

Network Address Translation NAT

<https://campus.barracuda.com/doc/19333760/>

Network Address Translation (NAT) maps private IP addresses to public IP addresses.

NAT allows you to:

- Conceal the private IP address from exposure on the public Internet.
- Reduce the demand for public IPv4 addresses. Private networks can use the private IPv4 address space and therefore are not in contention for public IPv4 addresses (which are no longer readily available).
- Direct external Internet traffic to the appropriate private IP address.

Source Network Address Translation (SNAT)

Source Network Address Translation (SNAT) maps private IP addresses to a public IP address. SNAT re-writes the IP address of the computer that originated the packet. SNAT is composed of two steps:

1. Translating a private IP address into a public IP address.
2. For returning traffic, rewriting the IP address of the computer that originated the packet.

On the **NETWORK > NAT** page, you can define a SNAT rule to allow the Real Servers to forward traffic to the Internet if they are located on a private network and the WAN is on a public network.

Create a Source NAT Rule

Use the following steps to create a source NAT rule:

1. Log into the Barracuda Load Balancer ADC as administrator and navigate to the **NETWORK > NAT** page.
2. In the **Add NAT Rule** section, enter values for the following:
 - **Pre-SNAT Source** - Enter the private IP address or source network that is to be translated.
 - **Pre-SNAT Source Mask** - Enter the subnet for the entered network; you can use a 32-bit netmask if required for a single IP NAT.
 - **Protocol** - Select the traffic to be used for the networks:
 - **TCP**
 - **UDP**
 - **Any**

- **Destination Port** - Enter the destination port. You can either specify an individual port number (for example, 80) or range of port numbers (for example, 100-200). The default value of 1 - 65,535 allows traffic from all ports.
- **Post SNAT Source** - Depending on your network configuration, this may be a public IP address or some other IP address on the WAN side of the Barracuda Load Balancer ADC that is translated by your firewall into a public IP address.
- **Outgoing Interface** - Select the outgoing network interface for traffic to pass through to the Internet.

3. Click **Save** to save the NAT rule.

When setting up [High Availability](#) (HA) between two Barracuda Load Balancer ADCs, you can create a custom virtual interface that associates a public IP address with the WAN port, and then use this IP address to create an SNAT rule. This interface is used by the backup system if failover occurs. For more information, log into the web interface, go to **ADVANCED > High Availability** and click the **Help** button.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.