



The Role of Session Border Controllers in the DMZ of Voice over IP(VoIP) Networks

Huihong Chen (Corresponding author)

School of Information Science Technology

Central South University

Changsha, Hunan 410083, China

E-mail: chenjin_2002@163.com

Zhigang Chen

School of Information Science Technology

Central South University

Changsha, Hunan 410083, China

Tel: 86-731-887-9636 E-mail: czg@csu.edu.cn

Abstract

SBCs usually sit between two service provider networks in a peering environment, or between an access network and a backbone network to provide service to residential and/or enterprise customers. They provide a variety of functions to enable or enhance session-based multi-media services (e.g., Voice over IP). This thesis analyzes the internet structure of SBC and shows single-box and dual-box SBCs in the DMZ and introduces firewalls and network address translation. And then explain how the SBC cooperates with the firewalls to ensure that VoIP signaling and media traverses the DMZ without compromising the security of the trusted network. And finally, describes topology hiding and bad protocol detection of other DMZ processing.

Keywords: VoIP, DMZ, SIP, SBC, NAT

Border Controllers (SBCs) have become an important element of modern Voice over IP(VoIP) networks, as service providers look to protect the integrity of their networks and business models while offering diverse services to their customers.

Most people would agree that an SBC is a kind of firewall for Voice over IP traffic. However, as soon as you start to look beyond this initial consensus, there is considerable disagreement as to what an SBC actually is, and what function it should offer! This is partly because SBC vendors are pushing out to cover a wide variety of niches in order to compete for market share, and partly due to the genuine range of scenarios where service providers are looking for solutions.

1. INTRODUCING SBCS AND DMZ

An SBC is a VoIP session-aware device that controls call admission to a network at the border of that network. Optionally (depending on the device), it can also perform a host of call-control functions to ease the load on the call agents within the network.

1.1 Internal structure of an SBC

An SBC device breaks down into two logically distinct pieces.

- The Signaling SBC function (SBC-SIG) controls access of VoIP signaling messages to the core of the network, and manipulates the contents of these messages. It does this by acting as a Back-to-Back User Agent (B2BUA).
- The Media SBC function (SBC-MEDIA) controls access of media packets to the network, provides differentiated services and QoS for different media streams, and prevents service theft. It does this by acting as an RTP proxy.

Some SBC devices offer both functions in a single box (referred to hereafter as single-box SBCs). Others take a distributed approach, and separate SBC-SIG and SBC-MEDIA onto separate machines (referred to hereafter as dual-box SBCs), using call control protocols such as H.248 and COPS-PR to link the two.

1.2 The Demilitarized Zone

The Demilitarized Zone (DMZ) is the conceptual term for a small subnetwork (or individual device) that sits between a trusted private network, such as a corporate private LAN, and an untrusted public network, such as the public Internet. Typically, the DMZ contains devices directly accessible to Internet traffic, such as web servers, FTP servers, or SBCs. The purpose of the DMZ is to prevent hostile or unwanted traffic from entering (or, in some cases, leaving) the private network.

2. DMZ PROCESSING

The DMZ is the “demilitarized zone” between two networks, as described in section 1.2, The Demilitarized Zone. This chapter provides more detail on the role played by SBCs in the DMZ.

2.1 Devices in the DMZ

All SBCs fall into one of the following two categories.

- Those that do not perform firewall processing in the DMZ, but instead rely on an external and internal firewall.
- Those that do perform firewall processing (i.e. that have a firewall on-board).

If an SBC does not perform firewall processing, then the DMZ looks like this

Figure 1. SBC does firewall processing

If the SBC is decomposed into the dual-box model, then the SBC-MEDIA device resides in the position indicated above, and the SBC-SIG device resides in the network core. In this case, SBC-SIG controls the firewall to allow VoIP signaling and media to pass through.

If the SBC does perform firewall processing, then the same DMZ looks like this:

Figure 2. SBC does firewall processing

If the SBC is decomposed into the dual-box model, then SBC-MEDIA implements a firewall that screens out unwanted signaling and media packets.

All SBCs typically incorporate NAT (Network Address Translator) function. The remainder of this section describes the role of firewall devices in the DMZ, and the role of the NAT component of the SBC.

2.1.1 The firewall

Firewalls prevent unwanted traffic from entering, or leaving, a network by performing basic packet filtering. Note that firewalls filter packets purely by examining packet headers, and do not parse or understand the payload of the packets. Therefore, they do not filter out all types of unwanted traffic. For example, firewalls do not perform Call Admission Control – SBCs do that. However, firewalls are valuable because they efficiently filter out large categories of unwanted traffic, leaving application-aware devices such as SBCs with much less work to do.

The external firewall in Figure 1 filters packets from the external network, but allows all packets from the internal network to pass through unfiltered. The internal firewall filters packets from the internal network, but allows all packets from the external network to pass through unfiltered (since they have already passed the external firewall).

Firewalls by default do not accept packets from the network, but are configured with rules that allow them to select and accept certain packets. Therefore, packets are admitted to (or from) the network based on *explicit configuration*, and not on default configuration. Firewalls are configured either

- by the network operator, using a human interface, *or*
- by trusted software, using an API.

There are no standards-defined APIs for configuring firewalls; however, the IETF’s MIDCOM working group is evaluating suitable protocols for this task. SNMP, RSIP, Megaco, Diameter, and COPS are all being considered. In addition, the MSF have made some steps towards defining their own protocol for firewall control (MSF2003.113.00 – Draft IA for RTP Proxy / FW Control Protocol).

2.1.2 The NAT

SBCs typically incorporate NAT function. NATs separate a network into distinct address spaces. In Figure 9, the NAT component of the SBC separates the internal network address space 10.1.0/24 from the external network address space 85.3/16. A few addresses from the 85.3/16 domain are used to represent all machines within the 10.1.0/24 domain, as described below.

The NAT maintains a table of mappings from {external address, port} to {internal address, port} and vice versa³. The table is a dual-index table, so a particular mapping can be looked up given either the internal or external addressing information. The NAT uses this table to rewrite the headers of the IP packets that it forwards.

- On receiving an IP packet from the external network, the NAT looks in its table for the destination address and port of the packet (which will be an address from the external address space). If a mapping is found, then the destination address header in the IP packet is changed to contain the corresponding internal address and port from the table, and the packet is forwarded towards the internal network. If no mapping is found, the packet is discarded.
- On receiving an IP packet from the internal network, the NAT looks in its table for the source address and port of the packet (which will be an address from the internal address space). If a mapping is found, then the source address header in the IP packet is changed to contain the corresponding external address and port from the table, and the packet is forwarded towards the external network. If no mapping is found, then a new mapping is created: the NAT dynamically allocates a new external address and port from the external address space for the packet (and all future packets from this source address and port tuple). Mappings in the table are created in one of two ways.
- By packets traversing the NAT from the internal network towards the external network, as described in the second bullet point above.
- By configuration, either from the network operator via a human interface, or programmatically from trusted software via an API.

2.2 How VoIP signaling packets traverse the DMZ

The NAT component of the SBC and the firewalls in the DMZ is configured (at start of day) as follows.

- The NAT is configured with a mapping that converts between the SBC's internal address (10.1.0.22 in Figure 9) and the port it uses for signaling, and some address and port taken from the external network's address space. This external address and port is used to identify the SBC in the public network. Packets sent from the external network and destined for the SBC are sent to this address and port.
- The external firewall is configured to permit IP packets whose destination address header contains the address and port that identify the SBC in the external network.
- The internal firewall is configured to permit IP packets whose destination address header contains the internal address of the SBC, and the port that it uses for signaling.

Note that this configuration could either come from human input, or from the SBC by programmatic API if the SBC and firewalls are collocated, or from the SBC by network protocol if the devices are separate.

This configuration allows all signaling packets addressed to the SBC to traverse the DMZ devices and reach the SBC, whether the packets originate from the internal or external network. In addition, it allows the SBC to send signaling messages towards either the internal or external networks.

This scheme relies on the fact that the external address and port that is used to identify the SBC on the public network for signaling is well-known to VoIP devices on the public network. Typically, this is achieved by using DNS records to associate this address with the SBC's hostname in the public network.

This scheme also relies on the SBC knowing its external IP address and port for signaling, because it must use these in the VoIP signaling headers that it sends in requests to the external network (as these fields are usually used to route the signaling response). This can be configured on the SBC.

2.3 How VoIP media packets traverse the DMZ

The situation with media packets is a little more complex than with signaling, because the media packets in a given call originate from, and are sent to, addresses and ports that are dynamically allocated by the RTP protocol when the call is established.

The SBC acts as a signaling Back-to-Back User Agent (B2BUA) and a media bridge, and so it terminates the media of a call on both the internal and external network sides. The ports that it uses to send and receive media on each side are allocated dynamically when the call is established.

Figure 3. VoIP media packets traversing the DMZ

This causes a couple of problems.

- The internal firewall needs to be configured to permit IP traffic sent to port 9900 on the SBC. Since 9900 is a dynamically allocated number, this must be done automatically during call set-up (i.e. without human intervention).
- The external firewall needs to be configured to permit IP traffic sent to the SBC's external address and port 12745. Again, this must happen automatically during call set-up.

If the firewall and SBC are on the same device, then these problems are easily overcome by implementing a programmatic interface that allows the SBC to dynamically configure the firewall software.

If the firewalls are separate from the SBC, then either

- the SBC dynamically configures the firewall over the network (although, as noted above, there are no standards for this at present), *or*
- the firewalls must be configured to permit all traffic sent to any port on the SBC (or at least, any port in the range used by the RTP protocol).

2.4 Other DMZ processing

SBCs also perform other DMZ-related processing, as described in the following sections.

2.4.1 Topology hiding

VoIP signaling messages convey information that can allow the recipient to determine both the internal topology of a network, and the route taken by a call across that network (and possibly out the other side). For example, the Via headers in SIP signaling messages carry this kind of information.

It is often undesirable to expose this information to users outside a network. For example, if you are a service provider who uses a second service provider to act as a carrier for your calls, you do not want to expose the identity of the carrier SP to your customers in case they approach the carrier SP directly for a better price.

To solve this problem, SBCs can remove sensitive information by rewriting the VoIP headers in the signaling messages that they send across the network boundary. SBCs achieve this by acting as B2BUAs. They terminate the VoIP signaling that they receive from within the private network, and signal a new call towards the public network. Since this is a new call, it does not require any of the routing information from the previous call (for example, none of the SIP Via

headers are carried over into the public network call leg).

2.4.2 Bad protocol detection

The SBC processes all signaling and media that enter or leave the network. It can therefore screen the network from bad protocol within signaling or media packets, discarding or sending negative responses to badly-formed packets. This has two advantages.

- It reduces the load on the VoIP servers within the network, which can be significant if someone is attempting to mount a DoS attack on the network by sending poorly-formed packets.
- It reduces the likelihood of the badly-formed messages causing a crash on a key piece of VoIP infrastructure within the network.

The amount of checking that an SBC does on signaling messages should be configurable. For example, it could be configured to check only those fields that it itself needs to process the message, or it could check all fields in the message, or anywhere in between.

References

- Rosenberg, J, Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler. (2002). SIP: Session Initiation Protocol. RFC 3261, June, 2002.
- Schulzrinne H, Rosenberg J. (2000). The Session Initiation Protocol: Internet-Centric Signaling. IEEE Communications Magazine, 2000, (3): 134-141.
- A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers. (2003). Session Initiation Protocol(SIP) Basic Call Flow Examples. RFC 3665, December, 2003. 82.
- M. Handley, V. Jacobson. (1998). SDP: Session Description Protocol. RFC 2327, April, 1998.
- H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. (2003). RTP: A Transport Protocol for Real-Time Applications. RFC 3550, July, 2003.
- P. Srisuresh, M. Holdrege. (1999). IP Network Address Translator(NAT). RFC 2663. IETF. 1999.8.
- J. Rosenberg, J. Weinberger, C. Huitema. (2003). STUN—Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). RFC 3489. IETF. 2003.4
- Alan B. Johnston. SIP—Understanding the Session Initiation Protocol Second Edition Section 3-3, 2004: section 3.3.
- J. Rosenberg. (2006). Traversal Using Relay NAT (TURN) draft-rosenberg-midcom-turn-08, May, 2006.
- Rosenberg. Interactive connectivity establishment(ICE): A methodology for network address translator (NAT) traversal for the session initiation protocol (SIP) [EB/OL].
- <http://www.jdrosen.net/papers/draft-rosenberg-sipping-ice-00.html>.

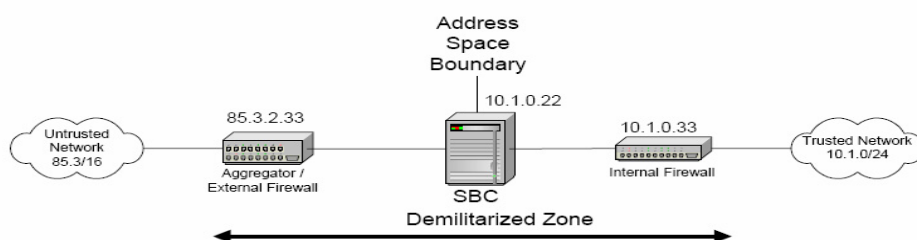


Figure 1. SBC does firewall processing

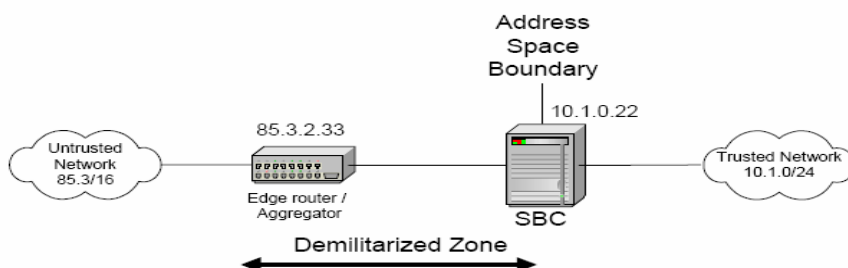


Figure 2. SBC does firewall processing

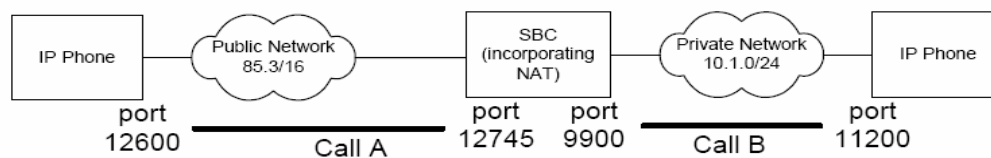


Figure 3. VoIP media packets traversing the DMZ