Service Provider Hosted NAT Traversal for SIP Calls Using Cisco IOS Session Border Controller

Problem Overview

With the increase in the use of multimedia and real-time traffic over the Internet, private network administrators are posed with the unique challenge of defending their networks from internal as well as external threats while allowing the voice, multimedia, and gaming traffic to flow through transparently.

The private residential user networks as well the small office or home office (SOHO) networks interface into the service provider cloud using a simple home gateway (HGW). HGWs can perform simple Network Address Translation (NAT) but are not sophisticated enough to modify the addresses embedded in the encapsulated Session Initiation Protocol (SIP) header. In order for the SIP calls to work with NAT in this solution, there is a possible alternative:

- The HGW needs to be replaced with an expensive application-level gateway (ALG) or the service provider session border controller (SBC) needs to modify the embedded SIP headers for packets before they reach the private networks.

The Cisco IOS® Session Border Controller helps in resolving this problem with this new feature called Service *Provider Hosted NAT Traversal* for SIP calls. This product bulletin outlines this new software feature.

SBC Definition and NAT Traversal Solution for SIP Calls

An SBC interworks with a variety of multimedia-capable network devices and is a toolkit of functions, including:

- H.323 and SIP signaling interworking
- Codec translation
- NAT and Port Address Translation (PAT)
- Billing and call-detail-record (CDR) normalization for authentication, authorization, and accounting (AAA)
- Quality of service (QoS) and bandwidth management

The network diagram in Figure 1 depicts a network scenario in which the private networks connect to the service provider's SBC. The working is discussed in more detail in the following sections.

Figure 1. Network Scenario

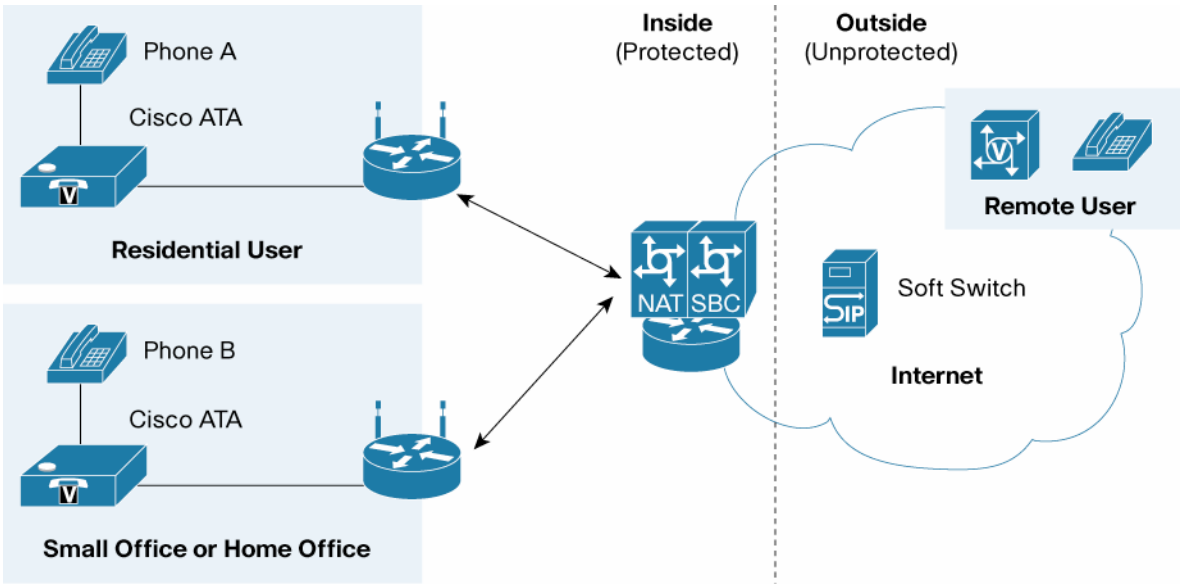
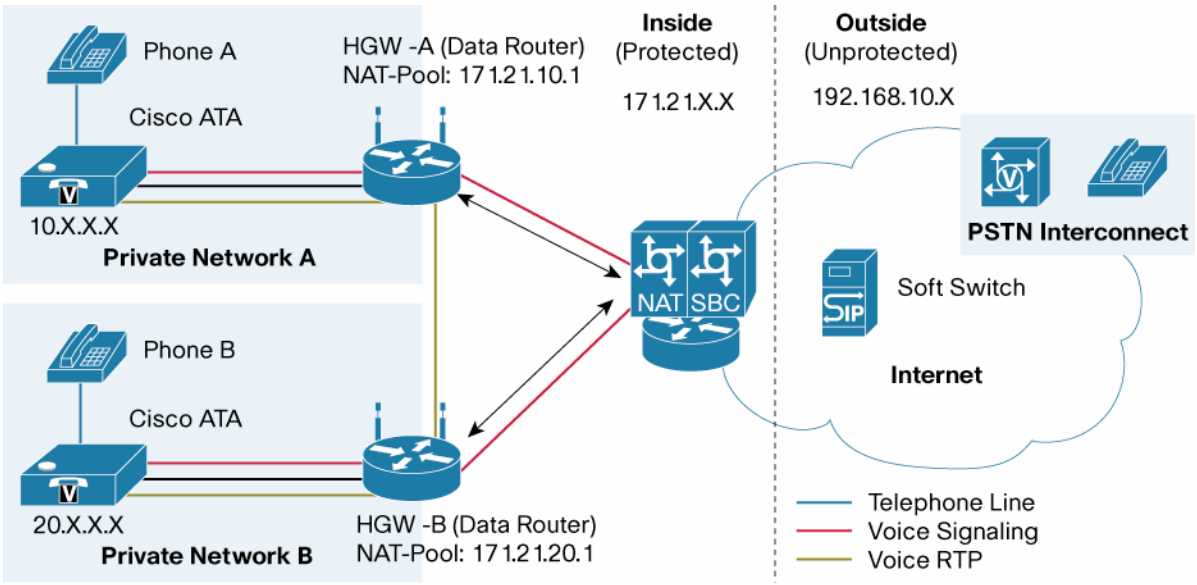


Figure 2. Private Network-to-Private Network Call Scenario (Media Flow-Around)



Consider a scenario in which the subscriber in network A calls the subscriber in network B (Figure 2).

- The phones in the private domain are configured with the NAT SBC as the SIP proxy. The NAT SBC intercepts the signaling packets and relays them to the soft switch as per the configuration. The SBC performs the NAT operation on the packet header as well as the embedded SIP address fields.
- When the call is established and the voice packet bearer path is cut through, the call proceeds in a flow-around mode with the Real-Time Transport Protocol (RTP) packets flowing directly between network A and network B.
- Flow-around here means that the RTP packets or the media packets do not pass through the NAT SBC.
- The private addresses in the RTP packets are directly routable between private network A and private network B.

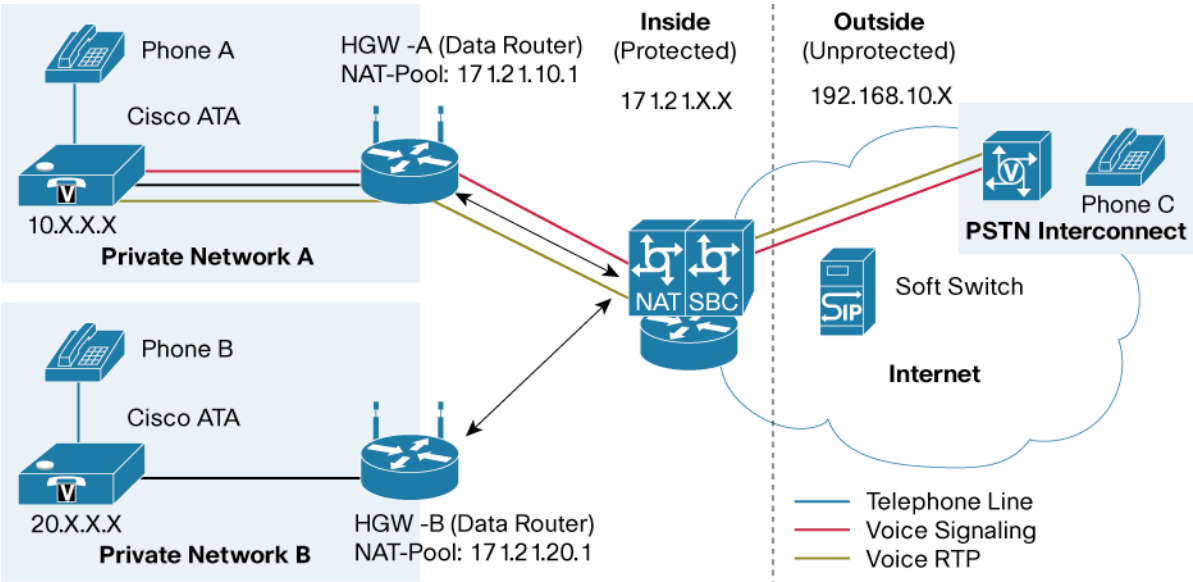
Feature Working on NAT SBC

The signaling packets going from private network A and from private network B to the SBC destined to the soft switch will have the source header address/port 171.21.10.1/1024 and 171.21.20.1/1024 respectively. The NAT SIP feature modifies these addresses to 192.168.10.1/1024 and 192.168.10.1/1025. It also creates a NAT entry for the flow and sends the packet to the soft switch.

NAT SBC also modifies phone A's *contact header address* to 192.168.10.1/2001 and phone B's contact header address to 192.168.10.1/2002. The NAT SBC modifies other relevant fields of the SIP payload and saves state information, enabling it to deliver the signaling packets destined to network A and network B.

The RTP packets do not go through the NAT SBC.

Figure 3. Private Network-to-Remote Private Network Call Scenario (Media Flow-Through)



Now consider the case in which the subscriber in network A calls a remote subscriber C connected to the PSTN.

- The call originates from the phone in private network A and the signaling as well as media is directed to the NAT SBC. The NAT SBC performs the NAT operation on both the signaling as well as the RTP packets and sends them to the remote voice gateway, which connects the call across the PSTN to phone C.
- The call proceeds in a *flow-through mode* with the RTP packets traversing through the SBC.
- The mode in this case is called flow-through because the RTP packets are flowing through the SBC.

Feature Working on NAT SBC

The signaling packets going from private network A to the SBC destined to the soft switch has the *source header* address/port 171.21.10.1/1024. The NAT SIP feature modifies these addresses to 192.168.10.1/1024. It also creates a NAT entry for the flow and sends the packet to the soft switch.

NAT SBC also modifies phone A's *contact header* address to 192.168.10.1/2001. The NAT SBC modifies other relevant fields of the SIP payload and saves the state information, enabling it to deliver the signaling and media packets from subscriber C that are destined to the address or port for subscriber A.

The RTP packets flow through the NAT SBC. For the packets going from subscriber A to subscriber C, the NAT SBC modifies the source address from 171.20.10.1/18000 to 192.168.10.1/20000, and conversely for the RTP packets flowing in the reverse direction.

Availability

The feature is available starting with the Cisco IOS Software Release 12.4(9)T.

Platforms Supported

The Cisco Systems® products that support the feature include the Cisco® AS5400XM and AS5350XM Universal Gateways, Cisco 2800 and 3800 Series Integrated Services Routers, Cisco 3700 Series Multiservice Access Routers, Cisco 7200VXR Series Routers, and the Cisco 7301 Router.

Restrictions

The following are the restrictions for the Hosted NAT Traversal feature for SIP calls:

- The SIP endpoints need to support symmetric media and signaling as well as early media in order for NAT and PAT to work on the HGW. Symmetric means the device uses the same port for sending and receiving.
- If the SIP endpoints do not support these media, the HGW can support NAT only without PAT.
- The embedded SIP addresses of one private network cannot be overlapping with the addresses of another private network.

For More Information

For more information about the Cisco IOS Hosted NAT Traversal using SBC, visit http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a008071c4ba.html.

For more information about SIP, visit http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_chapter09186a008075196f.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-364981-01 05/09