

PIX Firewall

Studiu de caz

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



contact@otos.ro

PIX Firewall

Sistemul firewall reprezinta prima bariera in calea atacurilor informatice. Sistemul firewall asigura respectarea politicilor de securitate pentru controlul accesului la resursele protejate.

Sistemele PIX Firewall furnizeaza servicii avansate de tip firewall implementate in diverse puncte ale retelei pentru a asigura respectarea politicilor de securitate.

Sistemele PIX Firewall reprezinta solutia firewall CISCO dedicata, folosita in mediile cu o nevoie mare de securitate, fiabilitate si putere de calcul.

Algoritmii de securitate adaptivi (CISCO Adaptive Security Algorithm) asigura analiza si supravegherea sesiunilor TCP prin identificarea sursei, a destinatiei si a porturilor, a succesiunii pachetelor TCP. Accesul prin sistemul firewall este permis doar conexiunilor validate.

CISCO PIX Firewall permite filtrarea traficului la nivelul aplicatie, utilizand algoritmi de analiza pentru cele mai folosite aplicatii: HTTP, FTP, SMTP, H.323, SIP. Deasemenea este posibila blocarea aplicatiilor Java, Javascript si ActivX.

Prin intermediul functiei "cut-through proxy", folosind pentru autentificare aplicatiile HTTP, HTTPS, FTP sau Telnet, sistemul PIX Firewall poate oferi acces temporar, pentru utilizatorii autentificati, la resursele protejate.

CISCO PIX Firewall permite creare de tunele IPSec pentru transportul criptat al datelor prin retea publică între mai multe puncte de prezență ale companiei, sau între sediul companiei și angajați.

Sistemul IDS (Intrusion Detection System) permite anticiparea și oprirea atacurilor DoS prin sistemele de alertare și analiză în timp real ale traficului.

Accesul la resursele WEB poate fi restricționat cu ajutorul modulului de filtrare URL. Astfel poate fi împiedicat accesul la site-uri internet cu conținut neadecvat.

CISCO PIX Security Appliance VPN & DMZ

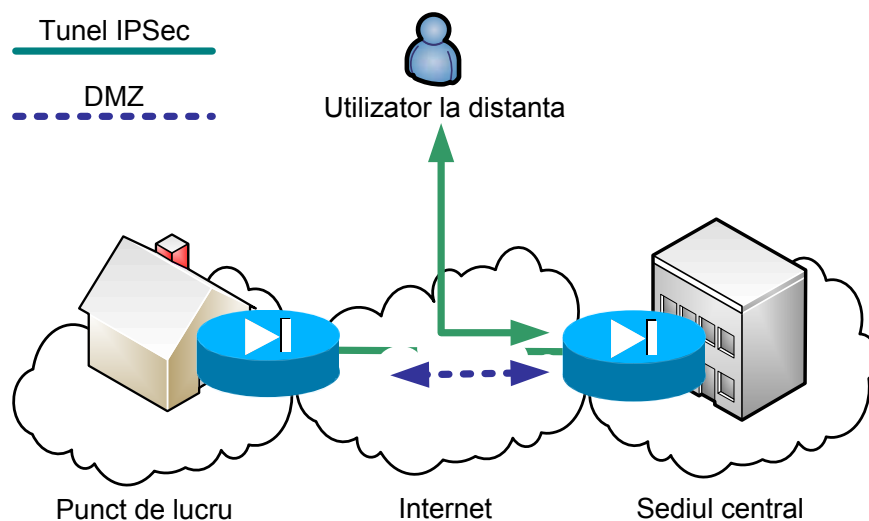


Figura 1: CISCO PIX Security Appliance VPN & DMZ

Tunelul IPSec asigura accesul criptat la resursele intranet ale companiei prin intermediul rețelei publice internet.

Zona demilitarizata (DMZ) este folosita pentru conectarea serverelor de servicii destinate accesului public.

Avantajele solutiei sunt urmatoarele:

1. Accesul sigur la resursele intranet;
2. Separarea serviciilor publice de cele protejate;
3. Viteza ridicata de procesare a informatiei;
4. Fiabilitatea software si hardware;
5. Numar mare de sesiuni simultane.