1.Introdução a Firewalls

Um **firewall é um sistema ou grupo de sistemas que aplica uma política de controle de acesso entre as redes, onde o todo o tráfego flui por ele**. É uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras/instruções que analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Ele age como uma barreira entre as redes, analisando se as mesmas são confiáveis ou não, com destaque para a navegação na Internet. Ao controlar e autorizar quais informações podem entrar na sua rede privada, a tecnologia isola os computadores da web, inspecionando os pacotes de dados à medida em que eles chegam ao outro lado da barreira de proteção.

Os primeiros Firewalls surgiram após o início da Internet, no final dos anos 80, depois que o primeiro vírus de computador conhecido atacou computadores de diversas entidades como a NASA e a universidade de Stanford. Eles eram apenas roteadores usados para separar a rede em pequenas LANs, pois desta forma, erros em algumas das LANs não seriam transmitidos para o resto da rede prejudicando seu funcionamento.

Hoje em dia, os firewalls são resistentes a ataques de rede, o único ponto de trânsito entre redes corporativas internas e redes externas e os firewalls aplicam a política de controle de acesso. Geralmente, firewalls impedem a exposição de hosts, recursos e aplicações sensíveis a usuários não confiáveis, além de “sanitizar” o fluxo do protocolo, o que impede a exploração de falhas no protocolo, e também bloqueiam dados maliciosos de servidores e clientes.

Também reduzem a complexidade do gerenciamento de segurança descarregando a maior parte do controle e acesso à rede para alguns firewalls de rede. Porém, firewalls mal configurados podem ter sérias consequências para a rede, como se tornar um único ponto de falha. Os dados de muitas aplicações não podem ser transmitidos por firewalls com segurança, usuários podem procurar proativamente maneiras de contornar o firewall para receber material bloqueado expondo a rede, o desempenho da rede pode diminuir e o tráfego não autorizado pode ser encapsulado ou escondido como tráfego legítimo através do firewall.

2.Firewall de filtragem de pacotes

Também conhecido como *Packet Filtering Firewall*, trata-se de um tipo de Firewall que inspeciona os pacotes de dados que circulam em uma rede e decide permitir ou bloquear o tráfego com base em regras definidas. Funciona da seguinte forma:

- **Inspeção de pacotes:** Quando um pacote de dados entra ou sai da rede protegida pelo Firewall, o Firewall de Filtragem de Pacotes o inspeciona. Ele examina informações essenciais do pacote, como endereços IP de origem e destino, portas de serviço, protocolos e outras informações relevantes.
- **Regras de filtragem:** O Firewall de Filtragem de Pacotes possui uma lista de regras (ACL) que define quais pacotes podem ser permitidos e quais devem ser bloqueados. Cada regra da ACL contém critérios específicos, como endereços IP, portas e protocolos, que são comparados com as informações do pacote para determinar a ação a ser tomada.
- **Ações permitir e negar:** Com base nas regras definidas, o Firewall toma uma das duas ações: "permitir" ou "negar". Se o pacote corresponder a uma regra que permite o tráfego, ele será liberado para continuar seu caminho na rede. Por outro lado, se o pacote corresponder a uma regra que bloqueia o tráfego, ele será descartado e não alcançará o destino pretendido.
- **Implicit Deny:** O Firewall de Filtragem de Pacotes geralmente possui uma política de negação implícita, o que significa que, se um pacote não corresponder a nenhuma das regras definidas na ACL, ele será automaticamente bloqueado. Essa política ajuda a garantir que apenas o tráfego permitido tenha acesso à rede, uma vez que todo o tráfego não explicitamente permitido é negado.
- **Eficiência e limitações:** Esse tipo de Firewall é eficiente em termos de desempenho, pois sua análise é baseada em informações de cabeçalhos de pacotes, tornando o processo de filtragem rápido e escalável. No entanto, a filtragem baseada apenas em informações de cabeçalhos tem algumas limitações, como dificuldade em detectar tráfego malicioso disfarçado ou oculto em pacotes legítimos.

Existem diferentes tipos de firewalls e suas capacidades específicas são determinadas e usadas para cada tipo de situação.

3.Firewall de filtragem de pacotes (sem estado - Stateless)

Os firewalls de filtragem de pacotes geralmente fazem parte de um firewall de roteador, que permite ou nega o tráfego com base nas informações da camada 3 e da camada 4 OSI. Eles são firewalls sem estado que usam uma simples pesquisa de tabela de políticas que filtra o tráfego com base em critérios específicos como endereço IP de origem e destino, protocolos, números de portas de origem e destino, pacotes SYN. Também analisam as informações de cabeçalho do pacote, além de examinar individualmente cada pacote sem considerar o histórico de antigas conexões.

As vantagens de se usar um firewall de filtragem de pacotes inclui os filtros de pacotes implementam conjuntos de regras de permissão simples, têm um baixo impacto no desempenho da rede, são fáceis de implementar e são suportados pela maioria dos roteadores, fornecem um grau inicial de segurança na camada de rede e executam quase todas as tarefas de um firewall high-end a um custo muito menor. Embora, eles não representam uma solução de firewall completa, mas são um elemento importante de uma política de segurança de firewall.

Suas desvantagens incluem que os filtros de pacote de informação são suscetíveis à falsificação de IP, os atores de ameaça podem enviar pacotes arbitrários que atendem aos critérios ACL e passam pelo filtro, os filtros de pacote não filtram de forma confiável os pacotes fragmentados, os filtros de pacotes usam ACLs complexas, que podem ser difíceis de implementar e manter e os filtros de pacotes não podem filtrar dinamicamente determinados serviços.

4.Firewall com monitoração de estado (com estado - Stateful)

Firewalls com estado são as tecnologias mais versáteis e mais comuns de uso. Eles fornecem filtragem de pacotes ***stateful*** usando informações de conexão mantidas em uma tabela de estado. Filtragem com estado é uma arquitetura de firewall classificada na camada de rede. Também analisa o tráfego na camada 4 e 5 OSI.

Os benefícios de se usar um firewall com estados incluem que, são frequentemente usados como um meio primário de defesa, filtrando tráfego indesejado ou desnecessário, fortalecem a filtragem de pacotes fornecendo um controle mais rigoroso sobre a segurança, melhora o desempenho em relação aos filtros de pacotes ou servidores proxy, se defendem contra ataques de falsificação e DoS, determinando se os pacotes pertencem a uma conexão existente ou são de uma origem não autorizada e fornecem informações de log.

As limitações apresentadas em firewalls com estados incluem que eles não podem evitar ataques à camada de aplicação porque não examinam o conteúdo real da conexão HTTP, nem todos os protocolos são stateful, é difícil rastrear conexões que usam negociações de porta dinâmica e firewalls com estado não suportam autenticação de usuário.

5.Firewall de gateway de aplicativo

Um firewall de gateway de aplicação (***firewall proxy***) filtra as informações nas camadas 3, 4, 5 e 7 OSI. A maior parte do controle e filtragem é feita em software. Quando um cliente precisa acessar um servidor remoto, ele se conecta a um servidor proxy. O servidor proxy se conecta ao servidor remoto em nome do cliente, logo, o servidor apenas vê uma conexão do servidor proxy.

6.Web Application Firewall (WAF)

O **Web Application Firewall** (***WAF***), em português Firewall de Aplicação Web, é uma camada de segurança de rede projetada especificamente para proteger aplicativos da web contra ameaças cibernéticas direcionadas a vulnerabilidades específicas em sites e aplicações. Diferente dos Firewalls tradicionais, que focam no controle de tráfego de rede em camadas mais baixas, o WAF é especializado em analisar e filtrar o tráfego HTTP/HTTPS, o que o torna mais eficaz na proteção contra ataques específicos a aplicações.

Veja seu funcionamento:

- **Inspeção de tráfego:** O WAF monitora todo o tráfego de entrada e saída da aplicação web, examinando detalhadamente as requisições e respostas HTTP/HTTPS que chegam ao servidor. Isso inclui parâmetros da URL, cookies, cabeçalhos, dados de formulários e outros elementos específicos das aplicações web.
- **Comparação com assinaturas e regras:** O WAF compara as informações do tráfego com um conjunto de assinaturas e regras pré-definidas. Essas assinaturas e regras identificam padrões e comportamentos associados a ataques conhecidos, como SQL injection, cross-site scripting (XSS), ataques de injeção de comandos, entre outros.
- **Bloqueio de ataques:** Se o WAF identificar alguma requisição ou resposta que corresponde a uma assinatura ou regra de ataque conhecida, ele tomará uma ação específica, que pode ser bloquear a requisição, redirecionar para uma página de erro, ou substituir o conteúdo malicioso por uma resposta segura.
- **Aprendizado e adaptação:** Além das assinaturas e regras pré-definidas, alguns WAFs possuem a capacidade de aprendizado e adaptação. Eles analisam o tráfego ao longo do tempo e podem ajustar suas configurações automaticamente para lidar com novas ameaças e padrões de ataque.
- **Personalização das regras:** Os administradores do WAF têm a flexibilidade de personalizar as regras e ajustar a configuração de acordo com as necessidades específicas da aplicação web. Isso permite um nível de controle mais granular sobre a segurança e ajuda a evitar falsos positivos que poderiam bloquear tráfego legítimo.

7.Appliance Firewall

É um dispositivo dedicado de segurança de rede que funciona como um firewall completo em um único hardware. Diferente de implementações de firewall baseadas em software, um Appliance Firewall é uma solução pronta para uso, que já contém todos os recursos e configurações necessários para proteger uma rede.

Ele é projetado para simplificar a implantação e a administração do firewall, oferecendo uma solução eficiente e de alto desempenho para garantir a segurança da rede. Funcionamento do Appliance Firewall:

- **Hardware especializado:** O Appliance Firewall é construído com hardware especializado para oferecer alto desempenho e eficiência na análise e filtragem do tráfego de rede. Ele é equipado com processadores rápidos, memória dedicada e interfaces de rede de alta velocidade.
- **Sistema operacional próprio:** O Appliance Firewall utiliza um sistema operacional proprietário, desenvolvido pelo fabricante do dispositivo, otimizado para as tarefas de segurança de rede. Esse sistema operacional é projetado para executar tarefas específicas de firewall de forma eficiente e segura.
- **Configuração simplificada:** A maioria dos Appliance Firewalls oferece uma interface gráfica de usuário (GUI) amigável para configurar e gerenciar as regras de segurança. Essa interface facilita a configuração de políticas de firewall, a definição de regras de filtragem e outras configurações relacionadas à segurança.
- **Recursos avançados:** Além das funcionalidades básicas de firewall, muitos Appliance Firewalls vêm com recursos avançados de segurança, como detecção e prevenção de intrusões (IDS/IPS), VPN (Virtual Private Network), proteção contra ameaças avançadas, filtragem de conteúdo, balanceamento de carga e muito mais.
- **Escalabilidade:** Os Appliance Firewalls são projetados para atender a diferentes necessidades de escalabilidade. Eles podem ser dimensionados para atender a demandas crescentes de tráfego de rede, seja através da adição de hardware complementar ou de licenças de software.

8.Host-based Firewall

Também conhecido como Firewall de Hospedeiro, é um software de segurança instalado diretamente em um sistema operacional de computador individual (como um servidor ou computador de usuário). Ele atua como uma camada adicional de proteção, controlando o tráfego de rede específico para o próprio hospedeiro onde está instalado.

Diferente do Firewall de Rede (que protege toda a rede), o Host-based Firewall concentra-se na segurança do próprio sistema local, permitindo que o administrador do sistema defina regras personalizadas de filtragem de pacotes.

Funcionamento

- **Inspeção do tráfego local:** O Host-based Firewall monitora o tráfego de entrada e saída do próprio sistema em que está instalado. Ele analisa os pacotes de dados que chegam e saem do sistema, examinando informações como endereços IP, portas, protocolos e outros dados relevantes.
- **Criação de regras:** O administrador do sistema pode configurar regras específicas no Host-based Firewall. Essas regras determinam como o firewall deve tratar os pacotes com base em critérios definidos, como permitir ou bloquear determinados tipos de tráfego, com base em endereços IP, portas e outros atributos.
- **Políticas de Default:** O Host-based Firewall tem uma política de "default" (padrão) que define o que fazer com pacotes que não correspondem a nenhuma regra específica. Essa política pode ser configurada para permitir ou negar todos os pacotes que não tenham uma regra correspondente.
- **Ações do firewall:** Quando um pacote é recebido ou enviado pelo sistema, o Host-based Firewall compara as informações do pacote com as regras definidas. Com base nessa análise, o Firewall tomará a ação especificada na regra correspondente, permitindo o pacote, bloqueando-o ou tomando outra ação definida.
- **Integração com o sistema operacional:** O Host-based Firewall é intimamente integrado ao sistema operacional do hospedeiro, permitindo que ele controle o tráfego de rede diretamente na pilha de rede do sistema. Isso proporciona um controle mais granular sobre as comunicações de rede em nível local.

9.Firewall de última geração

Os **firewalls de última geração** (***NGFW***) vão além dos firewalls de estado, fornecendo prevenção de intrusão integrada, reconhecimento e controle de aplicações para ver e bloquear aplicativos arriscados, caminhos de atualização para incluir feeds de informações e técnicas para lidar com ameaças de segurança em evolução.

10.Firewall híbrido

Uma combinação com vários tipos de firewall, como um de inspeção de aplicações combinada com um de estado e outro de gateway de aplicativo.

O design de um firewall é principalmente sobre interfaces de dispositivo que permitem ou negam tráfego com base na origem, destino e tipo de tráfego e os seus designs variam.

11.Público e Privado

Normalmente, um firewall com duas interfaces é configurado da seguinte forma: o tráfego proveniente da rede privada é permitido e inspecionado à medida que

viaja em direção à rede pública, além de que é permitido o tráfego inspecionado que retorna da rede pública e é associado ao tráfego de origem.

12.DMZ

Uma **zona desmilitarizada** é um projeto de firewall onde normalmente há uma interface interna conectada à rede privada, uma interface externa conectada à uma rede pública e uma interface DMZ.

O **tráfego proveniente da rede privada** é inspecionado à medida que ele viaja para a rede pública ou DMZ. Este tráfego é permitido com pouca ou nenhuma restrição. Tráfego inspecionado que retorna da DMZ ou da rede pública para a privada é permitido.

O **tráfego originado da rede DMZ** e que viaja para a rede privada geralmente é bloqueado e o tráfego originado da rede DMZ e viajando para rede pública é permitido seletivamente com base nos requisitos de serviço.

O **tráfego proveniente da rede pública** e que viaja em direção à DMZ é seletivamente permitido e inspecionado. Esse tipo de tráfego normalmente é o tráfego de e-mail, DNS, HTTP(S), e o tráfego originado da rede pública que viaja para a rede privada está bloqueado.

Este tipo de firewall utiliza o conceito de zona para fornecer flexibilidade adicional. Uma zona é um grupo de uma ou mais interfaces que têm funções ou recursos semelhantes. As zonas ajudam a especificar onde uma regra ou política de firewall do Cisco IOS deve ser aplicada.

Por padrão, o tráfego entre interfaces na mesma zona não está sujeito a nenhuma política e passa livremente. No entanto, todo o tráfego de zona para a zona está bloqueado. Para permitir o tráfego entre zonas, uma política que permite ou inspeciona o tráfego deve ser configurada. A única exceção a esta política padrão é ***deny any*** é a zona própria do roteador. A zona ***auto*** é o próprio roteador e inclui todos os endereços IP da interface do roteador.

O tráfego deve ser considerado ao projetar uma política para a auto zona incluir o tráfego de plano de gerenciamento e plano de controle, como SSH, SNMP e protocolos de roteamento.

Uma ***defesa em camada*** usa diferentes tipos de firewalls que são combinados em camadas para adicionar profundamente à segurança de uma organização. As políticas podem ser aplicadas entre as camadas e dentro das camadas e determina se o tráfego é encaminhado ou descartado.

Uma abordagem de defesa em camadas não é tudo o que é necessário para garantir uma rede interna segura. Um administrador de rede deve considerar muitos fatores ao construir uma defesa completa em profundidade porque, os firewalls

normalmente não interrompem as instruções provenientes de hosts dentro de uma rede ou zona, firewalls não protegem contra instalações de ponto de acesso desonesto, os firewalls não substituem os mecanismos de backup e recuperação de desastres resultantes de ataques ou falhas de hardware e os firewalls não substituem administradores e usuários informados.

Segurança do núcleo da rede (1): Protege contra software malicioso e anomalias de tráfego e impõe políticas de rede e garante a capacidade de sobrevivência

Segurança de perímetro (2): Protege limites entre as zonas

Segurança das comunicações (3): Fornece garantia de informações

Segurança do endpoint (4): Fornece identidade e conformidade com a política de segurança do dispositivo.

Além disto, **deve-se posicionar firewalls nos limites de segurança**, negar todo o tráfego por padrão, permitir apenas serviços que são necessários, assegurar-se de que o acesso físico ao firewall esteja controlado, monitorar regularmente logs de firewall, praticar o gerenciamento de alterações para alterações de configuração de firewall e lembrar-se de que os firewalls protegem principalmente contra ataques técnicos oriundos do exterior.

13.Cisco Firewall

Existem dois modelos de configuração para o Cisco Firewall

- **Firewall clássico:** O modelo de configuração tradicional em que a política de firewall é aplicada em interfaces
- **Firewall de política de zona (ZPF):** O modelo de configuração na qual as interfaces são atribuídas a zonas de segurança, e a política de firewall é aplicada ao tráfego em movimento entre as zonas

Existem vários benefícios de um ZPF, como, não é dependente de ACLs, a postura de segurança do roteador é bloquear a menos que seja permitido explicitamente, políticas são fáceis de ler e solucionar problemas com a linguagem de política de classificação da Cisco (C3PL).

O ***C3PL*** é um método estruturado para criar políticas de trânsito com base em eventos e condições e ações fornecendo escalabilidade porque uma política afeta qualquer tráfego, em vez de precisar de várias ações de ACls e inspeção para diferentes tipos de tráfego, as interfaces virtuais e físicas podem ser agrupadas em zonas e políticas são aplicadas ao tráfego unidirecional entre as zonas.

Projetar ZPFs envolve as seguintes etapas:

- **Etapa 1 - Determinar as zonas:** O administrador se concentra na separação da rede em zonas que estabelecem as fronteiras de segurança de uma rede. Uma zona define um limite onde o tráfego é submetido a restrições políticas à medida que cruza para outra região da rede
- **Etapa 2 - Estabelecer políticas entre as zonas:** Para cada par de zonas, defina as sessões que os clientes nas zonas de origem podem solicitar aos servidores nas zonas de destino. Essas sessões são mais frequentemente as sessões TCP e UDP, mas também podem ser sessões ICMP, como ICMP ECHO. Para o tráfego que não é baseado no conceito de sessões, o administrador deve definir fluxos de tráfego unidirecionais da fonte para o destino e vice-versa. As políticas são unidirecionais e são definidas com base nas zonas de origem e destino, que são conhecidas como pares de zona
- **Etapa 3:** Depois que as zonas foram identificadas e os requisitos de tráfego entre eles documentados, o administrador deve projetar a infraestrutura física, além de levar em conta os requisitos de segurança e disponibilidade ao projetar a infraestrutura física e isso inclui ditar o número de dispositivos entre as zonas mais seguras e menos seguras além de determinar dispositivos redundantes.
- **Etapa 4:** Cada dispositivo de firewall no design, o administrador deve identificar subconjuntos de zonas que estão conectados a suas interfaces e mesclar os requisitos de tráfego para essas zonas.

As políticas identificam ações que o ZPF executará no tráfego de rede. Três ações possíveis podem ser configuradas para processar o tráfego por protocolo, zonas de origem e destino e outros critérios, como.

- **Inspect:** Isso realiza inspeção de pacotes de estado de Cisco IOS
- **Drop:** Isso é análogo a ***deny***, uma declaração em uma ACL. Uma ***log*** opção disponível para registrar os pacotes rejeitados
- **Pass:** É análogo a uma ***permit***, declaração em uma ACL. A Ação de aprovação não rastreia o estado das conexões ou das sessões no tráfego.

O tráfego que transita através de interfaces de roteador está sujeito a várias regras que regem o comportamento da interface. As regras dependem se as interfaces de entrada e saída são membros da mesma zona.

- Se nenhuma interface é um membro da zona, a ação resultante é passar o tráfego
- Se ambas as interfaces são membros da mesma zona, a ação resultante é passar o tráfego

- Se uma interface é um membro da zona, mas o outro não é, então a ação resultante é derrubar o tráfego independentemente de existir um par de zona.
- Se ambas as interfaces pertencerem ao mesmo par de zona e uma política existir, a ação resultante é inspecionar, permitir ou drop, conforme definido pela política

  A tabela abaixo resume as regras acima

Membro da interface de origem da zona ?	Membro da interface de destino da zona ?	O par de zona existe ?	Política existe ?	Resultado
NÃO	NÃO	N/D	N/D	APROVADO
SIM	NÃO	N/D	N/D	DROP
NÃO	SIM	N/D	N/D	DROP
SIM (privado)	SIM (privado)	N/D	N/D	APROVADO
SIM (privado)	SIM (público)	NÃO	N/D	DROP
SIM (privado)	SIM (público)	SIM	NÃO	APROVADO
SIM (privado)	SIM (público)	SIM	SIM	INSPECT

A autoza é o próprio roteador e inclui todos os endereços IP atribuídos às interfaces do roteador. Este é o tráfego que se origina no roteador ou é endereçado a uma interface de roteador. As regras dependem se o roteador é a fonte ou o destino do tráfego, conforme a tabela a seguir irá mostrar.

Membro da interface de origem da zona ?	Membro da interface de destino da zona ?	O par de zona existe ?	Política existe ?	Resultado
SIM (auto zona)	SIM	NÃO	N/D	APROVADO
SIM (auto zona)	SIM	SIM	NÃO	APROVADO
SIM (auto zona)	SIM	SIM	SIM	INSPECT
SIM	SIM (auto zona)	NÃO	N/D	APROVADO
SIM	SIM (auto zona)	SIM	NÃO	APROVADO
SIM	SIM (auto zona)	SIM	SIM	INSPECT

14.IPTABLES

É uma ferramenta de firewall utilizada em sistemas operacionais Linux para filtrar e controlar o tráfego de rede. Ele permite definir regras específicas que determinam o que pode entrar, sair ou ser encaminhado pela máquina. O iptables

funciona dividido em tabelas, cadeias e regras, que em conjunto formam a lógica de filtragem.

- **Tabelas:** O iptables possui quatro tabelas principais: *filter*; *nat*; *mangle*; *raw*
- **Cadeias:** Cada tabela contém cadeias de regras predefinidas: *INPUT*; *OUTPUT*; *FORWARD*
- **Regras:** As regras são a essência do iptables e são aplicadas nas cadeias. Cada regra define um conjunto de condições que determinam como os pacotes devem ser tratados. As regras podem permitir ou negar pacotes, encaminhá-los para outra interface ou modificar campos de cabeçalho dos pacotes.
- **Fluxo de decisão:** O iptables segue um fluxo de decisão específico para cada pacote que entra ou sai da máquina:
  Verificação das regras da tabela
  Pré-processamento das regras da tabela *mangle*
  Filtragem nas cadeias *INPUT*, *OUTPUT* e *FORWARD*
  Verificação das regras da tabela *nat*