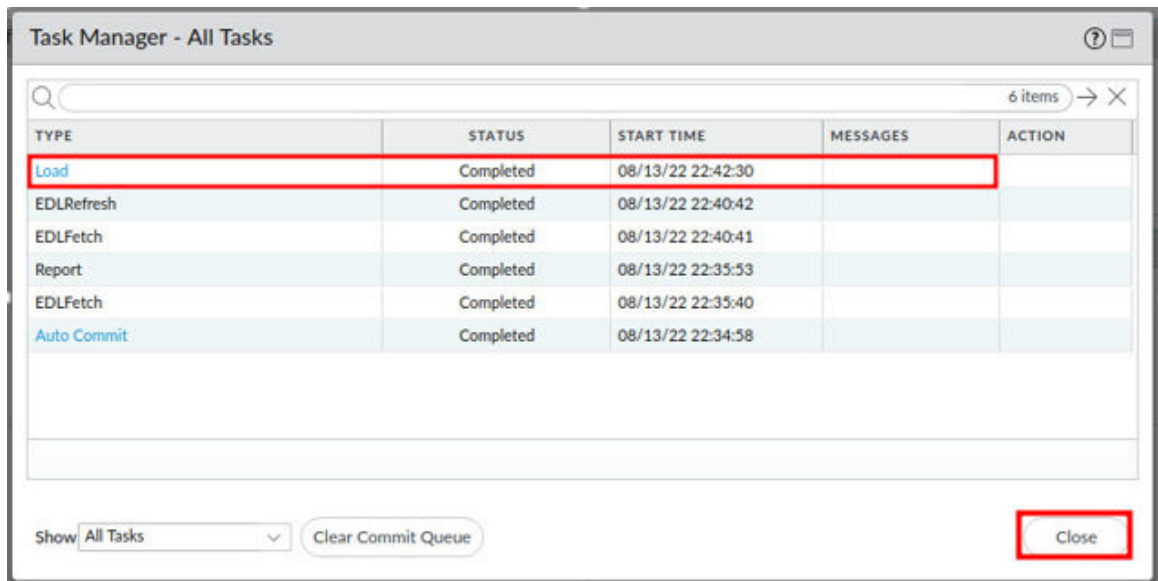




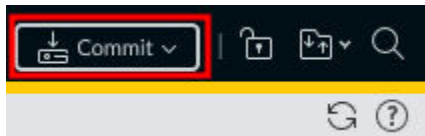
11. Click the **Tasks** icon located at the bottom-right of the web interface.



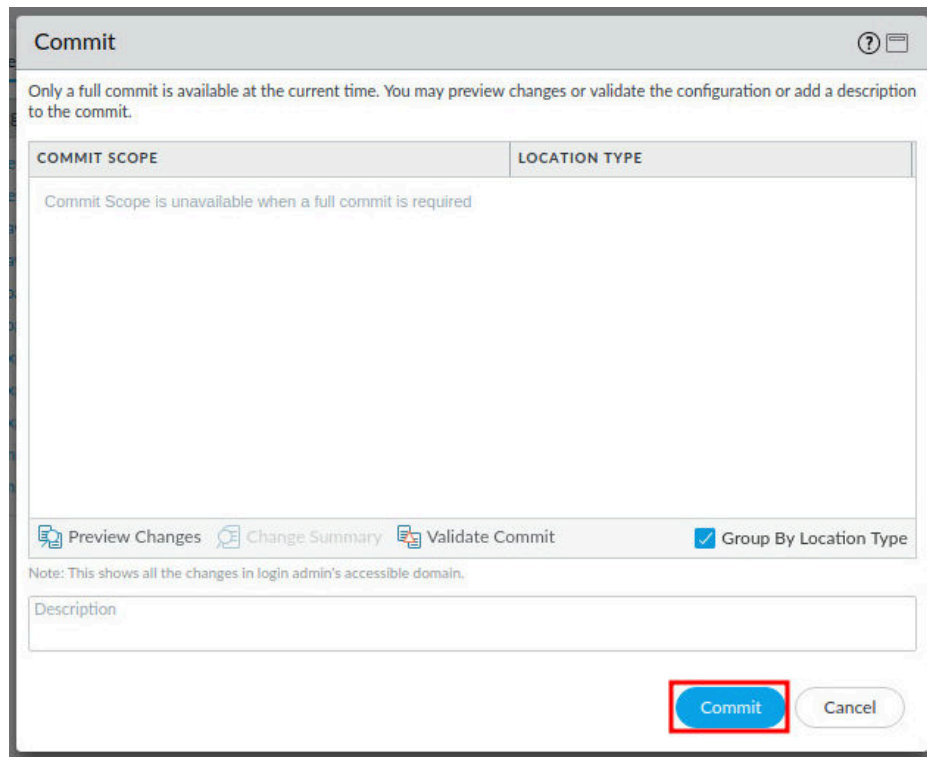
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



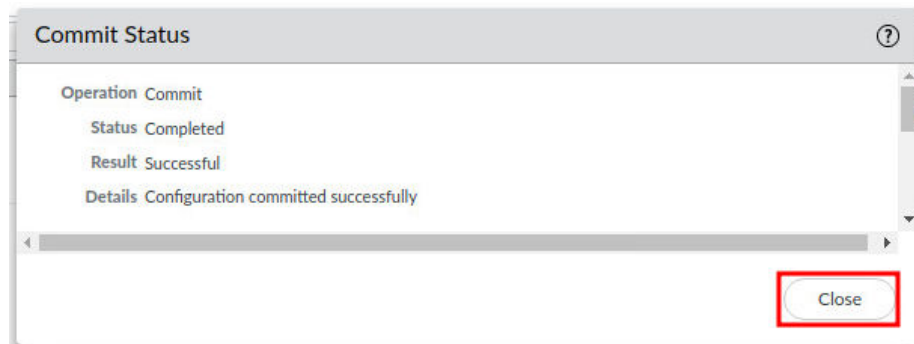
13. Click the **Commit** link located at the top-right of the web interface.



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



15. When the commit operation successfully completes, click **Close** to continue.

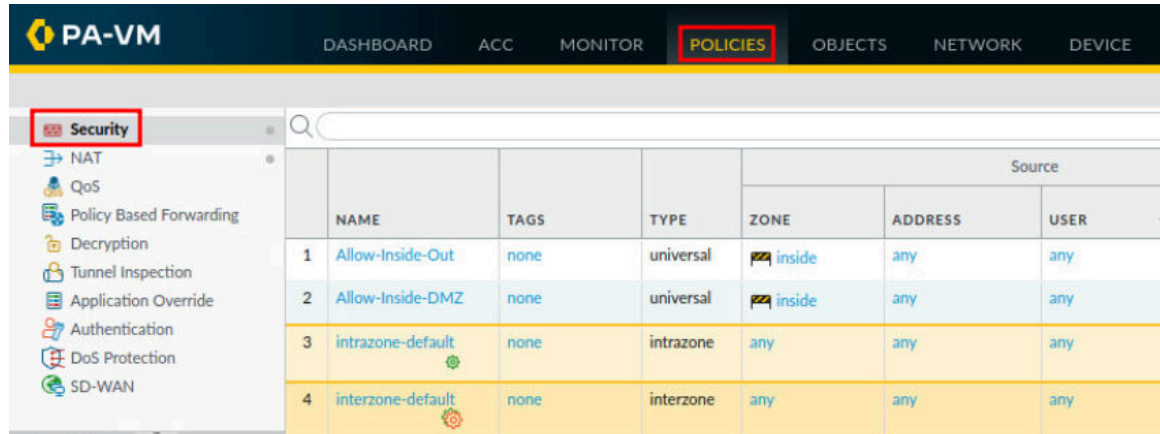


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

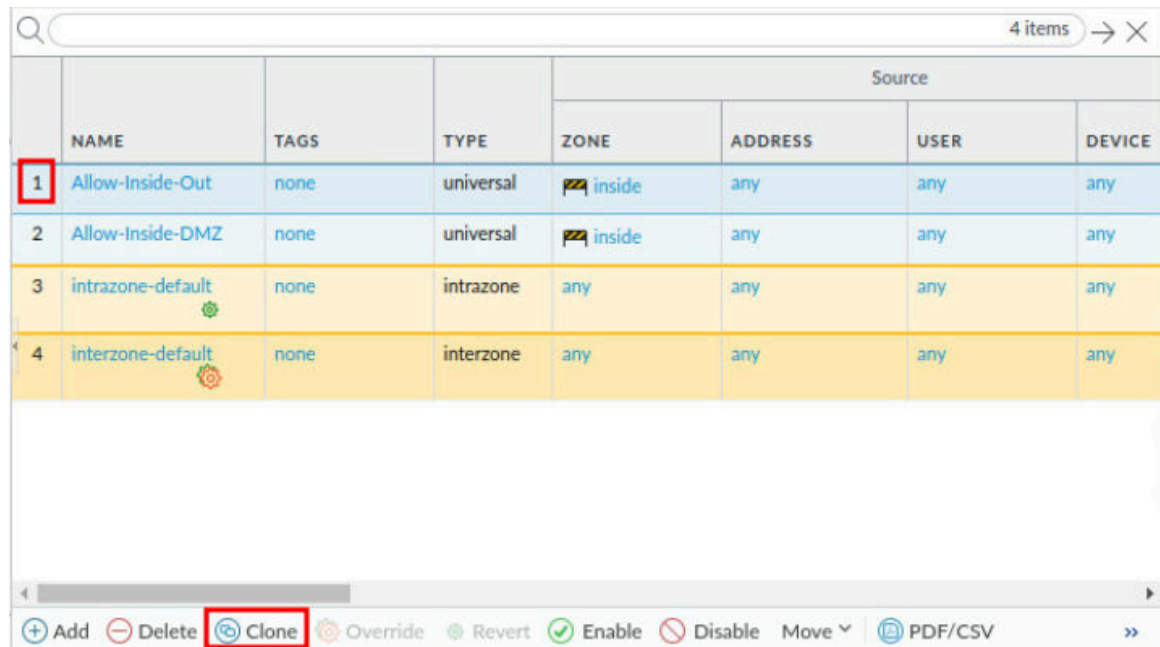
## 1.1 Clone a Security Policy

In this section, you will clone an existing Security Policy.

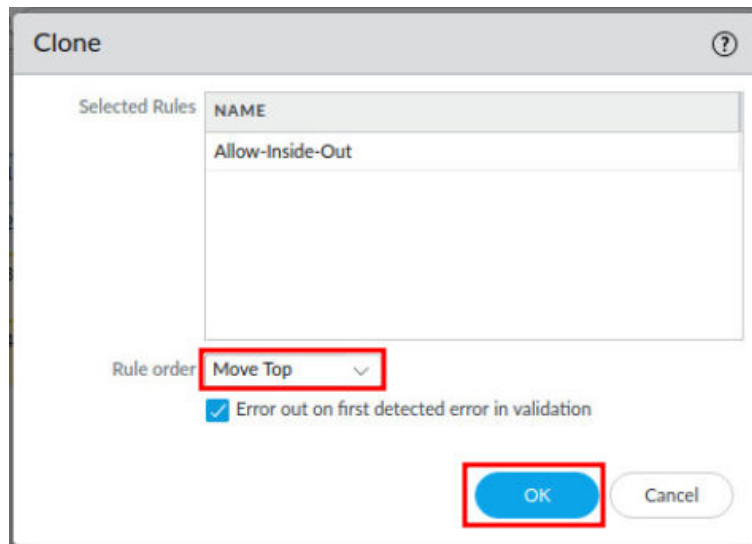
1. Navigate to **Policies > Security**.



2. Click on the number **1** to select the *Allow-Inside-Out* policy. Then, click the **Clone** button.



- In the *Clone* window, select **Move top** from the *Rule order* dropdown. Then, click the **OK** button.



Moving this rule to the top will allow it to be evaluated first, before the rule that allows all traffic.

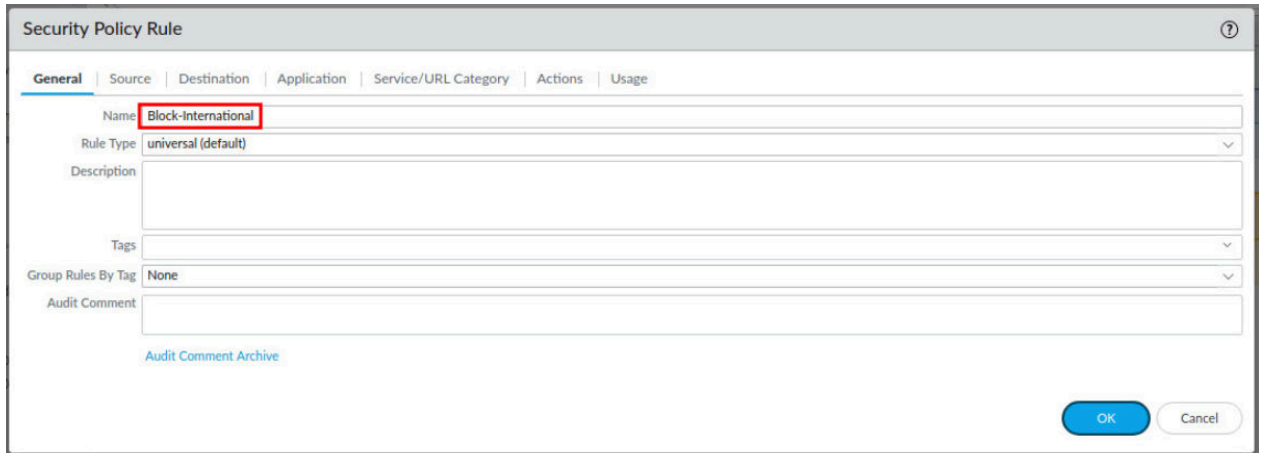
## 1.2 Modify a Security Policy and Commit

In this section, you will modify the cloned security policy to block malicious incoming traffic originating from three international locations of your choice. Then, you will commit your changes to the Firewall.

- Click on the **Allow-Inside-Out-1** Security Policy.

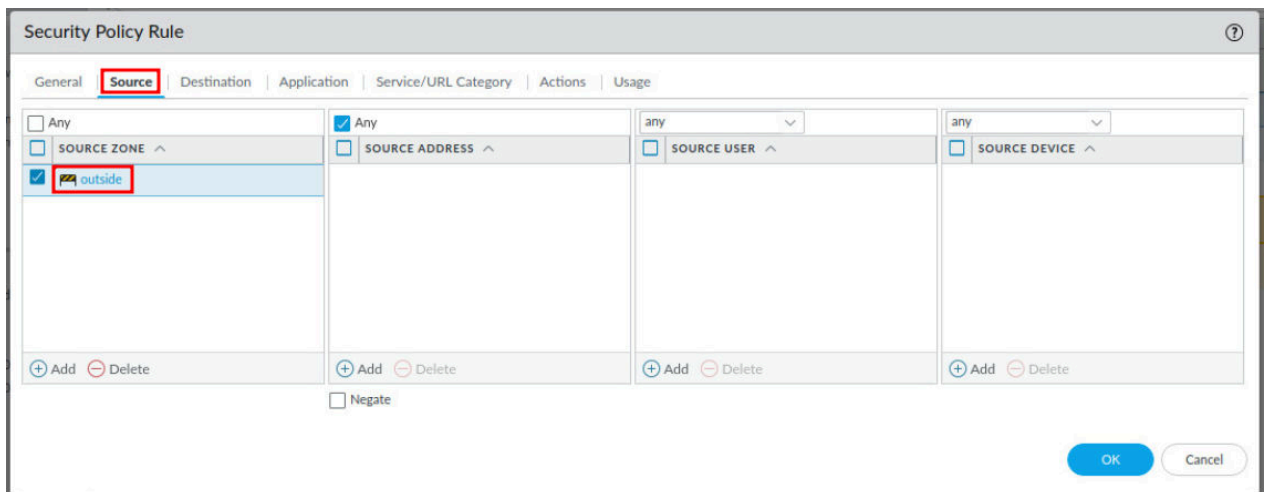
5 items → ×							
	NAME	TAGS	TYPE	Source			
				ZONE	ADDRESS	USER	DEVICE
1	Allow-Inside-Out-1	none	universal	inside	any	any	any
2	Allow-Inside-Out	none	universal	inside	any	any	any
3	Allow-Inside-DMZ	none	universal	inside	any	any	any
4	intrazone-default	none	intrazone	any	any	any	any
5	interzone-default	none	interzone	any	any	any	any

2. On the *Security Policy Rule* window, type **Block-International** in the *Name* field.



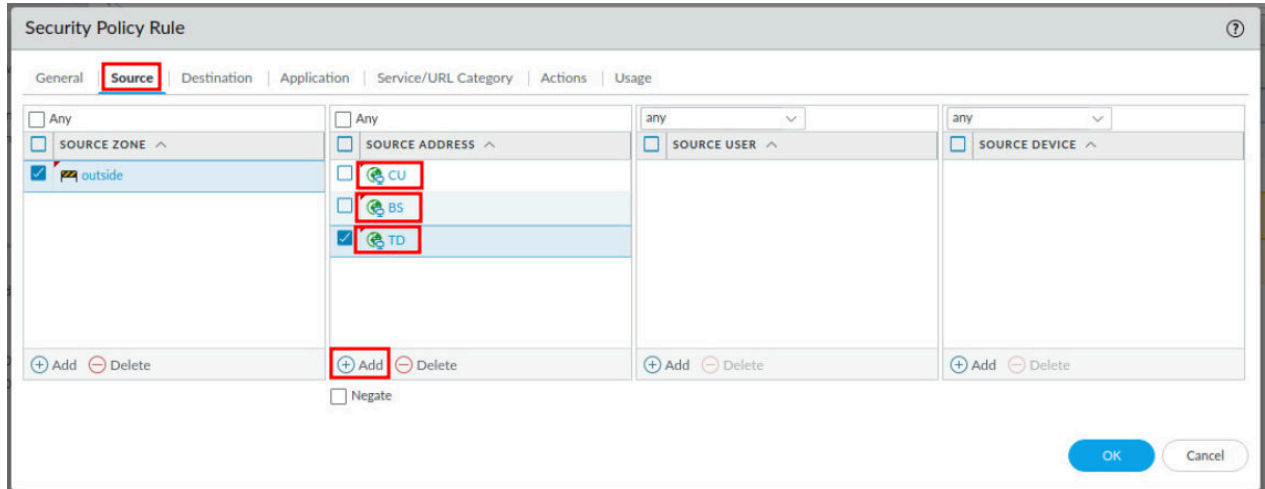
The screenshot shows the 'Security Policy Rule' window with the 'General' tab selected. The 'Name' field is highlighted with a red box and contains the text 'Block-International'. Other fields include 'Rule Type' (universal (default)), 'Description', 'Tags', 'Group Rules By Tag' (None), and 'Audit Comment'. There are 'OK' and 'Cancel' buttons at the bottom right.

3. On the *Security Policy Rule* window, click on the **Source** tab. Then, click on the **inside** zone and change it to the **outside** zone in the *Source Zone* section.



The screenshot shows the 'Security Policy Rule' window with the 'Source' tab selected. The 'Source Zone' section is highlighted with a red box and shows the 'outside' zone selected. Other sections include 'SOURCE ADDRESS', 'SOURCE USER', and 'SOURCE DEVICE'. There are 'Add' and 'Delete' buttons for each section, and a 'Negate' checkbox at the bottom. There are 'OK' and 'Cancel' buttons at the bottom right.

- On the *Security Policy Rule* window, click the **Add** button at the bottom of the *Source Address* section to select three international locations of your choice. For this lab, the first international location we chose to select is **CU**, which is the country code for Cuba. Next, click the **Add** button again. The second international location we chose to select is **BS**, which is the country code for the Bahamas. Next, click the **Add** button again. The third international location we chose to select is **TD**, which is the country code for Chad.

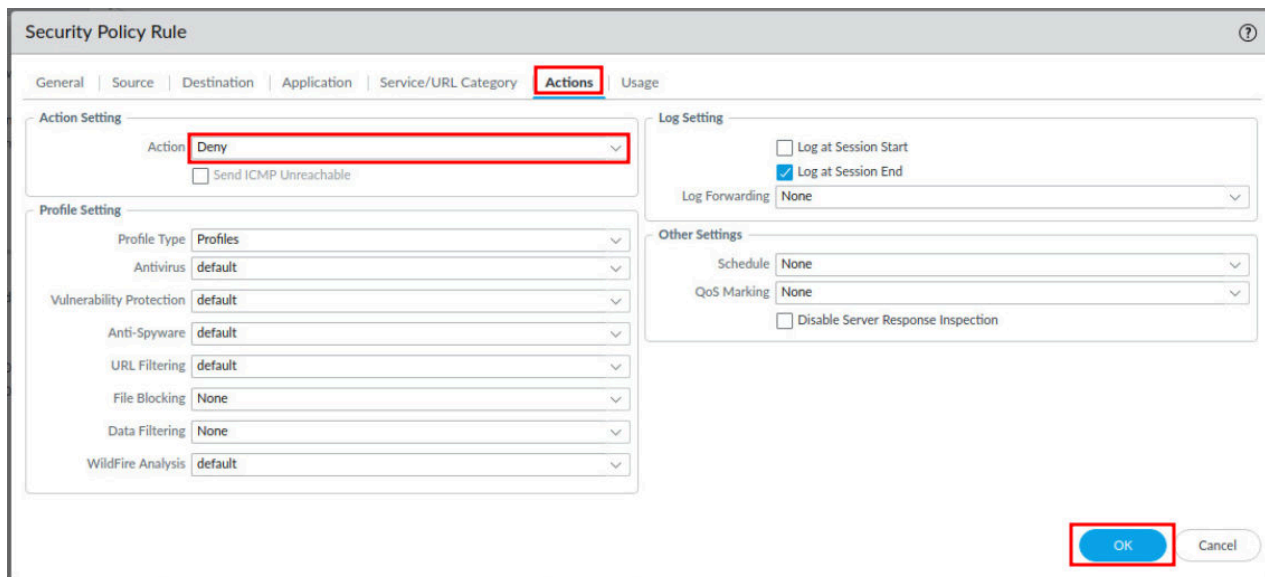


The screenshot shows the 'Security Policy Rule' window with the 'Source' tab selected. The 'SOURCE ADDRESS' section has three entries: 'CU', 'BS', and 'TD', each with a green globe icon. The 'Add' button at the bottom of this section is highlighted with a red box. The 'SOURCE ZONE' section shows 'outside' selected. The 'SOURCE USER' and 'SOURCE DEVICE' sections are empty. The 'Negate' checkbox is unchecked. The 'OK' button is highlighted with a red box.



For the purpose of this lab, you will select three international locations of your choosing. For this lab example, we chose to use CU for Cuba, BS for Bahamas, and TD for Chad.

- On the *Security Policy Rule* window, click the **Actions** tab. Then, select **Deny** in the *Action* dropdown. Next, click the **OK** button.

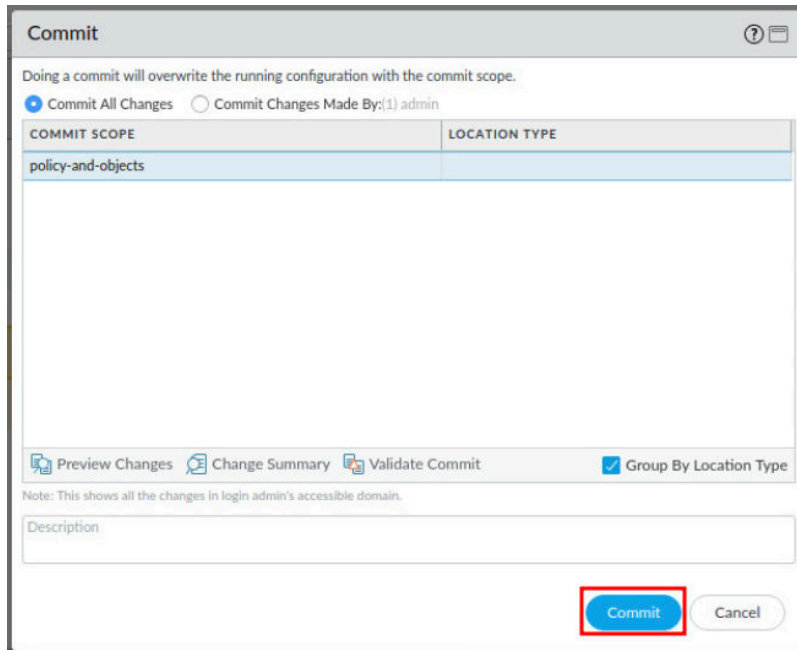


The screenshot shows the 'Security Policy Rule' window with the 'Actions' tab selected. The 'Action' dropdown menu is set to 'Deny'. The 'Send ICMP Unreachable' checkbox is unchecked. The 'Profile Setting' section shows various settings: Profile Type (Profiles), Antivirus (default), Vulnerability Protection (default), Anti-Spyware (default), URL Filtering (default), File Blocking (None), Data Filtering (None), and WildFire Analysis (default). The 'Log Setting' section shows 'Log at Session Start' (unchecked), 'Log at Session End' (checked), and 'Log Forwarding' (None). The 'Other Settings' section shows 'Schedule' (None), 'QoS Marking' (None), and 'Disable Server Response Inspection' (unchecked). The 'OK' button is highlighted with a red box.

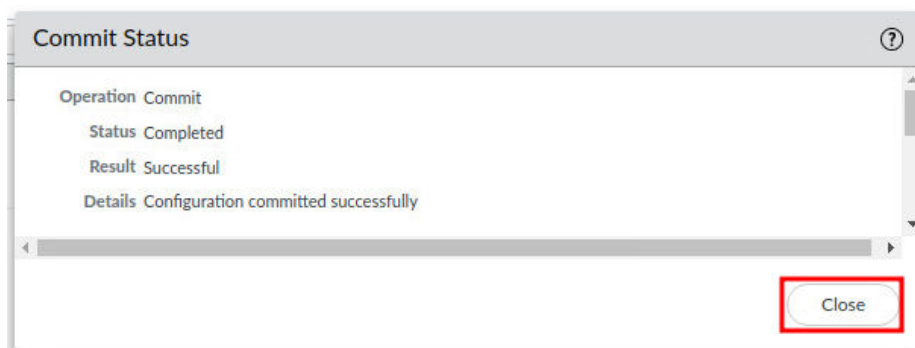
- Click the **Commit** link located at the top-right of the web interface.



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



- When the commit operation successfully completes, click **Close** to continue.



Due to the nature of this lab environment, you are unable to originate traffic from these international locations coming into your environment to confirm this policy.

- The lab is now complete; you may end the reservation.