

Horizon SIP – Secure Firewall/NAT Traversal

Product Facts:

- Works for any SIP compliant endpoint.
- Proprietary traversal protocols
- Maximum call completion rate across network borders
- Maintain network security policies with connectivity
- No Configuration required on Network or firewall/NAT
- AES encryption applies to all data transmission through public network
- Secured transparent traversal with less than 4ms latency

Deployment Options:

- Client/Server Secure Tunneling traversal
- Client-less deployment requires no software on premise.

Technical Specification:

Protocol Supported:

- UDP
- TCP
- TLS
- HTTP
- HTTPS
- RTP
- RTCP

Standard Supported:

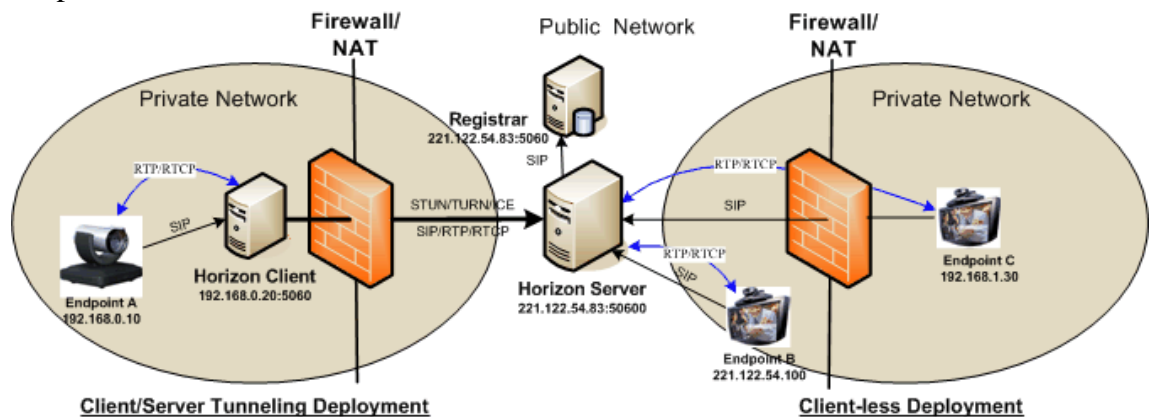
- Proprietary traversal protocols
- SIP over UDP/TCP/TLS
- HTTP over TCP/TLS
- STUN
- TURN
- T.120
- Symmetric Response
- Extension Header Field
- Locating SIP Server

Micromethod's Horizon SIP solution effectively overcomes the barrier for end-to-end multimedia IP communication across network boundaries with secure, transparent, seamless traversal while maintaining network security policies.

Horizon SIP unlocks the value of Multimedia over IP (MoIP) by enabling real-time IP communications cross organizational and network boundaries. As the most effective solution that enables maximum call completion rate across network boundaries, Horizon provides end-to-end connectivity with transparent multi-boundary traversal without requiring any network or firewall/NAT configuration.

Horizon SIP is comprised of Server and Client components. Server is typically deployed on the public network or in the domain of service provider and Client is deployed within the enterprise network or embedded with the SIP endpoint. Client negotiates with Server for the most feasible FW/NAT traversal methods for based on the network capabilities, ranging from simple symmetric response, to full HTTPS/TLS tunneling, for both SIP signaling and RTP/RTCP/T.120 media transport.

With implementation of TLS with mutual authentication and point-to-point encryptions, Horizon SIP supports Basic, Digest, Certification-based authentication with SIP endpoints.



Horizon supports two proprietary traversal protocols that can traverse all types of firewall and work with any SIP endpoint without any traversal standard implementation from endpoint.

1. Secure Tunneling Traversal is comprised of a client and server. The tunneling traversal can accomplish both-way call initiation with one open outbound port required on firewall.
2. Client-Less Traversal can also accomplish both-way call initiation without any customer premise software or equipment.

Horizon's proprietary traversal doesn't require endpoints to implement any of the standards such STUN, TURN or ICE.

Optional Components:

- Firewall/NAT traversal for H.323 based communications
- SIPoint Proxy Server
- SIPoint Registrar Server
- SIPoint Presence Server
- SIPoint XCAP Server
- SIP Instant Messaging Server
- SIP User Agent toolkit

Deployment Options:

- Hosted VoIP Provider, no software on premise.
- On-premise enterprise solution for intra-organization communication

Key Features:

- Works with any SIP endpoint, no standard support needed on endpoint.
- Ability to securely traverse multiple network boundaries of all types.
- Maintain network security policies while providing connectivity.
- Automatically detects the best traversal strategy based on preferences.
- Web based interface Operation Management and Monitoring.
- Secure channel with TLS with multiple encryption support.
- Load balancing and fault tolerance.
- Fail-over with automatic server hunting.

Protocols Supported:

- UDP
- TCP
- TLS
- HTTP
- HTTPS
- RTP
- RTCP
- T.120

Standards Support:

- Proprietary tunneling protocols
- SIP over UDP/TCP/TLS
- HTTP over TCP/TLS
- STUN (RFC 3489)
- TURN
- Symmetric Response (RFC 3581)
- Extension Header Field (RFC 3327)
- Locating SIP Server (SIP DNS)

Recommended Hardware Specification:

Horizon SIP Server:

- Linux, UNIX, Windows XP/Vista
- 1GB RAM or more
- 100Mbps Network adapter
- One public IP address

Horizon SIP Client (both group and personal editions):

- Linux, UNIX, Windows XP/Vista
- 256MB RAM or more
- 100Mbps Network adapter

