



## **PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES**

### **Lab 14: Quality of Service**

**Document Version: 2016-04-19**

Copyright © 2016 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

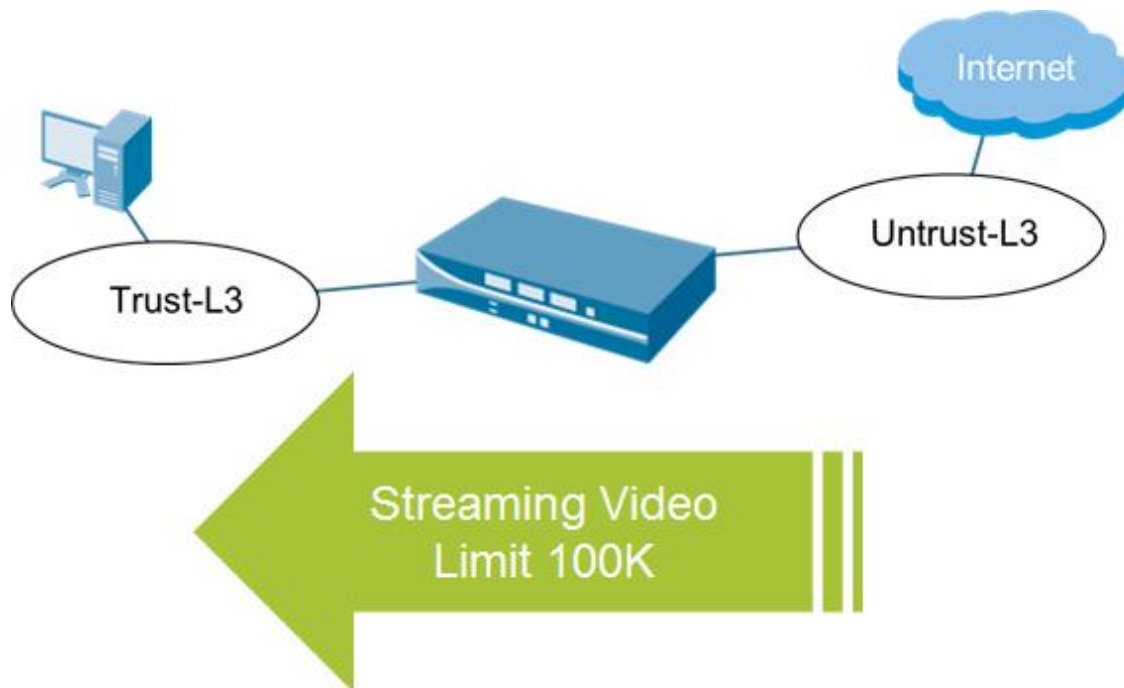
NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

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 Enable and Verify Applications .....	10
3 Define a QoS Profile .....	12
4 Define a QoS Policy .....	14
5 Assign the QoS Profile to an Interface .....	17
6 Test the QoS Policy .....	19

## Introduction



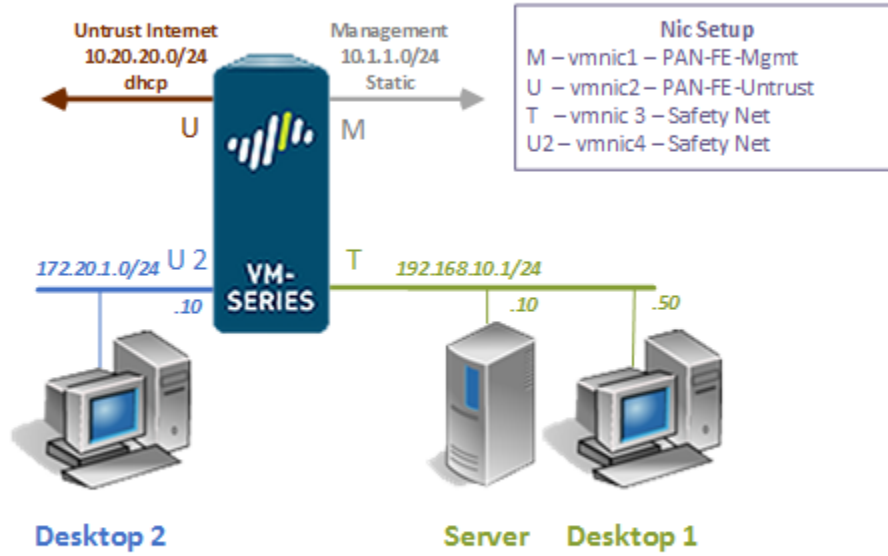
The network-monitoring group reports a high number of sessions using video streaming applications, which is impacting overall network throughput. You have been instructed to allow, but throttle, video streams from the site ustream.tv. You must not completely block the traffic and there should be as minimal impact to other traffic as possible.

## Objective

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

1. Configure QoS

## 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*.



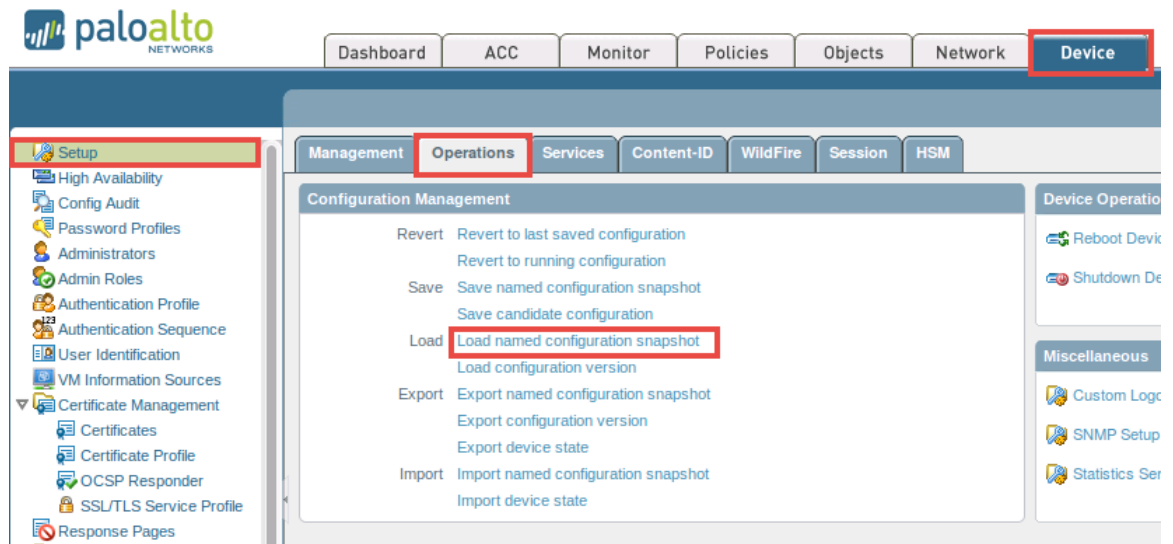
4. In the address field, type **https://192.168.10.1** and press **Enter**.

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.

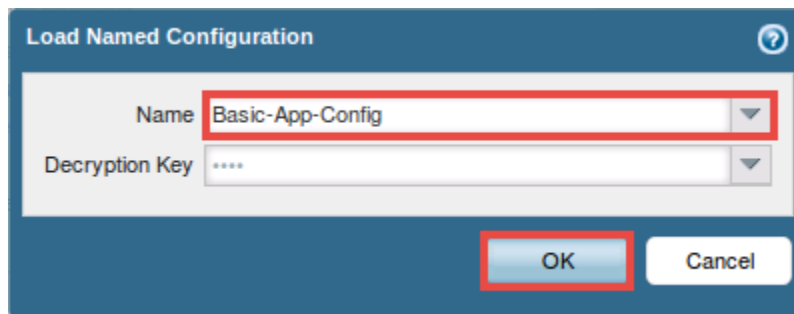
5. Login with the *username* **admin** and *password* **paloalto** on the firewall web interface.



- 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**.

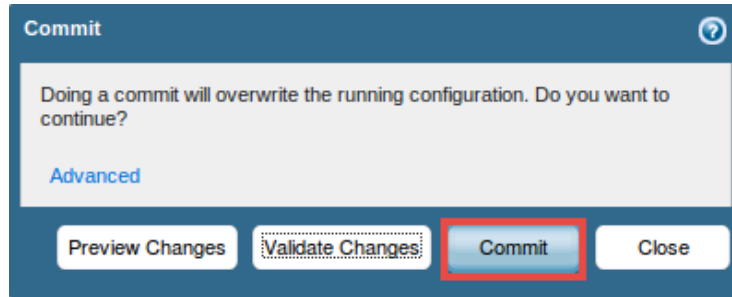


- When prompted with the config loaded message, click on the **Close** button to continue.
- Click on the **Commit** link located at the top-right of the *WebUI*.

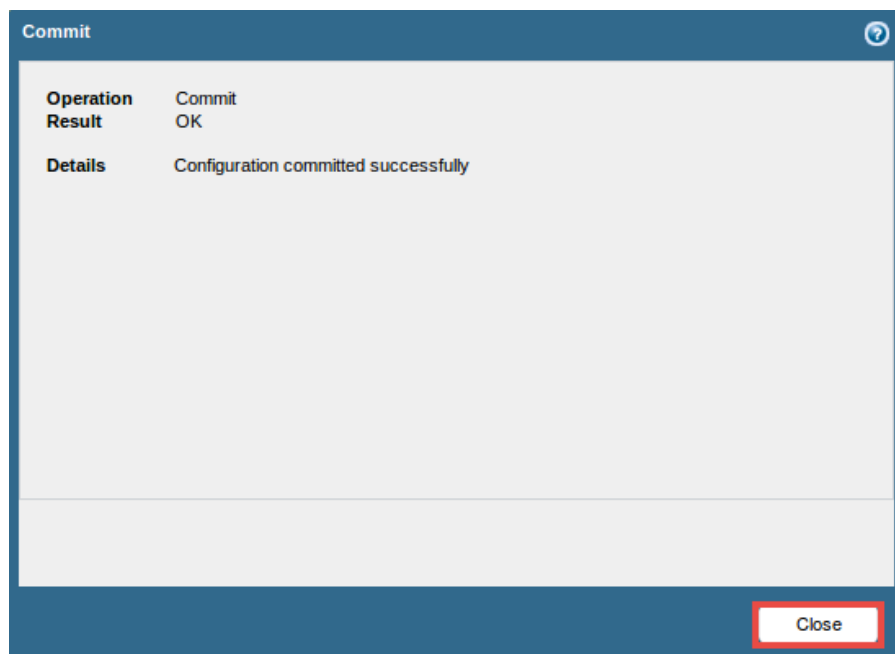




10. In the *Commit* window, click **Commit** to proceed with committing the changes.



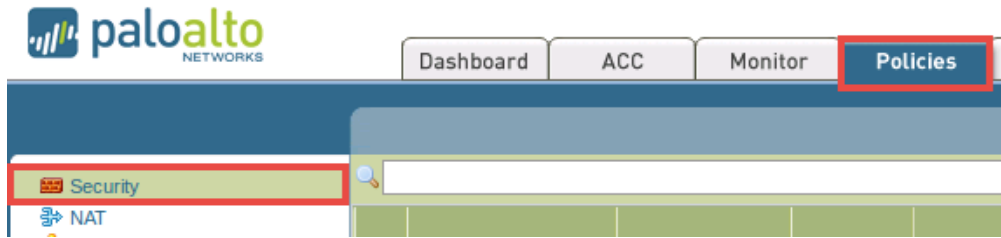
11. Once the operation successfully completes, click **Close** to continue.



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

## 2 Enable and Verify Applications

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

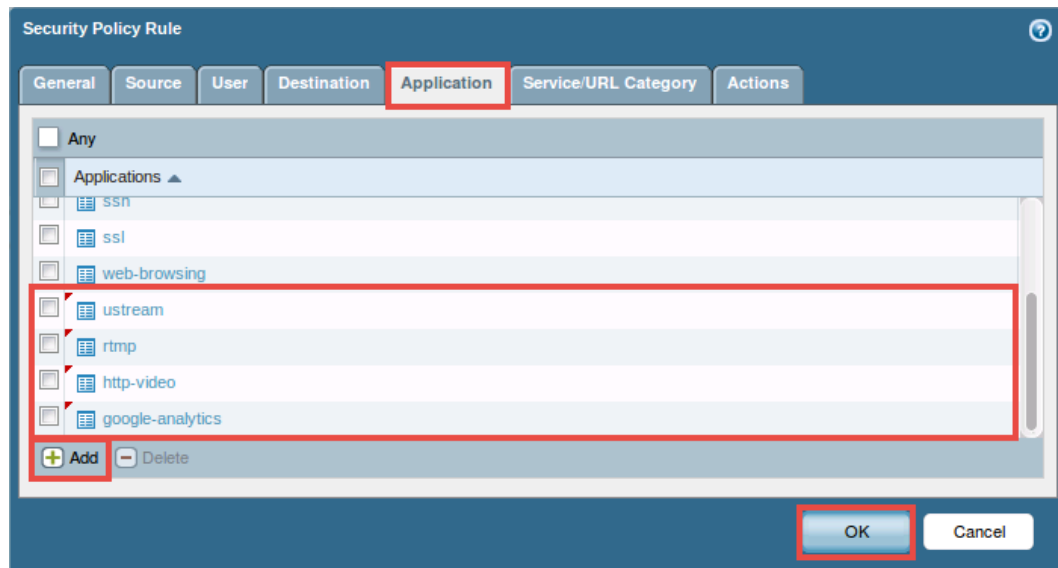


2. Click on the **Basic-Allowed-Apps** link, underneath the *Name* column.

	Name	Tags	Type	Zone
1	<b>Basic-Allowed-Apps</b>	none	universal	Trust-L3
2	MGMT-PORT-OUT	none	universal	Mgmt-L3
3	intrazone-default	none	intrazone	any
4	interzone-default	none	interzone	any

3. In the *Security Policy Rule* window, click on the **Application** tab and use the information from the table below to make the appropriate configurations.

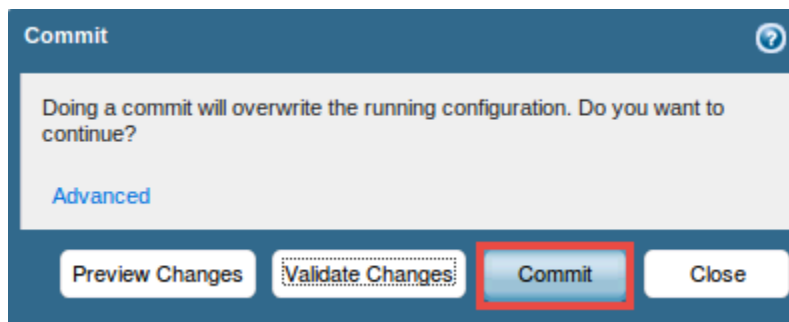
Field	Data/Selection
<i>Applications</i>	Click <b>Add</b> and select the following applications to be added to the list:  <b>ustream</b> <b>rtmp</b> <b>http-video</b> <b>google-analytics</b>



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.



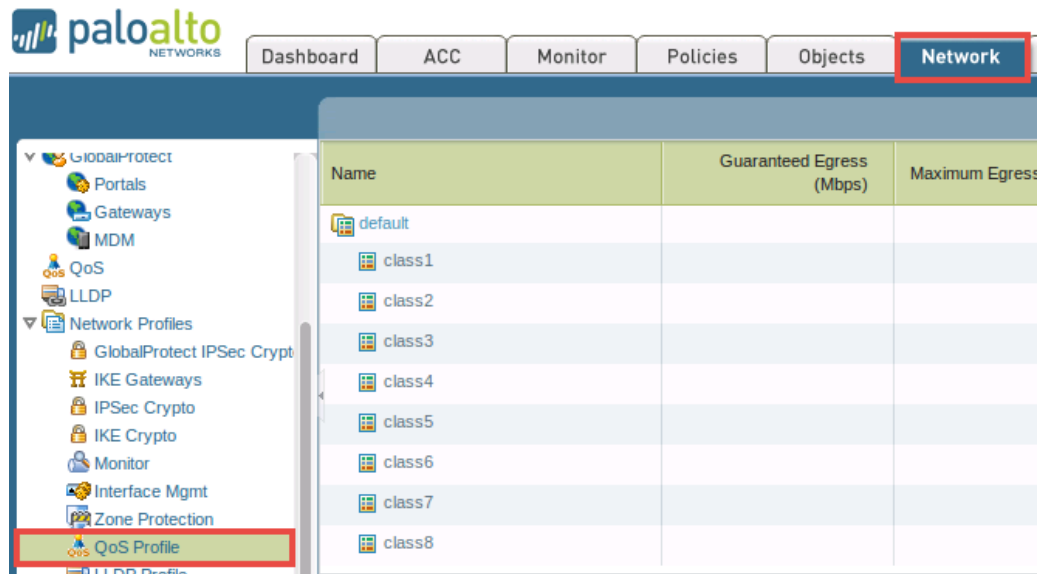
7. Once the operation successfully completes, click **Close** to continue.
8. Open the **Chrome** browser by clicking on its respective icon in the bottom panel.



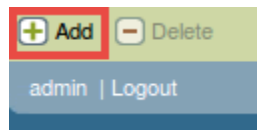
9. In the new browser, enter `http://www.ustream.tv/explore/all` into the address field. Press **Enter**.
10. Once on the *ustream* web page, click on any video to verify that the video can be viewed on the web browser.
11. After playing at least one video, close the **Chrome** web browser.
12. Return to the **Firefox** browser to continue with the next task.

### 3 Define a QoS Profile

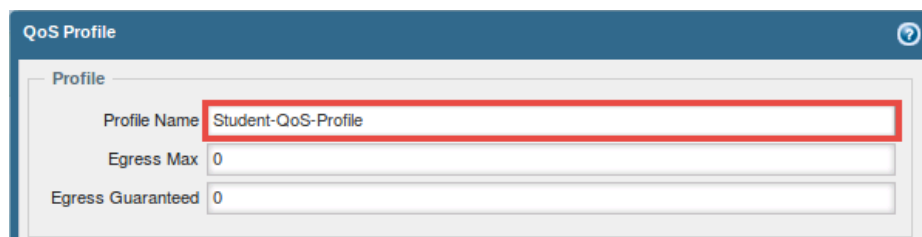
1. Using the *WebUI*, navigate to **Network > Network Profiles > QoS Profile**.



2. Click on **Add**, located near the bottom of the window, to create a new profile.

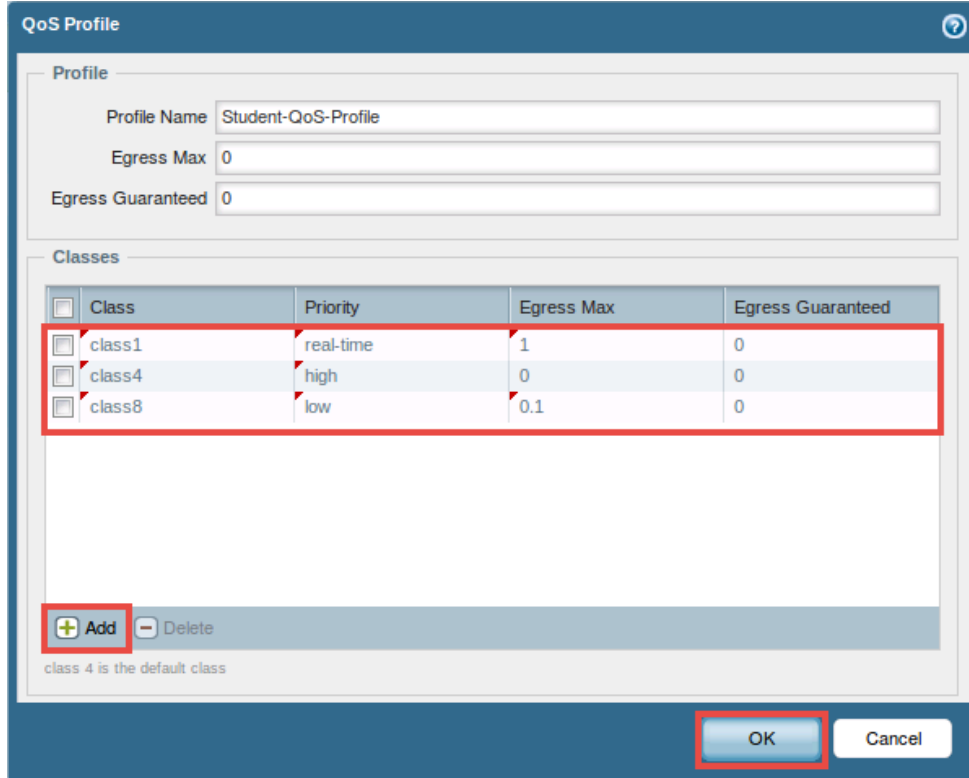


3. In the *QoS Profile* window, enter **Student-QoS-Profile** into the *Profile Name* field.



4. In the *QoS Profile* window, click **Add**.
  - a. Select **class 1** in the *Class* column.
  - b. Select **real-time** in the *Priority* column.
  - c. Enter **1** in the *Egress Max* column.
5. In the *QoS Profile* window, click **Add**.
  - a. Select **class 4** in the *Class* column.
  - b. Select **high** in the *Priority* column.

6. In the *QoS Profile* window, click **Add**.
  - a. Select **class 8** in the *Class* column.
  - b. Select **low** in the *Priority* column.
  - c. Enter 0.1 in the *Egress Max* column.



The screenshot shows the 'QoS Profile' window. The 'Profile' section has 'Profile Name' set to 'Student-QoS-Profile', 'Egress Max' set to 0, and 'Egress Guaranteed' set to 0. The 'Classes' section contains a table with the following data:

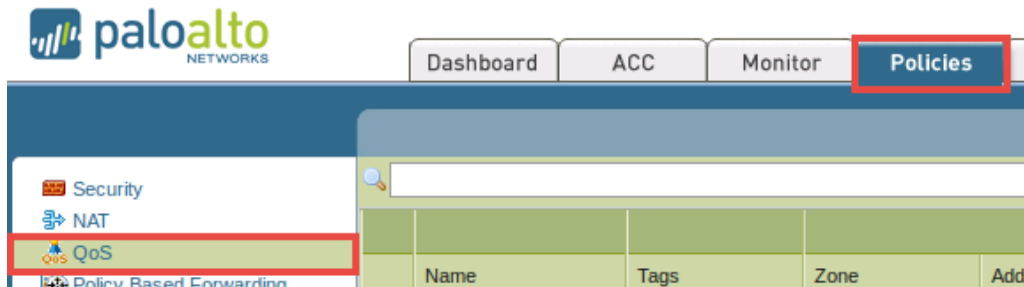
<input type="checkbox"/>	Class	Priority	Egress Max	Egress Guaranteed
<input type="checkbox"/>	class1	real-time	1	0
<input type="checkbox"/>	class4	high	0	0
<input type="checkbox"/>	class8	low	0.1	0

Below the table, there is an 'Add' button (with a plus icon) and a 'Delete' button (with a minus icon). The 'Add' button is highlighted with a red box. At the bottom of the window, there are 'OK' and 'Cancel' buttons, with the 'OK' button also highlighted with a red box. A note at the bottom left states 'class 4 is the default class'.

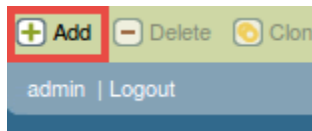
7. Click **OK** to save changes.
8. Verify that the *Student-QoS-Profile* appears in the list.
9. Leave the *WebUI* opened to continue with the next task.

## 4 Define a QoS Policy

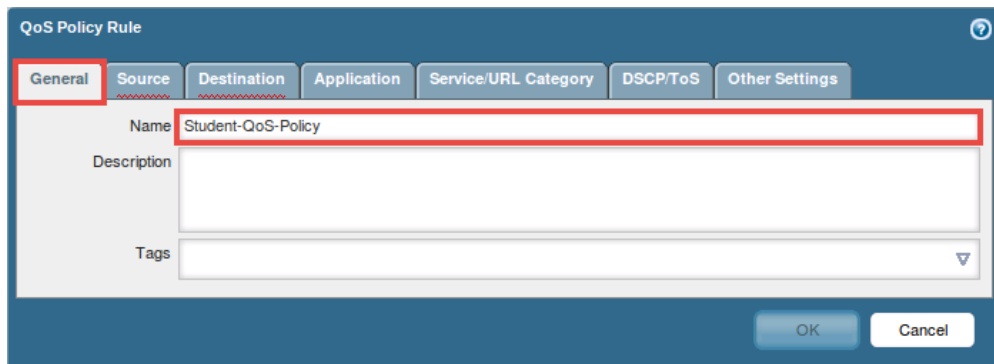
1. Using the *WebUI*, navigate to **Policies > QoS**.



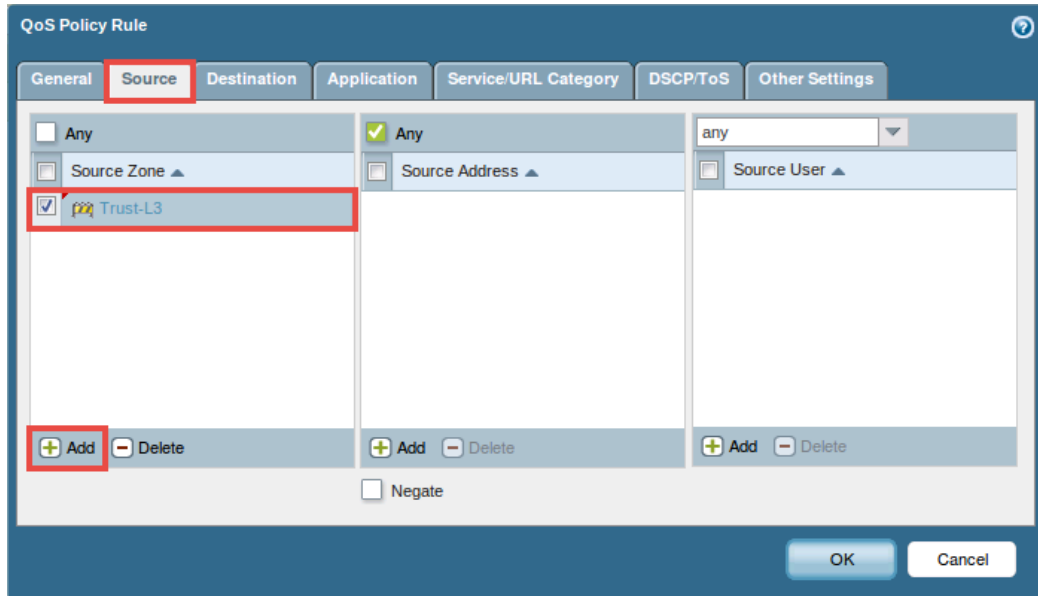
2. Click on **Add**, located near the bottom of the window, to create a new policy.



3. In the *QoS Policy Rule* window, click on the **General** tab and enter **student-QoS-policy** in the *Name* field.

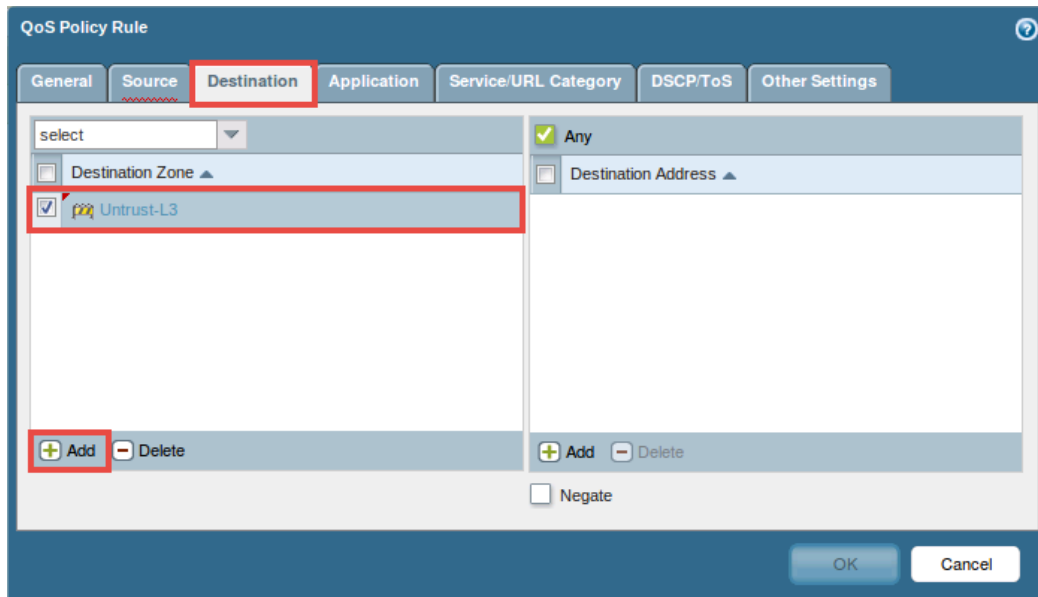


4. In the *QoS Policy Rule* window, click on the **Source** tab and click on the **Add** button, in the *Source Zone* pane, followed by selecting **Trust-L3**.



The screenshot shows the 'QoS Policy Rule' window with the 'Source' tab selected. The 'Source Zone' pane contains a list with 'Trust-L3' selected, indicated by a red box. The 'Add' button at the bottom of the pane is also highlighted with a red box. The 'Source Address' and 'Source User' panes are empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

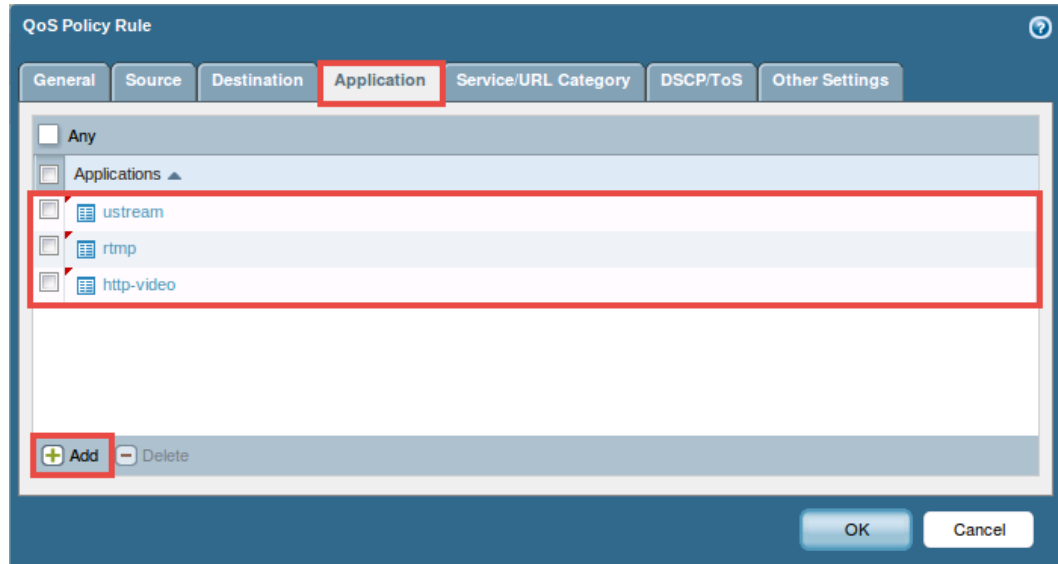
5. In the *QoS Policy Rule* window, click on the **Destination** tab and click on the **Add** button, in the *Destination Zone* pane, followed by selecting **Untrust-L3**.



The screenshot shows the 'QoS Policy Rule' window with the 'Destination' tab selected. The 'Destination Zone' pane contains a list with 'Untrust-L3' selected, indicated by a red box. The 'Add' button at the bottom of the pane is also highlighted with a red box. The 'Destination Address' pane is empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

- In the *QoS Policy Rule* window, click on the **Application** tab and use the information from the table below to make the appropriate configurations.

Field	Data/Selection
<i>Applications</i>	Click <b>Add</b> and select the following applications:  <div> ustream  rtmp  http-video </div>



The screenshot shows the 'QoS Policy Rule' window with the 'Application' tab selected. The 'Applications' list contains 'ustream', 'rtmp', and 'http-video'. The 'Add' button is highlighted with a red box.

- In the *QoS Policy Rule* window, click on the **Other Settings** tab and select **8** from the *Class* drop-down menu.



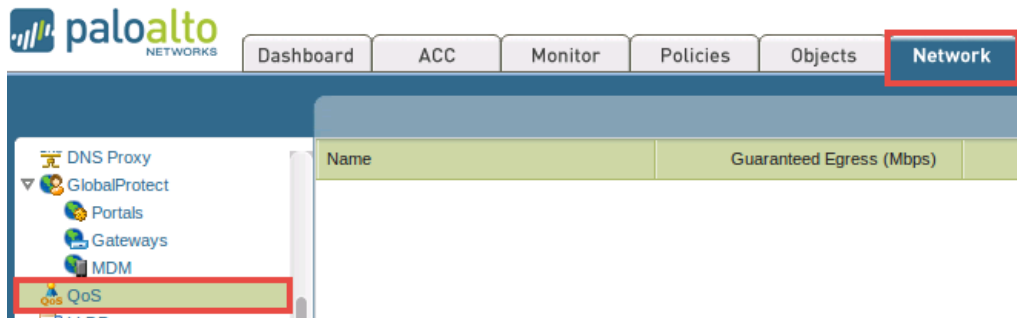
The screenshot shows the 'QoS Policy Rule' window with the 'Other Settings' tab selected. The 'Class' drop-down menu is set to '8'. The 'OK' button is highlighted with a red box.

- Click **OK** to save the configurations.
- Leave the *WebUI* opened to continue with the next task.

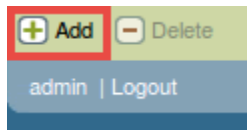


## 5 Assign the QoS Profile to an Interface

1. Using the *WebUI*, navigate to **Network > QoS**.

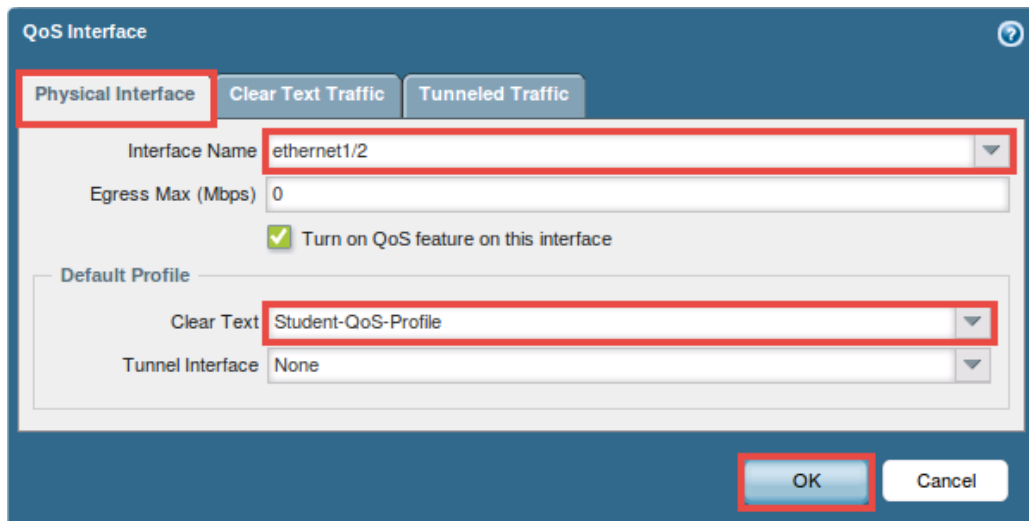


2. Click on **Add**, located near the bottom of the window, to create a QoS definition.



3. In the QoS Interface window, click on the **Physical Interface** tab and use the information from the table below to make the appropriate configurations.

Field	Data/Selection
Interface Name	Select <b>ethernet1/2</b>
Clear Text	Select <b>Student-QoS-Profile</b>

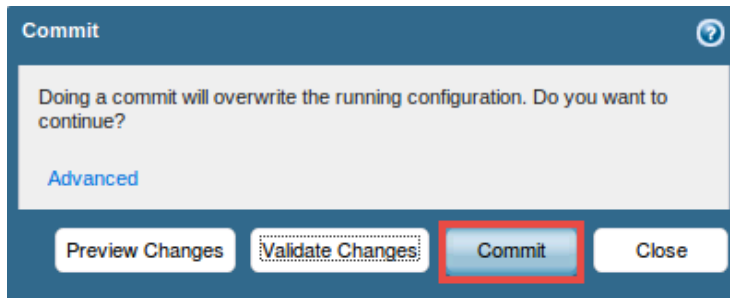


4. Click **OK** to save the configurations.

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.



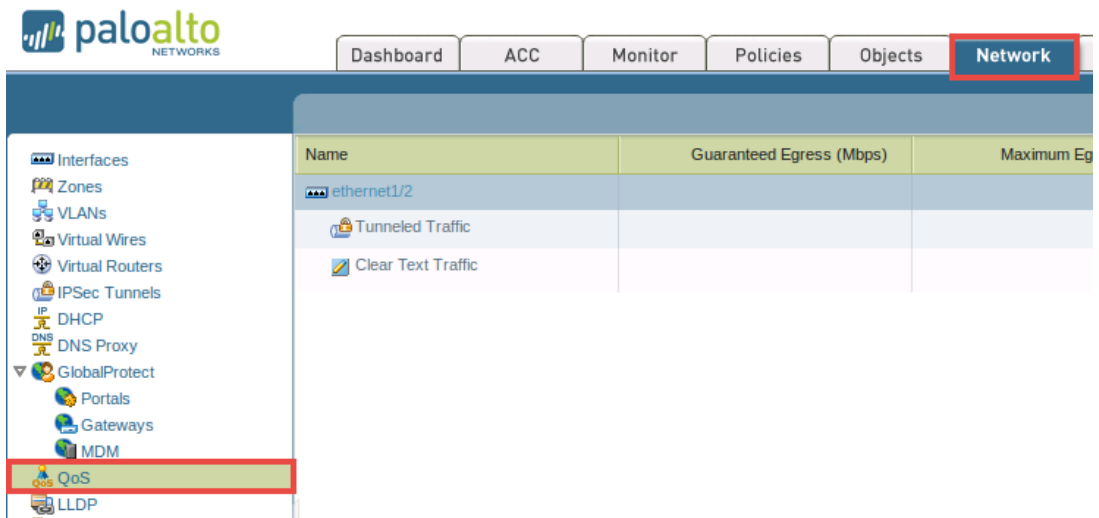
7. Once the operation successfully completes, click **Close** to continue.
8. Leave the *Firefox* web browser opened to continue with the next task.

## 6 Test the QoS Policy

1. Open a new **Chrome** web browser.



2. In the new browser, enter `http://www.ustream.tv/explore/all` into the address field.
3. Play a video by clicking on any video stream to generate traffic.
4. Open a **new tab** in *Chrome*.
5. After a few seconds of playing a video, close the **first tab**.
6. In the new tab, enter `https://192.168.10.1` in the address bar followed by pressing the **Enter** key.
7. If prompted with a “Your connection is not private” message, select **Advanced** followed by clicking on the **Proceed to 192.168.10.1 (unsafe)** link.
8. On the login prompt, login to the firewall as `admin` and password `paloalto`.
9. Select **Network > QoS**.

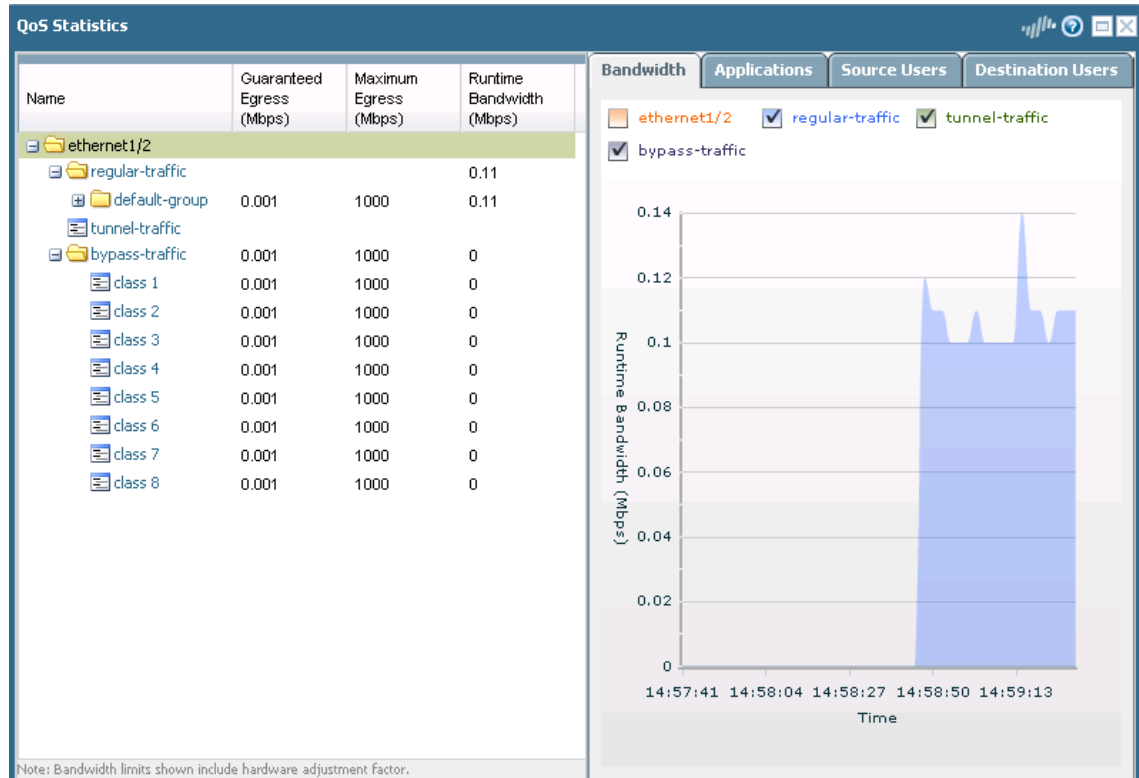


10. Click **Statistics** next to <Egress Interface>.

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	Enabled	
ethernet1/2				✓	Statistics
Tunneled Traffic					
Clear Text Traffic			Student-QoS-Profile		

11. In the *QoS Statistics* window, select **ethernet1/2** from the left pane to review application traffic through this interface. Normally the bandwidth is shaped to stay below the 100 Kbps (.1 Mbps) you set in the profile.

These results may vary depending upon your environment.



12. Close the **QoS Statistics** window.
13. Close **Chrome** to end the video sessions.
14. Close the **Desktop 1** PC viewer.