

## Firewalls i VPNs

---

Visió general.....	2
Seguretat perimètrica.....	2
VPNs o túnels segurs.....	3
Proxy cache i proxy transparent.....	4



especialistes en codi obert

## Visió general

---

Genos instal·la i administra servidors de comunicacions basats en Linux, amb un èmfasis especial en les arquitectures que poden ser instal·lades en cluster o alta disponibilitat.

Existeixen diferents aspectes a considerar quan s'examina la seguretat de les comunicacions:

- seguretat perimètrica: permetre des de la nostra xarxa i cap a la nostra xarxa només aquelles connexions permeses, per evitar accessos d'intrusos des de xarxes públiques
- connexions segures de baix cost a través de xarxes públiques entre xarxes privades situades en seus remotes (túnel IPsec LAN-to-LAN), o VPNs (*Virtual Private Network*)
- connexió segura a la xarxa privada des de xarxes públiques com Internet, a través de túnels d'usuari (IPsec amb certificat o Microsoft L2TP), amb validació contra un directori LDAP o Active Directory a través d'un servidor Radius

Així mateix, també s'inclouen paràmetres relacionats amb la qualitat de servei de les comunicacions i control del seu ús, com:

- QoS (*Quality of Service*) o prioritització de determinats tipus de tràfic
- Proxy cache (i proxy transparent)
- Monitoratge del tràfic de xarxa

## Seguretat perimètrica

---

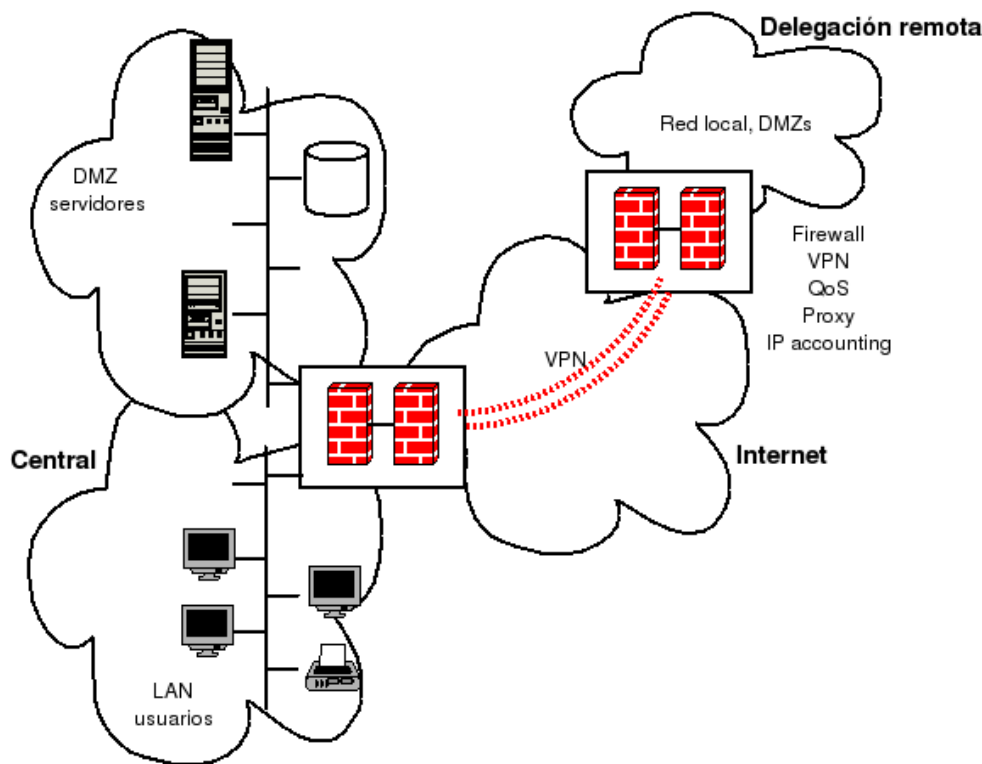
La funció bàsica d'un firewall és la de protegir la xarxa interna d'accessos no desitjats des de l'exterior.

Per això, els firewalls realitzen tasques de filtratge de paquets i d'enrutat, i altres funcions més complexes com translacions de ports i NATs (*Network Address Translation*).

Genos instal·la firewalls basats en Linux que proporcionen un nivell de seguretat molt elevat, alt rendiment i elevades prestacions inclús en servidors de gama baixa.

Aquests firewalls donen serveis de:

- filtratge de connexions entrants i sortints, *packet filtering*, *connection tracking*, NAT
- routing
- routing avançat (balanceig de tràfic a través de múltiples routers, enrutat dinàmic BGP, *failover* de línies de connexió)
- logging de connexions i tràfic
- IP accounting
- possibilitat de configuració en alta disponibilitat



## VPNs o túnel segurs

Les VPNs s'utilitzen per crear xarxes segures a través de xarxes públiques (i per tant insegures) com Internet. Aquest mecanisme permet connectar punts remots amb un cost baix i amb un protocol que garanteix la confidencialitat de la informació.

Les comunicacions utilitzen el protocol IPSec per a l'encriptació forta de les dades i garanteix la seva seguretat i integritat.

IPSec actua a nivell IP de la capa de xarxa i per tant es capaç de protegir tot el tràfic IP, independentment de l'aplicació que estigui generant el tràfic. A més a més, al tractar-se d'un protocol estàndard, és possible connectar-se amb sistemes d'altres fabricants com Cisco.

Els túnel IPSec poden establir-se també amb usuaris mòbils Linux o Windows que accedeixen als recursos de la xarxa corporativa interna a través d'una xarxa pública com Internet. La identitat dels usuaris es garanteix mitjançant certificats X.509 (clau pública, clau privada) i validació de login i password contra un directori LDAP o servidor d'Active Directory utilitzant com a passarel·la un servidor Radius instal·lat en el mateix gestor de VPNs.

Les configuracions de VPN en alta disponibilitat garanteixen que el temps de disponibilitat de les comunicacions sigui màxim.



especialistes en codi obert

---

## Proxy cache i proxy transparent

---

Un proxy és un sistema que permet accelerar l'accés a Internet de determinats protocols i reduir l'ample de banda utilitzat. Per tant, permet obtenir un millor rendiment utilitzant menys recursos.

Els proxies realitzen aquesta funció emmagatzemant còpies de les dades descarregades d'Internet (cache) de forma que si un altre usuari vol accedir a la mateixa informació ja no és necessari tornar-la a descarregar. Els proxies fan cache de les peticions a través del protocol HTTP, és a dir, de pàgines web i de tots els seus continguts (HTML i imatges).

Per a que els usuaris utilitzin el proxy cache és necessari configurar adequadament el navegador d'internet de cada màquina. Aquesta configuració local pot realitzar-se a través de polítiques de domini Windows o pot evitar-se utilitzant un proxy transparent.

El proxy transparent permet que totes les peticions web dels usuaris siguin enviades automàticament a través del proxy de forma totalment imperceptible per als usuaris.

El servidor incorpora un potent gestor d'ACLs (*Access Control List*) per a un control exhaustiu de qui està accedint a través del proxy i a quines pàgines, i pot integrar-se amb productes d'antivirus per comprovar tots els arxius descarregats pels usuaris.