



PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES

Lab 12: Custom Vulnerability Signatures

Document Version: 2016-04-19

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

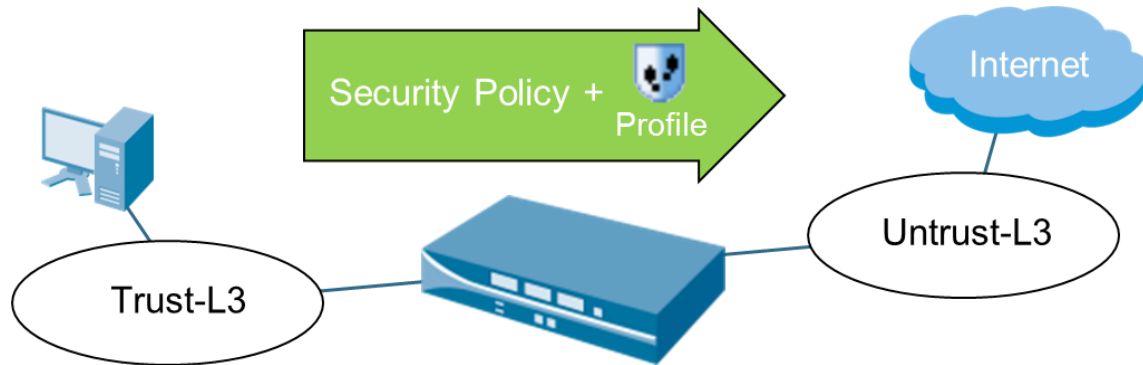
NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

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

Contents

Introduction	3
Objective	4
Pod Topology	5
Lab Settings	6
1 Initial Firewall Configuration.....	7
2 Create a Custom Vulnerability Signature (Threat 1).....	10
3 Test a Custom Vulnerability Signature (Threat 1).....	13

Introduction



Your security team has identified a set of threats unique to your environment that require custom signatures. These threats are an immediate concern and cannot wait for the standard update cycle from Palo Alto Networks.

- Threat 1: A PDF with malicious code has been downloaded by several users, infecting their systems. A sample of the file has been uploaded to <http://www.panedufiles.com/files/17717.pdf> for testing purposes. An excerpt of the specific code contained in the PDF will be made available to you by the security team.
- Threat 2: An XML-RPC exploit exists which allows remote attackers to execute PHP code via XML files. The details of this known exploit (detailed in CVE-2005-1921) will be provided to you. The Fiddler2 utility will be provided for you to generate traffic to test this signature.
- Threat 3: The security team has been asked to watch for IP addresses which generate HTTP 400 (e.g., file not found errors) or 500 (e.g., internal server error) errors repeatedly over a short period of time. Custom signatures exist for HTTP 400 and 500 errors that you can reuse for your checks.

You must check for these issues on traffic between the trusted zone and the Internet. For testing purposes only, create a rule that allows traffic from the trusted zone to the untrusted zone for all applications. Assign the profiles created for this lab to that rule and ensure that all traffic will use the testing rule.

Lab Notes

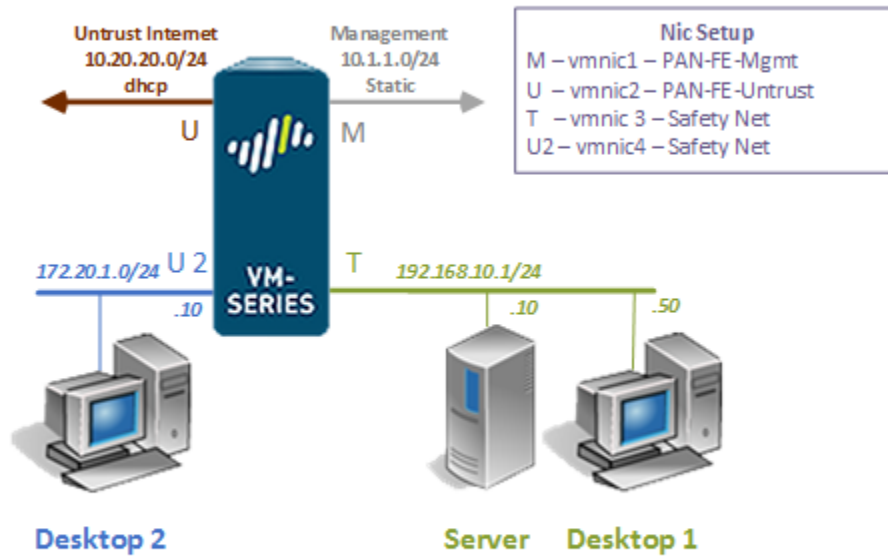
- The regular expression match engine in PAN-OS requires a minimum of 7 bytes for a string match.
- Remove the custom signatures from the firewall upon completion of this lab.

Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Configure a custom vulnerability signature

Pod 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)
Ubuntu Desktop 1	192.168.10.50	sysadmin	Train1ng\$
Ubuntu Server	192.168.10.10	sysadmin	Train1ng\$
Ubuntu Desktop 2	172.30.1.10	sysadmin	Train1ng\$
Palo Alto Firewall	192.168.10.1 172.30.1.1	admin	paloalto

1 Initial Firewall Configuration

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using **sysadmin** as the *username* and **Training\$** as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.



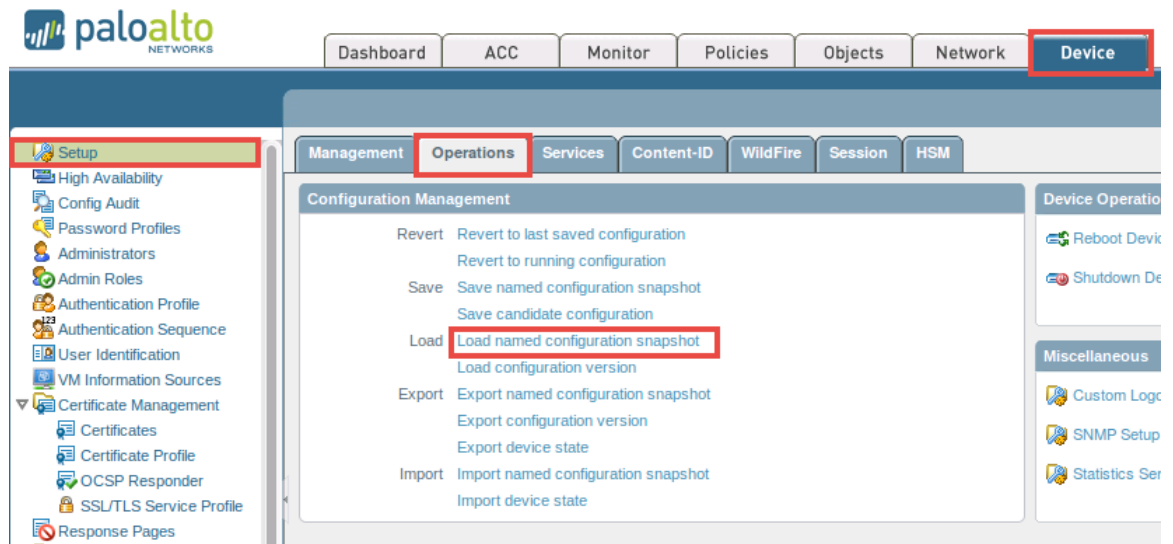
4. In the address field, type **https://192.168.10.1** and press **Enter**.

If you experience the “Unable to connect” message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

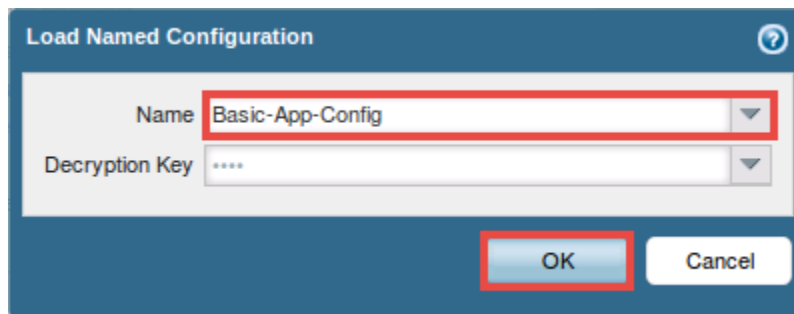
5. Login with the *username* **admin** and *password* **paloalto** on the firewall web interface.



- Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



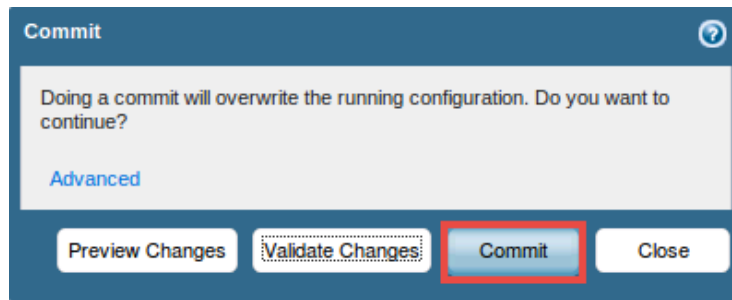
- In the *Load Named Configuration* window, select **Basic-App-Config** from the *Name* drop-down box. Click **OK**.



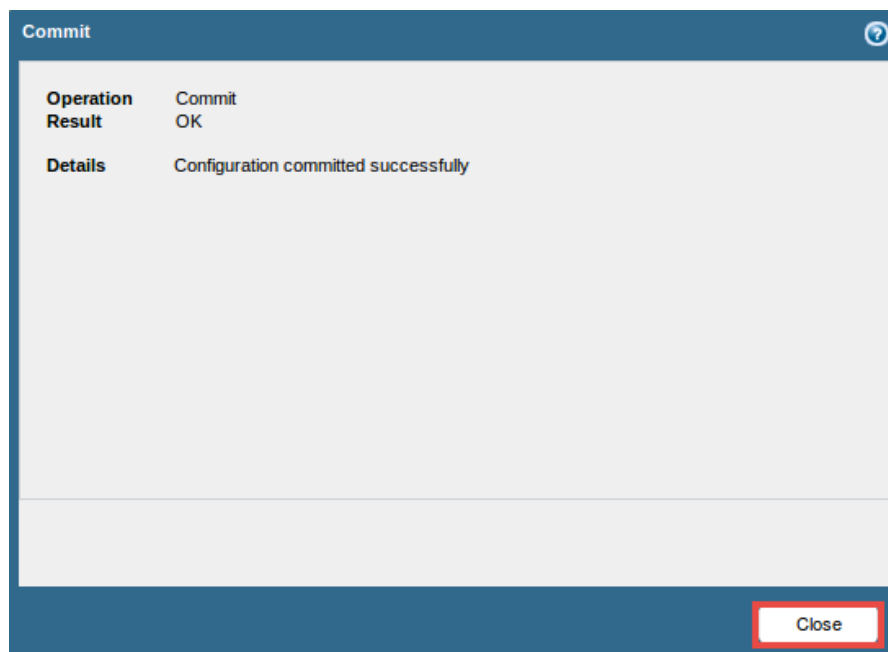
- When prompted with the config loaded message, click on the **Close** button to continue.
- Click on the **Commit** link located at the top-right of the *WebUI*.



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



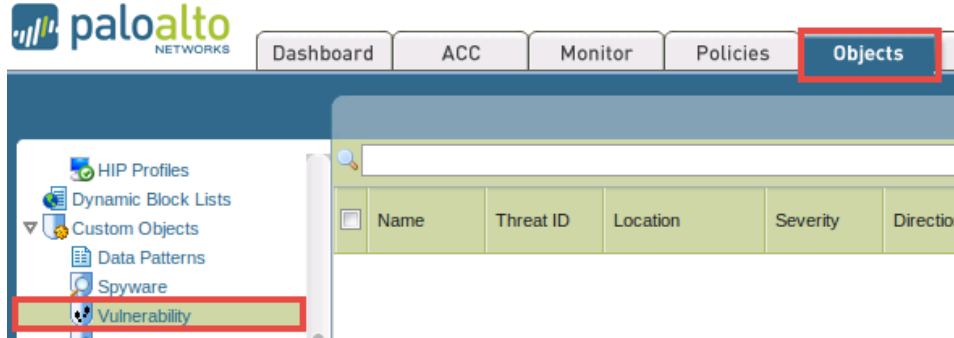
11. Once the operation successfully completes, click **Close** to continue.



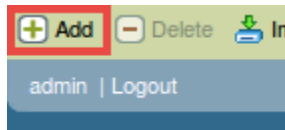
12. Leave the *Firefox* web browser opened to continue with the next task.

2 Create a Custom Vulnerability Signature (Threat 1)

1. Using *Firefox*, open a **new tab**.
2. In the new tab, enter `http://www.panedufiles.com/files/17717.pdf` and press the **Enter** key. Download the *PDF* file to the *Downloads* directory, but do not open it.
3. Close the **second tab** and navigate back to the first tab.
4. Using the *WebUI*, navigate to the **Objects > Custom Objects > Vulnerability**.

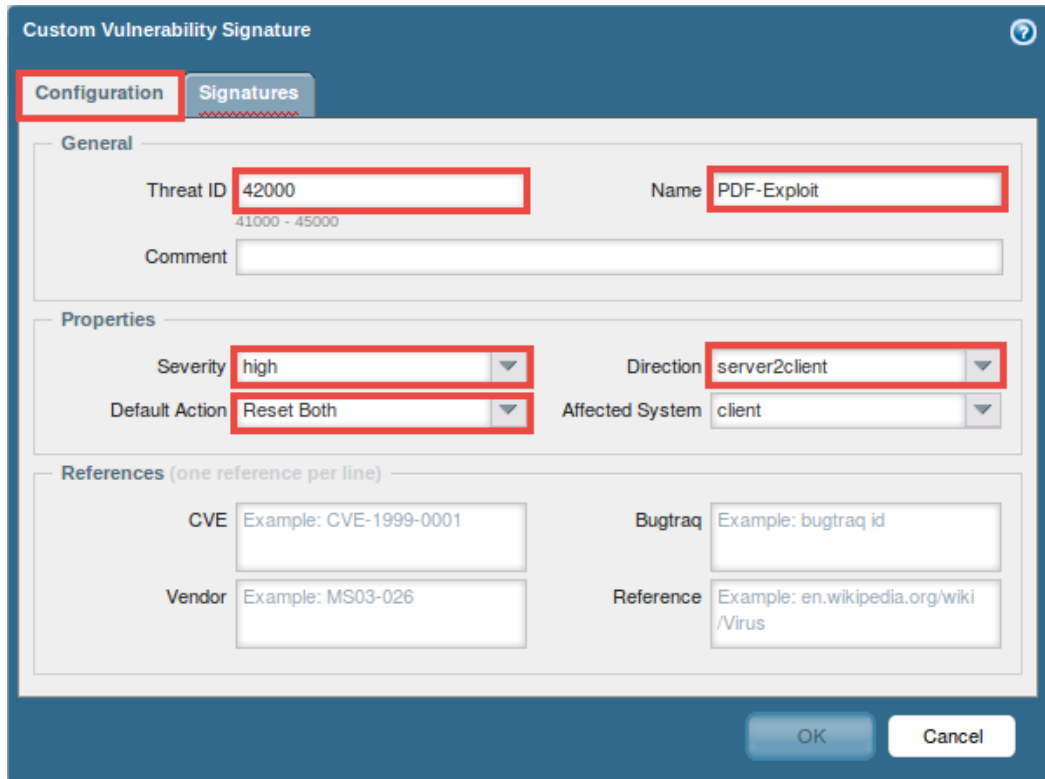


5. Click **Add**, located near the bottom of the window, to create a new vulnerability signature.



6. In the *Custom Vulnerability Signature* window, click the **Configuration** tab and use the information from the table below to make the appropriate configurations.

Field	Data/Selection
<i>Thread ID</i>	Enter 42000
<i>Name</i>	Enter PDF-Exploit
<i>Severity</i>	Select high
<i>Direction</i>	Select server2client
<i>Default Action</i>	Select Reset Both



Custom Vulnerability Signature

Configuration | Signatures

General

Threat ID: 42000
41000 - 45000

Name: PDF-Exploit

Comment:

Properties

Severity: high

Direction: server2client

Default Action: Reset Both

Affected System: client

References (one reference per line)

CVE: Example: CVE-1999-0001

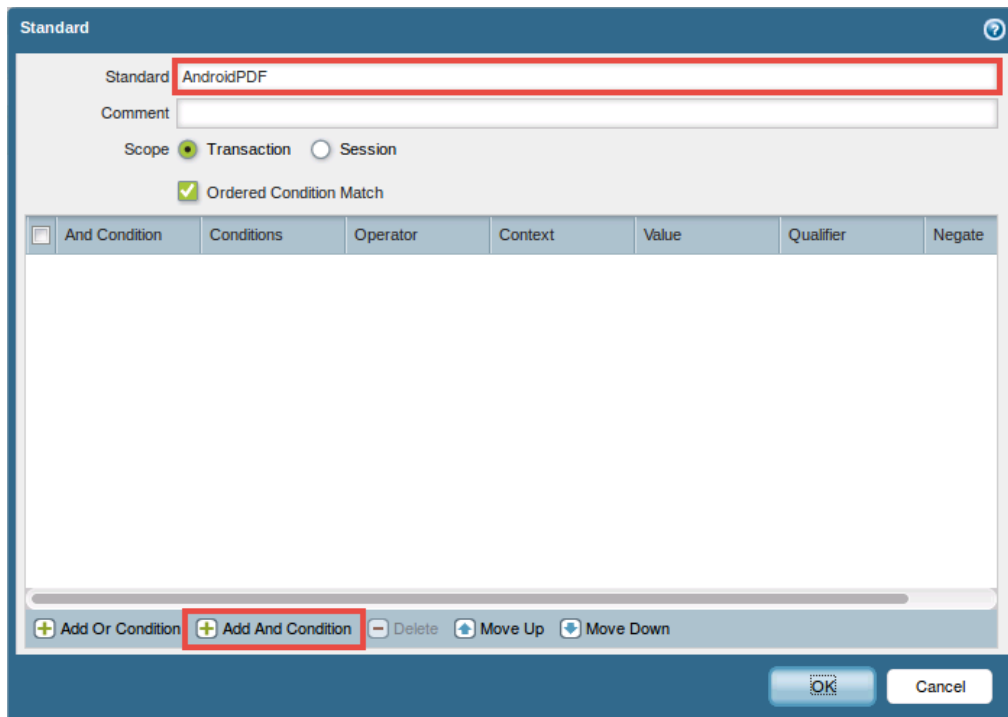
Bugtraq: Example: bugtraq id

Vendor: Example: MS03-026

Reference: Example: en.wikipedia.org/wiki/Virus

OK Cancel

7. In the *Custom Vulnerability Signature* window, click the **Signatures** tab and click the **Add** button.
8. In the *Standard* window, enter **AndroidPDF** into the *Standard* text field and click **Add And Condition**.



Standard

Standard: AndroidPDF

Comment:

Scope: ☒ Transaction ☐ Session

☒ Ordered Condition Match

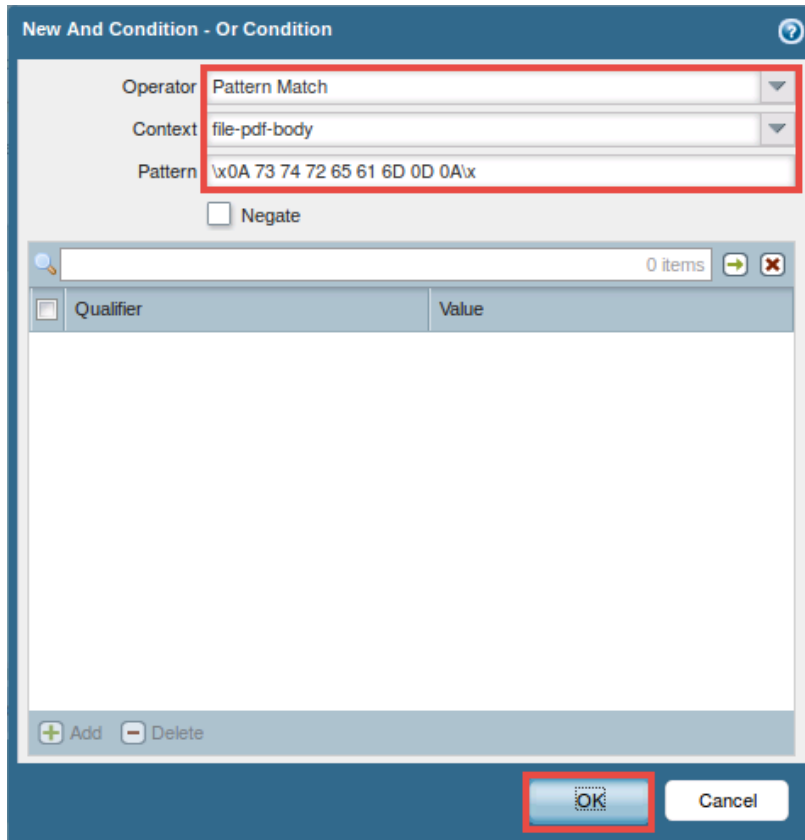
And Condition	Conditions	Operator	Context	Value	Qualifier	Negate

+ Add Or Condition + Add And Condition - Delete + Move Up + Move Down

OK Cancel

9. In the *New And Condition – Or Condition* window, use the information from the table below to make the appropriate configurations.

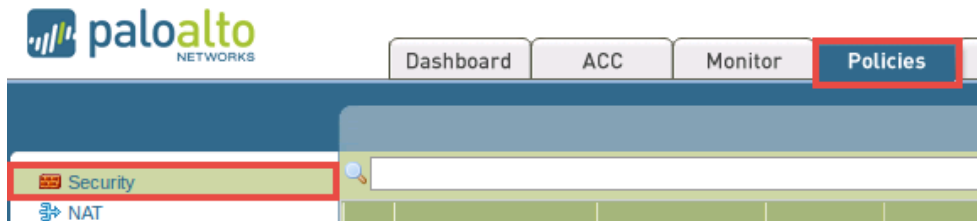
Field	Data/Selection
<i>Operator</i>	Select Pattern Match
<i>Context</i>	Select file-pdf-body
<i>Pattern</i>	Enter \x0A 73 74 72 65 61 6D 0D 0A\x



10. Click **OK** to save changes.
11. In the *Standard* window, verify that the new *add and condition* appears in the list and click **OK**.
12. In the *Custom Vulnerability Signature* window, verify that *PDFExploit* appears in the list and click **OK**.
13. Leave the *WebUI* opened to continue with the next task.

3 Test a Custom Vulnerability Signature (Threat 1)

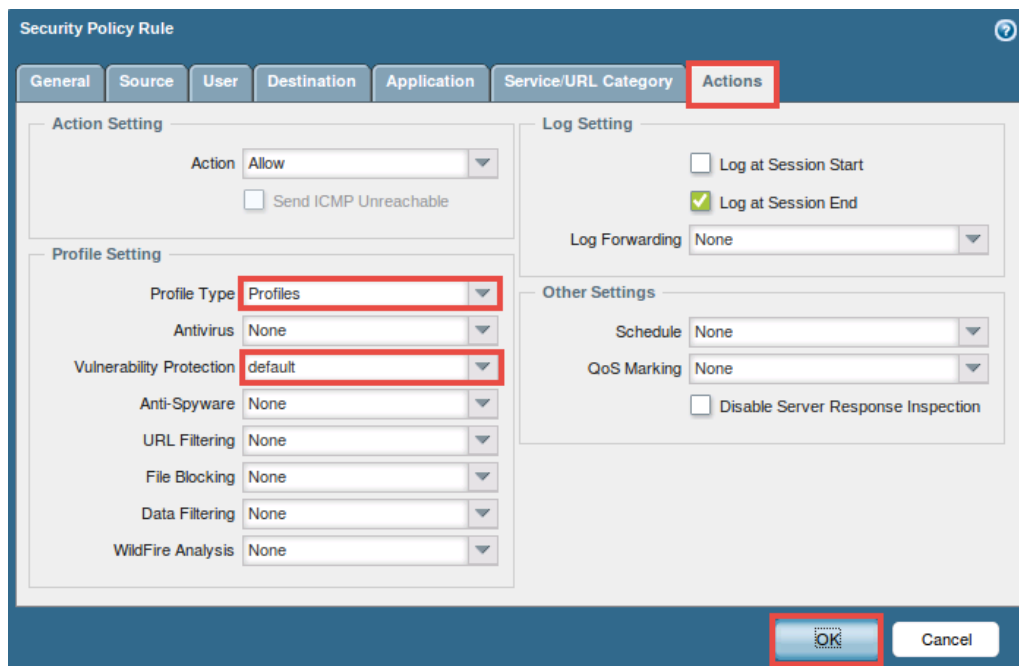
1. Using the *WebUI*, navigate to **Policies > Security**.



2. Click on the **Basic-Allowed-Apps** link underneath the *Name* column.

	Name	Tags	Type	Zone
1	Basic-Allowed-Apps	none	universal	Tr
2	MGMT-PORT-OUT	none	universal	Mg
3	intrazone-default	none	intrazone	any
4	interzone-default	none	interzone	any

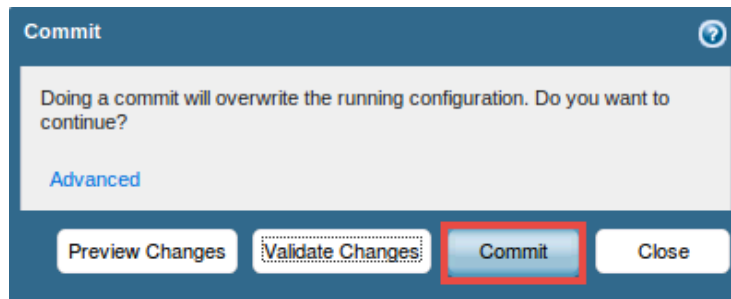
3. In the *Security Policy Rule* window, click on the **Actions** tab change the Profile Type to Profiles and select **default** for *Vulnerability Protection*.



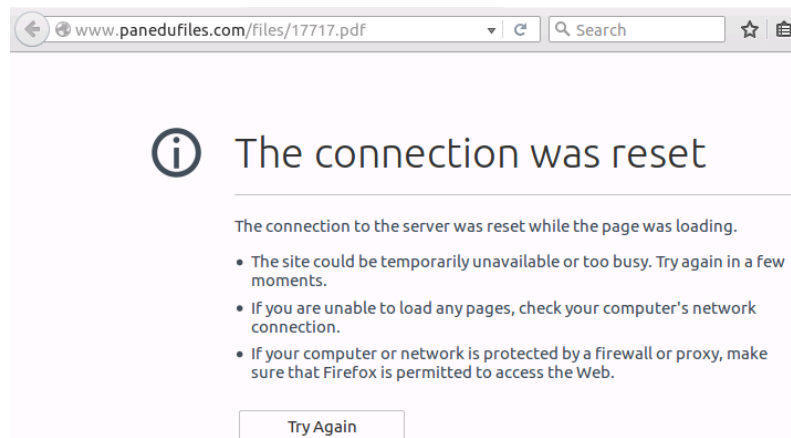
4. Click **OK** to save changes.
5. Click on the **Commit** link located at the top-right of the *WebUI*.



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



7. Once the operation successfully completes, click **Close** to continue.
8. Using the *Firefox* web browser, open a **new tab**.
9. Enter `http://www.panedufiles.com/files/17717.pdf` into the address field and press the **Enter** key.



Notice that the firewall resets the connection and now prevents the *PDF* file from being downloaded.

10. Close the **second tab** and navigate back to the **first tab**.
11. Using the *WebUI*, navigate to **Monitor > Logs > Threat** to review the log entry for the *PDF-Exploit*.
12. Close the **Desktop 1** PC viewer.