Configuring the SBC Edge for NAT Traversal

In this section:
- Overview - What is NAT Traversal?
  - NAT Traversal Using the Interactive Connectivity Establishment (ICE) and ICE-Lite Protocols
  - Configure an SBC Edge in a NAT Traversal Environment
  - Step 1: Create NAT Qualified Prefix Table
  - Step 2: Associate NAT Qualified Prefix Table to Signaling Group
  - Guidelines/Recommendations for using NAT Traversal

Related articles:
- Working with the SBC Edge and SWe Lite as an ICE-Lite Agent
- Creating and Modifying a NAT Qualified Prefix Table
- Creating and Modifying SIP Signaling Groups
- Viewing Registered Users

This Best Practice describes how to enable and configure NAT Traversal within the SBC Edge, including guidelines for usage.

Overview - What is NAT Traversal?

NAT Traversal (also known as RTP Latching) allows the SBC Edge to 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. In this scenario, the SIP Phone behind the NAT cannot properly communicate with the SBC Edge because the client used a local private address in SIP; the SBC cannot directly access the private address. NAT Traversal allows the SBC to communicate with SIP endpoints behind NATs regardless of the client's IP address.

NAT Traversal Using the Interactive Connectivity Establishment (ICE) and ICE-Lite Protocols

The SBC Edge integrates Microsoft Teams clients by acting as an ICE-Lite agent endpoint for SIP calls that involve a NAT. Microsoft Teams Clients act as controlling ICE agents (using Full ICE) and use the Session Traversal Utilities for NAT (STUN) protocol to overcome network address translation issues that can occur when an endpoint is behind a NAT device. Other NAT media-related features enabled in the SBC Edge configuration are overridden and do not operate to prevent conflict with ICE-Lite agent operation.

As an ICE-Lite agent, the SBC Edge connects to the public Internet with a single IPv4 address. The ICE-Lite functionality of the SBC Edge enables the controlling agent (Full-ICE communications client) to connect on the public address; pinholes punched in the NAT allow media exchange. This operation works with the firewall in front of the controlling ICE agent and supports opening NAT pinholes for UDP traffic in a Full-Cone, restricted, or symmetric NAT. The SBC Edge responds to connectivity checks using STUN bind requests to establish and verify connectivity so that the media session can progress.

The SBC Edge does not support ICE restarts or TURN server operation. If the full-ICE agent requires TURN server operation to traverse a NAT, the SBC Edge is unable to establish connectivity between endpoints in topologies for which an SBC-side TURN server is required.

For information about the configuration parameters for enabling ICE or ICE-Lite, refer to Working with the SBC Edge and SWe Lite as an ICE-Lite Agent.

Typical Network Layout

In a typical network layout (see below), an SBC Edge 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 with the SIP Phone's private IP address (i.e., 192.168.10.2). With Inbound NAT Traversal
enabled, the SBC Edge 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

![Typical Network Example Diagram]

**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, type a description for the table (i.e., **Default Private Prefixes**).

4. Click **OK**. The system creates the table.

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**.

**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.
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, refer to **Creating and Modifying SIP Signaling Groups**.

6. Click **Apply**.

---

**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 does not mean they have successfully registered. A NAT endpoint successfully registers only when the **Public Source IP** and **Public Source Port** are properly detected and display in the SIP Registrar User Table. For details on how to view these fields, see **Viewing Registered Users**.

**Configuration recommendation for NAT Traversal to function properly**

Ribbon recommends to disable SIP ALG in the connecting NAT routers to ensure NAT traversal functions properly.