



Módulo 12: Infraestrutura de segurança de rede



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do módulo: Infraestrutura de segurança de rede

Objetivo do módulo: Explicar como os dispositivos e serviços são usados para aprimorar a segurança da rede.

Título do Tópico	Objetivo do Tópico
Topologias de rede	Explicar como os projetos de rede influenciam o fluxo de tráfego pela rede.
Dispositivos de segurança	Explicar como os dispositivos especializados são usados para aprimorar a segurança da rede.
Serviços de segurança	Explicar como os serviços de rede melhoram a segurança da rede.

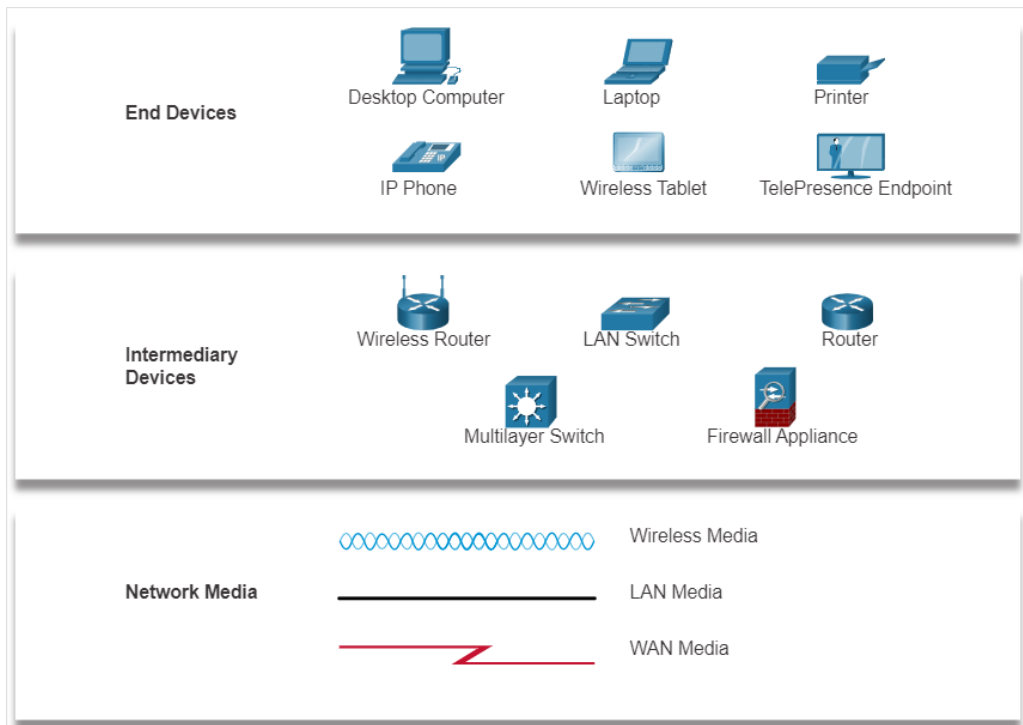
12.1 Topologias de rede

Infraestrutura de segurança de rede

Representações de rede

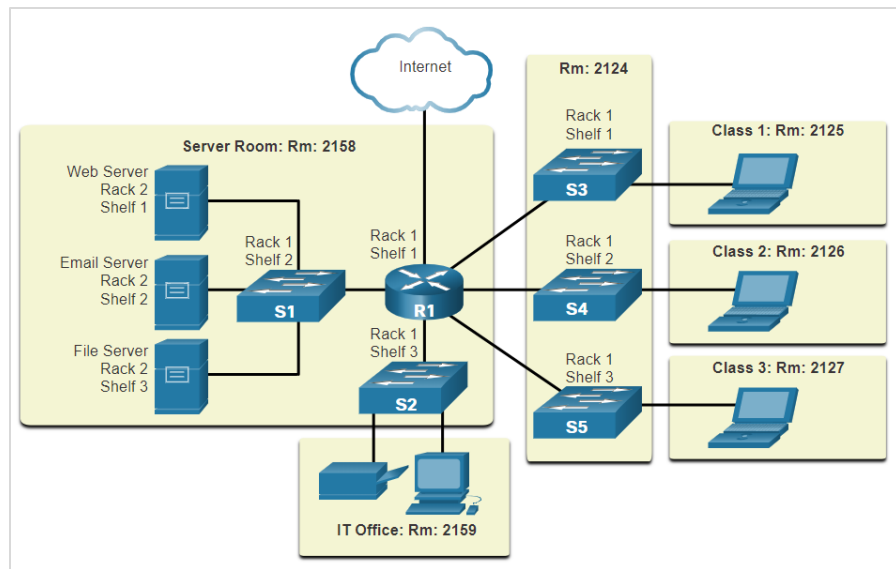
- Os diagramas de rede, geralmente chamados de diagramas de topologia, usam símbolos para representar diferentes dispositivos e conexões dentro da rede.
- As terminologias importantes a serem conhecidas incluem:
 - **Placa de rede**
 - **Porta Física**
 - **Interface**

Nota: Os termos porta e interface são frequentemente usados alternadamente.

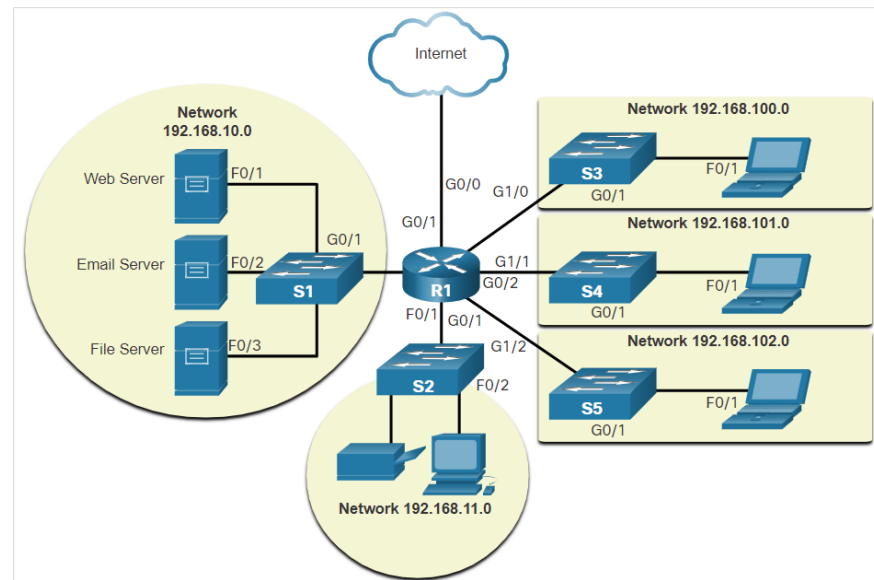


Diagramas de topologia de infra-estrutura de segurança de

Os diagramas de topologia física ilustram a localização física de dispositivos intermediários e a instalação de cabos.



Os diagramas de topologia lógica ilustram dispositivos, portas e o esquema de endereçamento da rede.



Redes de infraestrutura de segurança de rede de vários tamanhos

- Redes domésticas pequenas - conecte alguns computadores entre si e à Internet.
- Small Office and Home Office (SOHO) - permite que o computador em uma casa, escritório ou escritório remoto se conecte a uma rede corporativa ou acesse recursos compartilhados e centralizados.
- Redes de médio a grande porte - podem ter vários locais com centenas ou milhares de computadores interconectados.
- Redes mundiais - conecta centenas de milhões de computadores em todo o mundo - como a Internet.



Pequeno Home SOHO

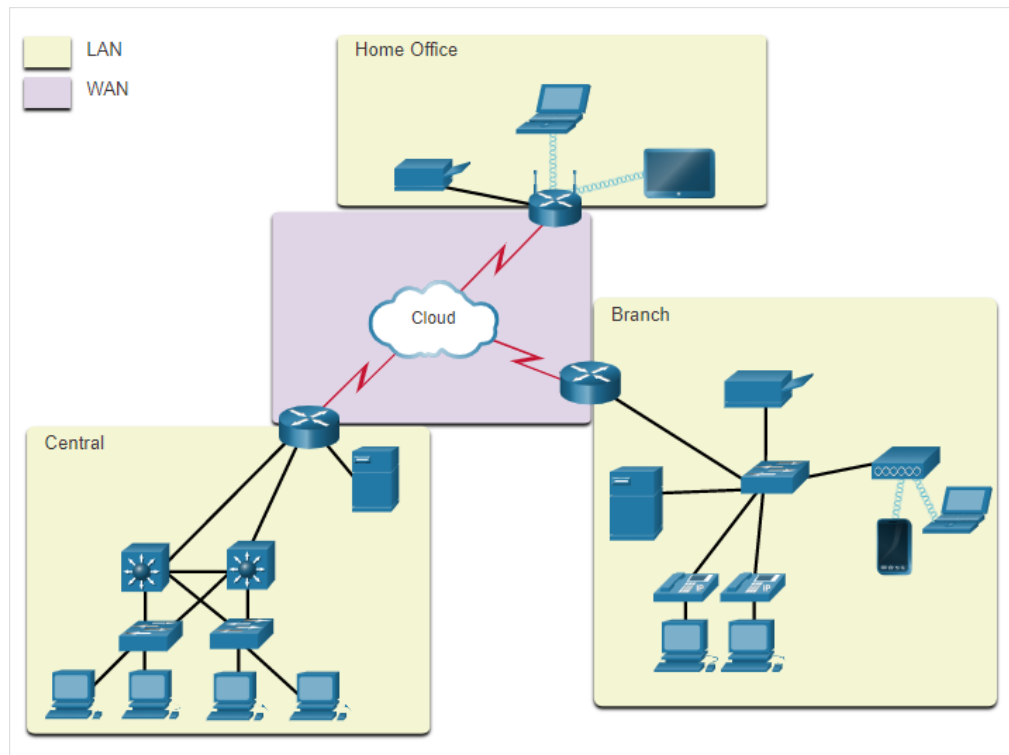


Médio/Grande Mundo

Topologias de rede

LANs e WANs

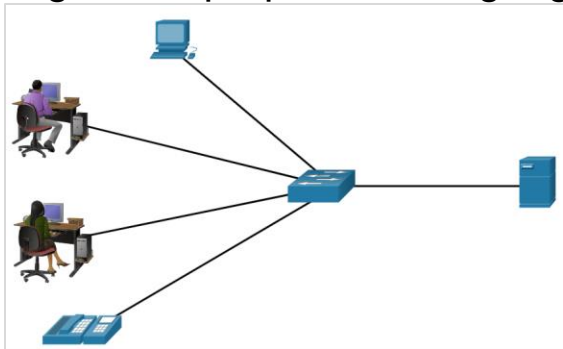
- As infra-estruturas de rede variam muito em termos de:
 - Tamanho da área coberta
 - Número de usuários conectados
 - Número e tipos de serviços disponíveis
 - Área de responsabilidade
- Os dois tipos mais comuns de infraestruturas de rede são
 - Redes locais (LANs)
 - Redes de longa distância (WANs)



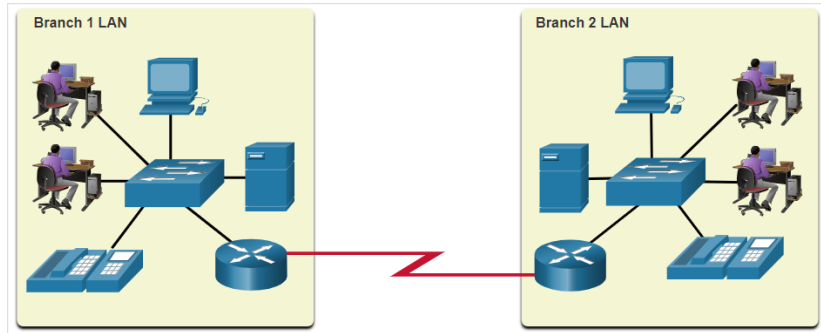
LANs conectadas a uma WAN

LANs e WANs (Cond.)

Uma LAN é uma infraestrutura de rede que abrange uma pequena área geográfica.



Uma WAN é uma infraestrutura de rede que abrange uma ampla área geográfica.



LAN (Local Area Network)

Interconecte dispositivos finais em uma área limitada.

Administrado por uma única organização ou indivíduo.

Fornecer largura de banda de alta velocidade para dispositivos finais internos e dispositivos intermediários.

WAN (Wide Area Network)

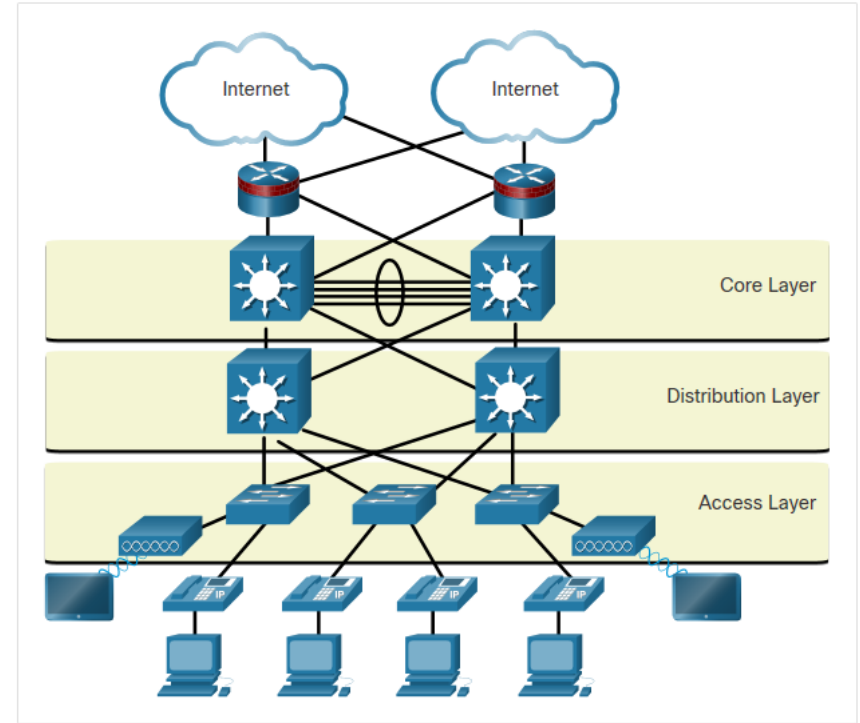
Interconecte LANs em áreas geográficas amplas.

Normalmente administrado por vários provedores de serviços.

Geralmente, fornece links de velocidade mais lenta entre LANs.

O modelo de projeto de rede de três camadas

- A LAN com fio do campus usa um modelo de design hierárquico para separar a topologia da rede em grupos ou camadas modulares.
- O design hierárquico da LAN inclui três camadas:
 - **Acesso** - Fornece terminais e usuários acesso direto à rede.
 - **Distribuição** - agrega camadas de acesso e fornece conectividade aos serviços.
 - **Core** - fornece conectividade entre camadas de distribuição para grandes ambientes de LAN.

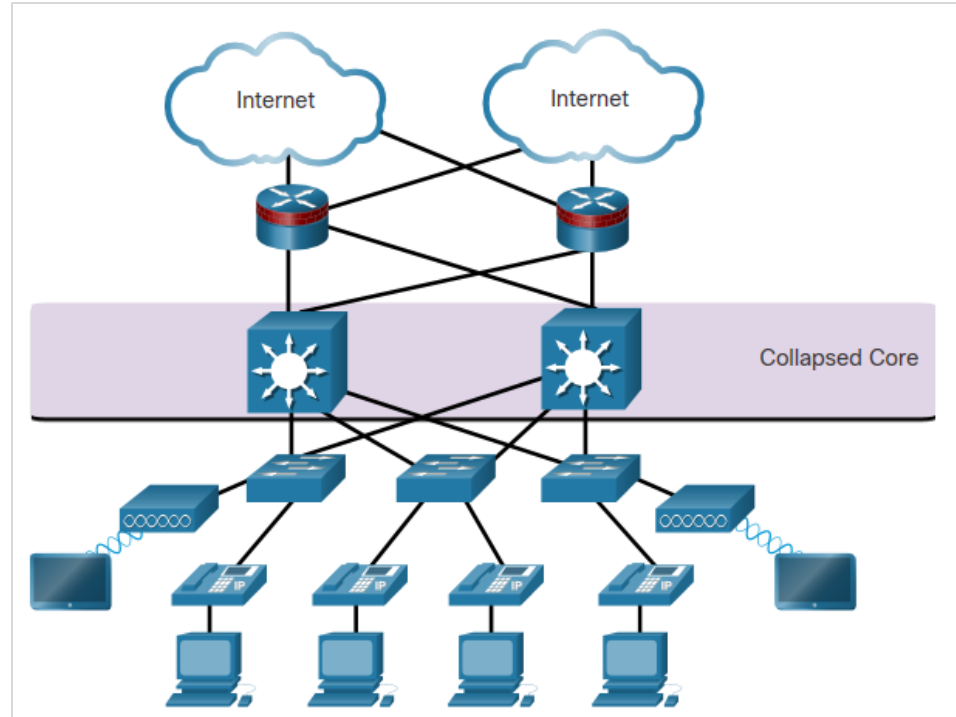


Modelo do projeto hierárquico

© 2020 Cisco e/ou suas afiliadas. Todos os direitos reservados.
Confidencial da Cisco

O modelo de projeto de rede de três camadas (Cont..)

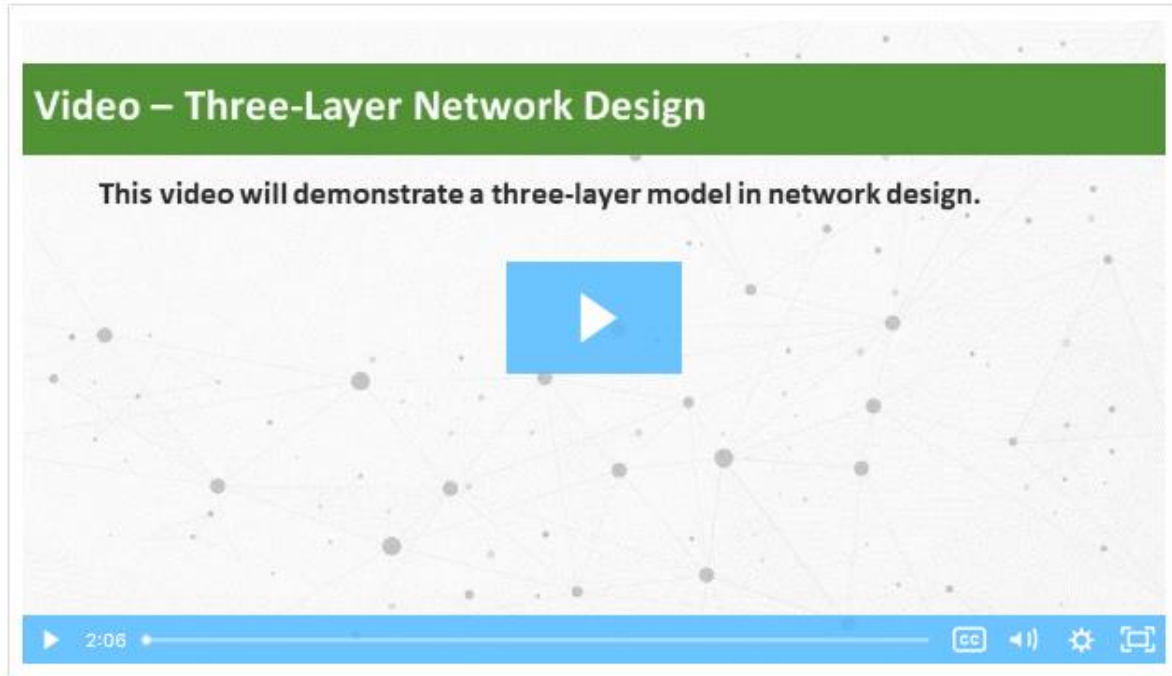
- Embora o modelo hierárquico tenha três camadas, algumas redes corporativas menores podem implementar um design hierárquico de duas camadas.
- Nesse projeto hierárquico de duas camadas, as camadas de núcleo e distribuição são agrupadas em uma camada, reduzindo assim o custo e a complexidade.



Switch de função dupla

Vídeo da Infraestrutura de Segurança de Rede - Projeto de Rede de Três Camadas

Reproduza o vídeo para ver uma demonstração do modelo de design de rede de três camadas.



Infraestrutura de segurança de rede

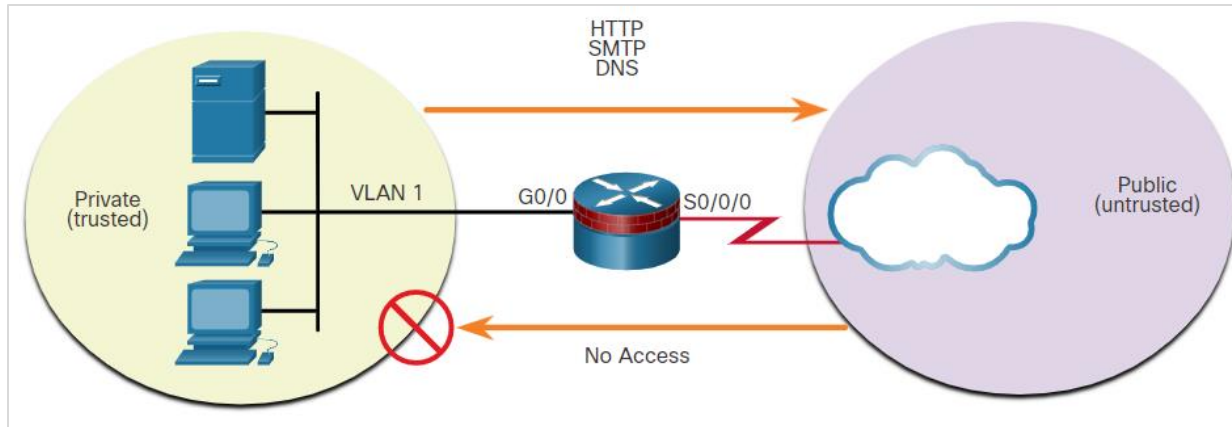
Arquiteturas de segurança

O design do firewall é principalmente sobre interfaces de dispositivo que permitem ou negam tráfego com base na origem, no destino e no tipo de tráfego.

Os três designs de firewall são:

- **Público e privado**

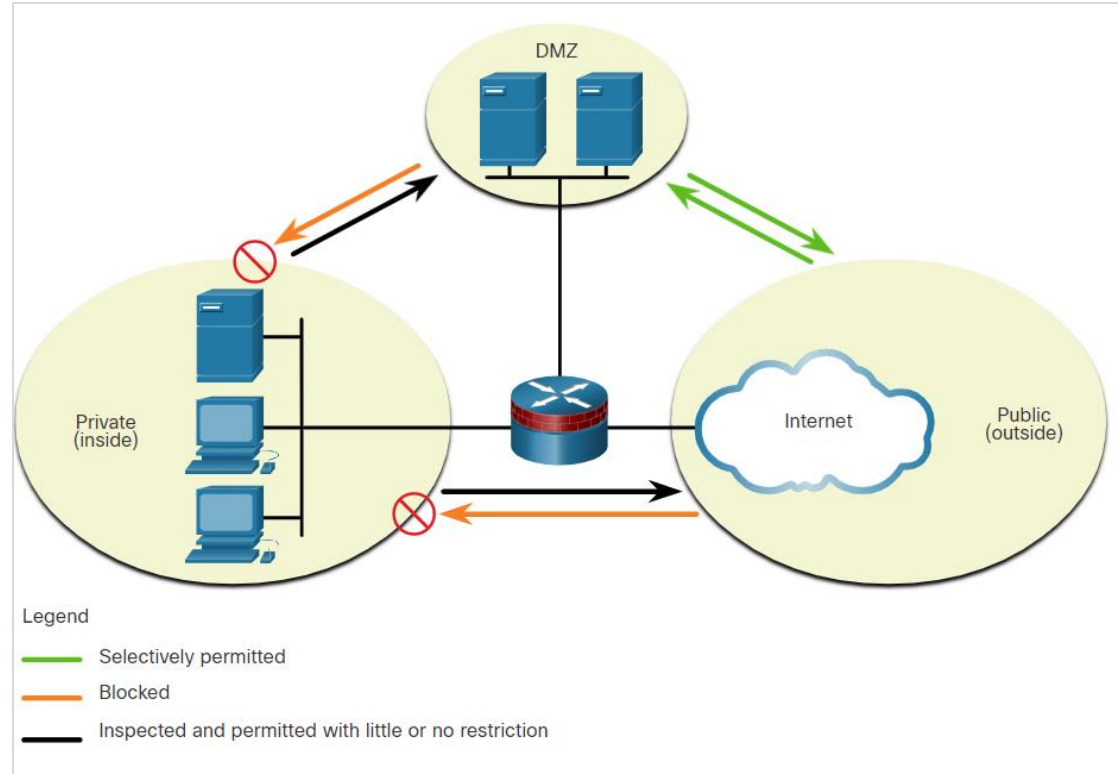
- A rede pública (ou rede externa) não é confiável e a rede privada (ou rede interna) é confiável.



Infraestrutura de segurança de redeArquiteturas de segurança comuns

(Cont.)

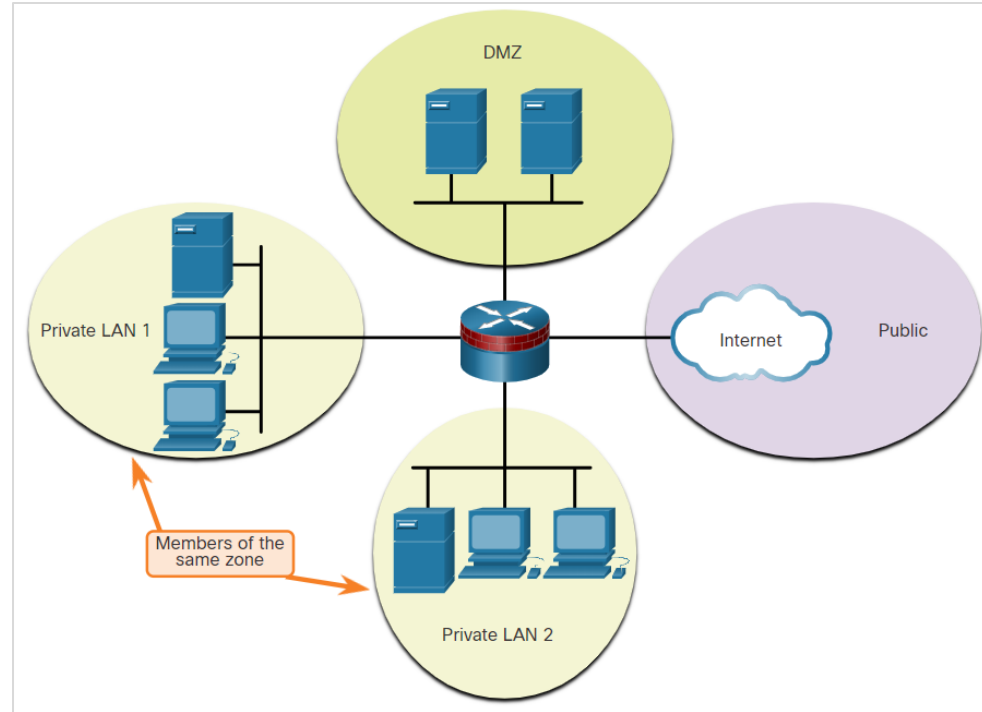
- **Zona Desmilitarizada (DMZ)**
 - Um design de firewall onde normalmente há um:
 - Interface interna conectada à rede privada
 - Interface externa conectada à rede pública
 - Interface DMZ



Infraestrutura de segurança de redeArquiteturas de segurança comuns

(Cont.)

- **Firewalls de política baseados em zona (ZPFs)**
 - ZPFs usam o conceito de zonas 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.



Rastreador de pacotes de infraestrutura de segurança de rede - Identificar fluxo

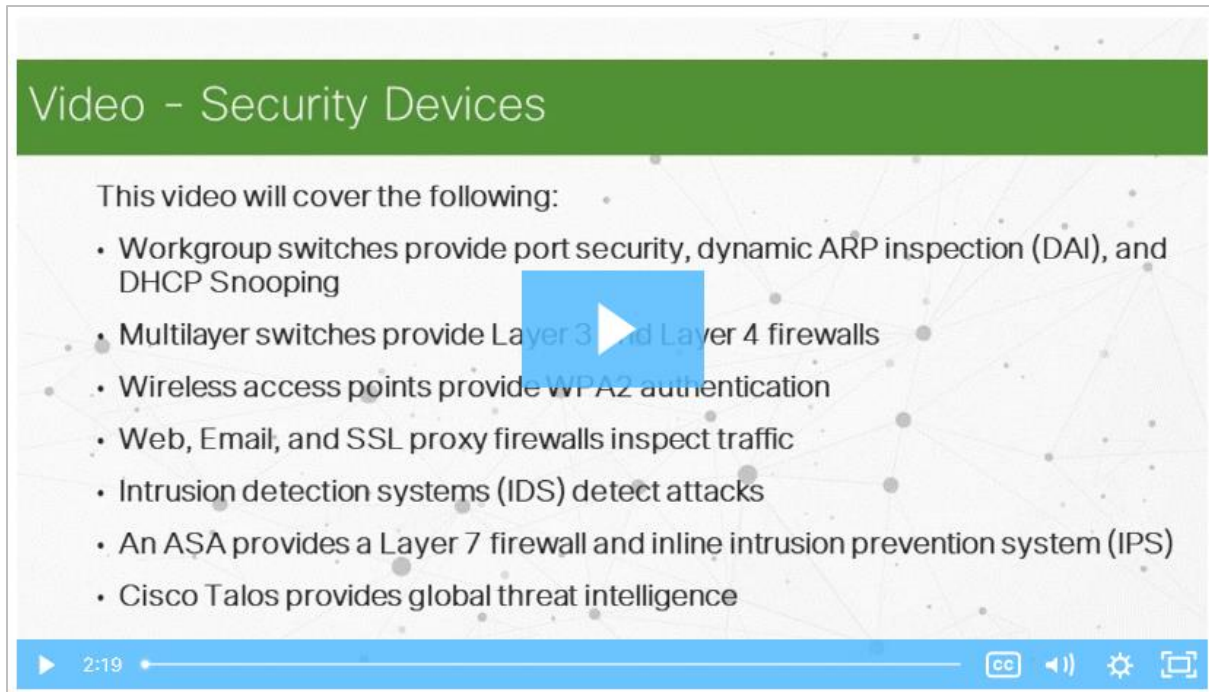
Nesta atividade do Packet Tracer, você observará o seguinte:

- Fluxo de pacotes em uma topologia LAN e WAN.
- Alteração no caminho do fluxo do pacote quando houver uma alteração na topologia da rede.

12.2 Dispositivos de segurança

Vídeo - Dispositivos de segurança

Reproduza o vídeo para saber mais sobre serviços de segurança .



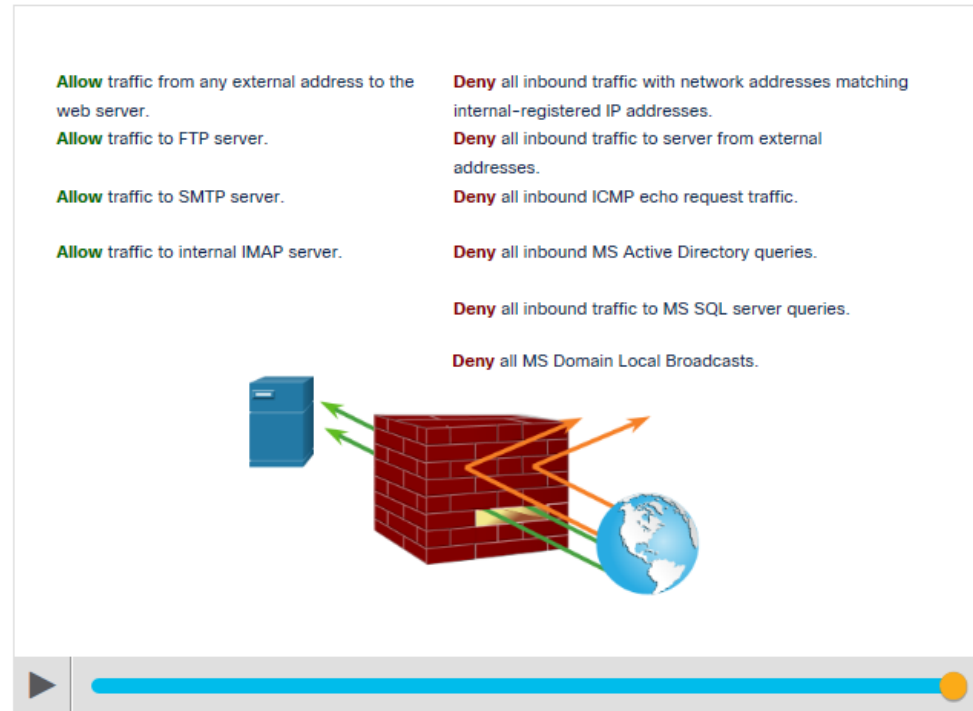
Firewalls de dispositivos de segurança

Um firewall é um sistema ou grupo de sistemas que aplica uma política de controle de acesso entre redes.

Propriedades comuns do firewall:

- Resistente a ataques de rede
- O único ponto de trânsito entre redes corporativas internas e redes externas porque todo o tráfego flui através do firewall
- Aplicar a política de controle de acesso

Reproduza a animação na figura para visualizar um firewall em operação.



Firewalls de dispositivos de segurança (Cont.)

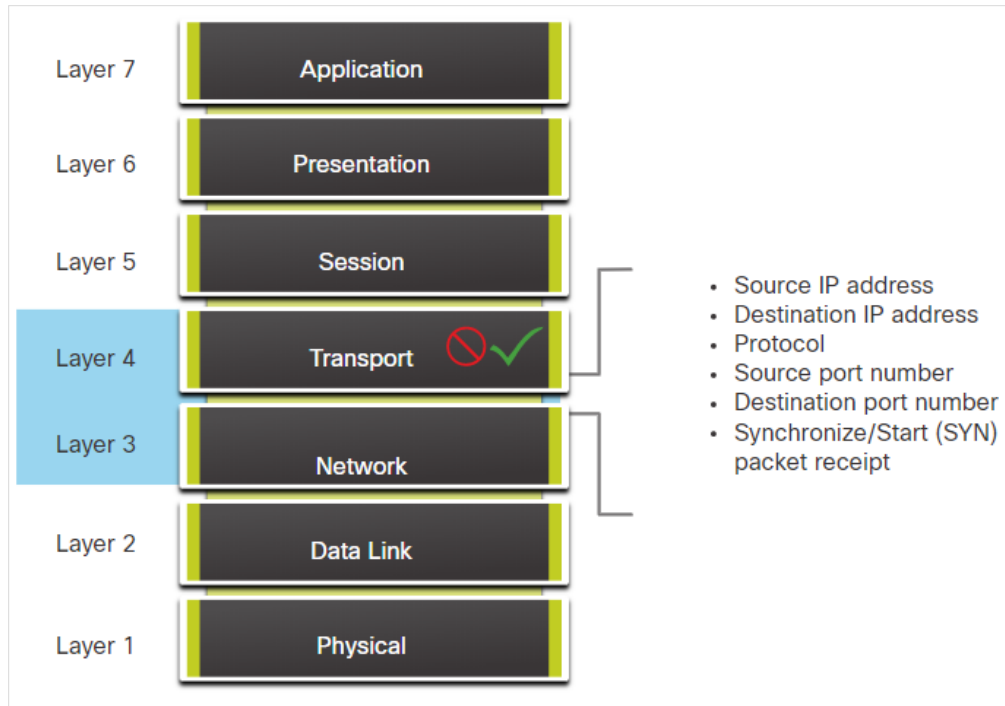
A seguir estão os benefícios e limitações dos firewalls:

Benefícios do firewall	Limitações do Firewall
Evite a exposição de hosts, recursos e aplicativos confidenciais a usuários não confiáveis.	Um firewall mal configurado pode ter sérias consequências para a rede, como se tornar um único ponto de falha.
Sanitize o fluxo do protocolo, o que evita a exploração de falhas do protocolo.	Os dados de muitos aplicativos não podem ser transmitidos por firewalls com segurança.
Bloqueie dados maliciosos de servidores e clientes.	Os usuários podem procurar proativamente maneiras de contornar o firewall para receber material bloqueado, o que expõe a rede a possíveis ataques.
Reduza a complexidade do gerenciamento de segurança.	O desempenho da rede pode diminuir.
	O tráfego não autorizado pode ser bloqueado ou oculto como tráfego legítimo através do firewall.

Descrições de tipos de firewall de dispositivos de

Os diferentes tipos de firewalls são:

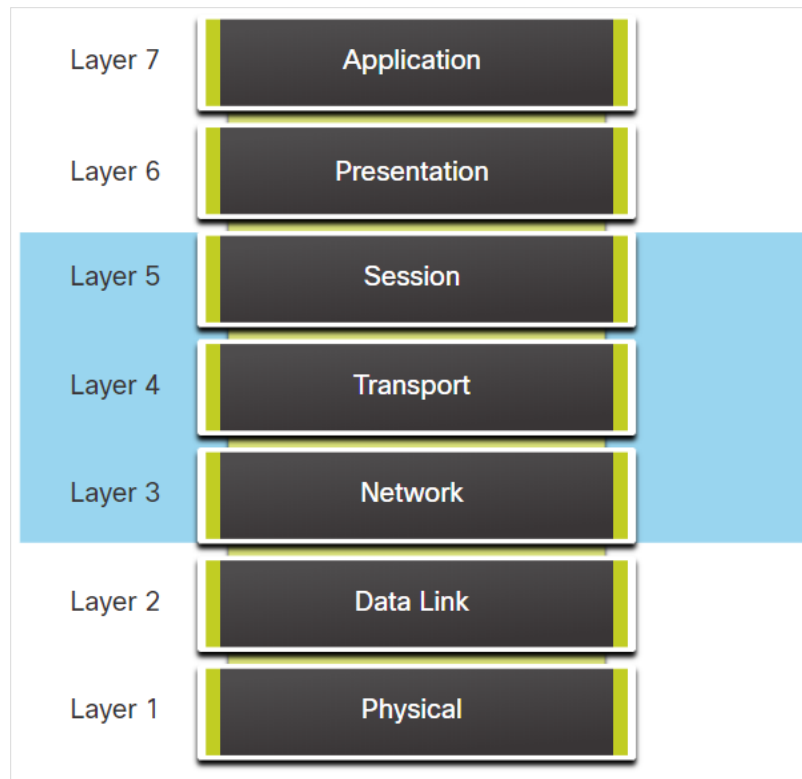
- **Firewall de filtragem de pacotes (sem estado)**
 - Os firewalls de Filtragem de Pacotes fazem parte de um firewall de roteador, que permite ou nega tráfego com base nas informações da Camada 3 e da Camada 4.
 - Eles são firewalls sem estado que usam uma simples pesquisa de tabela de políticas que filtra o tráfego com base em critérios específicos.



Descrições de tipos defirewall de dispositivos de segurança (Cont.)

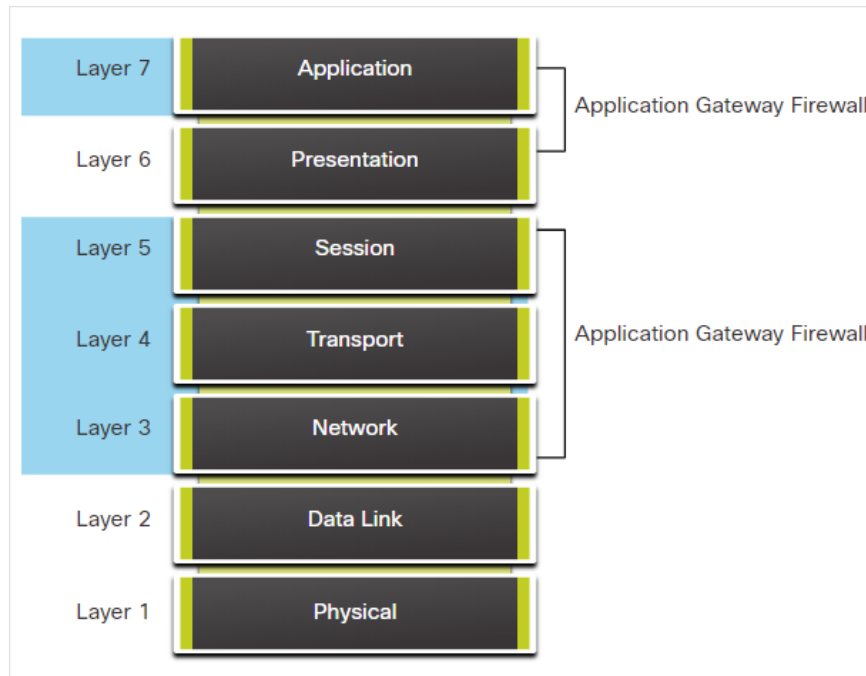
- **Firewalls com estado**

- Firewalls com estado são as tecnologias de firewall mais versáteis e mais comuns em uso.
- Esses firewalls fornecem filtragem de pacotes com monitoração de estado usando informações de conexão mantidas em uma tabela de estados.



Descrições de tipos defirewall de dispositivos de segurança (Condt.)

- **Firewall de gateway de aplicativo (firewall de proxy)**
 - O firewall do gateway de aplicativo filtra informações nas Camadas 3, 4, 5 e 7 do modelo de referência OSI.
 - A maior parte do controle e filtragem do firewall é feita no software.



Descrições de tipos defirewall de dispositivos de segurança (Condt.)

- **Firewalls de última geração (NGFW)**
 - O NGFW vai além dos firewalls de estado, fornecendo:
 - Prevenção de intrusão integrada
 - Reconhecimento e controle de aplicativos para ver e bloquear aplicativos arriscados
 - Caminhos de atualização para incluir futuros feeds de informações
 - Técnicas para lidar com ameaças de segurança em evolução



Descrições de tipos defirewall de dispositivos de segurança (Condt.)

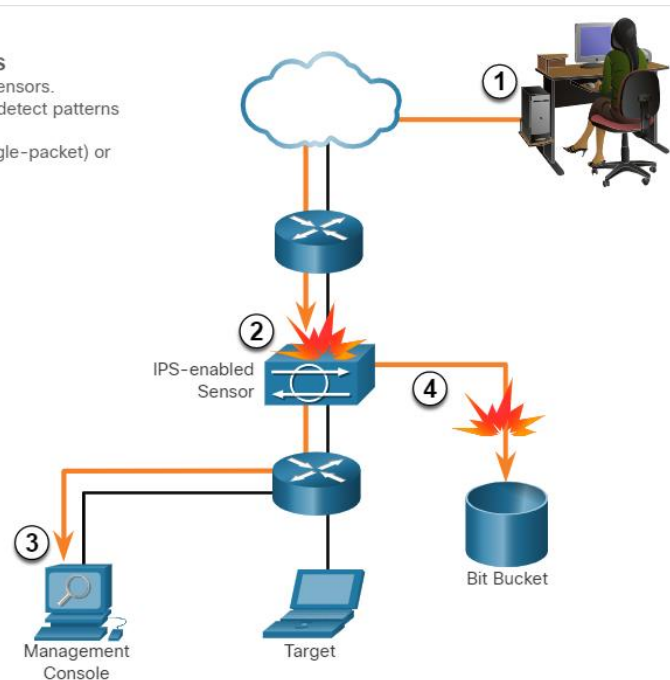
- Outros métodos de implementação de firewalls incluem:
 - **Firewall baseado em host (servidor e pessoal)** - Um PC ou servidor com software de firewall em execução nele.
 - **Firewall transparente** - Filtra o tráfego IP entre um par de interfaces em ponte.
 - **Firewall híbrido** - Uma combinação de vários tipos de firewall.

Dispositivos de segurança Dispositivos de prevenção e detecção de intrusões

- Uma mudança de paradigma de arquitetura de rede é necessária para se defender contra ataques rápidos e em evolução. Isto deve incluir sistemas de prevenção e de boa relação custo-eficácia, tais como:
 - Sistema de detecção de invasão (IDS)
 - Intrusion Prevention Systems (IPS)
- A arquitetura de rede integra essas soluções nos pontos de entrada e saída da rede.
- A figura mostra como um dispositivo IPS lida com tráfego malicioso.

Common Characteristics of IDS and IPS

- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).



1. Malicious traffic is sent to the target host that is inside the network.
2. The traffic is routed into the network and received by an IPS-enabled sensor where it is blocked.
3. The IPS-enabled sensor sends logging information regarding the traffic to the network security management console.
4. The IPS-enabled sensor kills the traffic. (It is sent to the "Bit Bucket.")

Vantagens e desvantagens de IDS e IPS

A tabela lista as vantagens e desvantagens do IDS e IPS:

Solução	Vantagens	Desvantagens
IDS	<ul style="list-style-type: none">Sem impacto na rede (latência, variação)Sem impacto na rede se houver uma falha no sensorSem impacto na rede se houver sobrecarga do sensor	<ul style="list-style-type: none">Ação de resposta não pode parar pacotes de gatilhoAjuste correto necessário para ações de respostaMais vulnerável a técnicas de evasão de segurança de rede
IPS	<ul style="list-style-type: none">Interrompe pacotes de gatilhoPode usar técnicas de normalização de fluxo	<ul style="list-style-type: none">Problemas de sensor podem afetar o tráfego de redeA sobrecarga do sensor afeta a redeAlgum impacto na rede (latência, tremulação)

Consideração de implantação:

- As tecnologias IPS e IDS podem se complementar.
- Decidir qual implementação usar se baseia nos objetivos de segurança da organização, conforme indicado em sua política de segurança de rede.

Tipos de dispositivos de segurança de IPS

Existem dois tipos primários de IPS:

- IDS de host
- IPS baseado em rede
- **IPS baseado em host (HIPS)**

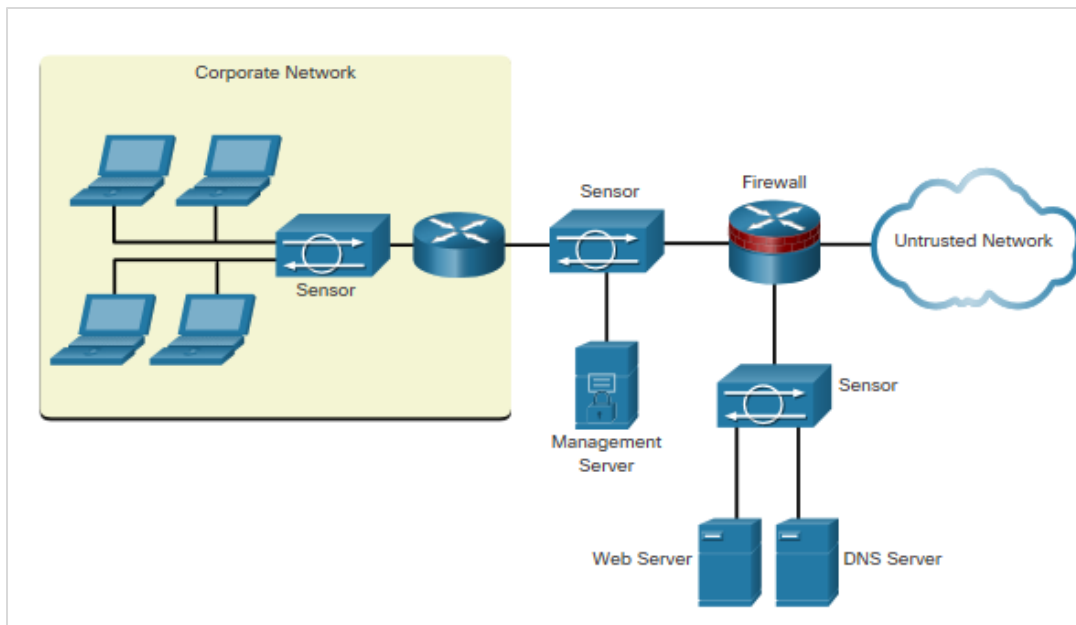
O HIPS é um software instalado em um host para monitorar e analisar atividades suspeitas.

Vantagens	Desvantagens
<ul style="list-style-type: none">• Fornece proteção específica para um sistema operacional host• Fornece proteção em nível de aplicativo e sistema operacional• Protege o host depois que a mensagem é descriptografada	<ul style="list-style-type: none">• Dependente do sistema operacional• Deve ser instalado em todos os hosts

Tipos de dispositivos de segurança de IPS (Cond.)

- **IPS baseado em rede**

- Os IPS baseados em rede são implementados usando um dispositivo IPS dedicado ou não dedicado.
- As soluções IDS/IPS baseadas em host são integradas a uma implementação IPS baseada em rede para garantir uma arquitetura de segurança robusta.
- Os sensores detectam atividades maliciosas e não autorizadas em tempo real e podem agir quando necessário.



Dispositivos de segurança especializados Appliances

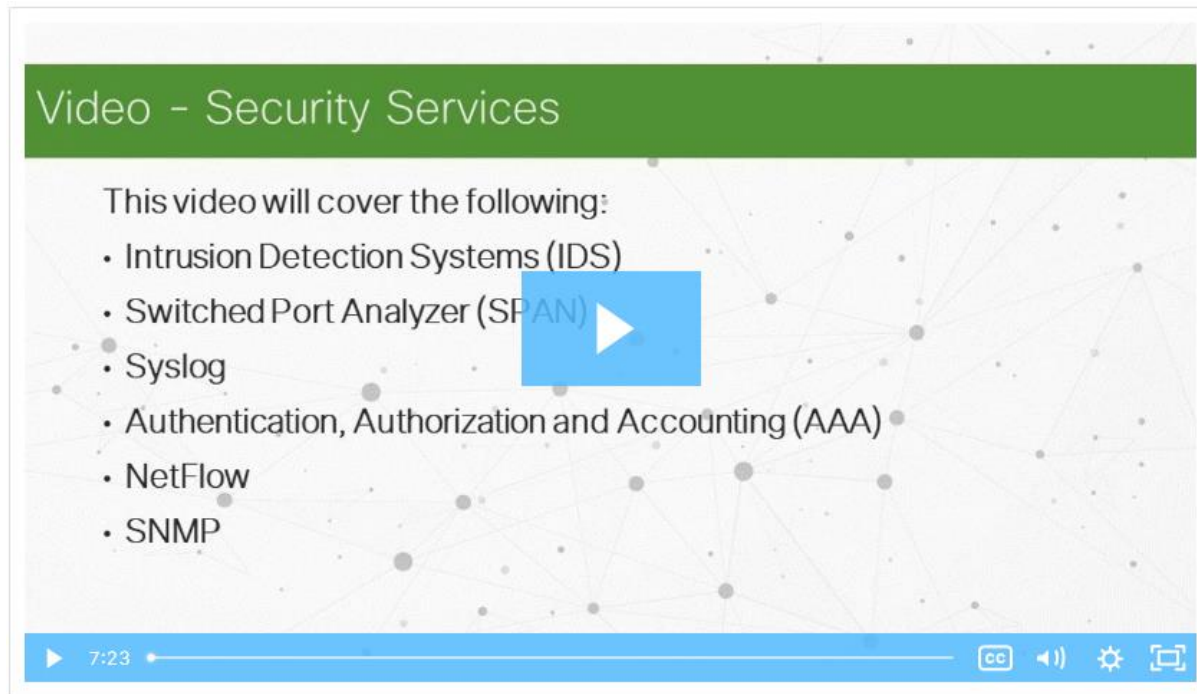
Alguns exemplos de dispositivos de segurança especializados.

Cisco Advanced Malware Protection (AMP)	Cisco Web Security Appliance (WSA)	Cisco Email Security Appliance (ESA)
Uma solução de proteção e análise de malware avançada de classe empresarial	Um gateway da Web seguro que combina proteções líderes para ajudar as organizações a enfrentar os desafios crescentes de proteção e controle do tráfego da Web	O ESA/CiscoCloud Email Security elps para mitigarameaças baseadas em e-mail e o ESA defende sistemas de e-mail de missão crítica
Ele fornece proteção abrangente contra malware para organizações antes, durante e depois de um ataque	Protege a rede bloqueando automaticamente sites arriscados e testando sites desconhecidos antes de permitir que os usuários acessem	Constantemente atualizado por feeds em tempo real do Cisco Talos, que detecta e correlaciona ameaças usando um sistema mundial de monitoramento de banco de dados
		Características: inteligência global contra ameaças, bloqueio de spam, proteção avançada contra malware, controle de mensagens de saída

12.3 Serviços de segurança

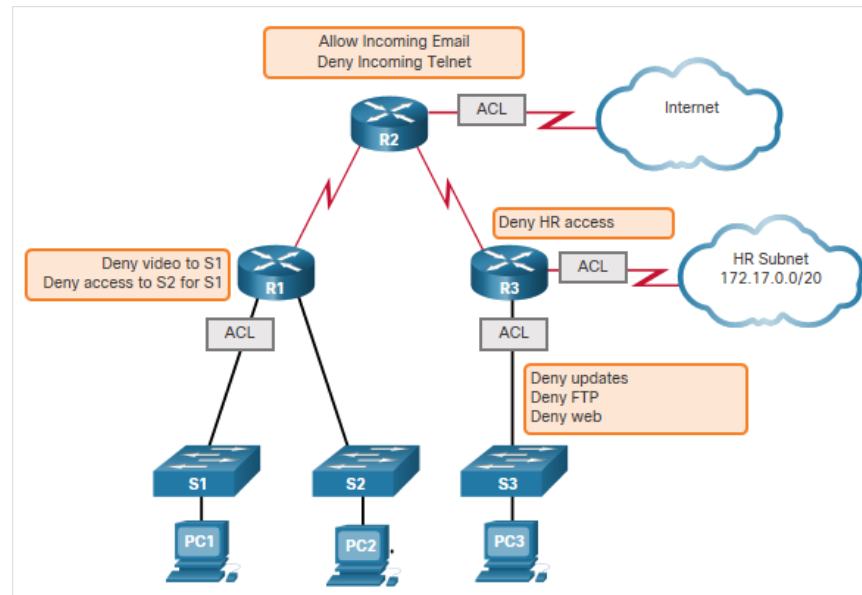
Vídeo de serviços de segurança - Serviços de segurança

Assista ao vídeo para saber mais sobre diferentes serviços de segurança.



Controle de tráfego de serviços de segurança com ACLs

- Uma lista de controle de acesso (ACL) é uma série de comandos que controlam se um dispositivo encaminha ou descarta pacotes com base nas informações encontradas no cabeçalho do pacote.
- Quando configuradas, as ACLs executam as seguintes tarefas:
 - Limitam o tráfego e aumentam o desempenho da rede.
 - Fornecer controle de fluxo de tráfego.
 - Fornece nível básico de segurança para acesso à rede.
 - Filtram tráfego com base no tipo de tráfego.
 - Selecionam hosts para permitir ou negar acesso aos serviços de rede.



Topologia de amostra com ACLs aplicadas aos roteadores R1, R2 e R3.

ACLs dos Serviços de Segurança: Recursos Importantes

Os dois tipos de Cisco IPv4 ACLs são:

- **ACL padrão** - Usado para permitir ou negar tráfego apenas de endereços IPv4 de origem.
- **ACL estendida** - Filtra pacotes IPv4 com base em vários atributos que incluem:
 - Tipo de protocolo
 - Endereço IPv4 origem
 - Endereço IPv4 destino
 - Portas TCP ou UDP origem
 - Portas TCP ou UDP destino
 - Informações opcionais do tipo de protocolo para o melhor controle
- As ACLs padrão e estendidas podem ser criadas usando-se um número ou um nome para identificar a ACL e sua lista de instruções.

Packet Tracer - Demonstração ACL

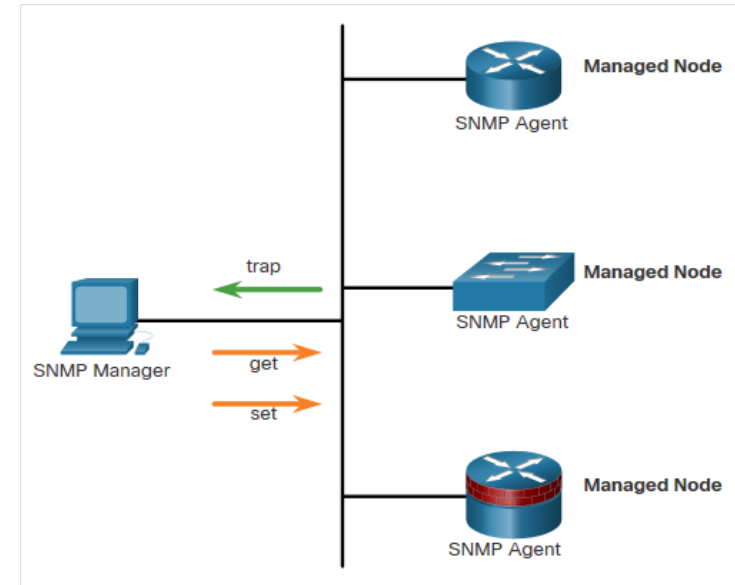
Nesta atividade, você observará o seguinte:

- Como uma ACL pode ser usada para evitar que um ping alcance hosts em redes remotas.
- Após remover a ACL da configuração, os pings terão êxito.

Serviços de segurança

SNMP

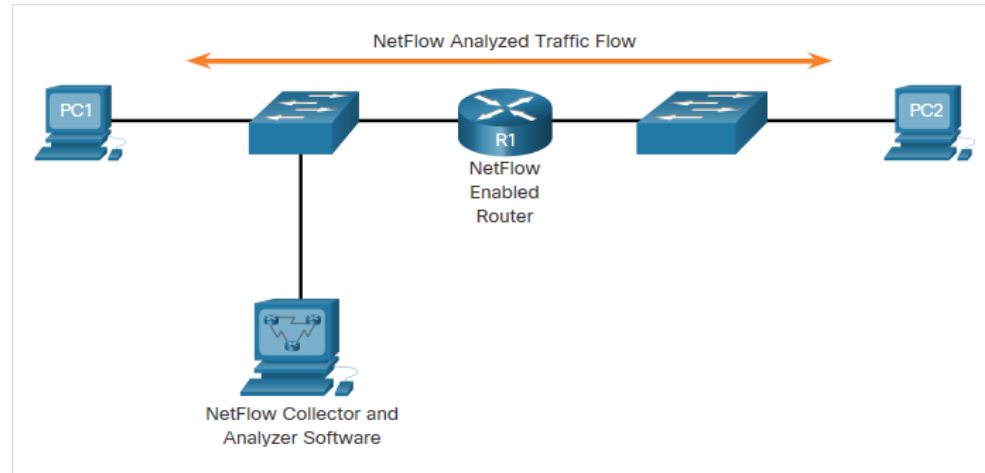
- SNMP (Simple Network Management Protocol) é um protocolo de camada de aplicativo que fornece um formato de mensagem para comunicação entre gerentes e agentes.
- Ele permite que os administradores de rede executem o seguinte:
 - Gerenciar dispositivos finais como servidores, estações de trabalho, roteadores, switches e dispositivos de segurança em uma rede IP.
 - Monitore e gerencie o desempenho da rede.
 - Encontre e resolva problemas de rede.
 - Planeje o crescimento da rede.
- O sistema SNMP consiste em dois elementos:
 - **Gerenciador SNMP:** Executa o software de gerenciamento SNMP.
 - **Agentes SNMP:** nós sendo monitorados e gerenciados.



Serviços de Segurança

NetFlow

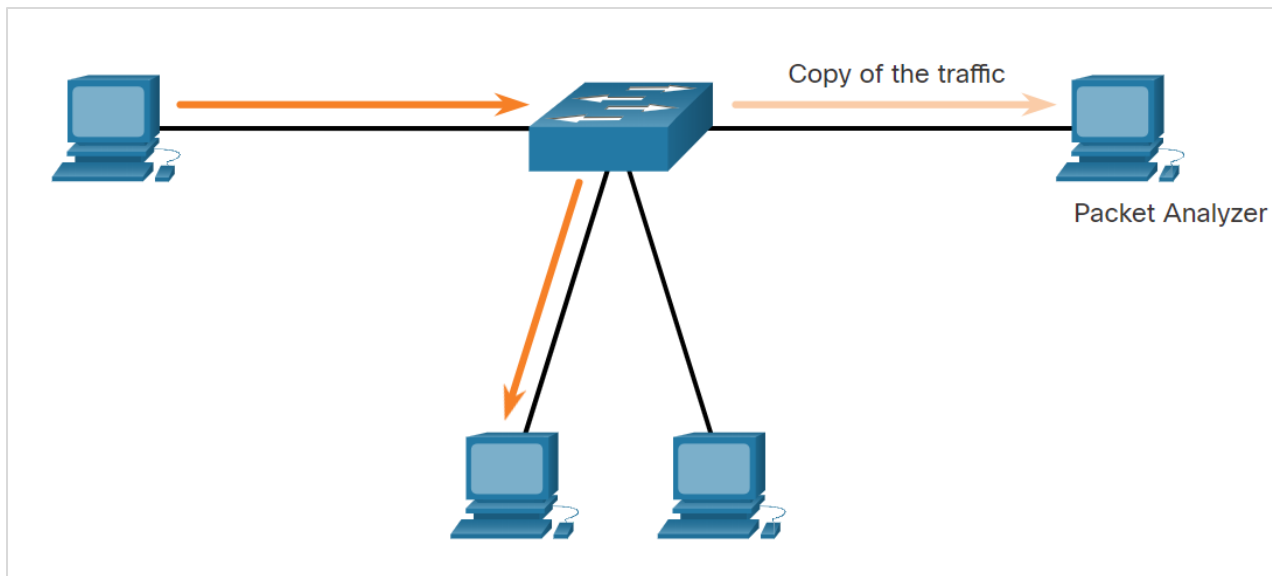
- NetFlow é uma tecnologia CISCO IOS que fornece estatísticas em pacotes que passam por meio de um switch multicamadas ou de um roteador da Cisco.
- O NetFlow fornece dados para habilitar:
 - monitoramento de rede e segurança,
 - planejamento de rede
 - análise de tráfego para incluir a identificação de gargalos na rede
 - Contabilidade IP para fins de faturamento.
- O NetFlow pode monitorar a conexão de aplicativos, rastreando contagens de bytes e pacotes para esse fluxo de aplicativo individual.
- Em seguida, envia as estatísticas para um servidor externo chamado coletor NetFlow.



PC 1 se conecta ao PC 2 usando HTTPS

Espelhamento de portas dos serviços de

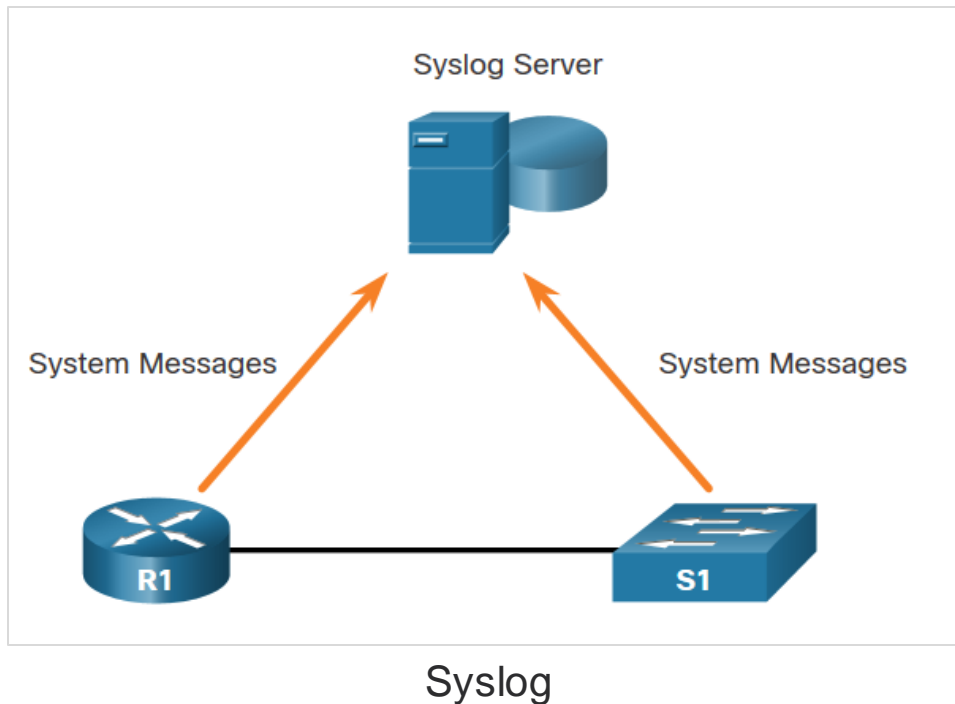
O espelhamento de portas é um recurso que permite que um switch faça cópias duplicadas do tráfego que passa por um switch e, em seguida, enviá-lo para fora de uma porta com um monitor de rede conectado.



Sniffing de tráfego usando um switch

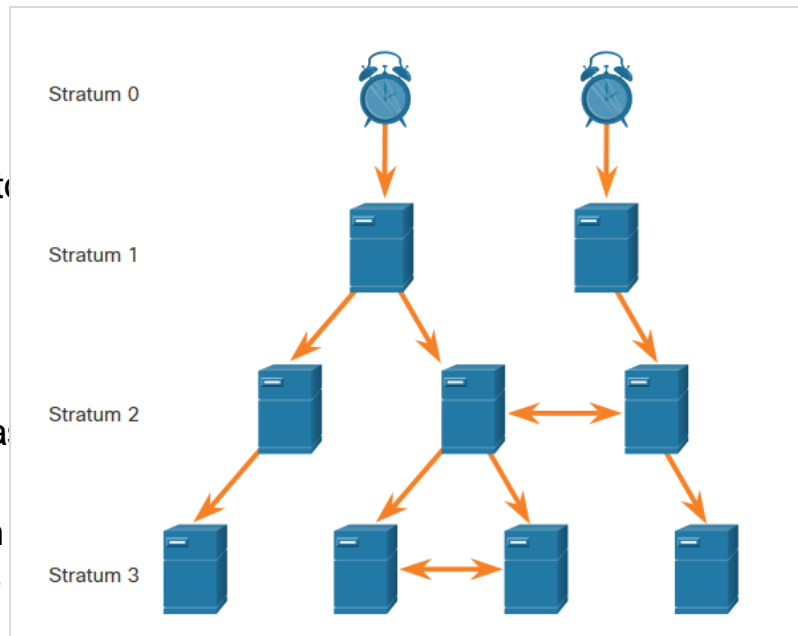
Servidores Syslog dos Serviços de Segurança

- O método mais comum de acessar mensagens do sistema é usar um protocolo chamado syslog.
- O protocolo Syslog permite que os dispositivos de rede enviem suas mensagens de sistema através da rede para servidores syslog.
- Ele fornece três funções principais:
 - A capacidade de coletar informações de registro para monitorar e solucionar problemas
 - A capacidade de selecionar o tipo de informações de registro que são capturadas
 - A capacidade de especificar o destino das mensagens syslog capturadas



NTP de serviços de segurança

- É importante sincronizar a hora em todos os dispositivos na rede. As configurações de data e hora em um dispositivo de rede podem ser definidas usando um dos dois métodos:
 - Configuração manual de data e hora
 - Configurando o Network Time Protocol (NTP)
- As redes NTP usam um sistema hierárquico de fontes de tempo, onde cada nível neste sistema é chamado de estrato. Os servidores NTP são organizados em três níveis conhecidos como estratos:
 - **Estrato 0:** Uma rede NTP obtém o tempo de fontes de tempo confiáveis.
 - **Estrato 1:** Os dispositivos são conectados diretamente às fontes de tempo autorizadas.
 - **Estrato 2 e estratos inferiores:** Os dispositivos Stratum 2, como clientes NTP, sincronizam seu tempo usando os pacotes NTP dos servidores stratum 1.



Níveis de estrato NTP

Servidores AAA de serviços de segurança

A tabela abaixo lista as três funções de segurança independentes fornecidas pela estrutura arquitetônica AAA.

Funções	Descrição
Autenticação	<ul style="list-style-type: none">• Os usuários e administradores devem provar quem são.• A autenticação pode ser estabelecido usando combinações de nome de usuário e senha, perguntas de desafio e resposta, cartões de token e outros métodos.• A autenticação AAA fornece uma maneira centralizada de controlar o acesso à rede.
Autorização	<ul style="list-style-type: none">• Após a autenticação do usuário, os serviços de autorização determinam quais recursos o usuário pode acessar e quais operações ele tem permissão para executar.• Um exemplo é "O usuário 'aluno' pode acessar o host serverXYZ usando apenas SSH."
Accounting	<ul style="list-style-type: none">• O accounting registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo em que o recurso é acessado e todas as alterações efetuadas.• O accounting rastreia como os recursos de rede são usados.• An example is "User 'student' accessed host serverXYZ using SSH for 15 minutes."

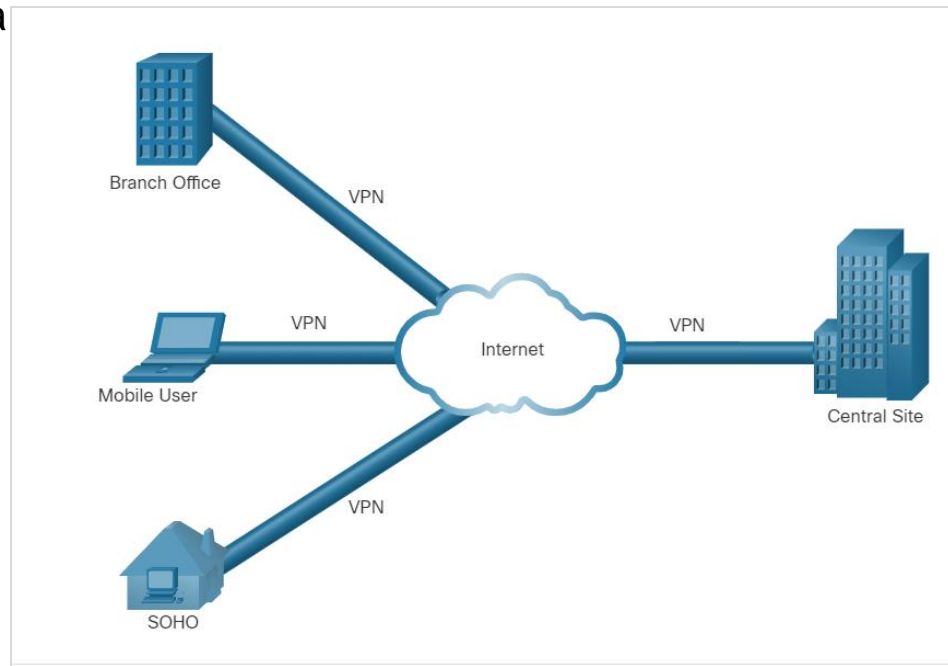
Servidores AAA dos Serviços de Segurança (Cond.)

A tabela abaixo lista a diferença entre os protocolos TACACS+ (Terminal Access Controller Access Control System Plus) e Remote Authentication Dial-In User Service (RADIUS) protocolos.

	TACACS+	RADIUS
Funcionalidade	Separa AAA de acordo com a arquitetura AAA,	Combina autenticação e autorização, mas separa a contabilidade,
Padrão	Principalmente com suporte Cisco	Padrão aberto/RFC
Transporte	TCP	UDP
Protocolo CHAP	Desafio bidirecional e resposta conforme usado no Challenge Handshake Authentication Protocol (CHAP)	Desafio unidirecional e resposta do servidor de segurança RADIUS para o cliente RADIUS
Confidencialidade	Pacote inteiro criptografado	Senha criptografada
Personalização	Fornece autorização de comandos de roteador por usuário ou por grupo	Nenhuma opção para autorizar comandos de roteador por usuário ou por grupo
Accounting	Limitado	Abrangente

VPN de serviços de segurança

- Uma VPN é uma rede privada criada em uma rede pública (geralmente a Internet).
- Uma VPN usa conexões virtuais roteadas pela Internet da organização para o site remoto.
- A VPN é um ambiente de comunicações no qual o acesso é controlado rigorosamente para permitir conexões de mesmo nível em uma comunidade com interesses definidos.
- A confidencialidade é alcançada criptografando o tráfego dentro da VPN.
- Em suma, a VPN conecta dois pontos finais através de uma rede pública, para formar uma conexão lógica que pode ser feita na Camada 2 ou Camada 3.



Rede Virtual Privada

12.4 Resumo da infraestrutura de segurança de rede

O que aprendi neste módulo?

- As redes são normalmente representadas como topologias físicas e lógicas.
- Uma topologia física representa conexões físicas e como os dispositivos finais são conectados, enquanto uma topologia lógica se refere aos padrões e protocolos que os dispositivos usam para se comunicar.
- Os dois tipos mais comuns de infraestruturas de rede são LANs e WANs.
- O design de LAN com fio do campus consiste em camadas hierárquicas (acesso, distribuição, núcleo) com funções específicas atribuídas a cada camada.
- Arquiteturas de segurança comuns definem os limites do tráfego de entrada e saída da rede.
- Os diferentes tipos de firewalls são firewalls de filtragem de pacotes, firewall de inspeção stateful, firewalls de gateway de aplicativo, firewalls de próxima geração.

O que aprendi neste módulo? (Continuação)

- Os sistemas de prevenção de intrusões (IPS) e os sistemas de detecção de intrusões (IDS) são usados para detectar potenciais riscos de segurança e alertar/parar tráfego inseguro.
- Dispositivos de segurança especializados estão disponíveis, incluindo o Cisco Advanced Malware Protection (AMP), Cisco Web Security Appliance (WSA) e Cisco Email Security Appliance (ESA).
- ACLs são uma série de instruções que controlam se um dispositivo encaminha ou descarta pacotes com base nas informações encontradas no cabeçalho do pacote.
- O SNMP permite que os administradores de rede monitorem e gerenciem o desempenho da rede, localizem e resolvam problemas de rede e planejem o crescimento da rede.
- O NetFlow fornece estatísticas sobre os pacotes que estão fluindo através de um roteador Cisco ou switch multicamadas.
- O espelhamento de porta é um recurso que permite que um switch faça cópias duplicadas do tráfego que está passando pelo switch e, em seguida, enviá-lo por uma porta que tenha um monitor de rede conectado.

O que aprendi neste módulo? (Continuação)

- Os servidores Syslog compilam e fornecem acesso às mensagens do sistema geradas pelos dispositivos de rede.
- O NTP sincroniza a hora do sistema em todos os dispositivos na rede para garantir um carimbo de data/hora preciso e consistente das mensagens do sistema.
- O AAA é uma estrutura para configurar serviços de autenticação, autorização e contabilidade do usuário. Normalmente, ele usa um servidor TACACS+ ou RADIUS para esse fim.
- VPNs são redes privadas criadas entre dois pontos de extremidade em uma rede pública.

