EXERCÍCIOS DE APLICAÇÃO

IP Security (IPSEc)

É um standard da IETF que permite encriptar comunicações. É um conjunto de protocolos que garantem a a confidencialidade e integridade dos dados e a autenticação. Uma Virtual Private network (VPN) pode ser definida como um túnel seguro sobre um caminho não protegido ou inseguro.

O IPSEC acabo por ser ideal para criar VPN sobre a internet ou outras redes inseguras, o que faz com que o IPSEC seja usado em muitos tipos de VPN

- **ESP (Encapsulating Security Payload):** Um dos dois principais protocolos que fazem parte do IPSEC. Este protocolo proporciona integridade, autenticação e confidencialidade. O ESP é usado para encriptar os dados transportados no cabeçalho IP.
- **AH (Authentication Header):** Este é o segundo dos principais protocolos do IPSEC, proporciona integridade, autenticação e deteção de repetição de dados. Não proporciona encriptação, pode funcionar como uma assinatura digital de forma a ser possível detetar a alteração de dados.
- **Internet Key Exchange (IKE):** Este é o mecanismo usado pela VPN para a troca de chaves de encriptação e autenticação IPSEC e a negociação de parâmetros de segurança do IPSEC, conhecido nos dispositivos Cisco entre outros como ISAKMP.
- **DES, 3DES, AES:** São protocolos de encriptação que equipamentos Cisco suportam, o DES é o mais fraco dos 3 suporta chaves de encriptação de 56bits, o 3DES usa encriptação de 168 bits e por fim o AES que suporta chaves de 129,192 ou 256bits.
- **Diffie-Hellman Group (DH):** é o protocolo de criptografia da chave pública que o protocolo IKE usa para estabelecer as sessões
- **MD5, SHA-1:** são algoritmos de HASH utilizados para autenticar os dados transmitidos, o protocol SHA é mais forte que o MD5.
- **Security Association (SA):** A SA representa a ligação entre dois pontos (peers) IPSEC. Cada peer mantem uma base de dados em memória com todos os parâmetros da ligação.

Funcionamento do IPSEC

Existem 5 passos principais no IPSEC:

1. Tráfego interessante: O IPSEC deve reconhecer o trafego a proteger usando listas de acesso (access lists).
2. Fase 1 (ISAKMP / IKEv1): Os dispositivos IPSEC negoceiam as políticas de segurança e estabelecem os canais de seguro de comunicação.
3. Fase 2 (IPSEc): Os dispositivos IPSEC negoceiam as políticas de segurança para a proteção de dados

4. Transferência de dados: A transferência de dados seguros entre peers IPSEC baseados nos parâmetros e chaves negociadas previamente.

5. Terminar Túnel IPSEc: O túnel termina quando a duração temporal terminar ou quando atingir um determinado volume de dados.