# 1.Fundamentos de uma rede segura

## 1.1 Princípios de redes seguras

As redes seguras devem considerar os princípios da segurança da informação: confidencialidade, integridade e disponibilidade

## 1.2 Fraquezas em redes seguras

Os principais pontos fracos em redes seguras são:

- **Pontos únicos de falha:** Referem-se a componentes, sistemas ou pontos na infraestrutura de rede que, se falharem, podem causar interrupções significativas ou falhas completas no funcionamento da rede. Esses pontos podem ser dispositivos críticos, como servidores ou roteadores, ou até mesmo conexões específicas. Em uma rede segura, é fundamental identificar esses pontos de falha e implementar medidas de redundância ou alternativas para evitar que uma única falha cause grandes problemas.
- **Dependências complexas:** Elas surgem quando vários componentes de rede estão interligados de maneira intrincada e dependem uns dos outros para funcionar corretamente. Se um desses componentes falhar ou for comprometido, isso pode afetar todo o sistema de rede. É importante compreender e gerenciar essas dependências para garantir que qualquer problema em um componente não cause um efeito cascata em toda a rede.
- **Disponibilidade acima de confidencialidade e integridade:** Este princípio estabelece que, em algumas situações, é preferível priorizar a disponibilidade da rede em vez de se concentrar exclusivamente na confidencialidade e integridade dos dados. Em certos contextos, como ambientes de negócios que dependem fortemente da disponibilidade contínua da rede, pode ser necessário tomar medidas que possam comprometer temporariamente a confidencialidade e a integridade dos dados. No entanto, é crucial encontrar um equilíbrio adequado entre esses três aspectos, garantindo que a segurança seja mantida sem prejudicar significativamente a disponibilidade.
- **Falta de documentação e controle de mudanças:** Quando as alterações na infraestrutura de rede não são devidamente registradas, documentadas e controladas, pode haver erros, falhas de configuração ou brechas de segurança introduzidas inadvertidamente. É essencial ter processos e procedimentos bem definidos para documentar todas as alterações e garantir que elas sejam revisadas, aprovadas e implementadas de forma segura.
- **Dependência exagerada na segurança perimetral:** Refere-se a uma abordagem em que a maioria dos esforços de segurança é concentrada na proteção da fronteira externa da rede. Embora a segurança perimetral seja importante, confiar exclusivamente nela pode deixar a rede vulnerável a ataques internos e violações. É crucial adotar uma abordagem em camadas, implementando medidas de segurança em toda a rede, em vez de apenas nos limites externos, para garantir uma proteção abrangente contra ameaças internas e externas.

## 1.3 Principais equipamentos de rede

Os seguintes equipamentos de rede devem estar presente na arquitetura de uma rede:

- **Switch (comutador):** É um dispositivo de rede presente na camada 2, a camada de enlace de dados, do modelo OSI. Ele é responsável por direcionar o tráfego de rede com base nos endereços MAC dos dispositivos conectados a ele. O switch permite a comunicação direta entre os dispositivos na mesma rede local (LAN), melhorando o desempenho e a segurança ao segmentar o tráfego em diferentes portas.
- **Wireless access point (WAP):** São dispositivos que operam na camada 2 (enlace de dados) e na camada 3 (rede) do modelo OSI. Eles permitem que os dispositivos sem fio, como laptops, smartphones e tablets, se conectem a uma rede local (LAN) sem a necessidade de cabos. Os pontos de acesso sem fio fornecem conectividade Wi-Fi, permitindo que os dispositivos se comuniquem entre si e acessem recursos da rede.
- **Roteadores:** São dispositivos de rede que operam na camada 3, a camada de rede, do modelo OSI. Eles são responsáveis por encaminhar pacotes de dados entre diferentes redes, determinando a melhor rota com base nas informações contidas nos cabeçalhos IP. Os roteadores são essenciais para a comunicação entre diferentes sub-redes ou redes remotas.
- **Firewalls:** São dispositivos de segurança de rede que operam nas camadas 3 (rede) e 4 (transporte) do modelo OSI. Eles monitoram e controlam o tráfego de rede, filtrando pacotes com base em regras predefinidas. Os firewalls ajudam a proteger a rede contra ameaças externas, como ataques de hackers, filtrando o tráfego indesejado ou malicioso.
- **Balanceamento de carga:** Os balanceadores de carga estão presentes na camada 4 (transporte) e, às vezes, na camada 7 (aplicação) do modelo OSI. Eles distribuem o tráfego de rede de forma equilibrada entre vários servidores para otimizar o desempenho e garantir a disponibilidade dos serviços. Os balanceadores de carga ajudam a evitar sobrecargas em servidores individuais e melhoram a escalabilidade e a confiabilidade dos aplicativos e serviços.
- **Servidores Domain Name System (DNS):** Os servidores DNS estão presentes na camada 7 (aplicação) do modelo OSI. Eles são responsáveis por traduzir nomes de domínio, como "www.exemplo.com", em endereços IP correspondentes para permitir a comunicação entre os dispositivos na Internet. Os servidores DNS ajudam a direcionar as solicitações de recursos de rede para os servidores corretos, facilitando a navegação na web e a comunicação em rede.

## 1.4 Encaminhamento de tráfego

O encaminhamento de tráfego no switching e roteamento é o processo de direcionar pacotes de dados de uma origem para um destino em uma rede. No switching, os switches de rede analisam o endereço MAC de destino em um pacote e o encaminham para a porta correta dentro da mesma rede local (LAN) com base em uma tabela de endereços MAC conhecida como tabela CAM.

Já no roteamento, os roteadores examinam o endereço IP de destino em um pacote e tomam decisões de roteamento com base em tabelas de roteamento que contêm informações sobre as redes vizinhas e os melhores caminhos para alcançar o destino desejado.

## 1.5 Internet Protocol (IP)

O Internet Protocol (IP) opera na camada de rede (camada 3) do modelo OSI e é responsável pelo encaminhamento dos pacotes de dados de origem para destino em uma rede. Utiliza endereços IP para identificar os dispositivos na rede. Cada dispositivo conectado a uma rede IP possui um endereço IP exclusivo, que é composto por uma combinação de números. Existem dois principais padrões de IP em uso atualmente: IPv4 e IPv6.

Quando um dispositivo envia um pacote de dados para outro dispositivo em uma rede, ele encapsula os dados dentro de um pacote IP. O pacote IP contém informações essenciais, como o endereço IP de origem e o endereço IP de destino.

Ao receber um pacote IP, os roteadores são responsáveis por encaminhar o pacote em direção ao seu destino. Eles examinam o endereço IP de destino e consultam suas tabelas de roteamento para determinar a melhor rota para o pacote. O roteador encaminha o pacote para o próximo salto na rota até que alcance o destino final.

Além do encaminhamento, o IP também fornece serviços básicos, como o controle de fragmentação de pacotes, quando um pacote é muito grande para ser transmitido em uma única unidade, e a detecção de erros no cabeçalho do pacote.

## 1.6 Address Resolution Protocol (ARP)

O Address Resolution Protocol (ARP) é um protocolo de rede utilizado para associar endereços de camada de rede (endereços IP) a endereços de camada de enlace de dados (endereços MAC). Ele opera na camada 2 (enlace de dados) e é essencial para o funcionamento das redes locais (LANs).

Quando um dispositivo precisa enviar um pacote de dados para outro dispositivo em uma mesma rede local, ele utiliza o endereço IP de destino para encapsular o pacote. No entanto, para que o pacote seja corretamente entregue, o endereço IP precisa ser associado a um endereço MAC, que é o endereço físico exclusivo atribuído a cada placa de rede.

ARP é responsável por essa resolução de endereço. Quando um dispositivo precisa descobrir o endereço MAC correspondente a um determinado endereço IP, ele envia uma mensagem de ARP na rede local, conhecida como ARP Request (Solicitação ARP).

Essa mensagem contém o endereço IP do destino que se deseja alcançar. Os dispositivos na rede recebem a mensagem de ARP Request e verificam se o endereço IP solicitado corresponde ao seu próprio endereço. Se houver correspondência, o dispositivo envia uma mensagem de ARP Reply (Resposta ARP) contendo seu endereço MAC.

O dispositivo que fez a solicitação de ARP recebe a resposta contendo o endereço MAC e, em seguida, pode enviar o pacote encapsulado com o endereço MAC de destino correto. Isso permite que o pacote seja entregue ao dispositivo de destino na mesma rede local.

Adicionalmente, os dispositivos em uma rede local mantêm uma tabela ARP, conhecida como cache ARP, que armazena as informações de mapeamento entre endereços IP e endereços MAC já resolvidos. Essa tabela é atualizada periodicamente ou quando ocorrem alterações na rede.

## 1.7 Segmentação de rede

Refere-se à divisão de uma rede maior em sub-redes menores ou segmentos independentes. Essa prática de segmentação de rede é usada para melhorar a segurança, o desempenho e a eficiência da rede como um todo. Cada segmento de rede pode ser isolado logicamente ou fisicamente dos outros, criando uma separação entre os dispositivos e os recursos conectados a cada segmento.

A segmentação de rede tem vários benefícios. Em termos de segurança, ela ajuda a limitar a propagação de ameaças e ataques cibernéticos, uma vez que um incidente em um segmento de rede não afeta diretamente os outros.

Além disso, a segmentação facilita a aplicação de políticas de segurança específicas em cada segmento, restringindo o acesso a recursos sensíveis apenas para usuários autorizados. Em relação ao desempenho, a segmentação de rede permite a otimização do tráfego, evitando congestionamentos e melhorando a qualidade do serviço.

Ela também ajuda na segregação de diferentes tipos de tráfego, como voz, vídeo e dados, garantindo uma alocação eficiente de recursos e uma experiência de usuário mais satisfatória.

## 1.8 Segregação de rede

Refere-se à separação lógica ou física de diferentes segmentos de rede. Pode ser alcançada por meio de várias técnicas, como o uso de VLANs (Virtual LANs), sub-redes ou firewalls. A segregação tem o objetivo de evitar a comunicação direta e não autorizada entre diferentes segmentos de rede, garantindo que apenas o tráfego permitido seja permitido entre eles.

Ao implementar a segregação, as organizações podem reduzir o risco de propagação de ameaças e minimizar a superfície de ataque. Ela permite um controle mais preciso sobre o fluxo de dados e ajuda a proteger informações sensíveis e recursos críticos, mantendo-os isolados de outros segmentos da rede.

## 2.Zonas e suas topologias

A Intranet e a Extranet são conceitos relacionados à segregação de redes com diferentes níveis de acesso e segurança. A zona de rede é uma área que agrupa dispositivos com um conjunto comum de requisitos de segurança e acesso.

## 2.1 Intranet

É uma rede interna de uma organização que é isolada do acesso externo não autorizado. Ela é projetada para fornecer comunicação e compartilhamento de informações dentro da organização. Geralmente, a Intranet é dividida em diferentes zonas de rede, como a zona interna e a zona de acesso restrito.

A zona interna é a área de rede mais segura, onde estão localizados os recursos e informações críticas da organização. A zona de acesso restrito permite que determinados usuários ou grupos acessem informações e recursos adicionais com base em suas permissões. O acesso à Intranet é controlado por firewalls e políticas de segurança que definem quem pode acessar quais áreas da rede.

## 2.2 Extranet

A Extranet estende a Intranet para fornecer acesso limitado a usuários externos, como clientes, fornecedores ou parceiros de negócios. Ela permite que esses usuários acessem recursos específicos da organização de forma controlada. A Extranet também pode ser dividida em zonas de rede, como a zona externa e a zona de parceiros.

A zona externa é a área menos confiável, que permite o acesso apenas a informações e serviços públicos da organização. Já a zona de parceiros concede acesso a usuários externos confiáveis, geralmente por meio de autenticação e autorização. A Extranet é protegida por firewalls e mecanismos de autenticação para garantir que apenas usuários autorizados possam acessar as áreas apropriadas.

## 2.3 DMZ

São áreas de uma rede de computadores que ficam separadas e isoladas das demais zonas de rede, com o objetivo de fornecer uma camada adicional de segurança. A DMZ atua como uma área intermediária entre a rede interna (intranet) e a rede externa (internet).

Uma DMZ é projetada para hospedar servidores, aplicativos ou serviços que precisam ser acessíveis a partir da internet, mas sem permitir um acesso direto à rede interna da organização. Essa separação cria uma barreira de proteção para impedir que ameaças externas cheguem aos recursos mais sensíveis e críticos da rede interna.

Dentro de uma DMZ, são implantados dispositivos como firewalls, servidores web, servidores de email e servidores de aplicativos públicos. Esses servidores são configurados com restrições de acesso e políticas de segurança específicas para limitar a exposição a possíveis ataques externos.

A DMZ pode ser implementada de diferentes maneiras, como descritas abaixo

## 2.4 Sub-rede com DMZ

A DMZ Screened Subnet, ou sub-rede com DMZ, é uma configuração comum em que uma rede intermediária é criada entre a rede externa e a rede interna. Nesse caso, um firewall é colocado entre a rede interna e a DMZ, e outro firewall é colocado entre a DMZ e a rede externa. A DMZ é uma área isolada onde são hospedados servidores e serviços que precisam ser acessíveis a partir da internet.

O firewall entre a DMZ e a rede interna possui regras de acesso que permitem apenas o tráfego necessário, protegendo a rede interna contra possíveis ameaças provenientes da DMZ. O firewall entre a DMZ e a rede externa controla o tráfego que entra e sai da DMZ, permitindo que apenas o tráfego autorizado chegue à rede interna. Essa configuração em camadas proporciona uma camada adicional de segurança e ajuda a proteger a rede interna contra ataques externos

## 2.5 Firewall triplamente protegido

Um Triple-Homed Firewall é um tipo de firewall que possui três interfaces de rede e pode ser usado para criar uma DMZ. No caso de um Triple-Homed Firewall, um único dispositivo é utilizado como roteador e firewall, possuindo três interfaces de rede. Uma das interfaces é conectada à rede interna da organização, a segunda interface é conectada à DMZ e a terceira interface é conectada à internet. Essa configuração permite que o tráfego de rede seja controlado de forma mais eficiente.

O firewall é responsável por monitorar e filtrar o tráfego que passa entre as interfaces. Ele pode aplicar políticas de segurança específicas para cada interface, controlando quais tipos de conexões são permitidas ou bloqueadas. Com um Triple-Homed Firewall, é possível definir regras de acesso para permitir que o tráfego da internet chegue à DMZ, permitindo assim que os serviços hospedados na DMZ sejam acessíveis externamente. Ao mesmo tempo, o firewall impõe restrições para evitar que o tráfego da DMZ acesse a rede interna diretamente, fornecendo uma camada adicional de proteção.

## 2.6 Host filtrado

É um servidor colocado em uma rede para fornecer um ponto de acesso seguro a recursos internos. Especificamente, um servidor proxy/gateway de duas interfaces, é um servidor que possui duas interfaces de rede conectadas a diferentes redes. Uma das interfaces está conectada à rede interna, enquanto a outra está conectada à rede externa, como a Internet. O servidor atua como um intermediário entre as duas redes, controlando e filtrando o tráfego que passa por ele.

Quando uma solicitação de um usuário externo é feita à rede interna, o servidor proxy/gateway recebe essa solicitação e a encaminha para o destino dentro da rede interna.

Ele atua como um intermediário para proteger os recursos internos, ocultando informações sobre a estrutura interna da rede.

O servidor proxy/gateway também pode fornecer funções adicionais de segurança, como filtragem de conteúdo, autenticação de usuários, inspeção de pacotes e balanceamento de carga. Ele pode analisar o tráfego, aplicar regras e políticas de segurança, e até mesmo armazenar em cache conteúdo comum para melhorar o desempenho da rede.

## 3.Considerações de design de redes seguras

- **Tráfego leste-oeste:** Refere-se à comunicação entre servidores e dispositivos dentro do próprio datacenter. Isso significa que os dados estão sendo trocados entre diferentes servidores e dispositivos internos ao ambiente. Essa comunicação é necessária para a interação entre aplicativos, o compartilhamento de recursos e a realização de processos de negócios dentro do datacenter. Para permitir o tráfego Leste-Oeste, os servidores são conectados a uma rede interna de alta velocidade, geralmente usando switches e roteadores de alto desempenho. Essa rede interna é projetada para fornecer uma conexão rápida e eficiente entre os dispositivos, permitindo a transferência de dados em alta velocidade e com baixa latência.
- **Tráfego norte-sul:** Refere-se à comunicação entre o datacenter e o mundo externo. Isso inclui a troca de dados entre os servidores no datacenter e a rede externa, como a Internet ou outras redes externas. O tráfego Norte-Sul geralmente envolve a comunicação entre usuários ou dispositivos externos e os serviços hospedados no datacenter, como sites, aplicativos ou armazenamento de dados. Para permitir o tráfego Norte-Sul, os datacenters geralmente têm uma conexão de alta velocidade com a Internet e implementam roteadores e firewalls para controlar e direcionar o tráfego externo. Esses dispositivos de rede garantem a segurança e a conformidade dos dados que entram e saem do datacenter.

## 4.Zero Trust

É uma abordagem que busca redefinir a maneira como as redes e os sistemas são protegidos. Tradicionalmente, os modelos de segurança de perímetro confiavam em uma defesa baseada na ideia de "confiança implícita". Ou seja, uma vez que um dispositivo ou usuário estivesse dentro do perímetro da rede, eles seriam considerados confiáveis e teriam acesso a recursos e dados.

Zero Trust adota uma mentalidade oposta, onde nenhum dispositivo ou usuário é confiável por padrão. Em vez disso, a segurança é baseada na autenticação, na autorização e na verificação contínua em todos os momentos. O princípio fundamental é que cada solicitação de acesso, seja de um dispositivo ou usuário interno ou externo, deve ser verificada e autenticada independentemente, independentemente de estar dentro ou fora do perímetro da rede.