SESSION BORDERS CONTROLLERS: NEXT STEP IN FULL DEPLOYMENT OF VOICE OVER IP SERVICES

Constantinescu Mihai Aurel[1], Cernăianu Doina Oana[2], Croitoru Victor[1]

[1] "Politehnica" University of Bucharest
Faculty of Electronics, Telecommunications & Information Technology
Department of Telecommunications |
Splaiul Independentei 313, sect. 6, Bucharest 77206, Romania

[2]Teletrans S.A. Bucharest, Romania

Abstract: Session Border Controllers (SBCs) became an important element in implementation of modern Voice over IP (VoIP) services, as service providers look to protect the integrity of their networks and business models while offering new services to the customers. Meanwhile, the status of near-ubiquitous use of Network Address Translators (NATs) across the Internet and the great diversity of their behavior raise a serious obstacle in the VoIP's deployment. The paper analyses one of the most popular and widely adopted VoIP signaling protocol, Session Initiation Protocol (SIP), the issues of NAT traversal, and the role of SBCs in solving it and extending the VoIP capabilities.

Keywords: VoIP, SIP, NAT, SBC

INTRODUCTION

The peer-to-peer model of SIP encounters serious problems at NAT traversal. First, NAT does not allow any incoming calls from public to private hosts. Second, SIP messages encapsulate the source address and port at application level. The NAT changes the address and port of packets, but only in IP and TCP/UDP headers, so the messages will be discarded by the SIP client. Moreover, SIP uses different ports to communicate, therefore several SIP messages will be blocked by NAT due to port filtering. Several solutions are proposed by IETF and by manufacturers, but the only one, the SBC, meet the unified method request

SESSION INITIATION PROTOCOL (SIP)

"Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences [1]."

SIP signaling consists of an exchange of short messages that contain session descriptions, which allow participants to agree on a common set of media parameters. The path between a pair of SIP clients is handled by SIP proxy/registrar servers. They keep information related to the current location of clients, authenticate and authorize users for services, and route requests to those clients.

FIREWALLS AND NETWORK ADDRESS TRANSLATORS (NAT)

"A firewall is a device with two interfaces-one on the "inside" and one on the "outside". Its function is generally to protect devices on the inside from those on the outside, and to sometimes prevent users on the inside from connecting to, or accessing services on the outside."[2]

"Network Address Translation is a method by which IP addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts. Traditionally, NAT devices are used to connect an isolated address realm with private unregistered address to an external realm with globally unique registered addresses."[3]

NATs are active units in the data path, usually included in a router or a gateway, whose primary role is to allow IP addresses to be shared between numerous devices. NATs make a clear separation of the network in two islands: inside (private/ hidden), and outside (public Internet). NATs intercept each IP packet from outside to inside and from inside to outside, may forward it with or without modification, or may discard it. They act as firewalls, being network topology sensitive, but are different from routers or firewalls, having the ability to modify the packet before forwarding it [4].

NAT Behavior and Classification

The lack of standardization with respect to NAT leaves manufacturers free to implement NATs that differ from each other not only on a vendor-to-vendor basis, but even on a model-to-model basis for the same vendor.

A basic difference in NAT behavior consists in the way in which the binding is done. This will result in four types of NATs [4]:

- *Symmetric*: Symmetric binding means that the mapping of the destination address initiated by the first outgoing packet remains unchanged for the lifetime of the binding. The mapping operation is based on a session 5-tuple state, including TCP/UDP protocol, the local IP address and port number, and the destination address and port number. This is the most restrictive type of NAT;
- *Full-cone*: In this case the binding of a local address and port to a public address and port can be used by any outside host on any port. Full-cone NAT is the least restrictive behavior;
- *Restricted-cone*: The binding for this kind of NAT is only available for the destination outside host, which can use any port to send packets;

- *Port-restricted-cone:* For this type of NAT the binding is available for any outside host, but the source port must be the same as the original one that initiated the binding.

Further Behaviors: Hairpin and Determinism

To make classification more complicated, some NATs can have different behaviors for TCP and UDP packets. They can treat a TCP session in a symmetric mode, and UDP packets in a full-cone mode. Even so, there are more differences in NATs behavior:

- *Hairpin support:* A NAT has hairpin facility if a local host can send outgoing packets using a public address and port already used for another binding. This address can be one used by other local host or even one of its own binding.
- *Determinism:* A NAT can react in different ways to the same type of packets, depending on the binding conflict situation that occurs. There are three types of reactions: *primary, secondary and tertiary* [4]. When a NAT tries to use the same binding for the next session, choosing the same external port as the internal one, the NAT has a primary determinist behavior. When other local host tries to use the same port, the NAT will use the same public address as before, but other external port. That's the secondary NAT behavior. At the same time, if a third local host tries to use the same pair of public address and port, the binding will be with other public address and other external port. This is the tertiary NAT behavior.

Conclusions related to NAT

The result of NAT behavior analysis is a very critical one:

"A NAT has no standard way in which to advertise its presence, nor does it have any standard way to advise protocols and applications of the particular behaviors it applies to packets being passed through the NAT."[4]

NAT/FIREWALL TRAVERSAL FOR SIP: ISSUES

The traversal of SIP communications through NAT/Firewall can be analyzed in two parts:

- SIP signaling and NAT traversal;
- Associated media and NAT traversal.

SIP signaling and NAT traversal

SIP signaling meets a number of problems at NAT traversal:

- *Source port in the request message changed by NAT:* The default operation for SIP using UDP consists in responses generated by SIP proxy/registrar (User Agent Server) to requests generated by SIP phones (User Agent Client). The response message contains the source address from the request message in the SIP "via" header and in the "received" parameter, and the source port from the request message in the SIP "via" header. The NAT changes the local port (the source specified in the request) with an external port. The SIP request message will be processed by the SIP proxy with the original port and sent to the SIP client. The response will use the original port, and the NAT will block the message, due to port mismatch;

- *Incoming signaling from public network:* In the context of an IP client behind a NAT and the SIP proxy/registrar on the public network, after a successful registration, any SIP message coming from the SIP proxy will be blocked. This happens due to SIP protocol's lack of any mechanism to allow new requests generated in the opposite direction to use the same address and port used for the initial direction (e.g. registration);
- *Binding timeout*: SIP does not provide any mechanism for keeping a connection alive. The SIP connection previously opened through NAT will be closed due to binding timeout after an inactive period of time, and the SIP client will not be able to receive any further calls.

Associated media and NAT traversal

The RTP is the most common media transport protocol used in SIP communications. Negotiation of RTP parameters is done using the SDP protocol. In the Session Description Protocol (SDP) [5] part of the SIP message there are specified the address and port of each client to receive media. Because the address and port belong to a private realm, the incoming traffic will be blocked by NAT due to address and port mismatch.

SESSION BORDER CONTROLLER (SBC)

"In its simplest form, a Session Controller enables interactive communication across the borders or boundaries of disparate Internet Protocol (IP) networks. In doing this, Session Controllers connect islands of IP voice and/or video traffic without requiring all IP traffic to first be converted into TDM at a handoff point between networks. Session Controllers operate at Layer 5 of the network and work with - but don't replace – devices such as softswitches, NAT devices and firewalls."[6]

A SBC cooperates with firewalls in order to enable authorized connectivity from the outside to inside, avoiding the "incoming signaling from public network" issue.

A SBC performs some NAT functions, but does not interfere with it. The address and port changes affect only the current SIP connection, the rest of data traffic being under NAT control.

A SBC contains two entities [7]: SBC signaling server and SBC media server (figure 1).

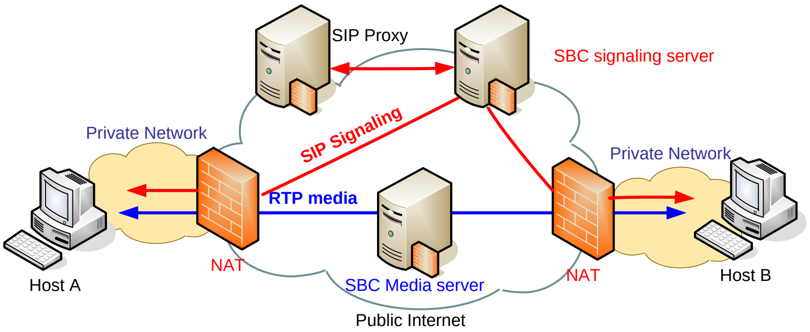

Figure 10 SBC components

SBC signaling server is dealing with SIP signaling between SIP clients behind the NAT and the SIP proxy server. It is configured as a transit point for SIP signaling messages and provides complete visibility and control of call establishment. The SBC signaling server also controls the interval for SIP register update, in order to avoid the “binding timer” issue. The SBC signaling server performs the following functions:

- Processing of the SIP user registration;
- SIP header modification (contact and via header), in order to allow the correct processing of SIP clients and SIP server messages;
- Address and port modification to permit NAT traversal;
- Communication with the SBC media server, for traffic management and synchronization;
- Resolution of SIP servers through DNS.

SBC media server operates under the control of the SBC signaling server. It acts as a transit point for RTP and RTCP traffic between SIP clients. It modifies SDP parameters to allow NAT traversal for media using NAT’s pin-holes, but without interfering with NAT security policy. Being under control of SBC signaling server, the SBC media server provides full visibility and control of the media traffic for each SIP connection. Additionally, it can act as a dynamic NAPT that hides details of the network elements and topology.

By having full control and visibility of all media sessions, a SBC can easy implement a scalable VoIP network architecture over multiple boundaries (figure 2), all existing equipment remaining unchanged. It also allows QoS and billing information management for calls.

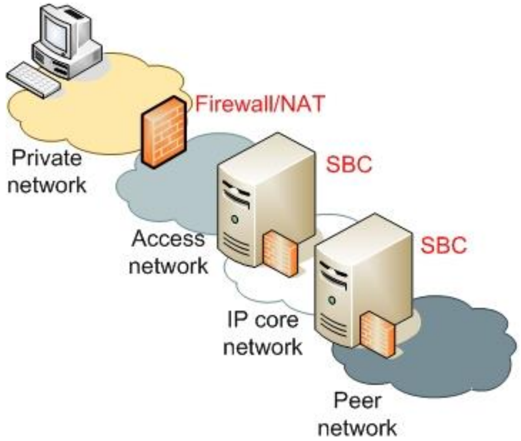

Figure 11 SBCs in a scalable VoIP architecture

CONCLUSIONS

SBCs play different roles and offer different functionality in a variety of scenarios. In each case, the issues that SBCs try to resolve are caused by boundaries of trust, administration, and policy. The SBCs act as a link between these boundaries and so extend over it the peer-to-peer model of VoIP communications. In this way, the SBCs have a key position in the full –scale deployment of VoIP services over multiple IP networks. The future large deployment of SBCs depends on a standardization that is still missing, and the need of assurance that the use of SBCs will not introduce any threat to network security, due to the increase of overall network architecture.

REFERENCES

[1] J. Rosenberg, et al., “SIP: Session Initiation Protocol”, RFC 3261, June 2002.

[2] J. Rosenberg, D. Drew,H. Schulzrinne, “Getting SIP through Firewalls and NATs”, Internet Draft, draft-rosenberg-sip-firewalls-00.txt, February 2000.

[3] P. Srisuresh, M. Holdrege, “IP Network Address Translator (NAT) Terminology and Considerations”, RFC 2663, August 1999.

[4] G. Huston, “Anatomy: A Look Inside Network Address Translators”, in The Internet Protocol Journal, vol. 7, Number 3, September 2004, pp. 2-32

[5] M. Handley, V. Jacobson, “SDP: Session Description Protocol”, RFC 2327, April 1998.

[6] Session Border Forum , http://www.sessioncontrollerforum.org/

[7] White Paper - SignallingProxy™ - Accelerating the Deployment of SIP Services, http://www.newport-networks.com/whitepapers/spwpes.html