LANCOM White Paper
Session Border Controller

New security requirements due to All-IP

With the move from legacy ISDN connections to All-IP, multimedia and associated signaling data are now joining the ranks of IP-based applications and the general data traffic. A consequence of this are various additional demands on the network infrastructure: These include a VoIP-enabled router that supports the Annex J standard, the use of suitable Quality-of-Service mechanisms and, importantly, the need to verify your network security. A firewall is absolutely essential for securing IP networks, be it integrated into the router or as a separate network component. This protects the network from unauthorized access, monitors the traffic passing through it and applies rules to decide whether certain data packets are allowed through.

However, firewalls are not adequately able to handle SIP-based voice packets (Voice over IP) because the ports used are negotiated dynamically and the packets are transmitted in the payload. Simply opening up all ports for VoIP and multimedia applications is not a good idea considering that VoIP terminals and "mini-computers" connected to the outside world offer full access to the corporate network—particularly if, after manipulation, they offer an easy means for intercepting and recording conversations by means of externally activated microphones, for example.

To counteract this potential vulnerability, a secure separation of the (insecure) external network from the (secure) internal network is essential. This job description matches exactly to what a session border controller does.

How it works

As the name "session border controller" (SBC) implies, it is placed at the borders of the network and controls the connection and disconnection of sessions (fig. 1).

Unlike a firewall, an SBC is able to inspect, control, and manage real-time SIP communication in terms of the signaling data (control plane) and the voice/media data (data plane) at the network boundary. It manages the establishment, connection and disconnection of telephone calls and the associated data streams for signaling and media (voice or video).

Working as a proxy for SIP communication, an SBC initially acts as an endpoint for every session, such as an external incoming call, and then sets up a new session for the internal component of the call. This process inspects, validates and, if applicable, transforms the signaling data and media streams. This is where the advantages of an SBC in terms of security and quality come into play:

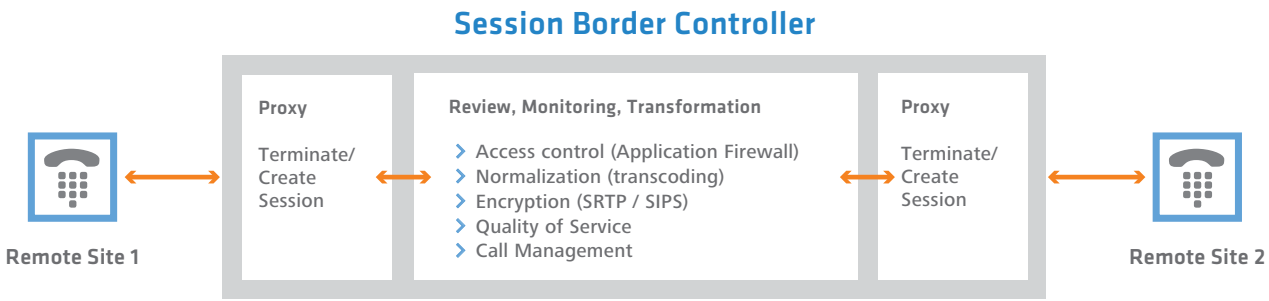

Fig. 1: How a session border controller works

LANCOM Systems

Security

Sessions incoming to and outgoing from the SBC are terminated and validated on layer 5 (SIP). Only known and supported control commands are forwarded. As an application firewall, the SBC provides access protection for voice, video and multimedia. It monitors allowed sessions and conceals their topological origins, such as the internal IP addresses of servers and phones. Furthermore, the SBC ensures the confidentiality of real-time voice data by protecting against interception, recording, and man-in-the-middle attacks. It optionally uses encryption and checksums (Secure Real-Time Transport Protocol, SRTP) provided that the remote site—e.g. an SBC on the provider side—is able to decrypt the encrypted SIP packets again. Similarly, outgoing signaling data is encrypted by TLS (Session Initiation Protocol Secure, SIPS) and decrypted upon receipt.

Quality

Although SIP is an IP-based protocol, it is not implemented uniformly: In practice, manufacturers and providers implement the SIP standard in very different ways, for example by using proprietary headers in SIP packets. In the worst case, the PBX system could interpret the unknown parameters of an incoming session to be part of an attack and drop the session altogether. A session border controller recognizes all types of SIP headers and "normalizes" them for the underlying PBX system, so ensuring cross-provider and multi-vendor interoperability.

A similar situation exists with the various codecs used or supported by the remote terminals. An SBC detects which codecs are supported by the participating PBXs, whether there are codecs in common, or whether transcoding is required in order to use a common codec. For example, if one of the two remote terminals is a modern HD-voice-capable PBX system and the other is a legacy ISDN system, a conversion between HD-Voice and the G.711 codec is necessary. The SBC handles this mediation for each session and selects the most efficient communication path or the best available codec available at both ends.

When it comes to fax transmission in mixed environments with an IP peer and an ISDN peer, an SBC can detect whether or not the remote terminal supports the IP-based fax protocol T.38. If not, it transcodes the fax packet into the ISDN-based T.30 to make the fax transmission work smoothly.

Furthermore, the SBC reserves the Internet bandwidth that VoIP calls require (Quality of Service) to ensure a high quality of the call. Emergency calls are recognized as such and prioritized over other telephony sessions.

In concert with the Voice Call Manager (VCM)

In practice the SBC works closely with another VoIP component, the Voice Call Manager. This refers to the components required for PBX features, for managing terminals, telephone-number mapping and manipulation, and the call-routing table.

This role is traditionally handled by a PBX system with the central task of assigning a call to a specific line or a specific terminal. This involves the dialed numbers being manipulated, resolved and forwarded to the called party in accordance with the rules defined in a call-routing table. An ongoing call can be manipulated and forwarded using commands such as hold call, swap call, or transfer call. Especially for smaller scenarios, these call-management functions often make the operation of a separate PBX superfluous.

Session border controller in action

In principle, a session border controller acts as an interface between the router/firewall and the internal telephony infrastructure. In corporate environments, the latter is usually a central PBX system. Increasingly, companies are relying on external, cloud-based PBXs to manage their telephony. The following illustration (fig. 2) shows a network topology where the firewall, SBC, router, and PBX system are operated as separate components.

A more elegant and slim-line solution (fig. 3) consists of a highly integrated business router that includes the functions of a firewall and a session border controller. In this case, the router is the foremost device on the network; it manages all of the data traffic and it implements the firewall rules. It acts as a SIP gateway between the PBX system and the All-IP network; acting as a session border controller it securely separates the internal and external networks, and it manages the QoS.

Fig. 4 illustrates the complete integration of all of these functions into a single router, where the VCM also handles the central functions of a PBX system. This scenario is particularly suitable for smaller companies.

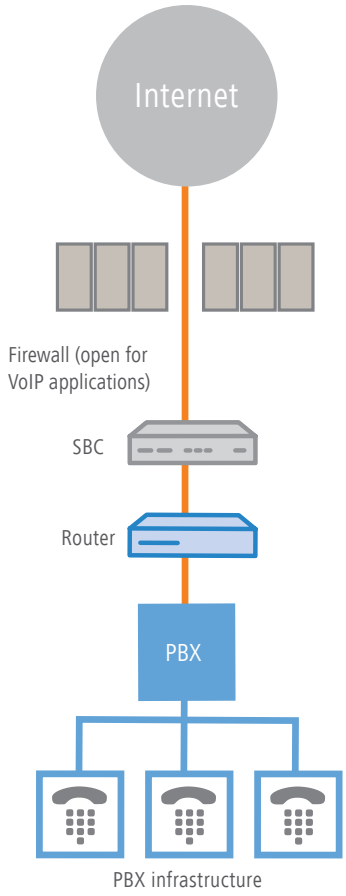

Fig. 2: Network topology with separate components for medium-sized and large networks

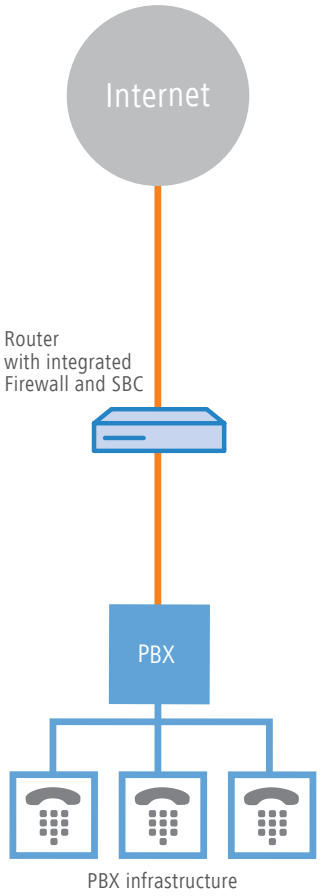

Fig. 3: Router with integrated firewall and SBC for medium and large networks

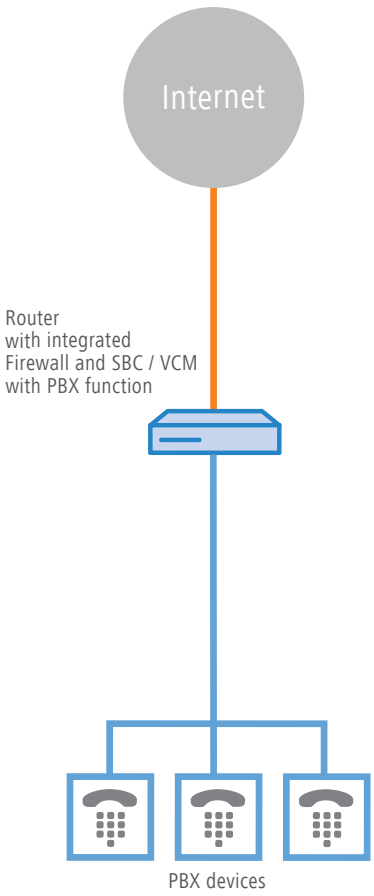

Fig. 4: Router with integrated firewall and SBC/VCM with PBX functions for small networks

Unequivocal recommendation

The German Federal Office for Information Security strongly recommends using the slim-line solution described above: In a publication dated August 2014 and outlining their technical guidelines for internal organization telecommunication systems with higher security requirements, they made a general recommendation for companies to use an SBC as a peripheral device between the WAN connection and internal PBX system or provider. They also issued the following explanation or restriction that applies to smaller organizations and smaller sites: "For smaller sites in particular, integrated devices can be used to simultaneously manage the firewall, SBC, and the Internet or WAN connection. The issue of availability must be considered here."

(German Source: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/TKAnlagen/TLSTK_II-Teil_2%E2%80%93Sicherheitskonzepte.pdf?__blob=publicationFile&v=1)

Summary

A session border controller is an essential part of secure and reliable business telephony because it securely separates the private network from the outside world, especially in the context of VoIP. When planning a network, the use of a suitable SBC is an important consideration. Integrated devices combine the features of the router, voice-call manager, firewall and SBC in a single device, thus minimizing the costs of purchase, installation, operation and maintenance.

In particular for companies with sensitive data communications and complex telephony infrastructures, a session border controller is a core element for security and reliable telephony.