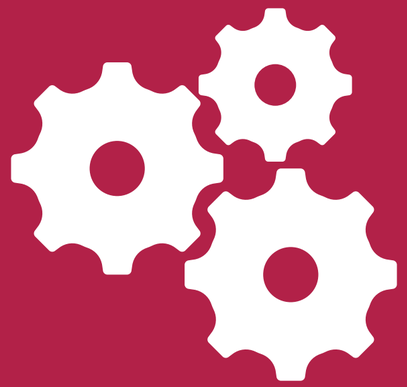
NEXT GENERATION FIREWALL

Integrantes

- Danielle Saidel
- Laíne Devesa
- Marcos Palácio
- Maurício Maia
- Melissa Romão
- Sabrina Pereira
- Vitor Bastos

NEXT GENERATION
FIREWALL



ARQUITETURA E FUNCIONAMENTO

O NGFW é uma evolução dos firewalls tradicionais, oferecendo recursos avançados de segurança e funcionalidades mais sofisticadas para lidar com ameaças cibernéticas em constante evolução.

Arquitetura

- O Firewall NG geralmente opera em uma arquitetura distribuída, composta por diferentes componentes que trabalham em conjunto para fornecer uma defesa abrangente contra ameaças. Os principais componentes incluem:

    1. Filtragem de pacotes
    2. Inspeção de estado
    3. Aplicação de políticas de segurança avançadas
    4. Integração com outros sistemas de segurança
    5. Funcionamento da filtragem de pacotes e inspeção de tráfego

1. Filtragem de pacotes

- Este é o núcleo do firewall, onde os pacotes de dados são analisados com base em regras definidas pelo administrador de segurança.
- Essas regras determinam se um pacote deve ser permitido ou bloqueado com base em critérios como endereço IP, porta de origem/destino, protocolo, entre outros.

2. Inspeção de estado

- O Firewall NG mantém uma tabela de estado das conexões de rede, permitindo a filtragem de pacotes com base no estado da conexão.
- Isso ajuda a evitar ataques como o seqüestro de sessões (session hijacking) e fornece um nível adicional de segurança.

3. Aplicação de políticas de segurança avançadas

- Além da filtragem básica de pacotes, o Firewall NG pode aplicar políticas de segurança avançadas, como controle de aplicativos, filtragem de conteúdo e prevenção de intrusões (IPS/IDS).

4. Integração com outros sistemas de segurança

- O Firewall NG pode ser integrado com outros sistemas de segurança.
- Como sistemas de detecção e resposta a incidentes (IDR), sistemas de gerenciamento de eventos e informações de segurança (SIEM) e soluções de prevenção de perda de dados (DLP)
- Para uma proteção mais abrangente e resposta a ameaças automatizada.

5. Funcionamento da filtragem de pacotes e inspeção de tráfego

- Quando um pacote de dados atravessa o firewall, ele é analisado em várias camadas para determinar se deve ser permitido ou bloqueado. Isso inclui:

    1. Camada de Rede
    2. Camada de Transporte
    3. Camada de Aplicação

1. Camada de Rede

- O Firewall NG verifica o endereço IP de origem e destino do pacote, bem como outras informações da camada de rede, para aplicar regras de filtragem básicas.

Camada de Transporte

- Aqui, o firewall analisa informações como portas de origem e destino, protocolo de transporte (TCP, UDP, etc.) e mantém uma tabela de estado para acompanhar o estado das conexões.

Camada de Aplicação

- O Firewall NG pode inspecionar o conteúdo dos pacotes em nível de aplicação, identificando o aplicativo ou serviço associado e aplicando políticas de segurança específicas para esse aplicativo, como controle de acesso, filtragem de conteúdo e prevenção de intrusões.

Essa abordagem de inspeção em várias camadas permite uma segurança mais eficaz, protegendo contra uma variedade de ameaças, incluindo malware, ataques de negação de serviço (DDoS) e violações de dados.

RECURSOS DE SEGURANÇA

O Firewall NG vai além da capacidade dos firewalls tradicionais, por isso ele contém alguns recursos de segurança avançados.

IDS: Sistema de Detecção de Intrusões

- Acelera e automatiza a detecção de ameaças de rede.
- Alerta administradores de segurança sobre ameaças em potencial.
- Envia alertas para uma ferramenta de segurança centralizada.
- **SIEM:** Sistema de gerenciamento de eventos e informações de segurança .
- Combina dados de outras fontes para ajudar as equipes de segurança a identificar e responder a ameaças cibernéticas que podem ser seguidas por outras medidas de segurança.

IPS: Sistema de Prevenção de Intrusões

- Mesmas funções de um IDS
- Monitora o tráfego de rede em busca de ameaças potenciais
- Automaticamente toma medidas para bloqueá-las
- Alerta a equipe de segurança, encerra conexões perigosas, remove conteúdo malicioso ou aciona outros dispositivos de segurança.

Filtragem de Conteúdo: Funcionalidade comum em Firewalls NG

- Permite que administradores controlem e monitorem o tipo de conteúdo que pode ser acessado por usuários na rede.
- Útil para aplicar políticas de segurança, proteção contra ameaças cibernéticas e garantir conformidade com regulamentos.
- Essas filtragens podem bloquear acesso a sites com base em URLs, palavras-chave, conteúdos de arquivos e protocolos de rede.

Filtragem de Aplicativos

- Permite que administradores controlem o acesso a aplicativos específicos com base em políticas de segurança.
- Não é filtrado o trafego com base apenas em endereços IP, portas ou protocolos
- A filtragem de aplicativos verifica o conteúdo dos pacotes de dados para identificar e controlar aplicativos individuais.

INTEGRAÇÃO COM TECNOLOGIAS EMERGENTES

O Firewall NG pode se integrar com tecnologias emergentes, envolvendo a implementação de software adicional.

Inteligência Artificial e Aprendizado de Máquina

- O firewall pode aprender com a experiência.
- Passar a reconhecer de forma automática comportamentos regulares e irregulares no tráfego de rede.
- **Automação:** Ao detectar um acesso indevido, ele pode agir imediatamente, como "fechar a porta de entrada" bloqueando o tráfego malicioso.

Análise de Big Data

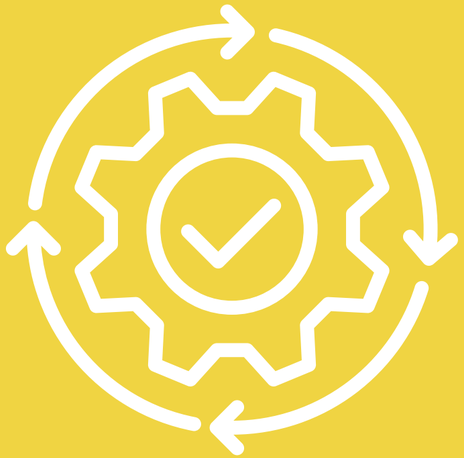
- Analisar grandes quantidades de informações sobre o comportamento de tráfego de rede.
- Ajudar na identificação de padrões de comportamento incomuns que podem indicar uma ameaça em potencial.

APIs e Integração de Plataforma

- O firewall pode se comunicar com outros sistemas de segurança.
- Como câmeras de vigilância (SIEM).
- Compartilhar informações sobre possíveis ameaças.

Segurança em Nuvem

- Pode proteger o acesso à entrada de diferentes locais.
- Nuvens públicas ou privadas.
- Verificar quem está tentando entrar e por onde.
- Garante que apenas autorizados tenham acesso.



GERENCIAMENTO E MONITORAMENTO

Muitos firewalls NG oferecem uma interface de gerenciamento centralizada, que permite aos administradores configurar e monitorar todos os aspectos da segurança da rede a partir de um único console.

Logging e Auditoria

- Mantêm registros detalhados de eventos de segurança relevantes.
- Tentativas de acesso não autorizado, tráfego bloqueado e atividades de firewall.
- Esses logs são fundamentais para investigações de segurança, análise de incidentes e conformidade regulatória.

Alertas e Notificações

- O firewall NG pode gerar alertas e notificações em tempo real sobre eventos de segurança importantes.
- Como tentativas de intrusão, tráfego suspeito ou violações de políticas.
- Esses alertas permitem uma resposta rápida a possíveis ameaças.

Relatórios Personalizados

- Os firewalls NG oferecem a capacidade de gerar relatórios personalizados sobre o desempenho e a segurança da rede.
- Esses relatórios podem incluir informações sobre tráfego, ameaças detectadas, atividades de usuários e conformidade com políticas de segurança.

Integração com SIEM

- Muitos firewalls NG podem ser integrados a sistemas de gerenciamento de informações e eventos de segurança (SIEM).
- Permitindo uma correlação mais avançada de eventos de segurança em toda a infraestrutura de TI e uma análise mais abrangente das ameaças em potencial.

Gerenciamento de Políticas de Segurança

- Os firewalls NG facilitam o gerenciamento de políticas de segurança.
- Permitindo aos administradores definir e aplicar regras granulares para controlar o tráfego de rede com base em critérios como aplicativos, usuários, horários e locais.

Auditoria de Configuração

- Alguns firewalls NG oferecem recursos de auditoria de configuração.
- Permitem aos administradores rastrear e revisar alterações nas configurações do firewall, garantindo conformidade e segurança contínuas.

Exemplos Next Generation Firewall...

Cisco Firepower Threat Defense (FTD)

- **Interface de Gerenciamento:** Cisco Firepower Management Center (FMC), que fornece uma plataforma centralizada para configurar políticas, monitorar eventos de segurança, analisar ameaças e gerar relatórios.

- **Recursos de Logging e Auditoria:** FMC mantém logs detalhados de eventos de segurança e oferece recursos avançados de análise de segurança.

- **Integração com SIEM:** Integrável com sistemas de gerenciamento de informações e eventos de segurança (SIEM) para uma visão holística da postura de segurança da rede.

Palo Alto Networks Next-Generation Firewall (NGFW)

- **Interface de Gerenciamento:** Panorama, uma plataforma centralizada para gerenciar políticas de segurança, monitorar tráfego de rede, analisar ameaças e criar relatórios personalizados.

- **Recursos de Logging e Auditoria:** Panorama fornece logs detalhados de eventos de segurança e oferece funcionalidades avançadas de auditoria.

- **Integração com SIEM:** Integrável com sistemas SIEM para uma correlação eficaz de eventos de segurança.

Fortinet FortiGate Next-Generation Firewall

- **Interface de Gerenciamento:** FortiManager, uma solução centralizada para gerenciamento de políticas, configuração de dispositivos, monitoramento de segurança e geração de relatórios.

- **Recursos de Logging e Auditoria:** FortiManager oferece recursos robustos de logging e auditoria para análise de eventos de segurança.

- **Integração com SIEM:** Integrável com sistemas SIEM para uma análise abrangente de eventos de segurança em toda a infraestrutura

IMPLEMENTAÇÕES E CASOS DE USO

Filtragem de Pacotes Avançada

- Os NGFWs oferecem filtragem de pacotes em nível de aplicativo.
- Permitindo inspeção profunda do tráfego para identificar e bloquear ameaças em potencial.
- Isso inclui inspeção de camada 7 (aplicação) para identificar e bloquear tráfego malicioso.

Prevenção de Intrusões (IPS)

- Muitos NGFWs incluem recursos de Prevenção de Intrusões (IPS).
- Para detectar e bloquear tentativas de exploração de vulnerabilidades conhecidas em sistemas e aplicativos.

Controle de Aplicativos

- Os NGFWs podem controlar e monitorar o uso de aplicativos na rede.
- Permitindo políticas granulares para permitir, bloquear ou restringir o acesso a aplicativos específicos com base em políticas de segurança.

Filtragem de Conteúdo Web

- Alguns NGFWs oferecem recursos de filtragem de conteúdo da web.
- Para bloquear sites maliciosos, URLs suspeitas e conteúdo indesejado.
- Ajudando a proteger os usuários contra ameaças da web.

Inspeção SSL/TLS

- Com o aumento do uso de criptografia SSL/TLS para proteger o tráfego da web, os NGFWs podem inspecionar o tráfego criptografado para identificar e bloquear ameaças ocultas dentro desse tráfego criptografado.

Segurança Avançada contra Ameaças (ATP)

- Alguns NGFWs oferecem recursos avançados de segurança contra ameaças, como detecção de malware avançado, análise comportamental e sandboxing para identificar e bloquear ameaças desconhecidas.

DESAFIOS E TENDÊNCIAS FUTURAS

NGFWs enfrentam uma série de desafios e estão sujeitos a várias tendências futuras devido à evolução constante das tecnologias de rede e segurança.

Crescente Complexidade das Ameaças

- Com o aumento da sofisticação das ameaças cibernéticas, os firewalls NG enfrentam o desafio de acompanhar e responder efetivamente a ataques cada vez mais complexos, como ataques de ransomware, ataques de dia zero e ataques de engenharia social.

NFV e SDN

- A virtualização de funções de rede (NFV) e redes definidas por software (SDN) estão transformando a arquitetura de redes, o que afeta diretamente os firewalls NG.
- Eles precisam se adaptar para operar eficientemente em ambientes virtualizados e programáveis, garantindo segurança sem comprometer o desempenho da rede.

Adoção de Nuvem e Mobilidade

- Com a crescente adoção de serviços em nuvem e o aumento do trabalho remoto, os firewalls NG precisam se adaptar para proteger efetivamente redes distribuídas, incluindo infraestruturas de nuvem pública, privada e híbrida, bem como dispositivos móveis e usuários remotos.

Visibilidade e Análise Avançada

- Com o aumento do volume e da diversidade dos dados de tráfego de rede, os firewalls NG precisam oferecer maior visibilidade e capacidades avançadas de análise para identificar padrões de comportamento suspeitos, anomalias de tráfego e violações de segurança em tempo real.

Integração de IA e Machine Learning

- Para lidar com a crescente complexidade das ameaças, os firewalls NG estão incorporando cada vez mais recursos de inteligência artificial (IA) e aprendizado de máquina (ML) para detecção proativa de ameaças, análise comportamental de tráfego e automação de respostas de segurança.

Integração com Ecossistemas de Segurança

- Para oferecer uma proteção eficaz contra ameaças cibernéticas em constante evolução, os firewalls NG estão se integrando cada vez mais a ecossistemas de segurança mais amplos, que incluem soluções de análise de segurança, inteligência de ameaças e serviços de resposta a incidentes.

NEXT GENERATION
FIREWALL