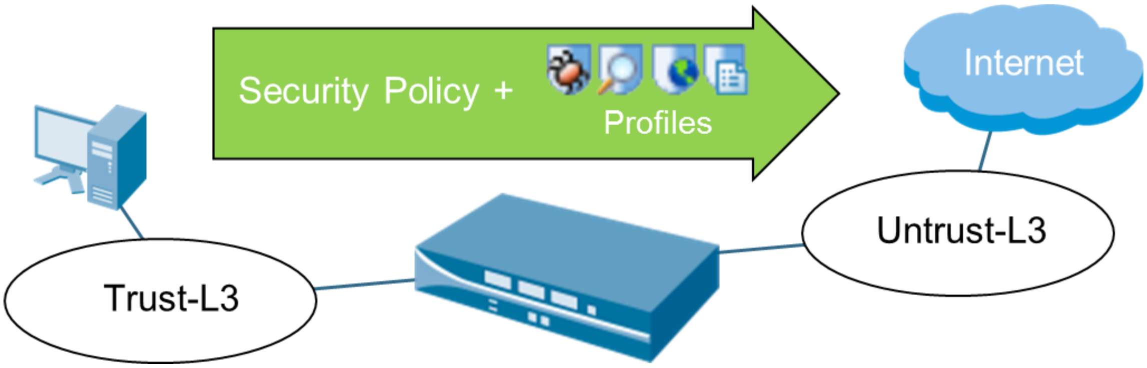
PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES

Lab 5: URL Filtering

Document Version: 2016-04-19

Contents

Introduction



Now that traffic is passing through the firewall, you decide to further protect the environment with security profiles. The specific security requirements for general Internet traffic are:

- Configure a custom URL filtering category TechSites specifying newegg, cnet, and zdnet.
- Log all URLs accessed by users in the Trust-L3 zone.
- Block these URL categories:
  - adult (or adult-and-pornography)
  - government
  - hacking
  - questionable
  - TechSites
  - unknown (set to continue)
- Then, send test traffic to verify that the protection behaves as expected. Test the antivirus profile by downloading a file over http from eicar.org. Test the URL filtering profile by trying to surf sites that have been prohibited.

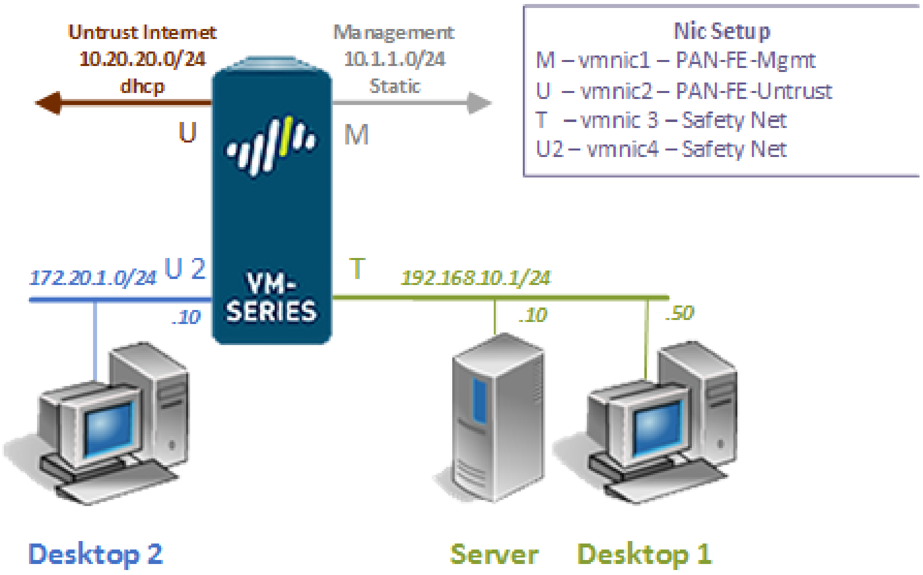
From Desktop 2, launch a web browser and terminal window to access the server via the web and ssh and connect to the Untrust2-L3.

Objective

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

1. Create custom URL categories
2. Configure a URL filtering profile to block certain types of websites from the internet
3. Apply the filters to the policies and log the web traffic

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

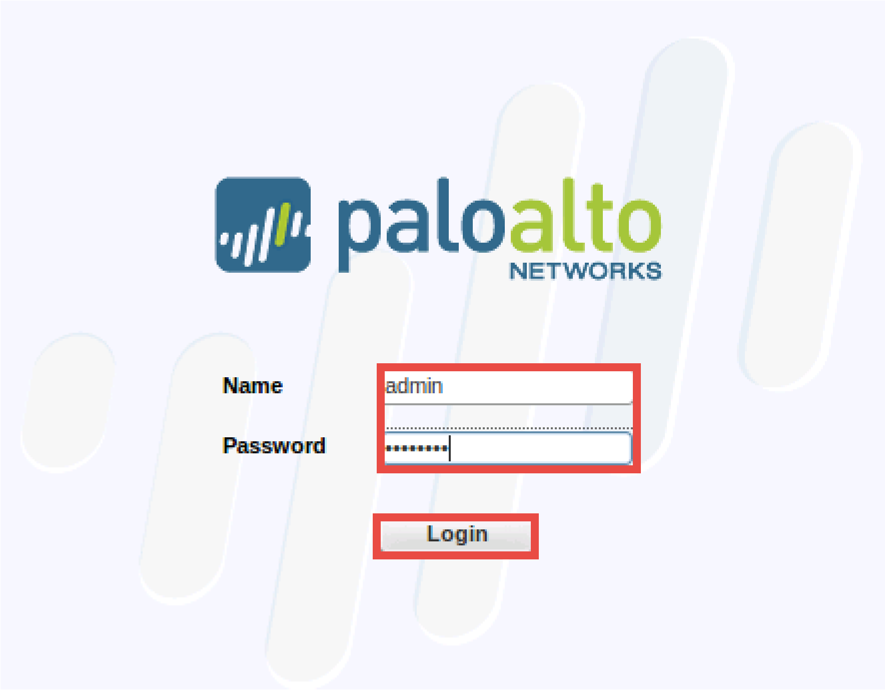
1 Initial Setup

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using `sysadmin` as the *username* and `Train1ng$` 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.

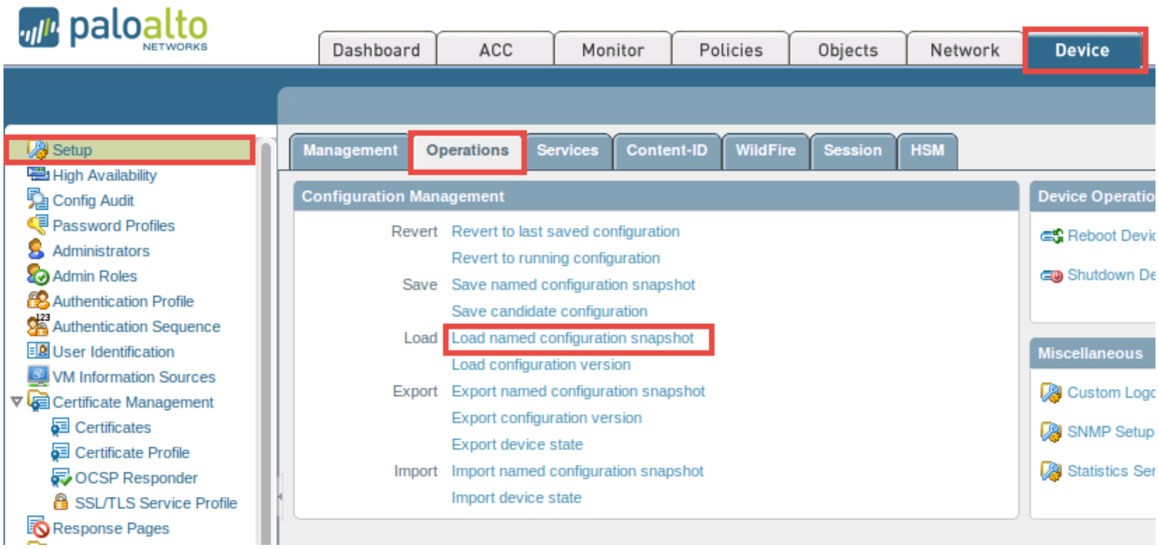
5. Login with the *username* `admin` and *password* `paloalto` on the firewall web interface.



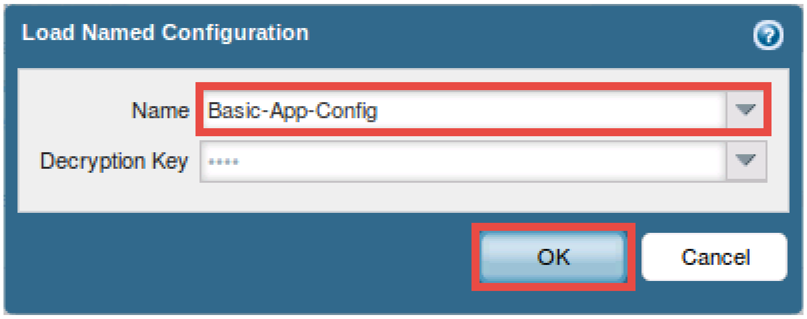
Name: admin

Password: ••••••••

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



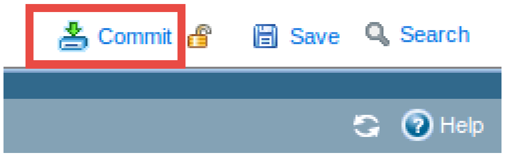
7. In the *Load Named Configuration* window, select **Basic-App-Config** from the *Name* drop-down box. Click **OK**.


Load Named Configuration

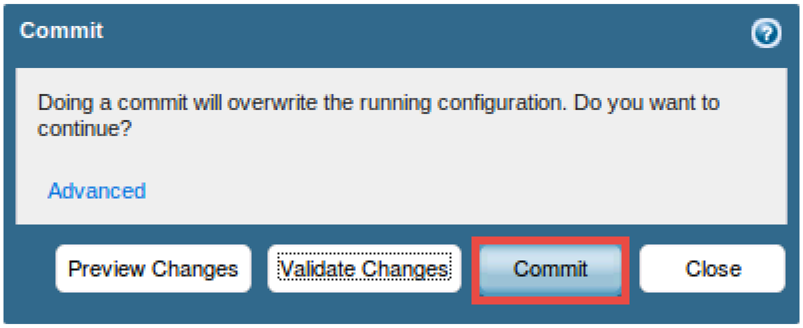
Name: Basic-App-Config

Decryption Key: ••••

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

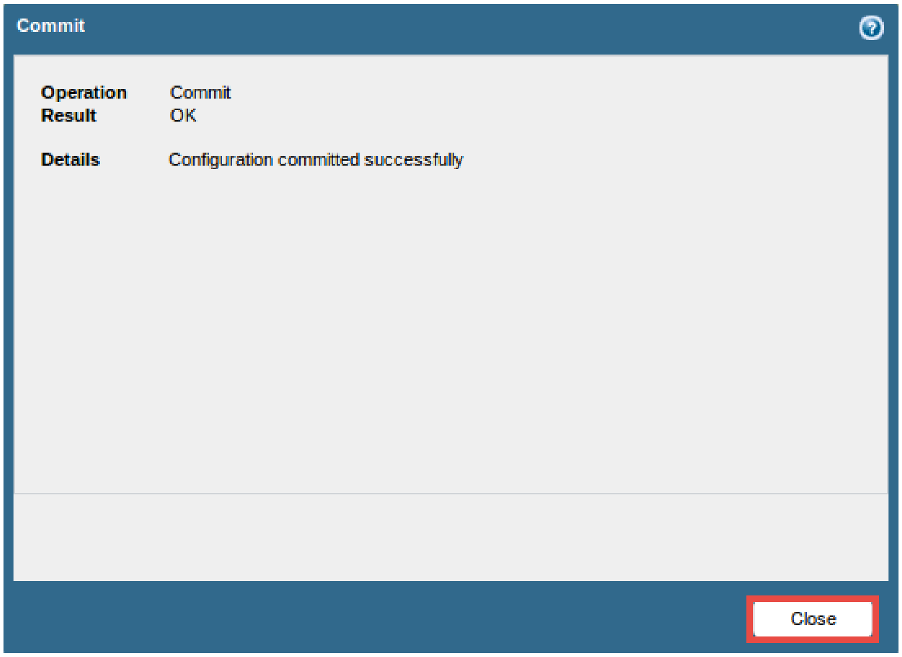


10. In the *Commit* window, click **Commit** to proceed with committing the changes.



Doing a commit will overwrite the running configuration. Do you want to continue?

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



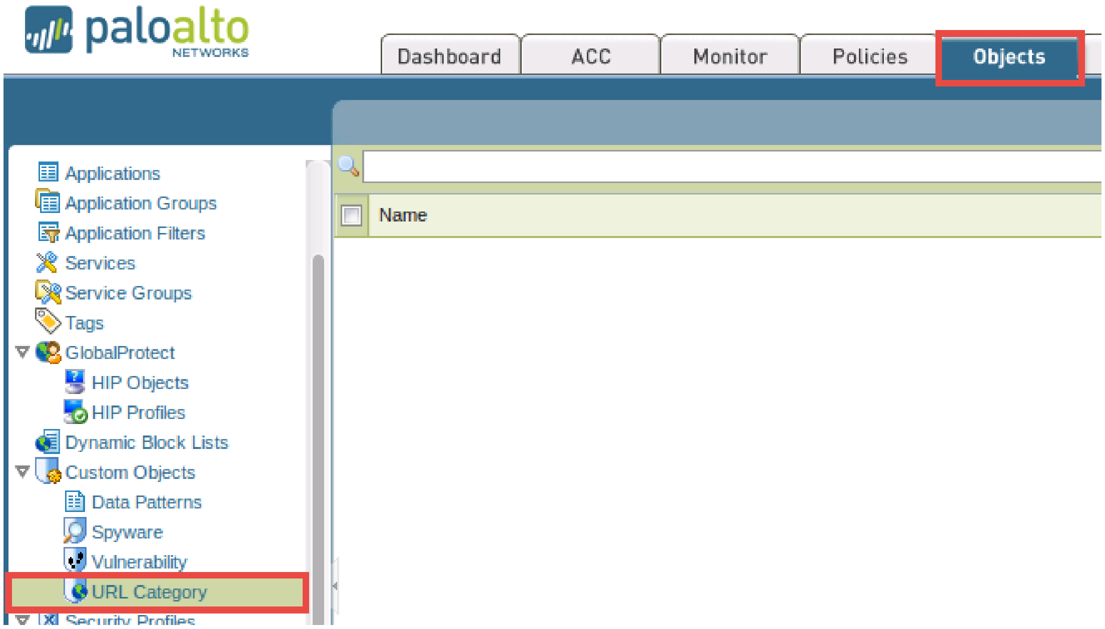
Operation Commit
Result OK

Details Configuration committed successfully

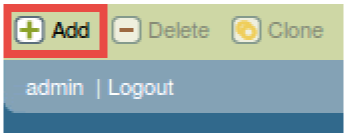
12. Leave the *WebUI* opened to continue with the next task.

2 Configure a Customer URL Filtering Category

1. Using the *WebUI*, navigate to **Objects > Custom Objects > URL Category**.

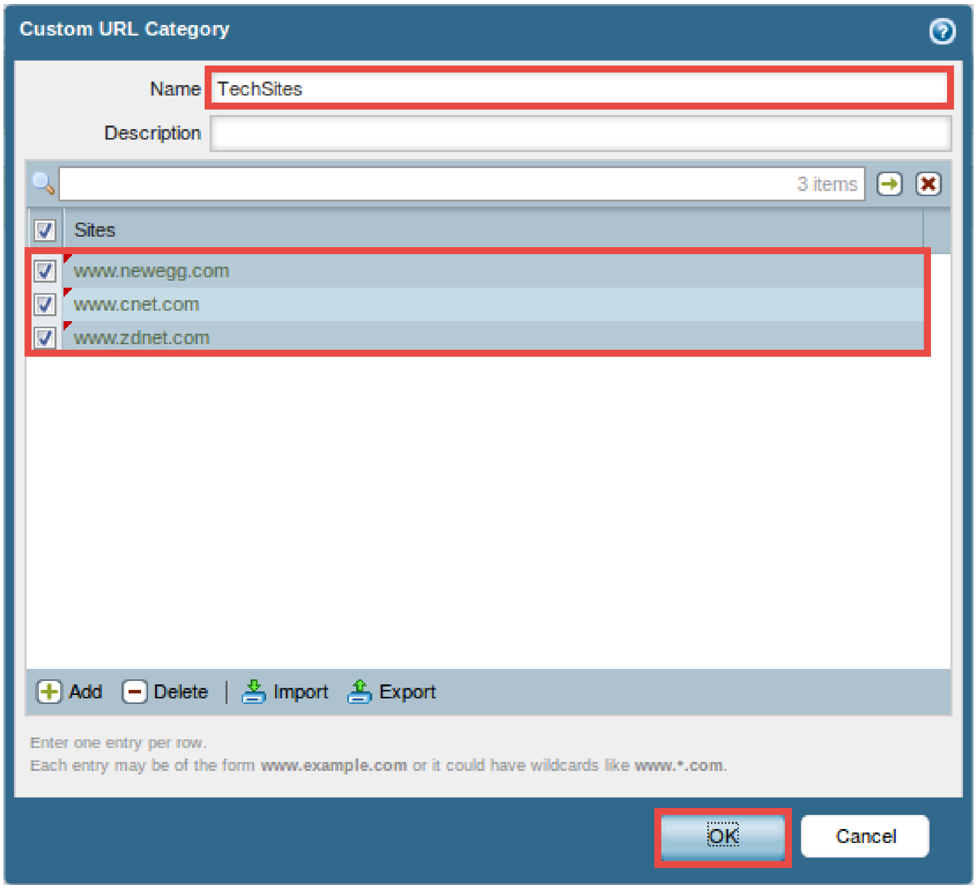


2. Click on **Add**, located near the bottom of the window, to create a custom URL category.



3. In the *Custom URL Category* window, use the information from the table below to fill out the form fields.

Field	Data/Selection
Name	Enter **TechSites**
Sites	Click **Add** and add each of the URLS below: • **www.newegg.com** • **www.cnet.com** • **www.zdnet.com**



Custom URL Category

Name: TechSites

Description:

3 items

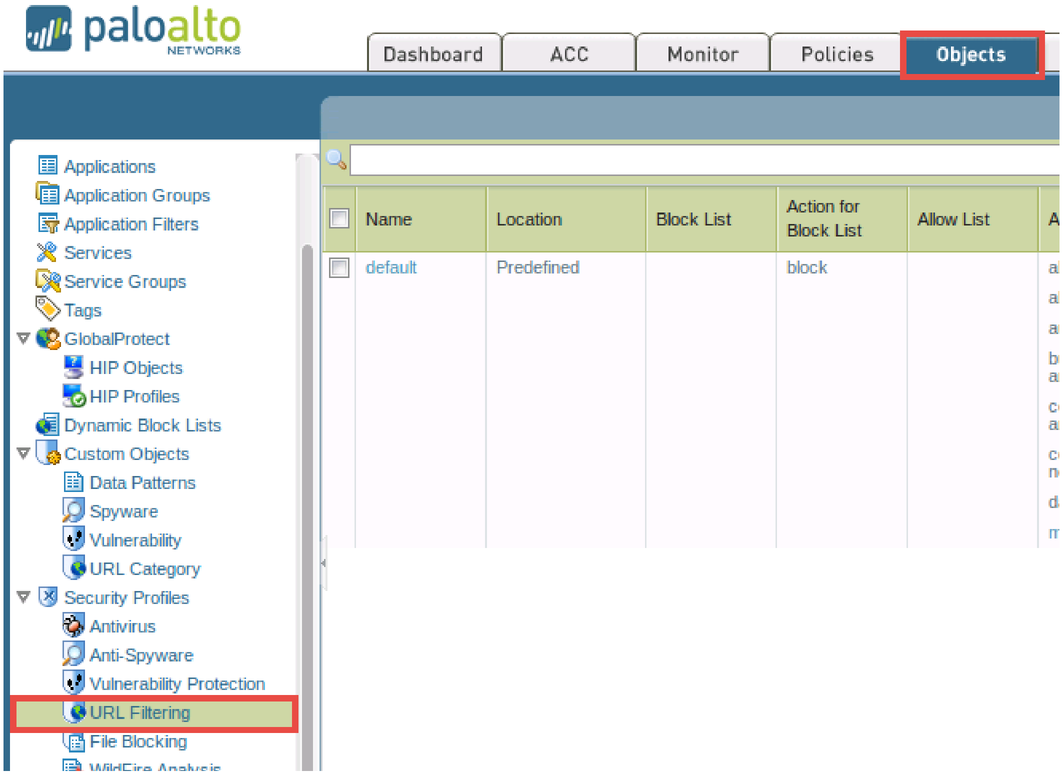
☑	Sites
☑	www.newegg.com
☑	www.cnet.com
☑	www.zdnet.com

Enter one entry per row.
Each entry may be of the form **www.example.com** or it could have wildcards like **www.*.com**.

4. Click **OK** to save changes.
5. Leave the *WebUI* opened to continue with the next task.

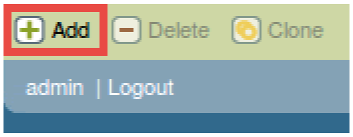
3 Configure a URL Filtering Profile

1. Using the *WebUI*, navigate to **Objects > Security Profiles > URL Filtering**.

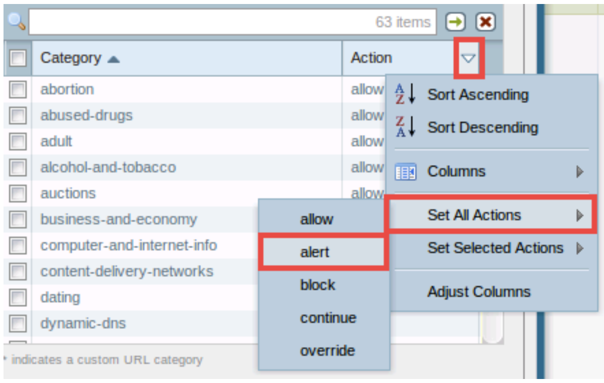


☐	Name	Location	Block List	Action for Block List	Allow List	A
☐	default	Predefined		block		a a a b a c a c n d n

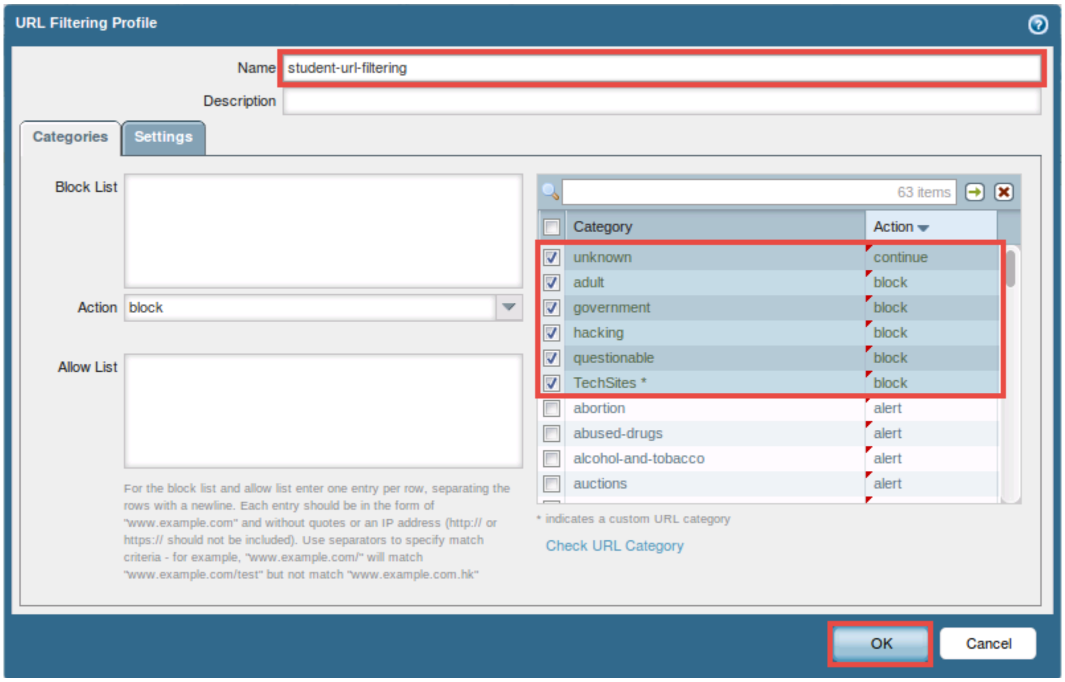
2. Click on **Add**, located near the bottom of the window, to define a URL filtering profile.



3. In the *URL Filtering Profile* window, use the information from the table below to fill the form fields.

Field	Data/Selection
Name	Enter **student-url-filtering**
Sites	Click the right side of the **Action** header to access the pull-down menu. Click **Set All Actions > alert**.  63 items Category Action Sort Ascending Sort Descending Columns Set All Actions Set Selected Actions Adjust Columns allow alert block continue override abortion allow abused-drugs allow adult allow alcohol-and-tobacco allow auctions allow business-and-economy computer-and-internet-info content-delivery-networks dating dynamic-dns * indicates a custom URL category Search the **Category** field for these six categories and set the *Action* to **block** for each except for the unknown category. Set the unknown category to **continue**. • adult (or adult-and-pornography): [Action = **block**] • government: [Action = **block**] • hacking: [Action = **block**] • malware: [Action=**block**] • questionable: [Action = **block**] • TechSites: [Action = **block**] • unknown: [Action = **continue**]

Notice that the *TechSites* category is available due to it being created in *Task 2*.



URL Filtering Profile

Name: student-url-filtering

Description:

Categories | Settings

Block List:

Action: block

Allow List:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

63 items

□	Category	Action
☑	unknown	continue
☑	adult	block
☑	government	block
☑	hacking	block
☑	questionable	block
☑	TechSites *	block
□	abortion	alert
□	abused-drugs	alert
□	alcohol-and-tobacco	alert
□	auctions	alert

* indicates a custom URL category

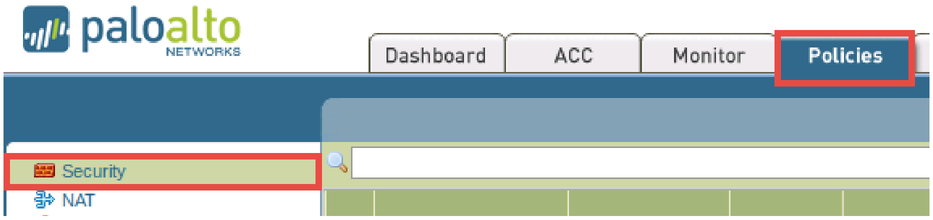
Check URL Category

OK | Cancel

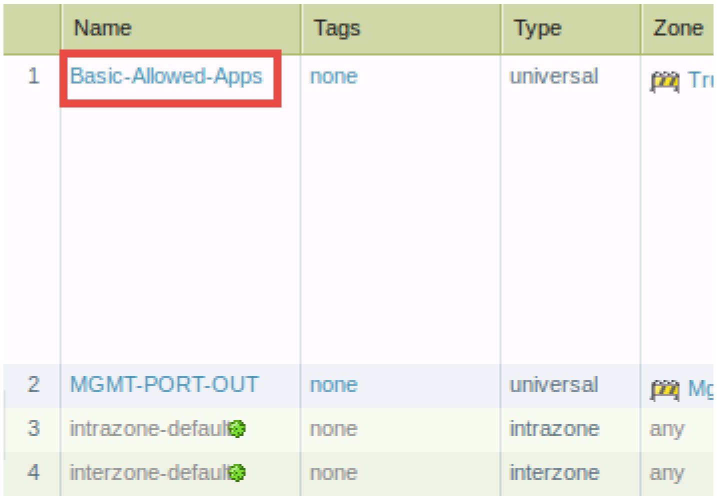
4. Click **OK** to save changes.
5. Leave the *WebUI* opened to continue with the next task.

4 Assign Profiles to a Policy

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



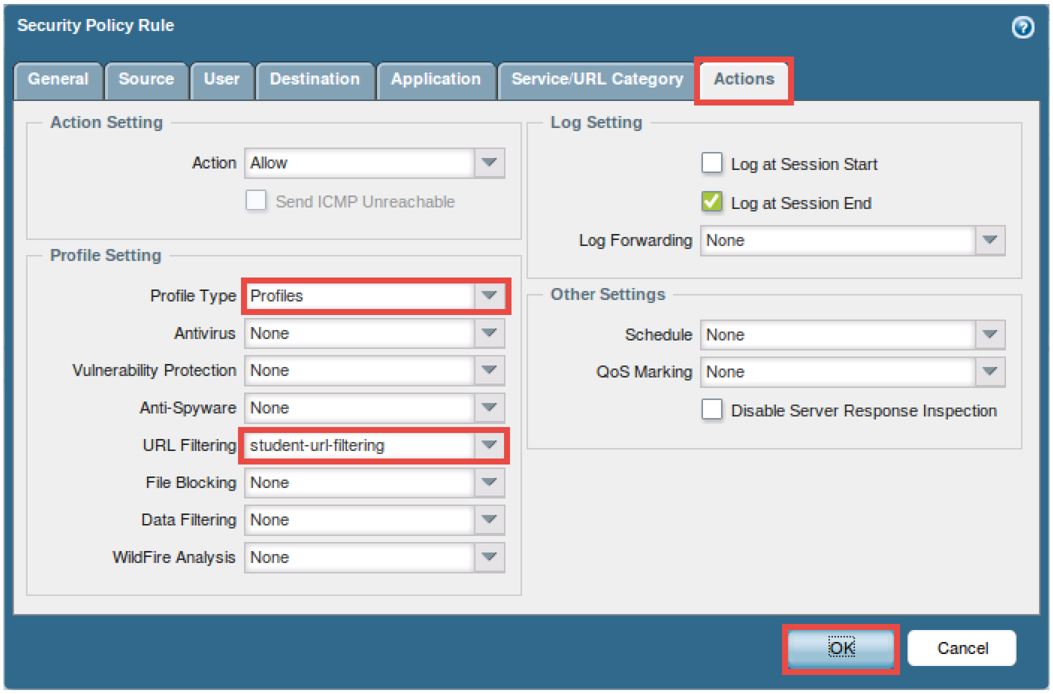
2. Click on **Basic-Allowed-Apps** from the list of policy names.



	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 and use the information from the table below to edit the policy rule to include newly created profiles.

Field	Data/Selection
Profile Type	Select **Profiles**
URL Filtering	Select **student-url-filtering**



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: student-url-filtering

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

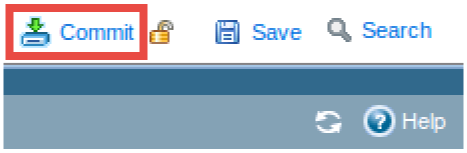
Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

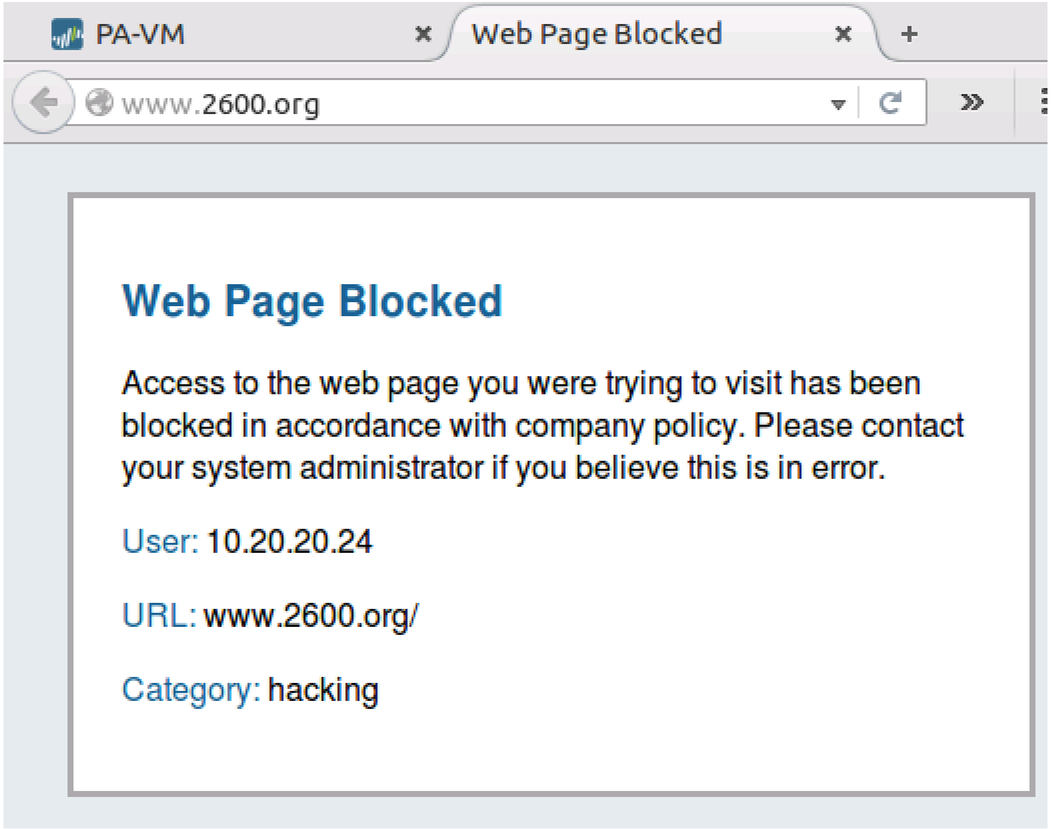
4. Click **OK** to save changes.
5. Click the **Commit** link, located at the top-right of the window.



6. In the *Commit* window, click the **Commit** button.
7. Once the commit process successfully completes, click **Close**.
8. Leave the *Firefox* window opened to continue with the next task.

5 Test the URL Filtering Profile

1. Using the *Firefox* browser, open a **new tab**.
2. In the address field, type **`www.cnn.com`** and press the **Enter** key. Browse to other popular websites such as *Google* and *Yahoo*. The URL filtering profile records each website that is visited by the user.
3. Navigate back to the **first tab**.
4. Using the *WebUI*, navigate to **Monitor > Logs > URL Filtering**.
5. Verify that the log entries track the sites that were just visited.
6. Navigate back to the **second tab**.
7. Test the block condition that was created earlier by visiting a site that is part of *hacking*, *government* or *TechSites* categories. Attempt to browse to **`www.2600.org`**.
8. Notice that the profile in place will block these actions.



Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 10.20.20.24

URL: www.2600.org/

Category: hacking

9. Test the custom category by trying to go to **`www.newegg.com`**.
10. Close the **Desktop 1** PC viewer.