

## 1. Network Appliances

Gerenciar dispositivos dentro de uma rede interna é relativamente simples, mas quando há necessidade de acesso remoto, soluções seguras são essenciais. **O jump server é um dispositivo de acesso controlado dentro da rede interna que permite conexões externas seguras.** Ele funciona como um ponto intermediário entre usuários externos e os sistemas internos, exigindo **credenciais específicas e controles rígidos de autenticação** para minimizar riscos de invasão.

Outra ferramenta importante na segurança de redes é o **proxy server**. Esse dispositivo atua como intermediário entre clientes internos e a internet, possibilitando funções como **caching de dados, filtragem de URLs e análise de tráfego**. Existem diferentes tipos de proxies:

- **Proxies explícitos**, que exigem configuração manual no dispositivo do usuário.
- **Proxies transparentes**, que operam sem que o usuário perceba sua presença.

Além disso, proxies podem atuar como **forward proxies**, usados para gerenciar acessos internos à internet, ou **reverse proxies**, que protegem servidores internos ao processar requisições externas antes de encaminhá-las.

O uso de **load balancers** é outra prática essencial para redes escaláveis e resilientes. Eles distribuem tráfego entre vários servidores, garantindo **alta disponibilidade e desempenho**. Load balancers também podem fornecer **offloading de SSL**, reduzindo a carga nos servidores ao gerenciar a criptografia e descriptografia de tráfego.

Monitoramento e gerenciamento de redes dependem de **sensores e coletores**, que capturam eventos de segurança e os enviam para um **SIEM (Security Information and Event Management)**. O SIEM analisa e correlaciona logs de diferentes dispositivos, como **firewalls, IDS/IPS e servidores de autenticação**, facilitando a detecção de ameaças e falhas de segurança.

Ferramentas como **port mirroring (SPAN)** e **network taps** permitem que administradores monitorem tráfego de rede sem interferir diretamente na comunicação. Isso é útil para **análises forenses e detecção de intrusões**, garantindo que comportamentos anômalos sejam identificados rapidamente.

A combinação de **jump servers, proxies, load balancers e SIEMs** melhora significativamente a segurança e o desempenho de redes corporativas, permitindo controle eficiente de acessos e prevenção de ataques cibernéticos.