SEGURANÇA DA INFORMAÇÃO

Firewalls

ROTEIRO

- Introdução
- O que um firewall faz e o que ele não faz
- Como funciona um firewall
- Tipos de firewalls

INTRODUÇÃO

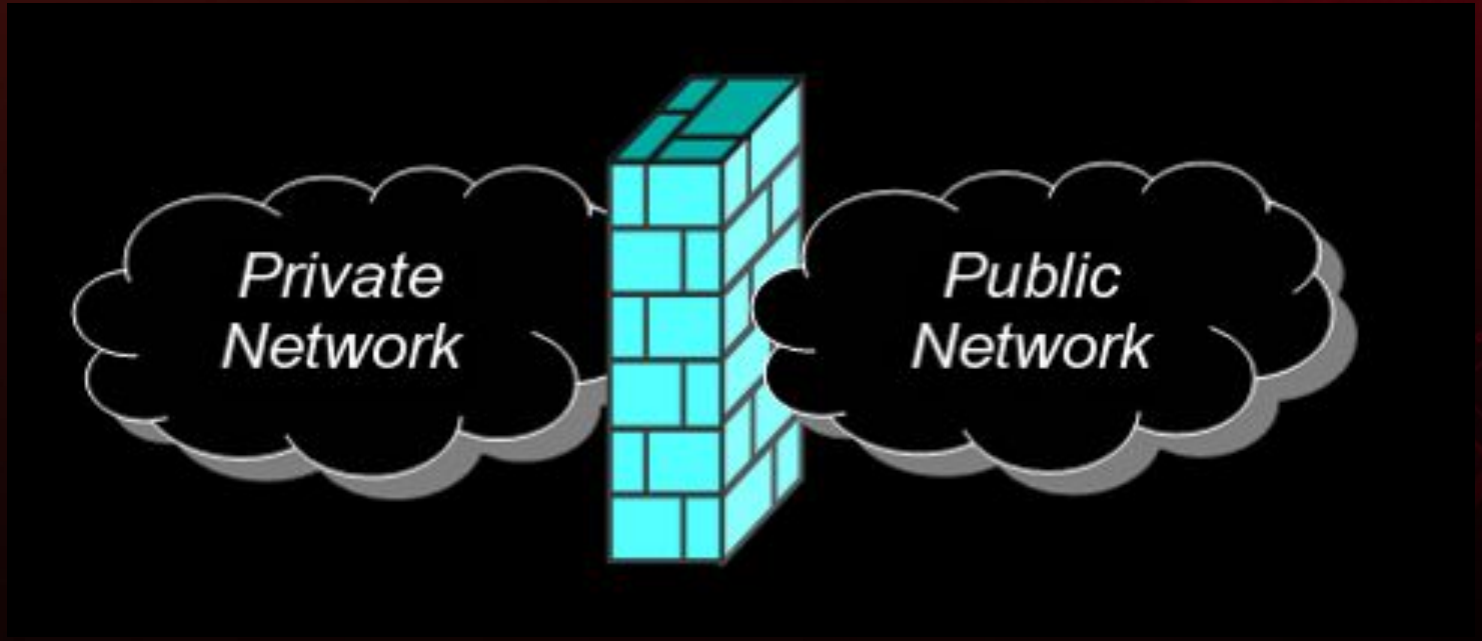
O termo foi utilizado originalmente com o objetivo de definir uma barreira construída para evitar a propagação do fogo de uma parte de um edifício ou estrutura para outra.

Os firewalls de rede fornecem uma barreira entre as redes, o que impede o tráfego indesejado ou não autorizado.

INTRODUÇÃO

Um firewall de rede é um sistema ou grupo de sistemas usado para controlar o acesso entre duas redes:

Uma rede confiável e uma rede não confiável - utilizando regras ou filtros pré-configurados.



INTRODUÇÃO

Dispositivo que fornece conectividade segura entre redes (interna/externa; níveis variados de confiança)

Usado para implementar e aplicar uma política de segurança para comunicação entre redes

Os firewalls podem ser baseados

- Em hardware e/ou software.
- Compostos por um único roteador, vários roteadores, um único sistema *host*, ou vários *hosts*, executando software de firewall

INTRODUÇÃO

Os firewalls podem ser compostos por um um ou vários roteadores, um ou vários sistemas hosts, executando o software de firewall em dispositivos de hardware projetados especificamente para fornecer serviços de firewall ou qualquer combinação deles. Eles variam muito em design, funcionalidade, arquitetura e custo.

INTRODUÇÃO

GERAÇÕES:

PRIMEIRA GERAÇÃO - filtros de pacotes

SEGUNDA GERAÇÃO - nível do circuito

TERCEIRA GERAÇÃO - camada de aplicação

- **Também conhecidos como firewalls baseados em proxy**

O QUE UM FIREWALL FAZ E O QUE NÃO FAZ

O QUE FAZ UM FIREWALL

Autenticação de usuário	Auditoria e registro
Podem ser configurados para exigir autenticação do usuário, o que permite que os administradores de rede controlem e rastreiem a atividade específica do usuário.	Ao configurar um firewall para registrar e auditar a atividade, as informações podem ser mantidas e analisadas posteriormente.

O QUE UM FIREWALL FAZ E O QUE NÃO FAZ

O QUE FAZ UM FIREWALL

Anti-Spoofing

Detecta quando a origem do tráfego de rede está sendo "*spoofed*", ou seja, quando um indivíduo tentando acessar um serviço bloqueado altera o endereço de origem na mensagem para que o tráfego seja permitido.

Network Address Translation (NAT)

Alterar os endereços de rede dos dispositivos em qualquer lado do firewall para ocultar seus endereços verdadeiros dos dispositivos em outros lados.

O QUE UM FIREWALL FAZ E O QUE NÃO FAZ

O QUE FAZ UM FIREWALL

VPNs

São sessões de comunicação que atravessam redes públicas que se tornaram virtualmente privadas por meio do uso de tecnologia de criptografia.

São definidas criando uma regra de firewall que exigem criptografia para qualquer sessão que atenda a critérios específicos.

O QUE O FIREWALL NÃO FAZ ?

O QUE O FIREWALL NÃO FAZ

Um firewall não pode e não garante que sua rede seja 100% segura.

Os firewalls não podem oferecer nenhuma proteção contra ataques internos.

Os firewalls não podem oferecer nenhuma proteção contra ataques internos.

- Grande percentual de incidentes de segurança tem origem dentro da rede confiável.

O QUE UM FIREWALL FAZ E O QUE NÃO FAZ

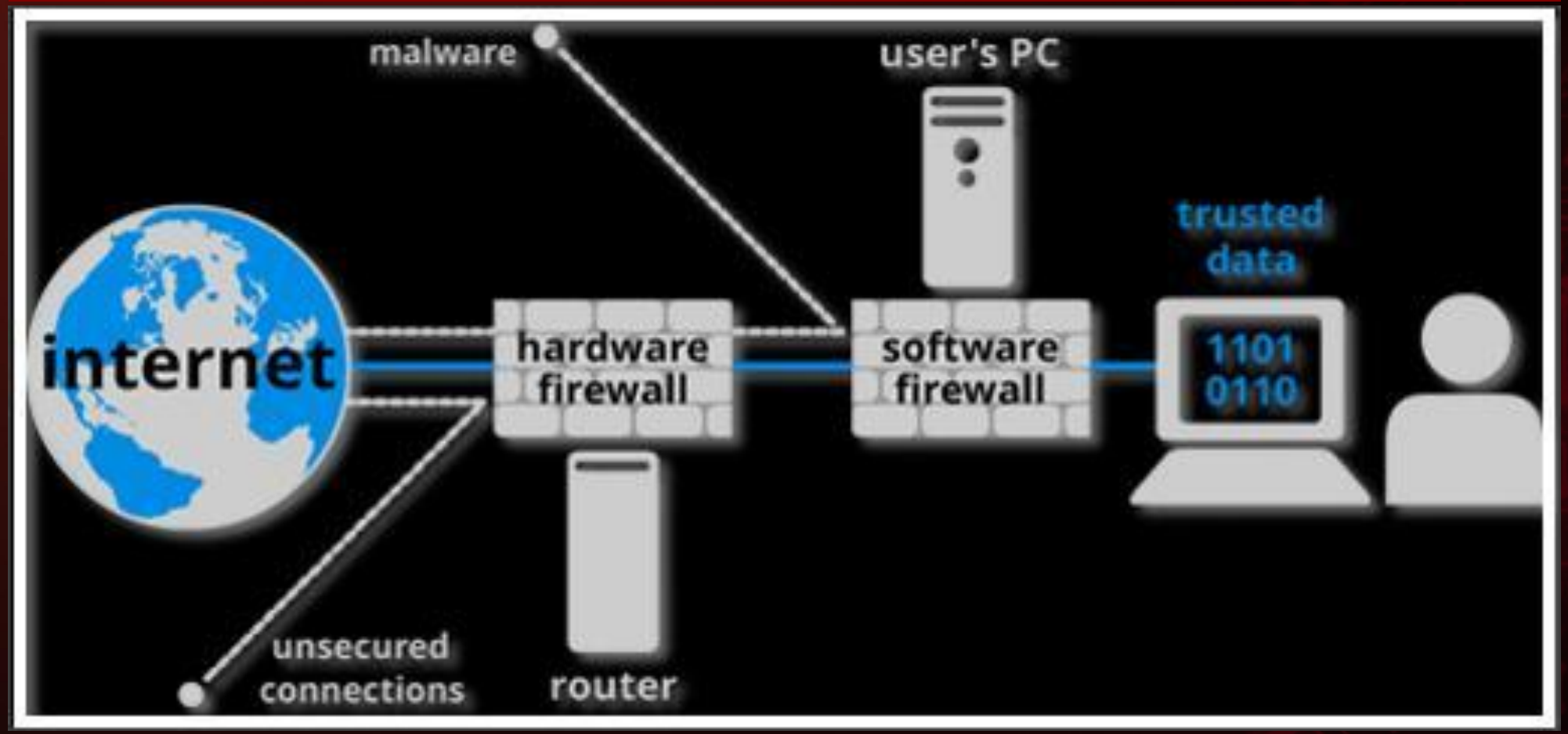
O QUE O FIREWALL NÃO FAZ

Não fornecem proteção contra vírus ou código malicioso.

A maioria dos firewalls não inspeciona a carga útil, ou o conteúdo do pacote, e por isso não estão cientes de qualquer ameaça que possa estar contida nele.

Nenhum firewall pode proteger contra políticas inadequadas ou mal gerenciadas.

COMO FUNCIONA UM FIREWALL



COMO FUNCIONA UM FIREWALL

Há duas abordagens de lógica no projeto de segurança que os firewalls de rede utilizam para tomar decisões de controle de acesso.

- Tudo o que não é especificamente permitido é negado.
- Tudo o que não é especificamente negado é permitido

O mais recomendado é que tudo o que não é especificamente permitido é negado.

TIPOS DE FIREWALLS

Podem ser categorizados dependendo:

Da função ou metodologia que o firewall usa

Se a comunicação está sendo feita entre um único nó e a rede, ou entre duas ou mais redes

Se o estado de comunicação está sendo rastreado no firewall ou não.

TIPOS DE FIREWALLS

Considerando a metodologia

- Filtragem de Pacotes
- Inspeção de pacote com estado
- Gateways/ proxies de aplicativos

TIPOS DE FIREWALLS

FILTRAGEM DE PACOTES

1. À medida que cada pacote passa pelo firewall, ele é examinado

2. As informações contidas no cabeçalho são comparadas a um conjunto pré-configurado de regras ou filtros

3. Uma decisão de permissão ou negação é feita com base nos resultados da comparação.

4. Cada pacote é examinado individualmente sem considerar outros pacotes que fazem parte da mesma conexão.

TIPOS DE FIREWALLS

FILTRAGEM DE PACOTES

As regras ou filtragem de pacotes podem ser configurados para permitir ou negar tráfego com base em uma ou mais das seguintes variáveis:

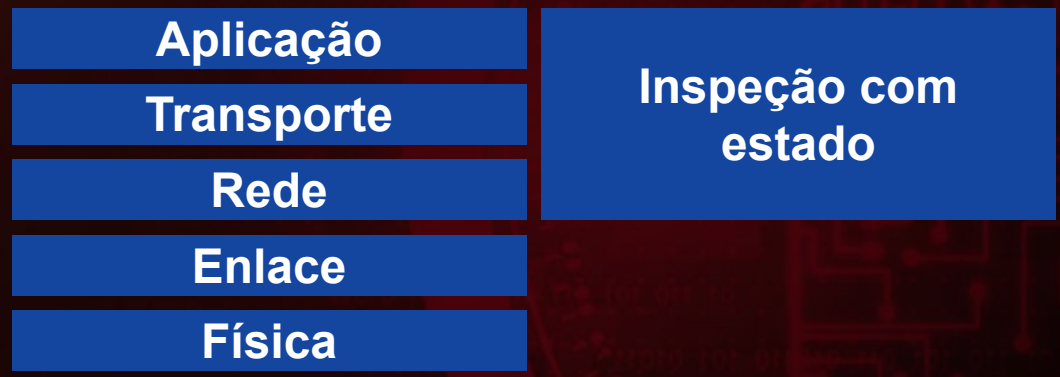
- Endereço IP de origem
- Endereço IP de destino
- Tipo de protocolo (TCP/UDP)
- Porta de origem
- Porta de destino

TIPOS DE FIREWALLS

INSPEÇÃO DE PACOTES COM ESTADO

Utiliza a mesma técnica da filtragem de pacotes

Além disso, ele examina as informações do cabeçalho do pacote da camada de rede para a camada de aplicação para verificar se o pacote faz parte de uma conexão legítima e se os protocolos estão se comportando conforme o esperado.



TIPOS DE FIREWALLS

PROXY DE APLICAÇÃO

Atua como tua como intermediário entre os de origem e destino entre os origem e destino

Quebra o modelo cliente/servidor em que duas conexões são necessárias: uma da origem para o gateway/proxy e uma do gateway/proxy para o destino.

Cada nó de extremidade só pode se comunicar com o outro passando pelo gateway/proxy.

TIPOS DE FIREWALLS

Se a comunicação está sendo feita entre um único nó e a rede, ou entre duas ou mais redes

FIREWALLS PESSOAIS

Software que filtra o tráfego que entra ou sai de um único computador.

FIREWALLS DE REDE

Executados em um dispositivo de rede dedicado ou computador posicionado no limite de duas ou mais redes.

TIPOS DE FIREWALLS

Se o estado de comunicação está sendo rastreado no firewall ou não

Firewall
Statefull

Mantém o controle do estado das conexões de rede (como fluxos TCP) que viajam por ele

Podem armazenar na memória atributos significativos de cada conexão do início ao fim

Esses atributos são os estados da conexão
Incluem os endereços IP e as portas envolvidas na conexão e os números de sequência dos pacotes que atravessam a conexão

TIPOS DE FIREWALLS

Se o estado de comunicação está sendo rastreado no firewall ou não

Firewall Stateless

Trata cada pacote IP de forma isolada

Não sabe se um determinado pacote faz parte de uma conexão existente, está tentando estabelecer uma nova conexão ou é apenas um pacote invasor.

Exemplo:
Quando utilizamos um FTP, esta aplicação por padrão abre novas conexões para portas aleatórias.

REFERÊNCIAS

1. Segurança de Computadores
2. Criptografia e segurança de redes: princípios e práticas
3. Introdução à Segurança de Computadores
4. Práticas de Segurança para Administradores de Redes Internet
5. Internet Firewalls
6. A Complete Guide To Firewall: How To Build A Secure Networking System