SEGURANÇA DE IP

O QUE É UM IP?

IP vem do inglês e significa Internet Protocol (Protocolo de rede), é ele quem identifica um determinado dispositivo para que não haja conflitos na rede, servindo como uma espécie de código de endereço único para cada host, ele é representado no geral por número decimal, e em certos países de forma hexadecimal.

SEGURANÇA DA INFORMAÇÃO

Se trata basicamente de um conjunto de regras para proteção dos dados do usuário presentes na internet, tendo este, 4 pilares principais: confidencialidade, integridade, disponibilidade, autenticidade

O QUE É O IPSEC

É uma tecnologia de segurança padrão aberta, desenvolvida pelo Internet Engineering Task Force (IETF), utilizada pelo sistema operacional, fornecendo proteção baseada em criptografia de todos os dados na camada IP da pilha de comunicações.

RESUMO DE FUNCIONAMENTO DO IPEC

1. O dispositivo emissor avalia se há necessidade de usar o IPSec;
2. O dispositivo emissor e o destinatário negociam quais são os requisitos de segurança;
3. O host envia e recebe dados criptografados, validando sua autenticidade;
4. Quando a transmissão for concluída ou a sessão tiver expirado, o computador encerrará a conexão de IPSec.

QUAL O TIPO DE CRIPTOGRAFIA DOIPSEC

A encriptação assimétrica e simétrica. Na encriptação assimétrica, a chave de encriptação é tornada pública enquanto a chave de desencriptação é mantida privada. A encriptação simétrica, usa a mesma chave pública para criptografar e descriptografar dados.

TÉCNICAS DE CRIPTOGRÁFICAS DO IPSEC

V3 - O processo pelo qual a identidade de um host ou terminal é verificada

Verificação de integridade -O processo que assegura que nenhuma modificação tenha sido feita nos dados enquanto em trânsito em toda a rede

Criptografia - O processo que assegura a privacidade, "ocultando" dados e endereços IP privados enquanto em trânsito em toda a rede

Fontes: https://www.ibm.com/docs/pt-br/aix/7.3?topic=overview-ip-security-operating-system
https://aws.amazon.com/pt/what-is/ipsec/#:~:text=O%20IPSec%20%C3%A9%20um%20conjunto,esse%20protocolo%20ainda%20mais%20seguro.