**VPN – Rede Privada Virtual**

**Conceito**

Uma **VPN (Virtual Private Network)** é uma conexão criptografada entre um dispositivo e uma rede por meio da Internet. Essa conexão segura:

* Garante a **confidencialidade** dos dados,
* **Impede interceptações** não autorizadas,
* Permite o **acesso remoto** a redes corporativas.

**Vantagens das VPNs**

* **Economia de custos**: Utilizam a Internet como meio de transporte, substituindo links WAN dedicados.
* **Segurança**: Utilizam criptografia e autenticação para proteção de dados.
* **Escalabilidade**: Permitem adicionar usuários sem grandes alterações na infraestrutura.

**Tipos de VPN**

**1. Site-to-Site VPN**

Conecta redes distintas, como filiais e sede, por meio de túneis VPN criados entre gateways de rede (roteadores, firewalls ou dispositivos ASA).

* O gateway encapsula e criptografa os dados,
* Transmite pelo túnel VPN,
* O gateway do destino descriptografa e entrega ao host final.

**2. Remote Access VPN**

Permite que usuários remotos (ex.: teletrabalhadores) acessem a rede interna de forma segura, usando:

* Cliente VPN,
* Conexão com gateway VPN,
* Tráfego criptografado ponto a ponto.

**Características de Segurança da VPN**

* **Confidencialidade**: Protege dados com criptografia e encapsulamento.
* **Integridade**: Garante que os dados não foram alterados.
* **Autenticação**: Verifica a identidade das partes por meio de:
  + Senhas,
  + Certificados digitais,
  + Cartões inteligentes,
  + Biometria.

**Técnicas e Tecnologias de Tunelamento**

O **tunelamento** encapsula pacotes inteiros em outros pacotes para transporte seguro em redes públicas.

**Criptografia**

* **DES (Data Encryption Standard)**: Chave simétrica de 56 bits.
* **3DES (Triple DES)**: Aplica criptografia-descriptografia-criptografia com diferentes chaves.
* **AES (Advanced Encryption Standard)**: Suporta chaves de 128, 192 e 256 bits; mais seguro e eficiente.
* **RSA**: Criptografia assimétrica com chaves de até 1024 bits ou mais.

**Protocolo de Segurança: IPsec (Internet Protocol Security)**

Protocolo para proteger comunicações IP, provendo:

* Criptografia,
* Autenticação,
* Integridade dos dados.

**Modos do IPsec:**

* **AH (Authentication Header)**: Fornece autenticação e integridade, mas não criptografa dados.
* **ESP (Encapsulating Security Payload)**: Fornece criptografia, integridade e autenticação (ao menos um deve ser selecionado).

**Algoritmos utilizados:**

* Criptografia: DES, 3DES, AES.
* Autenticação: MD5, SHA.
* Troca de chaves: Diffie-Hellman (DH1, DH2, etc.).

**Fases de Configuração IPsec**

**Fase 1 – IKE (Internet Key Exchange) Phase 1**

Objetivo: Estabelecer um túnel seguro para negociar a Fase 2.

1. Definir a interface da VPN.
2. Especificar o IP do peer remoto.
3. Autenticar com chave pré-compartilhada ou certificado.
4. Especificar políticas (padrão ou personalizadas).

**Elementos envolvidos:**

* Algoritmo de hash (MD5, SHA),
* Algoritmo de criptografia (DES, 3DES, AES),
* Grupo DH (Grupo 1: 768 bits, Grupo 2: 1024 bits, Grupo 5: 1536 bits),
* Método de autenticação (PSK ou RSA),
* Tempo de vida do túnel.

**Fase 2 – IKE Phase 2 / Túnel IPsec**

Objetivo: Proteger o tráfego dos usuários finais.

1. Negociar parâmetros do IPsec SA (Security Association).
2. Estabelecer as SA IPsec.
3. Realizar renegociação periódica.
4. Opcionalmente, executar troca adicional DH.

**Modos de Implementação de VPN**

1. **Gateway-to-Gateway**
2. **Gateway-to-Host**
3. **Host-to-Gateway**
4. **Host-to-Host** (maior segurança ponto a ponto)

**Checklist de Configuração**

1. **Escolher protocolo IPsec**: AH, ESP ou ambos.
2. **Selecionar algoritmo de criptografia**: DES, 3DES ou AES.
3. **Selecionar algoritmo de autenticação**: MD5 ou SHA.
4. **Escolher grupo Diffie-Hellman**: DH1, DH2, etc.
5. **Configurar ACLs**: Definem quais tráfegos serão protegidos.
6. **Confirmar configurações**: Em ambos os peers.

**Considerações Finais**

* O túnel da **Fase 1** é usado para negociação e gerenciamento.
* O túnel da **Fase 2 (IPsec)** é usado para transportar dados criptografados dos usuários.
* Ambos os dispositivos devem ter configurações correspondentes para estabelecer uma conexão funcional e segura.