Grandstream Networks, Inc.

GCC6000 Series -

Advanced NAT Guide

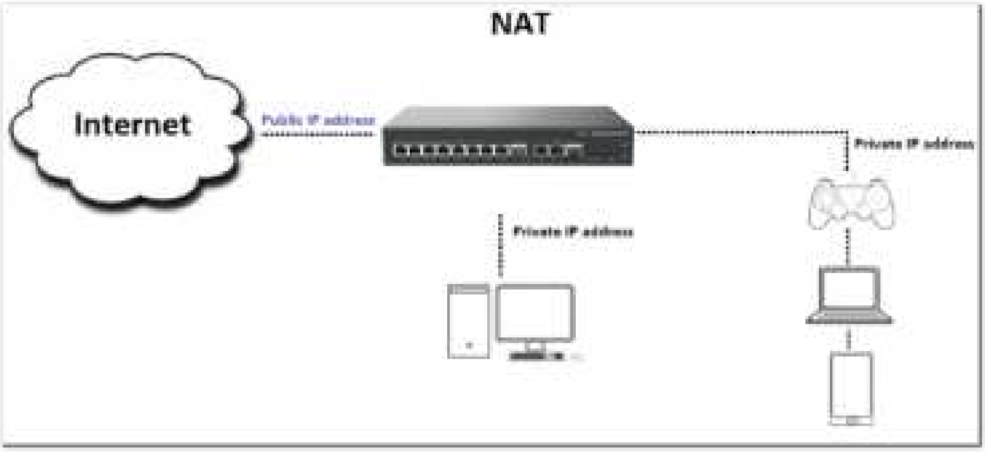
GCC6000 Series - Advanced NAT Guide

Introduction

NAT (Network Address Translation) is the process used by a router or similar device to translate one IP address into another. This translation is done from a private IP address to a public IP address and vice versa. In this guide, we will configure advanced NAT settings to control the NAT process for source and destination traffic. We will distinguish between two types of NAT: SNAT and DNAT. These processes allow us to alter the source and destination IP and port numbers, enabling users to access the internet.

- **SNAT:** Source NAT controls the change of the source IP address and layer 4 port number when connecting from an internal private host to an external host (LAN to internet).
- **DNAT:** Destination NAT controls the change of the destination IP address and Layer 4 port number when receiving traffic from an external host to a private host (internet to LAN).

Both variants work very much alike but generally differ in the way that a connection is established.

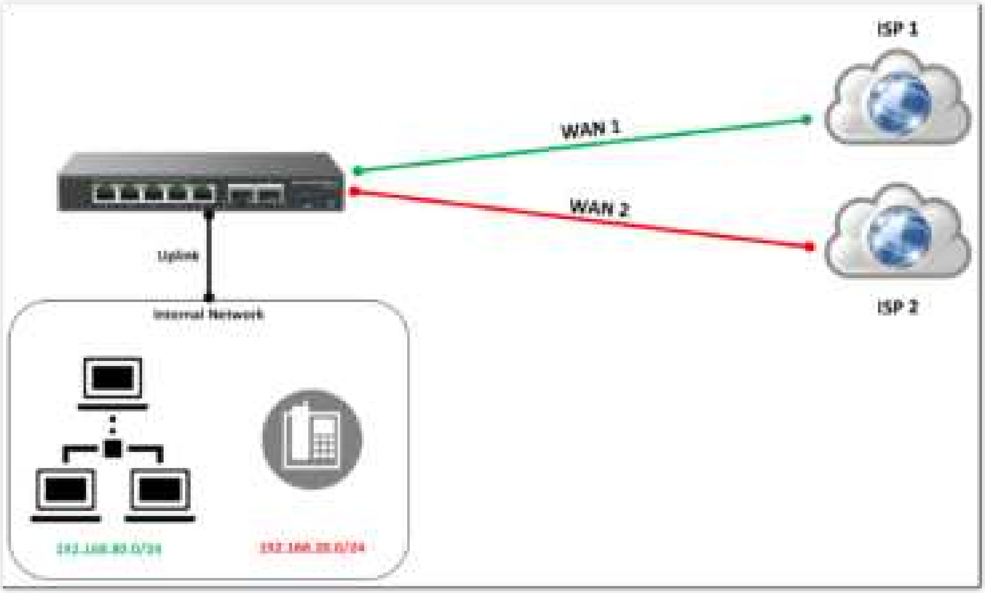


NAT for GCC device

In this guide we will walk through configuring both DNAT and SNAT on the GCC601x(W) convergence device.

SNAT Configuration

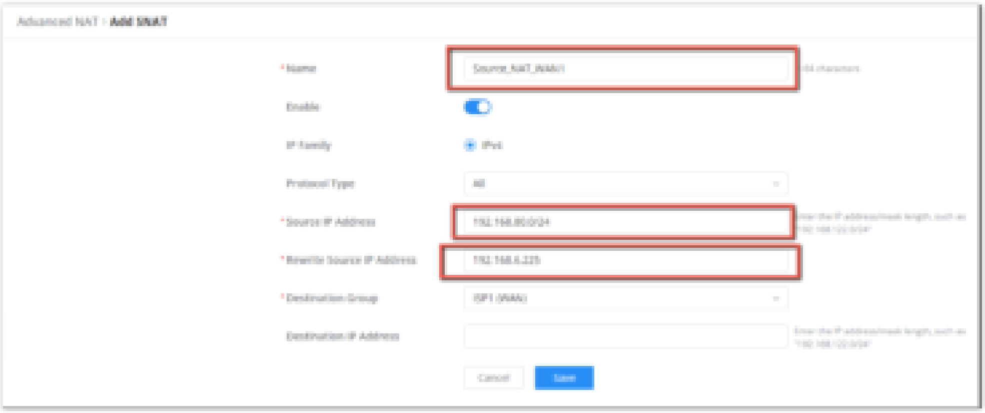
We will consider the following scenario: imagine the GCC device is connected to two different internet service providers to create link redundancy and a failover solution. Each WAN port is connected to a different ISP. Now, suppose we want to force traffic initiated from the default VLAN to use port 1 (ISP 1) and traffic from the voice VLAN (VLAN 20) to use port 2 (ISP 2). This can be achieved by creating a source NAT rule.



Please follow the steps below:

Configuring WAN 1

1. Navigate to "**Firewall Module → Firewall Policy → Advanced NAT → SNAT**", then click on "**Add**" button to add a new SNAT.
2. Enable the status
3. Set the protocol to "Any", this means that the source NAT rule will apply on all traffic coming from different transport protocols (UDP, TCP,..)
4. Set the Source IP address network, this will be the LAN subnet of the default VLAN: **192.168.80.0/24**
5. Set the Rewrite Source IP address, this will be the Public IP address provided by ISP 1, that we will use to reach internet, this will be : **192.168.6.225**
6. Under destination group, select the destination group where the rewrite source IP address belongs to. in our case, it is **WAN 1** port using ISP 1.



Advanced NAT > **Add SNAT**

* Name	Source_NAT_WAN1
Enable	●
IP Family	● IPv4
Protocol Type	All
* Source IP Address	192.168.80.0/24
* Rewrite Source IP Address	192.168.6.225
* Destination Group	ISP1 (WAN)
Destination IP Address	

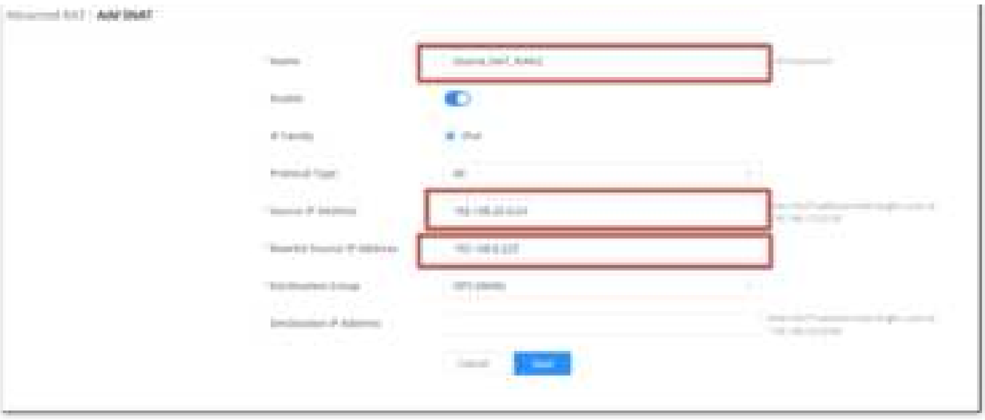
SNAT Rule

Note

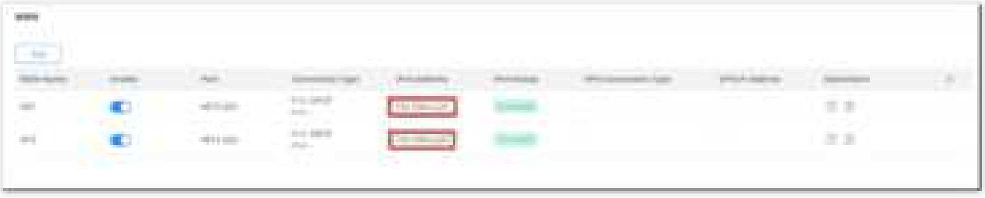
The destination IP Address can be used to specify the exact device where the traffic will be routed to internally

Configuring WAN 2

1. Navigate to "**Firewall Module → Firewall Policy → Advanced NAT → SNAT**", then click on "**Add**" button to add a new SNAT.
2. Enable the status
3. Set the protocol to "Any", this means that the source NAT rule will apply on all traffic coming from different transport protocols (UDP, TCP,..)
4. Set the Source IP address network, this will be the LAN subnet of the Voice VLAN: **192.168.20.0/24**
5. Set the Rewrite Source IP address, this will be the Public IP address provided by ISP 2, that we will use to reach internet. this will be **192.168.6.229**
6. Under destination group, select the destination group where the rewrite source IP address belongs to. in our case, it is **WAN 2** port using ISP 2.

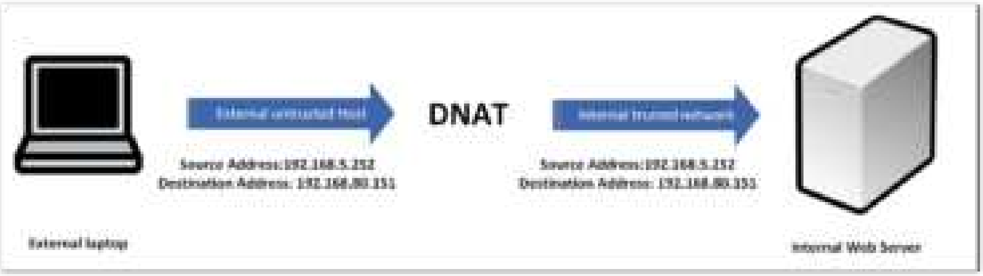


The Public IP addresses of both WANs can be found on the network module of the GCC device , under the path **Network Settings => WAN**:



DNAT configuration

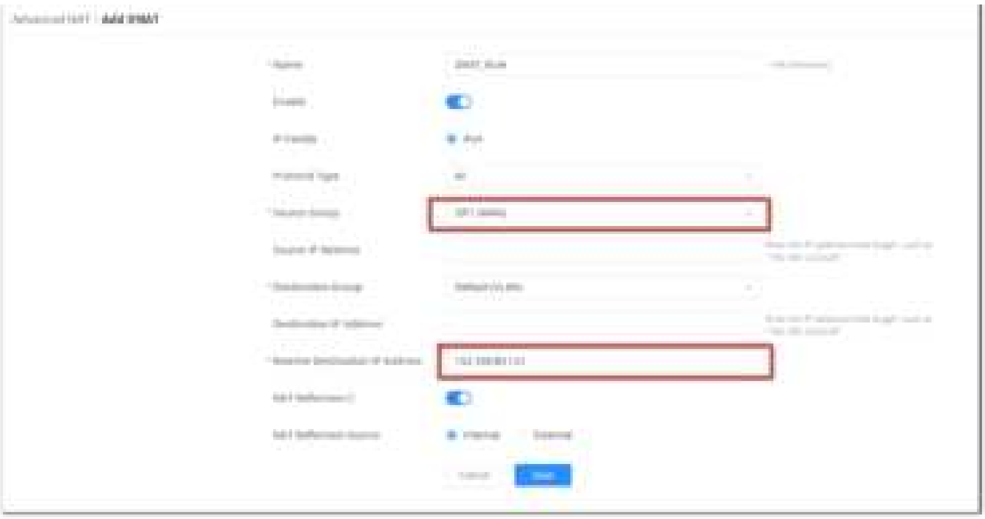
DNAT can be very similar to configuring port forwarding, the only difference, is that in DNAT, you are not obligated to specify the port to forward to, it is more of doing IP forwarding, from the internet, to the LAN, we will look at this example below to clarify:


External untrusted Host
Source Address:192.168.5.252
Destination Address: 192.168.80.151
DNAT
Internal trusted network
Source Address:192.168.5.252
Destination Address: 192.168.80.151
External laptop
Internal Web Server

Destination NAT

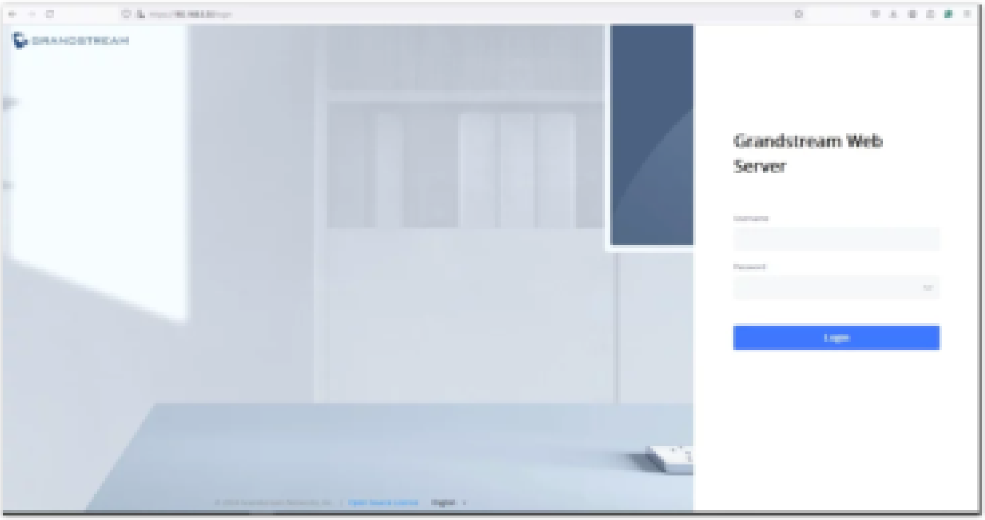
Consider that we want to make our local web server deployed in our LAN, available to our clients from outside the LAN, but we don't want them to know the private IP address of our local web server, instead, we want them to use a public IP address to access the web server, we can reach that using DNAT, and by following the below steps:

1. Navigate to "**Firewall Module → Firewall Policy → Advanced NAT → DNAT**", then click on "**Add**" button to add a new DNAT.
2. Enable the DNAT rule
3. Set the protocol type to "Any", this will include any type of traffic transport protocol coming to our LAN.
4. Set the Source group to WAN1, this is our default WAN
5. the destination group will be the default VLAN where the local Web server is connected
6. the Rewrite destination IP Address will be the private IP address of the web server.



DNAT Rule

The results will be, that when users want to access our local web server, they can use the defined public IP address, without them knowing our server private IP address.



Grandstream Web Server

Grandstream Web Server

NAT Reflection

NAT reflection, also known as NAT loopback, allows internal network clients to access services that are hosted on the same local network but addressed by the public IP.

In our configuration, we're using DNAT (Destination NAT) to allow clients from outside your LAN to access a local web server by mapping a public IP to a private one. NAT reflection comes into play when **internal devices** on the same LAN (like your IP phones or scanning tools) also need to access this web server, but you want them to use the same **public IP address** that external users use.

This is how it works :

- **Without NAT reflection**: If your internal devices (e.g., phones) try to access the web server using its public IP, the request would normally go out to the internet and back to the LAN, which can fail or slow things down if other firewall rules are applied.
- **With NAT reflection**: The router detects that the request is from the LAN but is addressed to the public IP. Instead of routing the traffic outside, it reflects the traffic internally, making the connection faster and bypasses external firewalls. The web server still sees the traffic as coming from the LAN, even though it was addressed to the public IP.

Supported Devices

Device Model	Firmware Required

GCC6010W	1.0.1.7+
GCC6010	1.0.1.7+
GCC6011	1.0.1.7+