NEaD
Núcleo de Educação a Distância

CYBER SECURITY

Faculdade IMPACTA

6

Segurança da infraestrutura de rede

Alex Sandro da Silva Feitosa

Resumo

O projeto de uma rede influencia o tráfego de dados e a eficiência geral do sistema. Elementos como topologia, segmentação e escolha de equipamentos fazem diferença no desempenho. Dispositivos como firewalls, switches e IDS ajudam a proteger a rede, enquanto serviços como autenticação, criptografia e VLANs aumentam o controle e a segurança dos acessos.

Introdução

Nesta aula, abordaremos como o projeto de redes impacta diretamente o fluxo de tráfego, o desempenho e a segurança. Serão apresentados dispositivos especializados usados para proteger os dados e controlar o acesso à rede. Também exploraremos brevemente como os serviços de rede contribuem para reforçar a segurança em ambientes conectados.

1.1. Segurança da infraestrutura de rede

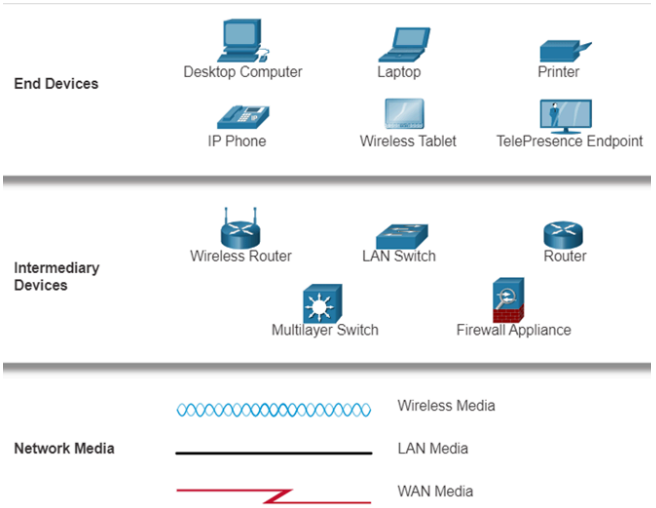
1.1.1 Topologias

Os diagramas de rede, geralmente chamados de diagramas de topologia, usam símbolos para representar diferentes dispositivos e conexões dentro da rede. Esses diagramas são ferramentas visuais importantes no planejamento, implementação e manutenção de redes, pois ajudam a ilustrar como os elementos estão interconectados e como o tráfego de dados circula entre eles. Dispositivos como *switches*, *roteadores*, pontos de acesso, servidores e estações de trabalho são representados por ícones padronizados, facilitando a compreensão da estrutura da rede tanto para profissionais quanto para equipes de suporte. Além disso, os diagramas de topologia podem ser físicos, mostrando a disposição real dos cabos e dispositivos, ou lógicos, focando na forma como os dados fluem e como os dispositivos se comunicam entre si.

As terminologias importantes a serem conhecidas incluem:

- Placa de rede
- Porta Física
- Interface

Figura 1.1. Simbologias



Fonte: CCNA Cyber OPS Associate v1, 2020.

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

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.

1.1.2 Classificação das Redes

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.

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)

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.

Tabela 1.1. LAN versus WAN

LAN (Local Area Network)	**WAN (Wide Area Network)**
Interconecte dispositivos finais em uma área limitada.	Interconecte LANs em áreas geográficas amplas.
Administrado por uma única organização ou indivíduo.	Normalmente administrado por vários provedores de serviços.
Fornece largura de banda de alta velocidade para dispositivos finais internos e dispositivos intermediários.	Geralmente, fornece links de velocidade mais lenta entre LANs.

Fonte: do autor, 2022.

1.1.3 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.

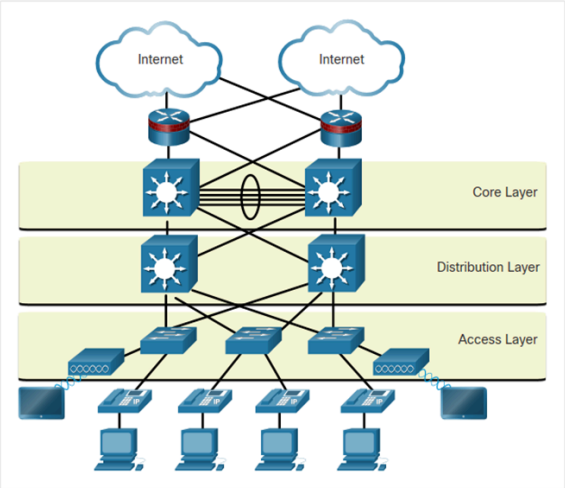
O design hierárquico da LAN inclui três camadas:

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.

Figura 1.2 Modelo Projeto Hierárquico

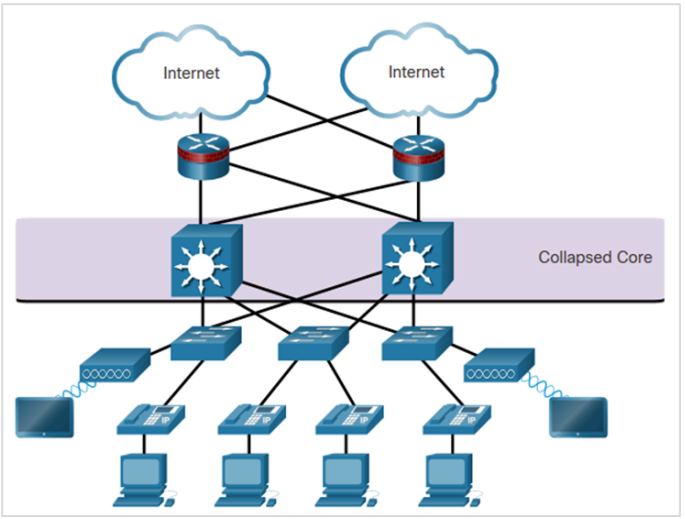


Fonte: CCNA Cyber OPS Associate v1, 2020.

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.

Figura 1.3 Switch Função Dupla



Fonte: CCNA Cyber OPS Associate v1, 2020.

1.1.4 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.

Zona Desmilitarizada (DMZ)

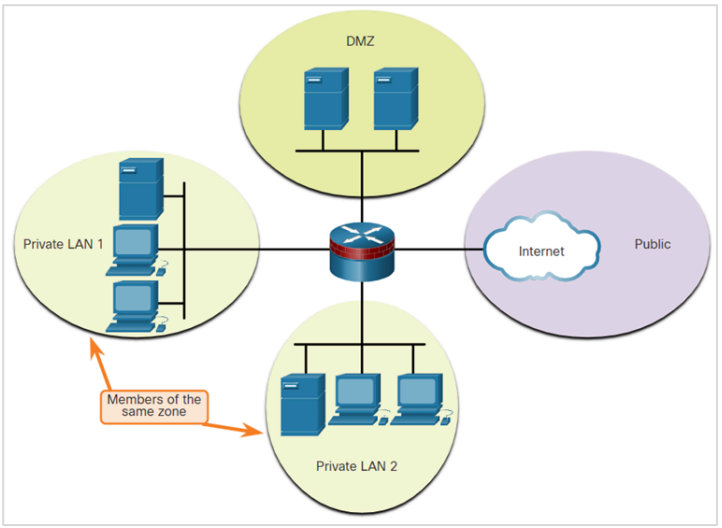
Um design de firewall onde normalmente há um:

- Interface interna conectada à rede privada
- Interface externa conectada à rede pública
- Interface DMZ

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.

Figura 1.4 Rede Pública, Privada e DMZ

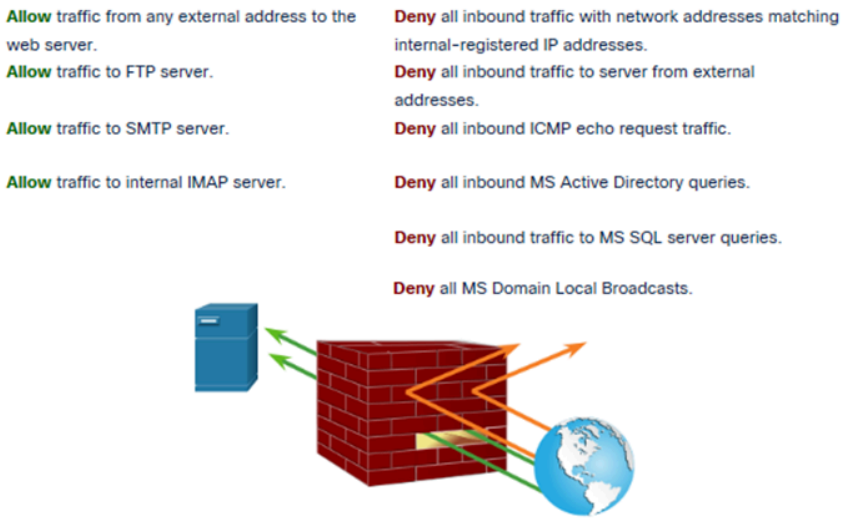


Fonte: CCNA Cyber OPS Associate v1, 2020.

2.1. Dispositivos de segurança

2.1.1 Firewall

Figura 1.5 Firewall



Fonte: CCNA Cyber OPS Associate v1, 2020.

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

Tabela 1.2. 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.

Fonte: do autor, 2022.

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.

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.

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.

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

Firewall baseado em host (servidor e pessoal)

Um PC ou servidor com software de firewall em execução nele.

Firewall transparente

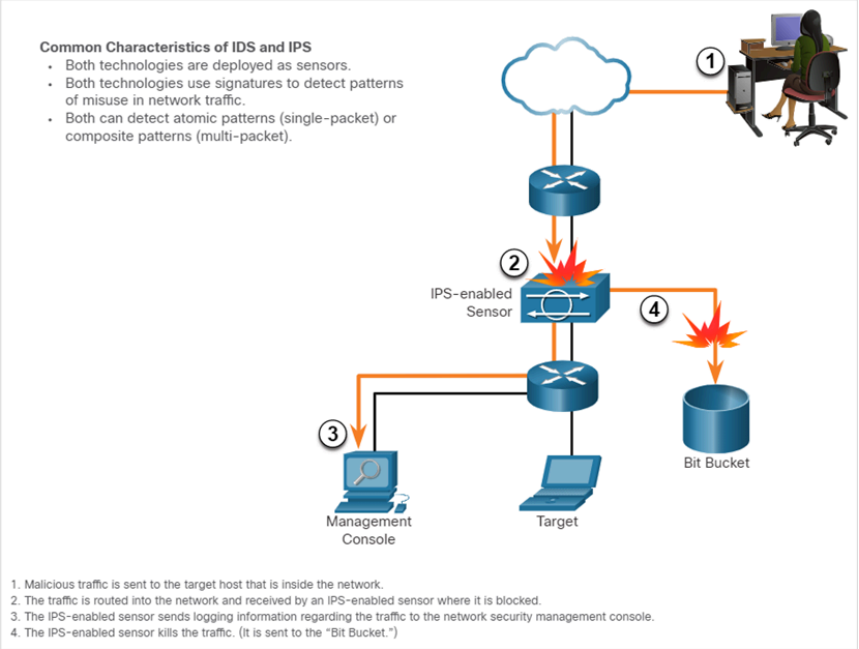
Filtra o tráfego IP entre um par de interfaces em ponte.

Firewall híbrido

Uma combinação de vários tipos de firewall.

2.2.1 IPS/IDS

Figura 1.6 IPS/IDS



Fonte: CCNA Cyber OPS Associate v1, 2020.

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.

Tabela 1.3. A tabela lista as vantagens e desvantagens do IDS e IPS

Solução	Vantagens	Desvantagens
IDS	•Sem impacto na rede (latência, variação) •Sem impacto na rede se houver uma falha no sensor •Sem impacto na rede se houver sobrecarga do sensor	•Ação de resposta não pode parar pacotes de gatilho •Ajuste correto necessário para ações de resposta •Mais vulnerável a técnicas de evasão de segurança de rede
IPS	•Interrompe pacotes de gatilho •Pode usar técnicas de normalização de fluxo	•Problemas de sensor podem afetar o tráfego de rede •A sobrecarga do sensor afeta a rede •Algum impacto na rede (latência, tremulação)

Fonte: do autor, 2022.

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.

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

- 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

Desvantagens

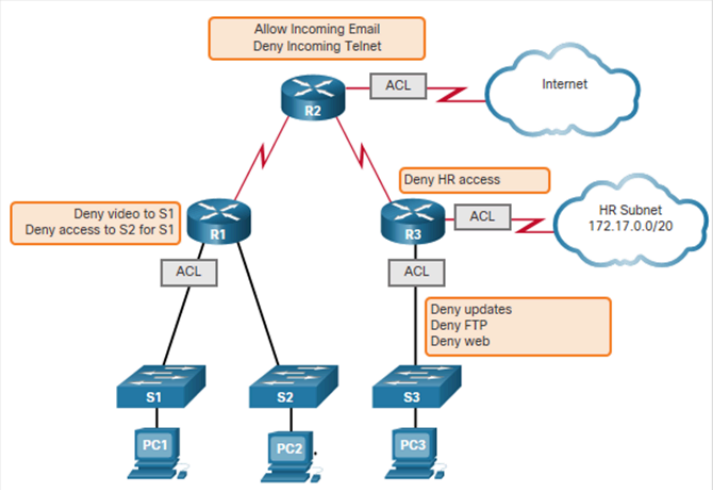
- Dependente do sistema operacional
- Deve ser instalado em todos os hosts
- IPS Baseado em rede
- Os IPS baseados em rede são implementados usando um dispositivo IPS dedicado ou não dedicado.
- As soluções IDS/IPS baseadas em host são integradas a uma implementação IPS baseada em rede para garantir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

3.1. Serviços de segurança

3.1.1 ACLs - Access Control List

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.

Figura 1.7 ACLs



Fonte: CCNA Cyber OPS Associate v1, 2020.

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.

Os dois tipos de Cisco IPv4 ACLs são:

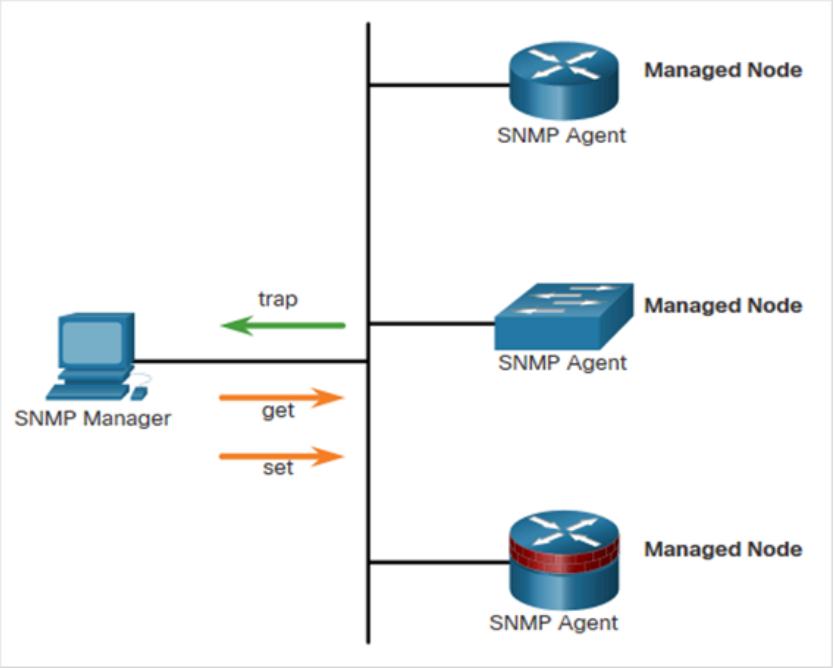
- ACL padrão - Usado para permitir ou negar tráfego apenas de endereços IPv4 de origem.
- ACL estendida - Filtra pacotes IPv4 com base em vários atributos que incluem:
    - Tipo de protocolo
    - Endereço IPv4 origem
    - Endereço IPv4 destino
    - Portas TCP ou UDP origem
    - Portas TCP ou UDP 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.

3.2.1 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.

Figura 1.7 SNMP



Fonte: CCNA Cyber OPS Associate v1, 2020.

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.

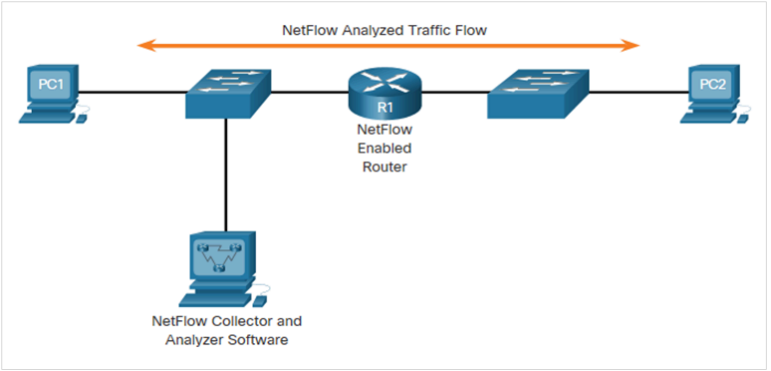
O sistema SNMP consiste em dois elementos:

- Gerenciador SNMP: Executa o software de gerenciamento SNMP.
- Agentes SNMP: nós sendo monitorados e gerenciados.

3.3.1 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.

Figura 1.7 NetFlow



Fonte: CCNA Cyber OPS Associate v1, 2020.

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.

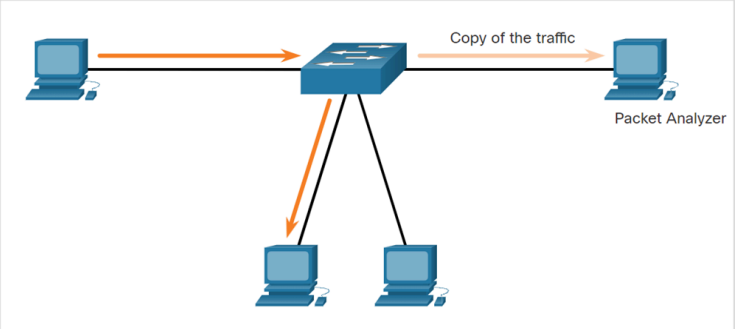
O NetFlow pode monitorar a conexão de aplicativos, rastreando contagens de bytes e pacotes para esse fluxo de aplicativo individual.

Em seguida, envia as estatísticas para um servidor externo chamado coletor NetFlow.

3.4.1 SPAM

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.

Figura 1.8 SPAM



Fonte: CCNA Cyber OPS Associate v1, 2020.

3.5.1 Syslog

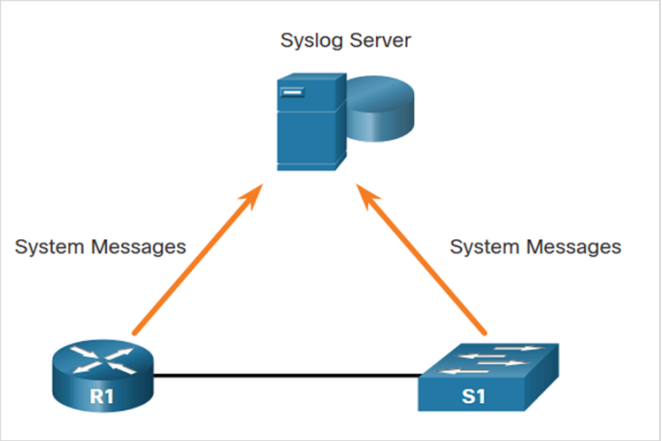
O método mais comum de acessar mensagens do sistema é usar um protocolo chamado syslog.

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

Figura 1.9 Syslog



Fonte: CCNA Cyber OPS Associate v1, 2020.

3.6.1 NTP

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.

3.7.1 AAA

Abaixo estão listadas três funções de segurança independentes fornecidas pela estrutura arquitetônica AAA.

Autenticação

- 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

- 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

- 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.
- Um exemplo é "O usuário ‘estudante’ pode acessar o host serverXYZ usando apenas SSH por 15 minutos."

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.

Tabela 1.4. Diferença entre protocolos TACACS+ e RADIUS

	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

Fonte: do autor, 2020.

3.8.1 VPN

Uma VPN é uma rede privada criada em uma rede pública (geralmente a Internet).

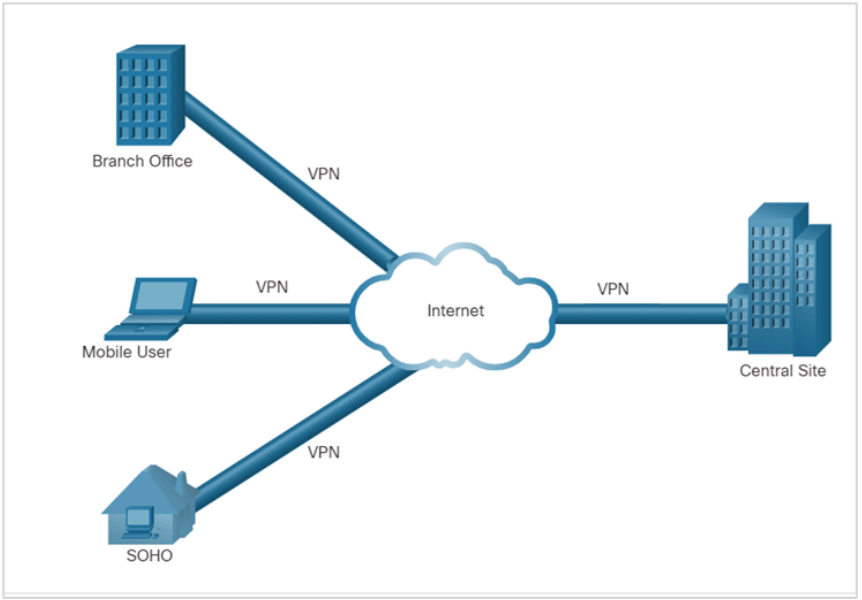
Uma VPN usa conexões virtuais roteadas pela Internet da organização para o site remoto.

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.

Figura 1.10 VPN



Fonte: CCNA Cyber OPS Associate v1, 2020.

Conclusão

Concluímos que um bom projeto de rede, aliado ao uso de dispositivos especializados e serviços adequados, é essencial para garantir não apenas o desempenho, mas também a segurança das informações. Esses elementos trabalham em conjunto para oferecer uma infraestrutura de rede mais eficiente, segura e confiável.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em: <https://www.netacad.com>.

SÊMOLA, Marcos**. Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes**: primeiros passos. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security**: applications and standards. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001 E 27002:** Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes**: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000.