Universidade Federal do Piauí - CSHNB

Auditoria e Segurança de Sistema de Informação

Professor: Júlio Vítor Monteiro Marques

João dos Santos Neto

Jamile Jovita da Silva

Luís Clício Carvalho Sá

Ueslei Ferreira dos Reis Ribeiro

Relatório sobre Ferramentas e Medidas de Segurança: Redes Virtuais, Firewalls e Antivírus

Picos - PI, 2023

O firewall é parte integrante do cenário da segurança cibernética. Ele atua como uma barreira entre a rede privada e ameaças do mundo exterior, como ataques maliciosos, malware e acesso não autorizado. O principal objetivo de um firewall é monitorar, controlar e, em muitos casos, bloquear o tráfego de dados com base em regras e protocolos de segurança predefinidos.

Ao fazer isso, o firewall desempenha um papel fundamental na prevenção de ataques cibernéticos, protegendo a integridade, a confidencialidade e a disponibilidade das informações que circulam pela rede. Amplamente utilizado em ambientes comerciais e domésticos, este componente essencial é uma importante linha de defesa contra as crescentes ameaças digitais na era da conectividade.

Existem algumas medidas de segurança e ferramentas que ajudam no fortalecimento de uma rede por meio de um firewall, como a Filtragem de Pacotes, Inspeção de Estado, Proxy de Aplicação, Web Application Firewall, Sandboxing e Sistema de Detecção de Intrusão. Ambas trabalham em conjunto, e são essenciais para assegurar a segurança do tráfego da rede, além de garantir a integridade dos dados trafegados.

A Filtragem de Pacotes em firewalls é uma abordagem fundamental que opera no nível básico da comunicação de rede. Analisando pacotes individuais com base em regras predefinidas, como endereços IP, portas e protocolos, ela permite ou bloqueia pacotes conforme os critérios estabelecidos. Essa medida eficaz previne tráfego indesejado e ataques simples, como varreduras de portas e pacotes maliciosos.

O Stateful Inspection (Inspeção de Estado) é uma abordagem avançada que vai além da filtragem de pacotes. Monitorando o estado da comunicação em andamento, o firewall mantém uma tabela de estado para tomar decisões mais inteligentes com base no contexto da conexão. Essa compreensão do estado permite ao firewall identificar e bloquear ataques mais sofisticados, como negação de serviço (DoS) e ataques de força bruta, proporcionando uma camada adicional de segurança.

O Proxy de Aplicação atua como intermediário entre a rede interna e a internet, recebendo e encaminhando solicitações de clientes. Diferentemente da filtragem de pacotes, ele inspeciona o tráfego de aplicativos em profundidade, analisando o conteúdo das solicitações e respostas. Com base em políticas de segurança avançadas, o proxy pode bloquear ou permitir tráfego, oferecendo uma camada adicional de segurança. Sua capacidade de realizar inspeção profunda de pacotes ajuda a detectar e bloquear ameaças específicas de aplicativos, protegendo contra ameaças que podem passar despercebidas em firewalls convencionais.

O Web Application Firewall (WAF) é um firewall especializado que protege aplicativos web contra ameaças como injeções SQL e cross-site scripting (XSS), monitorando e filtrando o tráfego entre o aplicativo e a Internet. Já as soluções de sandboxing executam aplicativos em ambientes isolados para identificar ameaças desconhecidas ou zero-day. Um Intrusion Detection System (IDS) monitora o tráfego em busca de comportamentos suspeitos, emitindo alertas em vez de bloquear ativamente o tráfego. Quando implementadas, essas ferramentas proporcionam uma proteção mais robusta contra ameaças específicas, desconhecidas e comportamentos suspeitos, fortalecendo assim a segurança da rede.

Relatório

1. Firewalls

Um firewall é o componente crucial na segurança de redes, atuando como uma barreira entre redes confiáveis e não confiáveis. Vamos destacar as informações mais importantes sobre firewalls, com foco em ferramentas e medidas de segurança.

Firewalls de hardware

Cisco ASA**:** Atua como firewalls, fornecendo uma variedade de recursos de segurança para proteger redes contra ameaças cibernéticas. O Cisco ASA oferece serviços avançados, como VPN (Rede Privada Virtual), inspeção de pacotes, prevenção contra intrusões (IPS), controle de aplicativos e filtragem de conteúdo. Essa abordagem integrada permite que as organizações implementem uma solução abrangente para proteção contra ameaças em suas redes.

Fortinet Fortigate **:** Semelhante ao Cisco ASA, o Fortigate oferece uma abordagem abrangente para a segurança de redes. Esses dispositivos combinam várias funções de segurança em um único hardware, incluindo firewall, VPN, prevenção contra intrusões (IPS), antivírus, filtragem de conteúdo e muito mais. O Fortigate é conhecido por sua segurança multicamada e pela capacidade de integrar serviços em nuvem, proporcionando uma defesa eficaz contra uma ampla variedade de ameaças cibernéticas.

A escolha entre Cisco ASA e Fortinet Fortigate muitas vezes depende das necessidades específicas da organização, das preferências do administrador de rede e da infraestrutura existente.

Firewalls de software

Iptables (Linux) : O iptables é uma ferramenta de filtragem de pacotes e sistema de tradução de endereços de rede (NAT) incorporada aos sistemas operacionais baseados em Linux. Ele permite configurar regras para controlar o tráfego de rede, decidindo quais pacotes são permitidos ou bloqueados. O iptables é essencialmente um firewall para sistemas Linux e fornece uma camada de segurança crítica para proteger servidores e dispositivos baseados nesse sistema operacional.

Principais características do iptables:

Filtragem de Pacotes

Tradução de Endereços de Rede (NAT)

Módulos Adicionais

Tabelas e Cadeias

Windows Firewall : O Windows Firewall é uma funcionalidade integrada aos sistemas operacionais Windows desde o Windows XP Service Pack 2. Ele oferece uma camada de segurança para proteger computadores Windows contra ameaças de rede. O Windows Firewall permite controlar o tráfego de entrada e saída com base em regras configuráveis pelo usuário.

Principais características do Windows Firewall:

Filtragem de Tráfego
Perfis de Rede
Monitoramento de Aplicações
Regras Predefinidas e Personalizadas
Integração com o Centro de Segurança do Windows
Tanto o iptables no Linux quanto o Windows Firewall são componentes fundamentais na segurança de sistemas operacionais, protegendo contra ameaças de rede e permitindo que os usuários configurem políticas de segurança adaptadas às suas necessidades específicas.

Ferramentas e Recursos de Firewalls

Proxy e Filtragem de Conteúdo:
Squid Proxy: O Squid é um servidor de proxy de código aberto amplamente utilizado em sistemas baseados em Unix e Linux. Ele atua como intermediário entre os clientes da rede (como navegadores da web) e os servidores, facilitando o acesso a recursos da Internet. O Squid Proxy tem várias funcionalidades, incluindo cache de conteúdo, controle de acesso, autenticação de usuários e filtragem de conteúdo.

Características importantes

Cache de Conteúdo
Controle de Acesso
Autenticação de Usuários
Aceleração SSL

DansGuardian: DansGuardian é um filtro de conteúdo de código aberto que geralmente é usado em conjunto com servidores de proxy, como o Squid, para fornecer uma camada adicional de filtragem de conteúdo. O DansGuardian é especialmente projetado para filtrar conteúdo da web com base em categorias e políticas predefinidas, tornando-o eficaz em ambientes onde é necessário um controle mais granular sobre o acesso à Internet.

O DansGuardian é frequentemente utilizado em escolas, bibliotecas e ambientes empresariais que buscam implementar políticas específicas de filtragem de conteúdo para garantir um ambiente de navegação seguro e controlado.

Características importantes

Filtragem de Conteúdo por Categoria
Configuração Flexível
Integração com Outros Proxies
Relatórios Detalhados
Filtragem Dinâmica

Detecção e Prevenção de Intrusões (IDS/IPS)

Snort: Snort é um sistema de prevenção contra intrusões (IPS) e sistema de detecção de intrusões (IDS) de código aberto. Ele foi desenvolvido pela Cisco e é mantido pela comunidade de software livre. O Snort é projetado para analisar o tráfego de rede em tempo real, identificar padrões de tráfego suspeitos ou maliciosos e responder proativamente para prevenir ou mitigar ameaças.

Características importantes

Análise de Pacotes em Tempo
Base de Dados de Assinaturas
Políticas de Segurança Configuráveis
Resposta Ativa
Integração com Outras Ferramentas

Suricata: Suricata é outra ferramenta de sistema de prevenção contra intrusões (IPS) e sistema de detecção de intrusões (IDS) de código aberto. Assim como o Snort, o Suricata é projetado para analisar o tráfego de rede em tempo real, identificar ameaças e responder de maneira proativa. O Suricata é conhecido por sua alta performance e suporte a protocolos avançados.
Ambas as ferramentas, Snort e Suricata, são fundamentais para a segurança de rede, fornecendo uma camada adicional de defesa contra ameaças cibernéticas.

Características importantes

Processamento Multithread
Assinaturas e Regras
Suporte a Protocolos Avançados
Resposta Ativa e Bloqueio de Tráfego
Modo IDS e IPS

Sistemas de Prevenção de Vazamento de Dados (DLP)

Symantec DLP: O Symantec DLP é uma solução de segurança da informação projetada para prevenir a perda de dados confidenciais e sensíveis. Essa solução ajuda as organizações a protegerem informações críticas, evitando vazamentos acidentais ou intencionais.

Características importantes

Descoberta de Dados Sensíveis
Monitoramento e Prevenção de Movimentação de Dados

Monitoramento de Comportamento do Usuário
Encriptação de Dados
Relatórios e Auditoria

McAfee Total Protection: O McAfee Total Protection é uma suíte de segurança abrangente oferecida pela McAfee, uma empresa líder em soluções de segurança cibernética. Essa suíte combina várias ferramentas de segurança para proteger dispositivos contra ameaças online, vírus, malware e outras formas de ataques.

Características importantes

Antivírus e Antimalware
Firewall Pessoal
Proteção contra Phishing
Controle Parental
Proteção de Identidade
Segurança de Navegação na Web

Ambas as soluções, Symantec DLP e McAfee Total Protection, são ferramentas essenciais para a segurança da informação e proteção contra ameaças cibernéticas. O Symantec DLP se concentra na prevenção da perda de dados, enquanto o McAfee Total Protection oferece uma abordagem mais ampla, protegendo dispositivos contra uma variedade de ameaças online.

VPN (Rede Privada Virtual)

OpenVPN: O OpenVPN é uma solução de software de código aberto que oferece a implementação de uma rede privada virtual (VPN). VPNs são usadas para estabelecer conexões seguras e criptografadas entre dispositivos ou redes através da Internet. O OpenVPN é conhecido por sua flexibilidade, confiabilidade e suporte multiplataforma, o que o torna uma escolha popular para implementação de VPN

Características importantes

Protocolos VPN Avançados
Segurança Avançada
Compatibilidade com Dispositivos Móveis
Código Aberto
Segurança
Suporte Multi Plataformas
Flexibilidade

Configuração e Gerenciamento Simplificados

Cisco AnyConnect: O Cisco AnyConnect é um cliente de VPN desenvolvido pela Cisco para fornecer conectividade segura a redes corporativas. Ele oferece uma ampla gama de recursos e é especialmente conhecido por seu uso em ambientes empresariais. O AnyConnect suporta vários protocolos VPN e fornece funcionalidades avançadas de segurança.

Características importantes

Protocolos VPN Avançados
Segurança Avançada
Compatibilidade com Dispositivos Móveis
Controle de Acesso Granular
Integração com Outras Soluções Cisco

Ambos o OpenVPN e o Cisco AnyConnect são utilizados para criar conexões VPN seguras, mas eles podem ser escolhidos com base nas necessidades específicas da organização, na infraestrutura existente e nos requisitos de segurança. O Cisco AnyConnect, em particular, é amplamente adotado em ambientes corporativos que buscam uma solução robusta e integrada.

2. Redes Virtuais

2.1. Introdução

As redes virtuais desempenham um papel crucial na esfera da segurança da informação ao facilitar a comunicação segura entre diversos dispositivos, ultrapassando o ambiente corporativo e abrangendo uma ampla gama de cenários. Estas redes possibilitam a interação segura entre computadores, máquinas virtuais (VMs), servidores virtuais e outros dispositivos distribuídos em diferentes locais e ambientes. Ao contrário das redes físicas tradicionais, que apresentam muitas vezes desafios em termos de segurança, as redes virtuais utilizam gerenciamento de software para criar túneis criptografados pela Internet, proporcionando uma camada adicional de proteção.

A natureza flexível das redes virtuais permite que dispositivos em várias regiões operem com os mesmos recursos encontrados em redes físicas convencionais, ao mesmo tempo em que reforça a segurança da comunicação. Essa abordagem é particularmente valiosa em ambientes distribuídos, como data centers em locais físicos distintos. Os administradores de segurança têm a capacidade de ajustar dinamicamente a configuração da rede, adaptando-se a diferentes aplicativos e atendendo a requisitos específicos de segurança, sem a necessidade constante de investir em hardware adicional.

Além disso, as redes virtuais proporcionam uma camada de mobilidade segura para cargas de trabalho, permitindo que elas se movam pela infraestrutura de rede sem comprometer a confidencialidade e integridade dos dados. A agilidade proporcionada pelas redes virtuais também facilita a implementação eficiente de medidas de segurança, como alterações rápidas nas políticas de firewall e detecção de intrusões.

Dessa forma, as redes virtuais não apenas ultrapassam a concepção convencional de conectividade, mas também fortalecem a postura de segurança de uma organização, oferecendo uma infraestrutura dinâmica e adaptável. Essa abordagem inovadora não apenas aprimora a eficiência operacional, mas também se alinha de maneira crucial com os princípios fundamentais da segurança da informação em ambientes distribuídos e globalmente conectados.

2.2. Técnicas para implantar redes virtuais

A utilização de redes virtuais traz consigo uma série de medidas de segurança que fortalecem a integridade e confidencialidade das informações em comparação com ambientes tradicionais. Uma das práticas-chave é a segregação de rede, uma estratégia fundamental para proteger dados sensíveis e mitigar riscos de segurança. Dentre as técnicas empregadas para a segregação de rede, destacam-se as VLANs (Virtual Local Area Networks), VXLANs (Virtual Extensible LANs) e VPNs (Virtual Private Networks).

Ao adotar redes virtuais, a segregação de rede é aprimorada por meio da criação de redes locais virtuais, onde o agrupamento é configurado por software. Isso permite que dispositivos em diferentes switches de rede se comportem como se estivessem conectados a um único switch, enquanto máquinas fisicamente conectadas podem ser mantidas em redes separadas, evitando a necessidade de conexão física através de equipamentos e hardware de cabeamento.

As VLANs representam uma abordagem eficaz para a segregação de rede virtual. Elas dividem uma rede física em várias redes virtuais lógicas, isolando o tráfego entre essas VLANs e, assim, aumentando a segurança. Cada VLAN é tratada como uma rede independente, com políticas de segurança específicas.

Por outro lado, as VXLANs são uma extensão da segregação de rede, projetadas para ambientes de data centers virtuais e em nuvem. Elas utilizam cabeçalhos adicionais para encapsular o tráfego, possibilitando a criação de redes virtuais em larga escala e superando limitações tradicionais.

Já as VPNs, por sua vez, oferecem uma camada adicional de segurança ao criar túneis criptografados sobre redes públicas, permitindo que dispositivos remotos acessem recursos de rede de maneira segura. Isso é particularmente relevante em ambientes distribuídos, pois os dados transmitidos pela VPN são protegidos contra interceptação e manipulação.

Essas medidas de segurança, combinadas com a flexibilidade e eficiência de gerenciamento proporcionadas por redes virtuais, resultam em ambientes mais resilientes e adaptáveis. A capacidade de acessar, conectar, proteger e modificar recursos é otimizada, tornando o gerenciamento de rede mais acessível, econômico e robusto em termos de segurança da informação.

2.2.1. VLANs

As Redes Virtuais Locais (VLANs) são uma parte essencial da arquitetura de rede moderna, fornecendo segmentação de rede, segurança aprimorada, e controle eficiente do tráfego de rede.

As VLANs operam agrupando um subconjunto de dispositivos que compartilham uma LAN física, isolando o tráfego para cada grupo. Eles funcionam aplicando tags aos quadros de rede e lidando com essas tags nos sistemas de rede, criando a aparência e a funcionalidade de tráfego de rede que está fisicamente em uma única rede, mas se comporta como se estivesse dividida entre redes separadas.

Existem diferentes tipos de VLANs que podem ser implementados na arquitetura da rede, dependendo de como eles são configurados e usados em uma rede. Os tipos mais comuns de VLANs são:

- VLANs baseados em portas: São frequentemente usados em redes pequenas e são baseados em portas físicas ou interfaces em switches de rede. Os computadores host conectados a portas específicas em um switch são atribuídos a uma VLAN específica, e os dispositivos conectados a essas portas fazem parte automaticamente dessa VLAN.

- VLANs baseados em tags: A associação à VLAN é determinada por marcar quadros Ethernet com um ID de VLAN em VLANs baseados em tags, que permite que várias VLANs coexistam em um único tronco físico (link).

- VLANs baseados em protocolos: essas VLANs são menos comuns do que as VLANs baseadas em portas e tags porque são baseadas no tipo de protocolo que o tráfego está usando, como IP ou IPX, em vez de uma porta ou tag.

A segurança das VLANs é crucial para prevenir acesso não autorizado e violações de dados, mitigar riscos de segurança potenciais e manter a integridade do tráfego de rede dentro de cada VLAN. As VLANs podem proteger contra acesso ilegal ou intervenção isolando diferentes tipos de tráfego.

Para a implantação de VLANs, os switches de rede são a principal tecnologia utilizada. Os switches de rede permitem que os administradores de rede agrupem dispositivos em VLANs com base em portas físicas ou interfaces em switches de rede. A configuração de

VLANs é feita por meio de comandos específicos fornecidos pelo fabricante do switch de rede.

2.2.2. VXLANs

As Redes Extensíveis Virtuais Locais (VXLANs) são uma extensão da VLAN que permite a segmentação de rede em uma escala maior e mais flexível. Elas foram projetadas para fornecer a mesma funcionalidade das VLANs, mas com maior extensibilidade e flexibilidade. A segurança das VXLANs é crucial para prevenir acesso não autorizado e violações de dados.

VXLANs são usadas para realizar a segmentação de rede além do que as VLANs clássicas podem oferecer. As VLANs clássicas oferecem apenas 4.094 redes virtuais, enquanto as VXLANs oferecem até 16 milhões. A segmentação de rede tem dois usos principais: permitir que vários inquilinos compartilhem uma única rede física sem ver o tráfego uns dos outros e permitir a reutilização do espaço de endereços IP, o que pode ajudar a reduzir o desperdício de recursos de rede.

Para a implantação de VXLANs, os switches de rede também são a principal tecnologia utilizada. Além disso, em um ambiente com um controlador (como um VMware NSX ou controlador Juniper Networks Contrail).

2.2.3. VPNs

As Redes Privadas Virtuais (VPNs) são uma tecnologia de segurança de rede que permite a criação de uma conexão segura e criptografada entre dois pontos em uma rede pública, como a internet. As VPNs criam um túnel seguro entre o dispositivo do usuário e a rede privada, garantindo que os dados transmitidos pela conexão permaneçam confidenciais e protegidos contra espionagem ou acesso não autorizado.

As medidas de segurança que as VPNs impõem incluem criptografia de dados, acesso remoto seguro, anonimato e a capacidade de contornar restrições geográficas. A criptografia de dados é uma das principais medidas de segurança que as VPNs fornecem, tornando os dados transmitidos pela rede ilegíveis para usuários não autorizados. Isso garante a confidencialidade das informações sensíveis. Além disso, as VPNs permitem o acesso remoto seguro às redes privadas, permitindo que os funcionários trabalhem remotamente enquanto mantêm uma conexão segura com os recursos da empresa.

As VPNs também podem fornecer anonimato ao mascarar o endereço IP do usuário, tornando difícil para terceiros rastrearem suas atividades online. Além disso, as VPNs permitem que os usuários contornem restrições geográficas e acessem conteúdo que pode ser

bloqueado em sua região. Elas também são comumente usadas para conectar filiais de uma empresa, ou para conectar uma rede de uma empresa a uma rede de outra empresa. Essa conexão permite que os usuários acessem recursos na rede conectada como se estivessem fisicamente conectados à rede local. Isso é útil para empresas que têm várias localizações geográficas e precisam compartilhar recursos e informações entre elas.

Para implantar VPNs, é necessário escolher um protocolo VPN, configurar um servidor VPN e configurar os clientes VPN. Os servidores VPN atuam como o gateway entre o dispositivo do usuário e a rede privada. Os clientes VPN são configurados para estabelecer uma conexão com o servidor VPN. Existem vários protocolos VPN disponíveis, cada um com suas próprias forças e fraquezas. Alguns dos protocolos comumente usados incluem Wireguard, OpenVPN, IPSec e L2TP/IPSec.

3. Antivírus

3.1. Introdução

O antivírus é um software que identifica e protege os dispositivos de malwares, também conhecidos como vírus. Esse programa pode ser instalado em computadores e dispositivos móveis, como celulares e tablets. A função mais simples de um antivírus é monitorar arquivos e outros programas de um dispositivo para detectar vírus. Quando novas aplicações são instaladas, o programa faz a verificação delas para saber se existe alguma ação suspeita. Se algo foi identificado, a instalação é bloqueada ou a nova aplicação é encaminhada para a quarentena.

A quarentena é um espaço de proteção criptografado e gerenciado pelo antivírus, para que o possível vírus não se espalhe pelo sistema operacional do dispositivo. Arquivos e programas são encaminhados para a quarentena quando o antivírus ainda não identificou exatamente o tipo de vírus ou problema apresentado.

3.2. Medidas de segurança

Escaneamento de vírus conhecidos: o antivírus compara os arquivos e programas do seu dispositivo com uma lista de assinaturas de malwares conhecidos, e bloqueia ou remove aqueles que são identificados como perigosos.

Sensoriamento heurístico: o antivírus analisa o comportamento dos arquivos e programas do seu dispositivo, e detecta possíveis malwares que ainda não foram registrados na lista de assinaturas. Esse recurso permite que o antivírus se adapte às novas ameaças que surgem constantemente.

Quarentena: o antivírus isola os arquivos e programas suspeitos em um espaço seguro, onde eles não podem se espalhar ou causar mais problemas. A quarentena permite que o usuário decida se quer restaurar, excluir ou enviar os arquivos para análise.

Proteção em tempo real: o antivírus monitora constantemente as atividades do seu dispositivo, e verifica se há malwares em downloads, e-mails, sites, redes sociais e outros serviços online. Esse recurso previne que você seja infectado por acidentes ou descuidos.

Atualização automática: o antivírus se mantém atualizado com as últimas informações sobre malwares, e baixa as novas assinaturas e versões do programa. Esse recurso garante que o antivírus esteja sempre pronto para enfrentar as ameaças mais recentes.

3.3. Ferramentas

Existem muitas marcas de antivírus no mercado, cada uma com suas características, vantagens e desvantagens. Algumas das mais populares são:

360 Total Security: um antivírus gratuito que combina quatro motores de detecção, dois da própria empresa Qihoo e dois de parceiros Bitdefender e Avira. Ele oferece proteção em tempo real, limpeza de arquivos inúteis, otimização de desempenho e outros recursos.

Avira: um antivírus que possui versões gratuita e paga, com uma interface simples e intuitiva. Ele detecta e elimina malwares, spywares, ransomwares e outras ameaças, além de oferecer proteção de privacidade, VPN, gerenciador de senhas e outros recursos.

AVG: um antivírus que também possui versões gratuita e paga, com uma interface moderna e fácil de usar. Ele protege o computador de vírus, spywares, ransomwares e outras ameaças, além de oferecer otimização de desempenho, bloqueio de webcam, VPN e outros recursos.

Avast: um antivírus que é um dos mais populares do mundo, com mais de 400 milhões de usuários. Ele possui versões gratuita e paga, com uma interface amigável e personalizável. Ele protege o computador de malwares, spywares, ransomwares e outras ameaças, além de oferecer proteção de rede, senha, navegador e outros recursos.