



CISCO IOS Firewall

Studiu de caz

Documentul este disponibil la adresa web <http://www.otos.ro/>



contact@otos.ro

CISCO IOS Firewall

Un sistem firewall reprezinta o bariera intre reseaua interna si reseaua internet, menit sa protejeze resursele intranet, sa controleze si sa monitorizeze accesul la si dinspre reseaua interna.

Cisco IOS Firewall, alaturi de Network Address Translation (NAT), Quality of Service (QoS) si IP security (IPSec) constituie o componenta importanta a infrastructurii de securitate a retelei.

CISCO IOS Firewall include urmatoarele functii:

- filtrarea traficului IP si protejarea retelei impotriva atacurilor din exterior;
- filtrarea traficului la nivelul aplicatie;
- controlul accesului la resurse pe baza informatiilor furnizate de serviciul de AAA (**A**uthentication, **A**uthorization, and **A**ccounting);

Stateful Packet Inspection (**SPI**) reprezinta componenta de baza a CISCO IOS Firewall. SPI asigura detectia si protectia impotriva atacurilor DoS, ca de exemplu: scanarea porturilor, initializarea abuziva de conexiuni TCP (SYN Flooding), trimiterea de pachete modificate cu scopul de a bloca accesul legitim la servicii.

CISCO IOS Firewall este capabil sa trimita alerte in timp real, sa semnaleze si sa preintampine utilizarea nelegitima a resurselor.

Accesul din internet la resursele intranet poate fi protejat prin utilizator si parola si actiunile utilizatorilor inregistrate cu ajutorul serviciului de AAA (authentication, authorization, and accounting).

CISCO IOS Firewall ofera analiza traficului la nivelul aplicatie, preintampina utilizarea abuziva a unora dintre cele mai cunoscute servicii: HTTP (Hypertext Transfer Protocol), POP (Post Office Protocol), IMAP (Internet Message Access Protocol), SMTP (Simple Mail Transfer Protocol).

Exemple de implementare a CISCO IOS Firewall

Exemplul 1

Angajatii au acces securizat la resursele companiei aflate in sediul central.

Vizitatorii au acces doar la reseaua internet.

Aplicatiile P2P (DC++, Torent) si aplicatiile de chat pot fi restrictionate.

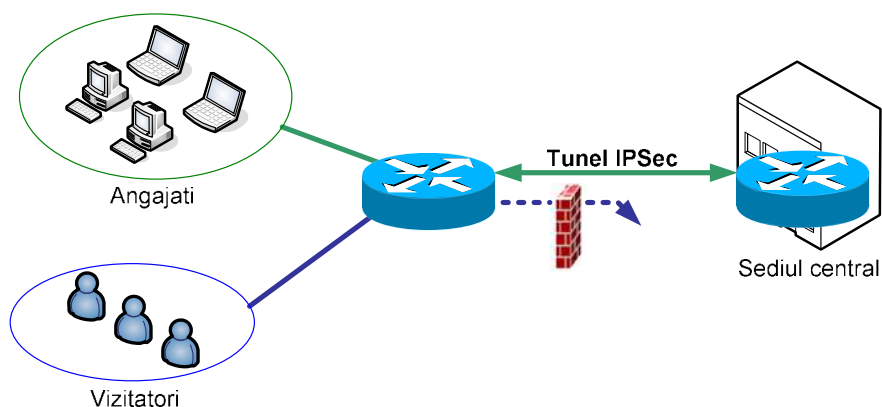


Figura 1: CISCO IOS Firewall – Exemplul 1

Exemplul 2

Angajatii au acces securizat la resursele companiei aflate in sediul central.

Vizitatorii au acces doar la reseaua internet.

Aplicatiile P2P (DC++, Torent) si aplicatiile de chat pot fi restrictionate.

Traficul catre serverele WEB este analizat, asigura protectia impotriva atacurilor DoS.

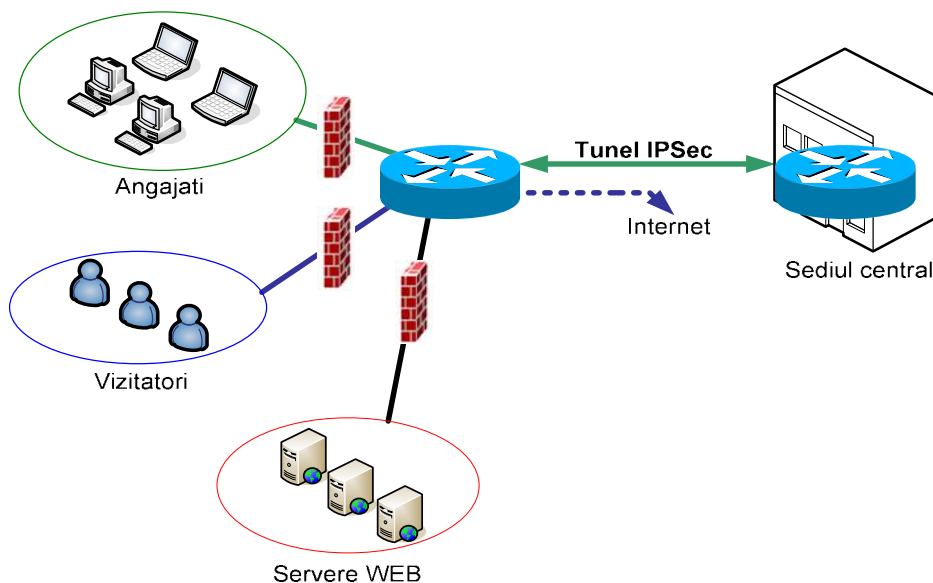


Figura 2: CISCO IOS Firewall – Exemplul 2

Exemplul 3

Accesul angajatilor la serverele WEB se face cu o autentificare prealabila, autentificare gestionata de catre serverul care asigura serviciul de AAA.

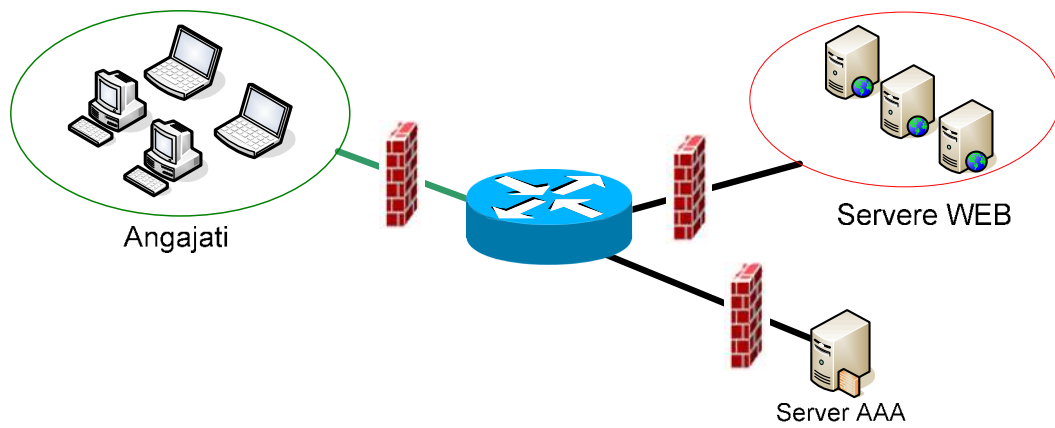


Figura 3: CISCO IOS Firewall – Exemplul 3