FUNDAMENTOS DE FIREWALL

PROF. JOAS ANTONIO

Sobre o instrutor

- Pesquisador de segurança da informação;
- Pentester;
- Cursou IoT pela Stanford EaD;
- Endpoint professional;
- Professor de informática, redes e segurança.

O que você vai aprender?

- O que é um firewall;
- Tipos de firewall;
- Filtragem de pacotes;
- Firewall Stateless;
- Firewall Stateful;
- Regras de Firewall;
- Politicas de Regras;
- Como funciona uma regra de firewall;
- Nat;
- VPN.

Requisitos

- Software e Hardware;
- Modelo OSI;
- TCP/IP;
- Protocolos e serviços;
- Segurança da informação e redes.

Definição de Firewall

- **Segundo o Wikipédia:** Um ***firewall*** (em português: parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, *Proxy de* aplicações, etc.
- Este dispositivo de segurança existe na forma de *software* e de *hardware*, a combinação de ambos é chamado tecnicamente de appliance (geralmente é um dispositivo de hardware separado e dedicado com software integrado (firmware), especificamente projetado para fornecer um recurso de computação específico.)
- https://pt.wikipedia.org/wiki/Firewall

CYBER SECURITY UP

Definição de Firewall

- **Segundo a Cisco:** Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
- Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.
- Um firewall pode ser um hardware, software ou ambos.

CYBER SECURITY UP

Tipos de Firewall

Firewall de proxy:

- Um firewall de proxy é um dos primeiros tipos de firewall e funciona como a passagem de uma rede para outra de uma aplicação específica. Servidores proxy podem oferecer recursos adicionais, como armazenamento em cache e segurança de conteúdo ao evitar conexões diretas de fora da rede. No entanto, isso também pode afetar a capacidade de taxa de transferência e as aplicações que eles podem comportar.

Tipos de Firewall

Firewall de Gerenciamento unificado de ameaças (UTM):

- Normalmente, um dispositivo UTM combina, de maneira flexível, as funções de um firewall com inspeção de estado e prevenção contra intrusões e antivírus. Ele também pode incluir serviços adicionais e, às vezes, gerenciamento em nuvem. O UTM concentra-se em simplicidade e facilidade de uso.

Tipos de Firewall

Firewall de próxima geração (NGFW):

- Os firewalls evoluíram para além da simples filtragem de pacotes e inspeção stateful. A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação.
- De acordo com a definição do Gartner, Inc., um firewall de próxima geração deve incluir:
- Recursos padrão de firewall, como inspeção stateful
- Prevenção de invasão integrada
- Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos
- Atualização de caminhos para incluir feeds futuros de informação
- Técnicas para lidar com as ameaças à segurança em evolução
- Embora esses recursos estejam se tornando cada vez mais a norma para a maioria das empresas, os NGFWs podem fazer mais.

CYBER SECURITY UP

Tipos de Firewall

NGFW focado em ameaças:

- Esses firewalls incluem todos os recursos de um NGFW tradicional e também oferecem detecção e remediação avançadas de ameaças. Com um NGFW focado em ameaças, você pode:
- Saber quais recursos sofrem um risco maior com reconhecimento completo de contexto
- Reagir rapidamente a ataques com automação de segurança inteligente que define políticas e fortalece suas defesas de forma dinâmica
- Detectar melhor as atividades evasivas e suspeitas com a correlação de eventos de rede e endpoint
- Reduzir expressivamente o tempo entre a detecção e a limpeza com segurança retrospectiva que monitora continuamente atividades e comportamentos suspeitos mesmo após a inspeção inicial
- Facilitar a administração e reduzir a complexidade com políticas unificadas que oferecem proteção durante todo o ciclo de ataque

CYBER SECURITY UP

Filtragem de Pacote

- Toda comunicação em uma rede de computadores é segmentada em pequenos pacotes de acordo com a unidade máxima de transferência entre as redes (MTU), geralmente de 1500 bytes. Em cada uma das camadas, existem informações de cabeçalho – úteis ao processamento – além da parte de dados (payload), onde a informação é, de fato, transportada.
- A filtragem de pacotes nada mais é do que um mecanismo capaz de analisar os cabeçalhos em determinadas camadas da suíte TCP/IP e, com base em um padrão de regras pré-estabelecido, encaminhar o pacote para o próximo passo ou desconsiderá-lo.
- Este é o conceito básico para entender uma estrutura completa de pacotes, somente possível pois os firewalls são colocados de maneira estratégica em uma topologia de rede, por onde o tráfego inter-redes é afunilado ou estrangulado.
- Uma vez que o pacote passa pelo firewall, e somente desta maneira ele pode chegar até o destino final, o mesmo tem o poder de definir se isso deve ou não ser encaminhado. O encaminhamento de pacotes é o recurso fundamental de roteamento, função também desempenhada por um **firewall**.

CYBER SECURITY UP

Stateless x Statefull

Filtragem stateless ou sem estado:

- A filtragem sem estado oferece um recurso de avaliação de pacotes de maneira independente, onde não há conhecimento sobre a conexão. Isso quer dizer que cada pacote que passa pelo firewall, independente de ser uma nova conexão ou já existente, é avaliado pelas regras estabelecidas pelo administrador.
- É comum nestas arquiteturas criar uma regra para cada direção de tráfego, prevendo tanto a saída (envio) de um pacote, quanto a entrada (recebimento) – o que ocorre comumente em interfaces de redes diferentes. Como não há conhecimento das conexões, não é possível prever o retorno da conexão.
- Os ambientes que possuem esse mecanismo de filtragem têm a tendência comum de ter um número maior de regras, por causa da necessidade de sempre se prever os dois sentidos de uma comunicação (entrada e saída).
- Os firewalls stateless são cada vez menos utilizados. Ainda assim, está está presente em dispositivos de rede cujo principal foco não é segurança e garante que regras básicas de acesso possam ser criadas, evitando exposições desnecessárias.
- O conceito mais importante a ser registrado sobre os firewalls stateless é que não possuem conhecimento acerca das conexões e, por causa disso, aplicam suas regras em todos os pacotes que atravessam o dispositivo.

CYBER SECURITY UP

Stateless x Statefull

- **Firewall stateful ou com estado:**
- Os **firewalls stateful** foram concebidos posteriormente, a fim de solucionar aspectos de segurança que surgiram com a primeira geração, como por exemplo o caso de forjar (spoof) informações de conexão.
- A importância fundamental foi de orientar a filtragem para conexão e permitir que o mecanismo de filtragem passasse a conhecer as conexões. Com base nisso, legitimaria um pacote ou não. Esse recurso auxiliar ficou conhecido como tabela de conexões ou tabela de estados.
- Com a tabela de estados, todo início de conexão é devidamente registrado (um novo estado é criado). Quando o pacote retorna, antes de iniciar o processo de avaliação das regras de acesso, o **firewall stateful** verifica a tabela de estados, valida se há alguma conexão associada e, caso afirmativo, aceita a conexão, sem processar as regras. Do contrário, descarta o pacote.

CONTINUA >>

CYBER SECURITY UP

Stateless x Stateful

- **Continuação stateful:**
- A segurança do ambiente é incrementada consideravelmente com a utilização de **firewall stateful**, tendo em vista que há rastreabilidade de parâmetros utilizados para validar uma conexão ativa na estrutura. O nível e complexidade do tracking depende do fabricante. Alguns utilizam somente parâmetros de endereços e portas de origem e destino, enquanto outros utilizam número de sequência e reconhecimento, tamanho de janela etc (no caso do protocolo TCP).
- A medida que a conexão evolui em termos de trocas de pacotes, a tabela de estados é sempre atualizada com as informações para garantir a continuidade de segurança e integridade. Este processo também garante a validade da conexão, sem que seja necessário avaliar as regras de acesso definidas pelo administrador.
- Em um **firewall stateful** há uma economia considerável de recursos computacionais, uma vez que há um esforço inicial para a criação de novas conexões, que é recompensado até o encerramento pela não necessidade de processar as regras de acesso. É muito comum encontrar esse mecanismo de filtragem nas mais modernas soluções, que continua sendo um elemento fundamental na estratégia de defesa em profundidade.

CYBER SECURITY UP

Regras de Firewall

- Um firewall atua como uma espécie de peneira, deixando apenas determinados tipos de dados passar. A escolha do que pode ou não passar é feito através do estabelecimento de políticas, isto é, regras de firewall.
- Regras de Firewall controlam o tráfego que tem permissão para entrar na interface de firewall. Uma vez que o tráfego passa pelo Firewall, uma conexão é criada na tabela de estado do Firewall, permitindo que todo o tráfego subsequente tenha permissão de entrada/saída.
- Existem dois modos na criação de políticas de firewall: modo restritivo e modo versátil. No modo restritivo, o firewall é configurado para bloquear todo o tráfego passando por ele e liberar somente o que foi configurado pelas regras. Já no modo versátil ocorre o oposto, todo tráfego pode passar e só é bloqueado o que as regras foram configuradas.
- As regras de Firewall possuem prioridades "Top down", ou seja, a primeira regra sempre terá maior prioridade que as demais.

CYBER SECURITY UP

Classificação de um Firewall

- Firewalls podem trabalhar de várias maneiras, e por isso existem alguns tipos diferentes de metodologias. Levando em conta o local em que a comunicação acontece, onde ela é interceptada, necessidades específicas do que será protegido, características do SO, estrutura da rede, entre outros fatores.

Politica de Regras

- Determine quais dos seus aplicativos, programas e utilitários são absolutamente necessários no seu computador.
- Liste quaisquer riscos ou vulnerabilidades associadas a cada aplicação necessária e qual é necessário para minimizar o risco . Por exemplo , se um programa exige que uma porta específica sempre estará aberta para o tráfego de saída , o seu computador pode estar vulnerável a um hacker ou um vírus , se você não tiver um software antimalware também instalado e funcionando.
- Tomar decisões sobre o que e lista o tráfego de entrada e de saída que você vai permitir que a partir de seu computador, e que o tráfego de entrada e de saída você irá bloquear.
- **Continuação >>**

Politica de Regras

- **Continuação:**
- Escrever um documento que lista suas decisões sobre firewall segurança em termos claros e inequívocos . O documento vai incluir descrições de suas ferramentas de firewall, sua estratégia de segurança , o que respostas ou ações que você vai fazer se um evento de segurança (violação ou desvio) ocorre e como você pretende gerenciar ou atualizar o firewall e suas configurações.
- Imprima uma cópia de suas configurações de firewall e compará-lo com o seu documento de orientação política para confirmar se as configurações de apoiar o documento de política . Se você encontrar discrepâncias , alterar o conjunto de regras de firewall de acordo com sua política escrita .

Como funciona uma regra de firewall? (EXEMPLOS)

- O firewall é um sistema de segurança que utiliza regras para bloquear ou permitir conexões e transmissão de dados entre o seu computador e a Internet. As regras de firewall controlam o modo como o Firewall inteligente protege o seu computador contra programas maliciosos e acesso não autorizado. O Norton Firewall automaticamente verifica todo o tráfego de entrada e de saída do computador com base nessas regras.
- O Firewall inteligente usa dois tipos de regras de firewall:

Regras de programas	Controlam o acesso à rede dos programas em seu computador.
Regras de tráfego	Controlam todo o tráfego de entrada e saída da rede.

CYBER SECURITY UP

Como funciona uma regra de firewall? (EXEMPLOS)

- **Regras de programas:**
- Na guia Controle de programas, você pode fazer o seguinte:
- Renomear a descrição do programa.
- Modificar as regras de um programa.
- Adicionar uma regra para um programa.
- Modificar as configurações de acesso de uma regra de programa.
- Modificar a prioridade de regras de programa alterando a sequência das regras na lista.
- Remover uma regra de programa.
- Exibir o nível de confiança de um programa.

CYBER SECURITY UP

Como funciona uma regra de firewall? (EXEMPLOS)

- **Regras de tráfego:**
- Algumas das regras de tráfego padrão são somente leitura e são bloqueadas. Você não pode modificar essas regras.
- As regras são exibidas na ordem de seus níveis de prioridade. As regras que ocupam a posição superior na lista prevalecem sobre as que são exibidas na posição inferior da lista.

O que é NAT?

- A Conversão de Endereço de Rede (NAT) foi projetada para conservar o endereço IP. Ela permite que as redes IP privadas que usam endereços IP não registrados se conectem à Internet. A NAT opera em um roteador, que geralmente conecta duas redes entre si e converte os endereços privados (não exclusivos globalmente) na rede interna em endereços legais, antes que os pacotes sejam encaminhados para outra rede.
- Outro aspecto desse recurso é que a NAT pode ser configurada para anunciar para o resto do mundo apenas um endereço para toda a rede, proporcionando segurança adicional ao ocultar o fato de que a rede interna está por trás desse endereço. A NAT disponibiliza funções duplas de segurança e conservação de endereço e é implementada em ambientes de acesso remoto.

CYBER SECURITY UP

Como o Nat funciona?

- Basicamente, a NAT permite que um único dispositivo, como um roteador, atue como um agente entre a Internet (ou rede pública) e uma rede local (ou rede privada), o que significa que somente um endereço IP único é necessário para representar um grupo de computadores em qualquer situação fora da rede.

O que é VPN?

- **“Virtual Private Network”** ou Rede Privada Virtual, é uma rede privada construída sobre a infra-estrutura de uma rede pública, **normalmente a Internet**. Ou seja, ao invés de se utilizar links dedicados ou redes de pacotes (como Frame Relay ou X.25) para conectar redes remotas, utiliza-se a infra-estrutura da Internet.
- O conceito de VPN surgiu da necessidade de se utilizar redes de comunicação não confiáveis para trafegar informações de forma segura. As redes públicas são consideradas não confiáveis, tendo em vista que os dados que nelas trafegam estão sujeitos a interceptação e captura. Em contrapartida, estas redes públicas tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.
- A principal motivação no uso das VPNs é a financeira, como alternativa para redução dos custos de comunicação de dados, oferecendo transporte de pacotes IPs de modo seguro através de Internet, com o objetivo de conectar vários sites .

CYBER SECURITY UP

Tipos de VPN

- Existem vários tipos de implementação de VPN's. Cada uma tem suas especificações próprias, assim como características que devem ter uma atenção especial na hora de implementar.
- Entre os tipos de VPN, destacam-se três principais:
- Intranet VPN
- Extranet VPN
- Acesso Remoto VPN

Intranet VPN

- Em uma Intranet VPN, que pode, por exemplo facilitar a comunicação entre departamentos de uma empresa, um dos quesitos básicos a considerar é a necessidade de uma criptografia rápida, para não sobrecarregar a rede (que tem de ser rápida).

- Outro requisito essencial é a confiabilidade que garanta a prioridade de aplicações críticas, como por exemplo, sistemas financeiros, banco de dados. E por último, é importante a facilidade de gerenciamento, já que numa rede interna, tem-se constantes mudanças de usuários, seus direitos,etc.

CYBER SECURITY UP

Acesso Remoto VPN

- Uma VPN de acesso remoto conecta uma empresa à seus empregados que estejam distante fisicamente da rede. Neste caso torna-se necessário um software cliente de acesso remoto. Quanto aos requisitos básicos, o mais importante é a garantia de QoS(Quality of Service), isto porque, geralmente quando se acessa remotamente de um laptop, você está limitado à velocidade do modem. Outro item não menos importante é uma autenticação rápida e eficiente, que garanta a identidade do usuário remoto. E por último, um fator importante, é a necessidade de um gerenciamento centralizado desta rede, já que ao mesmo tempo, pode-se ter muitos usuários remotos logados, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticação por exemplo, estejam centralizadas num único lugar.

Extranet VPN

- Extranet VPN's são implementadas para conectar uma empresa à seus sócios, fornecedores, clientes, etc... Para isso é necessário uma solução aberta,para garantir a interoperabilidade com as várias soluções que as as empresas envolvidas possam ter em suas redes privadas. Outro ponto muito importante a se considerar é o controle de tráfego, o que minimiza o efeitos dos gargalos existentes em possíveis nós entre as redes, e ainda garante uma resposta rápida e suave para aplicações críticas.

PRINT("FIM")

Quer aprender mais?
Acesse os grupos e páginas ao lado >>

Pericia forense computacional
https://www.facebook.com/groups/216366638481732/

https://www.facebook.com/Expersec/?ref=br_rs

https://www.facebook.com/como.hackear.curso/