Network Address Translation (NAT)

The Network Address Translation (NAT) protocol describes a procedure for automatically and transparently changing IP address information in IP data packets while still transmitting the packets to the intended destination.

NAT can be used when you do not want IP addresses of an internal network to be visible from outside. The reasons for this can include:

Keeping the structure of the internal network hidden from the outside world

Keeping private IP addresses hidden

Using IP addresses multiple times - for example, by forming identical production cells

This document describes the NAT configuration options available in the Eagle20/30 Industrial Firewall and Security Router.

Table of Contents

Featured Brands

lumbergautomation A BELDEN BRAND
HIRSCHMANN A BELDEN BRAND
TOFINO SECURITY A BELDEN BRAND
GarrettCom A BELDEN BRAND

Phone: **1.800.BELDEN1**
www.belden.com

IP Masquerading NAT

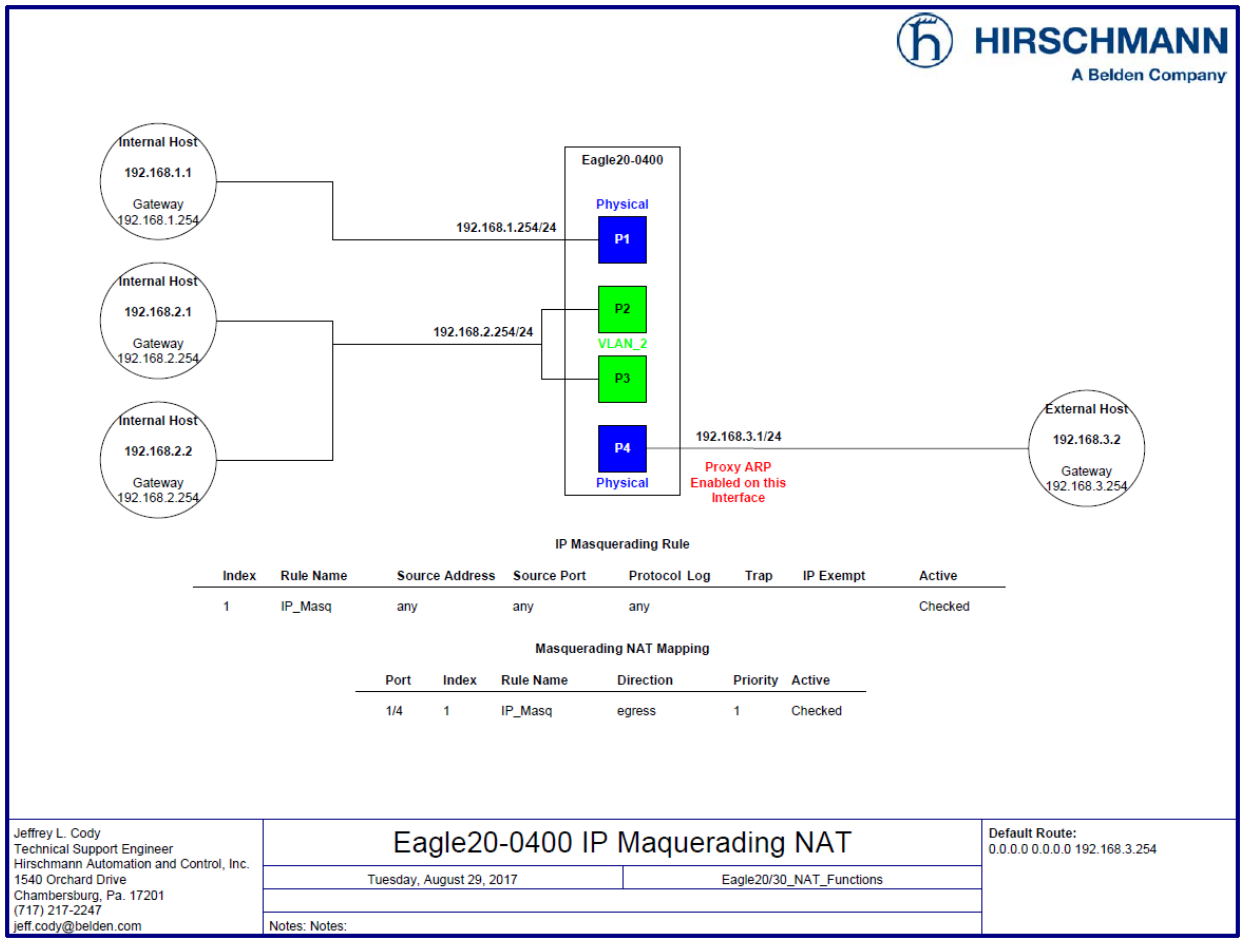
You can use IP Masquerading to hide the internal IP Addressing structure from hosts on the external IP network.

With IP Masquerading, the firewall replaces the source IP address of an IP data packet from the internal network with the external IP address of the firewall.

IP Masquerading also allows you to configure multiple internal IP networks using the same IP addressing schemes to connect to a common external network, which would not be possible without IP Masquerading.

However, as devices in the external network only know the external IP address of the firewall, they are unable to set up a direct communication connection to a device in the internal network.

Sample Network



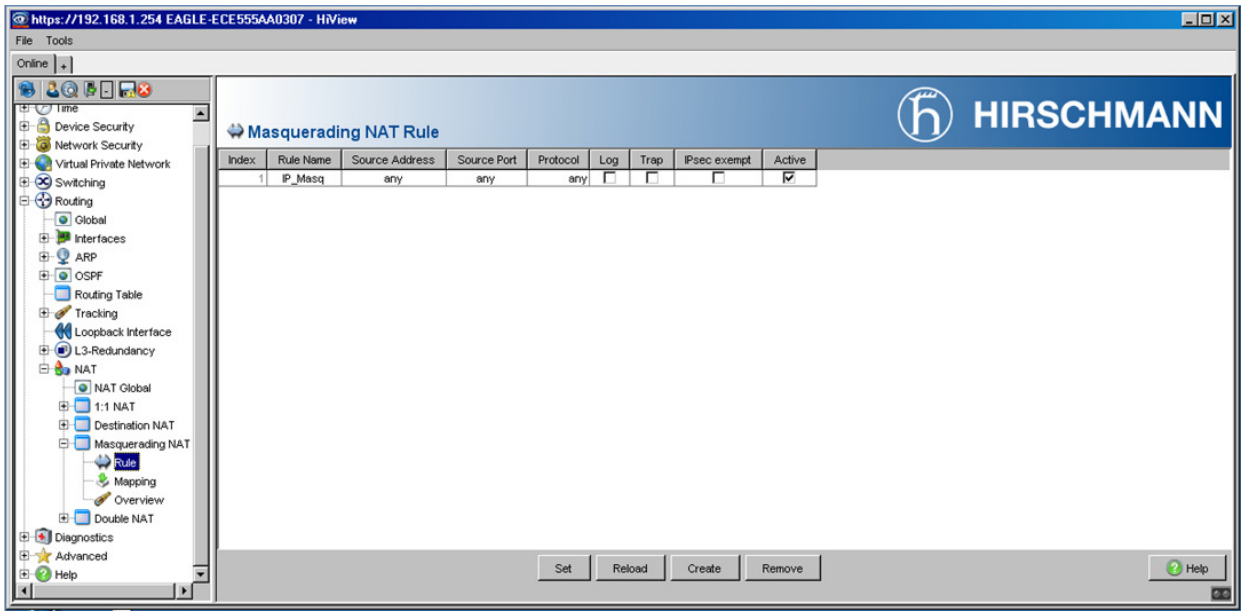
This sample networks depicts hosts on separate IP networks separated by an Eagle20/30 Firewall with IP Masquerading configured.

Pre-Requisites:

1. The Eagle20/30 Firewall must be configured to operate in **Router Mode**.
2. The internal and external networks must use unique IP Addressing schemes.
3. **Proxy ARP** must be enabled on the port(s) that are to be treated as an external port.
4. The **Network Security** / **Packet Filter** / **Global** page should have the **Default Policy** set to **Drop**.
5. Outbound packet filter rules must be configured and assigned that permits traffic to any destination.
6. The hosts residing on the internal network must have the IP Address of the Eagle20/30's internal interface defined as their Default Gateway address.

Configuration Steps:

1. Using the Eagle20/30's web interface (GUI), navigate to the **Routing** / **NAT** /**Masquerading NAT** / **Rule** page of the menu.
2. Click the **Create** button at the bottom of the page. Add a name to the **Rule Name** field.
3. Add **any** as the **Source Address**.
4. Click the **Set and Back** button at the bottom of the page.
5. Make the rule **Active** and then click the **Set** button.

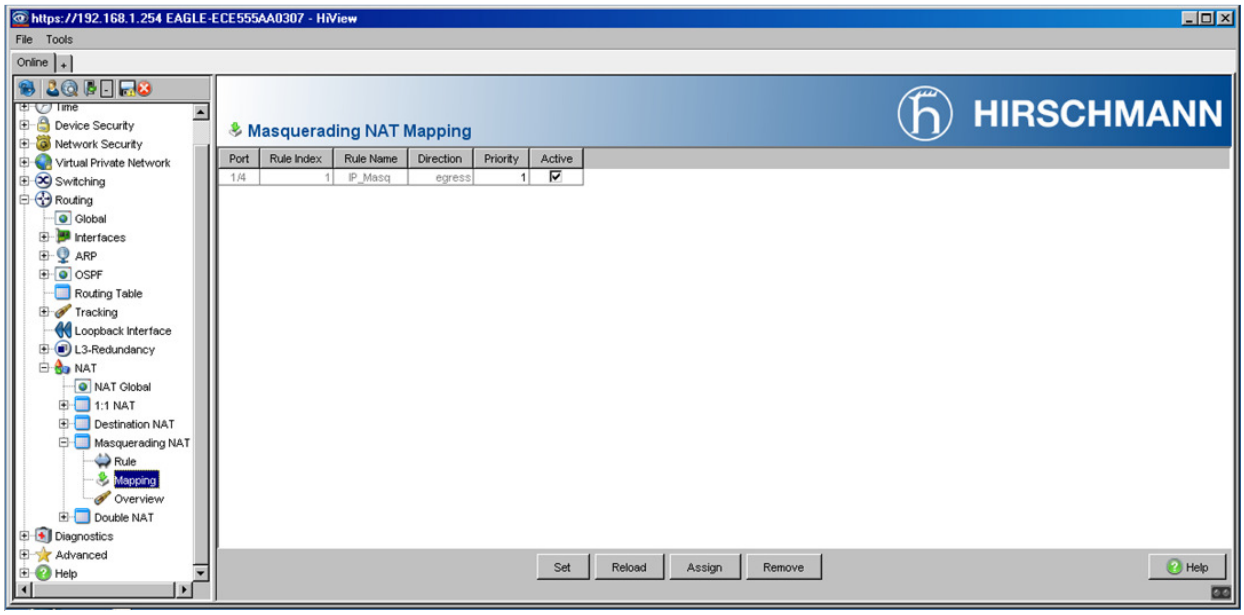


6. Navigate to the **Routing** / **NAT** / **Masquerading NAT** / **Mapping** page of the menu.

7. Click the **Assign** button.

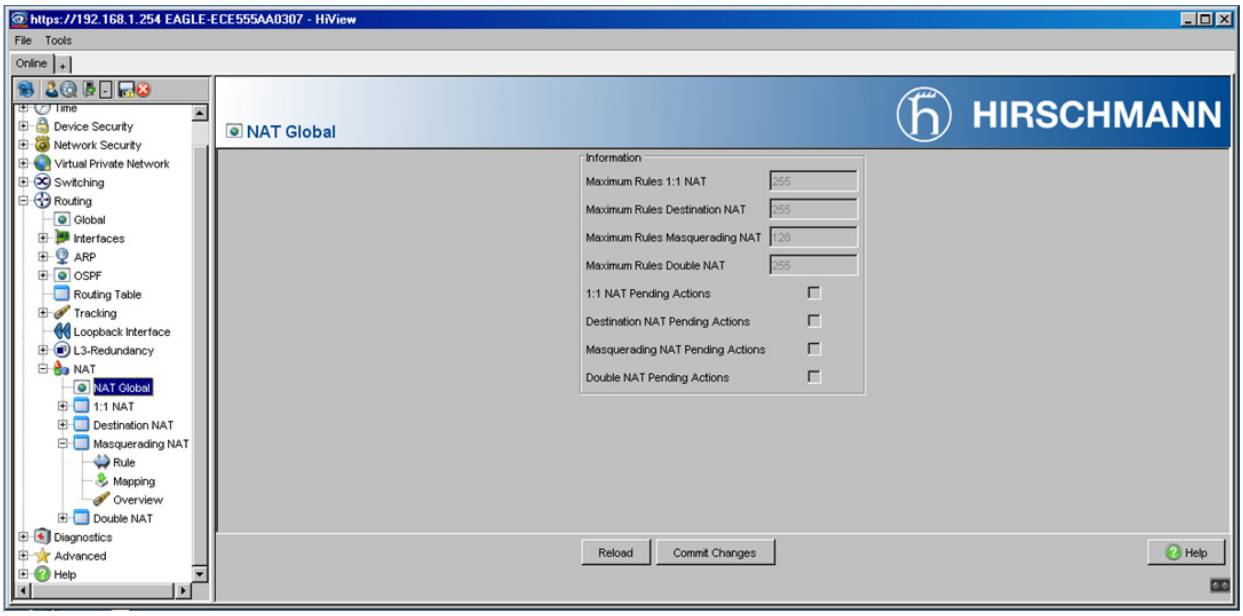
8. Select **Port 1/4**, set the **Direction** to **egress**, select the rule name that you defined above, and then click the **OK** button.

9. Make the rule **Active** and then click the **Set** button.



10. Navigate to the **Routing** / **NAT**/**Masquerading NAT** / **Global** page of the menu.

11. Click the **Commit Changes** button, and then the **Reload** button**.**



12. Ensure that there are no pending actions shown on this page.

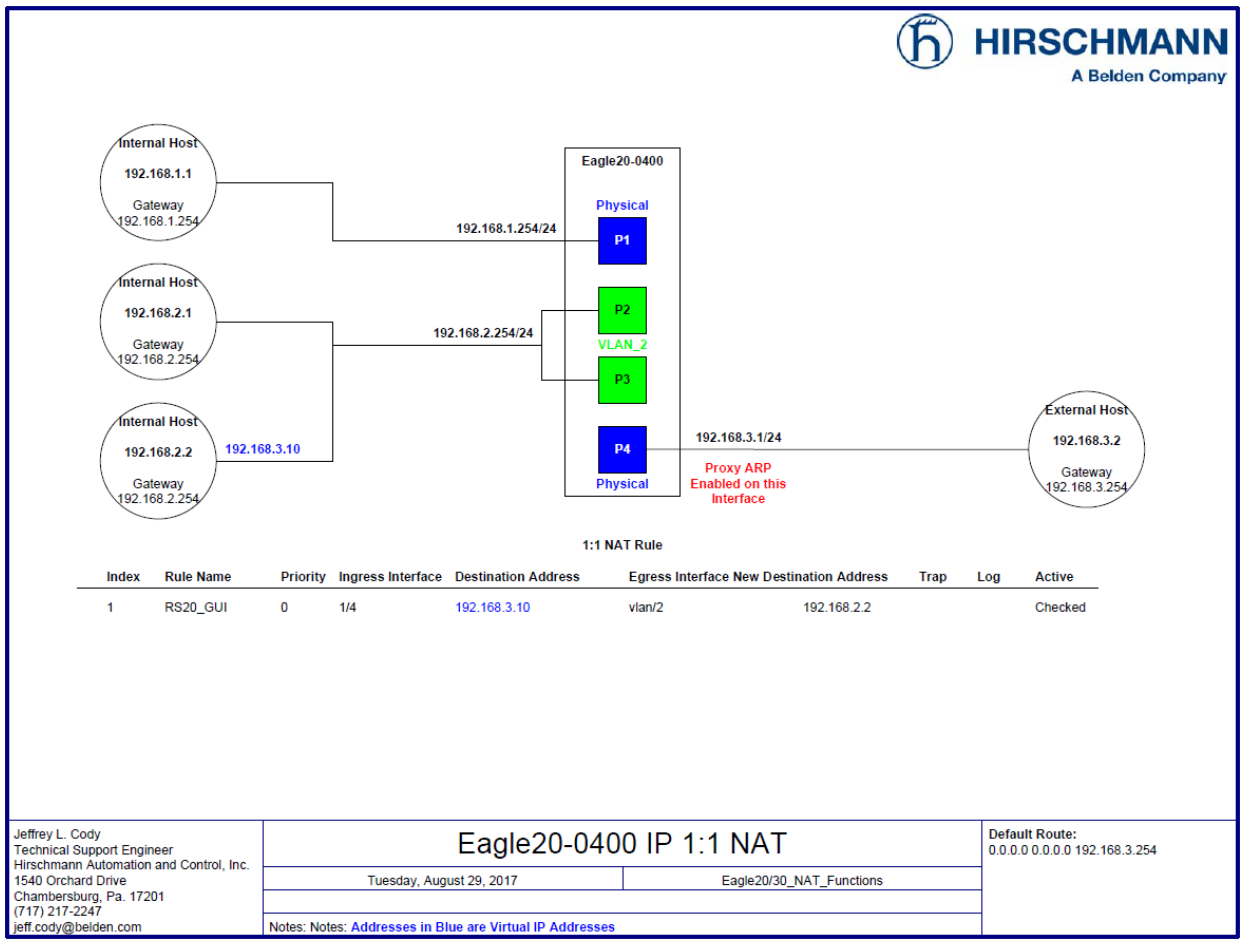
1:1 NAT

Using 1:1 NAT, you can configure the firewall so that a host on the internal network is accessible to hosts on the external network using a virtual IP Address assigned to the internal host when IP Masquerading is also configured on the firewall.

The external interface of the firewall will reply to ARP requests for any virtually assigned IP Address, and, if the traffic is permitted by a firewall rule, will be delivered to the host in the internal network. From the point of view on the external host, it appears as if it is communicating with a host on the external side of the firewall.

You can also use 1:1 NAT when you are setting up identical production cells with the same internal IP addressing schemes and want to connect them with the same common external network.

Sample Network



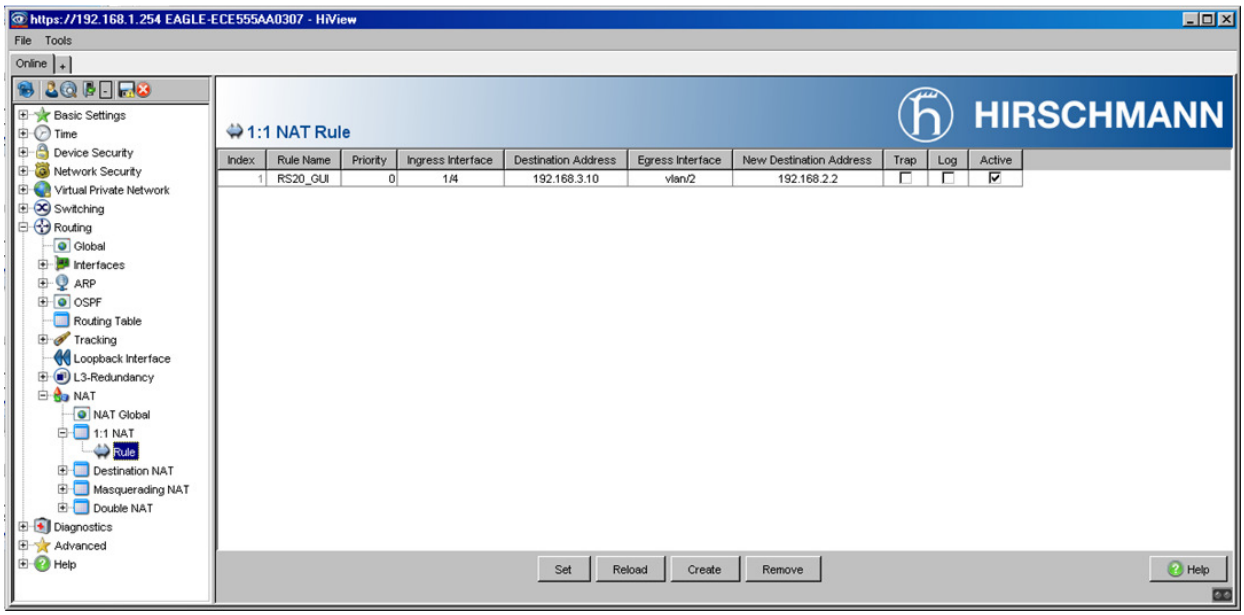
This sample networks depicts hosts on separate IP networks separated by an Eagle20/30 Firewall with IP Masquerading and 1:1 NAT configured. Host 192.168.2.2 can be reached on the external network using a virtual **192.168.3.10** IP Address.

Pre-Requisites:

1. The Eagle20/30 Firewall must be configured to operate in **Router Mode**.
2. The internal and external networks must use unique IP Addressing schemes.
3. **Proxy ARP** must be enabled on the port(s) that are to be treated as an external port.
4. The Eagle20/30 must be configured with **IP Masquerading**.
5. The hosts residing on the internal network must have the IP Address of the Eagle20/30's internal interface defined as their Default Gateway address.
6. The external virtual IP Address assigned must be unique and may not be already in use.

Configuration Steps:

1. Using the Eagle20/30's web interface (GUI), navigate to the **Routing** \ **NAT** \ **1:1 NAT** \ **Rule** page of the menu.
2. Click the **Create** button at the bottom of the page.
3. Enter a descriptive name for the rule in the **Rule Name** field.
4. Select the **ingress interface** for the **external** network. In this example, we will use **1/4**.
5. Enter the **external virtual IP Address** for the host on the internal network in the **Destination Address** field. In this example, we will use **192.168.3.10**.
6. Select the **egress interface** for the **internal network** where the desired host resides. In this example, we will use **vlan/2**.
7. Enter the **internal real IP Address** for the host on the internal network in the **New Destination Address** field. In this example, we will use **192.168.2.2**.
8. Click the **Set and Back** button at the bottom of the page.
9. Make the rule **Active** and then click the **Set** button.



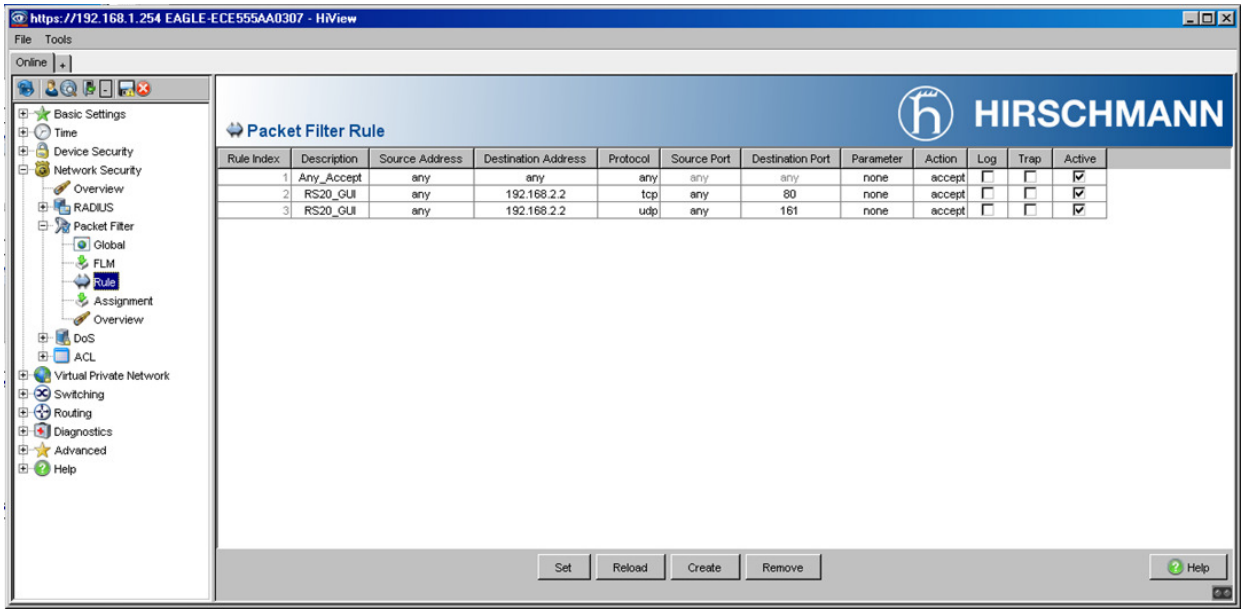
10. Navigate to the **Routing** \ **NAT** \ **NAT Global** page of the menu.

11. Click the **Commit Changes** button, and then click the **Reload** button.

12. Ensure that there are no pending actions shown on this page.

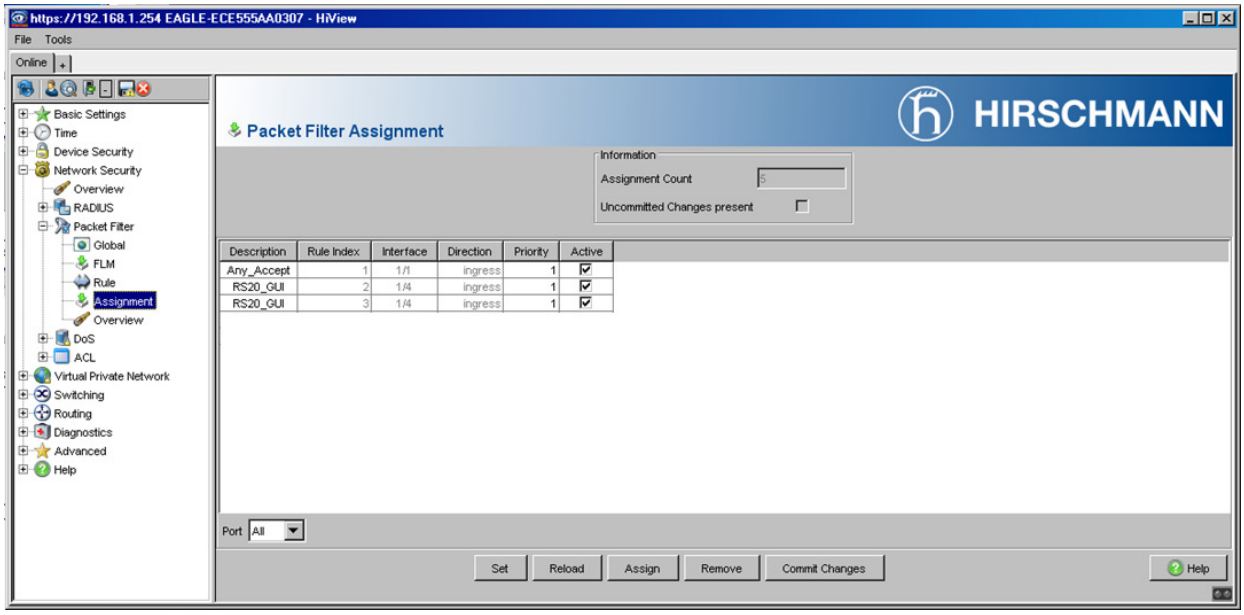
13. Navigate to the **Network Security** \ **Packet Filter** \ **Rule** page of the menu.

14. Create the Packet Filter rules that will enable incoming **HTTP & SNMP** traffic to the internal host using its real IP Address. In this case we will use **TCP Port 80 & UDP Port 161** going to the host at **192.168.2.2**.



15. Navigate to the **Network Security** \ **Packet Filter** \ **Assignment** page of the menu.

16. Click the **Assign** button.
17. Select the **external interface**. In this example, we will use interface **1/4**.
18. Select **ingress** in the **Direction** drop down box.
19. Select the **Packet Filter Rule Index** for the rule that you created above. In this example we will use **index 2**.
20. Click the **Set** button.
21. Repeat steps 16 through 20 selecting rule **index 3**, and then click the **OK** button.



22. Click the **Commit Changes** button.
23. Navigate to the **Network Security** \ **Packet Filter** \ **Global** page of the menu.
24. Click the **Reload** button.
25. Ensure that there are no **Uncommitted Changes Present** on this page.

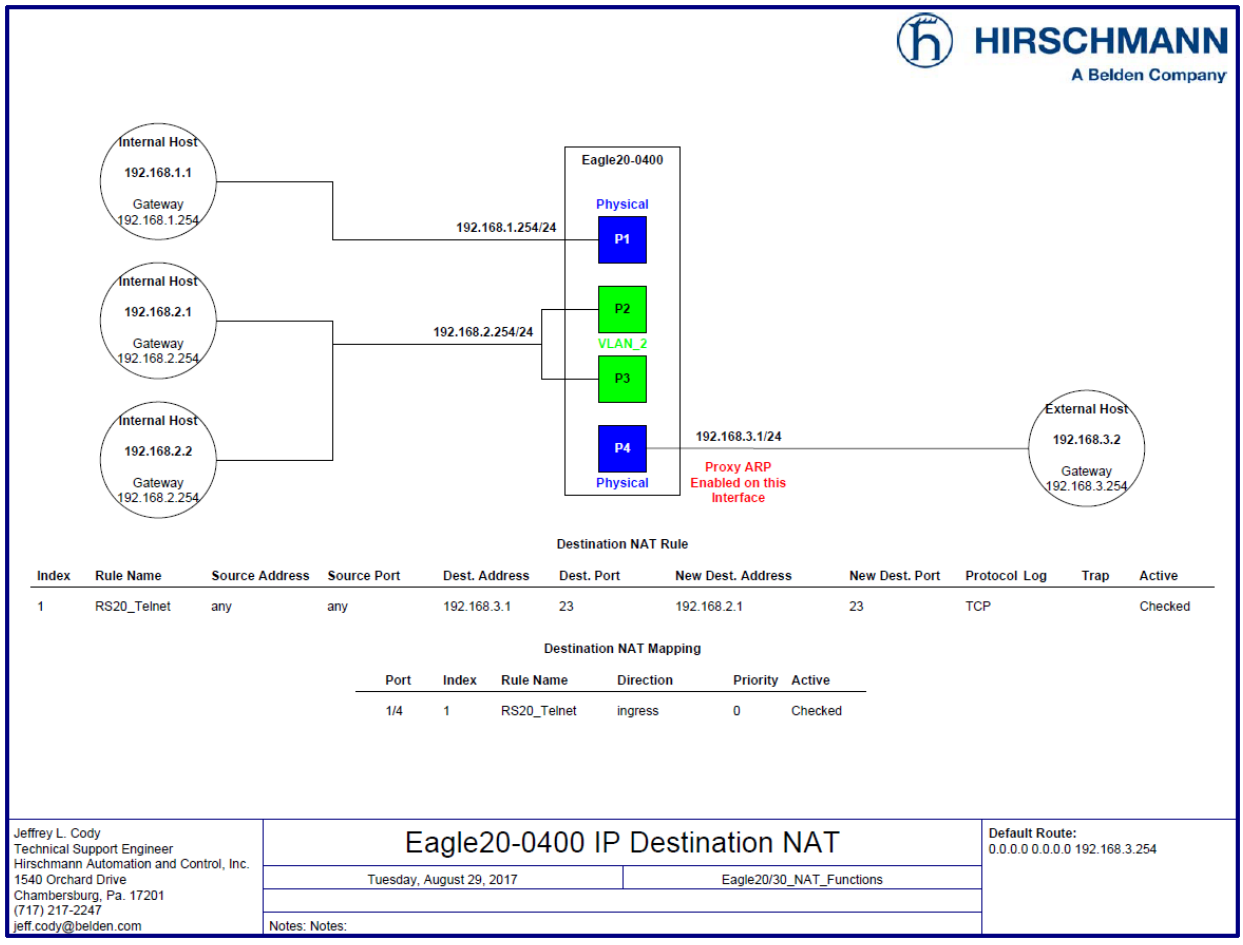
Destination NAT

Destination Network Address Translation (DNAT) is a technique for transparently changing the destination IP Address of an IP packet and performing the inverse function for any replies.

DNAT is commonly used to publish a service located in a private network on a publicly accessible IP Address. This use of DNAT is also called Port Forwarding.

The external interface of the firewall will forward the traffic sent to its IP Address for a specified port to the internal host's IP Address and specific port number. From the point of view on the external host, it appears as if it is communicating with the firewall's IP Address and specific port number.

Sample Network



This sample networks depicts two hosts on separate IP networks separated by an Eagle20/30 Firewall with IP Masquerading and Destination NAT configured.

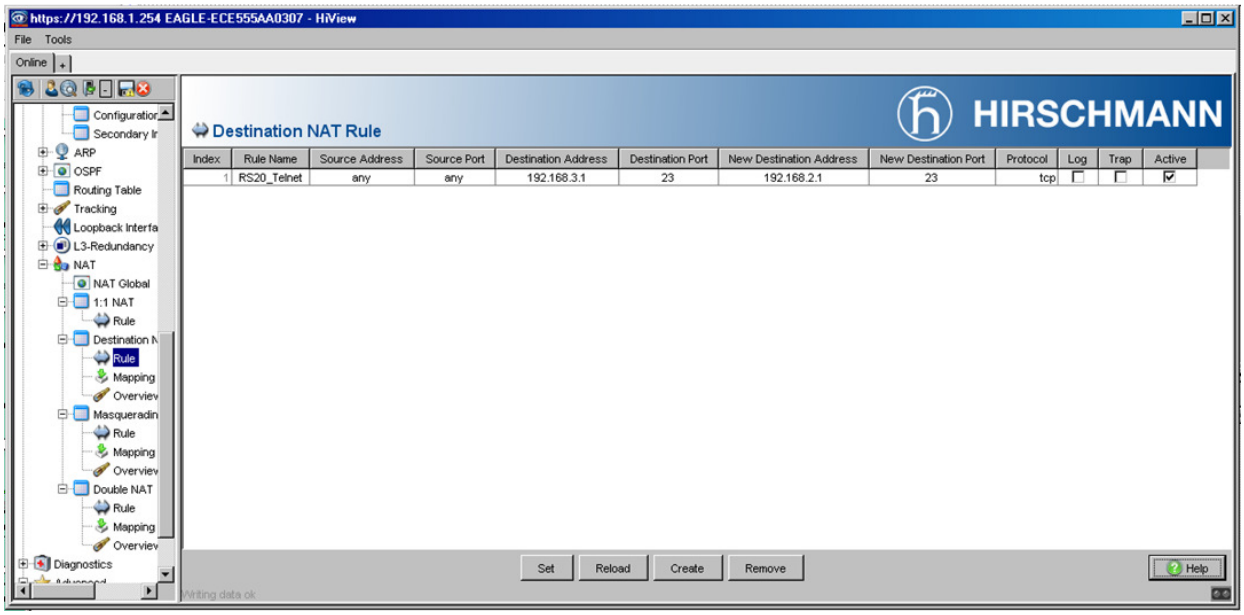
Telnet traffic sent to the external interface at 192.168.3.1 will be redirected to the internal host at 192.168.2.1 using TCP Port 23 as the destination port.

Pre-Requisites:

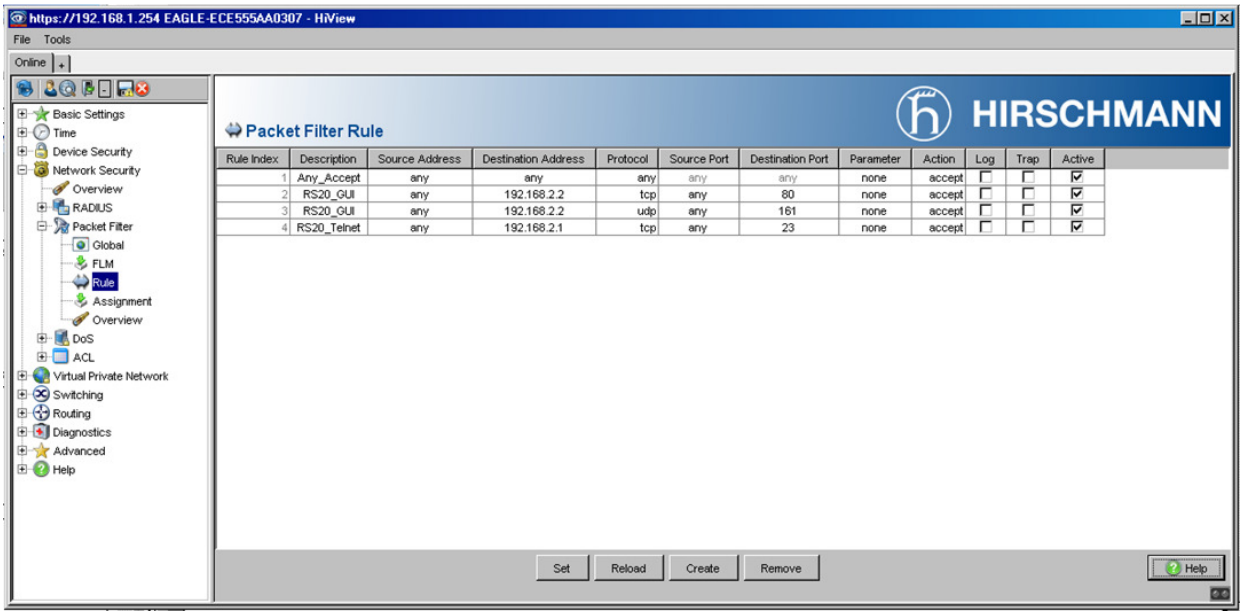
1. The Eagle20/30 Firewall must be configured to operate in **Router Mode**.
2. The internal and external networks must use unique IP Addressing schemes.
3. **Proxy ARP** must be enabled on the port(s) that are to be treated as an external port.
4. The Eagle20/30 must be configured with **IP Masquerading**.
5. The hosts residing on the internal network must have the IP Address of the Eagle20/30's internal interface defined as their Default Gateway address.

Configuration Steps:

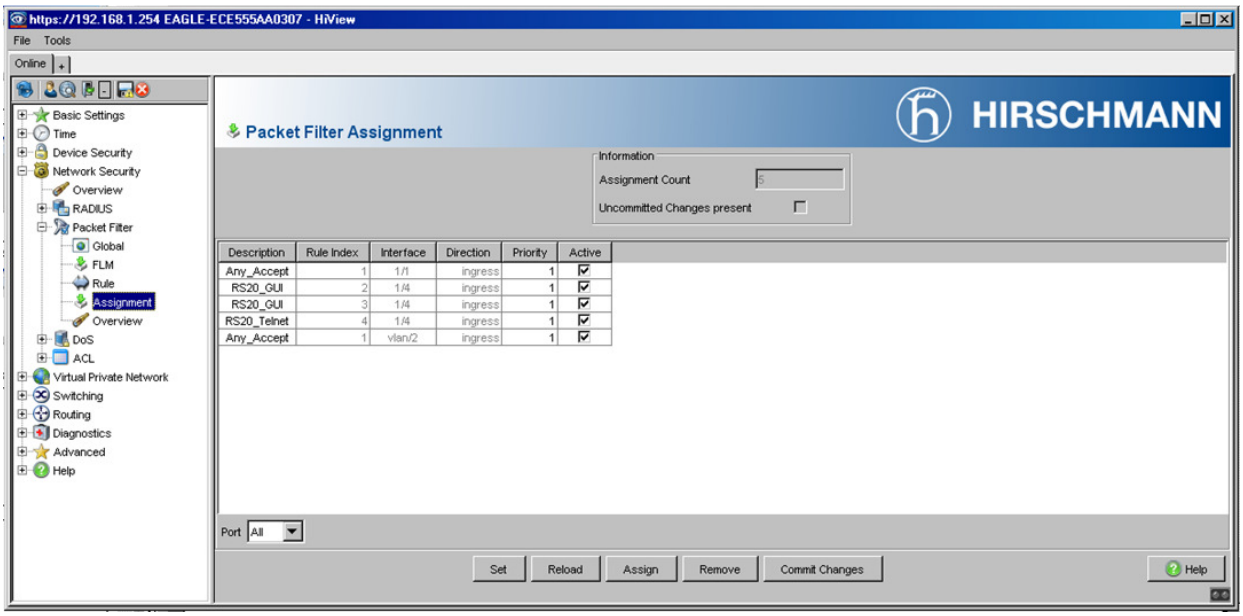
1. Using the Eagle20/30's web interface (GUI), navigate to the **Network Security** \ **NAT** \ **Destination NAT** \ **Rule** page of the menu.
2. Click the **Create** button at the bottom of the page.
3. Enter a rule name and define the **Destination Address** as the Eagle20/30's **external interface**. In this case we will use **192.168.3.1**.
4. Define **the Destination Port** for the application that you will forward to an internal host. In this case, we will use **TCP Port 23** for the Telnet protocol.
5. Define the **New Destination Address** as the IP Address of the **internal host** that you will forward this traffic to. In this case, we will use **192.168.2.1.**
6. Define the **New Destination Port** as **23**.
7. Define the **Protocol** as **TCP**.
8. Make the rule **Active** and click the **Set** button.



9. Navigate to the **Routing** / **NAT** / **Destination NAT** / **Mapping** page of the menu.
10. Click the **Assign** button.
11. Select **Port 1/4** for the **Port**.
12. Set the **Direction** to **ingress**.
13. Select **Rule Index 1**.
14. Make the rule **Active** and then click the **Set** button.
15. Navigate to the **Routing** \ **NAT** \ **NAT Global** page of the menu.
16. Click the **Commit Changes** button, and then click the **Reload** button.
17. Navigate to the **Network Security** \ **Packet Filter** \ **Rule** page of the menu.
18. Create the Packet Filter rules that will **enable incoming Telnet traffic** to the **internal host** at **192.168.2.1**. In this case we will use **TCP Port 23** for the Telnet protocol.
19. Make the rule **Active** and click the **Set** button.



20. Navigate to the **Network Security** \ **Packet Filter** \ **Assignment** page of the menu.
21. Click the **Assign** button.
22. Select the **external interface**. In this example, we will use interface **1/4**.
23. Select **ingress** in the **Direction** drop down box.
24. Select the **Packet Filter Rule Index** for the rule that you created above. In this example we will use **index 4**.
25. Click the **Set** button.
26. Click the **Commit Changes** button.
27. Click the **Reload** button and make sure that there are no **Uncommitted Changes Present**.

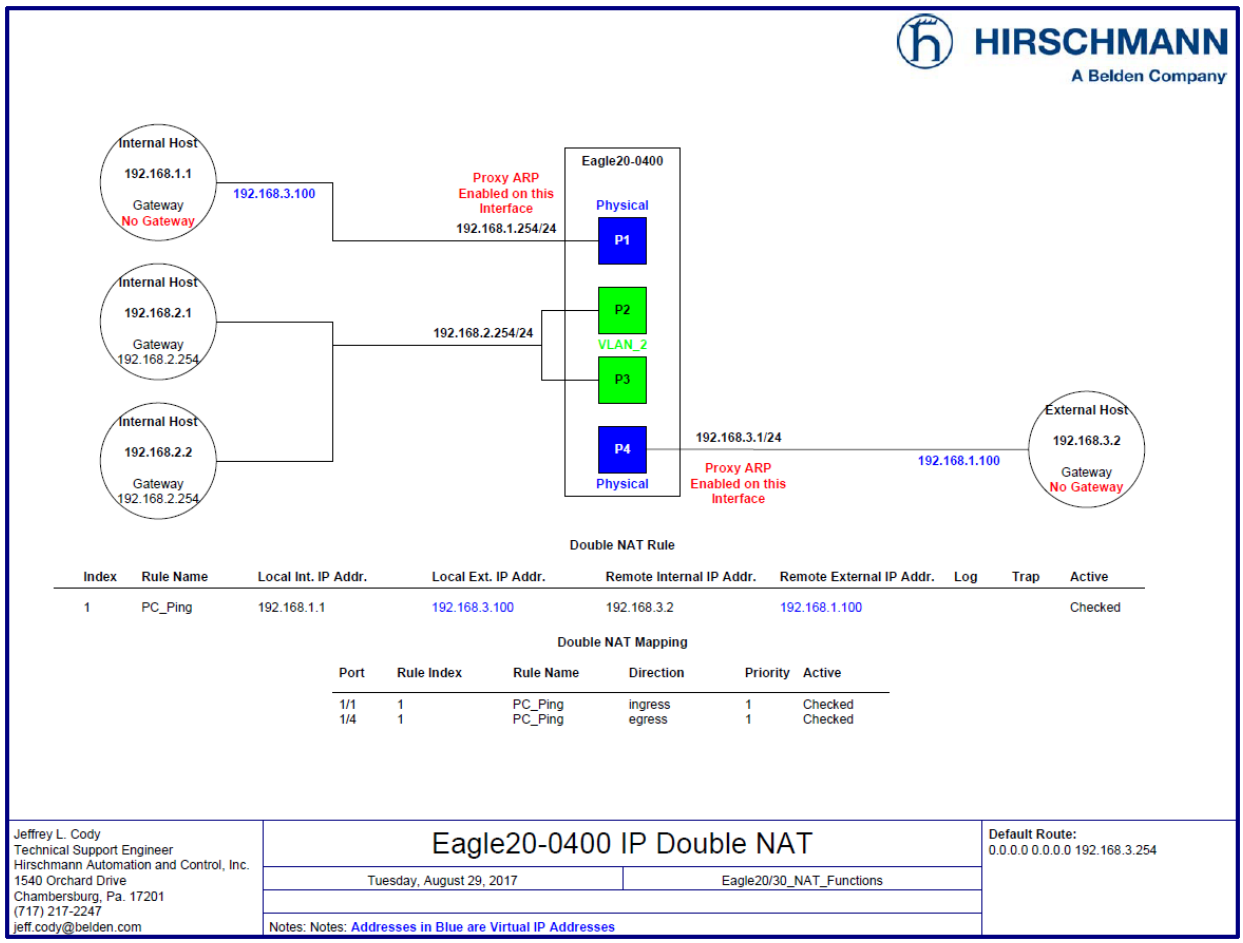


Double NAT

The Double NAT process enables communication between non-CIDR-compatible devices located in different networks. These devices have no way to specify a default gateway or default route. The NAT router virtually “shifts” the devices into the other network. To do this, the NAT router replaces the source address and the destination address in the data packet during sending. A typical application is the linking of controllers located in different networks.

Double NAT is helpful if the hosts on the internal and external networks cannot have a default gateway defined. The internal and external interfaces of the firewall will reply to ARP requests for the virtually assigned IP Addresses, and, if the traffic is permitted by a firewall rule, will be delivered to the hosts in the internal or external networks. From the point of view of the hosts, it appears as if they are communicating with a host on the same local IP network.

Sample Network



This sample networks depicts two hosts on separate IP networks separated by an Eagle20/30 Firewall with IP Masquerading and Double NAT configured.

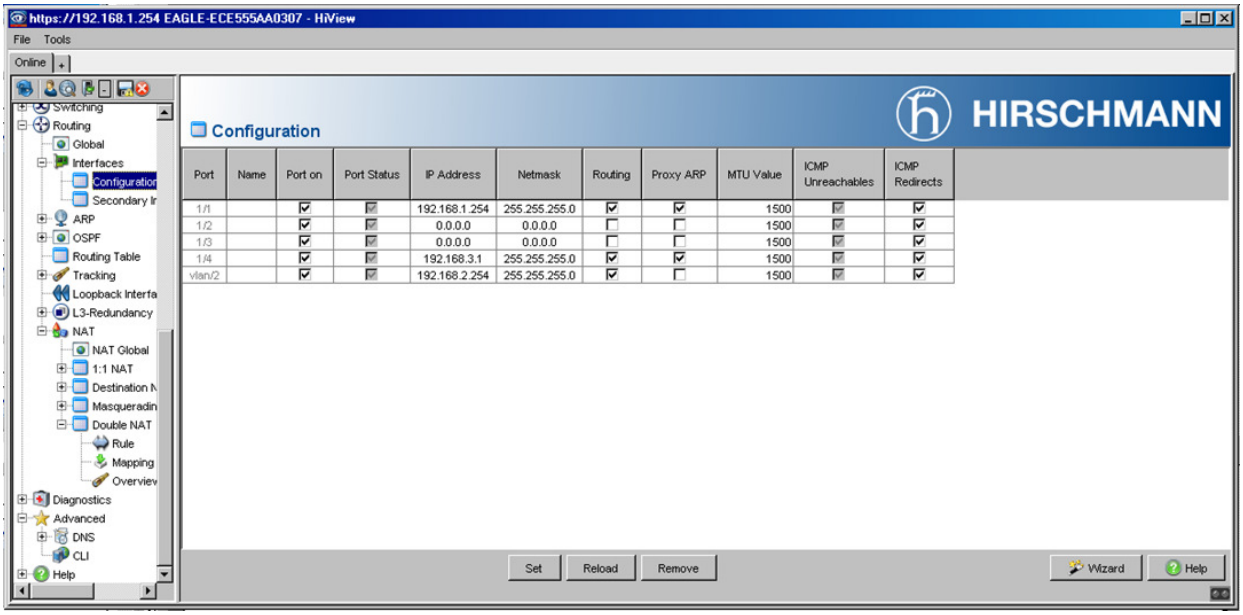
The two hosts (192.168.1.1 & 192.168.3.2) do not have any default gateways defined. By pining the other host’s virtual ip address, communications between the two hosts can be established.

Pre-Requisites:

1. The Eagle20/30 Firewall must be configured to operate in **Router Mode**.
2. The internal and external networks must use unique IP Addressing schemes.
3. **Proxy ARP** must be enabled on the port that is to be treated as an external port and also on the internal interface where the internal host with no default gateway defined is connected to.
4. The Eagle20/30 must be configured with **IP Masquerading**.

Configuration Steps:

1. Using the Eagle20/30's web interface (GUI), navigate to the **Routing** \ **Interfaces** \ **Configuration** page of the menu.
2. Enable **Proxy ARP** on the internal interface **Port 1/1**.
3. Click the **Set** button.



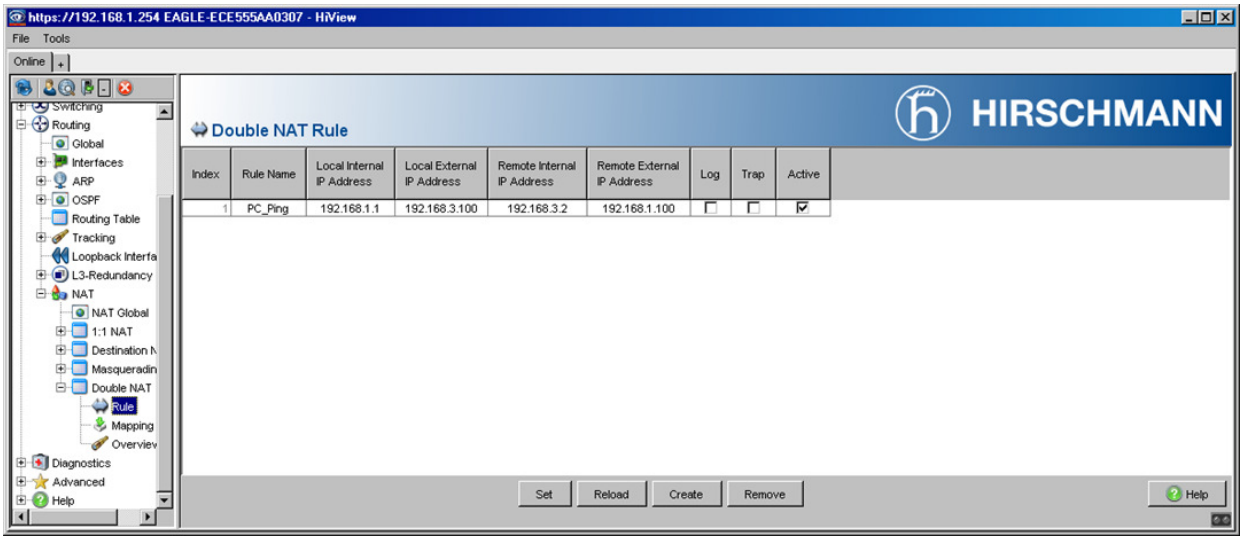
4. Navigate to the **Routing** \ **NAT** \ **Double NAT** \ **Rule** page of the menu.
5. Click the **Create** button.
6. Define a name for the rule.
7. Enter the IP Address of the **internal host** in the **Local IP Address** field. In this case, we will use 192.168.1.1.
8. Define a virtual IP Address for the **internal host** on the **external network**. In this case we will use **192.168.3.100**. This address must not be already in use on the external network.

9. Enter the IP Address for the **external host** in **the Remote Internal IP Address** field. In this case, we will use **192.168.3.2**.

10. Define a virtual IP Address for the **external host** on **the internal network**. In this case, we will user **192.168.1.100**. This address must not be already in use on the internal network.

11. Click the **Set and Back** button.

12. Make the rule **Active** and click the **Set** button.



13. Navigate to the **Routing** \ **NAT** \ **Double NAT** \ **Mapping** page of the menu.

14. Click the **Assign** button.

15. Select **Port 1/1**, select **ingress** for the **Direction**, and **Rule Index 1**, and then click the **OK** button.

16. Click the **Assign** button.

17. Select **Port 1/4**, select **egress** for the **Direction**, and **Rule Index 1**, and then click the **OK** button.

18. Make both rules **Active** and then click the **Set** button.

19. Navigate to the **Routing** \ **NAT** \ **NAT Global** page of the menu.

20. Click the **Commit Changes** button, and then click the **Reload** button.

21. Navigate to the **Network Security** \ **Packet Filter** \ **Rule** page of the menu.

22. Create the Packet Filter rules that will enable **incoming ICMP traffic** to the **internal host** at **192.168.1.1**.

23. Make the rule **Active** and click the **Set** button.

24. Navigate to the **Network Security** \ **Packet Filter** \ **Assignment** page of the menu.

25. Click the **Assign** button.
26. Select the **external interface**. In this example, we will use interface **1/4**.
27. Select **ingress** in the **Direction** drop down box.
28. Select the **Packet Filter Rule Index** for the rule that you created above. In this example we will use **index 5**.
29. Click the **Set** button.
30. Click the **Commit Changes** button.
31. Click the **Reload** button and make sure that there are no **Uncommitted Changes Present**.