



Build a Guest Network

Captive Portal
Firewalling

Skills learned

You'll be able to:

- > Create guest-isolating firewall rules
- > Create captive portal ESSes
 - Local authentication
 - RADIUS authentication
- > Add temporary captive portal users

Practice Description

Lab will cover

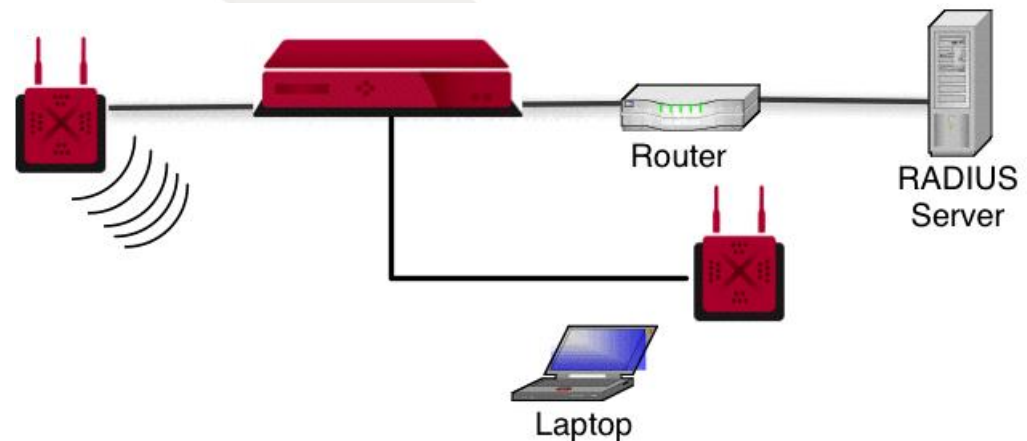
- > Configuring firewall rules
- > Configuring local captive portal users
- > Configuring captive portal authentication

Guest Network Types

> Open access

> Captive portal

- Username/password authentication via https
- Only traffic allowed is ARP, DNS, DHCP
- Can use local or RADIUS authentication



Guest VLANs

> Configured

- Use “Tunnel Type” VLAN

> RADIUS-assigned

- Use “Tunnel Type” RADIUS
- Use Firewall Filter ID
- Licensed Feature

ESS Profile - Update

ESS Profile

ESS-AP Table

Security Profiles

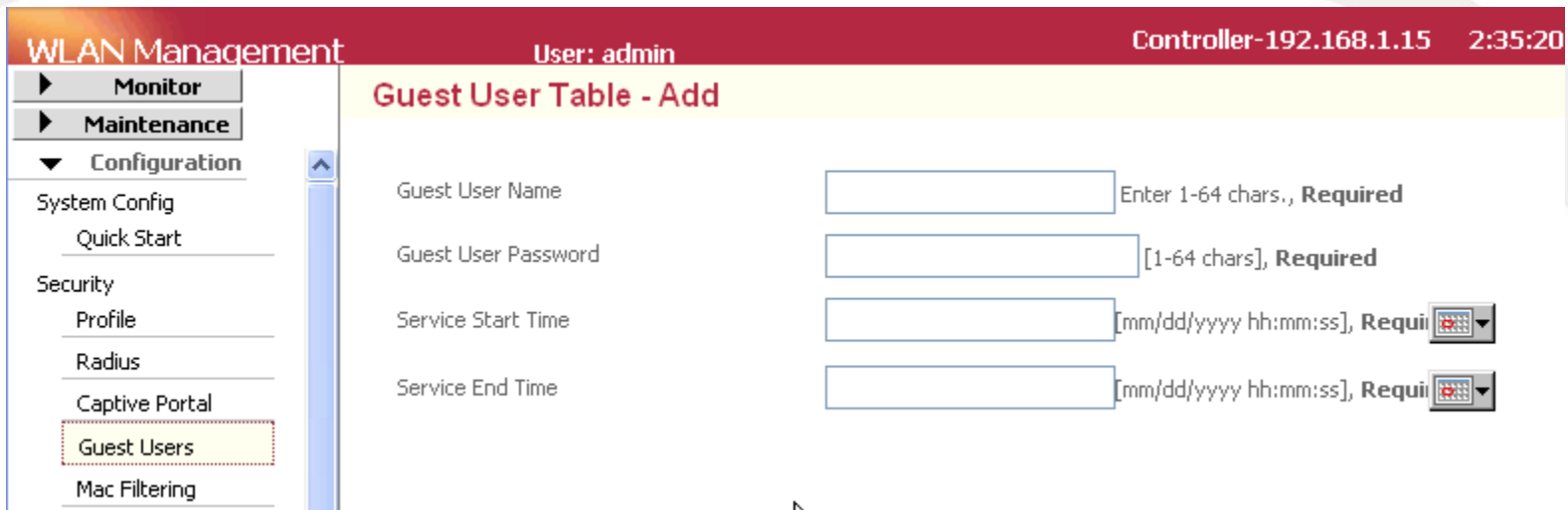
Summary Selection

No	6
ESS Profile Name	helsinki-voice
SSID	helsinki-voice
Security Profile Name	helsinki-voice
Primary RADIUS Accounting Server	No RADIUS
Secondary RADIUS Accounting Server	No RADIUS
Accounting Interim Interval (seconds)	3600 Valid range: [600-36000]
Beacon Interval (msec)	100 Valid range: [0-65520]
SSID Broadcast	On
Bridging	<input type="checkbox"/> AirFortress <input type="checkbox"/> IPV6 <input type="checkbox"/> AppleTalk
New AP's Join ESS	On
Tunnel Interface Type	Configured VLAN Only
VLAN Name	No Tunnel
GRE Tunnel Profile Name	Configured VLAN Only
Allow Multicast Flag	RADIUS VLAN Only
Silent Client Polling	RADIUS And Configured VLAN
Enable Virtual Cell	GRE
WMM Support	Off
DTIM Period (number of beacons)	On
Virtual Cell Type	Off
Dataplane Mode	1 Valid range: [1-255]
B Supported Transmit Rates (Mbps)	Per Station BSSID
	Tunneled
	<input checked="" type="checkbox"/> 1 Mbps <input checked="" type="checkbox"/> 2 Mbps <input checked="" type="checkbox"/> 5.5 Mbps <input checked="" type="checkbox"/> 11 Mbps

Creating Local CP Users

> Up to 32 local users

- Guest User name
- Guest Password
- Start time
- End time



The screenshot displays the 'WLAN Management' web interface. The top navigation bar includes 'Monitor', 'Maintenance', and 'Configuration'. The 'Configuration' menu is expanded, showing options like 'System Config', 'Quick Start', 'Security', 'Profile', 'Radius', 'Captive Portal', 'Guest Users' (highlighted), and 'Mac Filtering'. The main content area is titled 'Guest User Table - Add' and contains four input fields: 'Guest User Name' (with a hint 'Enter 1-64 chars., Required'), 'Guest User Password' (with a hint '[1-64 chars], Required'), 'Service Start Time' (with a hint '[mm/dd/yyyy hh:mm:ss], Required' and a calendar icon), and 'Service End Time' (with a hint '[mm/dd/yyyy hh:mm:ss], Required' and a calendar icon). The interface also shows the user 'admin' and the controller IP '192.168.1.15'.

QoS System: Firewalling and Rate Policing

> Configuration is a 3-step process

- Selection
 - Static ranges
 - ESS-based
 - Per-group “firewall”
- Action
- Apportion

QoS and Firewall Rules - Add

		Match	Flow Class
ID	<input type="text"/> Valid range: [0-6000], Required	<input type="button" value="On"/>	
Destination IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>		
Destination Port	<input type="text"/> Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>		
Source Port	<input type="text"/> Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	<input type="text"/> Valid range: [0-255], Required	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID	<input type="text"/> Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	<input type="text"/> Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	<input type="text"/> Valid range: [0-1500]		
QoS Protocol	<input type="text"/> SIP		
Average Packet Rate	<input type="text"/> Valid range: [0-200]		
Action	<input type="text"/> CAPTURE		
Drop Policy	<input type="text"/> Tail		
Token Bucket Rate	<input type="text"/> Valid range: [0-1000000]		
Priority	<input type="text"/> Valid range: [0-8]		
Traffic Control	<input type="text"/> Off		

QoS Selection

- > Match checkboxes
 - Unchecked = wild card
- > Need at least one address range selected for rule to be created

QoS and Firewall Rules - Add

		Match	Flow Class
ID	<input type="text"/> Valid range: [0-6000], Required	On ▾	<input type="checkbox"/>
Destination IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination Port	<input type="text"/> Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source Port	<input type="text"/> Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	<input type="text"/> Valid range: [0-255], Required	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID	<input type="text"/> Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	<input type="text"/> Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	<input type="text"/> Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>

SELECTION

QoS Protocol	SIP ▾
Average Packet Rate	<input type="text"/> Valid range: [0-200]
Action	CAPTURE ▾
Drop Policy	Tail ▾
Token Bucket Rate	<input type="text"/> Valid range: [0-1000000]
Priority	<input type="text"/> Valid range: [0-8]
Traffic Control	Off ▾

QoS Action

- > QoS treatment
- > Drop/
Forward/
Capture
- > Rate Policing

QoS and Firewall Rules - Add

		Match	Flow Class
ID	<input type="text"/> Valid range: [0-6000], Required	On ▾	
Destination IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>		
Destination Port	<input type="text"/> Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>		
Source Port	<input type="text"/> Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	<input type="text"/> Valid range: [0-255], Required	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID	<input type="text"/> Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	<input type="text"/> Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	<input type="text"/> Valid range: [0-1500]		

QoS Protocol	SIP ▾
Average Packet Rate	<input type="text"/> Valid range: [0-200]
Action	CAPTURE ▾
Drop Policy	Tail ▾
Token Bucket Rate	<input type="text"/> Valid range: [0-1000000]
Priority	<input type="text"/> Valid range: [0-8]
Traffic Control	Off ▾

ACTION

QoS Apportion

- > “Flow Class”
On/Off
- > Flow Class
checkboxes
 - Unchecked = wild
card

QoS and Firewall Rules - Add

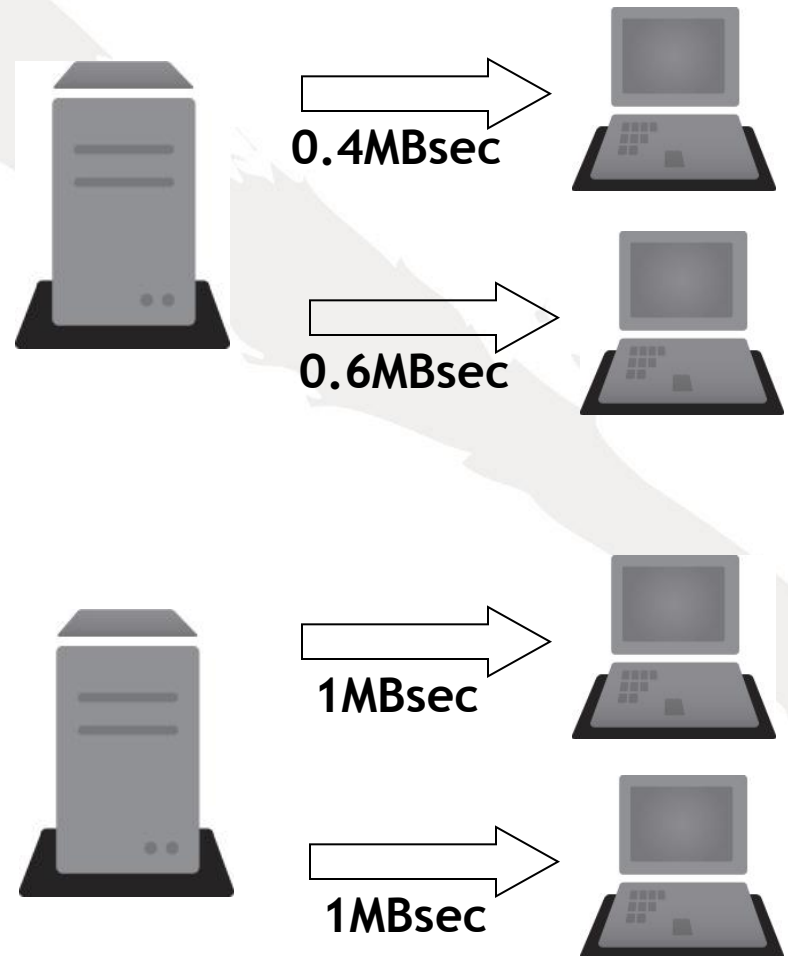
ID	<input type="text"/>	Valid range: [0-6000], Required	Match	Flow Class
Destination IP	<input type="text"/>		<input type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	<input type="text"/>		<input type="checkbox"/>	<input type="checkbox"/>
Destination Port	<input type="text"/>	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	<input type="text"/>		<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	<input type="text"/>		<input type="checkbox"/>	<input type="checkbox"/>
Source Port	<input type="text"/>	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	<input type="text"/>	Valid range: [0-255], Required	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID	<input type="text"/>	Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	<input type="text"/>	Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	<input type="text"/>	Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>

APPORTION

QoS Protocol	<input type="text"/>	
Average Packet Rate	<input type="text"/>	Valid range: [0-200]
Action	<input type="text"/>	
Drop Policy	<input type="text"/>	
Token Bucket Rate	<input type="text"/>	Valid range: [0-1000000]
Priority	<input type="text"/>	Valid range: [0-8]
Traffic Control	<input type="text"/>	

Apportion Example

- > Rate policing: limiting source to 1MBsec
- > Rate policing: limiting destination to 1MBsec



Firewall Rules – Example 1

QoS and Firewall Rules - Add

			Match	Flow Class
ID	40	Valid range: [0-6000], Required	On ▾	
Destination IP	192.168.14.0		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	255.255.255.0			
Destination Port	0	Valid range: [0-65535]	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Source IP	0.0.0.0		<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	0.0.0.0			
Source Port	0	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	0	Valid range: [0-255]	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID		Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	0	Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	0	Valid range: [0-1500]		
QoS Protocol	SIP ▾			
Average Packet Rate	0	Valid range: [0-200]		
Action	DROP ▾			
Drop Policy	Tail ▾			
Token Bucket Rate	0	Valid range: [0-1000000]		
Priority	0	Valid range: [0-8]		
Traffic Control	Off ▾			
DiffServ Codepoint	DiffServ Disabled ▾			

Firewall Rules – Example 2

QoS and Firewall Rules - Add

			Match	Flow Class
ID	50	Valid range: [0-6000], Required	On ▾	
Destination IP	192.168.14.0		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	255.255.255.0			
Destination Port	0	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	0.0.0.0		<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	0.0.0.0			
Source Port	0	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	6	Valid range: [0-255]	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID		Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	0	Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	0	Valid range: [0-1500]		
QoS Protocol	SIP ▾			
Average Packet Rate	0	Valid range: [0-200]		
Action	DROP ▾			
Drop Policy	Tail ▾			
Token Bucket Rate	0	Valid range: [0-1000000]		
Priority	0	Valid range: [0-8]		
Traffic Control	Off ▾			
DiffServ Codepoint	DiffServ Disabled ▾			

Firewall Rules – Example 3

QoS and Firewall Rules - Add

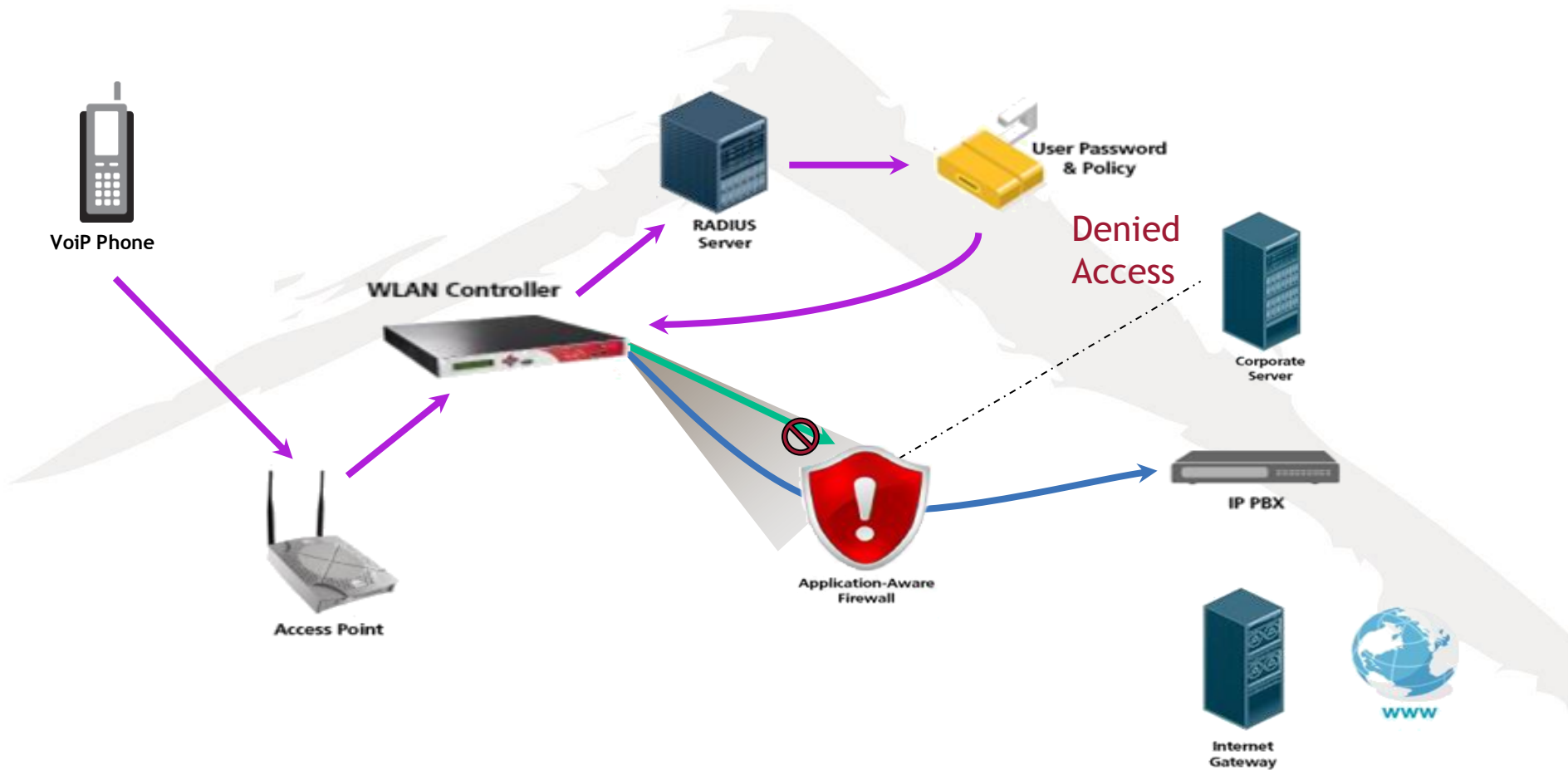
			Match	Flow Class
ID	60	Valid range: [0-6000], Required	On ▾	
Destination IP	192.168.14.0		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	255.255.255.0			
Destination Port	0	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	192.168.14.0		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Source Netmask	255.255.255.0			
Source Port	0	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	6	Valid range: [0-255]	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID		Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	0	Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	0	Valid range: [0-1500]		
QoS Protocol	none ▾			
Average Packet Rate	0	Valid range: [0-200]		
Action	DROP ▾			
Drop Policy	Tail ▾			
Token Bucket Rate	0	Valid range: [0-1000000]		
Priority	0	Valid range: [0-8]		
Traffic Control	Off ▾			
DiffServ Codepoint	DiffServ Disabled ▾			

Firewall Rules – Example 4

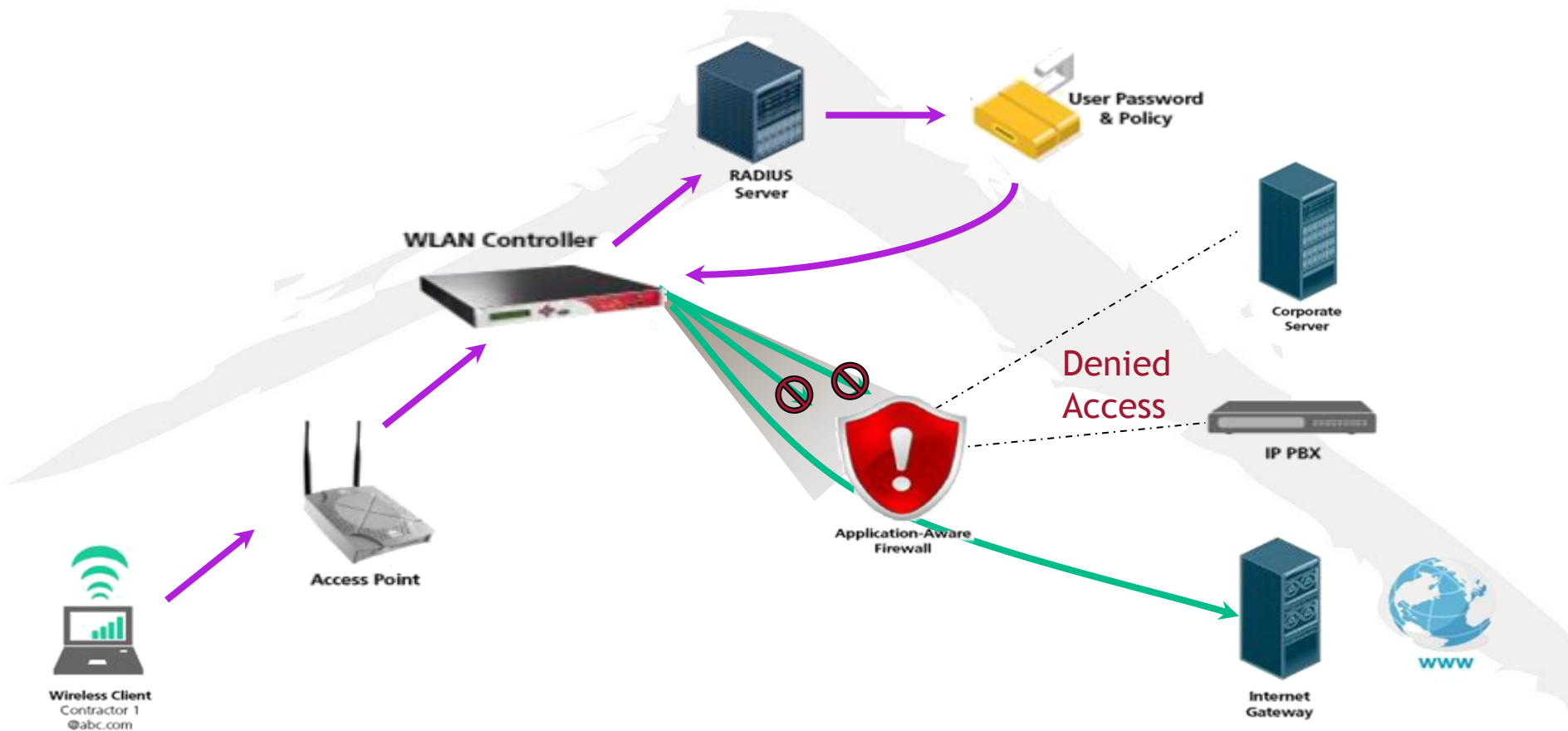
QoS and Firewall Rules - Add

			Match	Flow Class
ID	70	Valid range: [0-6000], Required	On	
Destination IP	192.168.14.0		<input type="checkbox"/>	<input checked="" type="checkbox"/>
Destination Netmask	255.255.255.0			
Destination Port	0	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	0.0.0.0		<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	0.0.0.0			
Source Port	0	Valid range: [0-65535]	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	17	Valid range: [0-255]	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Firewall Filter ID		Enter 0-16 chars.	<input type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	0	Valid range: [0-1500]	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	0	Valid range: [0-1500]		
QoS Protocol	none			
Average Packet Rate	0	Valid range: [0-200]		
Action	FORWARD			
Drop Policy	Tail			
Token Bucket Rate	1000000	Valid range: [0-1000000]		
Priority	0	Valid range: [0-8]		
Traffic Control	On			
DiffServ Codepoint	DiffServ Disabled			

PEM: Per-ESS Firewall Policies



PEM: Per-Group Firewall Policies



Lab Preview

- > Configuring local captive portal users
- > Configuring captive portal authentication
 - Local
 - RADIUS
- > Configuring firewall rules
 - Add firewall rules to previous test network
 - Add VLAN
 - Add firewall rules

Demonstration: Creating a Firewall Rule