

Deployment Guide

RWG - Microsegmentation Step-by-Step Configuration

June 2023

Rev. 1



Table of Contents

Changes
INTENDED AUDIENCE
OBJECTIVES
TEST BED
Test Components
Test Topology
CONFIGURATION
Step 1 - Verify that the vSZ Instance is Adopted and in Sync
Step 2 – Verify that the ICX Switch is Adopted and in Sync
Step 3 – VLAN Interfaces
Step 4 – Network Addresses
Step 5 – Enable the NAT Entry in RWG10
Architecture Recap
Step 6 – Switch Port Profiles
Step 7 – Check the RADIUS Realm in SmartZone15
SmartZone in a Remote Location
Step 8 - RADIUS Realms in RWG
Step 9 - WLAN Configuration
TESTING MICROSEGMENTATION
RWG Policies Overview
Using the Search Tool
Ping Test
Disable the Block Subnets Rule
TROUBLESHOOTING
The Wireless Client Does Not Associate to the 802.1x SSID27
The Wireless Client Does Receive an IP Adddress
There is No Internet Connectivity
CONCLUSION



Changes in Revision 1

- Minor corrections.
- Added new troubleshooting technique VLAN ID 4095 needs to be configured on ESXi.
- Added note about NAT and private networks defined by RFC 1918.
- Added details around non-proxy zones.

Intended Audience

This document is a step-by-step guide on how to configure microsegmentation using RWG.

The audience for this document is System Engineers who want to deploy the RUCKUS WAN Gateway (RWG) for L2/L3 microsegmentation using regular VLANs configured in the ICX switches, SmartZone controllers and access points. It is expected that the reader possesses a working knowledge on ICX switches and SmartZone, RADIUS, routing, and security concepts.

For more information on how to configure RUCKUS products, please refer to the appropriate RUCKUS user guide available on the RUCKUS support site at https://support.ruckuswireless.com/

The RWG documentation is embedded into the product. You can access the embedded documentation at <u>https://{your RWG_IP_address}/admin/manual/help_online</u>



Objectives

Deploy and test a L2/L3 microsegmentation solution using ICX switches and SmartZone controllers with the following features:

- The wireless clients will connect to an unsecure SSID configured with 802.1x and MAC Bypass.
- No portals will be presented to the client, and they will have full internet access.
- Each wireless client will be placed in a separate VLAN and IP subnet.
- The wireless clients will be isolated no traffic will be allowed from one client to another.

Test Bed

Test Components

The following components were used for the examples and tests described in this document:

Virtual SmartZone High-Scale (sw version 6.1.0.0.935)

- VM running in an Intel NUC mini-PC, using only one interface.
- Besides the Staging Zone, only one zone is configured (named Solar System)
- One R550 is onboarded and online in zone Solar System (fw version 6.1.0.0.1595)
- No wlans are configured.

ICX 7150C12-POE (sw version 9.0.10d, routing code)

- Before adoption by RWG, the only configurations were:
- The interface ve1 was created.
- DHCP-client was enabled for virtual interfaces (using ip dhcp-client ve default)
- A read-only SNMP community string was added (using snmp-community public ro)

RWG (build 14.065)

- Bare-metal installation in a Qotom 4-LAN mini-PC with 8GB RAM and 128GB SSD (Q190G4U-S02)
- Installed a non-wildcard SSL certificate from Let's Encrypt US
- The vSZ instance and the ICX switch are adopted and in sync.



Test Topology

In this test topology, the Qotom mini server running RWG uses interface **igb0** to connect to a Xfinity router. By default, igb0 is pre-configured as a DHCP client, and igb3 is pre-configured as a DHCP server.

Note that this is a test scenario - igb0 received a private IP address. In production networks, the server running RWG is generally connected to an ISP that provides a public IP address directly to the igb0 interface.

igb3 comes pre-configured with IP address 192.168.5.1/24.

The ICX switch, vSZ instance and R500 received their IP addresses from the DHCP server configured at igb3 in RWG.



FIGURE 1 – TEST TOPOLOGY



Configuration

Step 1 - Verify that the vSZ Instance is Adopted and in Sync

Navigate to **Network/Wireless** and to check the status of the vSZ instance. It should be online and in sync. Scroll down to see the discovered access point and zones. The access point should also be online.

WL	AN Cont	rollers												
	Name 🛆	Online	Туре	Host	Monitoring	Config sync status	WLANs	Locati events	ion s	Model	Version	Access Points		Monitoring interval
	vSZ- 6100395	\oslash	Ruckus SmartZon	192.168.5.249 e	1	Ø 01/05/2023 10:34 AM				vSZ-H	6.1.0.0.935	R550[34:20:e3:	28:0d:a0]	10
Acce	ess Points	5												
	Name 🛆	Online	Controller	AP Zone Profile	IP	MAC	Clients	2.4GHz	5GHz	State	Uptime	Last seen	Model	Version
	R550	0	vSZ- 6100395	Default Solar AP System Profile [Solar System]	Q 192.168.5.247	Q 34:20:e3:28:0d:a0	3	10	56	Connect	t 9 hours and 55 minutes	01/05/2023 08:22 PM	R550	6.1.0.0.1595
Acce	ess Point	Zones												
	Name	\bigtriangleup	Controller	Access	Points	AP Profiles				Enab	le DFS channe	els	5GHz cha	nnel width
	Solar Sys	stem	√SZ-610039	5 R550[3	4:20:e3:28:0d:a0]	Default AP Pr	rofile (Solar Sy	/stem]		\checkmark			20 MHz	
	Staging	Zone	√SZ-610039	5	-		-			~			20 MHz	

FIGURE 2 – SMARTZONE IS ONLINE AND IN SYNC

For details on how to adopt devices, please refer to the slide deck **RWG Adoption of Devices**.

Step 2 – Verify that the ICX Switch is Adopted and in Sync

Navigate to **Network/Wired** to check the status of the ICX switch. It should be online and in sync.

Swit	Switches												
	Name 🛆	Online	Туре	Host	Monitoring	Config sync status	Location events	Model	Version	Ports	Pms rooms	Monitoring interval	
	ICX 7150- B	\oslash	Ruckus ICX Switch	192.168.5.242	2	Ø 01/05/2023 10:47 AM		Stackable ICX7150- C12-POE	Version 09.0.10dT213	GigabitEthernet]/1/2, GigabitEthernet]/1/3, GigabitEthernet]/1/4, (16)	-	10	

FIGURE 3 – ICX IS ONLINE AND IN SYNC

For details on how to adopt devices, please refer to the slide deck **RWG Adoption of Devices**.



Step 3 – VLAN Interfaces

RWG supports IEEE 802.1Q VLANs with up to 4094 VLAN IDs. For further scalability, Q-in-Q is also supported.

No VLAN interfaces are created in RWG by default. A VLAN interface can include just one VLAN ID, or a range of VLAN IDs. You can also configure how many IP subnets each VLAN ID can support. Let's create a range of VLAN interfaces in RWG, then push the VLANs to the ICX switch.

Navigate to Network/LAN, and click Create New in the VLAN Interfaces section:

VLAN Interfaces Create											
	Name 🛆	Physical Interface $ riangleq$	Service VLAN 🛆	Parent	VLAN IDs	I-SIDs	Autoincrement	Addresses	Switch Port Profiles	WLANs	
					No Entrie	25					
0 Found	b										

FIGURE 4 – CREATE NEW VLAN INTERFACE

Enter the following information:

- Name: Enter a name for the VLAN interface. Here, we used Onboard VLANs.
- **Physical Interface**: select the RWG physical interface that is connected to the ICX switch. It is **igb3** in our test bed.
- VLAN IDs: Enter the first VLAN ID of the range. Here, we entered **300**.
- Autoincrement: The options are none, per-subnet, and per-IP. Select per-subnet.
- Ratio: Enter 1. This will allow only one subnet per VLAN. This a typical configuration for MDU use cases.

Create VLAN Interface		
Name	Onboard VLANs	
Note		
Parent (Hide)		
Physical Interface	igb3 v parent physical Ethernet interface	
Service VLAN	- select - v Q-in-Q parent VLAN interface	
Tags (Hide)		
VLAN IDs	300 ‡	first 802.1Q VID
I-SIDs		first SPBM I-SID ass
Autoincrement	per-subnet auto-increment L2 w/ L3 n tags = (subnets / ratio) ~
Ratio	1	number of autoincr
Networks (Hide)		
Addresses	Select All None Reset Management LAN	
	addresses assigned to this VLAN	
Infrastructure (Hide)		
Switch Port Profiles		
WLANS	no options WLANs that utilize this VLAN for dynamic VLAN assign	ments
Conference Tool (Hide)		
Conference options	no options	
Create Cancel		

FIGURE 5 – CREATE VLAN INTERFACE

Click **Create** to finish.



Step 4 – Network Addresses

In this step we will create the IP subnets which will be associated to the VLANs. When we configured the VLAN interface, we defined that there will be a 1:1 relationship between VLANs and IP subnets. The IP subnets are created using **Network Addresses**.

A network address entry can include only one IP address, or a range of IP subnets. Then the network address can be associated to a VLAN interface. We can also define that a DHCP scope will be automatically created for each IP subnet. Navigate to **Network/LAN**, and click **Create New** in the **Network Addresses** section:

Netwo	rk Addresses					Zend GARP 🔇	🕽 Refresh 🔀 Expo	ort 🛷 Batch	💠 Zoom ? Help	🔍 Sea	rch 🔘 C	reate New
	Name	\bigtriangleup	Primary	IPv6 PD Uplink	IP	Ethernet	VLAN	OpenVPN				
	Management LAN		V		192.168.5.1/24	igb3				Edit	Delete	Show
1 Found												

FIGURE 6 – CREATE NEW NETWORK ADDRESS

Note: The network address for the Management LAN entry is created in RWG during the installation.

Enter the following information:

- Name: Enter a name for the network address. Here, we used Onboard Addresses.
- Ethernet: Do not select any interface, otherwise there will be a conflict with the VLAN selection.
- VLAN: Select the Onboard VLANs interface created earlier.
- IP: Enter 20.0.0.1/30. That will be the first address of the first subnet. A /30 subnet has only four IP addresses hosts, and two are available for hosts.
- Autoincrement: Enter 64. That will result in 64 IP subnets being created.
- Create DHCP Pool: Enable the checkbox to create one DHCP pool for each IP subnet.

Create Network Address	
Name	Onboard Addresses
Note	
Interface (Hide)	
Ethernet	- select - v interface to configure address(es) with
VLAN	Onboard VLANs VLAN to configure address(es) with
OpenVPN	- select - OpenVPN server to assign address(es) with
Addresses (Hide)	
Primary	rimary and first configured subnet on the interface/VLAN
IP	20.0.0.1/30
IPv6 PD Uplink	- select - Vplink which will provide the IPv6 Prefix Delegation(PD
Autoincrement	64
Span	1
Provisioning (Hide)	
Create DHCP Pool	automatically configure a DHCP pool for entire subnet(s)
IP Group	- None - v assign this network to an IP Group
Create Cancel	

FIGURE 7 – CREATE NETWORK ADDRESS

Click **Create** to finish.



Step 4b – Check VLAN Interfaces and Network Addresses

In the **Network Addresses** section, the Onboard Addresses entry shows the IP subnet range from 20.0.0.1/30 to 20.0.0.253/30. That includes 64 subnets (each /30 subnet has 4 addresses).

Click the **Refresh** button under the **VLAN Interfaces** section. You will see a range of 64 VLAN IDs from 300 to 363. Start a SSH session to RWG and use the command ifconfig to see the interfaces.

The sample below shows vlan 300 and vlan 301. Note the starting IP address for the subnets in each VLAN.

												marcelo@rwg-home ~]\$ ifconfig vlan300 lan300: flags=8843 <up_broadcast_running_simplex_muuticast> metric</up_broadcast_running_simplex_muuticast>
	N Interface	Physical	Se	rvice _	Parent	VLAN	ŀ	Autoincremer	t Addres	efresh Export Switch ses Port	ØE	<pre>options=4600003<rxcsum,txcsum,rxcsum_ipv6,txcsum_ipv6,nomah ether ac:1fi6b:74:0c:5b inet 20.0.0.1 netmask 0xffffffc broadcast 20.0.0.3 groups: vlan nat refl</rxcsum,txcsum,rxcsum_ipv6,txcsum_ipv6,nomah </pre>
		Interface	VL	AN		IDS	SIDs			Profiles		vlan: 300 vlanproto: 802.1q vlanpcp: 0 parent interface: ig
	Onboard VLANs	igb3			igb3	300 - 363 (64)		1 tags per- subnet	Onboa	rd -		media: Ethernet autoselect (1000base⊺ <full-duplex>) status: active</full-duplex>
l Found	d vork Addre	sses						2 Send	IGARP 🕻	efresh 🛃 Export	0E	marcelo@rwg-home ~]\$ if config Vlan301 lan301: flags=8843 <up,broadcast,running,simplex,multicast> metric (</up,broadcast,running,simplex,multicast>
	Name	Δ	Primary	IPv6 P	D Uplink	IP			Ethernet	VLAN		options=4600003 <rxcsum,txcsum,rxcsum_ipv6,txcsum_ipv6,nomap></rxcsum,txcsum,rxcsum_ipv6,txcsum_ipv6,nomap>
	Managemer	nt LAN	13			192.168.5	3/24		igb3			inet 20.0.0.5 netmask 0xfffffffc broadcast 20.0.0.7
	Onboard Ad	dresses	123			20.0.0.1/	50 - 20.0.0.2	53/30 (64)		Onboard VLAN	s	groups: vlan
2 Foun	d											vlan: 301 vlanproto: 802.1q vlanpcp: 0 parent interface: igt media: Ethernet autoselect (1000baseT <full-duplex>) status: active</full-duplex>
												nd6 options=9 <performnud, ifdisabled=""></performnud,>



Step 4c – Check DHCP Pools in RWG

Navigate to **Services/DHCP** to see the entries for the DHCP pools created by RWG:

DHCP P	ools						E	🗟 Columns 십 Refresh 🔀 Export 🛷 Batch
	Name	\bigtriangleup	Start IP	End IP	Reserved	Option Group	Class	Network
	Management LAN		192.168.5.10	192.168.5.254			-	Ethernet igb3
	Onboard Addresses		20.0.0.2	20.0.0.254	-	-	-	VLAN "Onboard VLANs (300 – 363)
2 Found								

FIGURE 9 – DHCP POOLS

That entry **Onboard Address** is a collection of pools. To see the details, you need to open a SSH session to RWG. We will do that in the next section.



Step 4d – Check the DHCP Pools in RWG

You can also check the DHCP pools created by RWG for VLAN 300. Open a SSH session to RWG and use the following commands:

ifconfig vlan300 (to see the entry for VLAN 300)

cat /etc/dhcpd.conf (to see the entire DHCP server daemon configuration file)



FIGURE 10 – DHCP CONFIGURATION FILE

Step 5 – Enable the NAT Entry in RWG

RWG is a router, and it uses NAT to map its local private address to the RWG uplink – which normally uses a public IP address (in our tests it also uses a private IP address), otherwise the internal networks will not have Internet access.

When a new subnet is created, RWG creates a new NAT entry automatically, but keeps it disabled. You need to enable it manually. To enable NAT for the **Onboard Address** entry we created earlier, navigate to **Network/NAT**, and click **Edit** in the entry **Disable NAT on "Onboard Addresses":**

NATs						Columns	🕻 Refresh 🔀 Export 🛷 B	latch 💠 Zoom 💡 Helj	o 🔍 Sean	ch 🛈 C	reate New
	Name	\bigtriangleup	Uplinks	Start IP	End IP	Static port	Addresses	Static Routes			
	20221012202423_add_explicit_nat_rule		Uplink	-	-		Management LAN	-	Edit	Delete	Show
	Disable NAT on "Onboard Addresses"		-	-	-		Onboard Addresses	-	Edit	Delete	Show

FIGURE 11 - EDIT A NAT ENTRY

Note: A NAT entry will not be created for the private subnets defined by RFC 1918 (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16). RWG will automatically enable NAT for those subnets, even without a NAT entry showing in the NAT scaffold.



Enter the following information:

- Name: Change the name to NAT on "Onboard Addresses"
- Uplinks: Check Uplink
- Addresses: Make sure Onboard Addresses is selected. It shows at the right of the blank field.

Update Disable NAT on "On	board Addresses"
Name	NAT on "Onboard Addresses"
Note	
WAN Translation (Hide)	
Uplinks	Select All None Reset
	uplinks to perform NAT through (none to disable NAT for selected subnets)
Reverse NAT (not recommended)	Cause traffic sent via selected Uplink to be NAT'd to the first IP of the selected Address (not re
IP Adjustments (optional)	(Hide)
Start IP	first WAN IP to NAT to
End IP	last WAN IP to NAT to
Static port	retain packet source port - "cone" instead of "symmetric NAT" (not recommended)
Subnets (Hide)	
Addresses	Onboard Addresses
Static Routes	no options routed subnets to perform NAT for
Update Cancel	

FIGURE 12 - UPDATING THE NAT ENTRY

Click **Update** to finish.



Architecture Recap

When a wireless client associates to a WLAN configured with 802.1x and MAC bypass, the access point sends an authorization request to the RADIUS server running in RWG. The RADIUS server responds with a message that contains the VLAN tag that will be used for the wireless client traffic when it is forwarded across the switch ports.

The exact VLAN tag is determined by an algorithm used by the internal NAC in RWG, but it will ultimately come from the VLAN range that we defined earlier. Therefore, the switch ports used to forward the traffic (1/1/6 and 1/1/12) need to be pre-configured as tagged interfaces with all VLAN IDs defined in the VLAN range.

No configuration is required in the access point's ethernet interface, because by default, all RUCKUS access points come with the ethernet interface already configured as tagged (trunk) ports for all VLANs.



FIGURE 13 – VLANS WITH TAGGED INTERFACES IN THE ICX SWITCH

RWG includes a RADIUS server, and it acts as a NAC (Network Admission Control) server to assign VLANs dynamically to wired or wireless clients. As mentioned before, the WLANs use 802.1x Mac Bypass to send an authentication request to the RADIUS server. The RADIUS response sent by RWG includes the VLAN Tag Assignment (VTA) in the **Access-Accept** response.

Initially, the access point will use the native VLAN (normally VLAN 1) to send the RADIUS request to RWG. The RADIUS response also uses the native VLAN. After the access point receives the response with the VTA, it starts forwarding the traffic for the end-user device using the VLAN defined in the VTA.



The following diagram shows the entire process:



FIGURE 14 – DYNAMIC VLAN ASSIGNMENT PROCESS FLOW

Step 6 – Switch Port Profiles

Switch Port Profiles are used to assign switch ports to VLANs. When a switch is adopted, RWG creates the **Default** port profile, which contains all ports, without any VLAN association:

Swit	ch Port	Profiles						
	Name	Default	Ports	Media converters	RADIUS	Tagged VLAN(s)	Routed VLANs	Untagged VLAN
	Default		GigabitEthernet1/1/2, GigabitEthernet1/1/3, GigabitEthernet1/1/5, (16)	-	none			-
1 Foun	d							





Step 6a – Create a New Switch Port Profile

Navigate to Network/Wired, and click Create New in the Switch Port Profiles section:

Swite	h Port	Profiles						🔾 Re	efresh 🛃 E	export 👩	Batch 💠 Zoom	n ? Help	🔍 Search	Create	• New
	Name	Default	Ports	Media converters	RADIUS	Tagged VLAN(s)	Routed VLANs	Untagged VLAN	Native I-SID	NNI Port	Shutdown	Account			
	Default	V	GigabitEthernetl/1/2, GigabitEthernetl/1/3, GigabitEthernetl/1/5, (16)	-	none	-	-	-	-			-	Edit	Delete	Show
1 Found	k														

FIGURE 16 – CREATE A NEW SWITCH PORT PROFILE

Enter the following information:

- Name: Enter a name for the port profile.
- **Ports**: Click to see the dropdown with all interfaces, then select interfaces 1/1/6 and 1/1/12. The selected ports with show to the right of the blank field. If you click on the red **×**, you remove the selection.
- Tagged VLANs: Click to see the dropdown and select Onboard VLANs.

			16 switch ports found	
		ICX 7150-B:	GigabitEthernet1/1/1[ethernet 1/1/1]	
		ICX 7150-B:	GigabitEthernet1/1/2[ethernet 1/1/2]	
Croote Switch Bort Brofile		ICX 7150-B:	GigabitEthernet1/1/3[ethernet 1/1/3]	
Create Switch Fort Frome		ICX 7150-B:	GigabitEthernet1/1/4[ethernet 1/1/4]	
Name	Onboard VLANs	ICX 7150-B:	GigabitEthernet1/1/5(ethernet 1/1/5)	
		ICX 7150-B	GigabitEthemet1/1/0[ethemet1/1/0]	
Note		ICX 7150-B	GigabitEthemet1/1/8/ethemet 1/1/8	
		ICX 7150-B:	GigabitEthernet1/1/9/ethernet1/1/9)	
		ICX 7150-B:	GigabitEthernet1/1/10[ethernet 1/1/10]	
	L	ICX 7150-B:	GigabitEthernet1/1/11[ethernet 1/1/11]	
Provisioning (Hide)		ICX 7150-B:	GigabitEthernet1/1/12[ethernet 1/1/12]	
		ICX 7150-B:	GigabitEthernet1/2/1[ethernet 1/2/1]	
Default	assign this profile to an	ICX 7150-B:	GigabitEthernet1/2/2[ethernet 1/2/2]	
Maus parts	assign ports currently a	ICX 7150-B:	10GigabitEthernet1/3/1[ethernet 1/3/1]	profile upon save
Move ports		ICX 7150-B:	10GigabitEthernet1/3/2[ethernet 1/3/2]	
Ports				X ICX 7150-B: GigabitEthernet1/1/6[ethernet 1/1/6]
				ICX 7150-B: GigabitEthernet1/1/12[ethernet 1/1/12]
	ports currently assigned t	to this profil		
Media converters				media converters currently assigned to this profile
Port Configuration (Hide)				
· · · · · · · · · · · · · · · · · · ·				
Untagged VLAN				
Chusteleum				
Shutdown				
Tagged VLAN(s)				💢 Onboard VLANs
Routed VLANs				
	(manual)			
RADIUS	none			
Shortost Path Bridging (80	2 (Hido)			
Shortest Path Bridging (00	z. ray) (mue)			
Native I-SID				
NNI Port	U			
Advanced (Show)				
Auvaliceu (Silow)				
Create Cancel				



Click **Create** to finish. Right after the switch port profile is created, the VLAN configuration is pushed to the ICX switch using SSH.



Step 6b - Verify the ICX Configuration

Start a SSH session to the ICX switch, and use the commands show vlan brief and show running vlan to check the configuration. You should see VLANs 300 to 363 with tagged ports 1/1/6 and 1/1/12.

	SSH@ICX-7150-B#sh ru vlan vlan 1 name DEFAULT-VLAN by port ! vlan 300 by port tagged ethe 1/1/6 ethe 1/1/12 !
SSH@ICX-7150-B#sh vlan brief Gystem-max vlan Params: Max(4095) Default(1024) Current(1024) Default vlan Id :1 Fotal Number of Vlan Configured :66 /LANs Configured :1 300 to 363 999	vian 301 by port tagged ethe 1/1/6 ethe 1/1/12 ! vian 302 by port tagged ethe 1/1/6 ethe 1/1/12 ! vian 303 by port tagged ethe 1/1/6 ethe 1/1/12 ! vian 304 by port tagged ethe 1/1/6 ethe 1/1/12 ! vian 305 by port tagged ethe 1/1/6 ethe 1/1/12 !

FIGURE 18 – CHECK THE ICX CONFIGURATION

Step 7 – Check the RADIUS Realm in SmartZone

A **RADIUS Realm** and **RADIUS Proxy** authentication service are created automatically in the vSZ instance right after the vSZ instance is adopted and synchronized.

In the SmartZone UI, navigate to Services&Profiles/Authentication and select the tab Realm Based Proxy. Select the realm and click Configure to see its details. The RADIUS Realm has three entries using the RADIUS authentication service:

Non-I	Proxy (AP Authenticator)	Proxy (SZ A	Authenticator) Non-Proxy (Social	Login) Realm Based	I Proxy EAP	* Name: 192.168.5.1 RADIUS Pol Description:	ky				
TATION	DSystem		Profile Name 192.168.5.1 RADIUS Policy	Manage By System	Description N/A	Realm Based Authentication Service	8				T
UNIC VIII						Realm	Protocol	Auth Service	Auth Method	Dynamic VLAN ID	
à	Ś					192.168.5.1 RADIUS Policy Map	RADIUS	192.168.5.1 RADIUS Policy	Non-3GPP Call Flow	N/A	
						No Match	RADIUS	192.168.5.1 RADIUS Policy	Non-3GPP Call Flow	N/A	
						Unspecified	RADIUS	192.168.5.1 RADIUS Policy	Non-3GPP Call Flow	N/A	
						Note: If device onboarding was done wit corresponding authentication service to	h credential type 'remote', th properly handle legacy (nor	nen map your 'realm' value to its respectiv n-Hotspot 2.0) devices.	e authentication service PLUS define 'Unspe	cified' realm & map it to	

FIGURE 19 - RADIUS REALM IN SMARTZONE

Later, that RADIUS realm will be used for the WLAN configuration.



Step 7a – Check the RADIUS Authentication Service in SmartZone

In the SmartZone UI, navigate to Services&Profiles/Authentication and select the Proxy (SZ Authenticator). Select the service and click Configure to see its details. The IP address field is the RWG's IP address, and Shared Secret is the same secret that is configured in RWG.

	Non-Pro:	xy (AP Authenticator)	Proxy (SZ A	uthenticator) Non-Pr	oxy (Socia	l Login) Rea	Im Based P	roxy EAP-SIM-AK	A FILS Realm Profile	
			2 <	+ Create	Configure	(가 Clone	🌮 Test AAA	Delete		search table	
		D Sustam		Name 🔺		-0	Manage By		Friendly Name	Protocol	S
	ATION	Disystem		192.168.5	.1 RADIUS P	olicy	System		N/A	RADIUS	RADIUS
	ANIZ			Guest			System		N/A	GUEST	
	ORG			Local Dat	abase		System		N/A	LOCAL_DB	R
											Drimos
L											Primar

* Name: 192	.168.5.1 RADIUS Policy
Friendly Name:	
Description:	
Service Protocol:	RADIUS O Active Directory O LDAP
RADIUS Service Options —	
Encryption:	OFF TLS
RFC 5580 Out of Band L	elivery: OFF Enable for Ruckus AP Only
Primary Server	
• IP Address:	192.168.5.1
* Port:	1812
* Shared Secret:	
* Confirm Secret:	

FIGURE 20 – PROXY AUTHENTICATOR IN SMARTZONE

Note: If SmartZone is remote, then the authentication service needs to be configured as **Non-Proxy (AP Authenticator)**.

SmartZone in a Remote Location

The diagram below shows the SmartZone controller in a remote location. In that situation, authentication must start from the access point, so it needs to be configured in SmartZone as a **Non-Proxy (AP Authenticator).** RWG will configure that automatically when you create a zone with the checkbox **AAA requests originate at the controller** <u>unmarked</u> (the default is marked).







When RWG creates a zone with the checkbox **AAA requests originate at the** controller unmarked, it also creates a **Non-Proxy (AP Authenticator)** entry for that zone:

				General Options		
Non-Proxy (AP Authenticator) Proxy (SZ A	Authenticator) Non-Proxy (Social	Login) Realm Base	d Proxy	• Name: Description: Type: ()	10.0.0.144 RADIUS Policy RADIUS Active Directory LD/	NP Http/2 AAA
	+ Create Configure Clone	🎢 Test AAA 🛛 Delete		Backup RADIUS:	COFF Enable Secondary Server	
- D System	Name 🔺	Туре	Descri	Drimany Sonior		
Z Lua	10.0.0.144 RADIUS Policy	RADIUS	N/A	Fillinary Server		
C Moon				* IP Address: 1	0.0.0.144	
5				* Port: 1	812	
				* Shared Secret: ••		
				Confirm Secret:		

FIGURE 22 – SMARTZONE CONFIGURED AS NON-PROXY AP AUTHENTICATOR

In that topology, the IP address configured for the authenticator is the RWG's WAN interface address. SmartZone will configure that address in the access points for that zone, which will then start the authentication requests to RWG.

Step 7b – Check the RADIUS Server Options in RWG

In the RWG UI, navigate to **Services/RADIUS** and scroll down to the **RADIUS Server Options** section. This entry is created automatically when RWG is installed, and it is applied to the SmartZone instance and the ICX switch when they are in sync.

RAD	IUS Serv	er Optio	ons						<table-cell> Refr</table-cell>	esh 🔀 Export	Batch	‡ Zoom	? Help 🔍 Search
	Active 🖓	Name	Secret	802.1X(EAP)	EAP Certificate	MS- CHAP	RadSec(TLS)	RadSec Certificate	Minimum TLS Version	Maximum TLS Version	Debug Level	WAN Targets	Policies
		Default	wR- g76v3KSbeuGYlxndOSw		£.	2		5	TLS 1.2	TLS 1.2	Normal	54 ⁰	vSZ- 6100395
1 Foun	ıd		g76v3KSbeuGyIxnaOSw										6100395

FIGURE 23 - RADIUS SERVER OPTIONS



Step 8 - RADIUS Realms in RWG

A RADIUS realm in RWG defines how the authentication request will be processed, and which policy will be used to define the attributes in the RADIUS response message.

We will use a RADIUS realm that does the following: when there is a match with the WLAN information that is included in the request, the NAC service in RWG will run an algorithm to select a VLAN ID for the configured range, and the RADIUS realm will insert the VLAN ID in the response message. Navigate to Service/RADIUS, then click **Create New** under the **RADIUS Server Realms** section:

RAD	IUS Serv	er Rea	lms						Refresh	Export	Batch	🛟 Zoom ? Help	Search	Create New
	Name 🛆	Rank	Policies	CALEA Options	Attribute Patterns	Sharing	VLANs	Infrastructure Devices	RADIUS Servers	LDAP Domains	PMS Serve	Create ers Account	Usage Plans	Always deny
							N	o Entries						
0 Four	nd													

FIGURE 24 - CREATE A NEW RADIUS SERVER REALM

Enter the following information:

- Name: Enter a name for the realm.
- Realm admission logic: Select Policy OR Attribute Pattern logic must succeed. This defines the criteria to select the realm.
- **Policies**: Check the **Default** policy only.
- Priority: Select 0.
- Logic: Select OR.
- Attribute: Select Called-Station-Id (BSSID/SSID).
- **Pattern**: Enter the SSID for the WAN that needs to be matched, or a substring of the SSID. Here, we entered **micro**. We will create that WLAN later.
- Sharing: Select per-Device.
- VLANs: Check Onboard VLANs.
- Infrastructure Devices: Make sure to check the vSZ instance you are using.

Create RADIUS Server	Realm		
Name	Microsegmentation Realm]	
Note			
Request Matching (Hid	le)		
Rank	0 🗸 prioritize higher rank over group and attribute pattern prece	dence when matc	hing
Realm admission logic	Policy OR Attribute Pattern logic must succeed 🗸 logic to	use when determi	ining whether a request matches this realm
Policies	Select All None Reset	95	
	Account, MAC, and IP groups that may match this realm		
CALEA Options	no options Use this realm for Accounting for the specified CAL		
Attribute Patterns (Hi attributes to authenticate wi Priority Logic Attribute	de) een matched Pattern	WLAN	Note
0 V OR V Called-Sta	tion-Id (BSSID/SSID) V micro	- select - 🗸	1
Create Another RAE	IUS Attribute Pattern		
Dynamic VLANs (Hide)			
Sharing	per-Device how VLANs are shared between end-users		
VLANS	Calcot All Hanne Reset		
	dynamic VLANs available for assignment		
Reuse	reuse VLAN tag assignments when necessary		
Inherit static	new VLAN tag assignments inherit the static attribute of an exist		
Timeout	60	minutes ~	amount of time a VLAN tag assignment is kep
Expire at logout	immediately flush a VLAN tag assignment at logout		
VLANs/Called-Station		unlimited 🗹	maximum number of *unique* VLAN IDs assign
Infrastructure Devices	Select All None Decet		

FIGURE 25 - CREATE RADIUS SERVER REALM



Scroll down, and enter the following information:

 Inserted Attributes: Mark the checkboxes Tunnel-Type:VLAN, Tunnel-Medium-Type-IEEE-802 and Tunnel-Private-Group-Id:%vlan_tag_assignment.tag%

Click **Create** to finish.

Proxy Options (Hide)
Proxy packets	Accounting Authentication packet types to proxy
Proxy MAC auth	proxy MAC auth requests (authentication and accounting)
Replace username	replace User-Name attribute with account login before proxying
Create Account	Create accounts for new proxied authentications
Usage Plans	no options plan and group applied to new accounts created during provied requests
Behavior (Hide)	
Inserted Attributes	Select All None Reset
	Cisco-AVpairpsk=%account.pre_shared.key% Ruckus-DP5%%account.pre_shared.key%
	RADIUS attributes to include in an Access-Accept or proxied Access-Request or Accounting-Request depending on Attribute's insertion
Always deny	deny all requests to this realm
Accounting (Show)	
Contractor and the second s	

FIGURE 26 - CREATE RADIUS SERVER REALM (CONT'D)



Step 9 - WLAN Configuration

We will configure the WLAN using the RWG UI. The WLAN for microsegmentation uses **802.1x** and **MAC bypass**. Navigate to **Network/Wireless**, then click **Create New** under the **WLANs** section:

WI	LAN	s						Import WLANs	🖏 Refresh 🔀 Expo	rt 🛷 Batch 💠 Zoom	? Help 🔍 Search	Create New
5		Name	\bigtriangleup	Controller	AP Profiles	Access point zone	SSID	Encryption	Authentication	Default VLAN	Tunnel	VLANs
							No En	tries				
0 F	ound											

FIGURE 27 - CREATE A NEW WLAN

Enter the following information:

- Name: Enter a name for the WLAN.
- Access point zone: Select the zone where the WLAN will be created.
- **Controller**: Select the controller where the WLAN will be created.
- AP Profiles: Select the default [Solar System] profile.
- SSID: Enter the SSID. Here, we used microseg. This will match with the substring we used in the RADIUS realm.
- Authentication: Select MAC Authentication Bypass.
- Enabled: Check 2.4GHz and 5 GHz.
- RADIUS Server Realm: Select Local RADIUS server.
- VLANs: Select Onboard VLANs.

Create WLAN	
Name	Microsegmentation WLAN
Access point zone	Solar System V
Note	
Provisioning (Hide)	
Controller	√SZ-6100395 ✓
AP Profiles	Select All None Reset
Policies	
WLAN Configuration (Hid	e)
SSID	microseg
Encryption	none ~
Authentication	MAC Authentication Bypass ~
Pre-shared Key	
Default VLAN	1
Tunnel	tunnel WLAN traffic to the controller instead of locally bridging (tun
Enabled	24GHz SGHz enable this WLAN on the 2.4GHz and/or 5GHz r
RADIUS Realm Server	Local RADIUS server configure RADIUS server to be used for a
Dynamic VLANs (Hide)	
VLANS	Select All I None Reset
	VLANs to be assigned when RADIUS access requests include this WLA
RADIUS Accounting	receive RADIUS Accounting packets from the AP
Create Cancel	

FIGURE 28 - CREATE WLAN

Click **Create** to finish. The WLAN will be created automatically in the SmartZone controller.



Step 9a – Check the WLAN in SmartZone

In the SmartZone UI, navigate to **Wireless LANs**, select the zone, click on the WLAN named **Microsegmentation WLAN**, then click **Configure** to see the WLAN details. The relevant WLAN parameters are highlighted.

Wireless LANs	5				VIEW MODE:	List	Group	
+ 🖌 🗋 🗙 More 🗸	ଥ ଏ	🕂 Create Configure 🖓 Clone	Delete	More 🗸				
- D System		Name 🔺	Alerts	SSID	Auth Method	Encrypti	on Method	Clients
+ Z Solar System		Microsegmentation WLAN	0	microseg	MAC	NONE		3
General Options								V
* Name:	Microsegm	entation WLAN						
* SSID:	microseg							
Description:								
• WLAN Group:	default 5G	Hz, default, default 2.4GHz	· +					
Authentication Options								v.
Authentication Type:	Standare network	d usage (lor most regular wireless 🔹 🔘 Hotspo	t (WISPr)	O Guest Access	O Web Authentication			
	Hotspot	2.0 Access OHotspo	t 2.0 Onboardi	ng 🔵 WeChat				
Method:	Open (802.1X EAP MAC Address 802.1X EAP	& MAC					
MAC Authentication:	Off Us	se user-defined text as authentication password	l (default is de	vice MAC address):				
MAC Address Format:	aabbccdde	teff v						
Encryption Options								v.
Method:	WPA2	WPA3 WPA2/WPA3-Mixed OWE V	(PA-Mixed)	WEP-64 (40 bits) 🔘 WEP-12	18 (104 bits 🛞 None			
	Encryption	methods other than WPA3 and OWE wi	I not be supp	ported on Wi-Fi 6E device	35.			
Data Plane Options								Þ
Authentication & Accountin	ng Service							v
* [?] Authentication Servi	ce: ON (Use the controller as proxy						
	192.16	8.5.1 RADIUS Policy \vee 🕇 🖋						

FIGURE 29 – CHECK THE WLAN IN SMARTZONE

The configuration for microsegmentation is completed.



Testing Microsegmentation

Connect to WLAN **microseg** using two different devices. Check the IP addresses received by the devices. They should be in different /30 subnets.

Ni-Fi mic	roseg	< Wi-Fi 🛛 🗖	nicroseg
networks you select. Wh turned on, automatic upo tasks, such as Photos sy	en Low Data Mode is dates and background ncing, are paused.	you select. When Low E automatic updates and Photos syncing, are pair	Data Mode is turned on, background tasks, such as used.
Private Wi-Fi Addre	ss	Private Wi-Fi Addr	ess
Wi-Fi Address	7E:80:ED:35:FC:D9	Wi-Fi Address	F6:CA:DE:42:82:E
Using a private address I your iPhone across differ	nelps reduce tracking of rent Wi-Fi networks.	Using a private address iPhone across different	helps reduce tracking of your Wi-Fi networks.
		Limit IP Address Tr	acking
Limit IP Address Tra	cking	Limit IP address trackin from known trackers in	g by hiding your IP address Mail and Safari.
Limit IP address tracking from known trackers in N	by hiding your IP address fail and Safari.	IPV4 ADDRESS	
IPV4 ADDRESS		Configure IP	Automatic
Configure IP	Automatic >	IP Address	20.0.0.1
IP Address	20.0.0.6	Subnet Mask	255.255.255.25
Subnet Mask	255.255.255.252	Router	20.0.0.1
Router	20.0.0.5	DNS	
		Configure DNS	Automatic
DNS			
Configure DNS	Automatic >	HTTP PROXY	
		Configure Proxy	Off

Network Address	Usable Host Range	Broadcast Address
20.0.0.0	20.0.0.1 - 20.0.0.2	20.0.0.3
20.0.0.4	20.0.0.5 - 20.0.0.6	20.0.0.7
20.0.0.8	20.0.0.9 - 20.0.0.10	20.0.0.11
20.0.12	20.0.0.13 - 20.0.0.14	20.0.0.15

FIGURE 30 – TWO DEVICES CONNECTED TO THE SAME WLAN IN DIFFERENT SUBNETS

In our tests, we used two iPhones and got the addresses 20.0.0.6/30 and 20.0.0.14/30. Remember that a /30 subnet has four IP addresses only, 20.0.0.6/30 belongs to subnet 20.0.0.4, and 20.0.0.14/30 belongs to subnet 20.0.0.12.

In the RWG UI, navigate to **Instruments/MAC·DHCP·DNS** and go the section **DHCP Leases** to see the IP and MAC address, plus the VLAN ID used by each client:

DHC	P Leases										
	Issued \bigtriangledown	IP	MAC	Vendor	Hostname	Expires	Network	Pool	Fixed Host	Ethernet	VLAN
	01/08/2023 08:02:37 PM	Q 20.0.0.6	Q 7e:80:ed:35:fc:d9			01/09/2023 12:02:37 AM	vlan301	Onboard Addresses	Create New		Onboard VLANs
	01/08/2023 08:02:05 PM	Q 20.0.0.14	Q f6:ca:de:42:82:ee	-	-	01/09/2023 12:02:05 AM	vlan303	Onboard Addresses	Create New	-	Onboard VLANs

FIGURE 31 – CHECKING THE DHCP LEASES

The IP addresses come from the Onboard Addresses pool, and the VLAN IDs from the Onboard VLANs range.



RWG Policies Overview

Before continuing with the tests, some background on RWG policies is necessary. RWG policies use three types of records:

- Groups
- Policies
- Enforcements

Group records (account groups, MAC groups, IP address groups) identify and classify end-users and devices into roles.

Policy records associate the group records to the enforcement records and define who receives what treatment.

Enforcement records (splash portals, application forwards, bandwidth queues, packet filters) define and configure behaviors that are to be applied to some or all end-users and devices managed by RWG.

For example, a wireless client might initially start using a free account to login, so he will be identified as member of the **Free** account group. After some time, he decides to buy access to a premium service, so he automatically moves to the **Premium** access group, which uses a policy that give higher speed and more bandwidth allocation.



FIGURE 32 – EXAMPLES OF POLICIES



Click on **Policies** at the top menu to see the current policies configured at RWG. An IP group and policy is created automatically for every device that is adopted by RWG. The **DEFAULT** and **Webserver DDoS Abusers** groups and policies are created automatically when RWG is installed.



FIGURE 33 – THE RWG POLICIES PANEL

Using the Search Tool

The **Search** tool is not a help or documentation tool. It is used to locate client or infrastructure devices known by RWG. You can search by MAC address, IP address, client's last name or room number.

Enter the IP address of one of the wireless clients connected to microseg WLAN in the textbox at the top right corner, and click **Search**:

help build 14.065	logout marcelo	20.0.0.6	Search
Billing	Archives	Instruments	
	🔕 Flush All 🎇 Re	fresh 🛃 Export 💠 Zoom 🔍 Se	earch
IPv6			
	Connectio	ns Web Graph Show Flu	
	CONNECTIO	his web oldpit show the	sh

FIGURE 34 – THE SEARCH TOOL



You will see the policy panel with the policy membership details for the selected client. In our example, client 20.0.0.6 is using the **Default** policy (it is marked as **active**). Several enforcement rules are applied by default to the Default policy. Among them there is the **Block Subnets** enforcement rule, which prevents any traffic between any local subnets.





Ping Test

While both clients are connected to WLAN **microseg**, ping from one device to another. We used a ping app installed in one of the devices. At the time of this test, the client IP addresses were 20.0.0.10/30 and 20.0.0.22/30. The ping tests should fail. That's expected, because the clients are using the **Default** policy, which uses the **Block Subnets** rule that block traffic between different subnets.



FIGURE 36 – THE PINGS FAIL



Disable the Block Subnets Rule

Block Subnets is a packet filters rule that is enabled by default. To disable it, click **Policies** in the top menu, scroll down and click **Edit** in the **Default** policy.



FIGURE 37 – EDIT A POLICY

Scroll down and unselect Block Subnets at Subnets Filter.

Application Filters	Select All None Reset Webserver DDoS Abusers Block All	Network Ser	rvices Identities	Policies Billin	ng Archives Inst
Application Forwards	no options	vSZ-6100395	vSZ-610	0395	
Subnets Filter	- select - V	IP GROUP			
Radius servers	Select All None Reset	ICX 7150-B	ICX 715	ю-в	
WLAN to use for connection instructions/QR code displayed in portal	- select -	Webserver DDoS Abusers	Webserver DD	oS Abusers	Webserver DDoS Abusers Block All
Groups (Hide)					Webserver DDoS Prevention
MAC Groups	no options				LOG HITS TRIGGER
IP Groups	no options				0.*
Account Groups	no options	DEFAULT GROUP	Defau		Cache
Shared Credential Groups	Select All None Reset				100%
RADIUS Groups	no options				per Device BANDWIDTH QUEUE
LDAP Groups	no options	22			
Update Cancel					

FIGURE 38 – THE BLOCK SUBNETS RULE IS DISABLED.

Click **Update** to finish. Check the policies again. The **Block Subnets** enforcement rule no longer appears in the **Default** policy.



Disconnect and reconnect the wireless clients to WLAN microseg. Ping again from one device to another.



FIGURE 39 - THE PINGS ARE WORKING

The pings should work now.

Troubleshooting

The Wireless Client Does Not Associate to the 802.1x SSID

Case 1

If the wireless client cannot associate to the 802.1X SSID, it means authentication is failing. The access point is unable to communicate with the RADIUS server, or the authentication response is **Access-Reject**. You can check the RADIUS request and response in the RWG logs. If required, you can increase the debug level in the section **RADIUS Server Options** at **Services/RADIUS**.

To see the RADIUS server logs, navigate to **Archives/.log Files** and click **RADIUS Server**.





The example above shows an **Access-Reject** which was cause by a misconfigured SSID in the WLAN pattern field at the RADIUS realm created in RWG.



Case 2

If the RADIUS log does not show any requests arriving, check whether the **Default** and the SmartZone policy still exist (it is **vSZ-6100395** in our example). They must not be deleted. Also, check the associations at **RADIUS Server Options** and at the RADIUS realm:

				Opdate Microsegmentation	ream
Network Services Identities Pol	icles Billing	Archives		Name	Microsegmentation Realm
vSZ-6100395 9 rr eneur				Note	
KCX 7150-B 9 (CX 7150-B				Request Matching (Hide) Rank	or prioritize higher rank over group and attribute pattern precedence when matching
Webserver DDoS Abusers	Webs	erver DDoS Abusers Block All APPLICATION FILTER		Realm admission logic Policies	Policy OR Attribute Pattern logic must succeed v logic to use when determine
	~ W	LOG HITS TRIGGER		Chi FA Cestines	COnfount ICX 750-B VLAN 600 VLAN 700 Webserver CD03 Abuses V52-249 Account, MAC, and IP groups that may match this realm NO Options Use this realm for Accounting for the specified CALEA Options
DIFFAULT		Block Subnets		Attribute Patterns (Show) attributes to authenticate when m	artched
DerAult Berwalt GROUP		SUBNET PILTER		Dynamic VLANs (Hide)	
		Cache		Sharing	per-Device v how VLANs are shared between end-users
		WEB CACHE		VLANS	Select All None Reast
		per Device			dynamic VLANs available for assignment
		BANDWIDTH QUEUE		Reuse	reuse vLAN tag assignments when necessary
RADIUS Server Options	🗟 Columns 🖏 Refresh 🕻	Export 🕐 Batch 💠 Zoom	? Help 🔍 Search 🔘 Create New	Timest	60 minutes v and
Active V Name Secret 802.DX(EAP) E	AP Certificate MS- CHAP	Minimum Maximum TLS TLS Version Version	Debug WAN Policies Level Targets	Expire at logout	immediately flush a VLAN tag assignment at logout
Defsuit wR- I n g76/3KSbeuCYlandOSw h	ng- 🗹	TLS12 TLS12	Normal - v52-6100395	Infrastructure Devices	Scient All Noor Reset

FIGURE 41 – CHECKING THE POLICY ASSOCIATIONS

The Wireless Client Does Receive an IP Adddress

If the wireless client cannot associate, but you see the authentication response with the VLAN assignment in the RADIUS log, that means the client device is not receiving an IP address from the DHCP pool configured in RWG. Here is a RADIUS **Access-Accept** response with a vlan assignment:



FIGURE 42 – CLIENT IS RECEIVING AND ACCESS-ACCEPT RESPONSE

Check the following:

- Are the VLANs with tagged interfaces are configured in the ICX switch? The VLANs configured in the ICX must match the VTAs included in the RADIUS responses.
- Are the correct DHCP scopes configured and created by RWG in FreeBSD?
- If RWG is running on a ESXi VM, did you configure VLAN ID 4095 for the LAN port group in the VM? That's an ESXi requirement to enable trunk mode in VM interfaces. The traffic for tagged VLANs will not pass without that setting.
- Are the wireless devices receiving a duplicate IP address? If yes, you will see **DHCPDECLINE** messages in the **DHCP Server** log at **Archives/.log Files**.



There is No Internet Connectivity

The wireless client associates to the SSID and receives an IP address from the expected DHCP pool, but there is no Internet connection. That status is easy to see in an iPhone:

6:45	
Settings Wi-Fi	Edit
Wi-Fi	
microseg No Internet Connection	۰ 🔒
MY NETWORKS	
Sheldon	≜ হ 🚺
Simone	€ 奈 🚺
OTHER NETWORKS	
AAAAA	ê 🗢 🚺
ally&latte	≜ ≑ 🚺
Atlas	? (j)
ATT6dX99vS	≜ ≑ 🚺
ATT6dX99vS_2	€ 🗢 🚺
ATTpCaZWul	€ 🗢 🚺
ATTPGYnEUs	۵ 🗢 🚺
BearsBeetsBSG	€ 奈 🚺
Dance House	ê 후 🚺

FIGURE 43 – NO INTERNET CONNECTIVITY

Test the connectivity to the Internet directly from one of the addresses in the pool. You can use the default gateway configured in the iPhone as a source address for a ping to any Internet destination from a SSH session in RWG. The ping test failed in our example below:

	•11 🗢 🕞	
Wi-Fi microse	eg	
you select. When Low Data Mo automatic updates and backgrn Photos syncing, are paused.	de is turned on, ound tasks, such as	
Private Wi-Fi Address		
Wi-Fi Address	56:1E:F3:34:77:86	
Using a private address helps r iPhone across different Wi-Fi n	reduce tracking of your etworks.	
Limit IP Address Tracking	g 💽	[marcelo@rwg-home ~]\$ pipg -\$ 20 0 0 1 8 8 8 8
Limit IP address tracking by hid from known trackers in Mail an	ding your IP address d Safari.	PING 8.8.8.8 (8.8.8.8) from 20.0.0.1: 56 data bytes
IPV4 ADDRESS		<u>^c</u>
Configure IP	Automatic >	8.8.8.8 ping statistics
IP Address	20.0.0.2	8 packets transmitted, 0 packets received, 100.0% packet lo
Subnet Mask	255.255.255.252	
Router	20.0.0.1	
DNS		
Configure DNS	Automatic >	
HTTP PROXY		

FIGURE 44 - NO INTERNET CONNECTIVITY

In our case, the NAT entry for the **Onboard Addresses** was not enabled. Internet access was established immediately after that NAT entry was configured correctly.



Conclusion

This document covered the configuration for basic L2 and L3 microsegmentation using regular VLANs. Each client was assigned its own VLAN and /30 IP subnet, and they cannot communicate with each other by default.

Other scenarios have different requirements. For example, for MDU/MTU or HSP use cases we could use account groups, portals or DPSKs, and VLANs shared by each account to give to tenants or guests access to the same VLAN, using IP addresses in the same subnet. That way, tenants in the same unit, or guests in the same hotel room can communicate with each other, but not with clients in other units or hotel rooms.

RUCKUS solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit commscope.com to learn more about:

- RUCKUS Wi-Fi Access Points
- RUCKUS ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

www.ruckusnetworks.com

Visit our website or contact your local RUCKUS representative for more information.

© 2023 CommScope, Inc. All rights reserved.

All trademarks identified by $^{\rm TM}$ or $^{\otimes}$ are trademarks or registered trademarks in the US and may be registered in other countries. All product names, trademarks and registered trademarks are property of their respective owners.

