# Lista de Exercícios: IPSec

Prof. Gabriel Rodrigues Caldas de Aquino

Compilado em:
June 5, 2026

## 1 Tomada de Decisão sobre o fluxo do tráfego IPSec e fluxo comum

Um roteador de borda em uma Matriz possui uma VPN IPsec configurada para se comunicar com uma Filial. Um funcionário na Matriz realiza duas tarefas simultaneamente: "Envia um relatório confidencial para o servidor da Filial, que vai por dentro de um túnel IPSec e acessa a Internet pública".

1. Descreva o que é uma **Associação de Segurança (SA)**, sua característica e como é feito para gerenciar uma comunicação bidirecional.
2. Explique o que é a **SPD** (Security Policy Database).
3. Explique o que é a **SAD** (Security Association Database).
4. Explique como o roteador utiliza a **SAD** e a **SPD** no cenário acima. Descreva o que acontece com cada pacote ao entrar na Internet pública.

## 2 Protocolos e Modos de Operação IPSec

O IPSec define dois protocolos principais para fornecer serviços de segurança: o AH e o ESP. Esses protocolos podem ser usados em dois modos: Transporte ou Túnel.

1. Quais são os dois protocolos de segurança que fazem parte do IPSec e quais os serviços de segurança (Confidencialidade, Integridade e/ou Autenticidade) cada um é capaz de fornecer?
2. Descreva brevemente o que é o **AH** (Authentication Header) e como ele é aplicado a um pacote IP, indicando quais campos ele autentica.
3. Descreva brevemente o que é o **ESP** (Encapsulating Security Payload) e como ele é aplicado a um pacote IP, indicando quais serviços de segurança ele tipicamente fornece.

4. Explique a diferença entre o **Modo Transporte** e o **Modo Túnel** do IPSec.

5. No cenário da VPN entre Matriz e Filial, qual modo de operação (Transporte ou Túnel) é tipicamente utilizado e por quê?

# 3 Parâmetros da SA

As SADs são fundamentais para que sejam mantidas as SAs. Para isso, é necessário que dois roteadores, que estejam com uma SA entre eles, mantenham os parâmetros da SAD. Para fazer isso, é possível que sejam configurados manualmente os parâmetros da SAD em cada um, ou é possível que seja executado o IKE.

1. Explique brevemente qual é o objetivo do **IKE** (Internet Key Exchange).

2. Dado o objetivo do IKE, diga quais são as **3 responsabilidades** do IKE.

3. O IKE define uma **IKE SA**. Qual é o objetivo da IKE SA e como ela difere da SA do IPSec?

4. O IKE possui **duas fases**, quais são essas fases e qual o motivo de existirem duas fases?

5. Explique a necessidade do **Diffie-Hellman** e como os conceitos de chave pública e privada são úteis nesse cenário.

6. Explique como que é possível resistir a ataques **man-in-the-middle** (MITM) nesse cenário.

7. Considerando o custo computacional da **criptografia simétrica e assimétrica**, relacione com as fases do IPSec SA e IKE SA.

# 4 Transformação e Controle de Pacotes IPSec

**Como o pacote muda ao entrar no IPSec**

1. Explique brevemente o princípio **"Best-Effort"** do protocolo IP.

2. Ao utilizar o protocolo ESP no Modo Túnel, o pacote sofre encapsulamento e criptografia.

   (a) Explique a necessidade do campo Padding (Enchimento) antes da criptografia.

   (b) Como o campo de próximo protocolo do cabeçalho IP externo indica o IPSec?

3. Diferencie o tratamento de pacotes entre o protocolo **IP** (Best-Effort) e o IPSec. Especifique como o IPSec utiliza a **Associação de Segurança (SA)** contida na **SAD** para introduzir controle e mecanismos de segurança.

4. No contexto da SAD, explique a função do campo **Sequence Number** (Número de Sequência) e do **Sequence Number Overflow** (Número de Sequência Estourado) e como eles se relacionam com a resistência a ataques de **replay**.

# 5 O Papel do HMAC

O IPSec, através dos seus protocolos (AH e ESP), garante a integridade e autenticidade dos pacotes de dados. O mecanismo mais comum e robusto utilizado para atingir esse objetivo é o HMAC (Hashed Message Authentication Code).

1. Defina o que é o **HMAC** e qual é o seu principal objetivo em um protocolo de segurança como o IPSec.

2. Descreva o que é **Integridade de Dados** e **Autenticidade de Dados** e explique qual dos dois serviços o HMAC garante.

3. No contexto do protocolo **ESP**, onde o HMAC é tipicamente inserido e qual parte do pacote ele cobre?