Network Hosted NAPT - NAT Traversal

The SBC Core supports SIP peers located behind remote Network Address/Port Translation (NAPT) devices. NAPT is the most common type of Network Address Translation (NAT). The most common is a residential IAD behind a home NAPT device.

NAPT traversal is enabled on an individual IP Trunk Group basis. When configuring NAPT traversal, the Qualified Prefix table (qualifiedPrefix) is defined, which is a set of one or more IP network media and signaling prefixes that an IP address must match to be considered for NAT handling. If no entry is present in qualifiedPrefix table, the endpoint is automatically treated as existing behind a NAT device. As a result, SBC considers requests from all IP addresses to be behind a NAT device.

Two general issues apply to the problem where NAPT devices rewrite IP header addresses and ports for both signaling and media but do not modify embedded addressing information (i.e., NAPT devices exist that are SIP/SDP unaware):

- The “private” addressing local to the SIP peer is different from the “public” addressing SBC uses to reach the peer through the NAPT device. Consequently, addressing information that SIP peer embeds within signaling messages is insufficient for routing purposes and the SBC needs an alternate means of determining the appropriate destination IP address/port.
- Pinholes must be open in the NAPT device to exchange signaling and media between the SBC and the SIP peer. Otherwise, any “unsolicited” packets the SBC sends towards the SIP peer are dropped by the NAPT device. The implication for both signaling and media is that the SBC must first receive packets from a SIP peer located behind a NAPT device before it can send packets to such a peer. (See Adaptive NAT Pinhole Timer section below).

**Note**
The SBC Core does not support NAT traversal for IPv6 calls. Ensure NAT is disabled in pure IPv6 call scenarios.

**Signaling Traversal**

For the signaling aspect, the SBC supports a SIP registration relay service. No special support from the user endpoint/IAD is required for this method of NAPT traversal. REGISTER messages provide the SBC with a means for learning the destination IP address/port for signaling to the peer - the NAPT’d public source address/port in the IP header becomes the nexthop to reach the SIP peer’s registered contact address. The SBC can then learn the addressing information embedded in SIP signaling messages accordingly.

REGISTER messages also keep the signaling traffic pinhole open. When the SIP peer registers, the SBC specifies an expiration interval that is comfortably less than the NAPT device’s idle timeouts (typically a few minutes); the SIP peer is thus forced to send a refresh registration before the NAPT signaling pinhole closes. The majority of these relatively frequent external refreshes are handled locally by the SBC; after the initial registration, the SBC relays only a subset of subsequent REGISTER messages to the SIP Registrar based on a longer internal refresh interval.

**Secure Media Host Traversal**

The SBC also supports hosted NAT traversal for media, and exhibits similar behavior for sending media as it does for signaling. More specifically, the addresses embedded in the SDP specification are, in terms of the SIP peer’s private addressing, behind the NAPT device; whereas the SBC must actually send the RTP to the NAT’d public address/port. Since the RTP stream is generally symmetric, the SBC waits for RTP from the peer.
Secure media NAT validation applies to any one of the following scenarios:

- at initial call setup using network IP address obtained from INVITE message.
- using network IP address obtain from re-INVITE, UPDATE and REFER messages.
- with a HOLD followed by RETRIEVE.
- for video calls.

**Note**

Once a valid RTP packet is found against the signaling IP and the RTP stream is established, no further validation is required.

**Note**

To use this feature, the Media NAT Traversal flag "mediaNat" must first be enabled.

### Secure Media Hosted Traversal CLI Syntax

```
% set addressContext <address context name> zone <zone name> sipTrunkGroup <TG name> services
  natTraversal secureMediaNatPrefix <0-32>
```

To use this feature, the Media NAT Traversal flag "mediaNat" must first be enabled.

### Media NAT Traversal CLI Syntax

```
% set addressContext <name> zone <name> sipTrunkGroup <name> services natTraversal mediaNat <disable
  | enable>
```

Refer to `zone sipTrunkGroup - CLI` for CLI command details for these two flags.

### Adaptive NAT Pinhole Timer

For situations where SIP UA is behind NAT which does not support standard NAT traversal mechanism, the SBC can act as Registrar proxy by forwarding REGISTER messages to Registrar on behalf of SIP UA, refreshing REGISTER messages according to the expiry timer received from Registrar. The expiry timer between SIP UA and SBC is controlled by the SBC which supports NAT traversal of INVITE messages (call setup) towards SIP UA.

The SBC determines the expiry timer value which must be slightly less than NAT pinhole timer in SIP UA side. NAT pinhole closing timer is identified using SIP OPTIONS out-of-dialog mechanism mentioned in RFC 3261 and expires timer in 200 OK for REGISTER message is adjusted to ensure the pinhole remains open.