

Firewalls y VPN

Contenidos

Contenidos	1
Visión general	2
Seguridad perimetral	2
VPNs o túneles seguros	3
Proxy cache y proxy transparente	3

Visión general

Genos instala y administra servidores de comunicaciones basados en Linux con un énfasis especial en aquellas arquitecturas que pueden ser instaladas en clúster o alta disponibilidad.

Existen distintos aspectos a considerar cuando se examina la seguridad de las comunicaciones:

- seguridad perimetral: permitir desde nuestra red y hacia nuestra red sólo aquellas conexiones permitidas, para evitar accesos de intrusos desde redes públicas
- conexiones seguras de bajo coste a través de redes públicas entre redes privadas ubicadas en sedes remotas (túneles IPSec LAN-to-LAN), o VPNs (Virtual Private Network)
- conexión segura a nuestra red privada desde redes públicas como Internet, a través de túneles de usuario (IPSEC con certificado o Microsoft L2TP), con validación contra un directorio LDAP o Active Directory a través de un servidor Radius.

Así mismo, también se incluyen parámetros relacionados con la calidad de servicio de las comunicaciones y control de su uso, como:

- QoS (Quality of Service) o priorización de determinados tipos de tráfico
- Proxy cache (y proxy transparente)
- Monitorización del tráfico de red

Seguridad perimetral

La función básica de un firewall es la de proteger la red interna frente a accesos no deseados desde el exterior.

Para ello, los firewalls realizan tareas de filtro de paquetes y de enrutado, y otras funciones más complejas como traslaciones de puertos y NATs (Network Address Translation).

Genos instala firewalls basados en Linux que proporcionan un nivel de seguridad muy elevado, alto rendimiento y elevadas prestaciones incluso en servidores de gama baja.

Estos firewalls proporcionan servicios de:

- filtraje de conexiones entrantes y salientes, packet filtering, connection tracking, NAT
- routing
- routing avanzado (balanceo de tráfico por múltiples routers, enrutado dinámico BGP, failover de líneas de conexión)
- logging de conexiones y tráfico
- IP accounting
- posibilidad de configuración en alta disponibilidad

VPNs o túneles seguros

Las VPNs se utilizan para crear redes seguras a través de redes públicas (y por tanto inseguras) como Internet.

Este mecanismo permite conectar puntos remotos con un coste bajo y con un protocolo que garantiza la confidencialidad de la información.

Las comunicaciones usan el protocolo IPSec para la encriptación fuerte de los datos y garantiza su seguridad e integridad.

IPSec actúa a nivel IP de la capa de red. Por lo tanto, es capaz de proteger todo el tráfico IP, independientemente de la aplicación que esté generando el tráfico. Además, al tratarse de un protocolo estándar, es posible interoperar con otros sistemas como Cisco.

Los túneles IPSec pueden establecerse también con usuarios móviles Linux o Windows que acceden a los recursos de la red corporativa interna a través de una red pública como Internet. La identidad de los usuarios se garantiza mediante certificados X.509 (clave pública, clave privada) y validación de login y password contra un LDAP o servidor de Active Directory usando como pasarela un servidor Radius instalado en el mismo gestor de VPNs.

Las configuraciones de VPN en alta disponibilidad garantizan que el tiempo de disponibilidad de la conexión sea máximo.

Proxy cache y proxy transparente

Un proxy es un sistema que permite acelerar el acceso a Internet de determinados protocolos y reducir el ancho de banda consumido. Por lo tanto, permite obtener un mejor rendimiento consumiendo menos recursos.

Los proxies realizan esta función almacenando copias de los datos descargados de Internet (cache) de forma que si otro usuario quiere acceder a la misma información ya no es necesario volverla a descargar. Los proxies hacen cache de las peticiones a través del protocolo HTTP, es decir, de páginas web y de todos sus contenidos (HTML e imágenes).

Para que los usuarios utilicen el proxy cache es necesario configurar adecuadamente el navegador de Internet de cada máquina. Esta configuración local puede realizarse a través de políticas de dominio Windows o evitarse utilizando un proxy transparente.

Un proxy transparente permite que todas las peticiones web de los usuarios sean redirigidas automáticamente a través del proxy de forma totalmente imperceptible para los usuarios.

El servidor proxy incorpora un potente gestor de ACL (Access Control List) para un control exhaustivo de quien está accediendo a través del proxy y a qué páginas, y puede integrarse con productos antivirus para escanear todos los archivos descargados por los usuarios.

