Configuring the SBC Edge for NAT Traversal

This Best Practice describes how NAT Traversal is enabled and configured within the SBC Edge, including guidelines for usage.

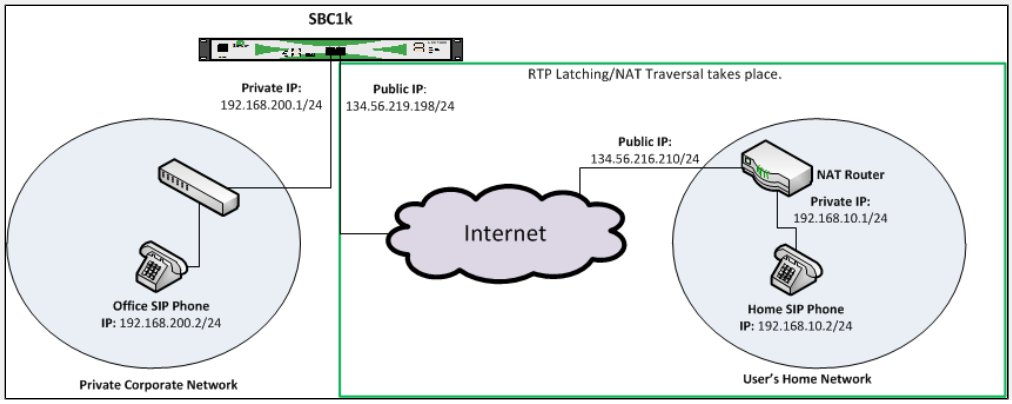
Overview - What is NAT Traversal?

NAT Traversal (also known as RTP Latching) allows the SBC Edgeto register and communicate with SIP endpoints that are behind NAT routers. The most common example of using NAT Traversal is a SIP phone or soft-client behind a home gateway, communicating with an SBC on the public internet. The SIP Phone behind the NAT could not properly communicate with the SBC Edge, as the client used its local private address in SIP, but the SBC could not directly reach this address. NAT Traversal gives the SBC the ability to communicate with SIP endpoints behind NATs, regardless of the client's address.

Typical Network Layout

In a typical network layout (see below), an SBC 1000 has both a public interface connected to the internet, and a private interface connected to the corporate network. A user's home network is also attached to the network with a NAT router and a SIP phone behind it. In this example, SIP requests arrive at the SBC from the Home SIP Phone wih the SIP Phone's private IP address (i.e., 192.168.10.2). With Inbound NAT Traversal enabled, the SBC 1000 can detect the public IP address (i.e. 134.56.216.210). Once this detection is made, all communication to this endpoint is sent to the public IP, rather than the private IP from the Home SIP Phone.

Figure 1: Typical Network Example



Configure an SBC Edge in a NAT Traversal Environment

These instructions assume you are logged into the SBC Edge WebUI.

Step 1: Create NAT Qualified Prefix Table

1. In the left navigation pane, go to **SIP > NAT Qualified Prefix Tables.**

2. Click the **Create NAT Qualified Prefix Table** Entry (

) icon at the top of the **SIP NAT Qualified Prefix Tables** page.

3. In the **Description** field, enter a description for the table (i.e., **Default Private Prefixes**).

4. Click **OK**. The table is created.

5. From the left navigation pane, click on the table just created.

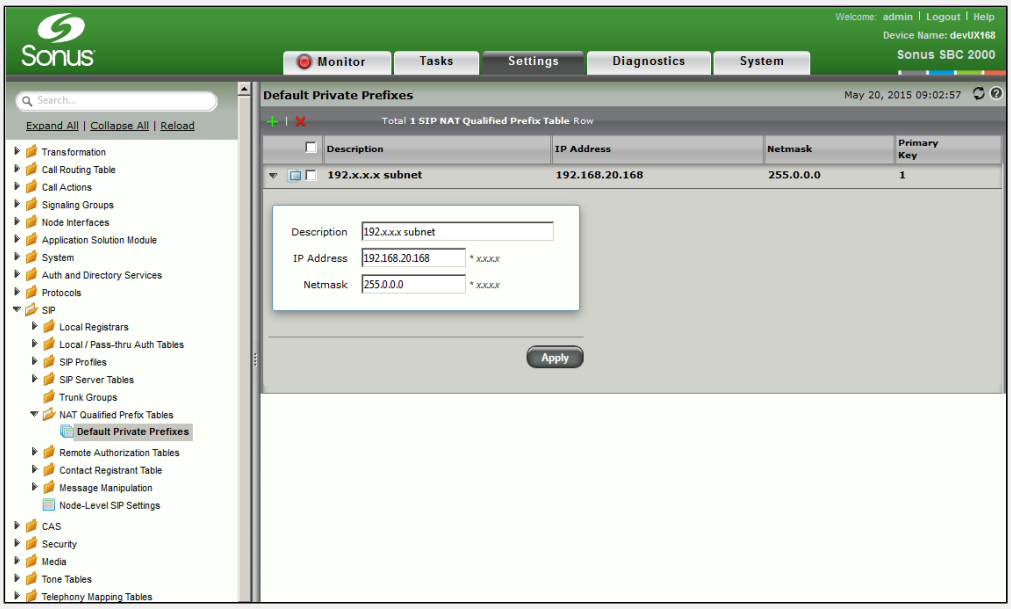
6. Click the **Create NAT Qualified Prefix Table** Entry (

) icon at the top of the table**.**

7. Configure the options. For field definitions, see **Creating and Modifying a NAT Qualified Prefix Table.**

8. Click **Apply.**

Figure 2: Create NAT Qualified Prefix Table



Step 2: Associate NAT Qualified Prefix Table to Signaling Group

⚠ A NAT Qualified Prefix Table must be created before associating it with a Signaling Group. See Step 1 .

1. Select the signaling group in which the NAT Qualified Prefix will be associated.

2. Access the **Inbound NAT Traversal** options.

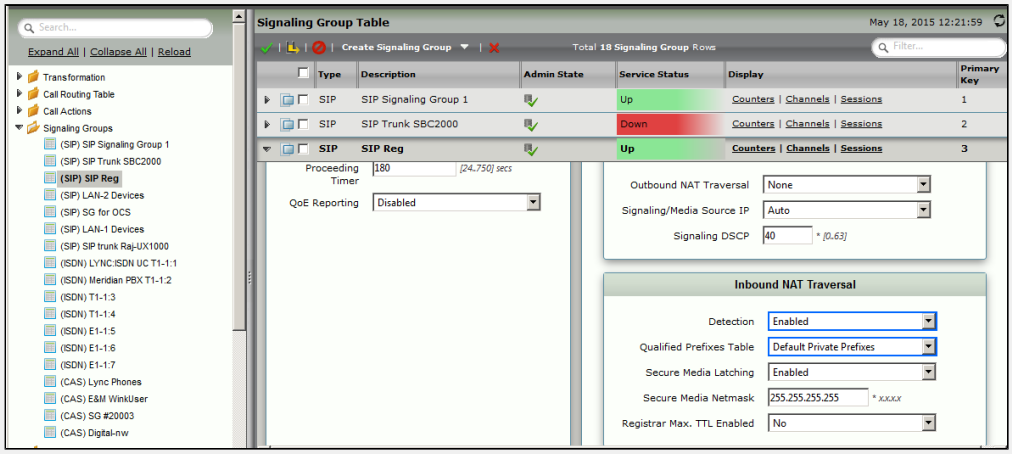
ⓘ Do not confuse the **Inbound NAT Traversal** fields with the **Outbound NAT Traversal** fields in the **SIP IP Details** section. The **Out bound NAT Traversal** fields are used when the SBC is on the private side of a NAT device.

3. From the **Detection** drop down list, select **Enable**.

4. From the **Qualified Prefixes Table** drop down list, select the applicable table you created in Step 1. When examining SIP packets, this table determines which Subnets should be treated as being behind a NAT device.

5. Configure optional fields (i.e, **Secure Media Latching**, **Secure Media Netmask** and **Registrar Max. TTL Enabled**). For field definitions, see Creating and Modifying SIP Signaling Groups.
6. Click **Apply**.

Figure 3: Associate NAT Qualified Prefix Table to Signaling Group



Guidelines/Recommendations for using NAT Traversal

The following are guidelines/recommendations for configuring and using the NAT Traversal feature.

NAT Endpoint Registrations must show in SIP Registrar User Table to be properly registered

When the Inbound NAT Traversal feature is disabled, registrations from NAT endpoints may show up in the SIP Registrar User Table, but that doesn't mean they've successfully registered. Only when the **Public Source IP** and **Public Source Port** are properly detected and displayed in the SIP Registrar User Table, does that mean that a NAT endpoint is properly registered. For details on how to view these fields, see Viewing Registered Users.

Configuration recommendation for NAT Traversal to function properly

We recommend that connecting NAT routers have SIP ALG disabled in order for NAT traversal to function properly.