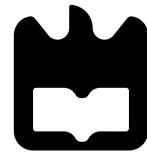


# Segurança em Redes de Comunicações Apontamentos PARTE2

Universidade de Aveiro

Sebastian D. González



# **Segurança em Redes de Comunicações Apontamentos PARTE2**

Dept. de Eletrónica, Telecomunicações e Informática  
Universidade de Aveiro

sebastian.duque@ua.pt(103690)

18 de junho de 2024

## **Warning!!**

Isto são apenas uns apontamentos realizados por uma pobre alma de MIECT, feitas a partir dos slides da disciplina e outras fontes . Por favor, não usem apenas estes apontamentos como material de estudo.

Dito isto, boa sorte a todos e ámen CT .

Agradecimentos ao Prof. Paulo Salvador [salvador@ua.p](mailto:salvador@ua.p) e ao Prof. António Nogueira. [nogueira@ua.pt](mailto:nogueira@ua.pt) por todo o material fornecido nas aulas.

# Conteúdo

<b>1</b>	<b>Secure Communications</b>	<b>1</b>
1.1	Symmetric Key Cryptography . . . . .	1
1.2	Public Key Cryptography . . . . .	1
1.3	Public Key Digital signatures for authentication . . . . .	2
1.3.1	RSA (Rivest, Shamir and Adleman) . . . . .	3
1.4	X.509 certificate contents . . . . .	4
1.5	SCEP . . . . .	5
1.6	Certificate Revocation Lists (CRL) . . . . .	5
1.7	Certificate usage and validity check . . . . .	6
1.8	Traffic Tunnel Concept . . . . .	6
1.9	Virtual Tunnel Interface (VTI) . . . . .	7
1.9.1	Virtual Tunnel Interface (VTI) . . . . .	7
1.9.1.1	Requisitos . . . . .	7
1.9.2	Loopback Interfaces as End-Points . . . . .	7
1.9.3	Tipos de Túneis IP . . . . .	8
1.10	Overlay Network . . . . .	8
1.11	Multipoint Tunnels . . . . .	9
1.12	Next Hop Resolution Protocol (NHRP) . . . . .	9
1.13	Hub-Spoke vs. Spoke-Spoke . . . . .	10
1.14	IPSec (Internet Protocol Security) . . . . .	10
1.14.1	IPSec Modes . . . . .	11
1.14.2	AH and ESP Header . . . . .	12
1.14.3	IPSec - Security Associations . . . . .	12
1.14.4	Establishing SA and Cryptographic Keys . . . . .	13
1.14.5	IPsec NAT Transversal . . . . .	14
<b>2</b>	<b>Virtual Private Networks (VPN)</b>	<b>15</b>
2.1	Variants of Site-to-Site IPsec VPN . . . . .	15
2.2	Dynamic Multipoint VPN . . . . .	16
2.3	SD-WAN . . . . .	17
2.4	Remote Access VPN . . . . .	17
2.5	Remote VPN Network Integration . . . . .	18
2.6	Integration with Flow Control . . . . .	18

<b>3</b>	<b>Intrusion Detection and Prevention</b>	<b>19</b>
3.1	Host-Based vs. Network-Based . . . . .	20
3.2	Signature vs. Anomaly Based . . . . .	20
3.3	Endpoint Detection and Response (EDR) . . . . .	21
3.4	Network Deployment (1) . . . . .	21
3.5	ERSPAN . . . . .	21
3.6	Network Deployment (2) . . . . .	22
3.7	IDS/IPS Actions . . . . .	23
<b>4</b>	<b>Monitoring &amp; SIEM &amp; NOC/SOC</b>	<b>24</b>
4.1	Remote CLI Access . . . . .	24
4.2	Log Files Access . . . . .	25
4.3	Core and End-to-End Monitoring . . . . .	26
4.4	Node Monitoring . . . . .	26
4.5	End-User/Host/App Monitoring . . . . .	27
4.6	Server/Service/Cloud Monitoring . . . . .	27
4.7	Per-Service Detailed Monitoring . . . . .	28
4.8	Data Sources . . . . .	28
4.8.1	SNMP . . . . .	28
4.8.1.1	SNMP versions . . . . .	29
4.8.1.2	SNMP Operations . . . . .	29
4.8.1.3	SNMP Names (numbers/OID) . . . . .	29
4.8.1.4	SNMP MIBs . . . . .	30
4.9	NetFlow . . . . .	30
4.9.1	NetFlow versions 1 and 5 . . . . .	30
4.9.2	NetFlow version 9 . . . . .	31
4.9.3	NetFlow Deployment . . . . .	31
4.10	IPFIX (v10) and Flexible NetFlow . . . . .	32
4.11	Network Passive Probing . . . . .	32
4.12	Log Management Systems (LMS) . . . . .	33
4.13	Security Information and Events Management (SIEM) . . . . .	34
4.14	LMS vs. SIEM . . . . .	34
4.15	SIEM Events (examples) . . . . .	35
4.16	Security Operations Center (SOC) . . . . .	35

# **Lista de Figuras**

1.1	RSA algorithm structure [1] . . . . .	3
1.2	Exemplo de um certificado X.509 [2] . . . . .	4
1.3	AH header placement . . . . .	11
1.4	ESP header placement . . . . .	11
2.1	Dynamic Multipoint VPN [3] . . . . .	16
3.1	Intrusion Detection vs Intrusion Prevention [4] . . . . .	19
4.1	Versões SNMP . . . . .	29
4.2	SNMP numbers . . . . .	30

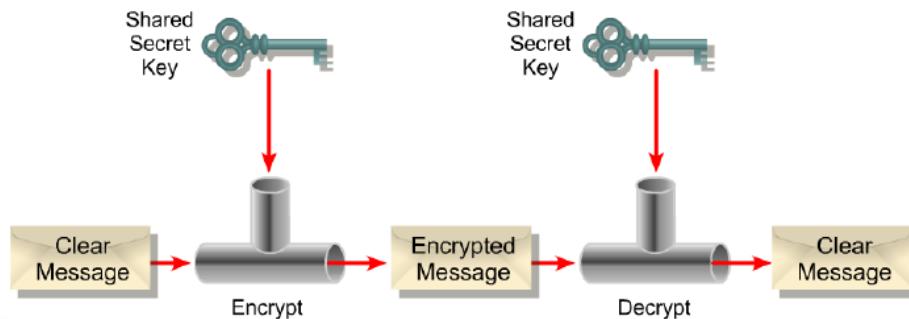
# Secure Communications

## 1.1 Symmetric Key Cryptography

Na criptografia simétrica, existem duas exigências principais para um uso seguro:

1. **Algoritmo de criptografia forte:** O algoritmo deve ser robusto contra ataques, garantindo que a mensagem cifrada não possa ser facilmente decifrada sem a chave correta.
2. **Chave secreta conhecida apenas pelo remetente e receptor:** A segurança depende da chave usada para cifrar e decifrar a mensagem. Essa chave deve ser mantida em segredo entre as partes envolvidas.

Dado que o algoritmo é conhecido, é essencial um canal seguro para distribuir a chave. Isso significa que a chave precisa ser transmitida de forma segura para evitar que terceiros a interceptem e comprometam a comunicação.

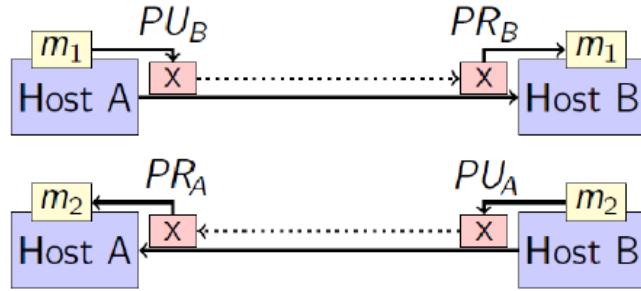


## 1.2 Public Key Cryptography

A criptografia de chave pública é uma forma de criptografia **assimétrica** que utiliza um par de chaves:

- **Chave pública:** Esta chave pode ser conhecida por qualquer pessoa e é usada para criptografar as mensagens ou verificar assinaturas digitais. Por exemplo, qualquer um pode usar a chave pública do destinatário para enviar uma mensagem cifrada para ele.
  - **Chave privada:** Esta chave é conhecida apenas pelo proprietário e é usada para descriptuar mensagens ou criar assinaturas digitais. Por exemplo, o destinatário usa sua chave privada para decifrar a mensagem que foi criptografada com sua chave pública.
- ⇒ Cada chave pública é divulgada livremente, enquanto a chave privada correspondente é mantida em segredo pelo proprietário.

A criptografia é assimétrica porque aqueles que usam a chave pública para criptografar mensagens ou verificar assinaturas não podem, com essa mesma chave, decifrar mensagens ou criar assinaturas. Isso garante que apenas o proprietário da chave privada possa realizar essas operações críticas, mantendo a segurança e a integridade da comunicação e das assinaturas digitais.



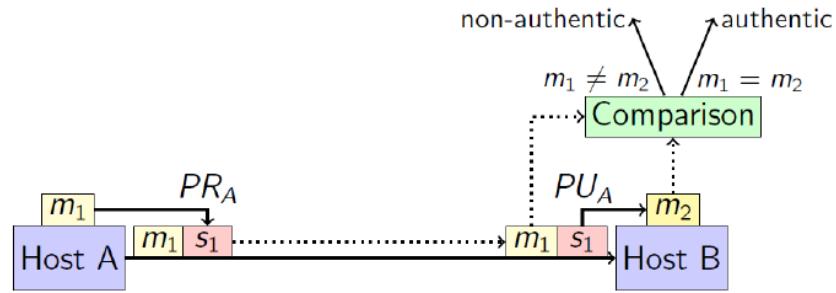
A criptografia de chave pública é inefficiente para criptografar grandes volumes de dados devido à sua complexidade computacional elevada. Devido a essa limitação, ela é tipicamente utilizada de forma complementar para criar canais de comunicação seguros nos quais uma chave simétrica temporária pode ser negociada. Essa chave simétrica é, então, usada para criptografar grandes quantidades de dados de maneira eficiente.

### 1.3 Public Key Digital signatures for authentication

Para enviar uma mensagem autenticada de A para B:

1. O Host A criptografa a mensagem com a sua chave privada (PRA) para criar um sinal de autenticação.
2. O Host A envia a mensagem e o sinal de autenticação para o Host B.

3. O Host B verifica a mensagem pela criptografia do sinal de autenticação com a chave pública do Host A (PUA).
4. O Host B compara o resultado da verificação com a mensagem recebida para confirmar a autenticidade



### 1.3.1 RSA (Rivest, Shamir and Adleman)

RSA é um algoritmo de chave pública, usado para criptografia e descriptografia. Possui comprimento de chave variável de 512, 1024 e 2048 bits. O tamanho do bloco é variável, mas deve ser menor que o comprimento da chave.

O comprimento do texto cifrado será igual ao comprimento da chave. RSA é mais lento que DES, AES e IDEA, tornando-o menos adequado para criptografar grandes mensagens. No entanto, RSA é frequentemente utilizado para criptografar chaves secretas e chaves secretas usadas para criptografar mensagens.

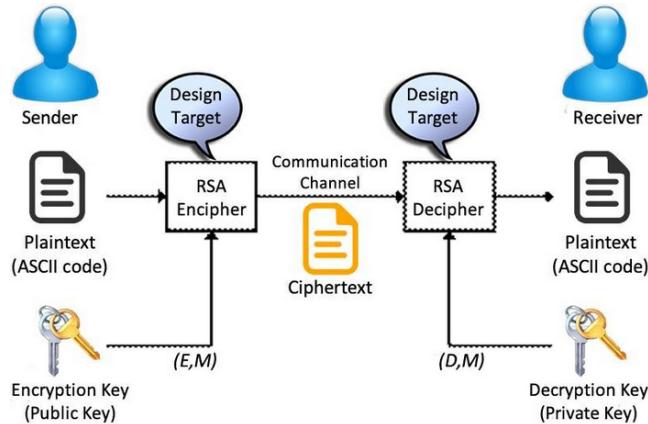


Figura 1.1: RSA algorithm structure [1]

## 1.4 X.509 certificate contents

Os certificados X.509 contêm informações cruciais para estabelecer identidades e segurança em redes e sistemas. Suas principais partes incluem:

- **Versão:** Versão do certificado, geralmente 3.
- **Número de série:** Identificador único do certificado.
- **Algoritmo de assinatura:** Algoritmo usado para assinar o certificado.
- **Emissor:** Entidade que emitiu o certificado.
- **Validade:** Período em que o certificado é válido.
- **Sujeito:** Entidade que possui o certificado.
- **Nome distinto (DN) do sujeito:** Identificação do sujeito, ex.: "CN=Java Duke, OU=Java Software Division, O=U.Aveiro, C=PT".
- **Informações da chave pública:** Detalhes da chave pública do sujeito.
- **Algoritmo da chave pública:** Algoritmo da chave pública, ex.: RSA.
- **Chave pública do sujeito:** Chave pública usada para criptografia.
- **Algoritmo de assinatura do certificado:** Algoritmo para a assinatura digital do certificado.
- **Assinatura do certificado:** Assinatura digital do certificado.

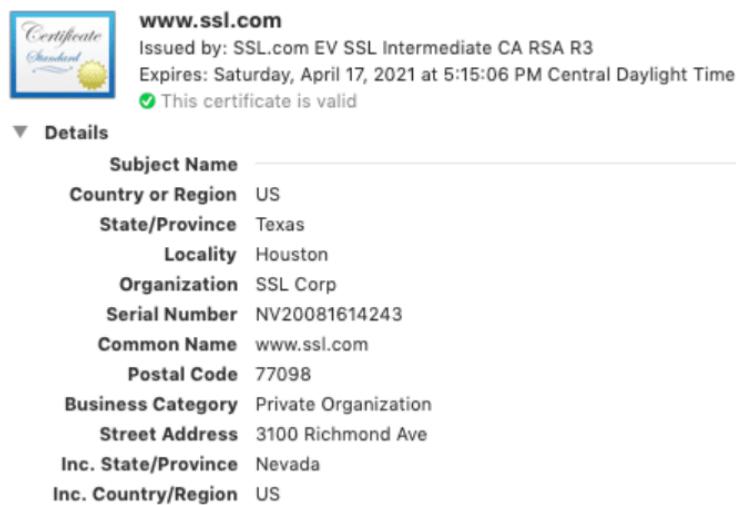


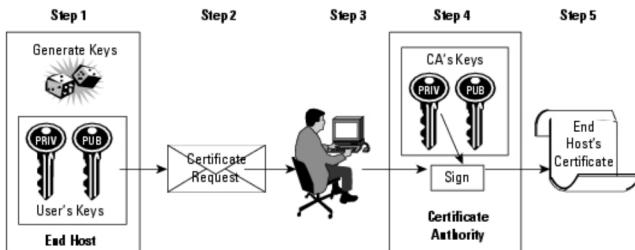
Figura 1.2: Exemplo de um certificado X.509 [2]

## 1.5 SCEP

Simple Certificate Enrollment Protocol (SCEP) é um protocolo que permite a troca segura de informações de chaves e certificados digitais entre um cliente (host final) e uma Autoridade Certificadora (CA). Ele é usado para simplificar a inscrição e distribuição de certificados, garantindo a segurança do processo.

### Processo de Inscrição:

1. O host final gera um par de chaves privada-pública.
2. O host final gera um pedido de certificado, que é encaminhado para a Autoridade Certificadora (CA).
3. É necessária intervenção manual e humana para aprovar o pedido de inscrição.
4. Após a aprovação, a CA assina o certificado com sua chave privada e devolve o certificado completo ao host final.
5. O host final armazena o certificado.



## 1.6 Certificate Revocation Lists (CRL)

As Listas de Revogação de Certificados (CRL) são componentes cruciais da Infraestrutura de Chave Pública (PKI). Elas são:

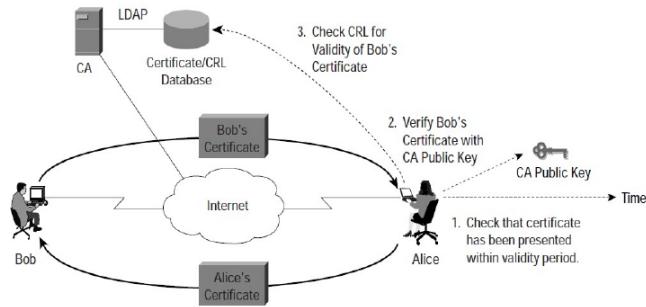
- **Definição:** Listas que enumeram certificados que já foram válidos na PKI, mas foram revogados por algum motivo.
- **Motivos de revogação:** Incluem comprometimento das chaves no certificado, perda de privilégios de acesso para usuário/dispositivo, ou mudança na estrutura da PKI que exige a reemissão do certificado.

As CRLs garantem a segurança da PKI ao informar quais certificados não devem ser mais confiados para autenticação e comunicação segura.

## 1.7 Certificate usage and validity check

Um certificado pode ser considerado válido e confiável para autenticação ou outras formas de comunicação segura se:

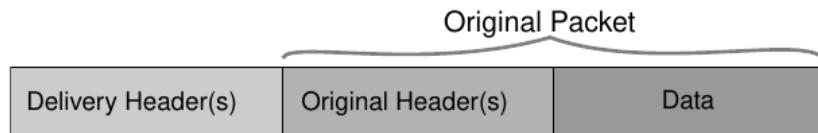
- O certificado é apresentado dentro do seu período de validade.
- A CA que assinou o certificado é conhecida e confiável.
- O certificado não está numa lista de revogação (opcional em alguns cenários).



## 1.8 Traffic Tunnel Concept

Um túnel assegura que um pacote enviado de um nó de rede alcance um nó específico em outra rede, independentemente dos processos de routing dos nós intermediários. Em situações onde os nós intermediários não suportam o protocolo de rede original do pacote, o túnel garante a entrega do pacote ao nó remoto ao adicionar cabeçalhos de protocolo adequados no ponto de entrada do túnel.

⇒ O túnel define um canal virtual que oferece recursos adicionais de transporte de dados, como garantia de qualidade de serviço (QoS), requisitos de segurança e routing otimizado, adicionando cabeçalhos de protocolo aos pacotes originais para guiá-los até o ponto de saída do túnel.



## 1.9 Virtual Tunnel Interface (VTI)

### 1.9.1 Virtual Tunnel Interface (VTI)

Um túnel é uma construção lógica que cria uma interface de rede virtual dentro de equipamentos de rede. Esta interface pode ser tratada como qualquer outra interface de rede. Embora um túnel não necessite de endereços de rede adicionais além dos já associados ao router de ponto final, na prática, muitas implementações exigem que um endereço de rede seja atribuído à interface do túnel para permitir o processamento de IP. Esse endereço pode ser explicitamente atribuído ou reutilizado de outra interface configurada no router. Essa abordagem permite estabelecer conexões virtuais eficientes entre redes utilizando recursos de endereçamento existentes.

#### 1.9.1.1 Requisitos

**Identificador numérico:** Necessário para identificação única.

**Endereço IP associado:** Essencial para processamento IP.

**Inclusão na tabela de routing:** Para routing de tráfego.

**Tipo de túnel definido:** Especifica o modo de túnel.

**Fonte do túnel:** Interface local ou endereço IP.

**Destino do túnel:** Domínio ou endereço IP de destino.

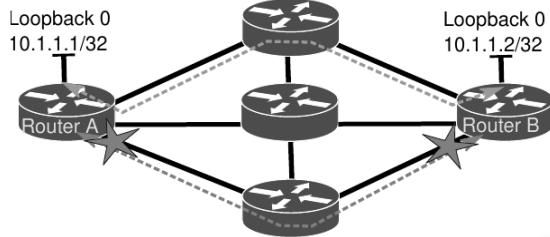
**Configurações adicionais:** Opcionais, como para routing, segurança e QoS.

```
1 #interface Tunnel 1
2 #ip address 10.1.1.1 255.255.255.252
3 #ipv6 address 2001:A:A::1/64
4 #ip unnumbered FastEthernet0/0
5 #ipv6 unnumbered FastEthernet0/0
6 #ip ospf cost 10
7 #ipv6 ospf 1 area 0
8 #tunnel mode ipip
9 #tunnel source FastEthernet0/0
10 #tunnel destination 200.2.2.2
```

### 1.9.2 Loopback Interfaces as End-Points

A interface loopback é uma construção lógica que cria uma interface de rede virtual totalmente independente das outras interfaces físicas e lógicas do router. O principal objetivo de uma interface loopback é fornecer um endereço de rede para servir como identificador do router em configurações de rede remota e distribuição de algoritmos.

A principal vantagem de usar interfaces loopback como pontos finais de túnel é a criação de um túnel que não está vinculado a nenhuma placa de rede ou ligação específica que possa falhar.



### 1.9.3 Tipos de Tuneis IP

**IPv4-IPv4:** Pacotes IPv4 são enviados usando IPv4 como protocolo de rede.

**GRE IPv4:** Pacotes originais são encapsulados com cabeçalho GRE e enviados usando IPv4.

**IPv6-IPv6:** Pacotes IPv6 são enviados usando IPv6 como protocolo de rede.

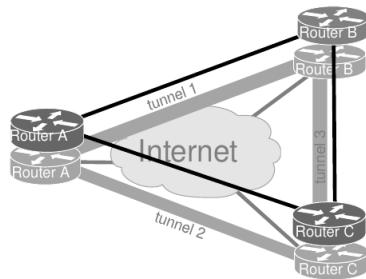
**GRE IPv6:** Pacotes originais são encapsulados com cabeçalho GRE e enviados usando IPv6.

**IPv6-IPv4:** Pacotes IPv6 são encapsulados e enviados usando IPv4 como protocolo de rede.

**IPv4-IPv6:** Pacotes IPv4 são encapsulados e enviados usando IPv6 como protocolo de rede.

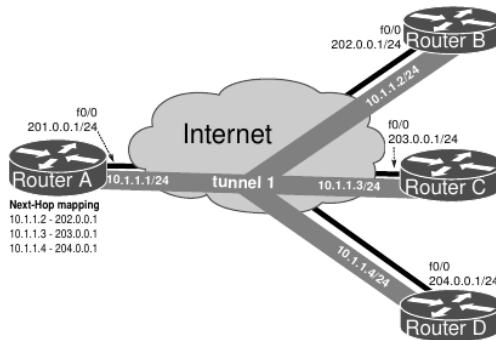
## 1.10 Overlay Network

Uma Overlay Network é uma rede virtual criada sobre outra rede, seja física ou virtual, para propósitos específicos como transporte privado, routing personalizado, QoS e segurança. Pode resultar em várias camadas de sobreposição e incluir protocolos de privacidade, sendo então chamada de Rede Privada Virtual (VPN).



## 1.11 Multipoint Tunnels

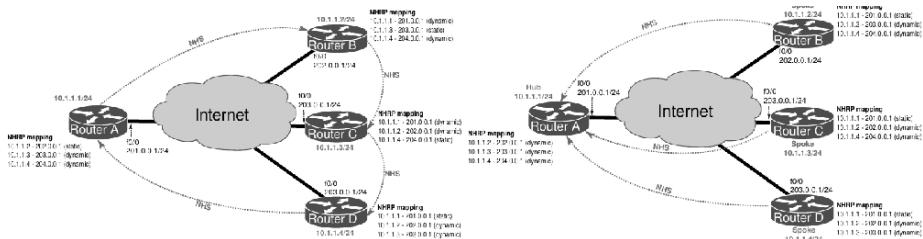
Em cenários com muitos a ser interligados, a abordagem mais simples e eficiente é usar um único túnel que conecta vários nós - um **Multipoint Tunnel**. Isto permite conexões diretas usando uma única rede IP virtual sobreposta dentro do túnel, onde o endereço de entrega é determinado pelo próximo salto na rede sobreposta. O mapeamento de endereços entre as redes *Overlay* e *underlay* pode ser estático ou dinâmico.



## 1.12 Next Hop Resolution Protocol (NHRP)

O NHRP permite mapear o endereço IP de uma interface de túnel (rede *Overlay*) para o respetivo endereço IP da interface de rede subjacente. Cada nó deve conhecer pelo menos um outro nó na rede *Overlay* (juntamente com os endereços sobrepostos e subjacentes) através do qual tentará encontrar os mapeamentos de endereços dos outros nós.

Além disso, todos os nós devem ser configurados de modo que tenham pelo menos um caminho válido para todos os outros nós, formando assim uma malha parcial.



## 1.13 Hub-Spoke vs. Spoke-Spoke

### Hub-Spoke:

- Conexões ponto-a-ponto de túneis GRE de cada site remoto para um nó central (Hub) pré-definido.
- Comunicação entre sites remotos passa pelo Hub.
- Pode ter múltiplos Hubs para redundância.

### Spoke-Spoke:

- Conexões de túnel dinâmicas diretamente entre sites remotos, sem passar pelo Hub.
- Comunicação direta entre sites remotos.
- Não suporta routing dinâmico entre sites remotos.
- Não interoperável com roteadores que não sejam Cisco IOS.

## 1.14 IPSec (Internet Protocol Security)

IPSec (Internet Protocol Security) é um framework de protocolos e algoritmos de segurança utilizados para proteger dados na camada de rede.

### Authentication Header (AH)

- Garante a integridade dos dados.
- Não fornece confidencialidade.
- Oferece autenticação de origem.
- Utiliza mecanismos de hash com chave.
- Não protege o cabeçalho IP.

### Encapsulating Security Payload (ESP)

- Fornece confidencialidade dos dados através de criptografia.
- Garante a integridade dos dados.
- Não protege o cabeçalho IP.
- Tanto AH quanto ESP utilizam algoritmos de chave secreta simétrica, embora algoritmos de chave pública sejam possíveis.

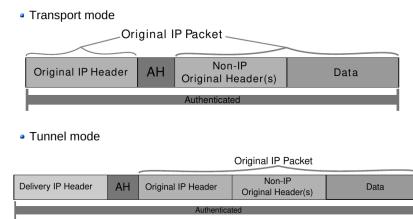
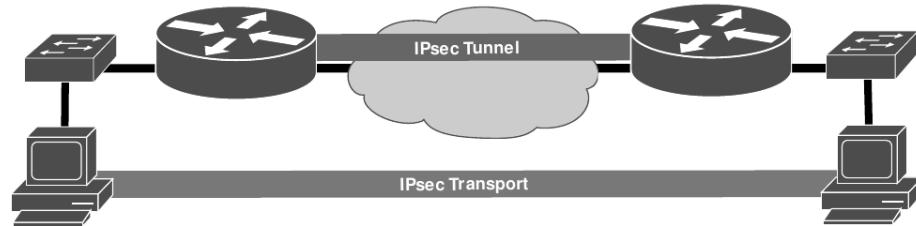
Esses protocolos são fundamentais para estabelecer comunicações seguras na Internet, protegendo contra intercetação, modificação e falsificação de dados durante a transmissão.

### 1.14.1 IPSec Modes

#### Tunnel

- Os gateways IPSec fornecem serviços IPSec para outros hosts em túneis ponto-a-ponto.
- Os hosts finais não estão cientes de que o IPSec está a ser usado para proteger o seu tráfego.
- Os gateways IPSec oferecem proteção transparente sobre redes não confiáveis.

Essas abordagens permitem proteger o tráfego de rede utilizando IPSec de maneiras diferentes, seja encapsulando todo o tráfego em túneis seguros entre gateways ou protegendo diretamente as comunicações de host a host.



#### Transport

- Cada host final faz a encapsulação IPSec de seus próprios dados, de host para host.
- O IPSec deve ser implementado nos hosts finais.
- O ponto de aplicação também deve ser endpoint IPSec.

Essas abordagens permitem proteger o tráfego de rede utilizando IPSec de maneiras diferentes, seja encapsulando todo o tráfego em túneis seguros entre gateways ou protegendo diretamente as comunicações de host a host.

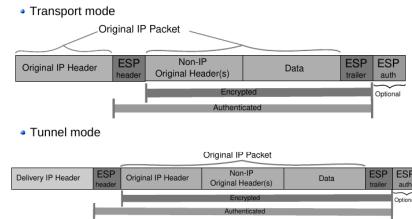


Figura 1.3: AH header placement

Figura 1.4: ESP header placement

#### 1.14.2 AH and ESP Header

##### AH (Authentication Header) do IPSec

- **Next Header:** Identifica o tipo do próximo payload após o AH.
- **Header Length:** Especifica o comprimento do cabeçalho em unidades de 4 bytes.
- **SPI:** Identifica a SA de saída do IPSec.
- **Sequence Number:** Contador de pacotes enviados pela mesma SA.
- **ICV:** Saída da função de hash de autenticação.

##### ESP (Encapsulating Security Payload) do IPSec

- **SPI:** Identifica a SA de saída do IPSec.
- **Sequence Number:** Contador de pacotes enviados pela mesma SA.
- **Padding:** Preenchimento para alinhar os campos corretamente.
- **Pad Length:** Indica o número de bytes de preenchimento.
- **Next Header:** Identifica o tipo de dados no payload.
- **ICV:** Saída da função de hash de autenticação aplicada aos dados protegidos.

#### 1.14.3 IPSec - Security Associations

Um SA (Security Association) é um contrato de política entre dois pares ou hosts para proteger o tráfego de rede usando IPSec. Ele inclui:

- **Algoritmo de Autenticação/Encriptação e Parâmetros:** Define o método de autenticação/criptografia, tamanho da chave e outros detalhes como tempo de vida da chave.
- **Chaves de Sessão:** Usadas para autenticação/criptografia, podem ser configuradas manualmente ou negociadas automaticamente.
- **Especificação do Tráfego:** Define o tipo de tráfego protegido, como tráfego IP geral ou sessões específicas como TELNET.
- **Protocolo de Encapsulação (AH ou ESP) e Modo (Túnel ou Transporte):** Especifica se será usado AH (para autenticação) ou ESP (para autenticação e criptografia), e se a proteção será em modo túnel (para rede a rede) ou transporte (para host a host).

#### 1.14.4 Establishing SA and Cryptographic Keys

Protocolos de gestão de Chave e Acordo de Chave no IPSec:

#### ISAKMP (Internet Security Association and Key Management Protocol)

- Estabelece Security Associations (SA) e chaves criptográficas no IPSec.
- Separado dos detalhes específicos de troca de chaves.
- Framework para gestão de associações de segurança e gestão de chaves.
- **Fase 1**
  - Define parâmetros para autenticação, encriptação de trocas, autenticação de pares e geração de chaves.
  - **Modo Principal:** Seis trocas de pacotes, segurança robusta.
  - **Modo Agressivo:** Três trocas de pacotes, configuração mais rápida mas menor segurança.
- **Fase 2 - Modo Rápido**
  - Negocia parâmetros para estabelecer um serviço de comunicação IPsec totalmente funcional.

#### Oakley Key Determination Protocol

- Protocolo de acordo de chave para troca de material de chave entre pares autenticados.
- Utiliza o protocolo Diffie-Hellman para estabelecer segredos compartilhados.

#### SKEME

- Protocolo de troca de chaves que oferece métodos seguros para autenticação e troca de chaves no IPSec.

#### IKE (Internet Key Exchange)

- Protocolo híbrido que combina partes do Oakley e SKEME com ISAKMP.
- Usado para estabelecer SA e chaves criptográficas de maneira eficiente e segura no IPSec.

### 1.14.5 IPsec NAT Transversal

Quando se trata de NAT/PAT e suas incompatibilidades com IPsec, aqui estão os pontos principais:

#### AH (Authentication Header)

- Incorpora os endereços de origem e destino IP no controlo de integridade da mensagem protegida por chave. Isso pode ser problemático com NAT/PAT, pois modifica os endereços IP.

#### ESP (Encapsulating Security Payload)

- Não apresenta problemas com NAT/PAT, pois o cabeçalho ESP não inclui informações de endereço IP que podem ser afetadas por tradução de endereços.

#### Checksums TCP e UDP

- Podem ser atualizados porque são protegidos pelo IPsec, não sendo afetados pela NAT/PAT.

#### Endereços IP como Identificadores no IKE

- São utilizados para determinar credenciais durante a troca de chaves. A NAT/PAT pode interferir com essa correspondência devido às alterações nos endereços IP.

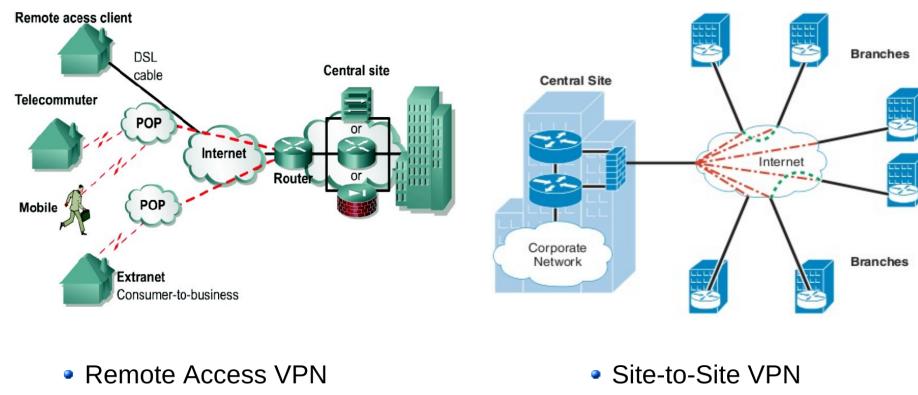
#### NAT Traversal com ISAKMP/IPsec

- Durante a primeira fase do ISAKMP/IPsec, os hosts podem detetar a necessidade de ativar a travessia de NAT.
- Fases subsequentes do ISAKMP/IPsec encapsulam pacotes em pacotes UDP, geralmente na porta UDP 4500.
- Os endereços IP originais são enviados como payloads NAT-OA (NAT Original Address) no ISAKMP.

# Virtual Private Networks (VPN)

Uma ligação encriptada entre redes privadas através de uma rede pública é geralmente conhecida como Rede Privada Virtual (VPN). Esta tecnologia permite a comunicação segura entre redes remotas ou geograficamente separadas ao cifrar o tráfego de dados sobre a internet pública ou outra rede pública.

As VPNs utilizam tecnologias como IPSec (Protocolo de Segurança IP), SSL/TLS (Secure Sockets Layer/Transport Layer Security) e outras para garantir que os dados transmitidos entre estas redes privadas permaneçam confidenciais e seguros. Este tipo de configuração permite que organizações estendam as suas redes privadas de forma segura através de redes públicas potencialmente inseguras, oferecendo um canal seguro para comunicação e troca de dados.



## 2.1 Variants of Site-to-Site IPsec VPN

- Túneis IPsec com Configuração Estática:
  - Requer conhecimento prévio dos endereços IP e parâmetros de segurança de todos os pares.
  - Alta complexidade de configuração.

- **Túneis IPsec com Configuração Dinâmica (na cabeça/hub):**
  - Configuração hub + spokes (estrelada).
  - Configuração genérica no hub, facilitando a adição de novos spokes (ramos).
  - Permite adicionar novos nós de forma simples.
- **Limitação:**
  - Túneis IPsec básicos não protegem tráfego multicast.
- **Solução: IPsec + Túneis GRE**
  - Encapsulamento Genérico de routing (GRE) permite a proteção de tráfego multicast sobre IPsec.
  - VPN Dinâmica Multiponto (DMVPN): facilita a configuração e a gestão de túneis dinâmicos, suportando tráfego multicast e simplificando a adição de novos nós.

## 2.2 Dynamic Multipoint VPN

**Dynamic Multipoint VPN (DMVPN)** é uma tecnologia que permite a criação de redes privadas virtuais (VPNs) de forma dinâmica e eficiente. Utilizando o **Protocolo de Resolução de Próximo Salto (NHRP)**, o DMVPN cria uma rede de sobreposição que facilita a conectividade em malha total com configuração simples de **hub e spoke**. Suporta dispositivos com endereços IP dinâmicos, permitindo a configuração **zero-touch** para adicionar novos pontos de acesso sem complicações. Além disso, o DMVPN ativa automaticamente túneis **IPsec** para assegurar a segurança das comunicações.

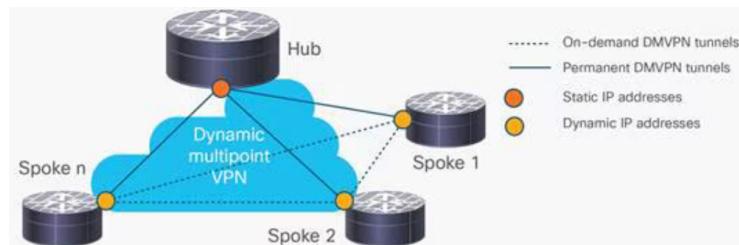


Figura 2.1: Dynamic Multipoint VPN [3]

## 2.3 SD-WAN

**Software Defined WAN (SD-WAN)** é uma tecnologia de rede que melhora a gestão e a eficiência das redes de longa distância (**WAN**).

### Principais Características:

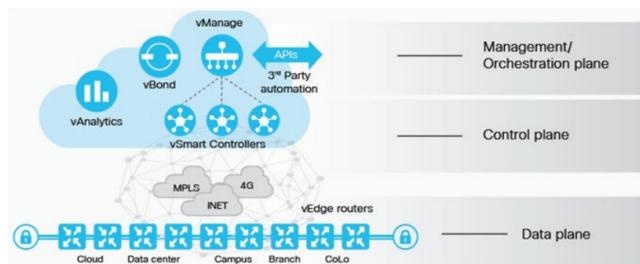
- **Abstração da Conectividade na Borda:** Facilita a conexão flexível e ágil nas extremidades da rede.
- **Virtualização da WAN:** Cria redes sobrepostas para otimizar o tráfego.
- **Gestão Centralizada:** Configura e gera a rede com políticas centralizadas.
- **Gestão de Tráfego Elástica:** Ajusta o tráfego conforme as necessidades.

**Vantagens:** 😊

- Fácil implementação e gestão.

**Desvantagens:** 😢

- Dependência de fornecedores externos.



## 2.4 Remote Access VPN

### Tipos Comuns de Serviços/Protocolos:

- L2TP/IPsec
- IKE + ISAKMP + L2TP
- OpenVPN
- SSL
- Proprietário (baseado em SSL ou IPsec)

### Tipos de Autenticação:

- Pré-compartilhada
- RADIUS/LDAP
- RSA com CA embutida
- RSA com CA externa
- Certificados/Credenciais devem ser distribuídos de forma segura

### **L2TP/IPsec - VPN de Acesso Remoto:**

- **Autenticação:** Certificados Digitais (RSA) ou mecanismos de autenticação PPP como PPTP
- **Integridade de Dados:** Garantida
- **Criptografia:** Fornecida pelo IPsec (protocolo ESP)
- **Supporte:** Múltiplos túneis simultâneos por usuário
- **Desempenho:** Mais lento que PPTP

### **Outros Tipos de VPN de Acesso Remoto:**

- **SSL/TLS VPN:** Criação de túnel VPN usando protocolo SSL/TLS
- **SSH VPN:** VPN sobre conexão SSH, incluindo túnel SSH e encaminhamento de porta
- **OpenVPN:** Implementa uma VPN SSL/TLS com suporte a autenticação por PSK, certificados e login/senha. Utiliza OpenSSL para criptografia.

## **2.5 Remote VPN Network Integration**

Na integração de redes VPN remotas, o servidor VPN pode ser implantado nos firewalls para garantir que o tráfego seja protegido e gerido centralmente. Alternativamente, pode ser colocado na DMZ para adicionar uma camada de segurança entre redes internas e externas. O routing do tráfego VPN pode ser configurado para passar pelo firewall pela mesma zona de rede ou por interfaces diferentes, possibilitando políticas de segurança variadas. No entanto, encaminhar o tráfego diretamente para a zona privada sem passar pelo firewall pode comprometer a segurança ao ignorar as políticas de segurança estabelecidas.

## **2.6 Integration with Flow Control**

### **OpenVPN:**

- Utiliza a porta UDP 1194 por padrão para comunicação.

### **IPsec:**

- Usa a porta UDP 500 para IKE.
- O protocolo ESP é identificado pelo número IP 50 e AH pelo número IP 51.
- Para travessia de NAT, utiliza a porta UDP 4500.

### **L2TP:**

- Utiliza a porta UDP 1701.
- Pode não ser necessário especificar uma exceção quando o L2TP é encapsulado dentro de pacotes IPsec.

# Intrusion Detection and Prevention

## Sistemas de Deteção de Intrusão (IDS):

- Analisam informações de várias fontes como computadores, servidores, serviços e tráfego de rede.
- Identificam intrusões e uso indevido.
- Não bloqueiam intrusões, apenas sinalizam alarmes.
- Alarmes são destinados para análise humana ou para respostas automáticas.

## Sistemas de Prevenção de Intrusão (IPS):

- No nível de rede, bloqueiam tráfego suspeito.
- No nível do host, podem tomar ações como encerrar processos, quarentena de arquivos, bloquear acesso, etc.

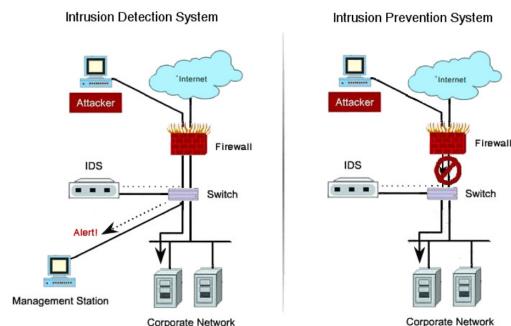


Figura 3.1: Intrusion Detection vs Intrusion Prevention [4]

### **3.1 Host-Based vs. Network-Based**

#### **Implantação no Nível do Host (Endpoint):**

- Monitora tráfego de rede, processos, acesso a arquivos e dispositivos, fluxos de dados, alocações de memória e características físicas do dispositivo (temperatura, consumo de energia, movimento, etc.).
- Conhecido atualmente como Endpoint Detection and Response (EDR).

#### **Implantação no Nível de Rede:**

- Monitora tráfego nos níveis de pacote e fluxo, além de sinais físicos como rádio, elétricos e ópticos.
- É implementado em vários pontos da rede, incluindo acessos à Internet, WAN, links entre zonas e redes sem fio.

### **3.2 Signature vs. Anomaly Based**

Para fazer a deteção de intrusões usam-se dois métodos distintos:

#### **Deteção Baseada em Assinatura:**

- Os dados monitorados são comparados a padrões de ataque pré-configurados e predefinidos conhecidos como assinaturas.
- Ataques possuem assinaturas distintas e conhecidas.
- As assinaturas devem ser constantemente atualizadas para mitigar ameaças emergentes.
- As assinaturas podem incluir valores individuais de cabeçalho de pacote, padrões de dados binários, sequências de pacotes com características específicas dentro do mesmo fluxo, ou conjuntos de fluxos de dados com características específicas.

#### **Deteção Baseada em Anomalia:**

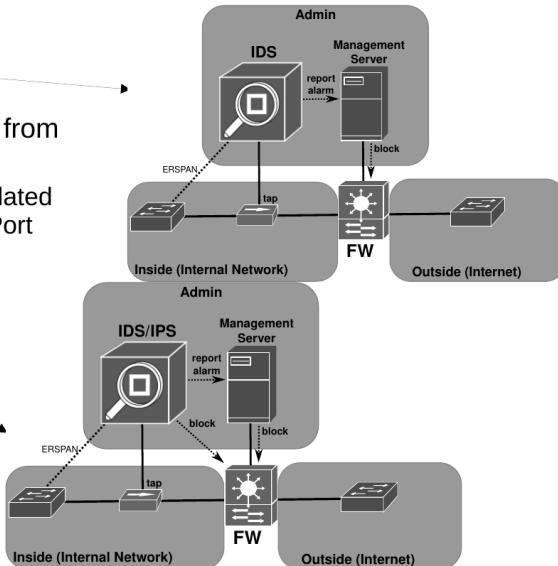
- Estabelece um perfil de comportamento (baseline) e detecta desvios desse perfil.
- Pode depender apenas de estatísticas de alto nível de sistemas ou redes, ou incluir múltiplas fontes de dados.
- Pode ser baseado em regras pré-definidas ou em modelos de inteligência artificial (IA).

### 3.3 Endpoint Detection and Response (EDR)

O Endpoint Detection and Response (EDR), também conhecido como Endpoint Detection and Threat Response (EDTR), é uma tecnologia que monitoriza, regista e analisa as atividades e eventos em dispositivos, fornecendo visibilidade contínua e abrangente dos processos e atividades dos utilizadores nos dispositivos. Além disso, permite uma resposta direta a incidentes em dispositivos e servidores. Essa tecnologia pode ser implantada tanto em dispositivos individuais quanto com um agente no dispositivo e análise/armazenamento de dados externos.

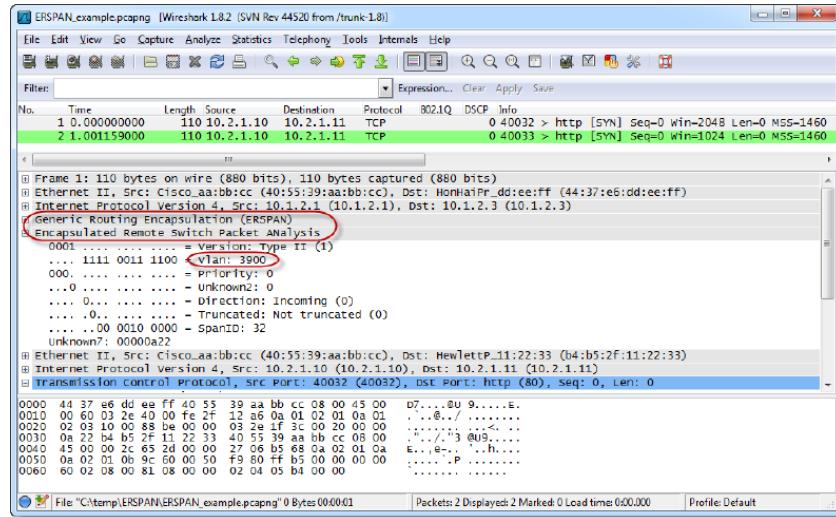
### 3.4 Network Deployment (1)

- IDS
  - ♦ Network tap.
  - ♦ ERSPAN GRE tunnel from switch.
    - ERSPAN: Encapsulated Remote Switched Port ANalyzer
  - ♦ Reports to network management system.
- IPS
  - ♦ IDS with firewall integration.



### 3.5 ERSPAN

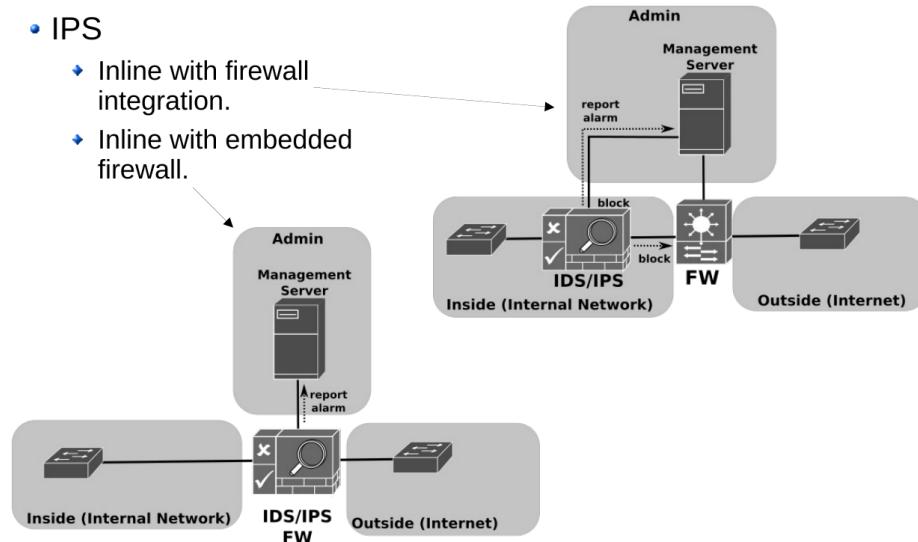
O Encapsulated Remote Switched Port Analyzer (ERSPAN) é uma tecnologia de espelhamento de tráfego de rede que espelha o tráfego de uma ou mais portas de switch, encapsula esse tráfego usando o protocolo GRE(Generic Routing Encapsulation) e envia-o para um ou mais destinos remotos. Isso permite a monitorização e análise do tráfego de rede de forma remota, sem a necessidade de estar fisicamente conectado à porta de switch.



### 3.6 Network Deployment (2)

- IPS

- ◆ Inline with firewall integration.
- ◆ Inline with embedded firewall.



## 3.7 IDS/IPS Actions

### Suricata:

- **alert:** gera uma alerta.
- **pass:** interrompe a inspeção do pacote.
- **drop:** dropa o pacote e gera uma alerta.
- **reject:** envia um erro de RST/ICMP para o remetente.
- **rejectsrc:** mesma ação que reject.
- **rejectdst:** envia um erro de RST/ICMP para o receptor.
- **rejectboth:** envia erros de RST/ICMP para ambos os lados da conversa.

### Snort:

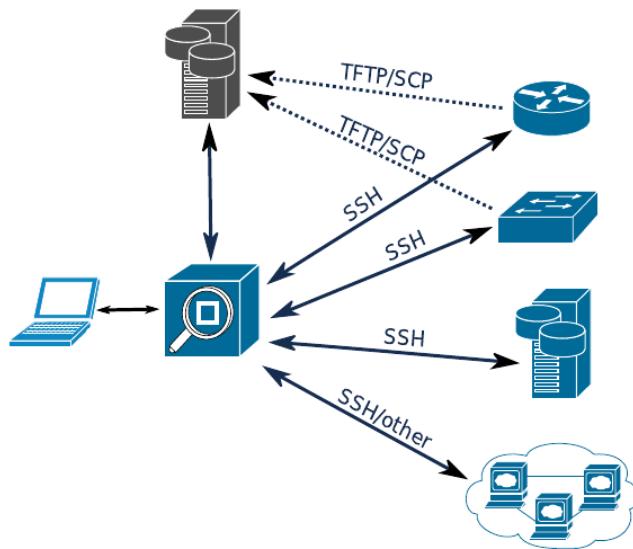
- **alert:** gera uma alerta e registra o pacote.
- **log:** registra o pacote.
- **pass:** ignora o pacote.
- **drop:** bloqueia e registra o pacote.
- **reject:** bloqueia o pacote, registra e envia um reset TCP ou um erro ICMP de porta inalcançável se o protocolo for UDP.
- **sdrop:** bloqueia o pacote, mas não registra.

# Monitoring & SIEM & NOC/SOC

## 4.1 Remote CLI Access

Utilizar uma consola remota para gerir dispositivos envolve:

- Utilizar SSH (seguro), telnet (inseguro) ou protocolos proprietários para estabelecer conexões.
- Recuperar configurações e verificar o estado dos processos do dispositivo.
- Enviar configurações para um ponto central utilizando TFTP (inseguro) ou SFTP/SCP (mais seguro, mas nem sempre suportado).
- Enviar comandos CLI como "show", recolher os resultados dos comandos e analisar as informações.



## 4.2 Log Files Access

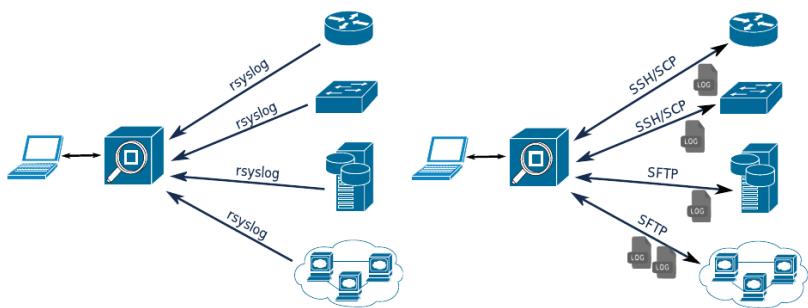
### Acesso a Arquivos de Log

#### rsyslog:

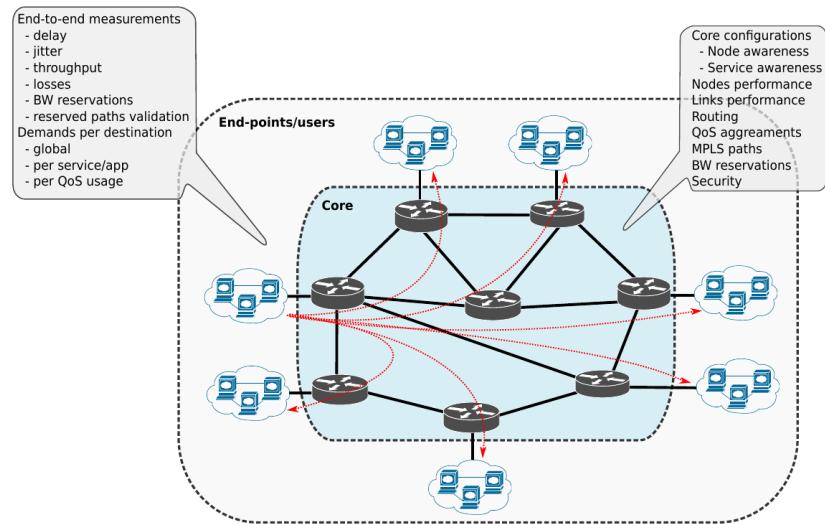
- Capaz de receber entradas de uma ampla variedade de serviços, transformá-las e enviar os resultados para diversos destinos de rede.
- Utiliza TCP e/ou SSL/TLS para comunicação segura.
- O controlo de tempo é realizado pelo nó/dispositivo monitorado.
- Muitas tarefas de pós-processamento e processamento cruzado podem ser executadas no próprio nó/dispositivo monitorado.

#### Acesso direto a arquivos de log:

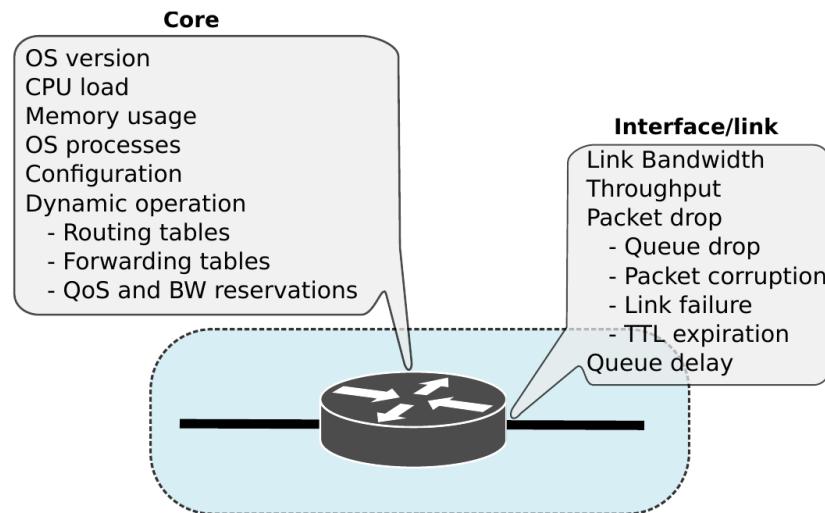
- Acesso remoto aos arquivos de log utilizando SSH/SCP, SFTP, entre outros.
- Requer permissões especiais para acessar os arquivos.
- O controlo de tempo é gerenciado pelo ponto central.
- Todos os processamentos pesados de pós-processamento e processamento cruzado ocorrem no ponto central.



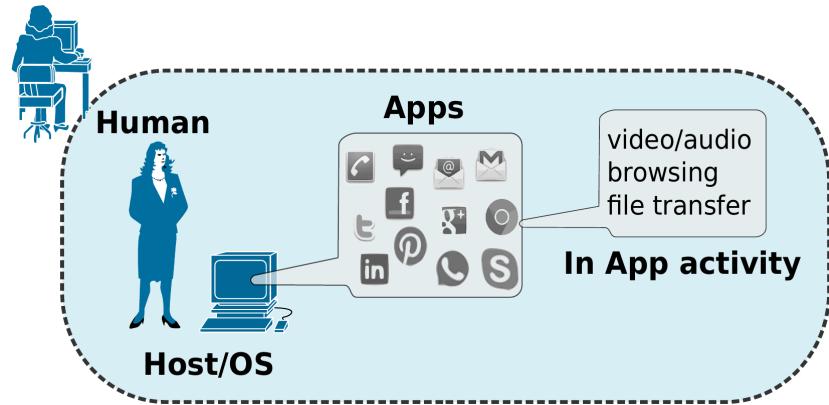
### 4.3 Core and End-to-End Monitoring



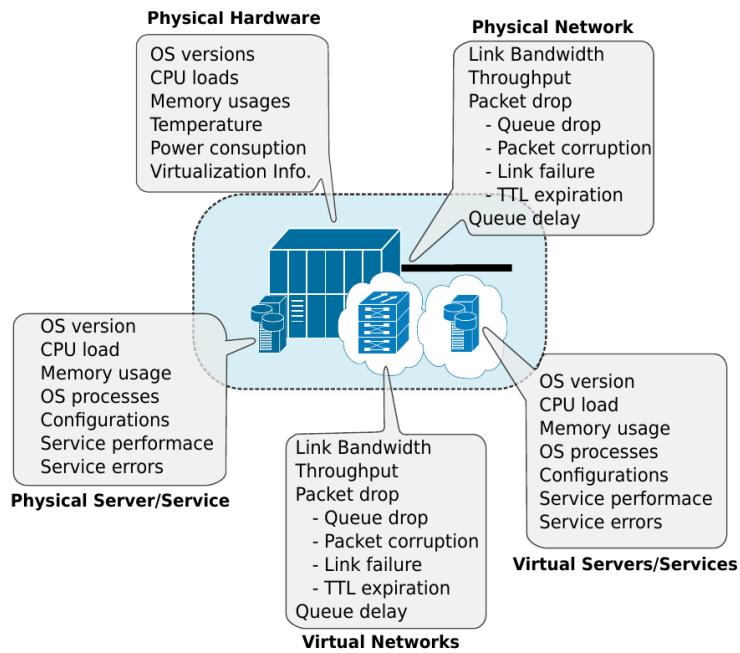
### 4.4 Node Monitoring



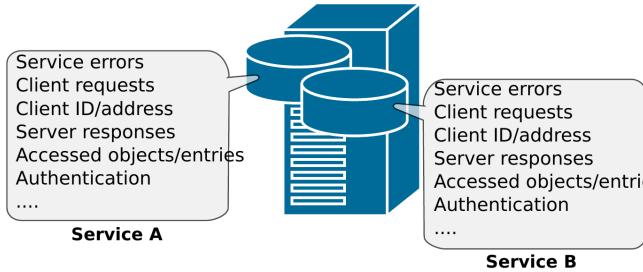
## 4.5 End-User/Host/App Monitoring



## 4.6 Server/Service/Cloud Monitoring



## 4.7 Per-Service Detailed Monitoring



## 4.8 Data Sources

### 4.8.1 SNMP

SNMP é um protocolo para gerir e monitorizar de redes de computadores. Ele é parte integrante de protocolos TCP/IP, e sua principal função é permitir aos administradores monitorizarem e controlem dispositivos de rede remotamente. SNMP é uma arquitetura cliente-servidor, onde os dispositivos geridos (como routers, switches, entre outros) são configurados para enviar informações para um servidor SNMP, conhecido como NMS (Network Management System).

- **SNMP agent:** Um módulo de software que reside em elementos de rede; recolhe e armazena informações de gestão especificadas nos módulos MIB suportados. O agente SNMP responde a pedidos SNMP de uma estação NMS para informações e ações. O agente SNMP pode enviar notificações de falha proativamente para o gestor SNMP.
- **Managed object:** Uma representação de algo que pode ser gerido. Os objetos geridos diferem das variáveis, que são instâncias específicas de objetos.
- **Management Information Base (MIB):** É uma base de dados virtual que contém informações sobre os dispositivos geridos numa rede. Essas informações são organizadas hierarquicamente e podem incluir dados como configurações, status, estatísticas e outros parâmetros relevantes.
- **Syntax notation:** Uma linguagem usada para descrever objetos geridos num formato independente de máquina. Sistemas de gestão baseados em SNMP utilizam um subconjunto da Notação de Sintaxe Abstrata 1 (ASN.1) da Organização Internacional de Normalização (ISO) para definir tanto os pacotes trocados pelo protocolo de gestão quanto os objetos a serem geridos.

- **Structure of Management Information (SMI):** Define as regras para descrever informações de gestão (a MIB).

#### 4.8.1.1 SNMP versions

<b>Model</b>	<b>Level</b>	<b>Authentication</b>	<b>Encryption</b>	<b>What Happens</b>
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit or CFB128-AES-128 encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Figura 4.1: Versões SNMP

#### 4.8.1.2 SNMP Operations

O SNMP fornece as seguintes cinco operações básicas:

1. **Operação Get:** Pedido enviado pelo NMS ao agente para recuperar um ou mais valores do agente.
2. **Operação GetNext:** Pedido enviado pelo NMS para recuperar o valor do próximo OID na árvore.
3. **Operação Set:** Pedido enviado pelo NMS ao agente para definir um ou mais valores do agente.
4. **Operação de Resposta:** Resposta enviada pelo agente ao NMS.
5. **Operação de Armadilha (Trap):** Resposta não solicitada enviada pelo agente para notificar o NMS dos eventos ocorridos.

#### 4.8.1.3 SNMP Names (numbers/OID)

Para nomear todos os objetos possíveis (protocolos, dados, etc.), é utilizado uma árvore de MIB da ISO:

- Nomenclatura hierárquica de objetos
- Cada folha da árvore possui um nome e número.

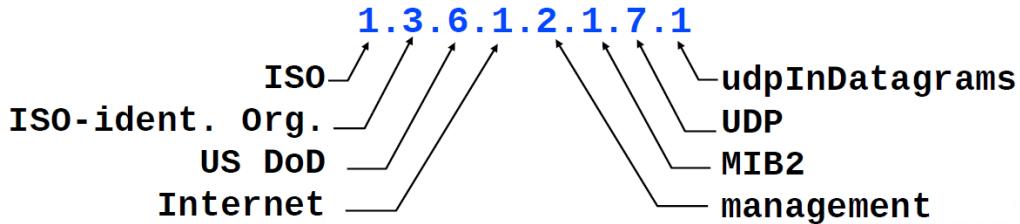


Figura 4.2: SNMP numbers

#### 4.8.1.4 SNMP MIBs

MIB é um conjunto de objetos geridos, utilizado para definir informações provenientes de equipamentos, criado pelo fabricante.

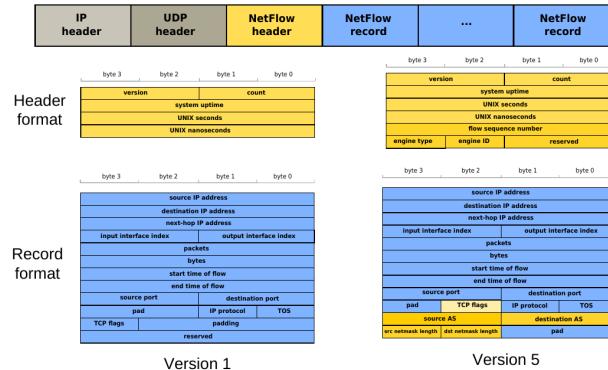
Um MIB armazena informações sobre os dispositivos de rede, como routers, switches, servidores, entre outros. Essas informações são organizadas numa árvore de hierarquia, e cada informação específica é identificada por um número único chamado OID (Object Identifier).

## 4.9 NetFlow

Os serviços de NetFlow da Cisco fornecem informações de fluxo de IP para administradores de rede. Coletam dados de pacotes de entrada e saída, estatísticas e detalhes de fluxos, incluindo endereços IP, contagem de pacotes e bytes, horários e mais. Existem três versões principais: v1, v5 e v9, com v1 recomendada apenas para dispositivos legados e v1 e v5 sem suporte a fluxos IPv6.

### 4.9.1 NetFlow versions 1 and 5

- NetFlow v1/v5 packets are UDP/IP packets with a NetFlow header and one or more NetFlow data Records

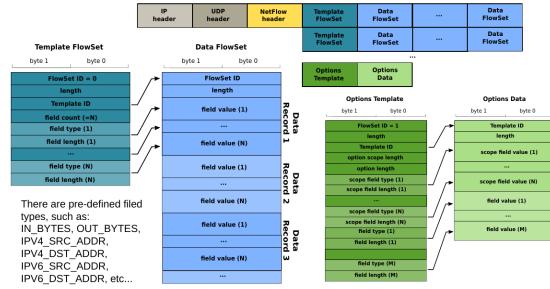


Version 1

Version 5

### 4.9.2 NetFlow version 9

- NetFlow v9 packets are UDP/IP packets with a NetFlow header, one or more Template FlowSets (may be suppressed, if sent previously), one or more Data FlowSets, and, optionally, an Options Template and Data Record.



O NetFlow é utilizado para caracterizar e analisar o tráfego de rede em ambientes complexos. Ele é empregado principalmente para quantificar o uso de usuários, grupos e serviços com base na quantidade de tráfego gerado. Essa caracterização é aplicada em interfaces VLAN para segmentar o tráfego de usuários e grupos, além de ser crucial em interfaces de data centers para monitorizar o tráfego de serviços específicos.

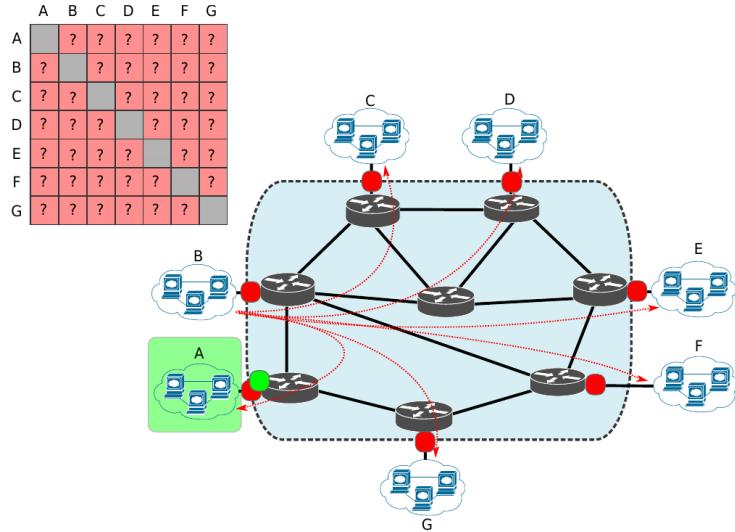
Além disso, o NetFlow é essencial para entender os destinos do tráfego, identificando os pontos de saída a partir de pontos de entrada específicos na rede. Isso é feito através da criação de matrizes de tráfego que destacam as interações entre diferentes partes da rede, incluindo links de acesso, borda do núcleo da rede e conexões de peering BGP.

No contexto do routing interno da rede, o NetFlow também desempenha um papel importante ao fornecer insights detalhados sobre como o tráfego é encaminhado e distribuído dentro da infraestrutura. No entanto, a implementação e o processamento do NetFlow podem ser complexos devido à vasta quantidade de dados gerados e à necessidade de análise detalhada para tomada de decisões informadas sobre a rede.

### 4.9.3 NetFlow Deployment

Para uma implementação eficaz do NetFlow, é essencial escolher quais interfaces monitorizar com base nos objetivos específicos:

- Matriz de Tráfego:** monitorizar interfaces principais de núcleo e borda para analisar padrões de tráfego dentro e entre redes.
- Fluxo de Usuário/Grupo:** Identificar e inferir o tráfego gerado por usuários específicos ou grupos.
- Entrada vs. Saída:** Analisar tanto o tráfego que entra quanto o que sai da rede para entender os padrões de comunicação e roteamento.



## 4.10 IPFIX (v10) and Flexible NetFlow

IPFIX (IP Flow Information Export) é uma evolução do NetFlow v9, utilizando o cabeçalho da versão 10 e mantendo conceitos como Templates e Registros de Dados. Introduz os Templates de Opções e os Registros de Dados de Opções, além de oferecer suporte expandido para elementos de informação compatíveis com NetFlow v9. IPFIX também suporta mais tipos de campos do que NetFlow v9, permitindo identificadores de elementos de informação e IDs de fornecedor para exportação de informações genéricas ou proprietárias. Flexível, suporta campos de comprimento variável, útil para exportar strings de tamanho variável como URLs. Por outro lado, o NetFlow v9 se expande com o Flexible NetFlow, que procura igualar a flexibilidade do IPFIX.

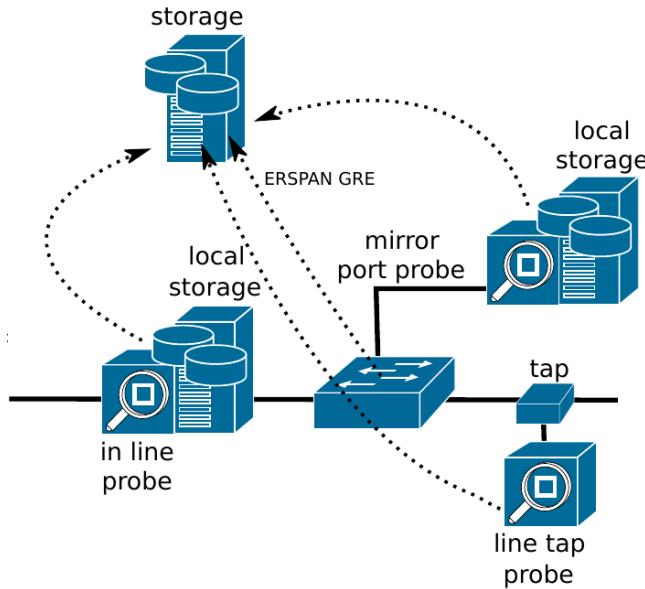
## 4.11 Network Passive Probing

Network Passive Probing é utilizado para inferir dados específicos e detalhados, assim como dinâmicas de curto e médio prazo em redes. As sondas são implementadas de várias formas:

- Porta espelho do switch: Replica o tráfego de uma porta para análise.
- In-line: Coloca uma sonda diretamente na rota do tráfego.
- Tap de rede: Dispositivo físico que intercepta e replica o tráfego de rede.
- Túnel ERSPAN GRE: Túnel GRE encapsulado para transmitir tráfego monitorado.

Os dados podem ser filtrados ou amostrados por endereço de usuário, VLAN, porta de acesso, protocolos (UDP/TCP), ou número de porta UDP/TCP. A análise pode incluir contagem de pacotes/bytes, fluxos, distribuição de endereços IP e portas, estatísticas de aplicativos/serviços, entre outros.

O armazenamento e processamento dos dados podem ser localizados ou centralizados. O upload centralizado não deve afetar as medições, enquanto o armazenamento/processamento local exige sondas mais robustas.



## 4.12 Log Management Systems (LMS)

Um Sistema de gestão de Logs (LMS) é um software essencial que coleta, armazena e faz a gestão de arquivos de log de várias fontes e sistemas de rede. Ele centraliza todos os dados de log em um único local, permitindo:

- Coleta e armazenamento centralizado de logs de diversas fontes.
- Visualização e correlação de eventos para detetar anomalias ou padrões.
- Deteção e resposta a Indicadores de Comprometimento (IoC).
- Análise forense para investigar eventos de rede e possíveis ataques.

Esses sistemas são fundamentais para garantir a segurança cibernética, oferecendo visibilidade e capacidade de resposta diante de ameaças e incidentes.

## 4.13 Security Information and Events Management (SIEM)

Security Information and Event Management (SIEM) integra três tipos de ferramentas de segurança numa única aplicação:

- **Security Event Management (SEM):** Similar ao LMS, mas voltado para analistas de segurança de TI. Agrega arquivos de log de múltiplos sistemas para análise de segurança.
- **Security Information Management (SIM):** Identifica, coleta e analisa dados de logs de eventos. Inclui recursos automatizados e alertas para condições pré-determinadas que podem indicar comprometimento da rede.
- **Security Event Correlation (SEC):** Processa e busca grandes quantidades de logs de eventos para descobrir correlações e conexões que podem indicar problemas de segurança.

## 4.14 LMS vs. SIEM

### LMS (Log Management System):

- Coleta de dados de log.
- Retenção eficiente de dados.
- Indexação e funções de pesquisa de logs.
- Relatórios detalhados sobre logs.

### SIEM (Security Information and Event Management):

- Detecção de ameaças e alertas.
- Correlação de eventos.
- Monitorização em tempo real com visibilidade personalizada.
- Dashboarding para monitorização de eventos.

Os LMS tradicionais eram mais voltados para suporte à administração de sistemas, enquanto os SIEM foram desenvolvidos desde o início como ferramentas de segurança. Com a evolução dos LMS, eles se tornaram funcionalmente mais próximos dos SIEM, integrando recursos avançados de detecção de ameaças e correlação de eventos.

## 4.15 SIEM Events (examples)

- Brute force detection
  - ◆ Excessive 404 errors (HTTP server Log) from a non-authenticated client (DB Log).
  - ◆ Excessive login failures (services or DB Logs) at one or multiple services.
    - From a specific IP address (or set of IP addresses).
    - From "strange" geographic regions or AS.
  - ◆ Non-matching credentials
    - From internal machines with non-matching user credentials (RADIUS/LDAP Logs).
- Impossible travel
  - ◆ Multiple logins from same user from different devices/locations.
  - ◆ Consecutive logins from same user from distant geographic regions within a small time window. VPN usage may trigger such an alarm.
- Anomalous data transference
  - ◆ Analyzing by individual source (IP or device group) and/or destination and/or by used protocol/port.
  - ◆ Excessive/Different data transference not compatible with past observations
    - Protocols and ports usage:
      - Usually firewall rules solve this!
    - Download/upload amounts, number of connections, ratio upload/download, ratio DNS/non-DNS, etc...;
    - Never contacted devices: external servers (unknown IP/ASN or country) or internal devices.;
    - Absolute time of day/week/month.
    - Relative time activity: mean or standard deviation of intervals between activity/flows/requests/etc...
  - ◆ Should be used to detect exfiltration (or propagation inside the network) and illicit C&C and data channels.
- DDoS attack
  - ◆ Excessive connection attempts from "never seen" devices/addresses/regions.
    - Ideal detection in the early phase of the attack.
  - ◆ Non-excessive attempts, but non-conformal behavior (time behavior, sequence of requests,etc...)
    - More difficult to define.
- Files/Configurations integrity fails
  - ◆ Specific device/service configuration file checksum failure, non justifiable by observed actions.
  - ◆ Generic file checksum failure, non justifiable by observed actions.

## 4.16 Security Operations Center (SOC)

O SOC realiza funções críticas numa organização:

### Prevenção e Detecção de Ataques:

- Monitora redes e serviços com SIEM.
- Detecta vulnerabilidades e atividades maliciosas.
- Identifica comportamentos anômalos.

### Investigação:

- Analisa atividades suspeitas.
- Avalia a extensão das ameaças.

### Resposta:

- Implementa contra medidas baseadas em playbooks.
- Ativa medidas de emergência quando necessário.

### Forense:

- Coleta evidências para investigações judiciais.

- Obtém dados para melhorar a segurança futura.

**Operação e Integração:**

- Tradicionalmente operado separadamente do NOC.
- Deve ser integrado ao NOC para melhorar a segurança geral.

# Bibliografia

- [1] H. Bodur, *Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application*, [https://www.researchgate.net/publication/298298027\\_Secure\\_SMS\\_Encryption\\_Using\\_RSA\\_Encryption\\_Algorithm\\_on\\_Android\\_Message\\_Application](https://www.researchgate.net/publication/298298027_Secure_SMS_Encryption_Using_RSA_Encryption_Algorithm_on_Android_Message_Application), 2015.
- [2] ssl, *What Is an X.509 Certificate?*, <https://www.ssl.com/faqs/what-is-an-x-509-certificate/>, 2019.
- [3] cisco, *Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications Data Sheet*, [https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data\\_sheet\\_c78-468520.html](https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html), 2017.
- [4] dataSilk, *Intrusion Detection - Prevention Systems : The Ultimate Guide*, <https://datasilk.com/intrusion-detection-prevention/>.