Deployment Guide

RWG - Microsegmentation Step-by-Step Configuration

June 2023

Rev. 1

Table of Contents

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 https://{your RWG_IP_address}/admin/manual/help_online

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.

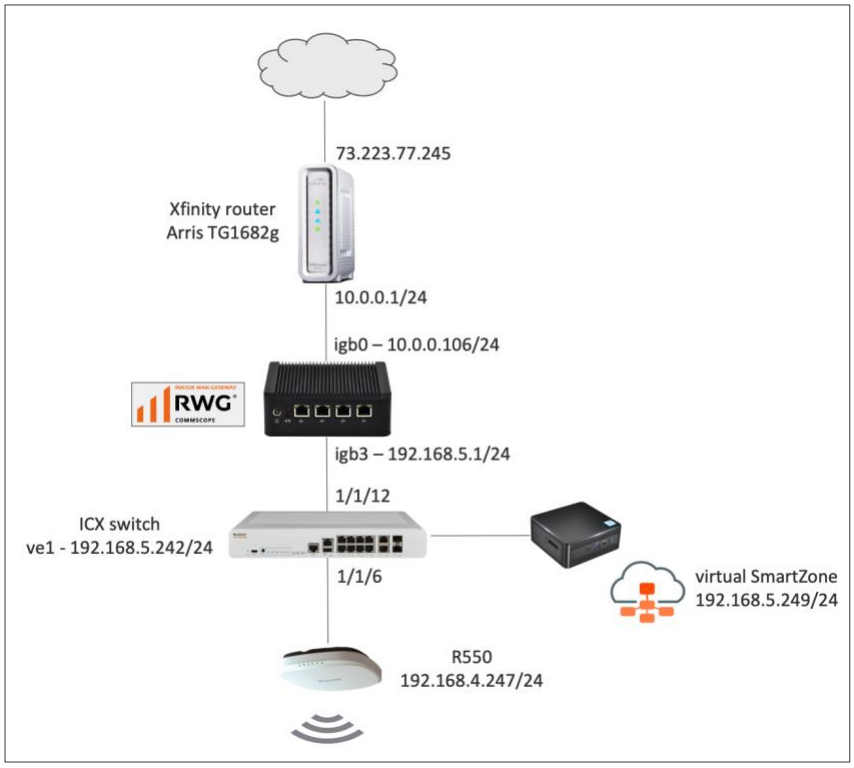


FIGURE 1 – TEST TOPOLOGY

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.

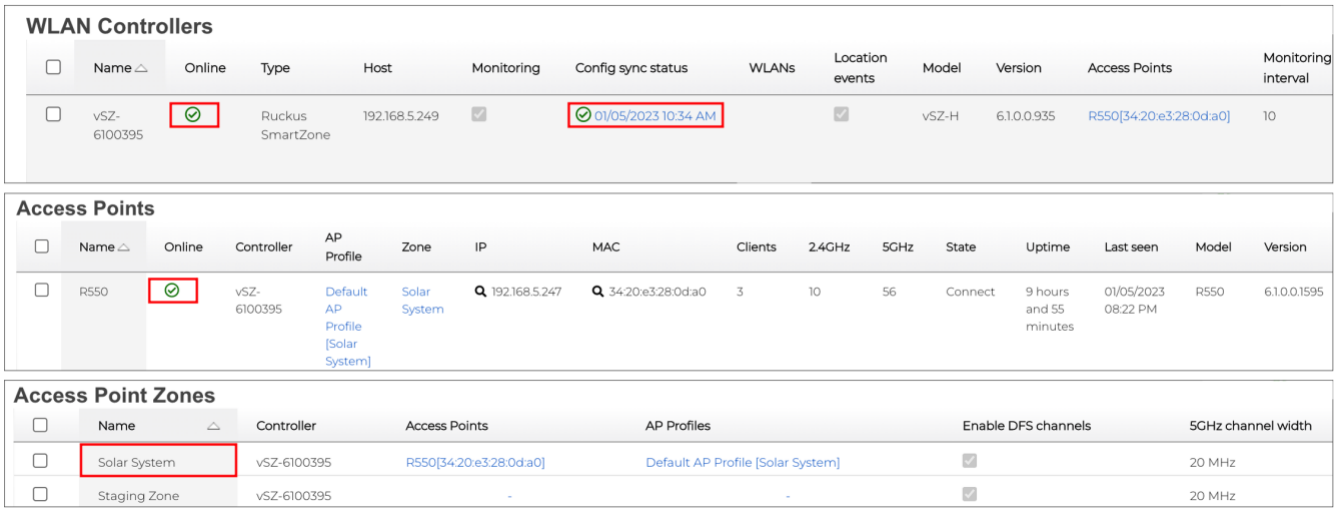


FIGURE 2 – SMARTZONE IS ONLINE AND IN SYNC

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.

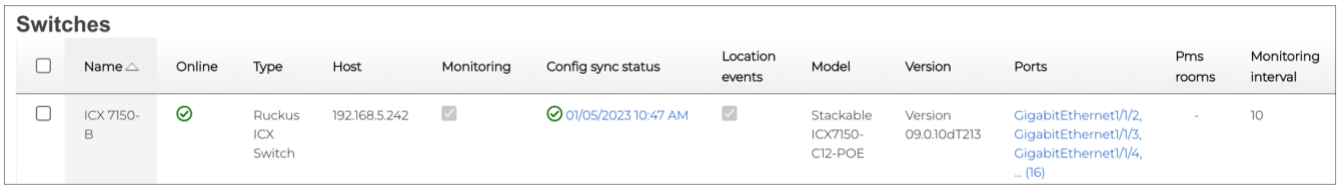


FIGURE 3 – ICX IS ONLINE AND IN SYNC

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:

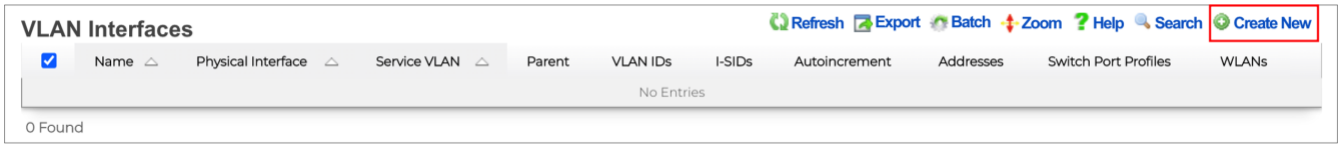


FIGURE 4 – CREATE NEW VLAN INTERFACE

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.

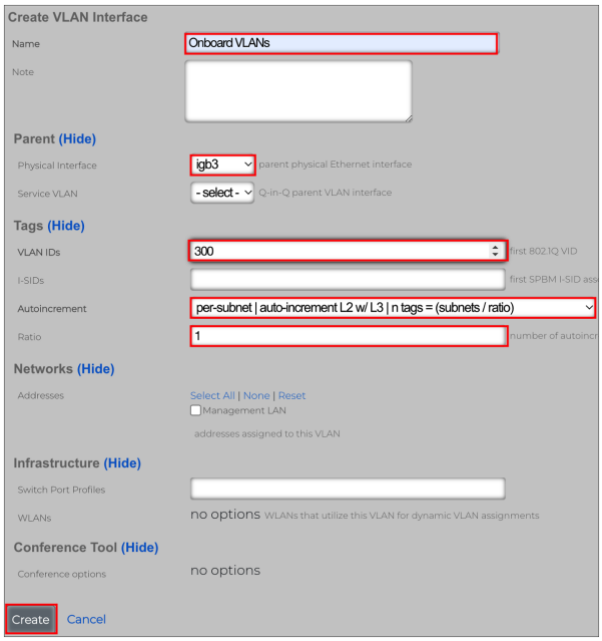


FIGURE 5 – CREATE VLAN INTERFACE

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:

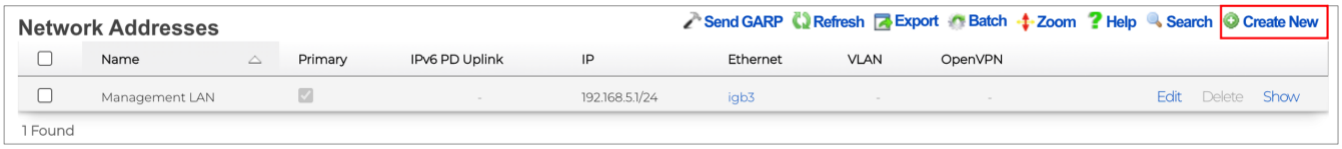


FIGURE 6 – CREATE NEW NETWORK ADDRESS

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.

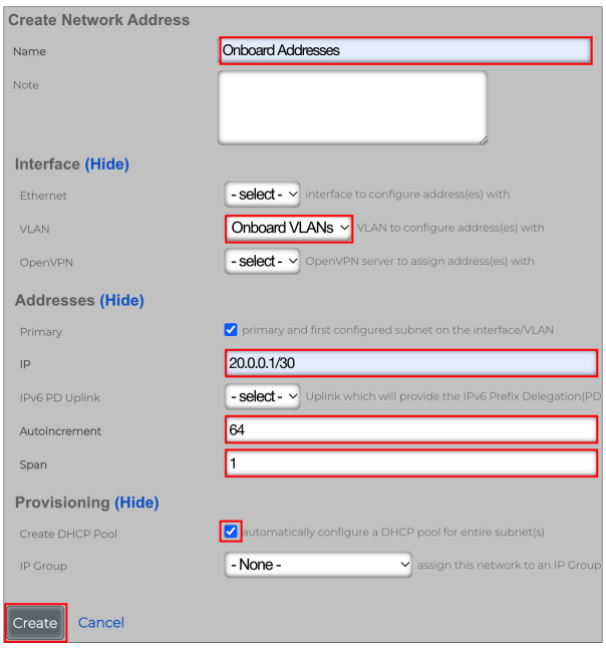


FIGURE 7 – CREATE NETWORK ADDRESS

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.

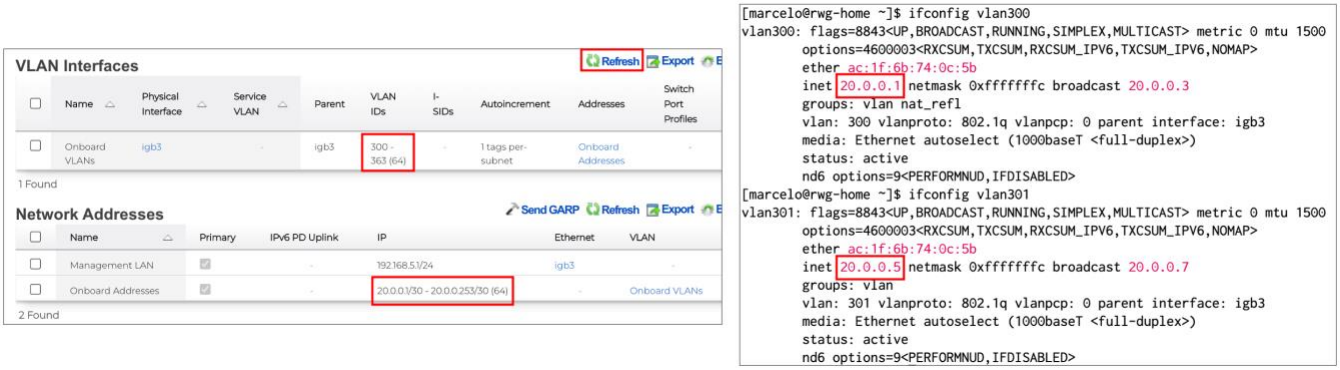


FIGURE 8 – ASSOCIATION BETWEEN VLAN INTERFACES AND NETWORK ADDRESSES

Step 4c – Check DHCP Pools in RWG

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

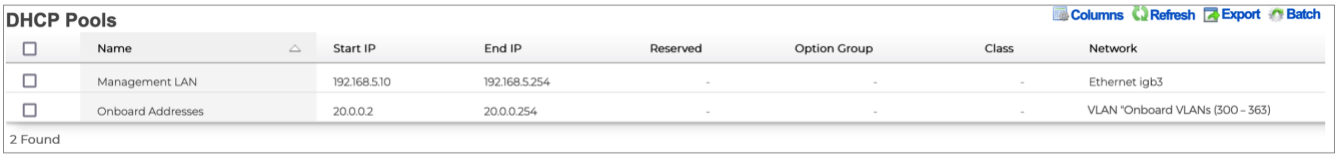


FIGURE 9 – DHCP POOLS

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)

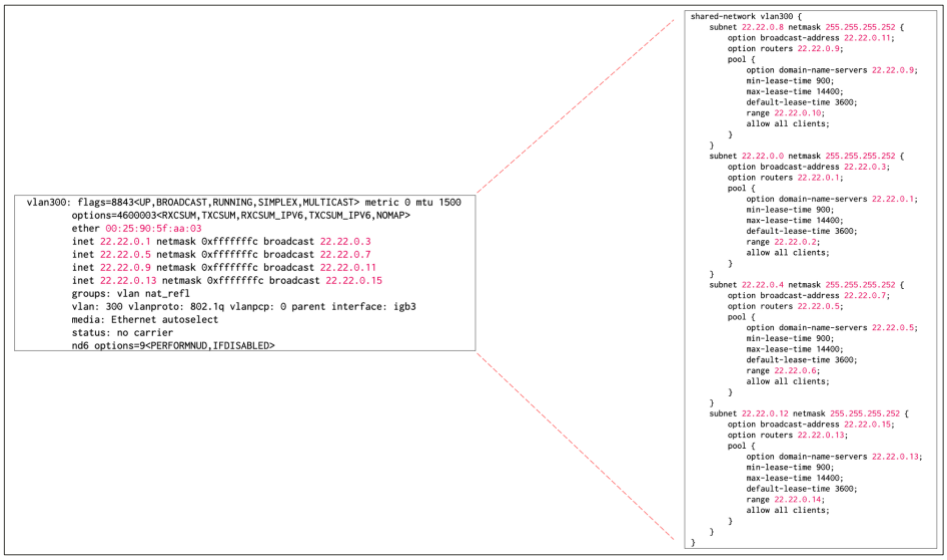


FIGURE 10 – DHCP CONFIGURATION FILE

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":**

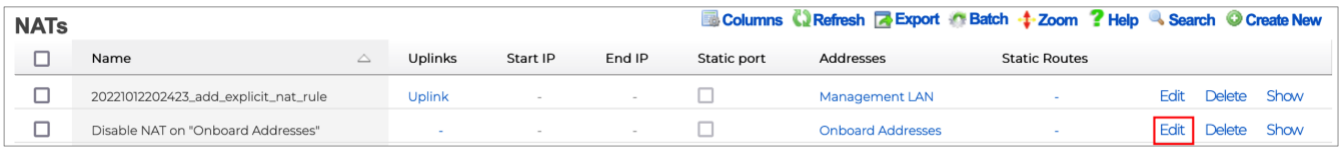


FIGURE 11 – EDIT A NAT ENTRY

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.

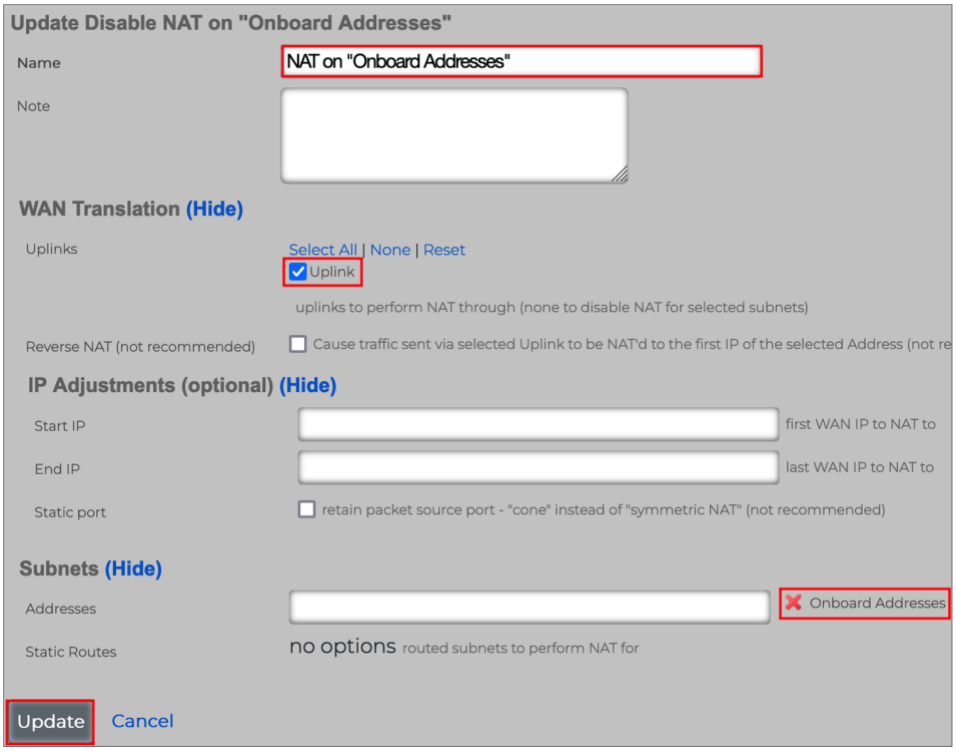


FIGURE 12 – UPDATING THE NAT ENTRY

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.

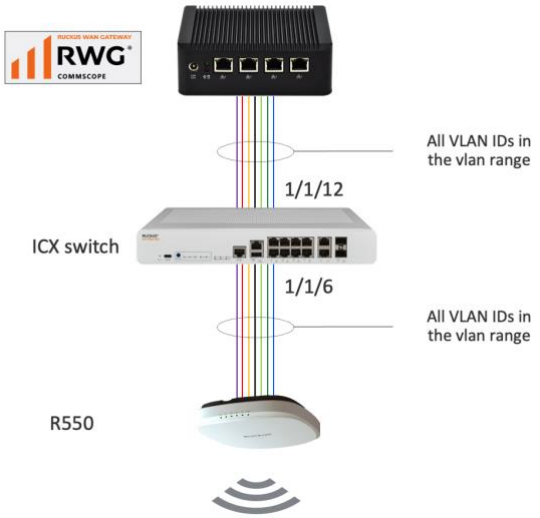


FIGURE 13 – VLANS WITH TAGGED INTERFACES IN THE ICX SWITCH

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:

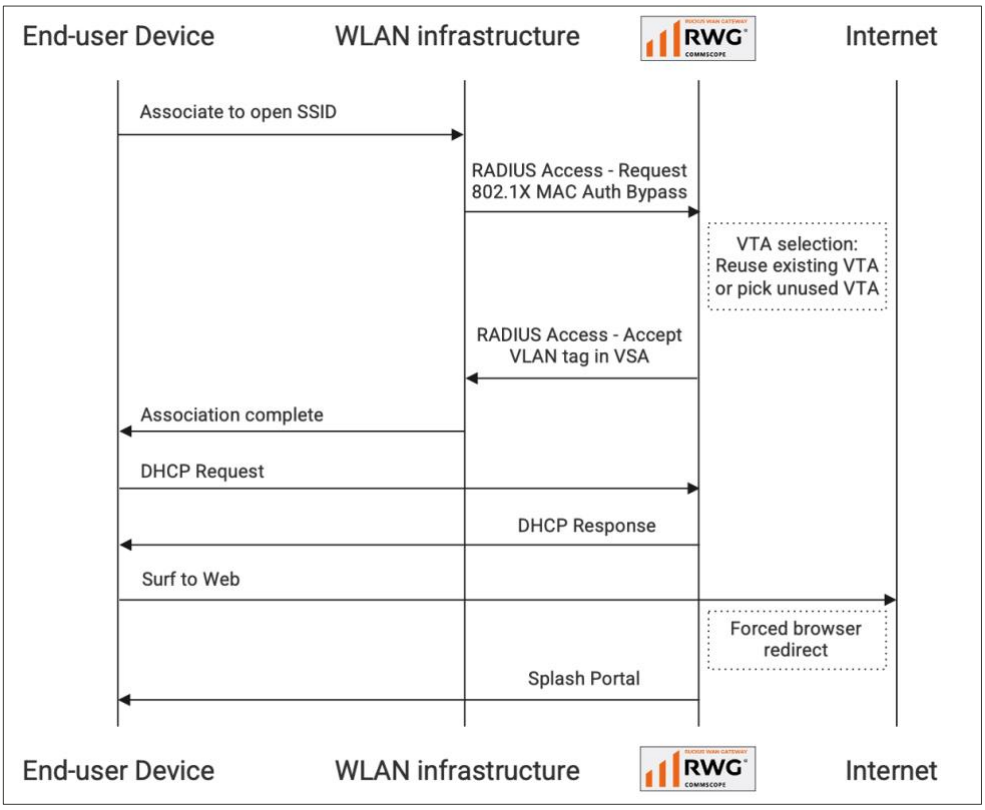


FIGURE 14 – DYNAMIC VLAN ASSIGNMENT PROCESS FLOW

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:

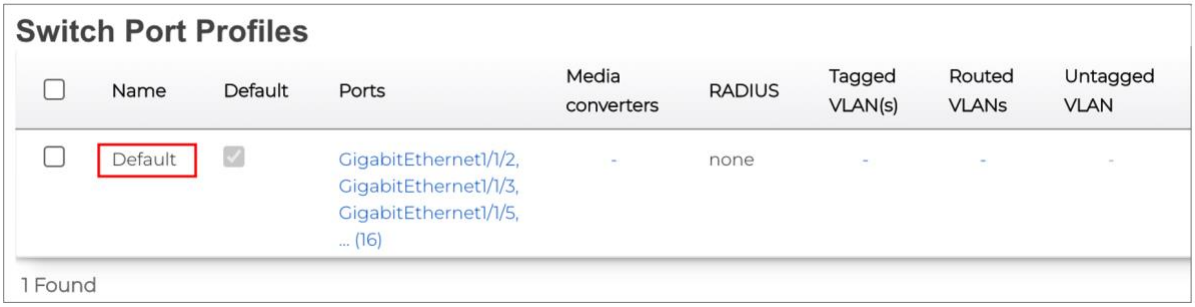


FIGURE 15 – THE DEFAULT SWITCH PORT PROFILE

Step 6a – Create a New Switch Port Profile

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

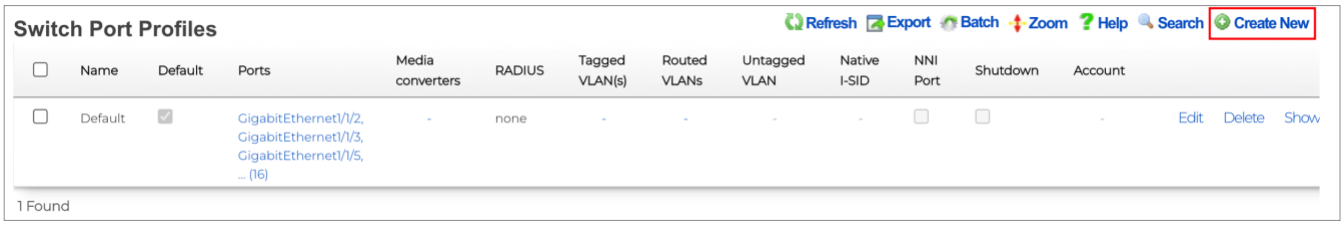


FIGURE 16 – CREATE A NEW SWITCH PORT PROFILE

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**.

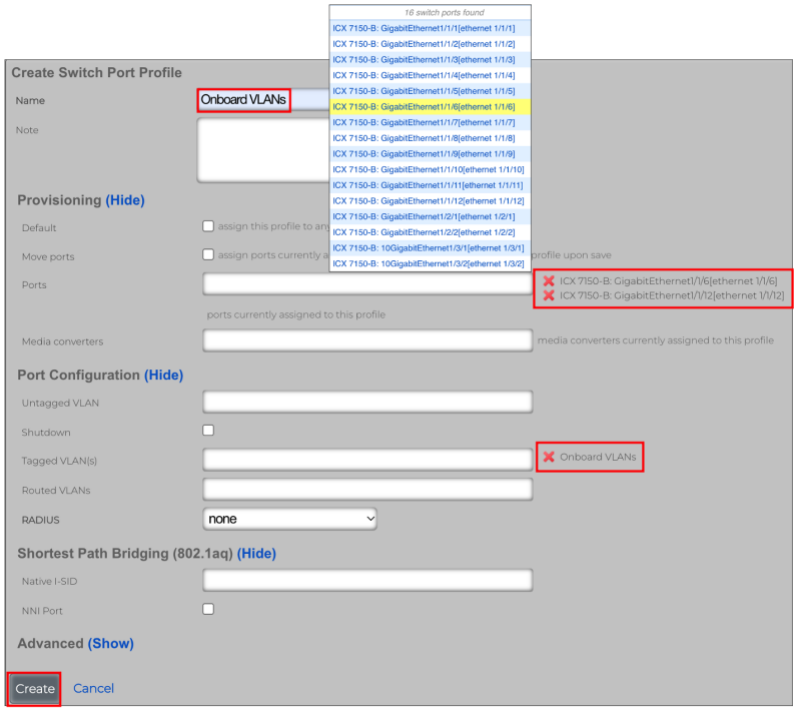


FIGURE 17 – CREATE SWITCH PORT PROFILE

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 vlan brief

System-max vlan Params: Max(4095) Default(1024) Current(1024)
Default vlan Id :1
Total Number of Vlan Configured :66
VLANs Configured :1 300 to 363 999
```

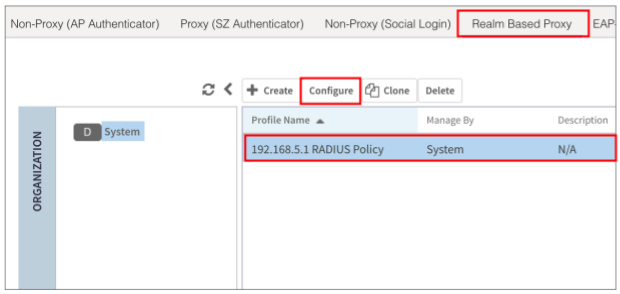
```
SSH@ICX-7150-B#sh ru vlan
vlan 1 name DEFAULT-VLAN by port
!
vlan 300 by port
 tagged ethe 1/1/6 ethe 1/1/12
!
vlan 301 by port
 tagged ethe 1/1/6 ethe 1/1/12
!
vlan 302 by port
 tagged ethe 1/1/6 ethe 1/1/12
!
vlan 303 by port
 tagged ethe 1/1/6 ethe 1/1/12
!
vlan 304 by port
 tagged ethe 1/1/6 ethe 1/1/12
!
vlan 305 by port
 tagged ethe 1/1/6 ethe 1/1/12
!
etc...
```

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:



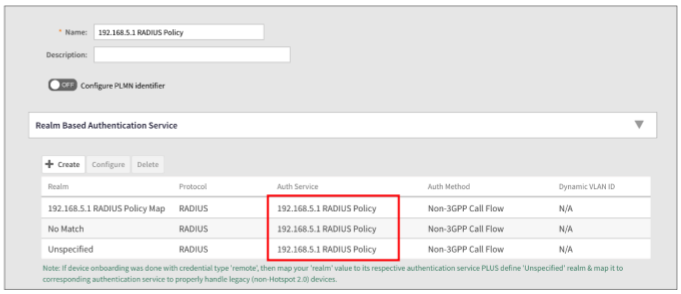


FIGURE 19 – RADIUS REALM IN SMARTZONE

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.

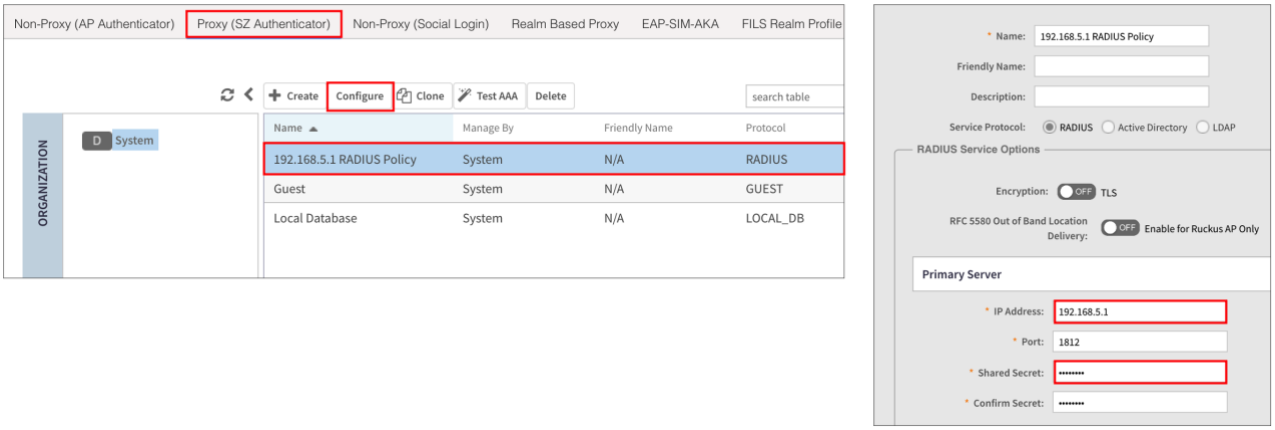


FIGURE 20 – PROXY AUTHENTICATOR IN SMARTZONE

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** unmarked (the default is marked).

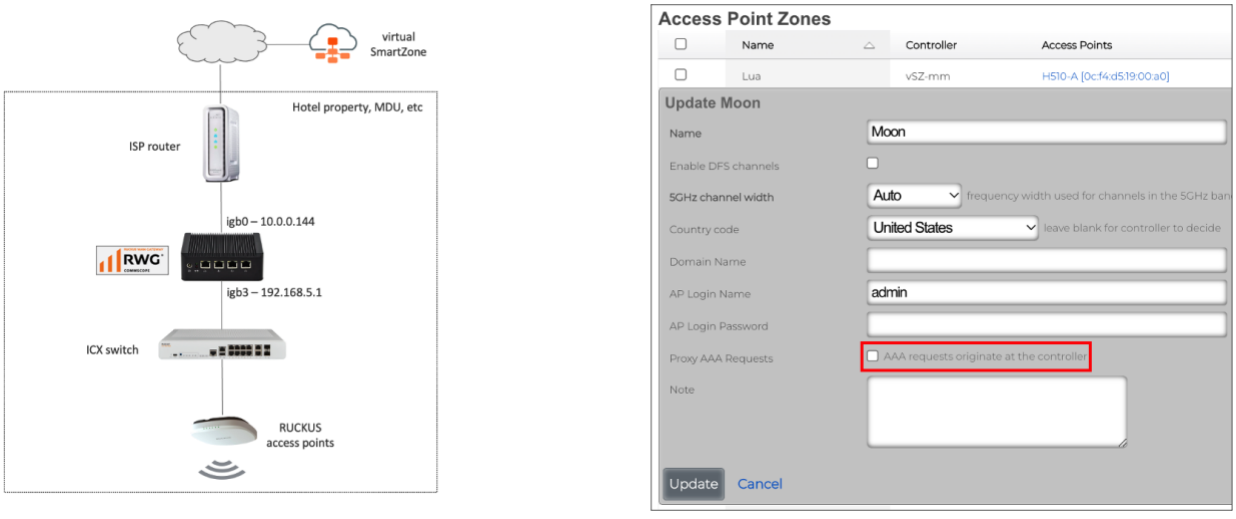


FIGURE 21 – REMOTE SMARTZONE AND ZONE CONFIGURED FOR NON-PROXY AP AUTHENTICATOR

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:

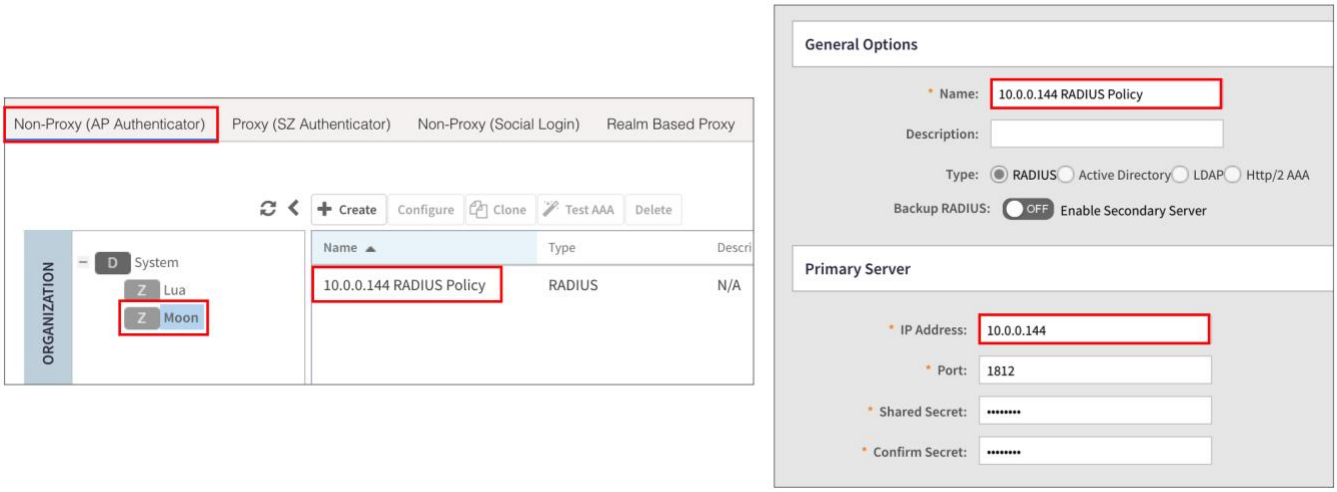


FIGURE 22 –SMARTZONE CONFIGURED AS NON-PROXY AP AUTHENTICATOR

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.

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:

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.

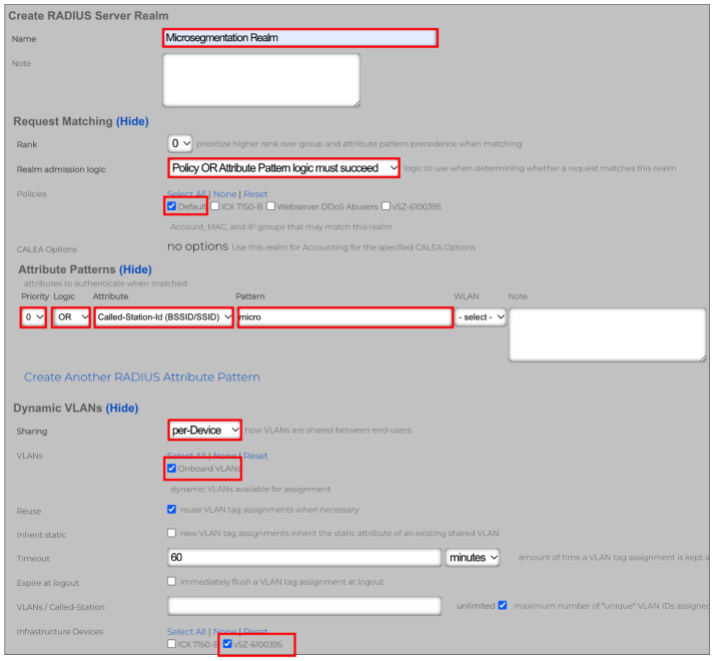


FIGURE 25 – CREATE RADIUS SERVER REALM

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.

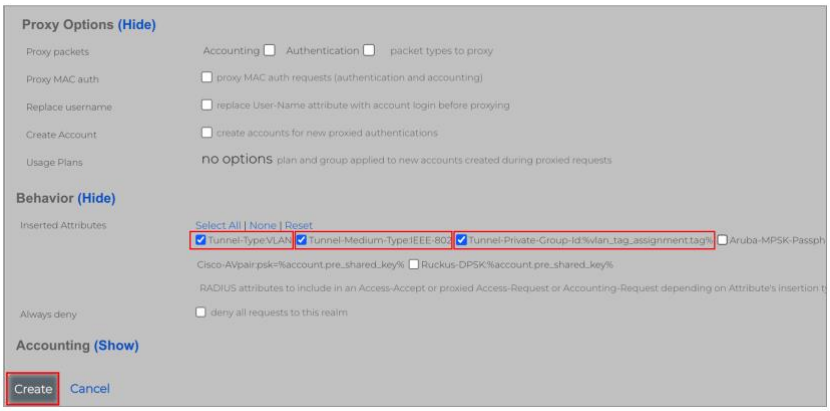


FIGURE 26 - CREATE RADIUS SERVER REALM (CONT'D)

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:

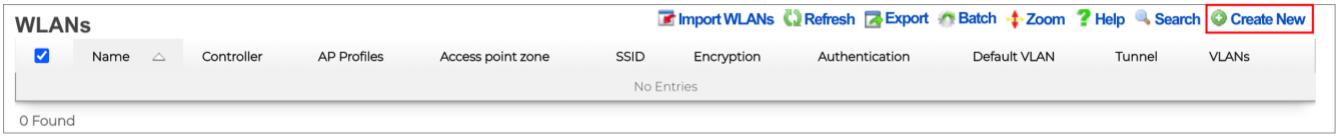


FIGURE 27 - CREATE A NEW WLAN

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**.

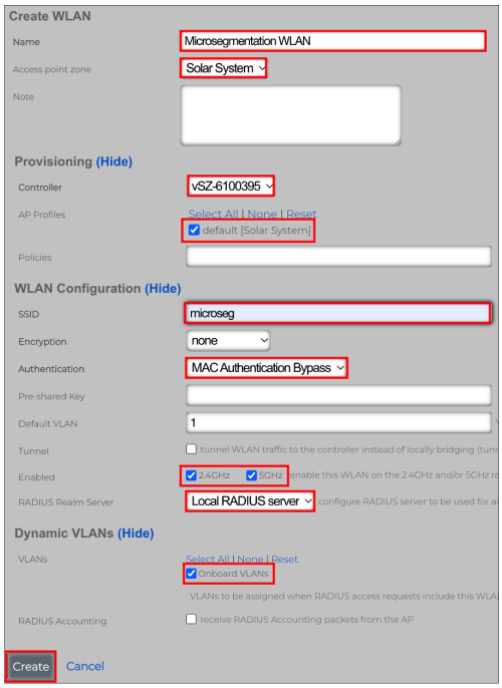


FIGURE 28 - CREATE WLAN

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.

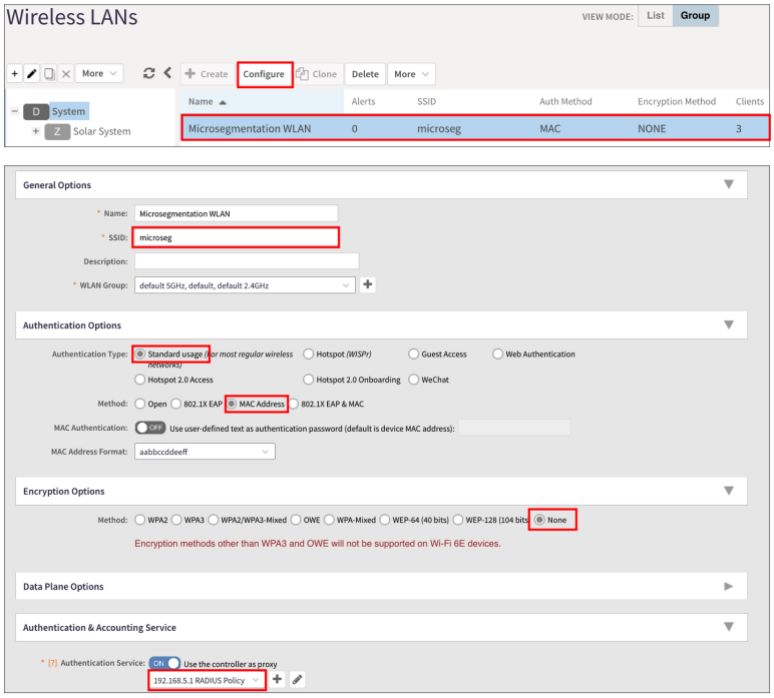
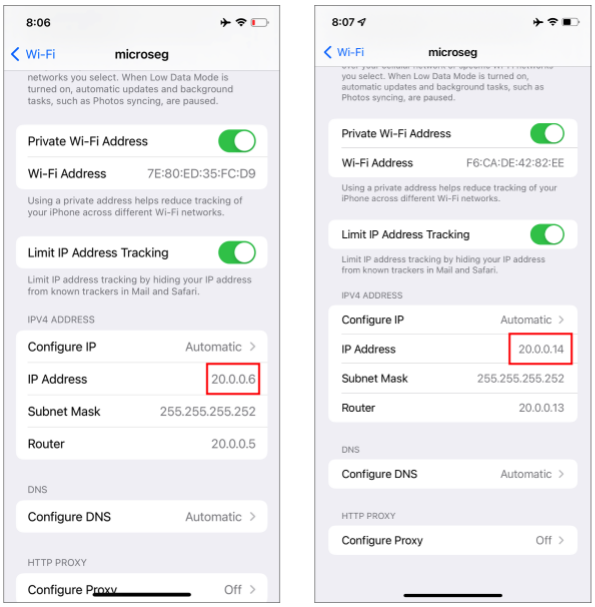


FIGURE 29 – CHECK THE WLAN IN SMARTZONE

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.



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
20.0.0.12	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:

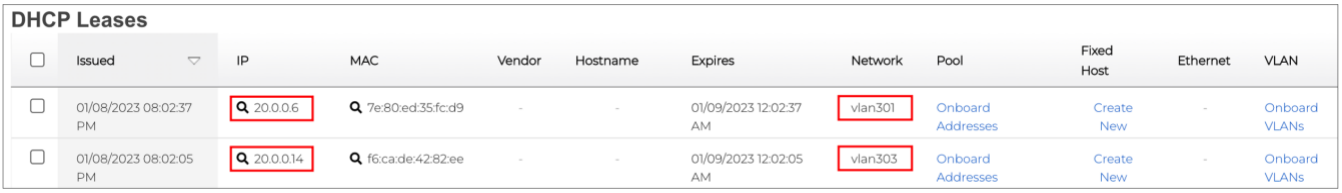


FIGURE 31 – CHECKING THE DHCP LEASES

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.

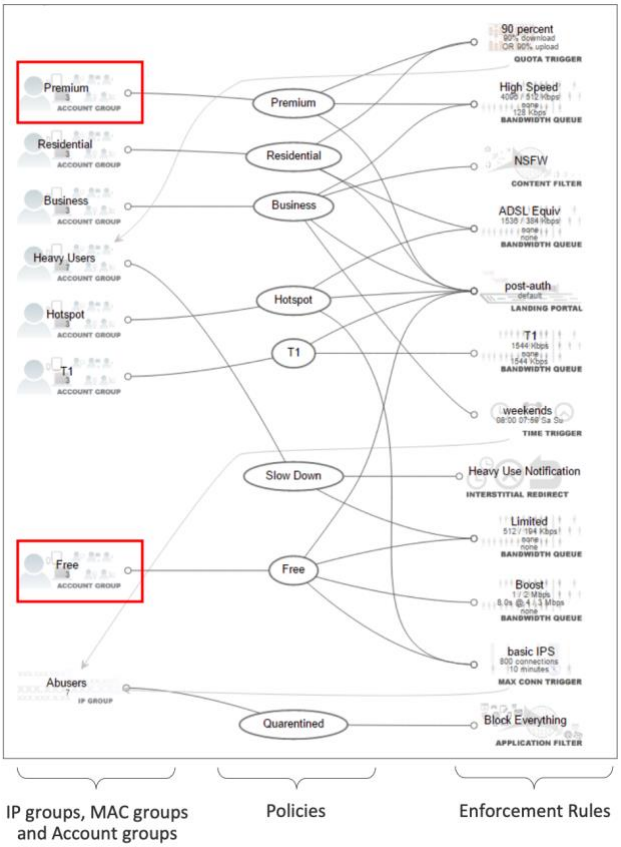


FIGURE 32 – EXAMPLES OF POLICIES

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.

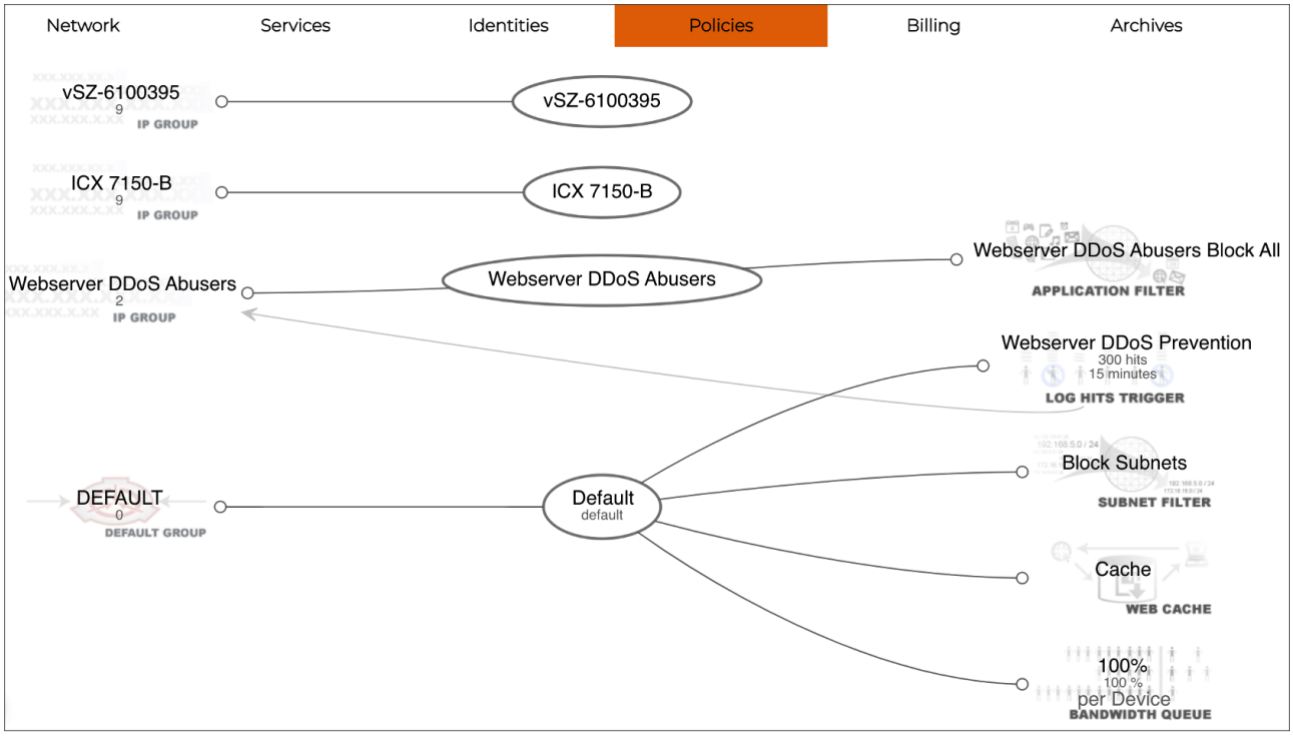


FIGURE 33 – THE RWG POLICIES PANEL

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**:

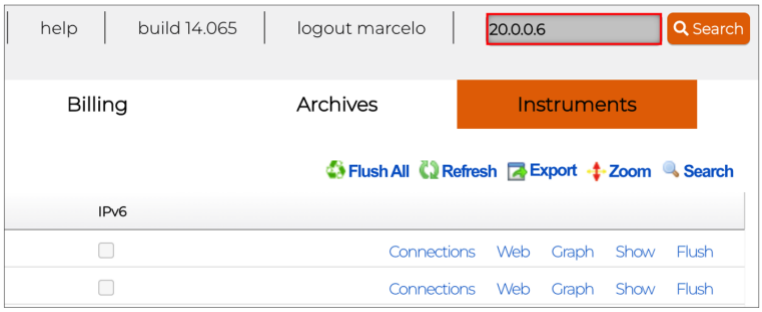


FIGURE 34 – THE SEARCH TOOL

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.

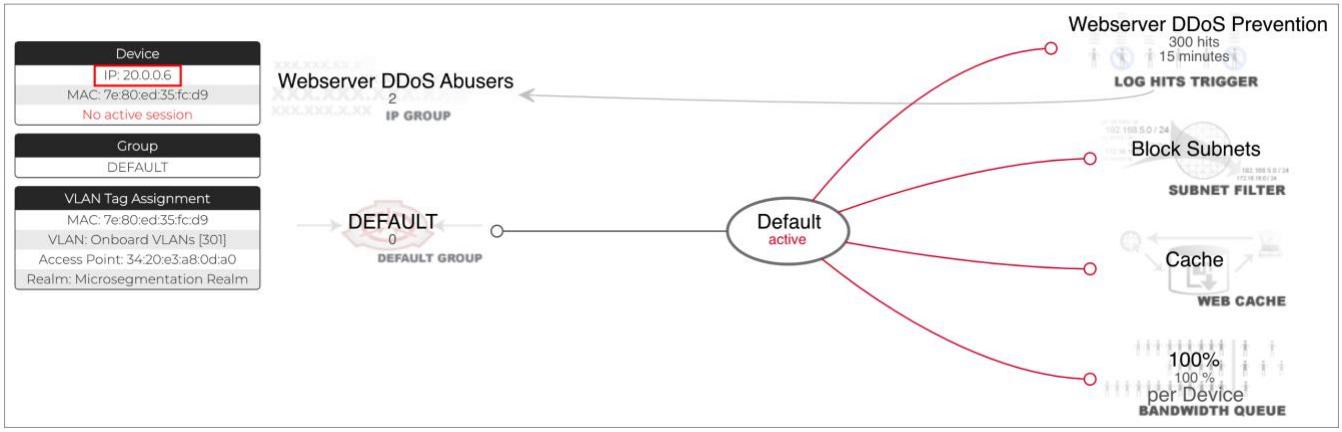


FIGURE 35 – POLICY FOR CLIENT 20.0.0.6

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.

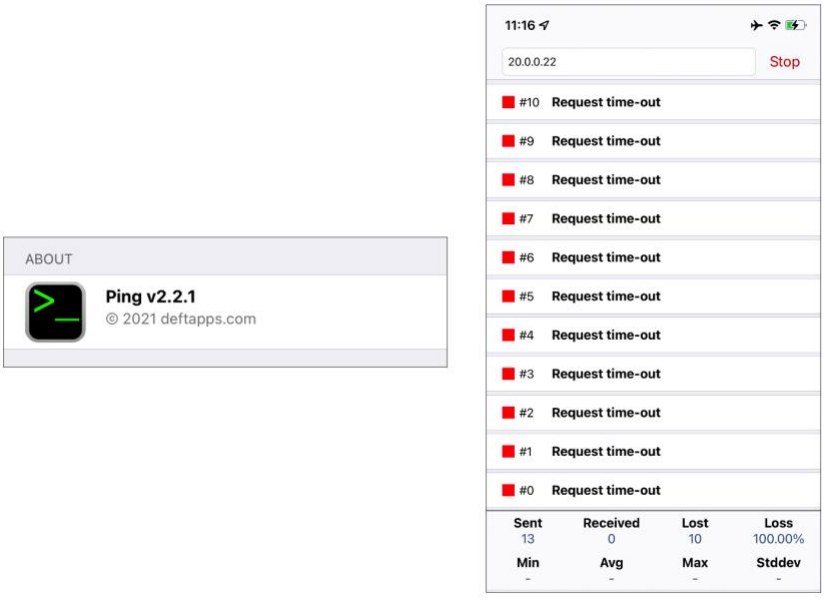


FIGURE 36 – THE PINGS FAIL

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.

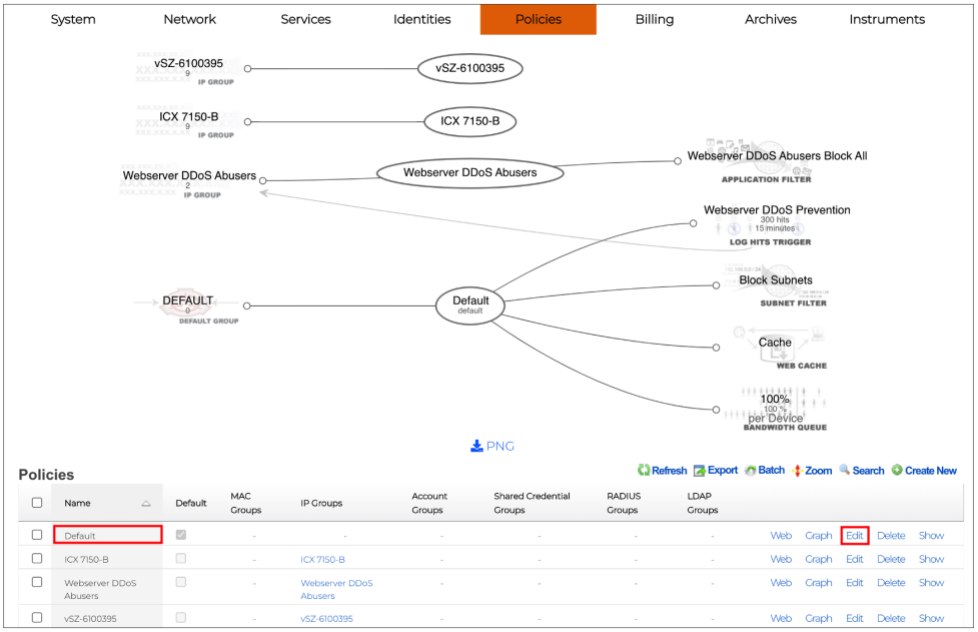


FIGURE 37 – EDIT A POLICY

Scroll down and unselect **Block Subnets** at **Subnets Filter**.

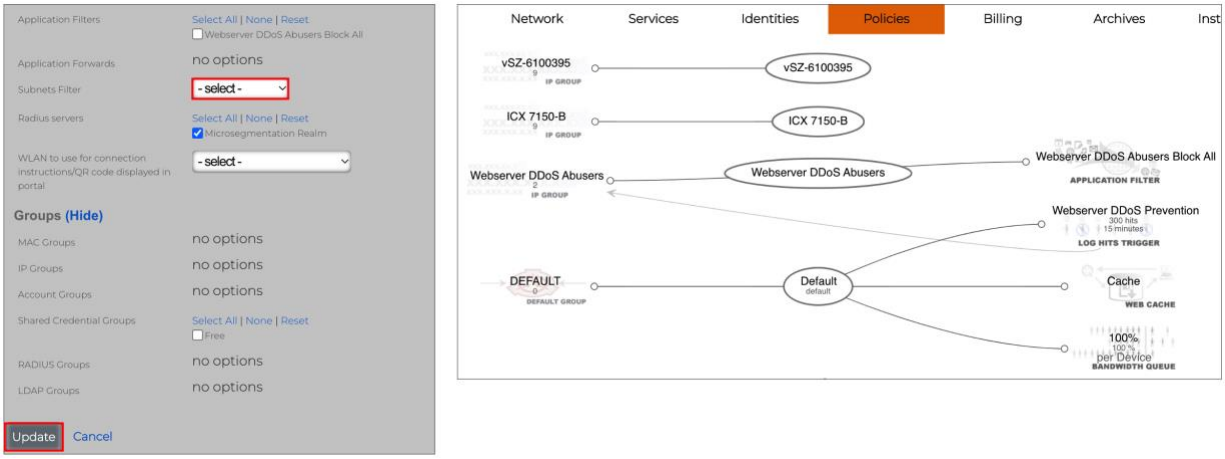


FIGURE 38 – THE BLOCK SUBNETS RULE IS DISABLED.

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.

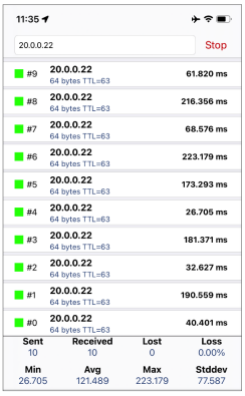


FIGURE 39 – THE PINGS ARE WORKING

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**.

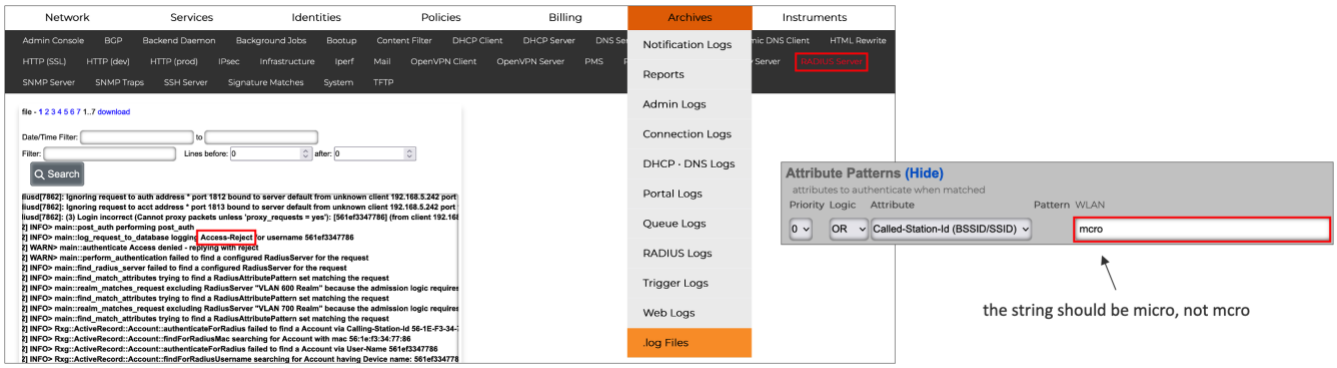


FIGURE 40 – THE PINGS ARE WORKING

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:

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:

```
log_request_to_database logging Access-Accept for username 561ef3347786
append_attributes reply AVP: Tunnel-Private-Group-Id => %vlan_tag_assignment.tag% (405)
append_attributes reply AVP: Tunnel-Medium-Type => IEEE-802
append_attributes reply AVP: Tunnel-Type => VLAN
append_attributes appending RadiusServer "Microsegmentation Realm" Attributes to the reply
perform_vta reusing existing VTA for MAC 56:1e:f3:34:77:86 with tag 405
perform_vta MAC 56:1e:f3:34:77:86 has an existing VTA with tag 405
perform_vta trying to assign a Vlan tag
perform_vta using Calling-Station-Id as the end-user's MAC: 56:1e:f3:34:77:86
find_radius_server found configured RadiusServer "Microsegmentation Realm" for the request
realm_matches_request selected highest priority(0) matching RadiusAttributePattern "micro" for the reques
realm_matches_request request matches pattern set in RadiusServer "Microsegmentation Realm" rank(0)
find_match_attributes AVP Called-Station-Id => B4-79-C8-0D-76-30:microseg matches RadiusAttributePatter
```

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:

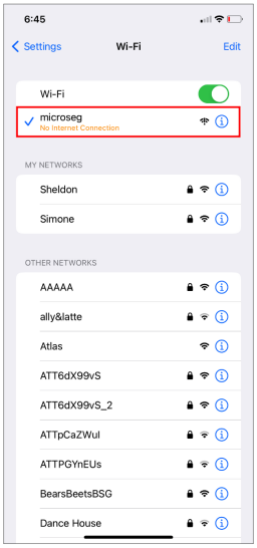


FIGURE 43 – NO INTERNET CONNECTIVITY

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:


```
[marcelo@rwg-home ~]$ ping -S 20.0.0.1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 20.0.0.1: 56 data bytes
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 0 packets received, 100.0% packet loss
```

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.

RUCKUS®
COMMSCOPE