

# SI 45 NAT FILTER

## Datasheet Version 2.10

4S

### Key Features

- **SIP Session Border Controller**
- **Comatible with RFC3261-compliant SIP Proxies**
- **Stateless operation**
- **Application Server Integration**
- **Recording of Signaling and Audio**
- **Built on Proven snom SIP Stack**
- **Available for Microsoft™ Windows™ and Linux**

**snom india**  
VoIP Solutions  
Snom Technology India Pvt Ltd.

### Purpose

The SI NAT Filter is a SIP session border controller (SBC) that enables non-NAT aware devices to operate in private networks and behind firewalls. The NAT Filter operates on a public IP address and is addressed as outbound proxy. Non-NAT aware devices are automatically refreshed; NAT-aware devices that operate behind symmetrical NAT may self-refresh their bindings using the built-in STUN server of the filter. Devices on public Internet traverse the filter without changes or refreshes. By supporting Interactive Communications Establishment (ICE), the number of calls that must go through the filter can be minimized.

The SBC can operate on devices with multiple IP addresses. By extracting the routing table it inserts the IP addresses that match the routing path. This feature makes it possible to use the SBC also as near-end NAT solution.

### Recording

The operator version of the product also offers recording capabilities. Through a separate management interface, operators can define numbers that are silently recorded. The filter records the voice part of the conversation is recorded in highly-compressed audio format.

### Transparency

The layout of the SBC as proxy makes it application agnostic. Users can use the SBC with any kind of media (audio, video and other applications like gaming). SIP services like presence traverse the SBC without changes on the application layer. This gives the SI NAT Filter a competitive advantage against implementations that rely on the B2BUA architecture.

### Applications

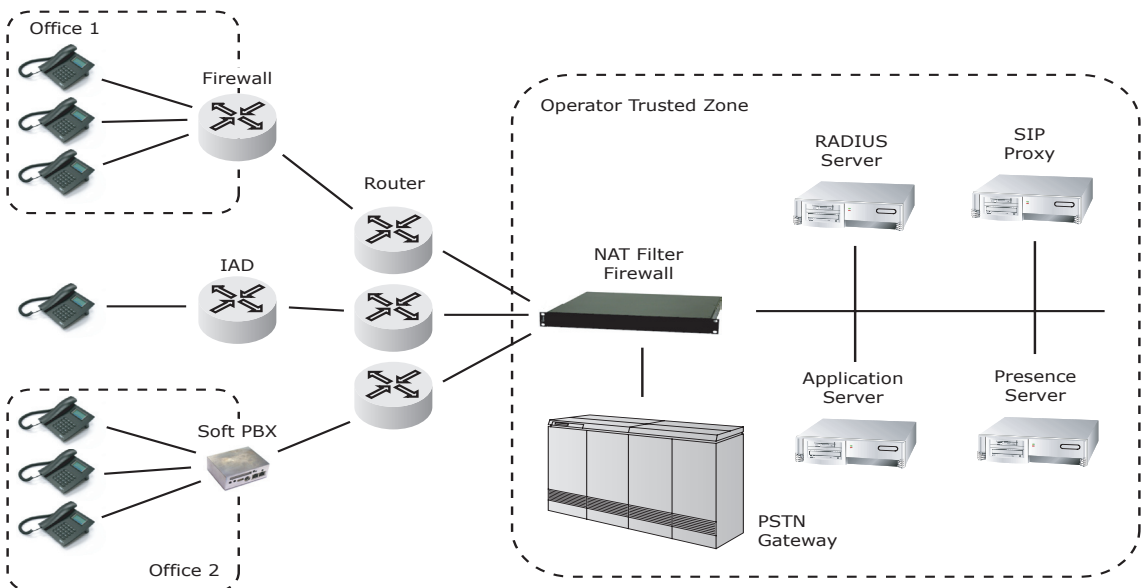
- Corporations. Corporations which operate their

infrastructure behind NAT and/or firewalls can talk to the public Internet through the filter.

- Operators. Operators offer the NAT traversal feature to their customers. Using the scalability feature of the filter, the operation of large networks becomes possible.
- Legal Intercept. Record specific calls for legal purposes. In many countries, operators must provide the possibility to record certain calls on request. The filter can perform this task.
- Proofing. Recording can be used for legal proofing (brokers, etc). The filter is fully compliant with other SIP equipment and can for example put between a PSTN gateway and SIP phones.

## Features

- The built-in RFC3261-compliant SIP proxy makes additional external SIP logic superfluous and simplifies the system setup.
- A built-in RFC3489-compatible STUN server for single IP addresses allows client to self-refresh their bindings
- Support for instant messaging, presence and all other SIP-compliant applications.
- Rich logging features allow easy maintenance.
- Recording functions based on number lists and expressions offer a flexible way of filtering out information.
- Recordings can be saved in WAV file



format (the data rate is 6 MB per hour).

- Almost stateless operation allows the filter to be used in server farms. This offers a tremendous scalability and redundancy making the product suitable for large operators.
- Both http and https as web interface for simple access from anywhere on the Internet.
- The filter supports Interactive Connectivity Establishment (ICE). User agents that support this feature will optimize the media path for the shortest possible delay.
- Media relay is established using connection-oriented media. User-agents that are not NAT-aware inherently support this feature. This makes the operation of the NAT filter backward compatible.
- Call-alive polling. During calls, NAT Filter checks if the call is still alive and terminates the call if this should not be the case. With this feature, charging users for broken calls can be avoided.
- Reliable and unreliable transport layers. NAT Filter supports both UDP and TCP transport layers.
- Support for TLS connections. User agents that use this transport layer and SRTP may establish completely secure communications.
- To and From headers may be changed for calls. The filter talks to a web application server to get this information.
- Application Server Integration. The web application server can also change the request-URI. This makes simple routing possible, which can be used for least cost routing, for example.
- Call Duration Limit. The web application server can define the duration of the call. This makes it possible to implement prepaid services.
- HTTP Registrar. The SBC may convert SIP register requests into HTTP requests and send the response back via SIP. This makes it possible to use the web server as registrar.
- Authentication. The SBC may authenticate incoming requests. It keeps a authentication cache updated by the web server. Trust relationships defined by IP address define exceptions.
- CLIR support. When a request leaves the data center, the SBC can change the From-header of the outgoing request and make it anonymous. This way, the caller ID can be hidden.

## Reasons to choose natf:

- **NAT support.** The solution supports full cone NAT, restricted NAT, symmetrical NAT, hairpinning, two-tier NAT and application layer gateways.
- **Application server integration.** Using a standard web server, you can implement large scale pre- and postpaid SIP systems.
- **TCP support.** User agents that support TCP can easily eliminate problems with NAT. natf sends keep-alive traffic on the connections and keeps the connection overhead off the proxy.
- **Security support.** User agents can use TLS and SRTP for secure communications.
- **Video support.** natf treats media transparent, which means that you can use audio, video and other applications like gaming or simulation as you like.
- **ICE support.** When user agents are smart, they can optimize the media path. In these cases, user agents will always use the shortest path, guaranteeing the best quality.
- **Stateful inspection.** Packets are inspected on application layer. Cryptographic hashes are used to make attacks difficult. Secure http can be used for maintenance.
- **No updates necessary for new applications.** The natf is a transparent proxy. That means it does not look at the SIP traffic if it does not have to. The only "application" that is intercepted is SDP, enabling voice and video streams.
- **No updates for new user agents.** We don't do tricks to deal with specific user agents. That means, when a vendor changes the firmware, the natf does not need to be software-upgraded.
- **No vendor dependency.** The methods used in the natf use generally available SIP mechanism. You can use the product with any SIP-compliant user agent or proxy.
- **Inherent scalability.** The natf works largely stateless. That means you can easily scale it in a centralized or decentralized server farm. You can grow your data center as your traffic grows. You can change your hard- or software setup without interrupting service. There is no problem with media path optimization across several natf instances.
- **Outbound proxy path optimization.** The natf has a built-in STUN server on the SIP port that allows user agents to automatically find the nearest natf server. This feature reduces the setup significantly.

# NAT Filter Specification

## ***VoIP Protocols***

- SIP (RFC3261)
- DNS NAPTR, SRV, A (RFC3264)
- TLS (RFC2246)
- Symmetrical Response (RFC3651)
- RTP/RTCP (RFC1889, RFC2833)
- SDP (RFC 3227)
- SUSCRIBE dialog support
- Presen/IM support
- Video/Gaming support (SIP/SDP-based)
- STUN (RFC3489)

## ***Management Interface***

- Web-based Interface
- http/https Access, password protection
- Registered user monitoring
- Call monitoring
- SIP activity trace
- Web-based log file access
- Rotating Logfiles
- Call Summary (incl. QoS)

## ***Application Server Interface***

- http interface to application server
- External Routing decisions
- To-/From header changing by application server (CLIR)

## ***Security***

- Topology Hiding/Route Hiding
- Call admission control via external application server
- E-911 support via external application server
- Call plugging support/timeout detection
- SRTP relay
- TLS transport layer support
- RTP relay destination locking (DoS protection)

## ***NAT Support***

- Supports all kinds of NAT (full cone, restricted, symmetrical)
- Multiple tiers NAT supported
- Support for local media path optimization (ICE)
- UDP and TCP/TLS NAT

## ***Scalability***

- Almost stateless operation
- No state replication between server farm elements necessary
- Multiple interface support (hardware redundancy)
- CPU scalability (performance scales with underlying hardware)
- Standard PC hardware requirements

Snom Technology India Pvt Ltd,  
No.1, 5th 'C' Cross  
BTM Layout, IAS officers colony  
Bangalore-560076  
India.  
Phone :+91- 80- 41200227  
Fax :+91- 80- 26782068  
Email :info@snomindia.com  
www.snomindia.com

### **About snom**

snom works in the VoIP area since 1999 and implemented the first SIP user agent in 2000. Since then, it has continuously improved the stability, feature set and interoperability of the SIP implementation. New products like the snom 4S media server and the snom 4S proxy are built on the snom technology and know-how.