

WiNG 5 Feature Guide

Role Based Firewall

Published: April 2017

Extreme Networks, Inc. Phone / +1 408.579.2800 Toll-free / +1 888.257.3000

www.extremenetworks.com

© 2017 Extreme Networks, Inc. All rights reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks.

Contents

Introduction	3
Overview	. 3
Distributed Stateful Inspection	. 4
Role Based Firewall	. 5
Components	. 6
Web UI Role-Policy Options	6
CLI Role-Policy Options	7
Use and Configuration	. 8
Scenario 1 – Match based on SSID	. 8
IP ACL and Application Policy Configuration	8
Role Policy Configuration	12
Applying Role Policy	16
Scenario 2 – Match based on the User Group	. 17
External RADIUS Configuration (Microsoft Network Policy Server)	17
AAA Policy Configuration	37
Application Policy Configuration	40
WLAN Configuration	41
Role Policy Configuration	43
Scenario 3 – Match based on Client Identity (DHCP Fingerprinting)	. 48
Client Identity Configuration	48
IP Access List and Application Policy Configuration	52
WLAN Configuration	55
Role Policy Configuration	56
Verification	61
Role Statistics - Web UI	. 61
Role Statistics - CLI	. 62
Troubleshooting	64
Role Assignment Debugging –Remote Debug Wireless	. 64
EAP-TLS client example, notice received User Group id highlighted:	64
Guest SSID client example:	65
Client Identity a.k.a DHCP Fingerprinting Debugging	. 65

Introduction

To augment the firewall services of WiNG 5, one may enable role-based firewall functionality to gain the most granular security filtering and policing based on the user role.

Role-based firewall gives enhanced security to the standard firewall features of WiNG 5. Whereas the standard IP/MAC or Application based firewall rules are applied to physical and logical interfaces as well as WLANs, role-based rules are applied to the wireless clients and follow them as they roam on the network based on various matching criteria.

For further information on the standard Firewall features of WiNG 5, please see the "*WiNG5 Firewall How To*" document.

Overview

Roles allow for dynamic assignment of IP/MAC firewall rules or Application Policies to wireless clients based on one or more match conditions that are evaluated when the client associates to the wireless network. These dynamic rules follow the clients, being migrated to other access points as the clients roam. If a role is established that would affect already connected clients, these roles will be evaluated immediately and put into effect against the client traffic.

Match criteria include:

Location: AP or group of AP's the wireless client is connected to

Authentication: The authentication method used by the client during association, i.e. EAP vs MAC-Auth vs Kerberos vs None

Encryption: The encryption type used by the client (not configured on the WLAN)

Group Membership: The local group the wireless client is assigned to as obtained from

AAA server or LDAP server.

LDAP attributes: emailid, employeeid, country, company, i.e. anything that can be returned back by an LDAP server.

Captive Portal Authentication State: post-login or pre-login

Client Identity: Based on DHCP fingerprint

MAC Address: MAC address or range of the wireless client(s)

SSID: The SSID the wireless client is associated to

Distributed Stateful Inspection

The major feature in WiNG 5 is distribution of services or services at the edge. Since controllers and access points alike run the same OS and thus feature set, processing of traffic for various services is pushed to the edge where it can be performed in real-time and done so dynamically.



The distributed nature of the firewall allows stateful flows to migrate with clients as they roam between access points. Rules are made up of one or more traffic matching conditions, for which an action is then performed (permit, deny, mark, log). As is the case with firewalls, at least one permit action must be met in order for traffic to be forwarded and at the end of a rule set, there is an implied deny for all traffic not meeting a match condition.

Role Based Firewall

Roles based firewall was designed to meet the security needs of the mobile enterprise



It is possible from time to time that while a role is being evaluated, multiple matches may be found. In this case, the role with the lowest precedence will be assigned to the wireless client.

For each user role administrators can define match criteria and values that can individually be ignored, matched and partially matched. For example a group name could be defined in a user role to exactly match the value Sales which would apply to all users in the Sales group. Likewise an ESSID could be defined to partially match the value Corp which would match any devices associated with the ESSIDs named CorpUsers and CorpGuest. Alternatively specific strings can be ignored by selecting a match of Not Contains or all criteria can be matched using a match condition **Any**.

Components

The components of role-based firewall are listed below:

- 1. Firewall Rules (Access Control Lists)
 - IPv4 Firewall Rules
 - IPv6 Firewall Rules
 - MAC Firewall Rules
- 2. Application Rules (Application Policy)
- 3. Bonjour Services Rules (Bonjour Discovery Policy)
- 4. Rate-Limiting (from/to client)
- 5. VLAN Assignment
- 6. Wireless Client Roles (Role-policy)
- 7. AAA Policy (optional based on match criteria)

Web UI Role-Policy Options

WiNG v5.8	[Dashboard Configu	ration Diagnostics Op	perations Statistics			 &	admin 🧗	
Devices Wireless Netw	ork	Profiles RF Domains	Security Services 1	Management		5 Revert	📥 Commit 🕴	금 Commit and Sav	/e
= 🚳 Wireless Firewall	R	ble Policy firewalled-use	ers					(5
🚃 Firewall Policy				L DAD Settinge	lee Default Firewall Dulee			-	
MAC ACL				LUAF Settings					
💶 🎅 IP Firewall	Co	onfiguration							
🙎 Wireless Client Roles		LDAP Query 🛛 📄 💿 Inte	rnal (Self) 🔘 Through Wireless C	ontroller					
Device Fingerprinting		Dead Period n 100	(60 to 300)						
🖸 🌄 Intrusion Prevention		•	(
🔂 EX3500 Time Range		Timeout (1 to 5)						
Map: Profile 💌	LC	AP Server Options		1	1				
Vient Roles	Ţ	Serverld	Host	Bind DN	Base DN	Bind Password	Port	1	
🕨 🎭 Unmapped	- *								
A firewalled-users									

CLI Role-Policy Options

vx9000#conf t

<pre>vx9000(config) #role commands:</pre>	e-policy firewalled-users vx9000(config-role-policy-firewalled-users)#? Role Policy Mode
Role Policy Mode co	ommands:
default-role	Configuration for Wireless Clients not matching any role
ldap-deadperiod	Ldap dead period interval
ldap-query	Set the ldap query mode
ldap-server	Add a ldap server
ldap-timeout	Ldap query timeout interval
no	Negate a command or set its defaults
user-role	Create a role
clrscr	Clears the display screen
commit	Commit all changes made in this session
do	Run commands from Exec mode
end	End current mode and change to EXEC mode
exit	End current mode and down to previous mode
help	Description of the interactive help system
revert	Revert changes
service	Service Commands
show	Show running system information
write	Write running configuration to memory or terminal

Use and Configuration

We will examine three scenarios throughout this guide; an easy method based on SSID followed by a slightly more complex method based on the user's group assignment, lastly a more granular role separation based on device OS type and version using DHCP fingerprinting.

During the configuration of the role-policy, the necessary IP or MAC access lists will be specified, so it is helpful to have these created already. Thus, following is a preferred order of configuration. This assumes that the general configuration of the controller and necessary WLAN's already exist. In the case of our second scenario, this document will also include the configuration of AAA and WLAN policies.

- 1. Configure IP / MAC based access lists
- 2. Configure Application Policies
- 3. Configure the Role-policy, define User Roles
- 4. Apply the role-policy to the device(s)

Scenario 1 - Match based on SSID

IP ACL and Application Policy Configuration

In the below example we will create an ACL named "**guest-users**", which allows DHCP, DNS, HTTP and HTTPS traffic going out to the internet, as well as traffic destined to the Captive Portal. Finally, we are going to drop any other IP traffic and also log drop hits. As a next step we will create an Application Policy that enforces restriction upon dynamic web-based applications that are difficult to track using standard ACLs. Note that Application Policy requires an Access Point to support DPI engine.

For the Web UI configuration navigate to "**Configuration** > **Security** > **IP Firewall Rules**" (or MAC Firewall Rules is so inclined). Click on "**Add**"

1. Web UI Creating New IPv4 ACL

WiNG v5.8	Dashbo	Configu)iagno	Operati	Statistics 🔍 🛚	9600 🔻	1111 -	k admin 💦
Devices Wireless	Network Profiles	RF Domains	Security	Services	Management	5 Revert	📥 Commit	🔚 Commit and Save
a 🌄 Wireless Firewall	IPv4 Firewall Rule	s						0
🧱 Firewall Policy	IP Firewall Policy							(4)
MAC ACL	BROADCAST-MULTICA	ST-CONTROL						
🗖 🅎 IP Firewall	guest-users							
Pt IPv4 ACL								
P SNMP ACL								
🕵 Network Group /								
Retwork Service								
Map: Inbound ACL By WL								
IP Firewall Rules								
BROADCAST-MUL	1							
▶ 📩 Unmapped								
Pgguest-users								
Type to search	Type to search in tables	:						Row Count: 2
					Add	Edit	Delete	Copy Rename

Give your ACL a name and begin adding rules, clicking "+Add Row" for each new line.

2. Web UI Adding ACL Rules

IP	• Firewall Policy guest-users • O											
		Preceder	Action	DNS Name	DNS Matc	Source	Destination	Protocol	Mark	Log	Enable	Description
1		3	🛛 Allow		Not Set	🔆 Any	🔆 Any	➡ UDP, DPort 68	Mark	Log	🕑 Ena	permit DHCP
	1	5	Allow		Not Set	🔆 Any	8.8.8.8	➡ UDP, DPort 53	Mark	Log	🕑 Ena	permit DNS Traffic
		10	Allow		Not Set	🔆 Any	🖳 1.1.1.1	DPort 444	Mark	Log	🕑 Ena	permit Captive Portal traffic
≢		20	Allow		Not Set	🔆 Any	4.1.1.1.2	DPort 444	Mark	🗌 Log	🕑 Ena	permit Captive Portal Stats 1
≢		30	Allow		Not Set	🔆 Any	🖳 1.1.1.3	DPort 444	Mark	🗌 Log	🕑 Ena	permit Captive Portal Locali:
≢		40	C Allow		Not Set	🔆 Any	🔆 Any	DPort 80	Mark	🗌 Log	🕑 Ena	HTTP Allow
=	1	50	📿 Allow		exact	🔆 Any	🐥 Any	➡ TCP, DPort 443	Mark	🗌 Log	🕑 Ena	HTTPS Allow
≢		102	🔀 Deny		Not Set	🔆 Any	🔆 Any	⇔ IP	N/A	🗹 Log	😨 Ena	

Once you have added all of your rules, click ">> Ok", then commit and save your work. Navigate to Configuration > Network > Application Policy. Click on "Add"

3. Web UI Creating Application Policy

WING v5.8		Dasl	nbo	Configu	Diagno	Operati	Statis	stics	500 •		admin	Þ
Devices Wireless N	let	work	Profile	es RF Dor	nains Secu	irity Service	s Mar	nagement	5) Revert	📥 Commit	금 Commit	and Save
🖳 Alias		Applica	tion Po	licy								0
😵 Application Policy		Name					۲	Description				
M Application		quest-us	ers					-				
🐻 Schedule Policy		- peap-us	ers									
📷 URL Filtering		tis-users	:									
📷 Web Filtering												
💦 EX3500 QoS Class												
🚯 EX3500 QoS Policy N												
Application Policy												
🤡 guest-users	-1											
😵 peap-users	1											
😵 tis-users												
Type to search	ŀ	Type to s	earch in t	ables							Row Count	: 3
		.,,						Add	Edit	Delete	Copy R	tename

Name your policy, add rules to deny all unwanted applications on a guest network.

Note	
Application policy unlike ACL permits all traffic by default.	

5. Web UI Adding Application Rules

tion Policy Enforce	ement Time —									
-						<u>م</u>				
Days		Start Time		End Time						
Ð										
							1			
						Add Row				
tion Policy Rules						+ Add Row				
tion Policy Rules Preceden ce	Action	Application Category	Default Application	Custom Application	Mark Type	+ Add Row	Outbound Traffic Rate	Inbound Traffic Rate	Schedule Policy	
tion Policy Rules	Action	Application Category streaming	Default Application	Custom Application	Mark Type	+ Add Row Mark Value Not Set	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	Schedule Policy	
Preceden ce	Action Deny Deny	Application Category streaming p2p	Default Application	Custom Application	Mark Type	+ Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set Not Set	Inbound Traffic Rate Not Set Not Set	Schedule Policy	
tion Policy Rules	Action Deny Deny Deny	Application Category streaming p2p video	Default Application	Custom Application	Mark Type	+ Add Row Mark Value Not Set Not Set Not Set	Outbound Traffic Rate Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set	Schedule Policy	
tion Policy Rules Preceden Ce 1 2 3 4	Action Deny Deny Deny Deny	Application Category streaming p2p video filetransfer	Default Application	Custom Application	Mark Type	+ Add Row Mark Value Not Set Not Set Not Set	Outbound Traffic Rate Not Set Not Set Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set Not Set	Schedule Policy	
tion Policy Rules Preceden t t t t t t t t t t t t t	Action Deny Deny Deny Deny	Application Category streaming p2p video filetransfer	Default Application	Custom Application	Mark Type	+ Add Row Mark Value Not Set Not Set Not Set	Outbound Traffic Rate Not Set Not Set Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set Not Set	Schedule Policy	
Preceden ce 1 2 3 4	Action Deny Deny Deny Deny	Application Category streaming p2p video filetransfer	Default Application	Custom Application	Mark Type	Add Row Mark Value Not Set Not Set Not Set Not Set	Outbound Traffic Rate Not Set Not Set Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set Not Set	Schedule Policy	
tion Policy Rules Preceden ce 1 2 3 4	Action Deny Deny Deny	Application Category streaming p2p video filetransfer	Default Application	Custom Application	Mark Type	+ Add Row Mark Value Not Set Not Set Not Set	Outbound Traffic Rate Not Set Not Set Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set Not Set	Schedule Policy	
tion Policy Rules Preceden ce 1 2 3 4	Action Deny Deny Deny Deny	Application Category streaming p2p video filetransfer	Default Application	Custom Application	Mark Type	Add Row Mark Value Not Set Not Set Not Set	Outbound Traffic Rate Not Set Not Set Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set Not Set	Schedule Policy	
tion Policy Rules Preceden ce 1 2 3 4	Action Deny Deny Deny	Application Category streaming p2p video filetransfer	Default Application	Custom Application	Mark Type	Add Row Mark Value Not Set Not Set Not Set	Outbound Traffic Rate Not Set Not Set Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set	Schedule Policy	
tion Policy Rules	Action Deny Deny Deny	Application Category streaming p2p video filetransfer	Default Application	Custom Application	Mark Type	Add Row	Outbound Traffic Rate Not Set Not Set Not Set Not Set	Inbound Traffic Rate Not Set Not Set Not Set	Schedule Policy	

6. Once you have added all of your rules, click ">> Ok", then commit and save your work.

The following section outlines CLI configuration snippet:

1. CLI IP Access List configuration

```
ip access-list guest-users
permit udp any eq 68 any eq dhcps rule-precedence 3 rule-description "permit DHCP"
permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description "permit DNS traffic"
permit tcp any host 1.1.1.1 eq 444 rule-precedence 10 rule-description "permit Captive Portal traffic"
permit tcp any host 1.1.1.2 eq 444 rule-precedence 20 rule-description "permit Captive Portal Stats
traffic"
permit tcp any host 1.1.1.3 eq 444 rule-precedence 30 rule-description "permit Captive Portal Localization
traffic"
permit tcp any any eq 80 rule-precedence 40 rule-description "HTTP Allow"
permit tcp any any eq 443 rule-precedence 50 rule-description "HTTPS Allow"
deny ip any any log rule-precedence 100
!
```

2. CLI Application Policy configuration

!

```
application-policy guest-users
deny app-category streaming precedence 1
deny app-category p2p precedence 2
deny app-category tunnel precedence 3
```

Role Policy Configuration

Next we are going to create a role-policy and apply it to the access point profile. We will also enable DPI engine to enable application recognition and control.

In the Web UI navigate to "Configuration > Security > Wireless Client Roles" and click on "Add" to create a new role policy:

1. Web UI Creating Role Policy

WING v5.8	Dashboard Configuration Diagnostics Operations Statistics	😪 HX9600 🔹 🛛 🚺 🛔 admin 🛛 🎼
Devices Wireless Net	work Profiles RF Domains Security Services Management	5 Revert 陆 Commit 🔚 Commit and Save
a 🐯 Wireless Firewall	Wireless Client Roles	0
🧱 Firewall Policy	Role Policy	۲
MAC ACL	firewalled-users	
💶 🏬 IP Firewall		
🙎 Wireless Client Roles		
Device Fingerprinting		
🖬 🌄 Intrusion Prevention		
🗒 EX3500 Time Range		
Map: Profile 🔻		
Client Roles		
▶ 📩 Unmapped	-	
▶ <u> </u>		
Type to search	Type to search in tables	Row Count: 1
🔁 🖪 🖬 📫		Add Edit Delete Copy Rename

2. Web UI Creating Role Policy

Role Policy firewalled-users			0
	LDAP Settings Roles	Default Firewall Rules	
Role Name	۲	Precedence	
Time to accord in tables			Daw Causting
lype to search in tables			Row Count: 0
		Add	Edit Delete Exit

Name the role policy and then click "Add" to begin adding match criteria for the user role.

3. Web UI Creating Role Policy

Role Policy Roles		×
Role Name 拔 guest-users		0
Liscovery Policy	Settings Firewall Rules	
Client Identity Name		
Match Expressions		
APLocation	O Any 🔻 O	
SSID Configuration	Exact	
Group Configuration	O Any V O	
Radius User	O Any V O	
Wireless Client Filter		
Wireless Client MAC/MAC Mask	● 00 - 00 - 00 - 00 - 00 - 00 or ✓ Any	
Captive Portal Connection		
Authentication State	💵 🕘 Pre-Login 🔘 Post-Login 💿 Any	
Authentication / Encryption		
Authentication Type	Any EAP Kerberos MAC Authentication	None
Encryption Type	Any CCMP KeyGuard TKIP WEP128	WEP
EDAP Attributes		
	🔛 OK Reset	Exit

As can be seen, you may select a number of variations for match criteria. We have selected an exact match on the SSID, however other options exist as shown below.

5. Web UI Role Policy Match Expressions

Client Identity	
Client Identity Name	Image: A state of the state
	0
Match Expressions	
APLocation	1 Any 🗸 🔹
SSID Configuration	🖉 Exact 🔹 🗸 Z-Guest
Group Configuration	1 Any 🗸 🔹
Radius User	1 Any 🗸 1

After selecting your match criteria, go to the "Firewall Rules" tab and select the previously configured IP access list or whatever firewall rules you have previously configured. Add additional rows for additional firewall rules as needed by clicking "+Add Row". Also assign Application Policy that you have created earlier.

6. Web UI Role Policy Assignements

Role Policy Roles						×
Role Name guest-users						0
	Set	ttings	Fire	wall Rules		
Application Policy 🖋 guest-user	S	•	•	IP Firewall Rules Name	Preceden ce	
IPv6 Inbound			0			
IPv6 Firewall Rules Name	Preceden ce	ŵ			Add B	
0			MA	C Inbound	Tridat	
	🕂 Add R	low		MAC Firewall Rules Name	Preceden ce	1
IPv6 Outbound			0			
IPv6 Firewall Rules Name	Preceden ce	Ŵ			🕂 Add R	Row
0			MA	C Outbound		
	🕂 Add R	low		MAC Firewall Rules Name	Preceden ce	ŵ
IP Inbound			0			
IP Firewall Rules Name	Preceden ce	ŵ			📥 Add R	low
🖋 🛨 guest-users 🛛 🔻 😭	* 1 🔹	Ŵ				
	🕂 Add R	low				
				🕪 ок 🛛 🚺	Reset	Exit

Note

On the "**Default Firewall Rules**" tab of your role policy, you may select default access lists to be applied whether or not match criteria have been met. Realize that these rules are applied at the level where the role policy has been applied (access point level). Exercise caution to ensure traffic is not interrupted inadvertently due to a default rule. In our case we have specified no defaults, as seen below.

7. Web UI Default Role

Role Policy firewalled-users					0
	LDAP Setting	gs Roles	Default Firewall Rules		
IP Inbound			MAC Inbound		
IP Firewall Rules Name	Precedence	ŵ	MAC Firewall Rules Name	Precedence	ð
0			0		
	+ A	dd Row		+ Add Rov	v
IP Outbound			MAC Outbound		_
IP Firewall Rules Name	Precedence	ŵ	MAC Firewall Rules Name	Precedence	ð
0			0		
	+ A	dd Row		+ Add Rov	1
			0	W Deset Fuit	

Applying Role Policy

The final step is to apply the role policy to your devices. This will usually be done at the access point level (profile or device override) as that is the point of ingress for the wireless clients.

Navigate to "Configuration > Profiles" and select / edit the profile you wish to apply the role policy to. Within the profile, navigate to "Security > Settings" and select your policy from the "Wireless Client Role Policy" drop-down box.

1. Web UI Applying Role Policy

Profile CAMPUS-AP8533	Type AP8533					0
General	General				_	
Adoption	Firew all Policy	*	default 🗸	} 🛞		
▶ Interface	Wireless Client Role Policy	ø	firevvalled-users 🗸 🗸	} 🛞		
► Network	WEP Shared Key Authentication	0				
▼ Security	Client Identity Group	0	default 🔻	8		
Settings	CMP Policy	_				
Certificate Revocation	CIVIF POICY	0	•	1 199		
Trustpoints	URL Filter				_	
VPN	Content Filtering Policy	0	•	1 🎲		
Auto IPSec Tunnel						
NAT						
Bridge NAT						
Application Visibility (AVC)						
VRRP						
Critical Resources						
Services						
▶ Management						
► Advanced						
					OK Reset	Exit

Click ">>Ok" and then Commit and Save your work.

The following shows the CLI configuration snippet:

2. CLI Role Policy configuration

```
!
role-policy firewalled-users
user-role guest-users precedence 1
ssid exact Z-Guest
use ip-access-list in guest-users precedence 1
use application-policy guest-users
!
profile ap8533 CAMPUS-AP8533
///configuration removed for brevity///
use role-policy firewalled-users
dpi
!
```

Scenario 2 - Match based on the User Group

Scenario 2 is the same basic setup, except for now our match criteria will be based on group membership as gathered from the external AAA server. This is useful when it is required to differentiate between client devices using the same ESSID, but different EAP types, like EAP-TLS vs PEAP-MSCHAPv2 or to differentiate between the users that belong to different user groups, like Sales vs Marketing vs Engineering and so on.

In this example we will use Microsoft NPS as an external RADIUS server that will provide Vendor Specific Attributes with the user group name that will be used by WiNG 5 Role Based Firewall as a match criteria. The same user account will be used for testing, while role assignments are based on returned user group name.

The following sections will just show the configuration of the additional components (in order of configuration), which are:

- 1. External RADIUS Configuration (Microsoft NPS)
- 2. AAA Policy
- 3. WLAN Authentication

External RADIUS Configuration (Microsoft Network Policy Server)

In this scenario, we are using Microsoft NPS as a RADIUS server, but similar approach can be used also with any other RADIUS server, including onboard RADIUS on WiNG5.

In Active Directory we will create a single user for this example that would be member of "corp-assets" group.

1. Active Directory Create New User Group



2. Active Directory Create New User Group

New C	bject - Group
🥵 Create in: cztac.zebra	a.local/TMELABS
Group name:	
corp-assets	
Group name (pre-Windows 2000);	
corp-assets	
Group scope	Group type
O Domain local	
● <u>G</u> lobal	O <u>D</u> istribution
◯ <u>U</u> niversal	
	OK Cancel

Following group creation, we will create a user and make this user a member of the corp-assets user group.

3. Active Directory Create New User



	New Object - User	x
Create in:	cztac.zebra.local/TMELABS	
<u>F</u> irst name:	john <u>I</u> nitials:	
Last name:		
Full n <u>a</u> me:	john	
User logon name:		
john	@cztac.zebra.local v	
User logon name (pre	- <u>Wi</u> ndows 2000):	
CZTAC\	john	
	< <u>B</u> ack <u>N</u> ext > Car	ncel

john Properties ?						x	
Remote control	Remote D	Remote Desktop Services Profile				M+	
General Address	Account	Account Profile Telephones Organ					
Member Of	Dial-in	Dial-in Environment Sessions					
Member of:							
Name	Active Directo	ory Domain	Services Folder				
Domain Users	cztac.zebra.lo	ocal/Users					
A <u>d</u> d E Primary group: Do Set Primary Group	emove omain Users There is n you have application	o need to c Macintosh 1s.	change Primary g clients or POSI	grout (-con	p unle nplian	255 tt	
0	K C	ancel	Apply		He	elp	

Select	Groups	x
Select this object type:		
Groups or Built-in security principals		Object Types
From this location:		
cztac.zebra.local		Locations
Enter the object names to select (<u>examples</u>): <u>corp-assets</u>		Check Names
Advanced	OK	Cancel

As a next step we will create new connection policy to allow 802.11 Wireless EAP Authentication using either PEAP-MSCHAPv2 or EAP-TLS, followed by a new Network Policy that will further differentiate between the two EAP types and send WiNG Vendor Specific Attribute back to apply correct user role:

4. Network Policy Server configuration

•	Network Policy Server	
<u>File Action V</u> iew <u>H</u> elp		
🗢 🔿 🞽 🖬 🛿 🎫		
 NPS (Local) RADIUS Clients and Servers Policies Connection Report 	Connection Request Policies Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in n request policy.	
Image: Network Polici N Image: Health Policies E Image: Health Policies E <td>sconnections Enabled 1 Unspecified efresh efresh efresh efresh efresh efresh</td> <td></td>	sconnections Enabled 1 Unspecified efresh efresh efresh efresh efresh efresh	
	Use Windows authentication for all users	
	Conditions - If the following conditions are met: Condition Value Day and time restrictions Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:0	<
	Settings - Then the following settings are applied:	
	Setting Value	~
< III >		

New Connection Request Policy	
Specify Connection Request Policy Name and Connection Type	
You can specify a name for your connection request policy and the type of connections to which the policy is applied.	
Policy name:	
Wireless Client Authentication	
Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server	
type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.	
Type of network access server:	
Unspecified V	
O Vendor specific:	
Previous Next Linish Cancel	
	Y
	~
Specify Conditions	
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required.	st. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required.	st. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions:	st. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	st. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	st. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	st. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	5t. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	bt. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	5t. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	st. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	bt. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value	bt. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request Conditions Condition Value Condition description	et. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value Condition Value Condition Value Condition Value	5t. A
Specify Conditions Specify Conditions that determine whether this connection request policy is evaluated for a connection req	5t. A
Specify Conditions Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request Conditions Condition Value Condition Condition description:	5t. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Conditions: Condition Value Condition description: Add Edt	st. A
Specify Conditions Sectify the condition is that determine whether this connection request policy is evaluated for a connecting policy is evaluated for a connecting policy is evalif	5t. A
Specify Conditions Specify the conditions that determine whether this connection request policy is evaluated for a connection request minimum of one condition is required. Condition: Condition Value Condition description:	st. A
Specify Conditions Specify conditions that determine whether this connection request policy is evaluated for a connection request Conditions: Condition Value Condition description: Add Edt Remove	5t. A

Select condition	x
Select a condition, and then click Add.	
NAS Identifier The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.	^
NAS IPv4 Address The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.	
NAS IPv6 Address The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.	
NAS Port Type The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.	
	≡
A <u>d</u> d Cano	cel

NAS Port Type
Specify the access media types required to match this policy. Common <u>d</u> ial-up and VPN tunnel types
Async (Modem) ISDN Sync Sync (T1 Line) Virtual (VPN)
Common 802.1X connection tunnel types
Ethemet FDDI Token Ring
✔ Wireless - IEEE 802.11
Others
ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation ADSL-DMT - Asymmetric DSL Discrete Multi-Tone Async (Modem) Cable
OK Cancel

	New Connection Request Policy	x
Specify Conn The connection reque remote RADIUS serv	ection Request Forwarding est can be authenticated by the local server or it can be forwarded to RADIUS servers in er group.	a
If the policy conditions match the conn	ection request, these settings are applied.	
Forwarding Connection Request	Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication. Authenticate requests on this server Forward requests to the following remote RADIUS server group for authentication: Interface configured> Accept users without validating credentials 	
	Previous Next Finish Cancel	
	New Connection Request Policy	
Specify Authent Configure one or more au authentication, you must Protected EAP.	ication Methods thentication methods required for the connection request to match this policy. For EAP configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure	
Verride network policy authentication These authentication settings are used rat connections with NAP, you must configure EAP types are negotiated between NPS a	settings her than the constraints and authentication settings in network policy. For VPN and 802.1X PEAP authentication here. nd the client in the order in which they are listed.	
EAP Types: Microsoft: Protected EAP (PEAP) Microsoft: Smart Card or other certificate	Move Up	
Add Edit Rer Less secure authentication method Microsoft Encrypted Authentication we User can change password after it User can change password after it Encrypted authentication (M User can change password after it Encrypted authentication (CHAP) Unencrypted authentication (PAP, SP. Allow clients to connect without negotive	nove Is: rsion 2 (MS-CHAP- <u>v</u> 2) has expired S-CHAP) has expired AP) ating an authentication method.	
	Previous Next Enish Cancel	

	New Connection Request Policy		
NPS applies setting: matched.	ettings s to the connection request if all of the connection request policy conditions for the policy are		
Configure the settings for this network If conditions match the connection red	policy. quest and the policy grants access, settings are applied.		
Settings: Specify a Realm Name Carlow Attributes Standard Carlow Vendor Specific	Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list. Attribute: Called-Station-Id Rules:		
Previous Mext Enish Cancel New Connection Request Policy X Completing Connection Request Policy Wizard			
Completing	New Connection Request Policy X Connection Request Policy Wizard		
You have successfully created the for Wireless Client Authentication	New Connection Request Policy Connection Request Policy Wizard		
You have successfully created the for Wireless Client Authentication Policy conditions: Condition Value NAS Port Type Wireless - IEEE 80	New Connection Request Policy Wizard Illowing connection request policy: 2.11		
Completing You have successfully created the for Wireless Client Authentication Policy conditions: Condition Value NAS Port Type Wireless - IEEE 80 Policy settings: Condition Authentication Provider Override Authentication Authentication Method Extensible Authentication Provider	New Connection Request Policy Wizard Connection Request Policy Wizard New Connection request policy: Illowing connection request policy: 2.11 Value Local Computer Enabled EAP Microsoft: Protected EAP (PEAP) OR Microsoft: Smat Card or other certificate		
Completing You have successfully created the for Wireless Client Authentication Policy conditions: Condition NAS Port Type Wireless - IEEE 80 Policy settings: Condition Authentication Provider Override Authentication Authentication Provider Override Authentication Protocol M Extensible Authentication Protocol M To close this wizard, click Finish.	New Connection Request Policy Wizard Idowing connection request policy: 2.11 Value Local Computer Enabled EAP Method Microsoft: Protected EAP (PEAP) OR Microsoft: Smart Card or other certificate		

6. NPS Create Network Policies

File Action View Help		inetwor	k Policy Server					^
🗢 🄿 🞽 🖬 🚺								
NPS (Local)	Network Pol	icies						
 Policies Connection Request Po 	Netwo under	ork policies allow you r which they can or c	i to designate who is annot connect.	authorized to	connect to	the network and the	ne circumstance	s
Contraction New					Status	Processing Order	Access Type	5 ^
▷ Solution Point	list	R-AUTH			Enabled	1	Grant Access	L_
Accounting View	•	ISCHAPv2			Disabled Disabled	3	Grant Access Grant Access	ι ι
Refresh		1		Ш	Disablad	1	Cont Access	>
Help								
	Conditions	If the following condi	tions are met:					^
			tions are met.					
	Condition	Vaiu	IE					=
	Settings - Th	nen the following sett	ings are applied:					
	Setting	Valu	ie					
< III > [<			Ш				>
lew								
Policy name:								
peap-users			untion manuart to 1					
Network connection method Select the type of network acces type or Vendor specific, but neth select Unspecified.	ss server tha ner is required	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentic	either the netwo ating switch or w	rk access sen ireless access	ver point,
Network connection method Select the type of network access gerv Type of network access gerv	ss server tha ner is required er:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentic	either the netwo ating switch or w	rk access sen ireless access	ver s point,
Network connection method Select the type of network accest type or Vendor specific, but neth select Unspecified. Type of network access gerv Unspecified	ss server tha her is required er:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentic	either the netwo ating switch or w	rk access ser ireless access	ver ; point,
Peap-users Network connection method Select the type of network access type or Vendor specific, but neith select Unspecified. Type of network access <u>serv</u> Unspecified <u>V</u> endor specific:	ss server tha her is required er:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentica	either the netwoi ating switch or w	rk access sen ireless access	ver ; point,
Network connection method Select the type of network acces type or Vendor specific, but neith select Unspecified. Unspecified Unspecified Vendor specific: 10 V	ss server tha her is required er:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentica	either the networ ating switch or w	rk access sen ireless access	ver ; point,
Network connection method Select the type of network acces type or Vendor specific, but neith select Unspecified. Type of network access serv Unspecified Vendor specific: 10 Type	ss server tha her is required rer:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentic	either the networ ating switch or w	rk access sen ireless access	ver ; point,
Peap-users Network connection method Select the type of network acces type or Vendor specific, but neith select Unspecified. Type of network access gerv Unspecified Unspecified Usedor specific: 10 \$\screwtyce\$	ss server tha her is required er:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentica	either the netwo ating switch or w	rk access sen ireless access	ver ; point,
Network connection method Select the type of network acces type or Vendor specific, but neit select Unspecified. Type of network access gerv Unspecified Vendor specific: 10 \vec{vendor}	ss server tha her is required ver:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentic	either the networ	rk access sen ireless access	ver ; point,
Peap-users Network connection method Select the type of network acces type or Vendor specific, but neith select Unspecified. Type of network access serv Unspecified Vendor specific: 10	ss server tha her is required er:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentica	either the networ	rk access sen ireless access	ver ; point,
Network connection method Select the type of network accellate the type of network accellate the type or Vendor specified. Type of network access gerv Unspecified Unspecified Unspecified Unspecified	ss server tha her is required rer:	t sends the conne d. If your network	v	NPS. You ca an 802.1X a	n select uthentic	either the networ	rk access sen ireless access	ver ; point,
Peap-users Network connection method Select the type of network acces type or Vendor specified. Type of network access gerv Unspecified Vendor specific: 10	ss server tha her is required ver:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentic	either the netwo	rk access sen ireless access	ver ; point,
Peap-users Network connection method	ss server tha her is required ver:	t sends the conne d. If your network	access server is	NPS. You ca an 802.1X a	n select uthentic	either the netwo	rk access sen ireless access	ver ; point,

	New Network Policy	x
	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection reques of one condition is required.	st. A minimum
Conditions:		
Condition	n Value	
Condition desc	cription: Add Edit	Remove
	Select condition	x
Coloret		
Select a conditi	tion, and then click Add.	
Windo Windo The W groups Mach The M	Jows Groups Aindows Groups condition specifies that the connecting user or computer must belong to one of the selected is. hine Groups Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.	
User (The U	Groups Jser Groups condition specifies that the connecting user must belong to one of the selected groups.	
Locat The H require networ	tion Groups HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups ed to match this policy. The HCAP protocol is used for communication between NPS and some third party ork access servers (NASs). See your NAS documentation before using this condition.	>
	Add	Cancel

User Groups X	
Specify the group membership required to match this policy.	
Groups Add Groups Remove OK Cancel	

	Select Group	x
Select this object typ	e:	
Group		Object Types
From this location:		
cztac.zebra.local		Locations
Enter the object nam	e to select (<u>examples</u>):	
corp-assets		Check Names
<u>A</u> dvanced	ОК	Cancel
	New Network Policy	X
Specify the co of one condition	ONGITIONS nditions that determine whether this network policy is evaluated for a on is required.	connection request. A minimum
Conditions:	Web a	
Liser Groups	CZTAC\corp-assets	
Condition description: The User Groups condition spec	cifies that the connecting user must belong to one of the selected groups.	Edit Remove
	Previous Next	Enish Cancel



Allowed EAP Types

Specify the EAP types required for client computer authentication method configuration to match this policy. Use of this condition requires that EAP is also configured in connection request policy.

Microsoft: Smart Card or other certificate Microsoft: Protected EAP (PEAP) Microsoft: Smart Card or other certificate
Microsoft: Secured password (EAP-MSCHAP v2)
OK

	New Network Policy
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access gra Grant acce Access der	nted ss if client connection attempts match the conditions of this policy. nied
Deny acce	ss if client connection attempts match the conditions of this policy.
Acce <u>s</u> s is o Grant or de	letermined by User Dial-in properties (which override NPS policy) ny access according to user dial-in properties if client connection attempts match the conditions of this policy.
	Previous Next Enish Cancel
	New Network Policy
	Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure
	Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are r	Protected EAP in connection request policy, which overrides network policy authentication settings. negotiated between NPS and the client in the order in which they are listed.
EAP types are r EAP <u>Types:</u> Microsoft: Pro	Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are r EAP Types: Microsoft: Pro	Protected EAP in connection request policy, which overrides network policy authentication settings. negotiated between NPS and the client in the order in which they are listed. tected EAP (PEAP) Move Up Move Down
EAP types are r EAP Types: Microsoft: Pro	Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are r EAP Types: Microsoft: Pro Add Less secure Microsoft E User car Microsoft E	Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are r EAP Types: Microsoft: Pro Add Less secure Microsoft E User car Microsoft E User car Compared a Unencrypted	Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are r EAP Types: Microsoft: Pro Add Less secure Microsoft E User car Microsoft E User car Allow client Perform ma	Protected EAP in connection request policy, which overrides network policy authentication settings.

New Network Policy X				
Configure Constraints Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.				
Configure the constraints for this networ if all constraints are not matched by the Constraints Constr	rk policy. a connection request, network access is denied. Specify the maximum time in minutes that the server can remain idle before the connection is disconnected Disconnect after the maximum idle time 1 Image: Connect after the maximum idle time			
	Previous Next Finish Cancel			
Configure Se NPS applies settings matched.	New Network Policy X Image: Configure Settings NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.			
Configure the settings for this network p If conditions and constraints match the Settings:	policy. connection request and the policy grants access, settings are applied.			
RADIUS Attributes Image: Standard Image: Vendor Specific Network Access Protection Image: NAP Enforcement Image: Extended State Routing and Remote Access Image: Protection Image: Multilink and Bandwidth Allocation Protected (RAP)	To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.			
IP Filters IP Filters IP Settings	Add EditRemove			
	Previous Next Enish Cancel			

At this stage we need to define a **WiNG-User-Group VSA** that RADIUS server will send back upon successful user authentication. <u>WiNG Vendor Code is 388, attribute number is 12, format is ASCII</u>.

	Add Vendor Specific Attribute	x
To add an attribute to the set	ttings, select the attribute, and then click Add.	
To add a Vendor Specific att	ribute that is not listed, select Custom, and then click Add.	
<u>V</u> endor:		
Custom	~	
Attri <u>b</u> utes:		
Name	Vendor	
Allowed-Certificate-OID	RADIUS Standard	
Generate-Class-Attribute	RADIUS Standard	
Generate-Session-Timeout	RADIUS Standard	
Tunnel-Tag	RADIUS Standard	n 💷
vendor-specific	RADIUS Standard	
Deserietien		
Description.		
Specifies the support of prop	rietary NAS features.	
	Add	
	BOOLUOSE	
		_
	Attribute Information	
Attribute name: Vendor-Specific	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: Octet String Attribute values:	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: Vendor Value	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: Vendor Value	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: Octet String Attribute values: Vendor Value	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: Octet String Attribute values: Vendor Value	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: Octet String Attribute values: Vendor Value	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: Vendor Value	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: Vendor Value	Attribute Information	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: Octet String Attribute values: Vendor Value	Attribute Information Add Edit Edit Remove Move Up Move Down	
Attribute name: Vendor-Specific Attribute number: 26 Attribute format: Octet String Attribute values: Vendor Value	Attribute Information Add Edit Edit Remove Move Up Move Down OK	

Vendor-Spec	ific Attribute Information
Attribute name: Vendor Specific	
Specify network access server	vendor.
○ <u>S</u> elect from list:	RADIUS Standard V
• Enter Vendor Code:	388
Specify whether the attribute c vendor specific attributes.	onforms to the RADIUS RFC specification for
Yes. It conforms No. It does not conform	
Configure <u>A</u> ttribute	
	OK Cancel
Configure \	/SA (RFC Compliant)
Vendor-assigned attribute	number:
Attribute format: String	~
Attri <u>b</u> ute value: peap-users	
	OK Cancel

	New Network Policy	
NPS applies setting matched.	e ttings is to the connection request if all of the network policy conditions and constraints for the policy are	
Configure the settings for this network If conditions and constraints match th	: policy. e connection request and the policy grants access, settings are applied.	
<u>S</u> ettings:		
RADIUS Attributes	To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.	
Network Access Protection		
NAP Enforcement	Attributes ·	
Extended State	Name Vendor Value	
Routing and Remote	Vendor-Specific RADIUS Standard peap-users	
Multilink and Bandwidth Allocation Protocol (BAP) IP Filters		
🚜 Encryption		
🗾 IP Settings	Add Edit Remove	
	Previous Next Einish Cancel	
	New Network Policy	2
You have successfully created peap-users	Ing New Network Policy	
Policy conditions:		
Condition Value		
User Groups CZTAC Allowed EAP Types Microso	\corp-assets ft: Protected EAP (PEAP)-Microsoft: Secured password (EAP-MSCHAP v2)	
Policy settings:		
Condition	Value	^
Authentication Method	EAP Grant Access	_
Update Noncompliant Clients		=
NAP Enforcement	Allow full network access	
Framed-Protocol	PPP Fermed	
To close this wizard, click Finis	h.	¥
	Previous Next Einish Cancel	

х

Repeat the process and add another Network Connection Policy for the EAP-TLS authenticated devices. Below are the configuration parts that should be different.

Allowed EAP Types	
Specify the EAP types required for client computer authentication method configuration to match this policy. Use of this condition requires that EAP is also configured in connection request policy.	
Microsoft: Smart Card or other certificate Microsoft: Protected EAP (PEAP) Microsoft: Smart Card or other certificate Microsoft: Secured password (EAP-MSCHAP v2) Microsoft: Secured password (EAP-MSCHAP v2)	
OK Cancel	
New Network Policy	x
Configure Authentication Methods Configure one or more authentication methods required for the connection required for the connection required for the connection required for the connection required to the source of the source	uest to match this policy. For EAP or VPN, you must configure entication settings.
EAP types are negotiated between NPS and the client in the order in which they are listed.	
Microsoft: Smart Card or other certificate Move Up	
Move Do <u>w</u> n	
Add Edit Bemove	
Less secure authentication methods:	
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)	
User can change password attent has expired Microsoft Encrypted Authentication (MS-CHAP)	
User can change password after it has expired	
Unencrypted authentication (PAP, <u>SPAP</u>)	
Allow clients to connect without negotiating an authentication method.	
Previous Next	<u>Fi</u> nish Cancel

Configure VSA	A (RFC Comp	liant) 🔽		
Vendor-assigned attribute nur	mber:			
<u>A</u> ttribute format: String		~		
Attri <u>b</u> ute value: tls-users				
	ОК	Cancel		
	New	Network Policy		×
Configure Se NPS applies settings matched.	to the connection required to the connection required to the connection request and connection request and	iest if all of the netwo	ork policy co	onditions and constraints for the policy are s are applied.
Settings: RADIUS Attributes Standard Vendor Specific Network Access Protection	To send additional at then click Edit. If you your RADIUS client of	tributes to RADIUS cli do not configure an a documentation for requ	ients, select attribute, it is uired attribute	a Vendor Specific attribute, and not sent to RADIUS clients. See es.
NAP Enforcement	Attributes:			
🕎 Extended State	Name	Vendor	Value	
Routing and Remote Access Image: Multilink and Bandwidth Allocation Protocol (BAP) Image: Protocol	Add	Edit	tls-users	
	,	Previous	Nex	t <u>F</u> inish Cancel

Last configuration part on the NPS side is to add a RADIUS client to allow Access Points to talk to RADIUS server. If Access Points are making requests directly to the RADIUS it is easier to add them using a subnet as a source IP address.

8. NPS Add RADIUS Clients

Network Pc	licy Server
File Action View Help	
NPS (Local) RADIUS Clients	
RADIUS Clients and Servers RADIUS Clients and Servers RADIUS Clients allow you to specify the network access servers, that provide access Remote RADI New Remote RADI Export List	to your network.
Connection B IP Address Device Manufacturer NAP-Capable Status	
Network Police View 192.168.7.60 RADIUS Standard No Enabled	
Health Policie Refresh 192.168.65.7 RADIUS Standard No Enabled	
Network Access 111-1-	
Accounting 192.168.88.8 RADIUS Standard No Enabled	
▶ Interplates Management No Enabled NX96 192.168.96.7 RADIUS Standard No Enabled	
New RADIUS Client	
Settings Advanced	
✓ Enable this RADIUS client	
Select an existing template:	
Name and Address	
rhendry name:	
Address (IP or DNS):	
172.27.0.0/24 <u>V</u> erify	
Shared Secret	
Select an existing Shared Secrets template:	
None V	
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.	
Manual Generate	
Shared secret:	
Confirm shared secret:	
•••••••	
OK	

AAA Policy Configuration

We need to create new AAA Policy that will point Access Points to authenticate against our RADIUS server. Navigate to Configuration > Network > AAA Policy and click on Add.

WING v5.8 Dashbo)	Configur	Dia	agnos	Operati	Statistics	マ NX9600 🔻	- 🚺 🕺 ad	min 🕞
Devices Wireless Network Pro	ofile	es RF Domain	ns	Security	Services	s Management	t 🌖 Revert	🛃 Commit 🔚	Commit and Save
물물Policy Based Routing 💧 🛔	1	Authentication, A	\uth	orization,	and Acco	unting (AAA)			0
QL2TPv3		AAA Policy		Accountin	g Packet	Request Interval	NAC Policy	Server Pooling N	Aode
Crypto CMP Policy			۲	Туре					
🖳 AAA Policy									
🗧 AAA TACACS Policy									
📷 IPv6 Router Advertisement Policy									
🖬 📲 BGP									
👜 Alias									
😵 Application Policy									
M Application									
🗟 Schedule Policy									
Man: None									
	-								
	1								
Type to search	ľ	Type to search in tab	les					Ro	w Count: 0
1 1 1						Add	Edit	Delete Copy	Rename
AAA Policy 岁 External-A	A٨	4			Contin	Je E	xit		

		ttings	nting Se	RADIUS Accou	entication	RADIUS Auth			
NAC Enabl	NAI Routing Enable	DSCP	Request Timeout	Request Attempts	Request Proxy Mode	Port	Host	Server Туре	Gerver d

erver id 🎲 1 🚔	(1 to 6)
ettings	
Server Type Host	 Host ▼ 192. 168. 7. 15 IP Address
Port Secret	 Allas \$ 1812 ↓ (1 to 65,535) ★ Antonica (1 to 65,535)
Request Proxy Mode Proxy Mint Host Request Attempts Request Timeout Retry Timeout Factor DSCP NAI Routing Enable Realm Realm Strip Realm	None \checkmark None \checkmark $3 \checkmark$ (1 to 10) $3 \checkmark$ (1 to 60) $100 \checkmark$ (50 to 200) $0 \checkmark$ (0 to 63) Routing \bigcirc Prefix \bigcirc Suffix
🕥 Revert 陆 Cor	nmit Commit and Save

Application Policy Configuration

In this step we create 2 new Application Policies for devices authenticating using PEAP-MSCHAPv2 and devices authenticating EAP-TLS.

Navigate to Configuration > Network > Application Policy > Add:

And the second s	o Net	Dashbo		gno O	perati	Statisti	cs			
VICES WIREless	s Netv	vork Profile	s RF Domains	Security	Services	Mana	igement	🄊 Revert	Commit 🗠	Commit and
Application Policy	v	pplication Poli	cy							
Application	· ·	lame				۲	Description			
Schedule Policy	9	guest-users								
URL Filtering	t	ls-users								
Web Filtering										
EX3500 QoS Cla	iss									
EX3500 QoS Poli	licy N .									
Application Policy										
guest-users	Ţ									
V peap-users	-									
W 113-03013										
e to search		vne to search in ta	bles							Row Count: 3
b b c		, po to couron inta					A 44	5-0	Delete	
							Add		Delete	Lopy Renar
e peap-users										
ication Policy Enforceme	ent Time ——									
ication Policy Enforceme	ent Time — St	lart Time		End Time			D			
lication Policy Enforceme Days	ent Time St	art Time		End Time			ŵ			
lication Policy Enforceme	ent Time St	lart Time		End Time			Ŵ			
Days	ent Time St	art Time		End Time			Û			
Days	ent Time St	art Time		End Time			Ŵ			
Days	ent TimeSt	art Time		End Time			ŵ			
Days	ent Time St	art Time		End Time			â			
Days	ent Time St	art Time		End Time			t Add Row			
Days Days Cation Policy Rules Presedence	ent Time St	art Time		End Time			Add Row	Orthound	bbund Ir off	Schardala Dalina
Days Days Cation Policy Rules Precedence	Action	art Time Application Category	Default Application	End Time	n \odot M	ark Type	Add Row	Outbound Traffic Rate	Inbound Traffie Rate	c Schedule Policy
Days Days Days Precedence 1	Action Deny	Application Category P2p	Default Application	End Time Custom Applicatio -	n ⓒ M	ark Type	Add Row Mark Value Not Set	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	c Schedule Policy
Cation Policy Enforcement	Action Centry rate-line	Application Category D2p at steaming	Default Application	End Time Custom Applicatio	n ⓒ M 	ark Type	Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	c Schedule Policy
Cation Policy Enforcement	Action Centry rate-lirr	Art Time Application Category 22 23 24 24 25 24 25 24 25 24 25 25 25 25 25 25 25 25 25 25 25 25 25	Defaut Application	End Time Custom Applicatio	n ⓒ M - -	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	C Schedule Policy
cation Policy Enforcement	Action Centry rate-lint	Art Time Application Category p2p at streaming	Defaut Application	End Time Custom Applicatio	n ⓒ M - -	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	E Schedule Policy
cation Policy Enforcement	Action Action Deny rate-lir	Art Time Application Category p2p at streaming	Defaut Application	End Time Custom Applicatio	n ⓒ M - -	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	E Schedule Policy
ication Policy Enforcement	Action Action Certy Cert	Art Time Application Category p2p at streaming	Default Application	End Time Custom Applicatio	n ⓒ M	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	Schedule Policy Image: Schedule Policy
ication Policy Enforcement	Action Action Compared Compare	Art Time Application Category p2p at streaming	Defaut Application	End Time Custom Applicatio	n ⓒ M - -	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	E Schedule Policy Image: Schedule Policy Image: Schedule Policy
ication Policy Enforcement	Action Action Conversion Conversi	Art Time Application Category p2p at streaming	Default Application	End Time Custom Applicatio	n ⓒ M	ark Type	Add Row Add Row Mark Value Not Set Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	Schedule Policy Image: Schedule Policy
ication Policy Enforcement	Action Action Derry rate-lin	Art Time Application Category p2p streaming		Custom Applicatio	n ⓒ M	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	s Schedule Policy
Lation Policy Enforcement	Action Action Deny rate-in	Application Category p2p streaming	Default Application -	Custom Applicatio	n ⓒ M	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	s Schedule Policy
cation Policy Enforcement	Action Constraints of the second seco	Application Category p2p streaming streaming		End Time Custom Applicatio	n © M	ark Type	Add Row Add Row Mark Value Not Set Not Set	Outbound Traffic Rate Not Set 512	Inbound Traffic Rate Not Set 512	c Schedule Policy

CLI

```
!
application-policy peap-users
deny app-category p2p precedence 1
rate-limit app-category streaming ingress rate 512 max-burst-size 2 egress rate 512 max-burst-size 2
precedence 2
!
application-policy tls-users
mark application "Skype for Business_generic" dscp 46 precedence 1
!
```

WLAN Configuration

Create a new WLAN and enabled EAP based authentication with CCMP encryption, assign newly created AAA policy. Navigate to Configuration > Wireless > Wireless LANs, click on Add.

WING v5.8)ashbo	. Conf	iaur	Diagnos.	Op	erati	Statistics	S (9600 🔹	- ()	4	admin	- 13
Devices Wireless Networ	'k Profi	les RF	Domain	s Securi	ty Sen	/ices N	lanagemei	nt	5) R	evert 🔼	Commit	🕞 🕞 Cor	nmit and Save
믪 Wireless LANs		Wireless	LANS										0
🖶 WLAN QoS Policy		WLA	SSID	Descripti	WLAN	VLAN	Bridging	DHCP	DHCPv6	Authenti	Encrypti	QoS	Associat
Radio QoS Policy		N 🍝		on	Status	Pool	Mode	Option	LDRA	cation	on Type	Policy	ion ACL
Association ACL								82		Туре			
SMART RF Policy													
🛣 MeshConnex Policy													
X Mesh QoS Policy													
Passpoint Policy													
🕎 Sensor Policy													
Wireless LAN													
	-												
	-												
	_												
	_												
	_												
Type to search		Type to se	arch in tabi	les								Row Co	unt: 0
	ET I						Ad	ld	Edit	Delete	0	DV	Rename

VLAN 拔 TMELABS-DOT1X	0
Basic Configuration	WLAN Configuration
Security	SSID 🏏 TMELABS-DOT1X
Firewall	Description
Client Settings	WLAN Status Disabled Enabled
Accounting	QoS Policy
Service Monitoring	Bridging Mode
Client Load Balancing	
Advanced	
Auto Shutdown	Boniour Gateway Discovery Policy
	Other Settings
	Broadcast SSID
	Answer Broadcast Probes
	VLAN Assignment
	Single VLAN VLAN Pool
	VLAN 25
	RADIUS V LAN Assignment
	Allow RADIUS Override 👔 📃
	IRI Filter
	URL Filter D crones
	22 OK Reset Exit
VIAN THELARS.DO	1712
Basic Configuration	Select Authentication
Security	
Firewall	
Client Settings	
Accounting	AAA Policy 🕕 External-AAA 🔹 🔛 🛞
Consiso Monitoring	Reauthentication 30 (30 to 86,400)
Service wontoring	
Client Load Balancing	
Advanced	Cantive Portal
Auto Shutdown	supero roman
WLAN TMELABS-DC	DT1X
Basic Configuration	Select Encryption
Occurrity	
SOCIER	



C

?

CLI

```
wlan TMELABS-DOT1X
ssid TMELABS-DOT1X
vlan 25
bridging-mode local
encryption-type ccmp
authentication-type eap
use aaa-policy External-AAA
use ip-access-list out BROADCAST-MULTICAST-CONTROL
use mac-access-list out PERMIT-ARP-AND-IPv4
```

Role Policy Configuration

Finally, we need to modify our role policy that was created in the first scenario to add the new role with new match criteria based on the returned user group attribute. In this way, users who associate to the WLAN using PEAP-MSCHAPv2 will get different policies compared to devices authenticated using EAP-TLS method. This can be useful when corporate laptop devices are being staged with client certificates, while mobile devices still use PEAP for simplicity.

Navigate to Configuration > Security > Wireless Client Roles > select "firewalled-users" > Roles > Add

WiNG v5.8 Dashbo	D	Configur	Diagnos	Operati	Sta	tistics			admin	Þ
Devices Wireless Network Pro	file	es RF Domains	Security	Services	Mana	gement	: 🌖 Revert	🛛 📥 Commit	금 Commi	t and Save
= 🌄 Wireless Firewall		Role Policy firew	alled-users							0
🧱 Firewall Policy				I DAP Set	tinas	Dolee	Default Firewall Rules			
MAC ACL				LDHI SOL	lings	Ruies	Derudit III Circuit Naico			
🖬 🌇 IP Firewall		Role Name				۲	Precedence			
Swireless Client Roles		guest-users					1			
Device Fingerprinting										
🖸 🗛 Intrusion Prevention										
🐻 EX3500 Time Range										
Map: Profile 🔻										
Client Roles	_									
▶ 🍓 Unmapped	4									
▶ <u>&</u> firewalled-users										
Type to search		Type to search in table	s						Row Count:	1
1							Add	Edit De	lete E	xit

Role Policy Roles	×
Role Name 拔 peap-users	0
	Settings Firewall Rules
Information	
To configure LDAP attributes in th	e Role, the LDAP Settings should be configured first.
Role Precedence	
Precedence	
Bonjour Gateway	
Discovery Policy	0
Client Identity	
Client Identity Name	
Match Expressions	
APLocation	O Any V O
SSID Configuration	í Any
Group Configuration	✓ Exact
Radius User	Any V
Wireless Client Filter	
Wireless Client MAC/MAC Mas	k 🕕 00 - 00 - 00 - 00 - 00 - 00 or 🖌 Any
Captive Portal Connection	
Authentication State	🛈 🔵 Pre-Login 🔘 Post-Login 💿 Any
Authentication / Encryption	
Authentication Type	Equals EAP Kerberos MAC Authentication None
Encryption Type	✓ Equals ✓ CCMP KeyGuard TKIP WEP128 WEP64 None
LUAP Attributes	
	OK Reset Exit

/ 44

Role Policy Roles					×
Role Name peap-users					0
	Se	ttings	Firewall Rules		
Vlan ID					
VLAN 1 (1 to 4,	094)				
Application Policy			IP Outbound		
Application Policy 🥒 peap-users	▼	÷	IP Firewall Rules Name	Precedence	Û
IPv6 Inbound			0		
IPv6 Firewall Rules Name	Precedence	ŵ			
0				🕂 Add	Row
•			MAC Inbound		
	🕂 Add	Row	MAC Firewall Rules Name	Precedence	Ŵ
IPv6 Outbound			0		
IPv6 Firewall Rules Name	Precedence	Û			
0				+ Add	Row
			MAC Outbound	Deserves	A
	+ Add	Row	MAC FILEWall Kules Name	Frecedence	
IP Inbound		~	0		
IP Firewall Rules Name	Precedence			+ Add	Row
0					
	📕 Add	Pow			
	- Add				
				Decet 5	
				Reset	xit

Role Policy Roles	×
Role Name 岁 tis-users	0
	Settings Firewall Rules
To configure LDAP attributes in Pole Precedence	n the Role, the LDAP Settings should be configured first.
Precedence	
Bonjour Gateway	
Discovery Policy	0
Client Identity	
Client Identity Name	
Match Expressions	
APLocation	1 Any 🗸 1
SSID Configuration	1 Any T
Group Configuration	Exact V Its-users
Radius User	1 Any 🗸 0
Wireless Client Filter	
Wireless Client MAC/MAC N	<i>l</i> ask
Captive Portal Connection	
Authentication State	🗊 🕘 Pre-Login 🔘 Post-Login 💿 Any
Authentication / Encryption	
Authentication Type	P Equals 🛛 🗸 P 🔽 Kerberos 🗌 MAC Authentication 🗌 None
Encryption Type	P Equals V CCMP KeyGuard TKIP WEP128 WEP64 None
± LDAP Attributes	
	OK Reset Exit

Role Policy Roles					×
cole Name tis-users					0
	Settings	Fire	wall Rules		
Vlan ID					
VLAN 1 (1 to 4,05	94)				
Application Policy		IP	Outbound		
Application Policy 🥜 tls-users	▼ ●		IP Firewall Rules Name	Precedence	Ŵ
IPv6 Inbound		- 6			
IPv6 Firewall Rules Name	Precedence				
0				+ Add	Row
		м	AC Inbound		•
	+ Add Row		MAC Firewall Rules Name	Precedence	Ш
IPv6 Outbound	A	6			
IPv6 Firewall Rules Name	Precedence III			+ Add	Row
0		м	AC Outbound		
	+ Add Row		MAC Firewall Rules Name	Precedence	ŵ
IP Inbound		- 6			
IP Firewall Rules Name	Precedence 前				
0				+ Add	Row
	+ Add Row				
			OK OK	Reset	xit
👫 Revert 陆 Commit	🔲 Commit a	and S	ave		
!					
role-policy firewalle user-role guest-user	ed-users s precedence	2 1			
ssid exact Z-Guest	in quest-use	rer	recedence 1		
use application-pol	icy guest-us	ers	Jiecedence i		
authentication-type	e eq eap	2			
encryption-type eq group exact peap-us	ccmp				
use application-pol	icy peap-use	ers			
authentication-type	precedence 3 e eq eap	5			
encryption-type eq group exact tls-use	ccmp ers				
use application-pol	icy tls-user	s			

Scenario 3 - Match based on Client Identity (DHCP Fingerprinting)

Scenario 3 will utilize a new approach in assigning roles, which involves client device/OS identification by using DHCP fingerprinting functionality. This is useful when it is required to differentiate between client devices using the same ESSID, same security type, same user identity, but different type of devices, like corporate IT managed Windows laptops and iOS or Android devices that employees are using on the same network, perhaps by enrolling them via company's MDM solution.

By leveraging built-in DHCP fingerprinting functionality it is possible to differentiate between different OS types and their versions. For instance an administrator may want to put a more restrictive policy to mobile devices, which are running outdated software, while only allowing laptops to access corporate apps, etc.

There are handful of built-in device signatures that come in WiNG 5 pre-installed by default, but custom ones can be defined as well based on DHCP options that clients are sending during the DHCP handshake. More details on how to easily track these values can be found in the Troubleshooting chapter of this guide.

In our example we will derive two additional roles out of existing "tls-users" role. All the mobile devices running latest iOS, Android or Windows Phone OS will get better service levels compared to devices running outdated software, while Windows-7 based laptops and only those which follow specific naming format will get access to internal corporate network.

The following sections will just show the configuration of the additional components (in order of configuration), which are:

- 1. Client Identity Configuration to identify corporate IT managed laptops
- 2. IP Access Lists Configuration
- 3. Application Policy Configuration
- 4. WLAN Configuration
- 5. Role Policy Configuration

Client Identity Configuration

In this section we will define a customized client identity based on Windows-7 identity to include a customized DHCP option 12 syntax that stands for the client name. All Windows 7 laptops that will contain 4 letter organization id will be matched against this identity.

Navigate to **Configuration > Security > Device Fingerprinting > Client Identity**. Find identity named "Windows-7", select it and click "Copy". Name it as "Corp-laptops".

Client Identity Configuration – Web UI

WING v5.8	Dashbo	Configur	Diagnos	Operati	Statistics	Q NX960	0 -		船 admin	Þ
Devices Wireless	Network Profiles	RF Domains	Security	Services	Managemen	t	튓 Revert	🛛 📥 Commi	t 금 Cor	mmit and Save
= 🎇 Wireless Firewall	Client Identity									0
🧱 Firewall Policy	Name									۲
MAC ACL	Blackberry									•
🗉 🌇 IP Firewall	Canon-Printer									
🙎 Wireless Client Rol	Galaxy-Note									
Device Fingerprinting	Galaxy-Tab									
🙎 Client Identity	Google-Android									
👤 Client Identity Gr	HP-LaserJet-Printer									
Intrusion Prevention	HTC-Android									
EX3500 Time Rang	iPhone-6									
(Gestobbe finite fraing	iPhone-iPad									
	Mac-OS-9									
🕵 Motorola-XOOM	Mac-OS-X									
Representation-3	Motoro									
🕵 Samsung-Galaxy-S-	Motorola-XUUM									
🕵 Sony-Ericsson-And	Samsung-Galaxy-S									
🕵 Symbian	Sonv-Ericsson-Androi	d								
🕵 Ubuntu-11	Symbian	-								_
🕵 Windows-10	Ubuntu-11									
🕵 Windows-10-Mobile	Windows-10									
Mindows-7	Windows-10-Mobile									
🕵 Windows-8	Windows-7									
Windows-Phone-7-	Windows-8									
🔐 Windows-XP	Windows-Phone-7-5									
C Xbox	Windows-XP									
Cebra-TC55	Xbox									
R Zebra-TCXX	Zebra-TC55									
Type to search	Zebra-TCXX									
	Type to search in tables	5							Row	Count: 36
						Add	Edit	Delete	Сору	Rename

×

Copy From Windows-7



Na	me Corp-lap	tops					0
DH	CP Match Criteria						
	Index	Message Type	Match Option	Match Type	Value Format	Option Value	Ŵ
	2	Request	55	Exact	Hex String	010f03062c2e2f1f2179f92b	ŵ
	9	Request	60	Exact	ASCII	MSFT 5.0	ŵ
0							
						+ Add Ro	ow.
Se	ttings						
	DHCP Match Mes	ssage Type 🕕 A	ny 🔻				
DH	CD Match Criteria						
211	Index	Message Type	Match Option	Match Type	Value Forma	t Option Value	Û
	2	Request	55	Exact	Hex String	010f03062c2e2f1f2179f92b	ŵ
	9	Request	60	Exact	ASCI	MSFT 5.0	ŵ
	*1	Request	Option 12 Option-Codes	Contains	1 ASCI	CZL0	ŵ
	> ок	Reset	Exit	·			1
5	Revert	🛃 Comr	nit 🛛 📄 Commit and Save				

Navigate to **Configuration > Security > Device Fingerprinting > Client Identity Group**. Now we need to add our new Client Identity to the default group to be able to use it for client identification.

Client Identity	Group	Configuration -	Web l	JI
------------------------	-------	-----------------	-------	----

WING v5.8	Dashboard	Configuration	Diagnostics	Operations	Statistics	IX9600	•		Å admin	- P
Devices Wireless Netw	vork Profiles	RF Domains Se	curity Servi	ces Manager	nent		5 Revert	🛃 Commit	🛛 🔒 Com	imit and Save
🗖 🎇 Wireless Firewall	Client Identity	/ Group								0
🧱 Firewall Policy	Name									(7)
MAC ACL	default									Ŭ
🚥 臍 IP Firewall										
🙎 Wireless Client Roles										
Device Fingerprinting										
🙎 Client Identity										
🙎 Client Identity Group										
Intrusion Prevention										
🐻 EX3500 Time Range										
Client identity Group										
Ma deladir	-									
	4									
Type to search	Type to search in	tables							Row C	Jount: 1
🔁 🖪 🗓 📫						Add	Edit	Delete	Сору	Rename

DHCP Match Criteria

	Client Identity	Precedence	Û
	Android-2-1	1,800	â 🛉
	Android-2-2	1,100	<u>ش</u>
	Android-2-3	1,000	û
	Android-2-3-x	1,200	ŵ
	Android-3	1,300	愈
U	Android-4	1,400	ŵ
	Android-4-1-X	2,200	ŵ
	Android-4-2-X	2,300	ŵ
	Android-6-0-X	10	愈
	Blackberry	2,900	<u></u>
			+ Add Row

Load Default Fingerprints -

Load Default Fingerprints 🛈 🗹

🐦 Corp-laptops	💌 📑 🎲 🌮 5	•	Ŵ
DK Reset	Exit		
5 Revert 🛃 Commit	🕞 Commit and Save		

Client Identity and Identity Group Configuration - CLI

```
client-identity Corp-laptops
 dhcp 1 message-type request option 12 contains ascii ZCZ09L
 dhcp 2 message-type request option 55 exact hexstring 010f03062c2e2f1f2179f92b
dhcp 8 message-type request option 60 exact ascii "MSFT 5.0"
client-identity-group default
client-identity Corp-laptops precedence 5
 client-identity Android-6-0-X precedence 10
 client-identity Windows-10 precedence 20
client-identity Windows-10-Mobile precedence 30
 client-identity iPhone-6 precedence 40
 client-identity Samsung-Galaxy-S precedence 50
 client-identity Google-Android precedence 100
 client-identity HTC-Android precedence 200
 client-identity Sony-Ericsson-Android precedence 300
 client-identity Galaxy-Note precedence 500
 client-identity Galaxy-Tab precedence 600
 client-identity Motorola-XOOM precedence 700
 client-identity Windows-XP precedence 800
 client-identity Windows-7 precedence 900
 client-identity Android-2-3 precedence 1000
 client-identity Android-2-2 precedence 1100
 client-identity Android-2-3-x precedence 1200
 client-identity Android-3 precedence 1300
 client-identity Android-4 precedence 1400
 client-identity iPhone-iPad precedence 1500
 client-identity Ubuntu-11 precedence 1600
 client-identity Windows-Phone-7-5 precedence 1700
 client-identity Android-2-1 precedence 1800
 client-identity Windows-8 precedence 1900
 client-identity Mac-OS-X precedence 2000
 client-identity Mac-OS-9 precedence 2100
 client-identity Android-4-1-X precedence 2200
 client-identity Android-4-2-X precedence 2300
 client-identity Symbian precedence 2400
 client-identity Playstation-3 precedence 2500
 client-identity Xbox precedence 2600
 client-identity HP-LaserJet-Printer precedence 2700
 client-identity Canon-Printer precedence 2800
 client-identity Blackberry precedence 2900
load default-fingerprints
```

IP Access List and Application Policy Configuration

In the below example we have created two ACLs named "**old-mobile-units**" and "**new-mobile-units**". For old mobile devices we will have a restricted ACL that will only allow outgoing web traffic, we are dropping any other IP traffic and logging hits. ACL for the new mobile devices will be more relaxed, only limiting these devices to access internal corporate network, while all the outgoing traffic to the internet is allowed.

Furthermore, we are going to create three application policies for each role. Application policy for legacy mobile devices will take care of dropping peer to peer application traffic, VPN and video streaming services, while app policy for new devices will only set up rate limiters on application markets to prevent these devices to consume all the bandwidth in the event of automatic update push, for example when Apple would release a new iOS version. Note that Application Policy requires an Access Point to support DPI engine.

Navigate to Configuration > Security > IP Firewall > IPv4 ACL > Add.

IP Access List Configuration – Web UI

IP	Fire	wall Policy	old-byod-	devices								0
		Preceden	Action	DNS Name	DNS Match	Source	Destination	Protocol	Mark	Log	Enable	Description
≢		3	Allow		Not Set	🔆 Any	🔆 Any	DDP SPort 68, DPort 67	Mark	Log	😨 Enable	"Permit DHCP"
≢	,	5	Allow		Not Set	🔆 Any	8.8.8.8	DDP , DPort 53	Mark	Log	😨 Enable	"Permit DNS"
≢	J.	40	Allow		Not Set	🔆 Any	🔆 Any	DPort 80	Mark	Log	😨 Enable	"Allow HTTP"
≢	<i>"</i>	50	Allow		Not Set	🔆 Any	🔆 Any	DPort 443	Mark	Log	😨 Enable	"Allow HTTPS"
≢	J.	100	🔀 Deny		Not Set	🔆 Any	🔆 Any	➡ P	N/A	🗹 Log	🕑 Enable	

IP	Fire	wall Policy	new-byod	-devices								0
		Preceden	Action	DNS Name	DNS Match	Source	Destination	Protocol	Mark	Log	Enable	Description
=	ļ	3	Allow		Not Set	🔆 Any	🔆 Any	DP SPort 68, DPort 67	Mark	🗌 Log	🕑 Enable	"Permit DHCP"
=	ļ	5	Allow		Not Set	🔆 Any	8.8.8.8	DP, DPort 53	Mark	Log	🕑 Enable	"Permit DNS"
=	ļ	10	🔀 Deny		Not Set	🔆 Any	<i>j</i> 192.168.0	D 🖨 IP	N/A	🗹 Log	🕐 Enable	"block access to internal r
≣	ļ	100	Allow		Not Set	🔆 Any	🔆 Any	⇔ P	Mark	Log	🕑 Enable	

Application Policy Configuration - Web UI

rime							
lime							
Time							
Start Time	En	d Time		ŵ			
				14 Dam			
			- AC				
ction Application Category	Default Application	Custom Application	Mark Type M	lark Value	Outbound Traffic Rate	Inbound Traffic Rate	Schedule Polic
Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 46	Tark Value	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	Schedule Policy
ction Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 48	lark Value	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	Schedule Policy
Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 46	fark Value S	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	Schedule Polic;
Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 46	Tark Value 5	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	Schedule Policy
Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 46	lark Value	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	Schedule Policy
Istion Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 46	lark Value	Outbound Traffic Rate Not Set	Inbound Traffic Rate Not Set	Schedule Polic
Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 46	lark Value S	Outbound Traffic Rate Not Set	Inbound Treffic Rate Not Set	Schedule Polic;
Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 48	Tark Value 3	Outbound Traffic Rate Not Set	Inbound Treffic Rate Not Set	Schedule Polic;
Application Application Category Mark -	Default Application Skype for Business_auc	Custom Application	Mark Type M dscp 46	Tark Value 3	Outbound Traffic Rate Not Set	Inbound Traffic Rate	Schedule Polic;
	Solit Inne		Sould linke		start i me u + Add Row	Seek Linne End Inne U	start rind the finite the fi



IP Access List Configuration - CLI

```
ip access-list old-mobile-units
permit udp any eq 68 any eq dhcps rule-precedence 3 rule-description "permit DHCP"
permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description "permit DNS traffic"
permit tcp any any eq 80 rule-precedence 40 rule-description "HTTP Allow"
permit tcp any any eq 443 rule-precedence 50 rule-description "HTTPS Allow"
deny ip any any log rule-precedence 100
!
ip access-list new-mobile-units
permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description "permit DHCP"
permit udp any eq 68 any eq dhcps rule-precedence 5 rule-description "permit DHCP"
permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description "permit DHCP"
permit udp any host 8.8.8.8 eq 53 rule-precedence 5 rule-description "permit DNS traffic"
deny ip any 192.168.0.0/16 log rule-precedence 10 rule-description "block access to internal network and
log hits"
permit ip any any rule-precedence 50 rule-description "Allow all outgoing traffic"
```

Application Policy Configuration - CLI

```
application-policy old-byod-devices
deny app-category streaming precedence 1
deny app-category p2p precedence 2
deny app-category tunnel precedence 3
!
application-policy new-byod-devices
rate-limit application ios-app-store ingress rate 1024 max-burst-size 16 egress rate 1024 max-burst-size
16 precedence 4
rate-limit application windows-store ingress rate 1024 max-burst-size 16 egress rate 1024 max-burst-size
16 precedence 5
rate-limit application Google_play ingress rate 1024 max-burst-size 16 egress rate 1024 max-burst-size 16
precedence 6
!
application-policy corp-laptops
mark application "Skype for Business_generic" dscp 46 precedence 1
!
```

WLAN Configuration

WLAN Configuration needs to be edited to allow dynamic VLAN assignments using our Role Based Firewall.

Navigate to Configuration > Wireless > Wireless LANs > select "TMELABS-DOT1X" > Click "Edit".

WLAN TMELABS-DOT1X		
Basic Configuration	WLAN Configuration	
Basic Configuration Security Firewall Client Settings Accounting Service Monitoring Client Load Balancing Advanced Auto Shutdown	WLAN Configuration SSID Description WLAN Status QoS Policy Bridging Mode DHCP Option 82 DHCPv6 LDRA Bonjour Gatew ay Discovery Policy Other Settings Broadcast SSID Answ er Broadcast Probes VLAN Assignment © Single VLAN © VLAN Pool VLAN 25 RADIUS VLAN Assignment Allow RADIUS Override © V	TMELABS-DOT1X Image: Constraint of the second state of the second st
		U <none></none>

CLI

```
wlan TMELABS-DOT1X
ssid TMELABS-DOT1X
vlan 25
bridging-mode local
encryption-type ccmp
authentication-type eap
radius vlan-assignment
use aaa-policy External-AAA
use ip-access-list out BROADCAST-MULTICAST-CONTROL
use mac-access-list out PERMIT-ARP-AND-IPv4
!
```

Role Policy Configuration

As a last step we need to modify our role policy that was created in the first two scenarios and replace "tlsusers" role with three new roles matching based on client identity. Also in this scenario we will make use of the default role for the devices that didn't match any defined identities. Each role will also assign a device into a different VLAN for traffic isolation.

First role will identify corporate Windows 7 laptops to give them no network access restrictions and prioritize Skype for Business traffic. Next role match will identify newer BYOD devices running latest Android, iOS, Windows 10 or MAC OS X and will give them full access to the internet, while restricting access to internal network and rate-limit app stores bandwidth utilization (apple itunes, google play, microsoft store). Last role will not have a match based on client identity, but since role assignment happens based on first-match principle, everything that will not fall under "corp-laptops" or "new-byod-devices" role based on client identity will end up under "old-byod-devices" automatically, since this is our lowest precedence rule.

Navigate to Configuration > Security > Wireless Client Roles > select "firewalled-users" > Roles > Add:

ole Name corp-laptops											6
		Setti	ngs	Fire	ewall Ru	les					
o configure LDAP attributes in t	the Role	, the LDAP	Settin	qs she	ould be co	onfiqu	red firs	t.			
lole Precedence						_					
Precedence	*	3	• (1 to 10	0,000)						
oniour Gateway		L	•								
Discovery Policy						••	.593.				
							238				
Client Identity Name	Γ						0				
Client Identity Name		<none></none>					¥ 💖	-			
	0	Corp-laptop	S								
latch Expressions											
APLocation	0	Апу		•	0						
SSID Configuration	0	Any		•	0						
Group Configuration	0	Exact		•	0 tis-u	isers					
Radius User	0	Any		•	0						
/ireless Client Filter											
Wireless Client MAC/MAC Ma	ask 🗿	00 - 00 - 0	0 - 00	- 00	- 00 or	🗸 An	у				
aptive Portal Connection											
Authentication State	0(Pre-Login		Post-l	.ogin 🖲	Any					
uthentication / Encryption											
Authoritie ation Truns	_										
Authentication Type	0	Equals	•	0 🗸	EAP	Kert	peros	MACA	uthentic	ation 📃	None
Encryption Type	0	Equals Equals	•	0 ∨	EAP	Kert	oeros [eyGuard OK	MAC A	uthentic WE	ation	None WE
Aumenication Type Encryption Type CUAP AUMOUTES ELUAP AUMOUTES Eleventes	0	Equals Equals	•	0 1	ЕАР [ССМР [Kert	oeros [yGuard OK	MAC A	uthentic WE	ation	None WE
Autoenclautor Type Encryption Type CDAP Autobutes ECOAP Autobutes Re Policy Roles Dele Name corp-laptops	1 0	Equals Equals	↓ ▼	0 🗸	EAP	Kert	oeros [yGuarc OK	MAC A	uthentic WE	ation	None WE
Autoentication Type Encryption Type ELDAP Autobutes Re Policy Roles Die Name corp-laptops		Equals Equals Sett	▼ ▼	0 V	EAP	Kert	oeros (yGuaro OK	MACA	uthentic Wt	ation	None WE
Autoentication Type Encryption Type ELDAP Attributes Re Policy Roles Die Name corp-laptops	3 0 3 0	Equals	▼ ▼	0 V	EAP	Kert	oeros (yGuarc OK	MACA	uthentic WE	ation	None WE
Authenication Type Encryption Type EDAP Authoutes le Policy Roles ble Name corp-laptops an ID	(1 to 4,05	Equals Equals Sett	v v	0 ✓ 0 ✓	EAP	Kert	overos (ayGuard OK	MAC A	uthentic WE	ation	None WE
Authentication Type Encryption Type ELDAP Attributes ILE Policy Roles Die Name corp-laptops an ID VLAN VLAN	(1 to 4,05	Equals Equals Sett	↓ ▼	0 ✓ 0 ✓	EAP	Kert	oeros [yGuard OK		uthentic	ation	None WE
Authentication Type Encryption Type ELDAP Attributes ILE Policy Roles ILE Policy	(1 to 4,05	Equals Equals Sett	tings	€ ✓ Fire	CCMP	Kert	operos (yyGuarco OK		uthentic WE	ation	None WE
Autoentication Type Encryption Type EDRY Autobutes Re Policy Roles ble Name corp-laptops an ID VLAN VIAN VIAN VLAN VIAN Application Policy Corp-laptop corp-laptop	(1 to 4,05	Equals Equals Sett	tings	O ✓ O ✓	CCMP	Kert Ke	oeros (oK oK		Prec	edence	None WE
Autoentication Type Encryption Type EDAP Attributes RePolicy Roles Die Name corp-laptops an ID VLAN VIAN VIAN VLAN VIAN Application Policy Corp-laptop Corp-laptop Corp-laptop	1 to 4,05	Equals Equals Sett 14)	tings	O ✓ O ✓ Fire	CCMP	Kert	or o		Prec	edence	None WE
Authenication Type Encryption Type EDAP AUTIDUCES EDAP AUTION EDAP AUTIDUCES EDAP AUTION EDAP AUTIDUCES EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTIDUCES EDAP AUTION EDAP AUTION ED	(1 to 4,05	Equals Equals Sett (4)	tings	O ▼ O ▼	CCMP	Kert Ke	oeros (OK OK		Prec	edence	None WE
Authenication Type Encryption Type EDAP AUTIDUTES EDAP AUTION EDAP AUTIDUTES EDAP AUTIDUTES EDAP AUTION EDAP AUTIDUTES EDAP AUTION EDAP AUTI	(1 to 4,05 ps	Equals Equals Set (4)	tings	O ✓ O ✓ Fire	ewall Rule	Kert	oeros (yyGuarco OK		Prec	edence	None WE
Authenication Type Encryption Type ELDAP AUTIDUCES Re Policy Roles De Name corp-laptops an ID VLAN VIAN VIAN VLAN VIAN pplication Policy Application Policy Corp-laptop for hoound IPo6 Firewall Rules Name	1 to 4,05	Equals Equals Set 14) cedence	tings	O ✓ O ✓ Fire	CCMP	Kert Ke	oeros (OK Rules N	MACA MACA	Prec	edence	None WE
Autoentication Type Encryption Type EDAP AUTIDUTES EDAP AUTION POLICY EDAP AUTIDUTES EDAP AUTION POLICY EDAP AUTION POLICY EDAP AUTION POLICY EDAP AUTION POLICY EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP AUTION EDAP	(1 to 4,05	Equals Eq	tings	€ V € V € V	CCMP	Kert Kee es d 	oeros (OK Rules N	MACA NACA	Prec	edence	None WE
Autoentication Type Encryption Type EDAP Attributes EDAP Attributes ED	(1 to 4,05 ps	Equals Eq	tings	€ ✓ Fire	EAP	Kerti Ke	oeros (OK Rules N	MACA TKIP	Prec	edence	None WE
Autoentication Type Encryption Type E LDAP AUTIDUCES E LDAP AUTIOUCES E LDAP AUT	1 to 4,05	Equals Equals (Sett (4) (+ Add I cedence	iings	G V Fire	CCMP	Kert	oeros (OK Rules N	MACA	Prec	edence	None WE
Autoentication Type Encryption Type EDAP AUTIDUCES EDAP AUTIOUCES EDAP AUT	1 to 4,05 Pre Pre	Equals Equals Set 14) cedence cedence	tings	E Fire	CCMP CCMP COMP CONTROL COMP CO	Kert	oeros (OK Rules N:	ame	Prec	edence	None WE
Autoentication Type Encryption Type EDRP Attributes EDRP Attributes ED	(1 to 4,05	Equals Eq	tings		EAP	d	oeros (OK Rules N	ame	Prec	edence	None WE
Authentication Type Encryption Type EDAP AUTIDUCES EDAP AUTIOUCES EDAP AUT	(1 to 4,05 Pre Pre	Equals Eq		G V G V Fire M M	EAP	Kert Ke	oeros (oK Quies N Rules N	MACA MACA	Vithentic Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite	edence + Add edence	None WEI it Row
Autoentication Type Encryption Type ELDAP Attributes ELDA	1 to 4,05	Equals Equals Equals (Set (+ Add I cedence	tings	G V Fire S	EAP	Kert Kert Ke	oeros (oK Rules N all Rules	MAC A	Preceive Pre	edence Add edence	None WEI it Row
Admendation Type Encryption Type Encryption Type EDAP Admonstrate EDAP Adm	1 to 4,05	Equals Equals Equals Set 14) (+ Add I cedence	tings	E Fire	EAP	Kert Kert Ke	oeros (OK Rules N all Rules	MAC A	Vithentic Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite Vite	edence Add edence	None WEJ it Row
Authentication Type Encryption Type Encryption Type EDAP AUTIDUCES De Policy Roles De Name corp-laptops an ID VLAN VIEN VLAN VIEN Polication Policy Corp-laptop Corp-laptop Corp-laptop Corp-laptop v6 Inbound IPv6 Firewall Rules Name Inbound IP Firewall Rules Name	(1 to 4,05 ps Pre Pre	Equals Equals Equals Set (+ Add I cedence cedence	tings		EAP	Kert Ke	oeros (OK Rules N all Rules	MACA MACA Reference	Vertication of the second seco	ation	None WEI it Row

	0.44	nge Firer	all Rules		
	Setti	ngs Firew			
Information					
configure LDAP attributes in th	e Role, the LDAP Setting	is should be ci	onfigured first.		
le Precedence					
Precedence	* 4 (1	to 10,000)			
niour Gateway					
Discovery Policy	0	_	≣0 <i>s</i> ∰.		
	•				
Client Identity					
Clent licentity Name	<none></none>				
	Android-6-0-X iPhone-6	ľ			
	Windows-10-Mob	ile 🖡			
tch Expressions				7	
APLocation	🚺 Any	• 0			
SSID Configuration	1 Any	• 0			
Group Configuration	Exact	🔻 🛈 tis-u	sers	1	
Radius User	0 Any	• 0			
reless Client Filter					-
Wireless Client MAC/MAC Mas	k 🕕 00 - 00 - 00 - 00	- 00 - 00 or	✓ Any		
ptive Portal Connection					_
Authentication State	0 🔘 Pre-Login 🄘 F	Post-Login 🖲	Any		
thentication / Encryption					-
Authentication Type	🚺 Equals 🛛 🔻	0 🗹 EAP [Kerberos MAC Authen	tication 📃 None	
Encryption Type	🚺 Equals 🛛 🔻		KeyGuard TKIP	WEP128 WEP64 N	lone
			р⊳ ок	Reset Exit	
			В ок	Reset Exit	
la Policy Poles			№ ок	Reset Exit	
le Policy Roles	vices		№ ок	Reset Exit	
ile Policy Roles Dile Name new-byod-de	vices		🕅 ок	Reset Exit	
le Policy Roles Die Name new-byod-de	vices	ttings Fir	ewall Rules	Reset Exit	
le Policy Roles Dile Name new-byod-de	vices	ttings Fir	ewali Rules	Reset Exit	
Ile Policy Roles Die Name new-byod-de	vices Se	ttings Fir	ewall Rules	Reset Exit	
Ile Policy Roles Die Name new-byod-de an ID VLAN VI 26	Vices Se	ttings Fir	ewall Rules	Reset Exit	
le Policy Roles Die Name new-byod-de an ID VLAN ₽₽ 26	Vices Se	ttings Fir	ewall Rules	Reset Exit	
le Policy Roles De Name new-byod-de an ID VLAN ♥♥ 26 ♥ Application Policy	Vices Se	ttings Fir	ewall Rules P Outbound	e Precedence	
le Policy Roles De Name new-byod-de an ID VLAN ♥♥ 28 € optication Policy Application Policy ● new-by	Vices Se (1 to 4,094) rod-devices	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam	e Precedence	
Ile Policy Roles De Name new-byod-de an ID VLAN IM I 26 Splication Policy Application Policy I new-by 76 Inbound	Vices Se (1 to 4,094) (1 to 4,094) vod-devices	ttings Fir	ewall Rules P Outbound	e Precedence	
Ile Policy Roles Dile Name new-byod-de an ID VLAN VIAN VIAN VLAN VIAN VLAN VIAN VLAN VLAN VLAN VIAN	vices Se (1 to 4,094) rod-devices Precedence	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam	e Precedence	
Ile Policy Roles Die Name new-byod-de an ID VLAN VIEW 26 Splication Policy Application Policy r6 Inbound IPv6 Firewall Rules Name	vices Se (1 to 4,094) (1 to 4,094) rod-devices Precedence	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam	e Precedence	: Id Ro
Ile Policy Roles Die Name new-byod-de an ID VLAN VIEW 26 Application Policy Application Policy f6 Inbound IPu6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,094) Vod-devices Vod-devices Vod-devices Vod-devices	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam	e Precedence	dd Ro
le Policy Roles Die Name new-byod-de an ID VLAN V 26 Application Policy Application Policy f6 Inbound IPu6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,094) Precedence		OK ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N	e Precedence	dd Ro
le Policy Roles Die Name new-byod-de an ID VLAN VIAN VIAN VLAN VIAN VLAN VIAN VLAN	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N	e Precedence	dd Ro
le Policy Roles De Name new-byod-de an ID VLAN IN IN 26 Splication Policy Application Policy Inew-by r6 Inbound IPv6 Firewall Rules Name Application Policy	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N	e Precedence ame Precedence	ld Ro
ie Policy Roles Die Name new-byod-de an ID VLAN IN IN 26 Application Policy Application Policy Inew-by r6 Inbound IPv6 Firewall Rules Name IPv6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,094) Precedence Add Precedence Precedence	ttings Fir	ewall Rules P Outbound P Outbound P Firewall Rules Nam MAC Inbound MAC Firewall Rules N	e Precedence ame Precedence	dd Ro
le Policy Roles De Name new-byod-de an ID VLAN IN IN ISON 26 Splication Policy Application Policy Inew-by r6 Inbound IPv6 Firewall Rules Name Pv6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N	e Precedence ame Precedence + Ad	Id Ro
Ile Policy Roles Die Name new-byod-de an ID VLAN VIEN VIEN VIEN VIEN VIEN VIEN VIEN VIEN	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N MAC Sirewall Rules N MAC Outbound	e Precedence ame Precedence + Ad ame Precedence	dd Ro
le Policy Roles Die Name new-byod-de an ID VLAN V 26 application Policy Application Policy f6 Inbound IPu6 Firewall Rules Name IPu6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir		e Precedence + Ad ame Precedence + Ad	Id Ro
le Policy Roles De Name new-byod-de an ID VLAN V 26 Application Policy Application Policy f6 Inbound IPu6 Firewall Rules Name IPu6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N MAC Sirewall Rules N MAC Firewall Rules N MAC Firewall Rules N	e Precedence ame Precedence t Ad ame Precedence	id Ro
le Policy Roles Die Name new-byod-de an ID VLAN V 26 pplication Policy Application Policy f6 Inbound IPv6 Firewall Rules Name Pv6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N MAC Cutbound MAC Firewall Rules N MAC Firewall Rules N	e Precedence ame Precedence t Ad ame Precedence	id Ro
le Policy Roles ple Name new-byod-de an ID VLAN IN IN IN 26 Splication Policy Application Policy Inew-by r6 Inbound IPv6 Firewall Rules Name IPv6 Firewall Rules Name IPv6 Firewall Rules Name	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	OK ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N MAC Firewall Rules N MAC Firewall Rules N MAC Firewall Rules N	e Precedence ame Precedence t Ad ame Precedence	dd Ro
le Policy Roles ple Name new-byod-de an ID VLAN IN IN IN 26 pplication Policy Application Policy Inew-by r6 Inbound IPv6 Firewall Rules Name Pv6 Firewall Rules Name IPv6 Firewall Rules Name IPv6 Firewall Rules Name new-byod-devices	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N MAC Firewall Rules N MAC Firewall Rules N MAC Firewall Rules N	e Precedence ame Precedence t Ad ame Precedence	id Ro
le Policy Roles Die Name new-byod-de an ID VLAN IN IN IN IN IN IN INC. Application Policy Inew-by r6 Inbound IN IN INC. IPv6 Firewall Rules Name IPv6 Firewall Rules Name IPv6 Firewall Rules Name IPv6 Firewall Rules Name Inbound INC.	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N MAC Cutbound MAC Firewall Rules N MAC Firewall Rules N	e Precedence ame Precedence t Ad ame Precedence t Ad ame Precedence	id Ro
le Policy Roles De Name new-byod-de an ID VLAN IN IN IN IN IN INC. Application Policy Application Policy Application Policy IPv6 Firewall Rules Name IPv6 Firewall Rules Name IPv6 Firewall Rules Name IPv6 Firewall Rules Name IPv6 Firewall Rules Name New-byod-devices	Vices Se (1 to 4,094) (1 to 4,0	ttings Fir	ewall Rules P Outbound IP Firewall Rules Nam MAC Inbound MAC Firewall Rules N MAC Firewall Rules N MAC Coutbound MAC Firewall Rules N	e Precedence	id Ro

Role Policy Roles					×
Role Name old-byod-device	ces				0
	Se	tinge Firewall Rules			
	30				
Information					_
To configure LDAP attributes in th	e Role, the LDAP Sett	ngs should be configured fir	st.		
Role Precedence					
Precedence	* 6	(1 to 10,000)			
Bonjour Gateway					
Discovery Policy	0	v 🖻 🌞			
Client Identity					
Client Identity Name	<none></none>	- P (8)			
	0				
	•		-10°		
Match Expressions					
APLocation	Apv	v 0			
SSID Configuration					
Group Configuration	O Any	• •			
Group Configuration	O Exact	▼ 0 tis-users			
Radius User	1 Any	▼ 0			
Wireless Client Hiter	k 🕷 💿 💿 💿				
Cantiva Partal Connection	0 00 - 00 - 00 - 00 - 00 - 00 - 00 - 0	Any			
Authentication State	0 Pre-Login	Post-Login @ Any			
Authentication / Encryption	C Tro-Edgin (Tost-Edgin @ Aity			
Authentication Type	6 Equals	0 ✓ F∆P Kerberos	MAC Authentication	None	
Encryption Type	Equals				
	E COOLOGIO 1		d TKID WED128	WEDGA I	None
		CCMP ReyGuar	d TKIP WEP128	WEP64	None
		CCMP ReyGuar	d TKIP WEP128	eset Exi	None 🕌
Role Policy Roles		KeyGuar	d TKIP WEP128	s WEP64 I	None 💌
Role Policy Roles Role Name old-byod-devi	ces	KeyGuar	d TKIP WEP128	WEP64 I	t ×
Role Policy Roles Role Name old-byod-devi	ces	CONP KeyGuar	d TKIP WEP128	Set Exi	t x
Role Policy Roles Role Name old-byod-devi	ces	ttings Firewall Rules	d TKIP WEP128	: WEP64 I	t ×
Role Policy Roles Role Name old-byod-devi	ces	ttings Firewall Rules	d TKIP WEP128	set Ext	t ×
Role Policy Roles Role Name old-byod-devi	ces S	ttings Firewall Rules	d TKIP WEP128	Set Ext	t X
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VLAN 25	ces \$ (1 to 4,094)	ttings Firewall Rules		WEP64	t x
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VIAN 25	CES S	ttings Firewall Rules	d TKIP WEP128	WEP64	None X
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VLAN V 25 Application Policy Application Policy old-byoc	Ces S (1 to 4,094)	ttings Firewall Rules	d TKIP WEP128	Precedence	None × 2
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VIAN VIAN VIAN VIAN VIAN VIAN VIAN VI	Ces S (1 to 4,094) 4-devices	IP Outbound	d TKIP WEP128	Precedence	
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VIAN VIAN VIAN VIAN VIAN VIAN VIAN VI	Ces S (1 to 4,094)	IP Outbound IP Firewall	d TKIP WEP128	VEP64 I	
Role Policy Roles Role Name old-byod-devi Vlan D VLAN VLAN VLAN VLAN VLAN VLAN VLAN VLAN	Ces (1 to 4,094) d-devices Precedence	IP Outbound	d TKIP WEP128	Precedence	x 2
Role Policy Roles Role Name old-byod-devi Vlan D VLAN P 25 Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Name	Ces (1 to 4,094) 4-devices Precedence	IP Outbound -	d TKIP WEP128	Precedence	None v t 2 2 Row
Role Policy Roles Role Name old-byod-devi Vlan D VLAN VLAN V 25 Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Hame	ces s (1 to 4,094) 4-devices Precedence	ttings Firewall Rules IP Outbound - IP Outbound - IP MAC Inbound -	d TKIP WEP122	Precedence	None T
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VLAN VIAN VIAN VIAN VIAN VIAN VIAN VIAN VI	Ces (1 to 4,094) (1 to 4,094) d-devices Precedence + Ad	IP Outbound IP Outbound IP Firewall IP Machine MAC Inbound Row	d TKIP WEP128	Precedence Precedence Precedence	None T
Role Policy Roles Role Name old-byod-devi Vlan D VLAN VLAN VLAN VLAN VLAN VLAN VLAN VLAN	Ces (1 to 4,094) (1 to 4,094) A-devices Precedence Add Addevices	IP Outbound	d TKIP WEP128	Precedence Precedence Precedence	None
Role Policy Roles Role Name old-byod-devi Vlan D VLAN 25 Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Name IPv6 Outbound IPv6 Firewall Rules Name	Ces (1 to 4,094) (1 to 4,094) (1 to 4,094) Precedence Precedence Precedence	IP Outbound - IP Outbound - IP Firewall MAC Inbound Row MAC Fire	d TKIP WEP128	Precedence Precedence Precedence	None t X Row Row
Role Policy Roles Role Name old-byod-devi Vlan D VLAN P 25 Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Name IPv6 Outbound IPv6 Firewall Rules Name	Ces S (1 to 4,094) 4-devices Precedence Ad Precedence	IP Outbound IP Outbound IP Firewall IIP Machine IIII IIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	d TKIP WEP122	Precedence Precedence Add	None
Role Policy Roles Role Name old-byod-devi Vlan D VLAN P 25 Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Name IPv6 Outbound IPv6 Firewall Rules Name IPv6 Pirewall Rules Pirewall Rul	CES (1 to 4,094) (ttings Firewall Rules IP Outbound IP Outbound IP Firewall IP MAC Inbound MAC Inbound IR OW IMAC Inbound INAC Inbound	d TKIP WEP122	Precedence Add Precedence Add	None t
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VLAN VIAN VIAN VIAN VIAN VIAN VIAN VIAN VI	Ces S (1 to 4,094) d-devices Precedence + Ad	IP Outbound IP Outbound IP Firewall IP MAC Inbound MAC Inbound MAC Inbound MAC Inbound	d TKIP WEP128	Precedence + Add Precedence + Add	None T
Role Policy Roles Role Name old-byod-devi Vlan D VLAN VLAN VLAN VLAN VLAN VLAN VLAN VLAN VLAN	Ces (1 to 4,094) (IP Outbound IP Outbound IP Firewall Rules MAC Inbound MAC Inbound MAC Inbound MAC Fire MAC Outbound Row	d TKIP WEP128	VVEP64 VVEP64 VEP64 Exi Precedence Precedence Add Precedence Add Precedence	Row Row
Role Policy Roles Role Name old-byod-devi Vlan D VLAN 25 Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Name IPv6 Outbound IPv6 Firewall Rules Name IPv6 Pirewall Rules Name IPv6 Dutbound	Ces S (1 to 4,094) 4-devices Precedence Precedence Additional and a second	IP Outbound IP Outbound IP Firewall IIP Firewall III MAC Inbound III MAC Inbound III MAC Fire III MAC Outbound III MAC Fire III MAC Fire III MAC Outbound	d TKIP WEP128	VVEP64 VVEP64 VVEP64 VEV VVEP64 Exi Precedence Add Precedence Add Precedence Add	None
Role Policy Roles Role Name old-byod-devi Vlan D VLAN 25 Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Name IPv6 Outbound IPv6 Firewall Rules Name IPv6 Pirewall Rules Name IPv6 Pirewall Rules Name IPv6 Pirewall Rules Name IPv6 Na	Ces s (1 to 4,094) 4-devices Precedence Add Precedence Add Precedence	IP Outbound IP Outbound IP Firewall IP Firewall IIP MAC Inbound III MAC Fire III MAC Outbound III MAC Fire III MAC Fire	d TKIP WEP128	VEP64 1 Sect Exi Sect Exi Sect Add Precedence Add Precedence Add Precedence Add	None
Role Policy Roles Role Name old-byod-devi Vlan D VLAN P VLAN P Application Policy Application Policy Application Policy IPv6 Inbound IPv6 Firewall Rules Name	Ces (1 to 4,094) d-devices Precedence Precedence Precedence Precedence 1	IP Outbound IP Outbound IP Firewall Rules IIP Firewall IIP MAC Inbound IIII IIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	d TKIP WEP122	VVEP64 1 Sect Exi Precedence + Add Precedence + Add	None t t Row Row Row
Role Policy Roles Role Name old-byod-devi Vlan ID VLAN VLAN IPus Firewall Rules Name	Ces Ces (1 to 4,094) (1 to 4,09	IP Outbound IP Outbound <t< td=""><td>d TKIP WEP122</td><td>VVEP64 VVEP64 V VEP64 V VEP64 V VEP64 V VE V V V V V V V V V V V V V V V V V</td><td>Row Row</td></t<>	d TKIP WEP122	VVEP64 VVEP64 V VEP64 V VEP64 V VEP64 V VE V V V V V V V V V V V V V V V V V	Row Row

CLI

```
role-policy firewalled-users
user-role guest-users precedence 1
 ssid exact Z-Guest
 use ip-access-list in guest-users precedence 1
 use application-policy guest-users
user-role peap-users precedence 2
 authentication-type eq eap
 encryption-type eq ccmp
 group exact peap-users
 use application-policy peap-users
user-role corp-laptops precedence 3
 assign vlan 27
 authentication-type eq eap
 encryption-type eq ccmp
 group exact tls-users
 client-identity Corp-laptops
 use application-policy corp-laptops
user-role new-byod-devices precedence 4
 assign vlan 26
 authentication-type eq eap
 encryption-type eq ccmp
 group exact tls-users
 client-identity Android-6-0-X
 client-identity Mac-OS-X
 client-identity iPhone-6
 client-identity iPhone-iPad
 client-identity Windows-10-Mobile
 client-identity Ubuntu-11
 use ip-access-list in new-byod-devices precedence 1
 use application-policy new-byod-devices
user-role old-byod-devices precedence 6
 assign vlan 25
 authentication-type eq eap
 encryption-type eq ccmp
 group exact tls-users
 use ip-access-list in old-byod-devices precedence 1
 use application-policy old-byod-devices
```

Verification

The configuration has been completed and now we can verify that roles are being assigned correctly. We expect that clients connecting to SSID "Z-Guest" will match our role-policy and will thus only be allowed to go out to the internet without any access to p2p or streaming services. Clients that authenticate using PEAP-MSCHAPv2 will be assigned a different role with p2p services disabled and video streaming services limited to 1024Kbps up and downstream. Finally, clients authenticating using EAP-TLS method will have access to all of the services on the network, additionally Skype for Business traffic will be marked with DSCP 46. All other clients that do not match any criteria will be assigned a default role with no restrictions.

After we connect few clients to our network we can view role policy state under client statistics: CLI Role Policy Verification

WING v5.8	Dashboard Configur	ratio	n Diagnostics	Operations	Statistics			Q NX96	00 🔻		🚺 🔒 admin	Þ
System Guest Acces	3											
🖃 🔇 System 🕤	RF Domain BUILDING-1											. ?
E Drno	🔇 Health		MAC Address	IP Address	Hostname	Role	Client	Vendor	Band	AP	WLAN	VLAN
■ Crzech Republic ■ mo ■ Tebra ■ CEDA ■ CEDA	Inventory □ Devices □ Device Upgrade □ Wireless Clients □ Device Upgrade □ Wireless LANs □ Pavice Upgrade □ Wireless LANs □ Pavice Upgrade □ Wireless LANs □ Bluetooth □ Mesh □ Mesh □ Captive Portal □ Device Portal □ A WIPS □ Coverage Hole Detection	*	MAC Address 40-83-DE 78-EF-EF 8C-70-5A-80-4E-A8 40-83-DE 78-EF-F1	IP Address 192.168.25.94 192.168.27.100 192.168.26.99	Hostname android-13e3efe6 ZC209L01CGJ854 android-dc688368	Role guest-users Its-users peap-users	Client Identity Zebra-TCSS Windows-7 Zebra-TCXX	Vendor Zebra Tech Intel Corp Zebra Tech	Band 11an 11an	AP Hostmane CEDAR-D-3 CEDAR-B-4 CEDAR-B-4 CEDAR-B-4	VQLAN Z-Guest TMELABS-DOT1X TMELABS-DOT1X	VLAN 25 27 26
		Тур	e to search in tables								Row	Count: 3
Search								lisconnect A	II Client	Is Disconn	ect Client	Refresh

Role Statistics - Web UI

Statistics							
Wireless Client 8C-70-54	A-60-4E-A8						
😵 Health	Wireless Client		Association				
🍮 Details	SSID	TMELABS-DOT1X	AP	74-67-F7-07-08-1B			
and Traffic	Hostname	ZCZ09L01CGJ864	BSS	74-67-F7-64-A2-E0			
WMM TSPEC	Device Type	Non Voice	Radio Number	2			
lassociation History	RF Domain	BUILDING-1	Radio Type	11an			
⊗Graph d	os	Unknow n	Rates	6 9 12 18 24 36 48 54 mcs-1s mcs-2			
	Browser	Unknow n	802 11 Protocol				
	Туре	Unknow n					
	Role	corp-laptops	High-Throughput	 Supported 			
	Role Policy	firew alled-users	RIFS	X Unsupported			
	Client Identity	Corp-laptops	Unscheduled PASD	Disabled			
	Client Identity Precedence	5	AID	1			
	Client Identity Precedence	Ŭ	Max AMSDU Size	7,935			
	User Details		Max AMPDU Size	65,535			
	UserName	john@cztac.zebra.local	Interframe Spacing	0			
	Authentication	eap	Short Guard Interval	✓ Supported			
	Encryption	ccmp					
	Captive Portal Auth.	× No					

Role Statistics - CLI

NX9600-Controller-	·l#show wireless client detail on <ap hostname=""></ap>
ADDRESS :	40-83-DE-78-EE-F1 - android-dc688368 192.168.26.99(vlan:26)
USERNAME :	john
WLAN :	TMELABS-DOT1X (ssid:TMELABS-DOT1X)
ACCESS-POINT :	Name:CEDAR-B-4 Location:BUILDING-1
RADIO-ID :	74-67-F7-07-08-1B:R2, alias CEDAR-B-4:R2
RADIO-NAME :	radio2 Bss:74-67-F7-64-A2-E0
STATE :	Data-Ready
CLIENT-INFO :	802.11an, vendor: Extreme Tech
SECURITY :	Authentication: eap Encryption: ccmp
FAST-ROAMING :	Fast-BSS-Trans: N
DATA-RATES :	6 9 12 18 24 36 48 54 mcs-1s
MAX-PHY RATE :	150 M
MAX-USER RATE	112 M
802.11n/802.11ac	: Short guard interval: Y Channel width (capability: 40MHz Current: 40MHz)
:	AMSDU Max-Size: 3839 AMPDU Max-Size: 65535 AMPDU Min-Spacing: 0 uSec
:	STBC: Y Transmit BeamForming: N MU-MIMO: N
OoS :	WMM: Y Type: Non Voice
POWER-MGMT :	PS-Mode: Y Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
TPC :	Y : TPC Power 7
ACTIVITY :	Last Active: 00:27.22 ago
SESSION INFO :	Session Timeout: 0 days 23:59.56 Idle Timeout: 00.:30.00
RF-DOMAIN :	BUILDING-1
ROLE :	peap-users/firewalled-users
DHCP INFO :	Client Identity: Extreme-TCXX Precedence: 3100
HTTP INFO :	Type: Unknown OS: Unknown Browser: Unknown
ADDRESS :	8C-70-5A-60-4E-A8 - ZCZ09L01CGJ864 192.168.27.100(vlan:27)
USERNAME :	john@cztac.extreme.local
WLAN :	TMELABS-DOT1X (ssid:TMELABS-DOT1X)
ACCESS-POINT :	Name:CEDAR-B-4 Location:BUILDING-1
RADIO-ID :	74-67-F7-07-08-1B:R2, alias CEDAR-B-4:R2
RADIO-NAME :	radio2 Bss:74-67-F7-64-A2-E0
STATE :	Data-Ready
CLIENT-INFO :	802.11an, vendor: Intel Corp
SECURITY :	Authentication: eap Encryption: ccmp
FAST-ROAMING :	Fast-BSS-Trans: N
DATA-RATES :	6 9 12 18 24 36 48 54 mcs-1s mcs-2s
MAX-PHY_RATE :	300 M
MAX-USER_RATE :	225 M
802.11n/802.11ac	: : Short guard interval: Y Channel width (capability: 40MHz Current: 40MHz)
:	AMSDU Max-Size: 7935 AMPDU Max-Size: 65535 AMPDU Min-Spacing: 0 uSec
:	STBC: Y Transmit BeamForming: N MU-MIMO: N
QoS :	WMM: Y Type: Non Voice
POWER-MGMT :	PS-Mode: N Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
TPC :	Y : TPC Power 8
ACTIVITY :	Last Active: 00:00.01 ago
SESSION INFO :	Session Timeout: 0 days 23:48.42 Idle Timeout: 00.:30.00

© 2017 Extreme Networks, Inc. All rights reserved.

```
: BUILDING-1
 RF-DOMAIN
         : Client Identity: Windows-7 Precedence: 900
: Type: Unknown OS: Unknown Browser: Unknown
 HTTP INFO
Total number of clients displayed: 2
NX9600-Controller-1#show wireless client detail on CEDAR-D-3
         : 40-83-DE-78-EF-EE - android-13e3efe6... 192.168.25.94(vlan:25)
 ADDRESS
           : 40-83-DE-78-EF-EE
 USERNAME
 WLAN
            : Z-Guest (ssid:Z-Guest)
 ACCESS-POINT : Name:CEDAR-D-3 Location:8533-bld1-fl1
          : 74-67-F7-07-09-3D:R2, alias CEDAR-D-3:R2
 RADIO-ID
           : radio2 Bss:74-67-F7-64-9C-51
: Data-Ready
 RADIO-NAME
 STATE
 CLIENT-INFO : 802.11an, vendor: Extreme Tech
 SECURITY : Authentication: mac Encryption: none
FAST-ROAMING : Fast-BSS-Trans: N
           : 6 9 12 18 24 36 48 54 mcs-1s
 DATA-RATES
 MAX-PHY RATE : 150 M
 MAX-USER RATE : 112 M
 802.11n/802.11ac : Short guard interval: Y Channel width (capability: 40MHz Current: 40MHz)
           : AMSDU Max-Size: 3839 AMPDU Max-Size: 65535 AMPDU Min-Spacing: 0 uSec
           : STBC: Y Transmit BeamForming: N MU-MIMO: N
           : WMM: Y Type: Non Voice
 OoS
           : PS-Mode: Y Spatial-Multiplexing-PS: off WMM-PS/U-APSD: Disabled
 POWER-MGMT
 TPC
           : Y : TPC Power 14
           : N
 PMF
 ACTIVITY
 ACTIVITY : Last Active: 00:00.05 ago
SESSION INFO : Session Timeout: 7 days 00:00.00 Idle Timeout: 12.:00.00
 RF-DOMAIN : BUILDING-1
 MCAST STREAMS :
           : guest-users/firewalled-users
: Client Identity: Extreme-TC55 Precedence: 3200
 HTTP INFO
           : Type: Android Tablet OS: Android Browser: Chrome
Total number of clients displayed: 1
NX9600-Controller-1#show role wireless-clients on CEDAR-B-4
_____
           Role policy: firewalled-users
_____
Role: guest-users
                  _____
____
    -----
     8C-70-5A-60-4E-A8
_____
     40-83-DE-78-EE-F1
_____
_____
NX9600-Controller-1#show role wireless-clients on CEDAR-D-3
_____
           Role policy: firewalled-users
_____
     40-83-DE-78-EF-EE
_____
Role: tls-users
_____
Role: peap-users
_____
_____
```

Troubleshooting

The easiest way to troubleshoot or verify role-based firewall functionality is to use remote-debug wireless feature that allows to take logs from the whole site filtered by a particular client MAC.

Role Assignment Debugging -Remote Debug Wireless

EAP-TLS client example, notice received User Group id highlighted:

```
////part of the output remove for brevity///
NX9600-Controller-1#remote-debug wireless rf-domain BUILDING-1 clients 8C-70-5A-60-4E-A8 max-events 999
duration 999 events eap management radius system wpa-wpa2
Printing up to 999 messages from each remote system for up to 999 seconds. Use Ctrl-C to abort
[CEDAR-B-4] 14:45:19.275: mgmt:rx auth-req from 8C-70-5A-60-4E-A8 on radio 1 (mgmt.c:3842)
[CEDAR-B-4] 14:45:19.275: mgmt:tx auth-rsp to 8C-70-5A-60-4E-A8 on radio 1. status: success (mgmt.c:1305)
[CEDAR-B-4] 14:45:19.276: mgmt:rx association-req from 8C-70-5A-60-4E-A8 on radio CEDAR-B-4:R2 signal-
strength is -38dBm (mgmt.c:3823)
[CEDAR-B-4] 14:45:19.276: mgmt:Client 8C-70-5A-60-4E-A8 negotiated WPA2-EAP on wlan (TMELABS-DOT1X)
(mgmt.c:3382)
[CEDAR-B-4] 14:45:19.276: mgmt:tx association-rsp success to 8C-70-5A-60-4E-A8 on wlan (TMELABS-DOT1X)
(ssid:TMELABS-DOT1X) with ftie 0 (m
[CEDAR-B-4] 14:45:19.277: client:state MU STATE DOT1X for client 8C-70-5A-60-4E-A8 (mgmt.c:1209)
[CEDAR-B-4] 14:45:19.277: client:wireless client 8C-70-5A-60-4E-A8 changing state from [Roaming] to
[802.1x/EAP Auth] (mgmt.c:625)
[CEDAR-B-4] 14:45:19.277: eap:sending eap-code-request code 1, type 1 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.277: eap:sending eap-id-req to 8C-70-5A-60-4E-A8 (eap.c:990)
[CEDAR-B-4] 14:45:19.331: eap:rx eap id-response from 8C-70-5A-60-4E-A8 (eap.c:696)
[CEDAR-B-4] 14:45:19.331: radius:aaa-policy External-AAA user: john@cztac.extreme.local mac: 8C-70-5A-60-
4E-A8 server is candidate: 1 0 0 0
[CEDAR-B-4] 14:45:19.332: radius:access-reg sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (rad
[CEDAR-B-4] 14:45:19.335: radius:RAD MSG AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.335: radius:rx access-challenge from radius server for 8C-70-5A-60-4E-A8
(radius.c:3811)
[CEDAR-B-4] 14:45:19.335: eap:sending eap-code-request code 1, type 25 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.335: eap:sending eap-req [eap type:25(peap)] to 8C-70-5A-60-4E-A8 (eap.c:998)
[CEDAR-B-4] 14:45:19.336: eap:rx eap pkt from 8C-70-5A-60-4E-A8 (eap.c:719)
[CEDAR-B-4] 14:45:19.337: radius:access-req sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (radius.c:1181)
[CEDAR-B-4] 14:45:19.338: radius:RAD_MSG_AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.338: radius:rx access-challenge from radius server for 8C-70-5A-60-4E-A8
(radius.c:3811)
[CEDAR-B-4] 14:45:19.338: eap:sending eap-code-request code 1, type 13 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.338: eap:sending eap-req [eap_type:13(eap-tls)] to 8C-70-5A-60-4E-A8 (eap.c:998)
[CEDAR-B-4] 14:45:19.366: eap:rx eap pkt from 8C-70-5A-60-4E-A8 (eap.c:719)
[CEDAR-B-4] 14:45:19.366: radius:access-req sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (rad
[CEDAR-B-4] 14:45:19.368: radius:RAD MSG AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.368: radius:rx access-challenge from radius server for 8C-70-5A-60-4E-A8
(radius.c:3811)
[CEDAR-B-4] 14:45:19.368: eap:sending eap-code-request code 1, type 13 to 8C-70-5A-60-4E-A8 (eap.c:963)
[CEDAR-B-4] 14:45:19.368: eap:sending eap-req [eap_type:13(eap-tls)] to 8C-70-5A-60-4E-A8 (eap.c:998)
[CEDAR-B-4] 14:45:19.370: eap:rx eap pkt from 8C-70-5A-60-4E-A8 (eap.c:719)
[CEDAR-B-4] 14:45:19.371: radius:access-req sent to 192.168.7.15:1812 (attempt 1) for 8C-70-5A-60-4E-A8
(user:john@cztac.extreme.local) (rad
[CEDAR-B-4] 14:45:19.375: radius:RAD MSG AUTHENTICATOR (radius.c:1181)
[CEDAR-B-4] 14:45:19.375: radius:rx
                                                                                         (radius.c:1825)
[CEDAR-B-4] 14:45:19.375: radius:rx access-accept for 8C-70-5A-60-4E-A8 (radius.c:3565)
[CEDAR-B-4] 14:45:19.375: radius:radius: updating interim acct timeout of 8C-70-5A-60-4E-A8 to 1800 seconds
(radius.c:2137)
[CEDAR-B-4] 14:45:19.375: eap:sending eap-success to 8C-70-5A-60-4E-A8 (eap.c:1006)
[CEDAR-B-4] 14:45:19.375: client:802.1x authentication success for client 8C-70-5A-60-4E-A8 (eap.c:1139)
[CEDAR-B-4] 14:45:19.375: client:starting WPA2-CCMP keying for client 8C-70-5A-60-4E-A8 (eap.c:1215)
[CEDAR-B-4] 14:45:19.375: client:wireless client 8C-70-5A-60-4E-A8 changing state from [802.1x/EAP Auth] to
[802.11i Keying] (mgmt.c:625)
[CEDAR-B-4] 14:45:19.376: wpa-wpa2:tx msg #1 to 8C-70-5A-60-4E-A8 attempt: 1 (80211i.c:617)
[CEDAR-B-4] 14:45:19.380: wpa-wpa2:rx msg #2 from mu 8C-70-5A-60-4E-A8 (80211i.c:1164)
[CEDAR-B-4] 14:45:19.381: wpa-wpa2:tx msg #3 to 8C-70-5A-60-4E-A8 attempt: 1 (80211i.c:891)
```

[CEDAR-B-4] 14:45:19.382: wpa-wpa2:rx msg #4. WPA2-AES handshake done. 8C-70-5A-60-4E-A8 DATA-READY
(80211i.c:1148)
[CEDAR-B-4] 14:45:19.386: client:wireless client 8C-70-5A-60-4E-A8 changing state from [802.11i Keying] to
[Data-Ready] (mgmt.c:625)
[CEDAR-B-4] 14:45:19.386: client:starting mu-idle timer for 8C-70-5A-60-4E-A8 (mgmt.c:104)
[CEDAR-B-4] 14:45:19.386: client:8C-70-5A-60-4E-A8 session-timeout: unlimited idle-timeout: 1800
(mgmt.c:455)
[CEDAR-B-4] 14:45:19.386: client:credcache_apply_app_policy_name (credcache.c:1111)
[CEDAR-B-4] 14:45:19.386: client:update_app_policy_name_to_credcache (credcache.c:1032)
[CEDAR-B-4] 14:45:19.386: client:Adding app_policy_name to credcache and sync8C-70-5A-60-4E-A8
(credcache.c:1035)
[CEDAR-B-4] 14:45:19.390: client:RoleInfo: 8C-70-5A-60-4E-A8 idx: 3, client_idx: 0, vlan_id: 27, role_name:
tls-users (extif.c:2149)
[CEDAR-B-4] 14:45:19.390: client:client 8C-70-5A-60-4E-A8 assigned rate-limit (to-air/from-air = 0/0 on
wlan TMELABS-DOT1X (mgmt.c:218)

Guest SSID client example:

```
////part of the output remove for brevity///
NX9600-Controller-1#remote-debug wireless rf-domain BUILDING-1 clients E8-B1-FC-
4B-B0-81 max-events 999 duration 999 events all
Printing up to 999 messages from each remote system for up to 999 seconds. Use Ctrl-C to abort
[CEDAR-C-2] 14:56:35.130: mgmt:rx auth-req from E8-B1-FC-4B-B0-81 on radio 1 (mgmt.c:3842)
[CEDAR-C-2] 14:56:35.130: mgmt:tx auth-rsp to E8-B1-FC-4B-B0-81 on radio 1. status: success (mgmt.c:1305)
[CEDAR-C-2] 14:56:35.131: mgmt:rx association-req from E8-B1-FC-4B-B0-81 on radio CEDAR-C-2:R2 signal-
strength is -65dBm (mgmt.c:3823)
[CEDAR-C-2] 14:56:35.131: client:MU E8-B1-FC-4B-B0-81 panBU enab cap=00 00 00, supp cap=00 00 00 00
(mgmt.c:3085)
[CEDAR-C-2] 14:56:35.131: client:using cached vlan 25 for wireless client E8-B1-FC-4B-B0-81 (mgmt.c:3317)
[CEDAR-C-2] 14:56:35.131: mgmt:tx association-rsp success to E8-B1-FC-4B-B0-81 on wlan (Z-Guest) (ssid:Z-
Guest) with ftie 0 (mgmt.c:3437)
[CEDAR-C-2] 14:56:35.131: client:wireless client E8-B1-FC-4B-B0-81 changing state from [Roaming] to [MAC
Auth] (mgmt.c:625)
[CEDAR-C-2] 14:56:35.131: radius:aaa-policy Internal-NX user: E8-B1-FC-4B-B0-81 mac: E8-B1-FC-4B-B0-81
server is candidate: 1 0 0 0 0 0 (r
[CEDAR-C-2] 14:56:35.132: radius:access-req sent to wireless controller to be proxied via its adopter
centralized controller (if any) to 1
[CEDAR-C-2] 14:56:35.132: client:restarting mac auth timer for E8-B1-FC-4B-B0-81 (radius.c:4677)
[CEDAR-C-2] 14:56:35.133: client:transmitting roam notification for E8-B1-FC-4B-B0-81 (mgmt.c:348)
[CEDAR-C-2] 14:56:35.136: radius:rx access-reject for E8-B1-FC-4B-B0-81 (radius.c:3711)
[CEDAR-C-2] 14:56:35.136: radius:failover to captive-portal for non data-ready MU E8-B1-FC-4B-B0-81
(radius.c:3752)
[CEDAR-C-2] 14:56:35.136: client:wireless client E8-B1-FC-4B-B0-81 changing state from [MAC Auth] to [Data-
Ready] (mgmt.c:625)
[CEDAR-C-2] 14:56:35.137: client:starting mu-idle timer for E8-B1-FC-4B-B0-81 (mgmt.c:104)
[CEDAR-C-2] 14:56:35.137: client:E8-B1-FC-4B-B0-81 session-timeout: unlimited idle-timeout: 43200
(mgmt.c:455)
[CEDAR-C-2] 14:56:35.137: client:credcache_apply_app_policy_name (credcache.c:111)
[CEDAR-C-2] 14:56:35.137: client:update app policy name to credcache (credcache.c:1032)
[CEDAR-C-2] 14:56:35.137: client:Adding app_policy_name to credcache and sync E8-B1-FC-4B-B0-81
(credcache.c:1035)
[CEDAR-C-2] 14:56:35.231: client:RoleInfo: E8-B1-FC-4B-B0-81 idx: 1, client_idx: 1, vlan_id: 25, role_name:
 uest-users (extif.c:2149)
[CEDAR-C-2] 14:56:35.232: client:client E8-B1-FC-4B-B0-81 assigned rate-limit (to-air/from-air = 0/0 on
wlan Z-Guest (mgmt.c:218)
```

Client Identity a.k.a DHCP Fingerprinting Debugging

```
#debug role dhcpfp level debug on <AP hostname>
#show logging on <AP hostname> | include <client MAC>
DPD2: 2016-07-11 16:45:18 dhcpfp.c:493 dhcp_fingerprint_client 8C-70-5A-60-4E-A8: client identified as
(Windows-7, 900), fp state=0x0c
DPD2: 8C-70-5A-60-4E-A8: message-type request option 81 exact hexstring
000005a435a30394c303143474a3836342e637a7461632e7a656272612e6c6f63616c
DPD2: 8C-70-5A-60-4E-A8: message-type request option 61 exact hexstring 018c705a604ea8
DPD2: 8C-70-5A-60-4E-A8: message-type request option 60 exact ascii MSFT 5.0
DPD2: 8C-70-5A-60-4E-A8: message-type request option 55 exact hexstring 010f03062c2e2f1f2179f92b
DPD2: 8C-70-5A-60-4E-A8: message-type request option 50 exact hexstring c0a81b64
DPD2: 8C-70-5A-60-4E-A8: message-type request option 12 exact ascii ZC209L01CGJ864
DPD2: 8C-70-5A-60-4E-A8: message-type request option-codes exact hexstring 353d320c513c37
DPD2: 2016-07-11 16:37:21 dhcpfp.c:577 handle_dhcp_fingerprint fingerprint from wireless client
```