PROTOCOLOS DE SEGURANÇA

Raissa Sabino de Gouveia

Localizado na camada TCP/IP, a principal finalidade do protocolo TLS é garantir a segurança e a privacidade dos dados na internet.

Principais objetivos:

1. Segurança com criptografia
2. Interoperabilidade
3. Extensibilidade
4. Eficiência Relativa

Composto por duas camadas:

- Protocolo de Registro que efetua as operações necessárias para garantir a segurança da conexão .

- Protocolo de Handshaking que realiza a negociação de parâmetros de segurança.

Funcionamento do Protocolo de Registro

- Recebe as mensagens para serem transmitidas

1. Fragmenta os dados em blocos
2. Realiza a compressão dos dados
3. Aplica o MAC
4. Encripta e transmite o resultado

- Dados recebidos

1. Realiza a decriptação
2. Verificação da integridade
3. Realiza descompressão
4. Reagrupa os blocos e os entrega para as camadas superiores.

Responsibiladades do Handshaking

Identificador da sessão

Uma seqüência de bytes escolhida pelo servidor para identificar uma sessão ativa ou uma sessão reiniciável.

Método de compressão

Qual o método de compressão que será utilizada antes da criptografia dos dados.

Cipher Spec

Especifica qual o algoritmo de criptografia vai ser utilizado, qual algoritmo de MAC e define alguns atributos criptográficos.

Chave mestre

Chave secreta de 48 bytes que será compartilhada entre o cliente e o servidor

Is Resumable

Flag que indica se a sessão pode ser utilizada para iniciar novas conexões.

O IPsec foi desenvolvido para fornecer segurança na camada IP por meio de autenticação e criptografia de pacotes de rede IP.

Principais protocolos:

- Authentication Header (AH) que fornece integridade de dados e sérvios anti-replay.
- Encapsulating Security Payload (ESP) que criptografa e autentica os dados.
- IKE que é usado para gerar chaves de segurança compartilhadas para estabelecer uma associação de segurança (SA)
- ISAKMP É uma estrutura para estabelecimento de chave, autenticação e negociação de uma SA para uma troca segura de pacotes na camada IP

Funcionamento IPsec

5 principais etapas

1- Reconhecimento do anfitrião

Sistema host reconhece que um pacote precisa de proteção e e acionam as políticas de segurança. Para pacotes de saída, a criptografia e a autenticação apropriadas são aplicadas. Quando um pacote recebido o sistema host verifica se ele foi criptografado e autenticado corretamente.

2- Negociação ou IKE - Fase 1

Os hots se autenticam entre si e configuram um canal seguro entre eles que é usado para negociar a forma como o circuito IPsec irá criptografar ou autenticar os dados enviados por ele.

3-Circuito do IPsec ou IKE - Fase 2

Configura um circuito IPsec pelo canal seguro estabelecido na IKE Fase 1

4- Transmissão

Os hosts trocam os dados reais pelo túnel seguro que estabeleceram. As SAs IPsec configuradas anteriormente são usadas para criptografar e descriptografar os pacotes.

5- Terminação do IPsec

O túnel IPsec é encerrado. isso acontece depois que um número de bytes especificado anteriormente passa pelo túnel IPsec ou a sessão atinge o tempo limite. Quando um desses eventos acontece, os hosts se comunicam e ocorre o encerramento.