Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Técnicas de Defesa
(VPN - Rede Privada Virtual e IPSec)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Pergunta???

O que é Rede Privada?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Conceitos

Rede Privada

É uma rede de comunicação desenvolvida para uso interno em uma organização. Ela possibilita o acesso a recursos compartilhados e, ao mesmo tempo, fornece privacidade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Conceitos

Intranet

É uma rede privada (LAN) que usa o modelo Internet. Entretanto, o acesso à rede é limitado aos usuários dentro da organização. A rede usa programas de aplicação definidos para a Internet global, como HTTP, e pode ter servidores de impressão e servidores de arquivos Web.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Pergunta???

Quais as faixas de endereçamento IP podemos utilizar numa intranet?

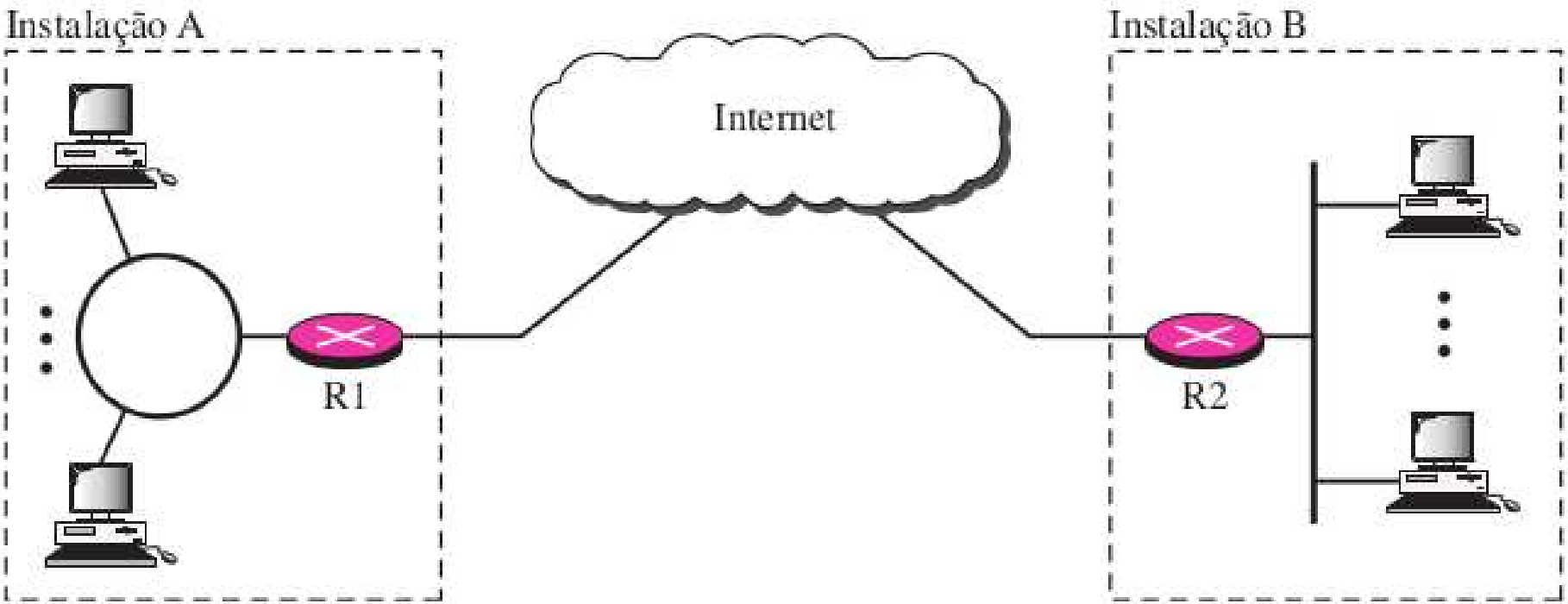
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Endereçamento LAN

Prefixo	Intervalo	Total
10/8	10.0.0.0 a 10.255.255.255	2^{24}
172.16/12	172.16.0.0 a 172.31.255.255	2^{20}
192.168/16	192.168.0.0 a 192.168.255.255	2^{16}

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Se uma organização deseja interligar várias instalações em locais diferentes, ele poderá usar a Internet. Mas como garantir a privacidade na troca de dados?



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

VPN

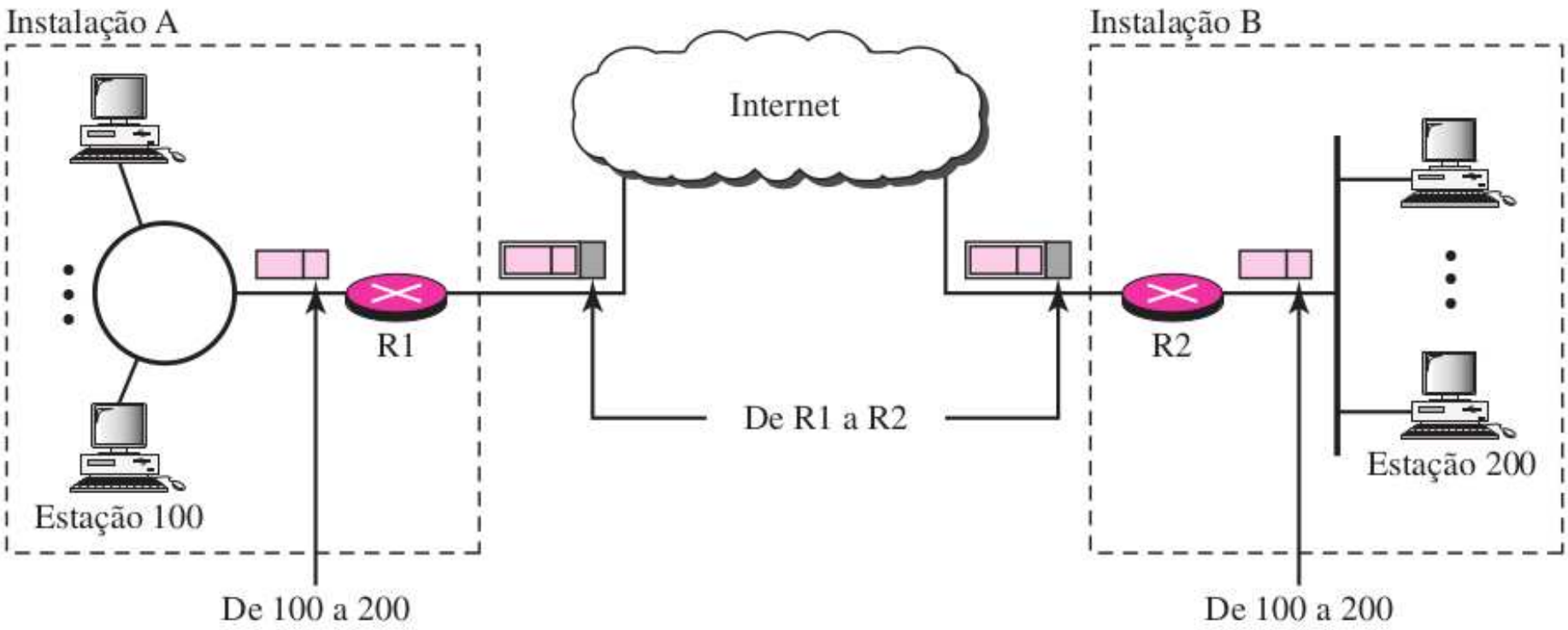
A VPN cria uma rede que é privada, mas virtual. É privada, pois garante sigilo dentro da organização. E é virtual, porque não usa enlaces privadas reais. A tecnologia VPN usa IPSec no modo túnel para fornecer autenticação, integridade e privacidade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

VPN

No modo IPSec túnel, cada datagrama IP destinado ao uso privado na organização é encapsulado em outro datagrama. Para empregar IPSec no tunelamento, as VPNs precisam usar dois conjuntos de endereçamento.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE



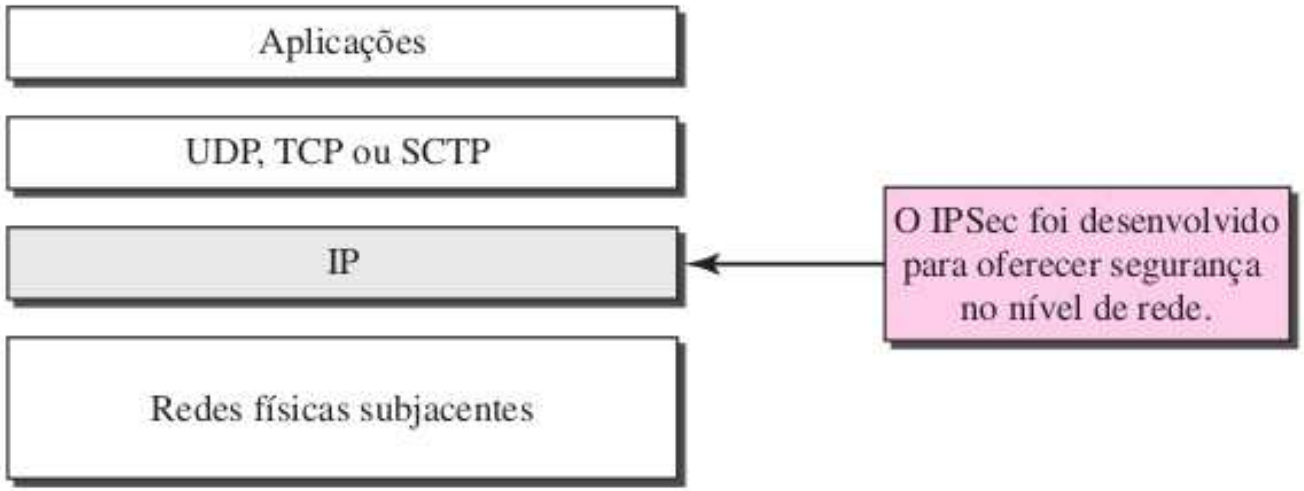
O datagrama IP normal é encapsulado em um datagrama IPSec no roteador R1. Na Internet os equipamentos não conseguem decifrar o conteúdo do pacote nem os endereços de origem e de destino. A decriptação ocorre em R2, que localiza o endereço de destino do pacote e o entrega.

Pergunta???

O que é IPSec?

IPSec

IPSecurity (IPSec) é um conjunto de protocolos desenvolvido para oferecer segurança (confidencialidade e autenticidade) para um pacote no nível de rede.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec

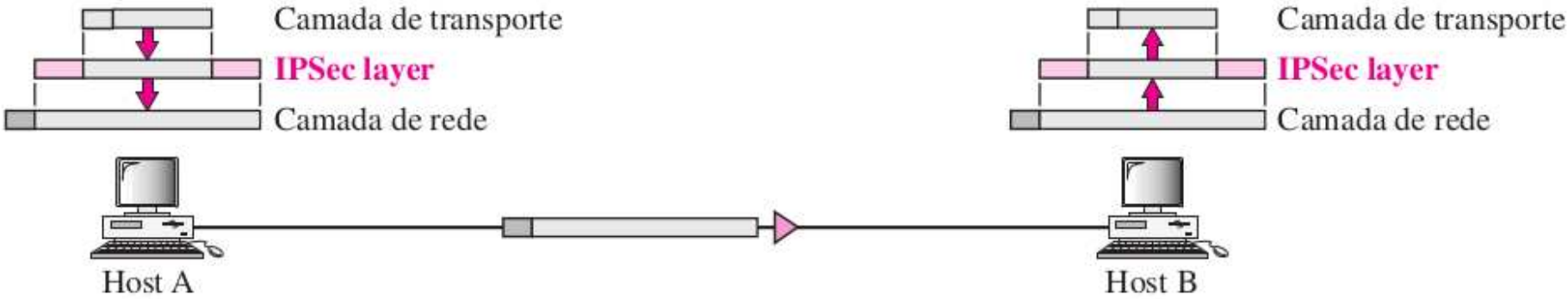
O IPSec opera em um de dois modos distintos:

- Transporte: não protege o pacote IP inteiro, protege apenas as informações da camada de transporte (ou seja, o payload da camada IP). O cabeçalho IPSec são acrescentados às informações provenientes da camada de transporte e o cabeçalho IP é adicionado posteriormente.
- Túnel: protege o pacote IP inteiro. Ele pega um pacote IP, inclusive o cabeçalho, aplica os métodos de segurança a todo o pacote e, em seguida, acrescenta um novo cabeçalho IP. O novo cabeçalho IP, como veremos em breve, tem informações distintas do cabeçalho IP original.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - Transporte

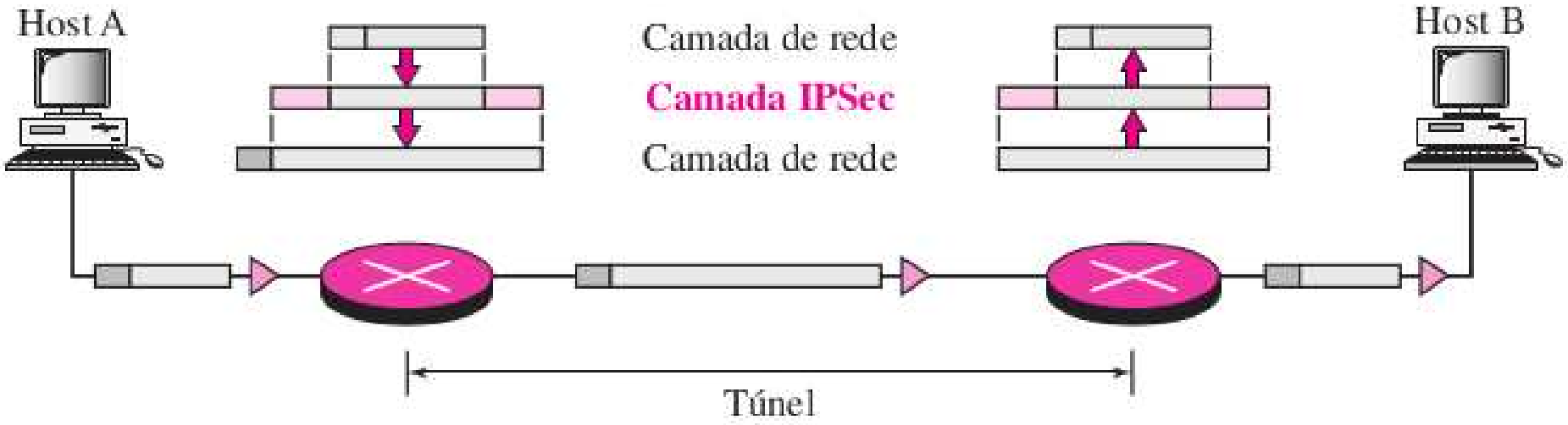
Normalmente, o modo de transporte é usado quando precisamos de proteção de dados fim a fim (*host* a *host*). O *host* emissor usa o IPSec para autenticar e/ou criptografar os dados da camada de transporte. O *host* receptor usa IPSec para verificar a autenticação e/ou decriptografar o pacote e entregá-lo à camada de transporte.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - Túnel

Normalmente, o modo túnel é usado entre dois roteadores ou entre um *host* e um roteador.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - Túnel

O IPSec define dois protocolos:

- O protocolo AH (Authentication Header - cabeçalho de autenticação) ;
- O protocolo ESP (Encapsulating Security Payload - payload de segurança de encapsulamento).

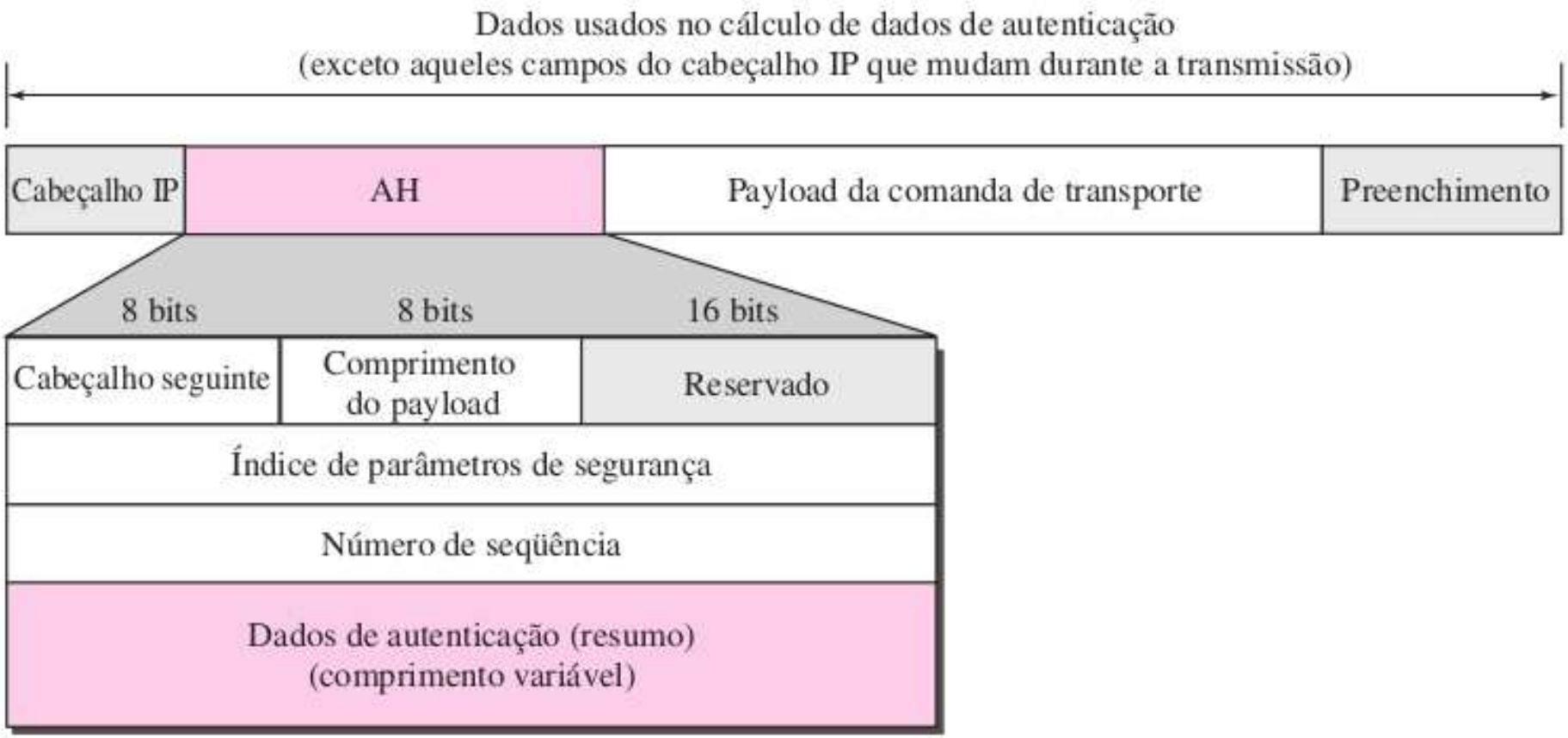
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - AH

O protocolo AH foi desenvolvido para autenticar o host de origem e para garantir a integridade dos dados. O protocolo usa uma função hash e uma chave simétrica para criar um resumo de mensagem (chamado de HMAC). Pode usar qualquer função hash padrão sem chaves, como o SHA-1, e acrescentar a chave na mensagem antes de realizar os cálculos. O resumo (mensagem + chave) é inserido no cabeçalho de autenticação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - AH



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

IPSec - AH

- Cabeçalho seguinte: define o tipo de payload transportado pelo datagrama IP (como TCP, UDP, ICMP ou OSPF). Ele tem o mesmo valor do campo de protocolo no cabeçalho IP antes do encapsulamento. Em outras palavras, o processo copia o valor do campo de protocolo no datagrama IP para esse campo. O valor do campo de protocolo no novo datagrama IP agora é configurado para 51 para mostrar que o pacote carrega um cabeçalho de autenticação.
- Comprimento do Payload: define o comprimento do cabeçalho de autenticação em múltiplos de 4 bytes. Ele, porém, não inclui os 8 primeiros bytes.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - AH

- Índice de parâmetros de segurança: identifica o circuitos virtuais que é o mesmo para todos os pacotes enviados durante uma conexão chamada associação de segurança. Esse parâmetro, em conjunto com o endereço de destino (de saída) ou endereço de origem (de entrada) e o protocolo (AH ou ESP), define uma associação de forma exclusiva.
- Número de sequência: fornece informações de ordenação para uma sequência de datagramas. Ele não é repetido nem mesmo se um pacote for retransmitido. Um número de sequência não repete um ciclo após atingir 2^{32}, deve ser estabelecida uma nova conexão. Impede-se o ataque de reprodução.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - AH

- Dados de Autenticação: é o resultado da aplicação de uma função hash a todo o datagrama IP, exceto para os campos que são modificados em trânsito (O campo TTL). Ele fornece autenticação de fonte e integridade de dados, mas não privacidade.

Podem ser acrescentados bits de preenchimento para tornar par o comprimento total, dependendo do algoritmo de hashing.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

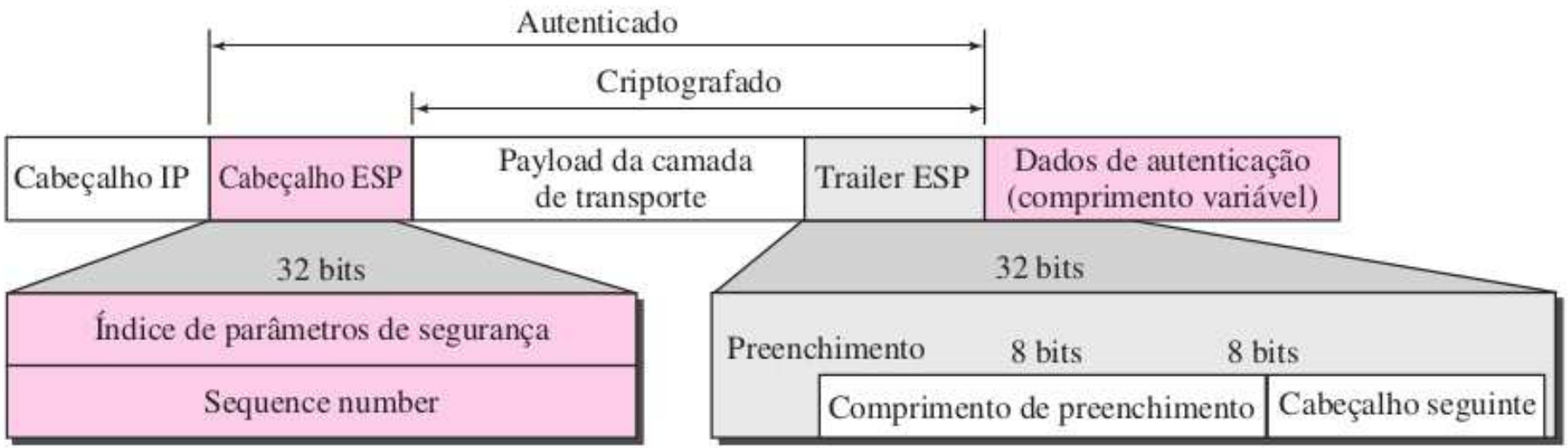
IPSec - ESP

O IPSec definiu, posteriormente, um protocolo alternativo que oferecer recursos de autenticação de fonte, integridade e privacidade, denominado ESP (payload de segurança de encapsulamento).

Quando um datagrama IP transporta trailer e cabeçalho ESP, o valor do campo de protocolo no cabeçalho IP é 50.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - ESP



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - ESP

- Índice de parâmetros de segurança: identifica o circuitos virtuais que é o mesmo para todos os pacotes enviados durante uma conexão chamada associação de segurança. Esse parâmetro, em conjunto com o endereço de destino (de saída) ou endereço de origem (de entrada) e o protocolo (AH ou ESP), define uma associação de forma exclusiva.
- Número de sequência: fornece informações de ordenação para uma sequência de datagramas. Ele não é repetido nem mesmo se um pacote for retransmitido. Um número de sequência não repete um ciclo após atingir 2^{32}, deve ser estabelecida uma nova conexão. Impede-se o ataque de reprodução.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - ESP

- Comprimento de preenchimento: define o número de bytes de preenchimento. O preenchimento poderá ser de até 255 bytes, formado por 0s.
- Cabeçalho seguinte: é similar àquele definido no protocolo AH. Ele atende ao mesmo objetivo do campo de protocolo no cabeçalho IP antes do encapsulamento.
- Autenticação de dados: é o resultado da aplicação de autenticação. No AH, parte do cabeçalho IP é inclusa no cálculo dos dados de autenticação; no ESP, ele não é.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - ESP

O procedimento ESP segue as etapas:

01. É acrescentado um trailer ESP (preenchimento, comprimento de preenchimento e cabeçalho seguinte).
02. O payload e o trailer são criptografados.
03. É adicionado o cabeçalho ESP.
04. O cabeçalho ESP, o payload e o trailer ESP são usados para criar os dados de autenticação.
05. Os dados de autenticação são acrescentados no final do trailer ESP.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - ESP

O protocolo ESP foi desenvolvido após o protocolo AH estar em uso. O ESP faz tudo que o AH faz, além de ter outras funcionalidades (privacidade).

Por que precisamos do AH?

Não precisamos realmente. Entretanto, a implementação do AH já está inclusa em alguns produtos comerciais, o que significa que ele permanecerá como parte da Internet até que esses produtos saiam de linha.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - Associação de Segurança

O protocolo IPSec precisa de um conjunto de parâmetros de segurança antes da comunicação se tornar possível. Dessa forma, um conjunto de parâmetros de segurança é estabelecido entre um emissor e determinado receptor na primeira vez que o emissor tiver um datagrama a ser enviado. Esse conjunto pode ser salvo para transmissão futura de pacotes IP para o mesmo receptor.

Podemos dizer que, quando o transmissor e receptor chegam a um acordo sobre um conjunto de parâmetros de segurança entre ambos, estabeleceram uma conexão lógica entre si (denominada associação).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

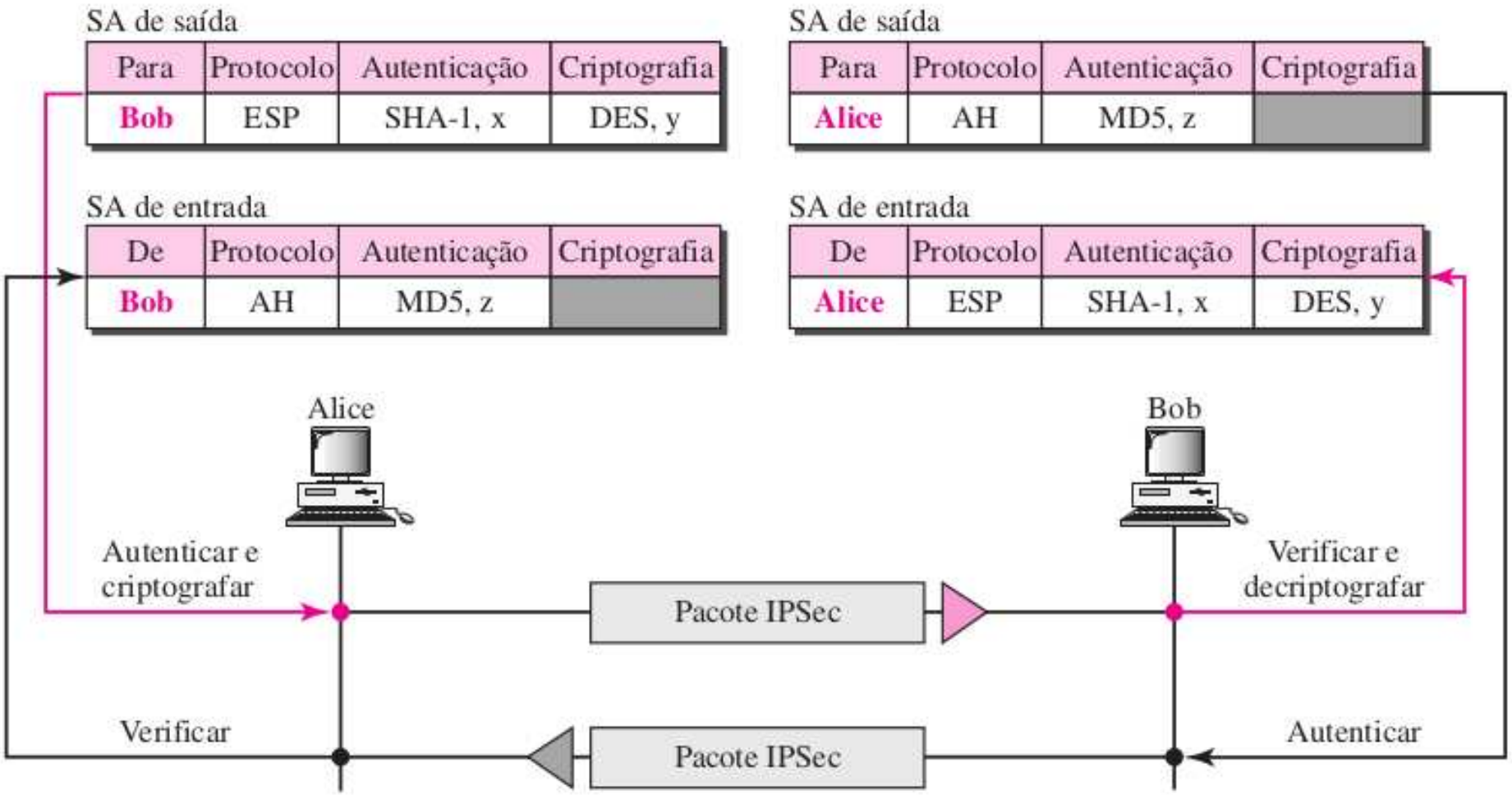
IPSec - Associação de Segurança

O IPSec transforma um protocolo sem o estabelecimento de conexão (o IP) em um protocolo orientado a conexão (IPSec).

Cada entidade necessita ter tanto SAs (Associação de segurança) de entrada quanto de saída para possibilitar uma comunicação bidirecional.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IPSec - Associação de Segurança



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE