ShoreTel®

Brilliantly simple™

SIP Trunks

Keeping your UC System Secure

Jeff Ridley

Sr. Director of Product Management

Feb, 4, 2011

Agenda

- Executive summary
- Security considerations for SIP trunks
  - Threats
  - Importance of stable platform
- SIP, NATs and Enterprise Firewalls
  - Methods for solving NAT/firewall traversal if SIP
  - SIP-capable firewalls
  - Enterprise session border controllers
  - Session border controllers at the service provider edge
- SIP proxy-based firewalls and enterprise SBCs: Security advantages of the SIP proxy
- Which NAT/firewall traversal solution is right for you?
- Conclusion

Executive Summary

- SIP trunks use IP-based protocols
  - UC system opens up to a wide area network (WAN)
  - WAN should be assumed insecure.
- Customers
  - Should educate themselves about salient security issues
  - Choose an appropriate security solution.

Security considerations for SIP trunks : Threats

- UC Systems connected to the Internet / WAN can expose the entire network to many types of threats e.g.

  1. Brute force attack where the intruder tries to log into a service using a massive user/password database.
     - Once a service has been compromised it provides a springboard to the entire network.
  2. Denial of service (DoS) attacks where attackers command numerous hosts or "bots" to send a large number of packets to overwhelm and crash a service.

SIP , NATs and Enterprise Firewalls : The NAT Problem

- SIP – based communications originating from outside the enterprise, cannot reach enterprise users directly
  - Firewalls are designed to prevent unsolicited inbound communications.
- Network Address Translation (NAT) is provided by most firewalls and routers.
  - Mapping of private to public IP addresses creates challenges for SIP communications.
- Many older firewalls are not aware of the SIP protocol.
  - Can create problems.

SIP , NATs and Enterprise Firewalls : Questions to ask around Firewall Traversal

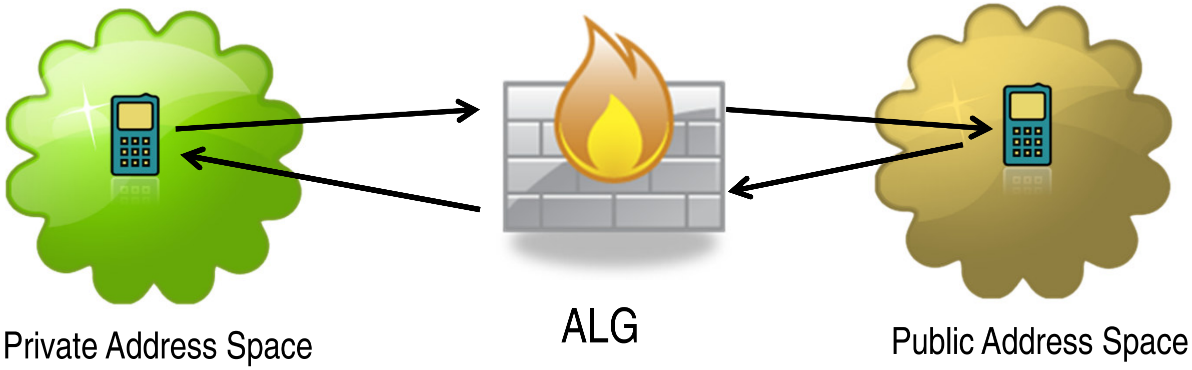
- Every method of firewall traversal has pros/cons w.r.t. the amount of control and security you maintain of your network.
- Questions to ask ?
  - Who maintains control of your network security ? ITSP or you ?
  - Does you solution lock you into a single ITSP ? Is it future proof ?
  - SIP protocol variations are common. Is your solution flexible enough ?
  - SIP is about much more than voice. Does your solution support the performance needs to deploy IM, presence, video and/or collaboration in the future ?

SIP , NATs and Enterprise Firewalls : Firewall Traversal Options

- SIP Aware Firewalls
  - SIP ALG-based firewalls
  - SIP Proxy-based firewalls
- Enterprise Session Border Controllers (SBC)

SIP ALG-based firewalls

- Most common variation of SIP- aware firewalls
  - ALG = Application Level Gateway
  - Works for basic call scenarios
  - May have limitations for enterprise SIP-based real-time communications.
  - Handles SIP packets on the fly , making sure that they reach the right destination in the enterprise.

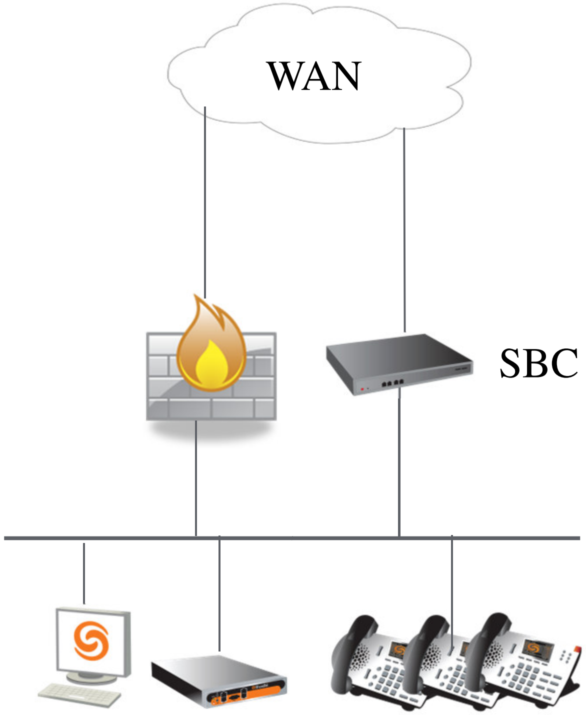


SIP Proxy-based firewalls

- A SIP proxy firewall performs deep packet inspection before delivering them to appropriate endpoints.
  - Provides better control.
  - Handles
    - Encrypted SIP signaling (TLS) and media (SRTP)
    - Authentication
    - Advanced filtering
    - Advanced routing and control features
- May include a back-to-back-user-agent (B2BUA)
  - The B2BUA allows the firewall to have two different call legs in the same session, one on each side of the firewall. The firewall can then utilize “local call transfer” by just changing the call leg on the LAN side from one client to the other.

Enterprise Session Border Controllers (SBC)

- Enterprise customers who have fine-tuned their firewall and security policies, may be reluctant to replace their existing firewalls with new SIP-capable firewalls.
- An enterprise SBC (e.g. Ingate SIParator) can complement any existing firewall.
  - Operates in parallel just on SIP traffic
  - Standalone or in DMZ of existing firewall.
  - SIP proxy based implementation for max flexibility



Security Advantages of a SIP proxy (SBC) : Media handling

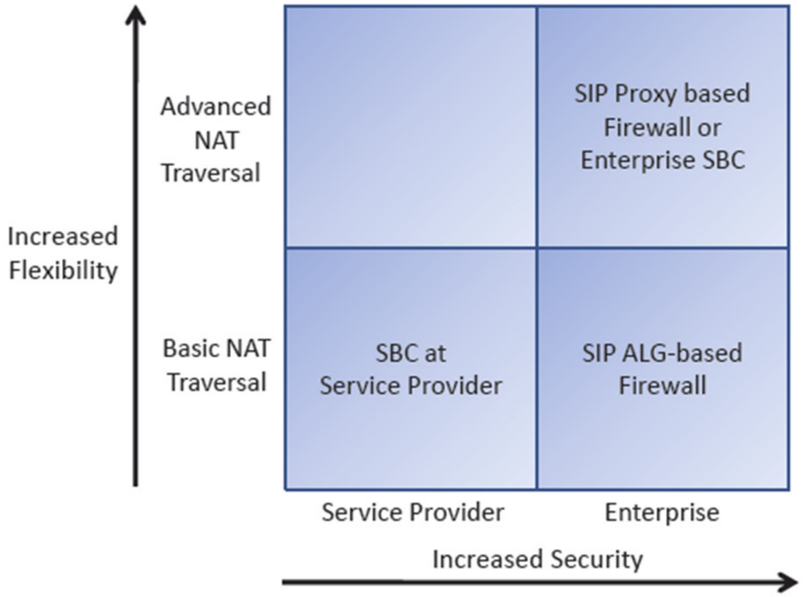
- SIP is about establishing media sessions – SRTP/ RTP based
  - Ports dynamically opened as needed
  - Ports closed again when call / session ends
- More secure than STUN/TURN/ICE methods, which require that ports are left open from the “inside” of the firewall to allow media port negotiation to succeed.
- Protects against rogue media injection
  - Only accepts media from the endpoint that receives media from the SBC.

Security Advantages of a SIP proxy (SBC) : Signaling

- SBC implements a SIP parser
  - Verifies that SIP message is valid and that it may be forwarded to the local LAN. Malformed SIP messages are discarded.
  - Hackers often use malformed packets attacks to crash a system and gain control.
  - Needs to be robust enough to handle Denial of Service attacks
- SBC supports signaling encryption
  - SIP signaling consists of messages in ASCII text (plain text), and is therefore easy to read and manipulate. It is strongly recommended to encrypt and authenticate SIP signaling (TLS or MTLS)
- SBC offers flexible filtering e.g. They can control
  - Which SIP methods are allowed / disallowed per network.
  - Whitelists for incoming callers

Which Security solution is right for your SIP trunks ?

- Your choice largely depends on these questions:
  - Who should be in control of your security infrastructure: the IT administrator or a service provider?
  - Do you want a solution that is predictable and functions reliably within the entire SIP standard or something that is limited to certain call scenarios with specific ITSP's only ?



Increased Flexibility

	Service Provider	Enterprise
Advanced NAT Traversal		SIP Proxy based Firewall or Enterprise SBC
Basic NAT Traversal	SBC at Service Provider	SIP ALG-based Firewall

Increased Security