Firewall

Introdução

A segurança da rede é parte integrante da rede de computadores, independentemente de a rede estar em uma casa com uma única conexão à Internet ou se é uma corporação com milhares de usuários.

A segurança da rede deve considerar o ambiente, bem como as ferramentas e os requisitos da rede.

Ele deve poder proteger os dados e, ao mesmo tempo, permitir a qualidade do serviço que os usuários esperam da rede.

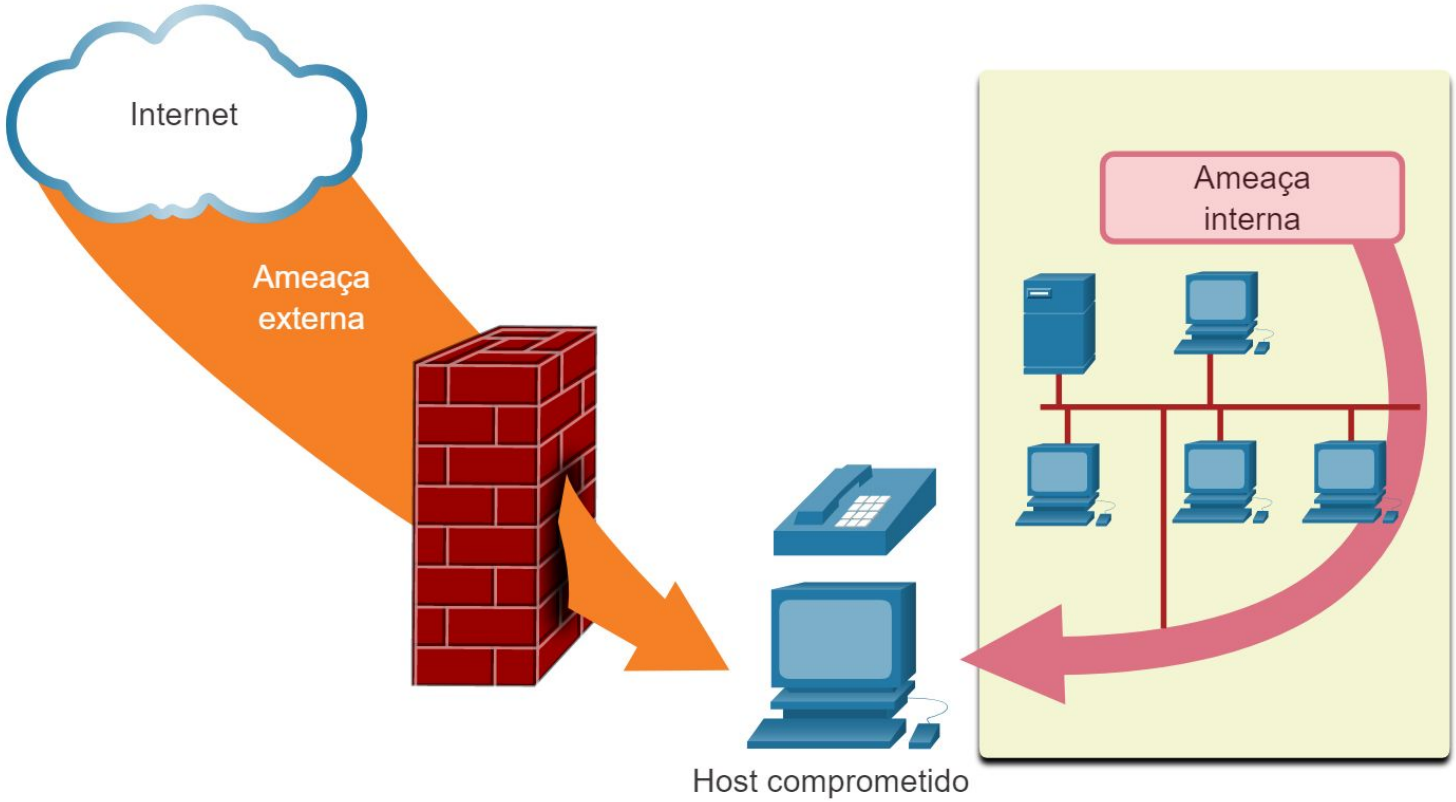
Introdução

A proteção de uma rede envolve protocolos, tecnologias, dispositivos, ferramentas e técnicas para proteger dados e mitigar ameaças. Vetores de ameaça podem ser internos ou externos. Hoje, muitas ameaças à segurança de rede externa se originam da Internet.

Exemplo de Ameaças

- **Vírus, worms e cavalos de Tróia** - Eles contêm software ou código malicioso em execução no dispositivo do usuário.
- **Spyware e adware** - Estes são tipos de software que são instalados no dispositivo de um usuário. O software, em seguida, coleta secretamente informações sobre o usuário.
- **Ataques de dia zero** - Também chamados de ataques de hora zero, ocorrem no primeiro dia em que uma vulnerabilidade se torna conhecida.
- **Ataques de ator de ameaça** - Uma pessoa mal-intencionada ataca dispositivos de usuário ou recursos de rede.
- **Ataques de negação de serviço** - Esses ataques atrasam ou travam aplicativos e processos em um dispositivo de rede.
- **Interceptação de dados e roubo** - Esse ataque captura informações privadas da rede de uma organização.
- **Roubo de identidade** - Esse ataque rouba as credenciais de login de um usuário para acessar informações privadas.

Firewall


Internet
Ameaça externa
Ameaça interna
Host comprometido

Componentes básicos de segurança

Estes são os componentes básicos de segurança para uma rede doméstica ou de pequeno escritório:

- **Antivirus e antispyware** - Esses aplicativos ajudam a proteger os dispositivos finais contra a infecção por software malicioso.
- **Filtragem por firewall** - A filtragem por firewall bloqueia o acesso não autorizado dentro e fora da rede. Isso pode incluir um sistema de firewall baseado em host que impede o acesso não autorizado ao dispositivo final ou um serviço básico de filtragem no roteador doméstico para impedir o acesso não autorizado do mundo externo à rede.

Componentes avançados de segurança

Em contrapartida, a implementação de segurança para uma rede corporativa geralmente consiste em vários componentes incorporados à rede para monitorar e filtrar o tráfego. Idealmente, todos os componentes trabalham juntos, o que minimiza a manutenção e melhora a segurança. Redes maiores e redes corporativas usam antivírus, antispyware e filtragem por firewall, mas também têm outros requisitos de segurança:

Componentes avançados de segurança

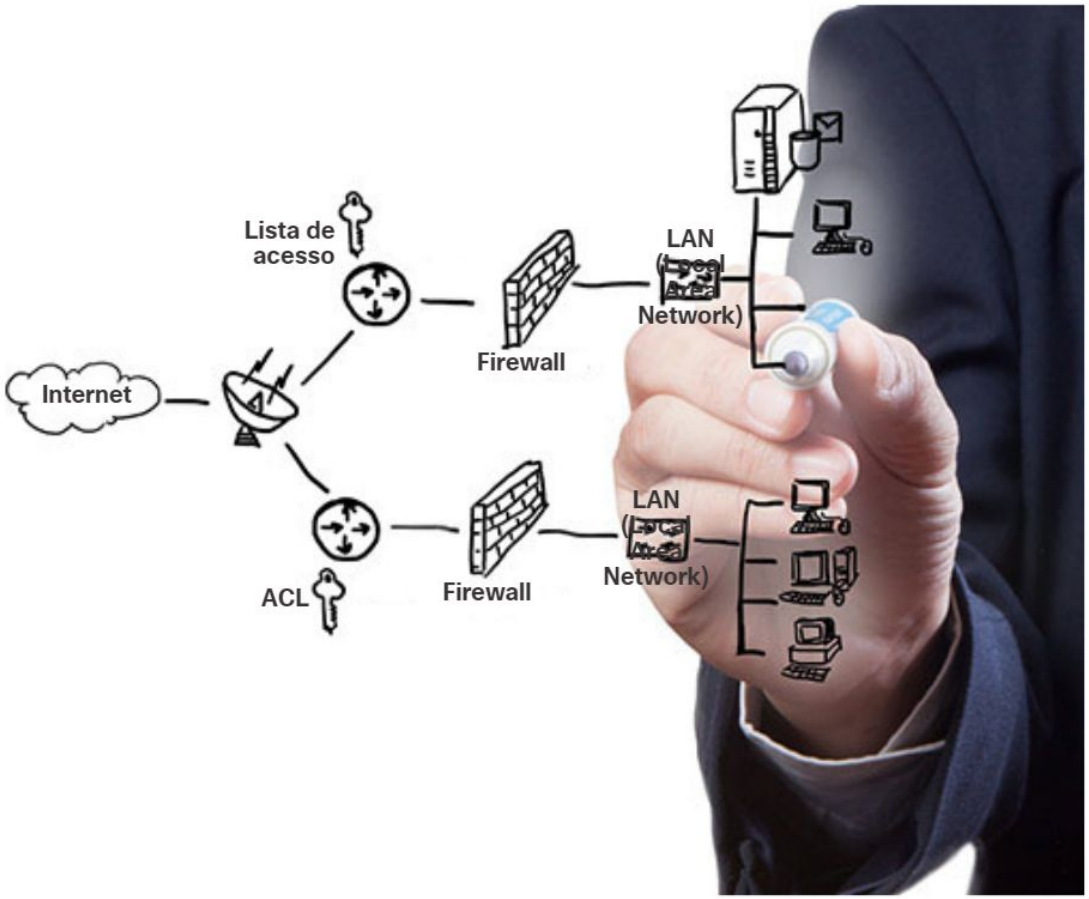
Sistemas de firewall dedicados - Eles fornecem recursos de firewall mais avançados que podem filtrar grandes quantidades de tráfego com mais granularidade.

Listas de controle de acesso (ACL) - Eles filtram ainda mais o acesso e o encaminhamento de tráfego com base em endereços e aplicativos IP.

Sistemas de prevenção de intrusões (IPS) - Identificam ameaças de rápida disseminação, como ataques de dia zero ou hora zero.

Redes privadas virtuais (VPN) - fornecem acesso seguro a uma organização para trabalhadores remotos.

Componentes de segurança



SENAI-SP

SENAI SÃO PAULO