

Network Address Translation

HOW TO GUIDE



July 2011

© 2016 ZIH Corp. All rights reserved. Zebra and the Stylized Zebra Head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. All other trademarks are property of their respective owners.

Table of Contents

1.	Introduction	4
1.1	Overview.....	4
1.2	Applications.....	5
1.3	Restrictions	5
2.	Pre-Requisites:.....	6
2.1	Requirements	6
2.2	Components Used:	6
3.	Configuration:	7
3.1	Dynamic NAT:.....	7
3.2	Static NAT	14
4	Viewing NAT Translations.....	19
4.	Reference Documentation.....	21

1. Introduction:

Network Address Translation (NAT) provides the translation of an Internet Protocol (IP) address within one network to a different known IP address within another network while in transit across a traffic routing device. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

The NAT feature is available on all controller models, the RFS40x0, RFS6000 and RFS7000. It is also available on all access points (AP7131N, AP532, AP6511, AP650) when routing the traffic from the wired and wireless clients, and is not restricted to the standalone access points.

1.1 Overview:

NAT functions by designating one or more interfaces as **Inside** while others as **Outside**.

- Inside – A set of networks subject to translation.
- Outside – All other addresses (typically valid public Internet addresses)

NAT uses a stateful translation table to dynamically map the **Inside** addresses to a single **Outside** address and then rewrites the IP headers so that the source IP packets appear to originate from the traffic routing device's **Outside** IP address. In the reverse path, responses from hosts through the **Outside** address are forwarded to the originating **Inside** IP address using the state information for the session in the translation table. The translation table rules and state are established dynamically and are flushed when no new traffic refreshes their state.

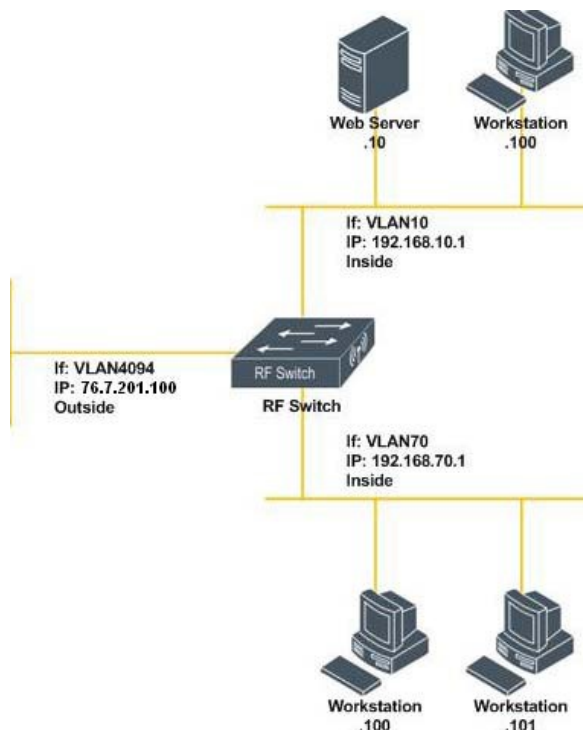


Figure 1.1 – Network Address Translation

NAT translation can occur in both directions. Most commonly translation will occur from the **Inside** interfaces to **Outside** interfaces providing private addressed hosts with Internet access. However static address translation can also be configured to translate specific ports on the **Outside** interface to a specific host a port on the **Inside** interface. A typical application for static NAT would be to allow hosts on the public internet to communicate with a web server behind the traffic routing device that is using private IP addresses which is not reachable from the public internet. The NAT service is used to provide outbound Internet access to wired and wireless hosts connected to a traffic routing device like RFS4000, RFS6000, RFS7000 or the access points AP7131N, AP6532, AP6511 or AP650, when routing traffic from connected devices.

1.2 Applications:

The most common application for NAT is to provide internet access by translating private addresses (RFC 1918) with one or more public internet addresses. This application often called **dynamic or many-to-one NAT** allows multiple hosts on the inside network to communicate with hosts on the public internet without exhausting valuable IPv4 space.

Other common application includes providing communications between hosts on overlapping networks during mergers and acquisitions which is common in banking and healthcare verticals. Additional common NAT applications include providing access to specific hosts and services on the inside network from hosts on the outside network allowing HTTP and other services to be served to public hosts without having to locate the server on the internet.

1.3 Restrictions:

Network Address Translation (NAT) only provides IP address translation services and does not provide firewall or filtering. The RF Controller includes a stateful packet inspection(SPI) firewall which can be used with NAT to restrict which IPv4 traffic can be received and routed by the individual IP interfaces on the RF Switch.

When deploying dynamic or static NAT it is recommended that a firewall rule be created and applied to the outside interface. For example when dynamic NAT is being used, a single firewall rule can be created and applied to the outside interface to deny all inbound traffic. As the integrated firewall is fully stateful, traffic originating from hosts on the inside network will pass freely through the firewall, however traffic originating from the outside network attempting to go inside will be blocked.

When static NAT is being deployed, the firewall rule can be modified to permit inbound traffic on the outside interface for the specific ports that are being translated. For example to allow HTTP a permit rule for destination TCP port 80 could be added before the deny all rule.

For examples of how to configure the stateful packet inspection firewall, please reference the Wireless Firewall How-To Guide.

2. Pre-Requisites:

2.1 Requirements:

The following requirements must be met prior to attempting this configuration:

- One (or more) RF Switches are installed and operational on the network with two or more virtual

interfaces defined.

- One (or more) Access Ports configured and adopted by the RF Switch.
- One (or more) WLAN profiles are configured and assigned to adopted radios.
- A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration.
- Two (or more) wireless workstations are available to test and verify NAT operations.
- Optionally a web server is available on the internal network to test port forwarding.
- The reader has read the Zebra Technologies WiNG5 System Reference Guide.

2.2 Components Used:

The information in this document is based on the following Zebra hardware and software versions:

- 1 x RFS6000 Version 5.1.0.0-074R.
- 1 x AP7131N.



Registered users may download the latest software and firmware from the Zebra Technologies Support Site <http://support.zebra.com>.

3. Configuration:

The NAT can be configured on the controllers or the access point profiles. Or the NAT profile can be configured on the device to override the service at the device level.

The following sections outline the configuration steps required to enable dynamic and static NAT on an RF Switch:

- 1) Dynamic NAT [[Section 3.1](#)]:
- 2) Static NAT [[Section 3.2](#)]:

3.1 Dynamic NAT:

Dynamic NAT provides a simple way to provide Internet access for private addressed hosts by dynamically translating private addresses to a single public IP address. This allows enterprises to provide Internet access to users without having to address internal hosts with publically routable IP addresses using valuable IPv4 address space and exposing the hosts to threats.

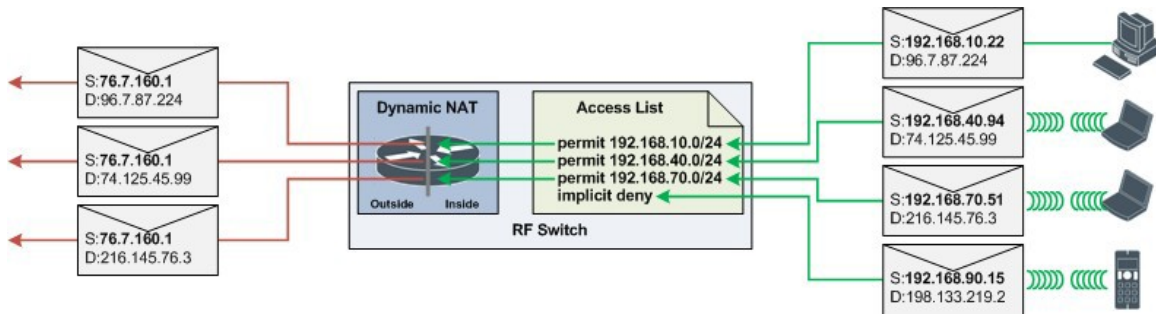


Figure 3.1 – Dynamic NAT Example

As shown in figure 3.1, wired and WLAN clients located on management, data and guest subnets are provided with Internet access through the RF Switch using Dynamic NAT. In this example the RF Switches internal interfaces vln10 (management) , vln40 (data) and vln70 (guest) have been designated as NAT **Inside** interfaces and the public interface vln4094 has been designated as a NAT **Outside** interface. This configuration will allow the RF Switch to translate packets received on the management and guest **Inside** interfaces to the **Outside** public IP address.

In addition a firewall IP Rule has been created with entries to only allow NAT translation for wired and wireless hosts in specific subnets. In this example, the IP rule allows the following:

- 1) Packets received from hosts in the 192.168.10.0/24 management subnet and the 192.168.40.0/24 data subnet will be translated.
- 2) Packets received from hosts in the 192.168.70.0/24 guest subnet will be translated.
- 3) Packets received hosts in the 192.168.90.0/24 voice subnet will not be translated.

3.1.1 Web UI Configuration:

The following configuration example will demonstrate how to enable dynamic NAT for internet access for specific IP subnets using the Web UI. The configuration is done on the RFS6000 controller at device level.

- 1) Specify the interface **Type** for the virtual **Interface**. In this example the management vln10, data vln40 and guest vln70 virtual interfaces will be designated as **Inside** and the Internet vln4094 will be designated as **Outside**. Click **OK**.

Interface	Type
Vlan10	Inside
Vlan40	Inside
Vlan70	Inside
Vlan4094	Outside

- 2) Navigate to the **Configuration > Devices > RFS6000-81C203 > Interface > Virtual Interfaces** window. Select the virtual Interface for **VLAN 10** and click **Edit**.

Dashboard Configuration Diagnostics Operations Statistics

RFS6000 WiNG v5.1 admin

Devices Wireless Profiles RF Domains Security Services Management

Device Configuration

Auto-Provisioning Policy
Critical Resource Policy
Event Policy
Mint Policy

Group By RF Domain

All Controller

RF Domain
default
rfs6000-81C20E
ep71xx-C78704

Type to search

Device rfs6000-81C20E (00-15-70-81-C2-0E) Type rfs6000 Profile Name default-rfs6000

Name	Type	Description	Admin Status	VLAN	IP Address
vlan1	VLAN		Disabled	1	
vlan10	VLAN		Enabled	10	192.168.10.1/24
vlan40	VLAN		Enabled	40	192.168.40.1/24
vlan4094	VLAN		Enabled	4094	dhcp
vlan70	VLAN		Enabled	70	192.168.70.1/24
vlan90	VLAN		Enabled	90	192.168.90.1/24

Type to search in tables

Row Count: 6

Add Edit Delete Exit

Event Summary

Find Functional Area

3) Select the NAT Direction as **Inside** for VLAN 10, vlan 40 and vlan 70. Click **Ok**.

Virtual Interfaces

VLAN ID vlan10

Basic Configuration Security

Properties

Description

Admin Status Disabled Enabled

IP Addresses

Enable Zero Configuration None Primary Secondary

Primary IP Address 192.168.10.1 / 24

Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers (Allowed on 1 virtual interface)

Secondary Addresses

DHCP Relay

Respond to DHCP Relay Packets

DHCP Relay

IP Address

0.0.0.0 Clear

0.0.0.0 Clear

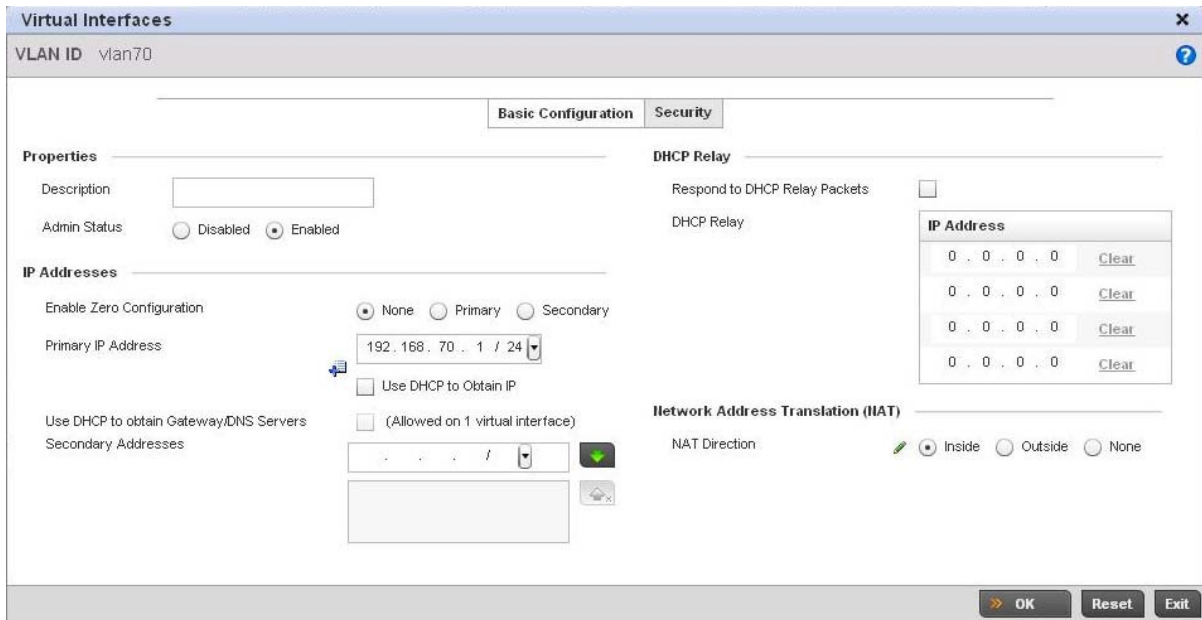
0.0.0.0 Clear

0.0.0.0 Clear

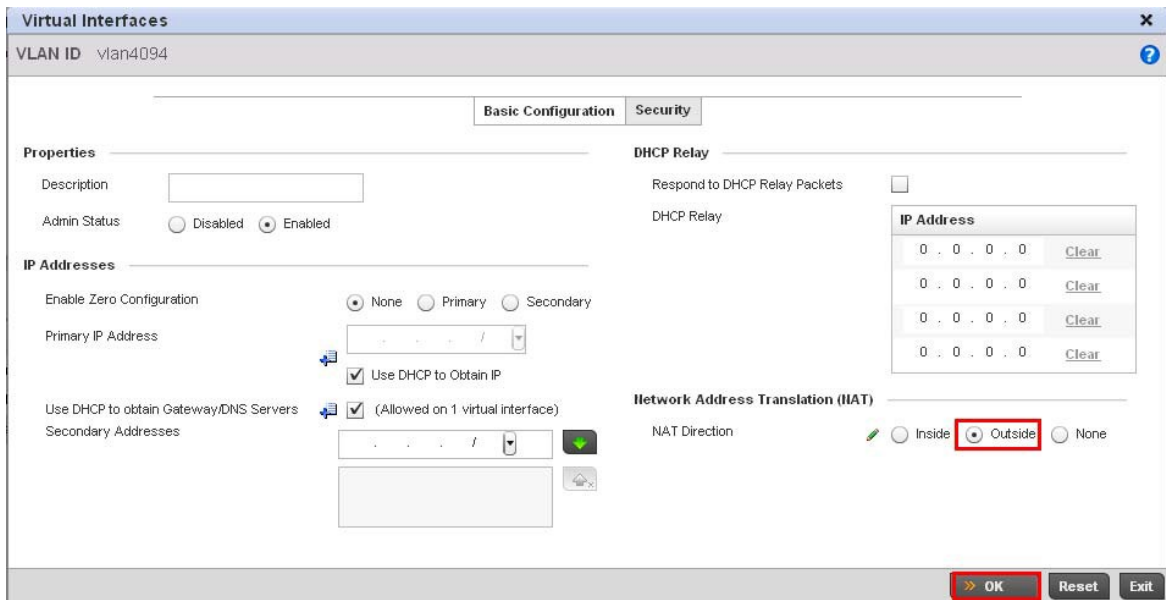
Network Address Translation (NAT)

NAT Direction Inside Outside None

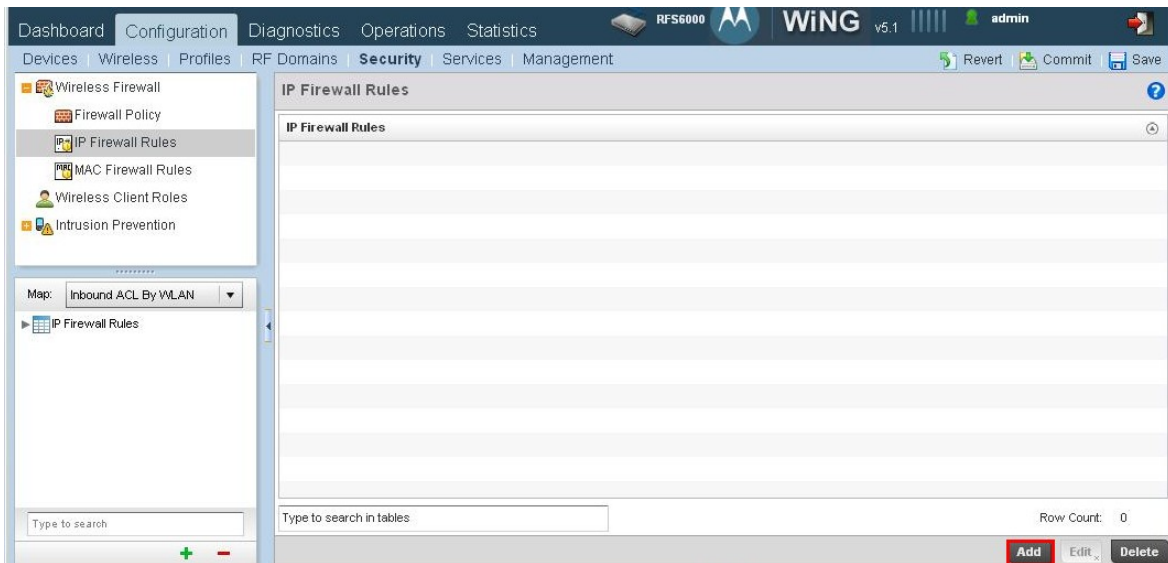
>> OK Reset Exit



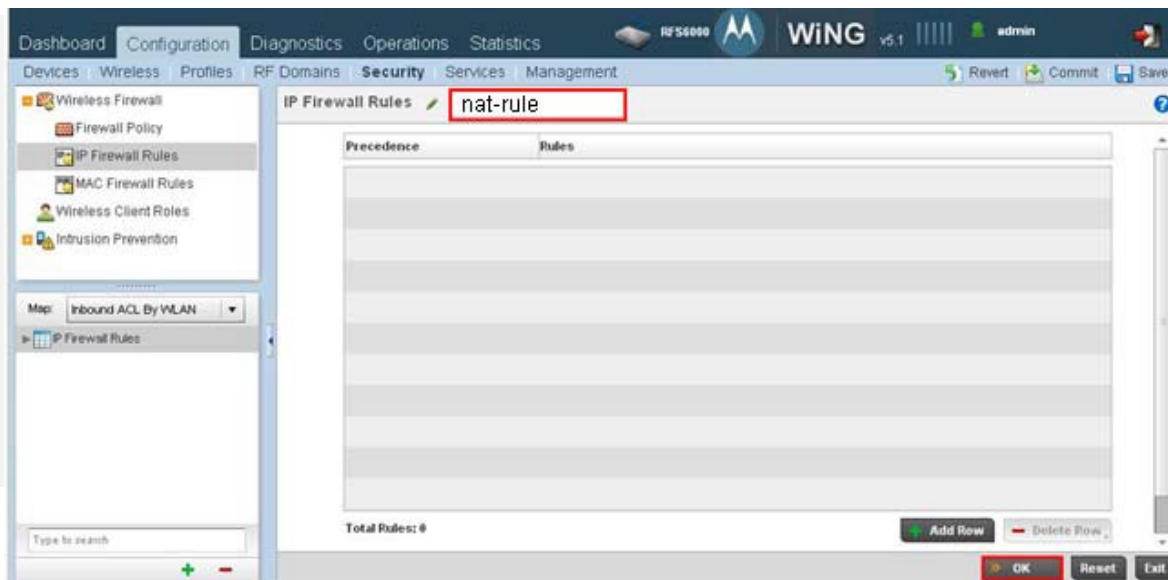
4) Select the NAT Direction as **Outside** for **VLAN 4094**. Click **Ok**.



- 5) Navigate to the **Configuration > Security > Wireless Firewall > IP Firewall Rules** window. Click **Add** to create an ACL to tell the RF Switch which source subnets to NAT for Internet access.



- 6) Enter a unique name **nat-rule**. Click **OK**.



- 7) In the **Add Row** window create a rule for each subnet you wish to provide Internet access to. For each rule set the **Operation** to **Permit** and specify the **Source Mask** and **Source Address**. In this example the management (192.168.10.0/24), WLAN data (192.168.40.0/24) and WLAN guest (192.168.70.0/24) subnets will be permitted Internet access. Click **OK** after creating each rule.

The screenshot shows the 'IP Firewall Rules' configuration window with the 'Rules' tab selected. A single rule is displayed with the following configuration:

- Precedence:** 10
- Operation:** Permit (checked)
- Source:** Mask, 192.168.10.0/24
- Destination:** Any, 0.0.0.0/0
- Protocol:** ip, 0
- Action:** Log, Mark (unchecked)
- Description:** (empty)

Buttons for 'Add Row' and 'Delete Row' are visible at the bottom right. The 'Total Rules: 1' indicator is at the bottom left. The window title is 'IP Firewall Rules nat-rule'.

The screenshot shows the 'IP Firewall Rules' configuration window with the 'Rules' tab selected. Two rules are displayed, with the second rule selected:

- Precedence:** 20
- Operation:** Permit (checked)
- Source:** Mask, 192.168.40.0/24
- Destination:** Any, 0.0.0.0/0
- Protocol:** ip, 0
- Action:** Log, Mark (unchecked)
- Description:** (empty)

Buttons for 'Add Row' and 'Delete Row' are visible at the bottom right. The 'Total Rules: 2' indicator is at the bottom left. The window title is 'IP Firewall Rules nat-rule'.

IP Firewall Rules nat-rule

Precedence Rules

10 permit ip mask 192.168.40.0/24 any

20 permit ip mask 192.168.40.0/24 any

30 permit ip mask 192.168.70.0/24 any

Allow: Permit

Source: Mask 192.168.70.0 / 24 Destination: Any 0.0.0.0 / 0

Protocol: ip 0

Action: Log Mark

Precedence: 30 Description:

Total Rules: 3

Add Row Delete Row

OK Reset Exit



Optionally, the RF Switch may permit NAT for any source subnet by creating a **permit any** rule.

- 8) Navigate to the **Configuration > Devices > RFS6000-82c201 > Security > NAT window**. Select the **Dynamic NAT** tab then click **Add**. This will create a dynamic NAT rule translating private addresses defined in the ACL received on *inside* interfaces to the public *outside* internet **vlan 4094**.

Device rfs6000-81C20E (00-15-70-81-C2-0E) Type rfs6000 Profile Name default-rfs6000

Basic Configuration Licenses Certificates RF Domain Overrides RF Domain Sensor Configuration WLAN Override Profile Overrides General Cluster Interface Network Security General Certificate Revocation ISAKMP Policy Transform Set VPN Configuration NAT Services

NAT Pool Static NAT **Dynamic NAT**

Source List ACL	Network	Interface	Overload Type	NAT Pool	Overload IP

Type to search in tables

Row Count: 0

Add Edit Delete Exit

- 9) Select the Source List ACL **nat-rule** created in step 5. Set the **Network Type** to **Inside**. Set the Interface to the public outside virtual interface **vlan 4094**. Select the **Overload Type** as **Interface IP Address** to automatically select the IP address assigned to the Virtual Interface vlan 4094. Click **OK** and **Exit**.

The screenshot shows the 'Source' configuration window. The 'Source List ACL' is set to 'nat-rule' and the 'Network' is set to 'Inside'. Under 'Settings', the 'Interface' section has 'VLAN ID' set to '4094'. The 'Overload Type' section has 'Interface IP Address' selected. The 'NAT Pool' and 'Overload IP' fields are empty. At the bottom right, the 'OK' button is highlighted.

- 10) Click **Commit** to apply and **Save** to save changes.



For security it is recommended that a firewall rule be created and applied to the outside interface to block all inbound traffic. For examples of how to configure the stateful inspection firewall, please reference the Wireless Firewall How-To Guide.

3.12 CLI Configuration:

The following configuration example will demonstrate how to enable dynamic NAT for internet access for specific IP subnets using the CLI:

- 1) Specify the interface **Type** for the virtual **Interface**. In this example the management vlan10, data vlan40 and guest vlan70 virtual interfaces will be designated as **Inside** and the Internet vlan4094 will be designated as **Outside**. Click **OK**.

Interface	Type
Vlan10	Inside
Vlan40	Inside
Vlan70	Inside
Vlan4094	Outside

```
rfs6000-81C20E*#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. rfs6000-81C20E(config)*#rfs6000 00-15-70-81-C2-0E rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#interface vlan 10 rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan10)*#ip nat inside rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan10)*#.. rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#interface vlan 40 rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan40)*#ip nat inside rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan40)*#.. rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*# rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#interface vlan 70 rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan70)*#ip nat inside rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan70)*#.. rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*# rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#interface vlan 4094 rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan4094)*#ip nat outside rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan4094)*#.. rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#exit rfs6000-81C20E(config)*#
```

- 2) Create an ACL to identify which source subnets to NAT for Internet access

```
rfs6000-81C20E(config)*#ip access-list nat-rule rfs6000-81C20E(config-device-00-15-70-81-
C2-0E)*# rfs6000-81C20E(config-ip-acl-nat-rule)*# permit ip 192.168.10.0/24 any rule-
precedence 10 rfs6000-81C20E(config-ip-acl-nat-rule)*# permit ip 192.168.40.0/24 any
rule-precedence 20 rfs6000-81C20E(config-ip-acl-nat-rule)*# permit ip 192.168.70.0/24 any
rule-precedence 30 rfs6000-81C20E(config-ip-acl-nat-rule)*#exit

rfs6000-81C20E(config)*#
```

- 3) Create a dynamic NAT rule translating private addresses defined in the ACL received on *inside* interfaces to the public *outside* internet **vlan 4094**.

```
rfs6000-81C20E(config)*#rfs6000 00-15-70-81-C2-0E rfs6000-81C20E(config-device-
00-15-70-81-C2-0E)*# ip nat inside source list nat-rule interface vlan4094 overload
rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#exit

rfs6000-81C20E(config)*# commit write
```

3.2 Static NAT:

Static NAT can be used for multiple applications such as providing a direct one-to-one translation for Internet access; however the most common application is to provide port forwarding services allowing specific ports on a public interface to be forwarded to a host on the private network such as a web server or VPN gateway. Often referred to as port forwarding or port address translation, static NAT can be configured to forward TCP or UDP packets received from hosts on the public internet to hosts located on the private network without having to obtain public addresses or deploy dedicated servers in a DMZ.

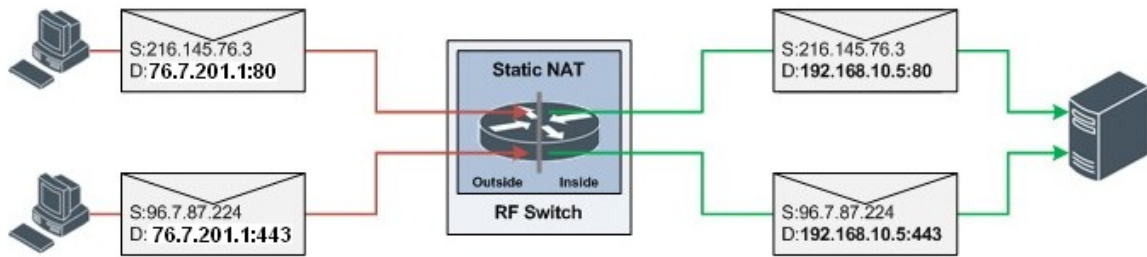


Figure 3.2 – Static NAT Example

As shown in figure 3.2, static NAT translation has been used to translate TCP port 80 and 443 packets received on the **Outside** public interface vlan4094 to a web server located on the **Inside** management interface vlan10.

Static NAT can only translate unique TCP or UDP ports on the outside interface to an internal host. If translation is required for multiple instances of a common port (example HTTP), unique ports must be defined on the outside interface. Table 4.3.2 shows an example Static NAT configuration unique TCP ports have been defined on the outside interface that are translated to two internal hosts listening on TCP port 80 & 443.

Outside IP Address	Outside TCP Port	Inside IP Address	Inside TCP Port
76.7.207.1	80	192.168.10.5	80
76.7.207.1	81	192.168.10.6	80
76.7.207.1	443	192.168.10.5	443
76.7.207.1	444	192.168.10.6	443

Table 3.2 – Static NAT Translation Example

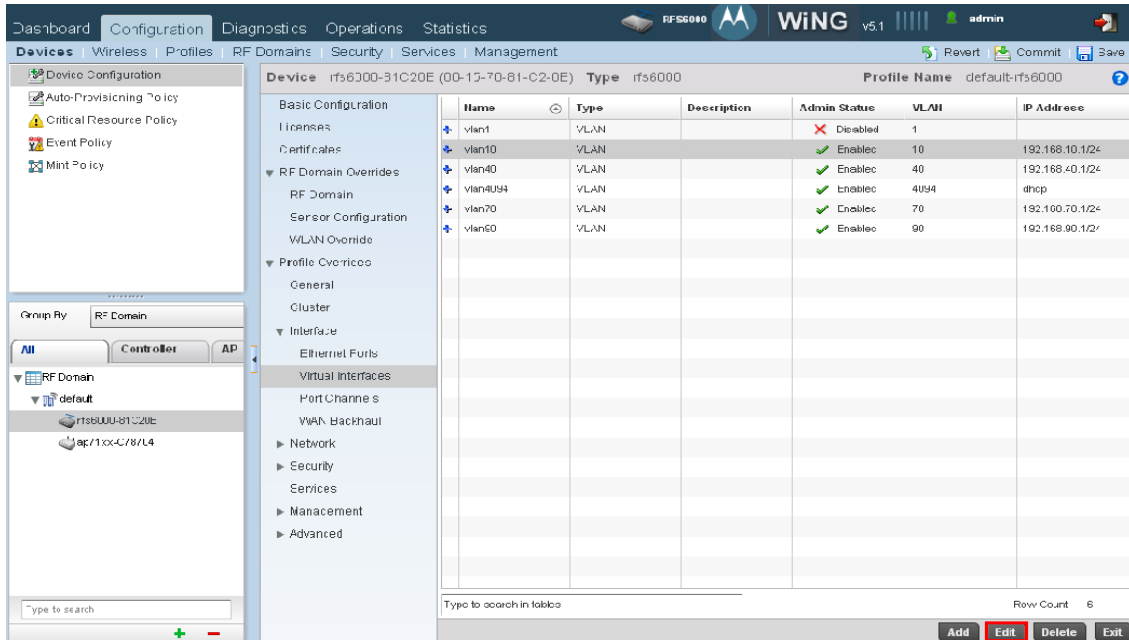
3.2.1 Web UI Configuration:

The following configuration example will demonstrate how to enable static NAT to provide port forwarding for specific ports using the Web UI:

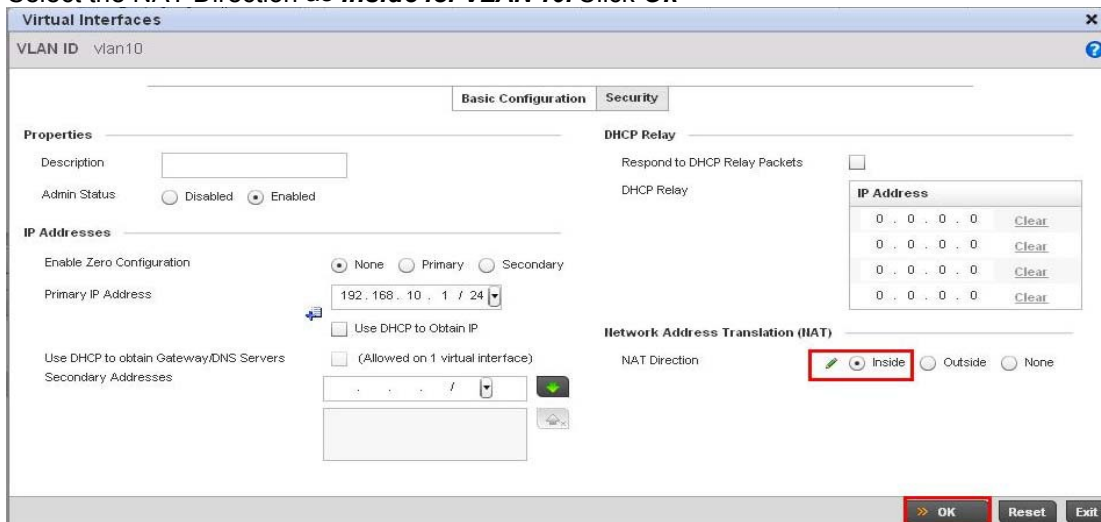
- 1) Specify the interface **Type** for the **virtual Interface**. The management vlan10 will be designated as **Inside** and the Internetvlan4094 will be designated as **Outside**.

Interface	Type
Vlan10	Inside
Vlan4094	Outside

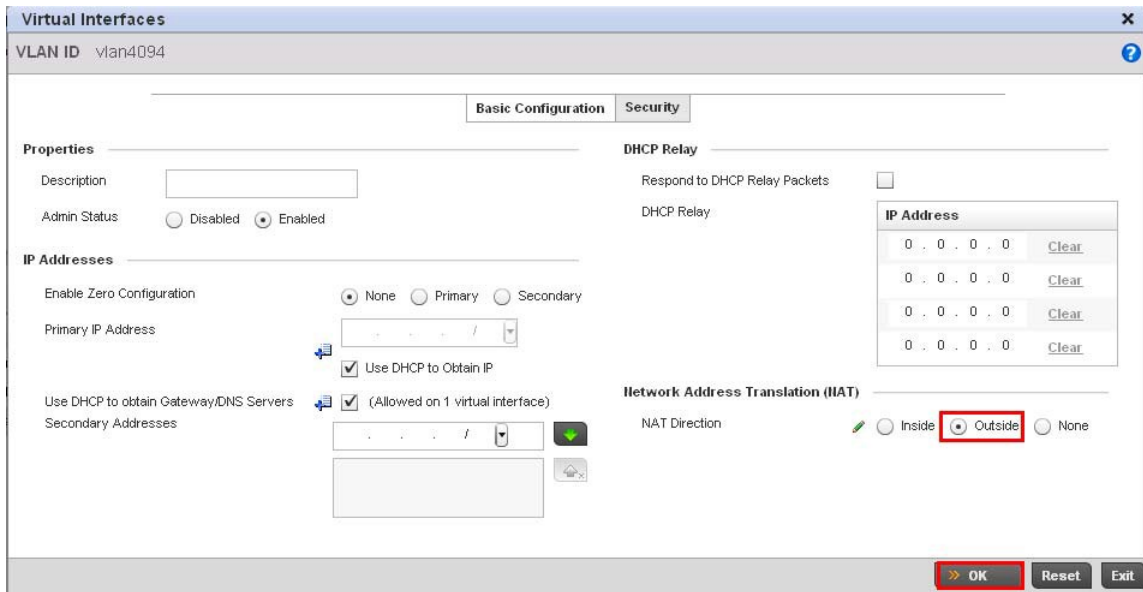
- Navigate to the **Configuration > Devices > RFS6000-81C203 > Interface > Virtual Interfaces**. Select the virtual Interface for **VLAN 10** and click **Edit**.



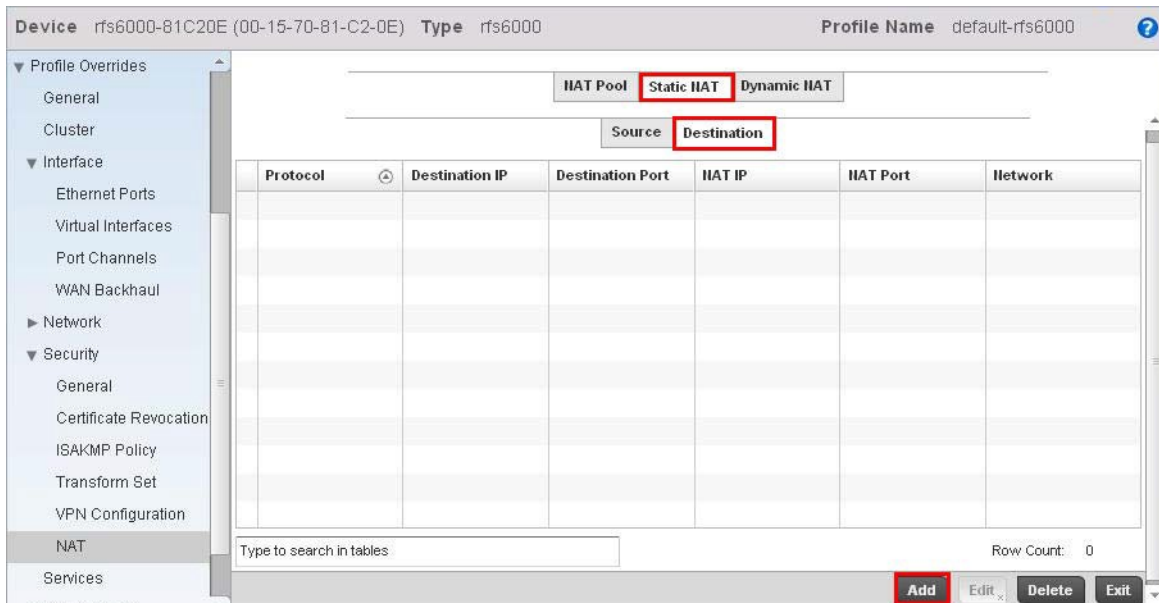
- Select the NAT Direction as **Inside for VLAN 10**. Click **Ok**



Select the NAT Direction as **Outside** for **VLAN 4094**. Click **Ok**.



- 4) In this example we will create two static NAT rules to translate **TCP** port **80** and **TCP** port **443** traffic received on the public **Outside** interface **vlan4094** to a web server **192.168.10.20** on the **Inside** management interface **vlan10**. Navigate to the **Configuration > Devices > RFS6000-name > Security > NAT** window. Select the **Static NAT > Destination** tab and click **Add**.



- 5) Select the **TCP** protocol. Set the **Destination IP** to the IP address of the public outside Interface and the **NAT IP** to the private server IP address. Define the **Destination Port** and NAT port values (80 and 443 in this example). Select the Network type as **Outside**. Click **OK** and **Exit**.

The screenshot shows a configuration window titled "Destination" with a sub-header "Add Destination NAT". Under the "Settings" section, the following fields are visible and highlighted with red boxes:

- Protocol: TCP
- Destination IP: 76 . 7 . . 207 . 1
- Destination Port: 80 (with a "www" dropdown and "(1 to 65,535)" range indicator)
- NAT IP: 192 . 168 . . 10 . 20
- NAT Port: 80 (with a "www" dropdown and "(1 to 65,535)" range indicator)
- Network: Outside

At the bottom right of the window, there are three buttons: "OK", "Reset", and "Exit", all of which are also highlighted with red boxes.

x
Destination

?
Add Destination NAT

Settings

Protocol TCP

Destination IP 76 . 7 . 207 . 1

Destination Port 443 www (1 to 65,535)

NAT IP 192 . 168 . 10 . 20

NAT Port 443 www (1 to 65,535)

Network Outside

>> OK
Reset
Exit

5) Click **Commit** to apply and **Save** to save changes.



For security it is recommended that a firewall rule be created and applied to the outside interface that will permit destination TCP port 80 and 443 traffic but block all other traffic. For examples of how to configure the stateful inspection firewall, please reference the Wireless Firewall How-To Guide.

3.2.1 CLI Configuration:

The following configuration example will demonstrate how to enable static NAT to provide port forwarding for specific ports using the Web UI:

- 1) Specify the interface **Type** for the **virtual Interface**. The management vlan10 will be designated as **Inside** and the Internetvlan4094 will be designated as **Outside**.

Interface	Type
Vlan10	Inside
Vlan4094	Outside

```
rfs6000-81C20E*#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. rfs6000-81C20E(config)*#rfs6000 00-15-70-81-C2-0E rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#interface vlan 10 rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan10)*#ip nat inside rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan10)*#.. rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*# rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#interface vlan 4094 rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan4094)*#ip nat outside rfs6000-81C20E(config-device-00-15-70-81-C2-0E-if-vlan4094)*#.. rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#exit rfs6000-81C20E(config)*#
```

- 2) Create two static NAT rules to translate **TCP** port **80** and **TCP** port **443** traffic received on the public **Outside** interface **vlan4094** to a web server **192.168.10.20** on the **Inside** management interface **vlan10**. **Save** and **Apply** the changes.

```
rfs6000-81C20E(config)*#rfs6000 00-15-70-81-C2-0E rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*# ip nat outside destination static 76.7.207.1 80 tcp 192.168.10.20 80
```

```
rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*# ip nat outside destination static 76.7.207.1 443 tcp 192.168.10.20 443
```

```
rfs6000-81C20E(config-device-00-15-70-81-C2-0E)*#exit  
rfs6000-81C20E(config)*# commit write rfs6000
```

4. Viewing NAT Translations

The NAT translations can be seen in the **Statistics > <Rf-domain> > RFS6000-81C2OE > Firewall > NAT Translations**.

The screenshot shows the Zebra WiNG 5 management interface. The main content area displays a table of NAT Translations statistics for the Wireless Controller 'rfs6000-81C2OE (00-15-70-81-C2-0E)'. The table has the following columns: Protocol, Forward Source IP, Forward Source Port, Forward Dest IP, Forward Dest Port, Reverse Source IP, Reverse Source Port, Reverse Dest IP, and Reverse Dest Port. The table contains 8 rows of data, all with a green status icon in the Protocol column.

Proto col	Forward Source IP	Forward Source Port	Forward Dest IP	Forward Dest Port	Reverse Source IP	Reverse Source Port	Reverse Dest IP	Reverse Dest Port
tcp	192.168.10.20	3,367	203.126.136.201	1,080	203.126.136.201	1,080	157.235.207.168	38,335
tcp	157.235.207.8	2,972	157.235.207.168	21	192.168.10.20	21	157.235.207.8	2,972
tcp	192.168.10.20	3,366	203.126.136.201	1,080	203.126.136.201	1,080	157.235.207.168	45,133
tcp	192.168.10.20	3,369	203.126.136.201	1,080	203.126.136.201	1,080	157.235.207.168	34,166
tcp	192.168.10.20	3,371	203.126.136.201	1,080	203.126.136.201	1,080	157.235.207.168	52,293
tcp	192.168.10.20	3,368	203.126.136.201	1,080	203.126.136.201	1,080	157.235.207.168	55,459
tcp	192.168.10.20	3,370	203.126.136.201	1,080	203.126.136.201	1,080	157.235.207.168	53,159
udp	192.168.10.20	1,026	157.235.188.210	161	157.235.188.210	161	157.235.207.168	60,222

The interface also shows a search bar at the bottom with the text 'Type to search in tables' and a 'Refresh' button. The Row Count is 8.

5. Reference Documentation:

Description	Location
Zebra Technologies WiNG 5 System Reference Guide	http://support.zebra.com
Zebra Technologies WiNG 5 CLI Reference Guide	http://support.zebra.com