

SBC - Session Border Controller

Studio di fattibilità finanziato dal Parco Scientifico e Tecnologico della Liguria
 Docup Obiettivo 2 (2000–2006), Misura 3.7, Sottomisura D Diffusione e Trasferimento dell'Innovazione

Un Session Border Controller (SBC) è un apparato posto ai bordi delle reti IP allo scopo di controllare il traffico relativo sia alla segnalazione che ai flussi dati di sessioni di comunicazione audio e/o video ed in generale di sessioni multimediali.

Il controllo della segnalazione si esprime principalmente in funzioni relative all'autorizzazione delle richieste di servizio, alla tariffazione del servizio richiesto ed in generale in funzioni relative al controllo ed alla intercettazione del traffico ai fini della sicurezza.

Il controllo dei flussi di dati audio/video si esprime principalmente in funzioni di configurazione automatica e dinamica dei dispositivi di rete preposti al filtraggio del traffico (firewall) ma anche nelle tipiche funzionalità di sicurezza svolte ai bordi delle reti come ad esempio la difesa da attacchi di tipo Denial of Service (DOS), il supporto all'attraversamento dei dispositivi che attuano il NAT (Network Address Translation), la gestione della Qualità del Servizio (QoS), il controllo delle congestioni ed il controllo della banda assegnata.

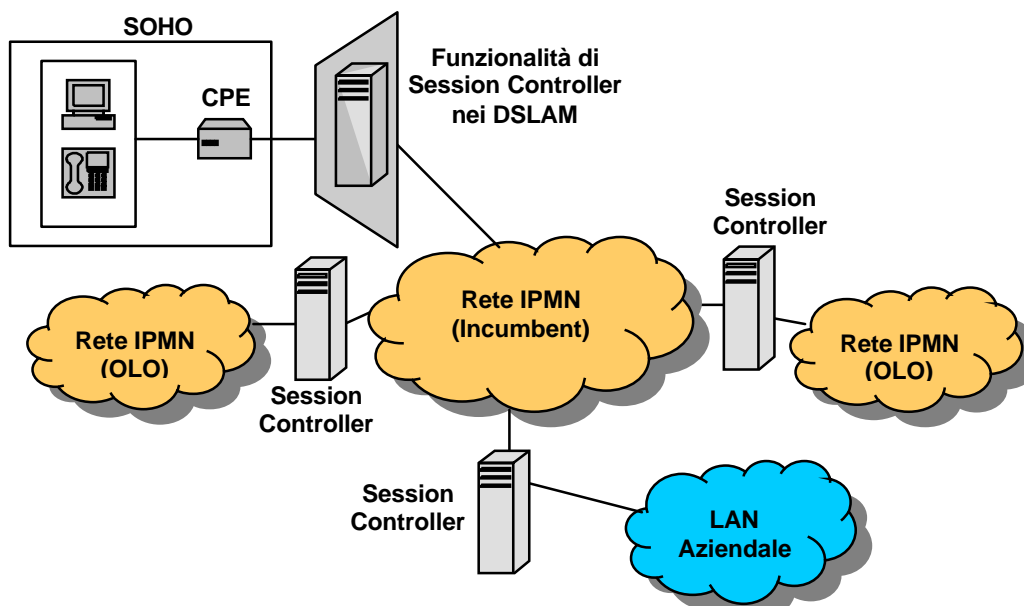
La figura sottostante illustra gli scenari di utilizzo per un SBC che può essere collocato sia nei punti di accesso alla rete del network provider da parte dell'utenza residenziale ed aziendale sia nei punti di interconnessione fra network provider.

Il compito principale di un SBC è quello di proteggere sia le reti dell'utenza che le reti di accesso e di dorsale del provider. Questo compito viene svolto agendo a livello delle singole sessioni ed attuando quindi il controllo di ogni singola comunicazione che attraversi i bordi della rete.

La particolare specificità dei servizi VoIP e più in generale dei servizi multimediali su reti IP ha condotto a suddividere l'architettura di un SBC in due elementi principali: il primo elemento è dedicato ad analizzare il traffico relativo alla segnalazione (signaling plane) mentre il secondo è dedicato al controllo del traffico dati multimediale (media plane).

Il *signaling plane* gestisce la registrazione degli utenti, l'autorizzazione degli utenti e l'autorizzazione di ogni sessione tipicamente realizzate mediante protocollo SIP.

Il *media plane* gestisce il traffico dati veicolato tramite protocollo RTP/RTCP assicurando che venga filtrato tutto il traffico che non appartenga a sessioni già instaurate e comunque solo a quelle configurate dal signaling plane.



Più in dettaglio un Session Border Controller svolge i seguenti compiti:

Admission Control - Un SBC è in grado di analizzare il traffico sia a livello di rete che a livello applicativo e di configurare dinamicamente gli apparati firewall per consentire il passaggio del traffico di segnalazione e del traffico dati esclusivamente in corrispondenza degli indirizzi e delle porte strettamente necessari e solamente per la durata delle sessioni autorizzate.

Nell'elemento denominato signaling plane un SBC identifica e controlla il traffico di segnalazione proveniente dalle reti residenziali e aziendali e relativo alla registrazione degli utenti costituendo ed aggiornando continuamente la lista degli utenti autorizzati. Sulla base di questa lista il signaling plane è in grado di controllare il traffico di segnalazione proveniente da utenti autorizzati ed di generare opportuni comandi di configurazione che realizzano l'apertura e la chiusura delle porte corrispondenti negli apparati firewall sia per consentire il passaggio del traffico di segnalazione che il passaggio del traffico multimediale relativo alle sessioni autorizzate. Tutto il traffico non riconosciuto ed autorizzato viene in questo modo bloccato azzerando o limitando al minimo i rischi di attacchi.

Topology hiding - Un SBC contribuisce a rafforzare la sicurezza delle reti sia dell'operatore che dell'utenza separando fisicamente le due reti e ponendosi come unico canale di comunicazione fra di loro. Questa funzionalità di sicurezza implica in modo particolare la possibilità di nascondere completamente qualsiasi informazione sulla topologia delle reti presente all'interno dei messaggi di controllo delle sessioni e quindi di rendere il traffico di segnalazione anonimo.

Infatti i messaggi di segnalazione possono attraversare differenti domini durante il loro percorso verso la destinazione e, a causa della natura del protocollo SIP, possono accumulare al loro interno informazioni sulle reti e sui dispositivi attraversati come ad esempio gli indirizzi di rete degli apparati. Un SBC può nascondere tali informazioni rimuovendole ove possibile oppure sostituendole riuscendo quindi a garantire che il traffico di segnalazione non contenga informazioni sensibili sulle reti attraversate con particolare riferimento agli indirizzi di rete, tipicamente provata, utilizzati dagli apparati.

Firewall and NAT traversal - Le reti dell'utenza sono tipicamente protette da apparati firewall che filtrano e limitano il traffico per ragioni di sicurezza. Inoltre è frequente la presenza e l'utilizzo di tecniche NAT/PAT sui firewall sia per ragioni di sicurezza che di riutilizzo degli indirizzi di rete pubblici. Normalmente questi apparati consentono il passaggio solomamente ai pacchetti appartenenti a sessioni iniziate dall'interno della rete protetta e li bloccano se appartenenti ad una sessione iniziata al suo esterno.

In un contesto VoIP questi apparati rappresentano un notevole ostacolo perchè le sessioni sono necessariamente iniziate dall'esterno delle reti protette dai firewall e nessun utente o amministratore di rete è giustamente disposto a modificare tale politica di sicurezza.

Un SBC consente di superare tale ostacolo mantenendo costantemente attiva una connessione con l'utente che si è registrato presso il SBC ed è quindi in grado di garantire costantemente la raggiungibilità mediando la segnalazione proveniente dall'esterno delle reti protette da firewall che altrimenti verrebbe bloccata.

Quality of Service - Un SBC è in grado di realizzare meccanismi che garantiscano adeguati livelli di qualità del servizio sia all'utenza che agli operatori principalmente avendo cura di evitare situazioni di congestione del traffico nelle reti.

Questo risultato si ottiene sia in alla realizzazione di meccanismi di Controllo di Ammissione per ogni nuova sessione che siano basati sulla conoscenza dello stato di occupazione della rete, sia grazie alle funzioni di controllo del traffico di segnalazione allo scopo di contrastare ed impedire attacchi di tipo Denial of Service. Inoltre il controllo viene effettuato anche sui flussi multimediali allo scopo di garantire che la banda utilizzata dall'utenza non sia superiore a quella richiesta e concessa ovvero allo scopo di garantire usi impropri della rete.

Lo studio ha consentito di definire con precisione le funzionalità che un SBC deve realizzare, di identificare gli scenari del suo utilizzo e conseguentemente di fornire gli elementi per la definizione delle caratteristiche che i prodotti che ne incorporano le funzionalità, tipicamente apparati dedicati e/o componenti software, devono avere per potersi collocare a vari livelli nel mercato dei sistemi per la sicurezza delle reti.