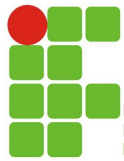
Segurança de Redes

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

Aula 10
IPSec, SSL/TLS e VPN



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

"A felicidade depende das qualidades próprias do indivíduo e não do estado material do meio em que se acha."
(Allan Kardec)

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

O que Aprenderemos?

- Entender a finalidade e a importância das VPN;
- Aprender como as VPNs podem ser implementadas;
- Conhecer o IPSec;
- Compreender os protocolos SSL/TLS;
- Conhecer algumas implementações de VPNs.

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

IPSec

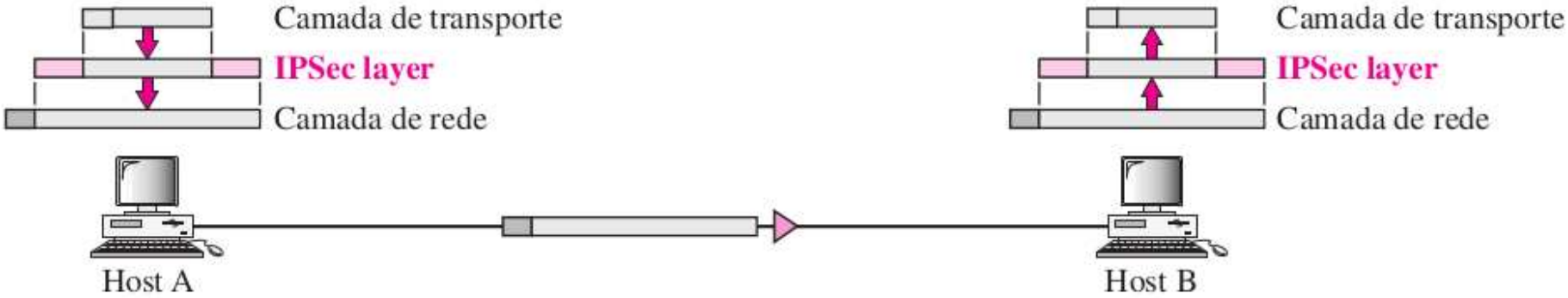
O IPSecurity (IPSec) é um conjunto de protocolos desenvolvido para oferecer segurança para um pacote no nível de rede, criando mensagens confidenciais e autenticados para a camada IP. O IPSec opera em um de dois modos distintos:

- Transporte: oferece proteção principalmente para os protocolos das camadas superiores (transporte), criptografando todo o payload do pacote IP. Nele, o cabeçalho IPSec é acrescentado com as informações da camada de transporte, e o cabeçalho IP é adicionado posteriormente.
- Túnel: oferece proteção a todo pacote IP. 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 tem informações distintas do cabeçalho IP original.

EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

IPSec - Modo Transporte

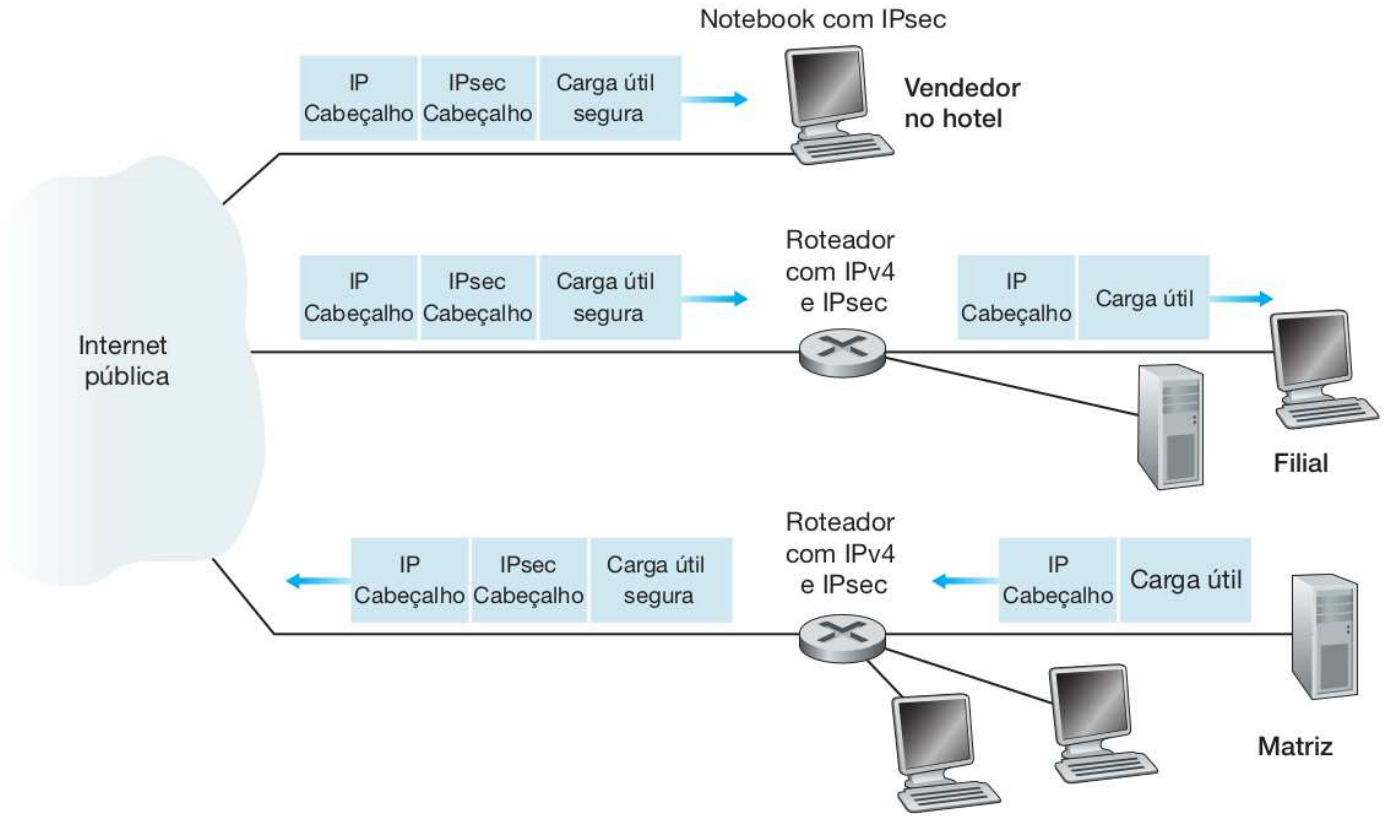
Normalmente, o modo de transporte é usado quando precisamos de proteção de dados fim a fim (host a host), por exemplo em redes distintas. O host emissor usa o IPSec para autenticar e/ou criptografar o payload entregue pela camada de transporte. O host receptor usa IPSec para verificar a autenticação e/ou decriptografar o pacote IP e entregá-lo à camada de transporte.



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

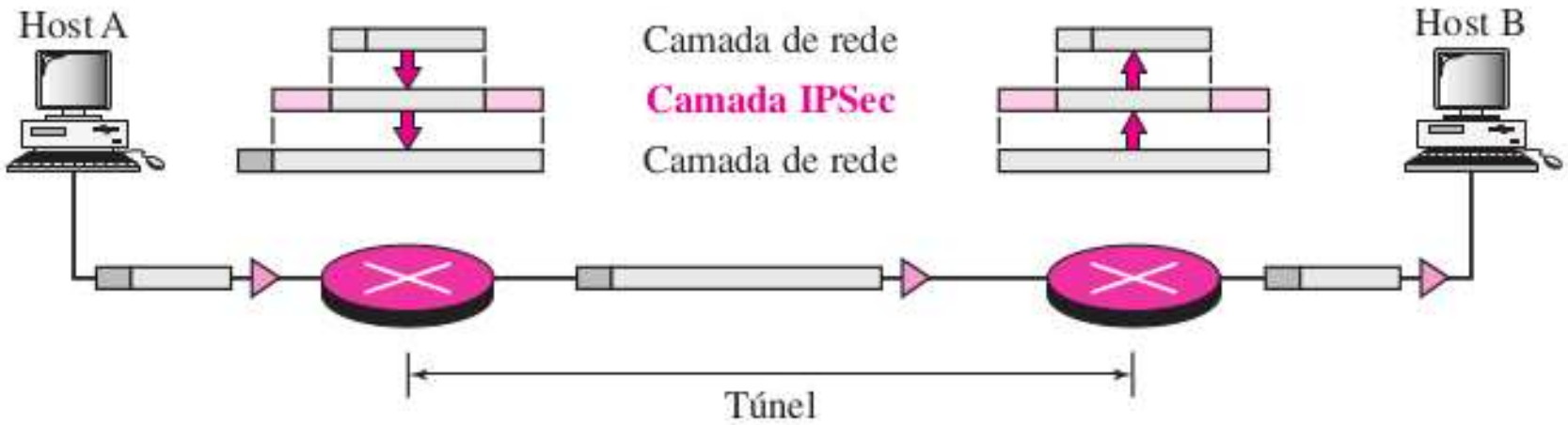
IPSec - Modo Transporte

Quando os equipamentos já tem suporte a IPsec, a informação segura vem até ele, caso contrário os roteadores de borda, fazem a verificação/decriptografia e encaminham ao equipamento final.



IPSec - Modo Túnel

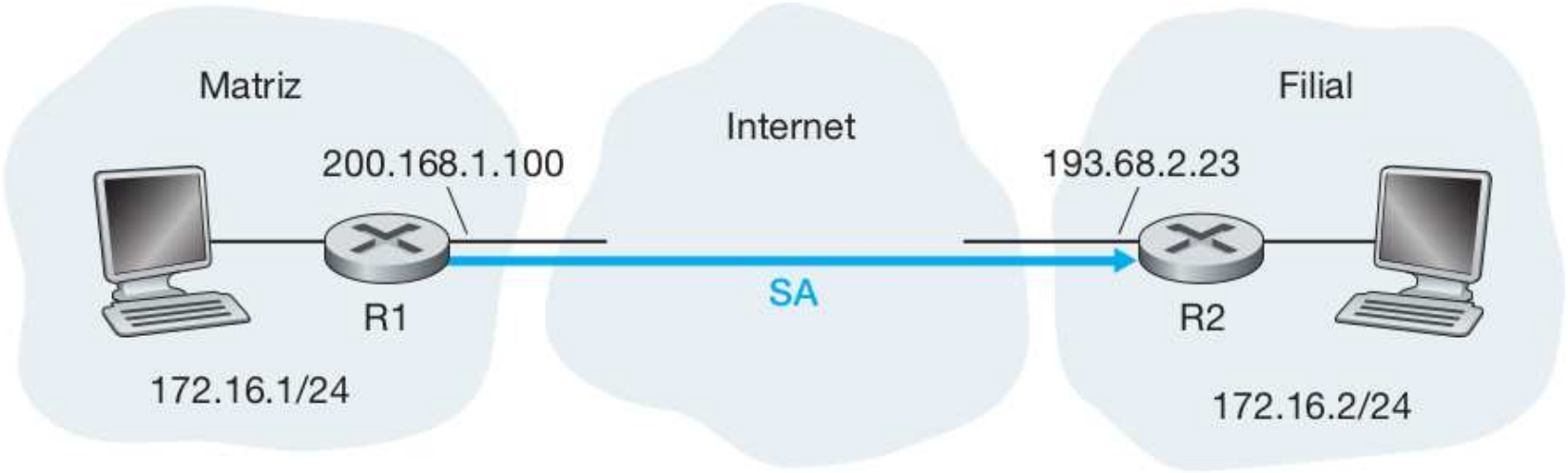
Em geral, o modo túnel é usado entre dois roteadores, entre um host e um roteador ou entre um roteador e um host. Em outras palavras, usamos o modo túnel quando o emissor ou o receptor não for um host.



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

IPSec - Modo Túnel

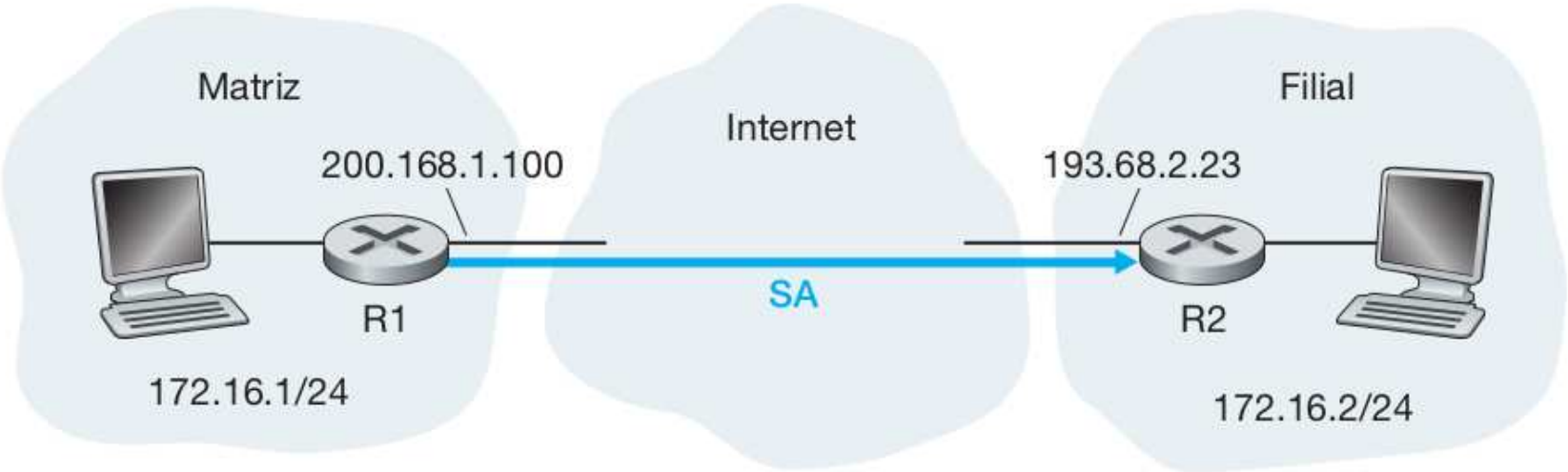
Por exemplo, considere uma comunicação utilizando a Internet com IPsec modo túnel sendo realizado entre roteadores de borda. Neste caso, o datagrama IP original possuia o endereço IP remetente 172.16.1.17 e o endereço IP destinatário 172.16.2.48, e é trocado pelos endereços das interfaces do roteador remetente e destinatário nas duas extremidades dos túneis, isto é, 200.168.1.100 e 193.68.2.23.



IPSec - Modo Túnel

Após R1 enviar um datagrama IPsec à Internet pública, ele passará por diversos roteadores antes de chegar ao R2. Cada um desses roteadores processará o datagrama como se fosse um datagrama comum.

Caso um cliente deseje acessar ao servidor Web (como Amazon ou Google) na Internet pública, o roteador de borda emitirão na Internet tanto datagramas IPv4 comuns como datagramas IPsec seguros.



IPSec – Protocolos

O IPSec define dois protocolos:

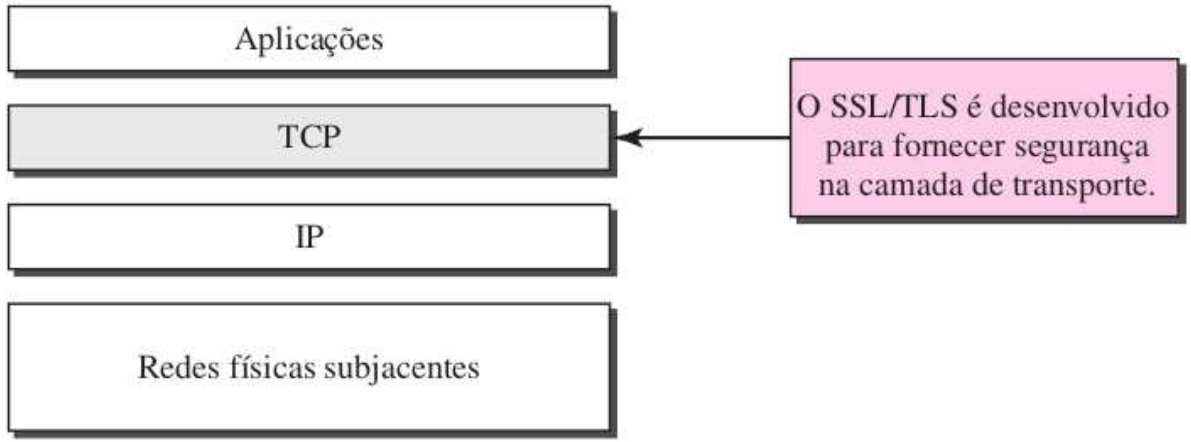
- O protocolo AH (*Authentication Header*): permite a autenticação e a integridade dos dados utilizando a função hash e uma chave simétrica para criar um resumo de mensagem autenticada (HMAC). Ele não garante a privacidade;
- O protocolo ESP (*Encapsulating Security Payload*): implementa autenticação, integridade e privacidade dos dados. O protocolo ESP foi desenvolvido após o protocolo AH acrescentando novas funcionalidades, por exemplo, criptografia simétrica. Ele é muito mais utilizado do que o protocolo AH.

No IPv6 o AH e o ESP fazem parte do cabeçalho de extensão.

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

SSL/TLS

O IPSec opera na camada de rede. Para oferecer segurança na camada de transporte foi desenvolvido o protocolo SSL (*Secure Sockets Layer*) e o protocolo TLS (*Transport Layer Security*). Eles são projetados para utilizar com o TCP para oferecer um serviço seguro confiável de ponta a ponta. Desta forma, é possível estabelecer comunicações seguras na Internet para atividades como navegação na Web, e-mail, mensagens instantâneas e outras transferências de dados.



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

SSL/TLS

O uso mais comum e conhecido de SSL /TLS é uma navegação segura na web através do protocolo HTTPS. Um site HTTPS público devidamente configurado inclui um SSL /TLS certificado assinado por uma autoridade de certificação pública. Os usuários que visitam um site HTTPS podem ter certeza de:

- Autenticidade: O servidor que apresenta o certificado está na posse da chave privada que corresponde à chave pública no certificado.
- Integridade: assinado pelo certificado (por exemplo, páginas da web) não foram alteradas em trânsito.
- Criptografia: as comunicações entre o cliente e o servidor são criptografadas.

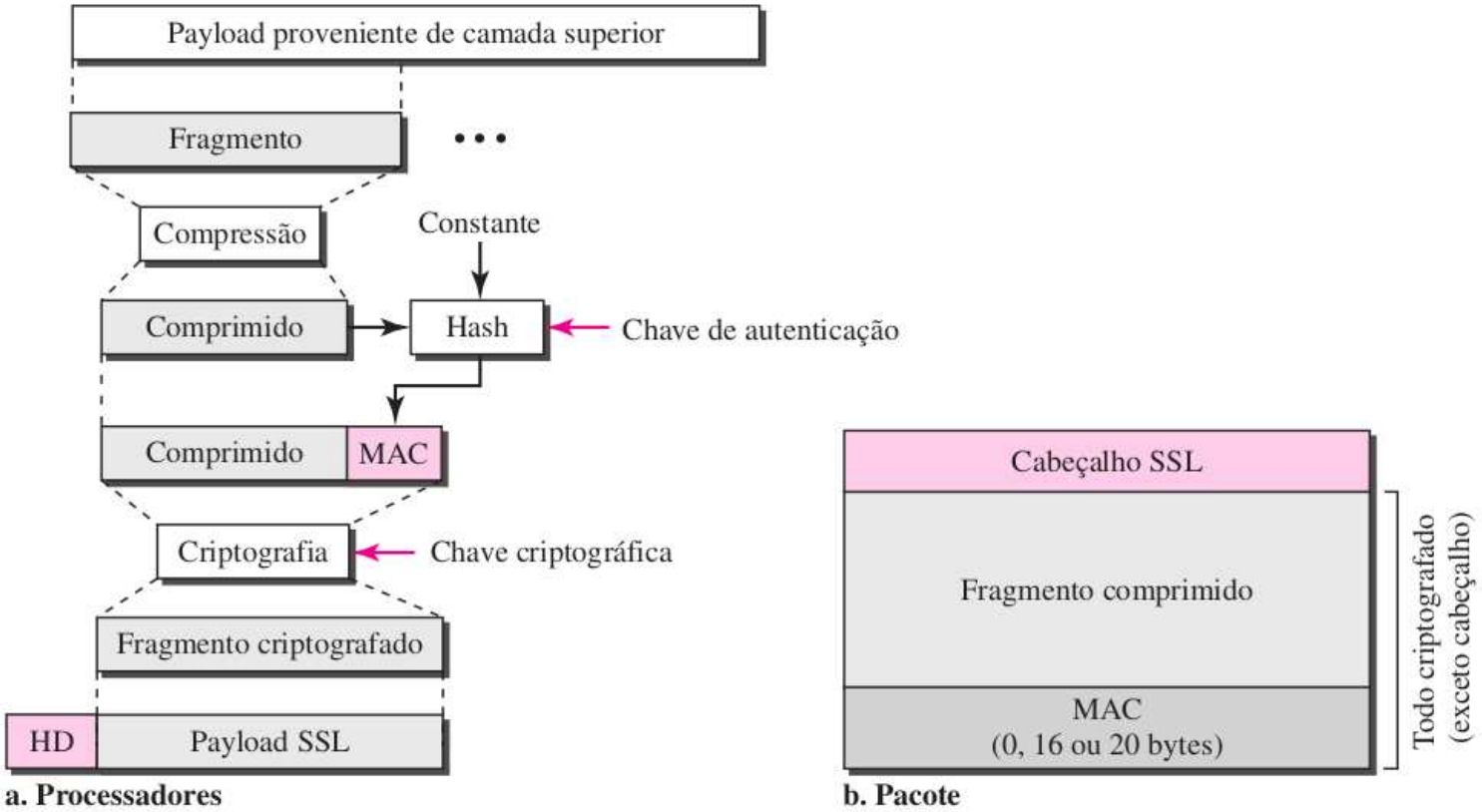
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

SSL (*Secure Sockets Layer*)

O SSL foi desenvolvido para oferecer serviços de segurança e de compressão de dados na camada de transporte. Os dados recebidos da aplicação são comprimidos (serviço opcional), calculado o Hash e critografado. O SSL usa uma função hash (por exemplo, SHA) com segredo (MAC) visando preservar a integridade e autenticação dos dados. Para oferecer confidencialidade, os dados originais e o MAC são criptografados utilizando-se criptografia de chave simétrica (por exemplo, 3DES, AES, RC4). O estabelecimento das chaves simétricas é feita com o auxílio de criptografia de chave pública.

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

SSL – Funcionamento



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

SSL – Funcionamento

A primeira etapa é a fragmentação. Cada mensagem de camada superior é fragmentada em blocos de até 2^{14} bytes. Em seguida, a compactação é, opcionalmente, aplicada. No SSLv3 (além da versão atual do TLS), nenhum algoritmo de compactação é especificado, de modo que o algoritmo de compactação default é nulo.

Na sequência, é calculado um código de autenticação de mensagem. Para essa finalidade, é usada uma chave secreta compartilhada. É utilizado como algoritmo de hash criptográfico SHA.

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

SSL – Funcionamento

Em seguida, a mensagem compactada mais o MAC são encriptados usando a encriptação simétrica. Os algoritmos utilizados são:

Cifra de bloco		Cifra de fluxo	
Algoritmo	**Tamanho da chave**	**Algoritmo**	**Tamanho da chave**
AES	128, 256	RC4-40	40
IDEA	128	RC4-128	128
RC2-40	40		
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

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

SSL – Protocolo de Handshake

Esse protocolo permite que o servidor e o cliente autentiquem um ao outro e negociem um algoritmo de encriptação e MAC, e chaves criptográficas a serem usadas para proteger dados enviados em um registro SSL.

1. O cliente inicializa a conexão lógica e estabelecer as capacidades de segurança que serão associadas a ela (a versão de SSL, algortimos de criptografias, compactação e hash possíveis).
2. O servidor responde a cliente, quais dos parâmetros foram selecionados pelo servidor a partir daqueles propostos pelo cliente. Além disso, o servidor especifica como será a troca de chaves da sessão (RSA, Diffie-Hellman ou Fortezza);

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

3. O servidor envia seus certificados (padrão X.509) que contém a sua chave pública RSA ou com parâmetros Diffie-Hellman. O servidor pode, opcionalmente exigir o certificado do cliente;
4. O cliente verifica se o servidor forneceu um certificado válido (através de uma Autoridade Certificadora). Se o servidor tiver solicitado um certificado, o cliente deverá enviar uma mensagem de certificado.
5. O cliente gera um segredo aleatório de 48 bytes e o encripta com a chave pública RSA do certificado do servidor. Este segredo será utilizado para gerar a chave de sessão simétrica usado na criptografia entre o cliente e o servidor.
6. O servidor, descriptografar a mensagem e de posse do segredo gera tambémm a chave simétrica, e partir de agora cliente e servidor trocarão mensagens seguramente nesta sessão SSL.

TLS - *Transport Layer Security*

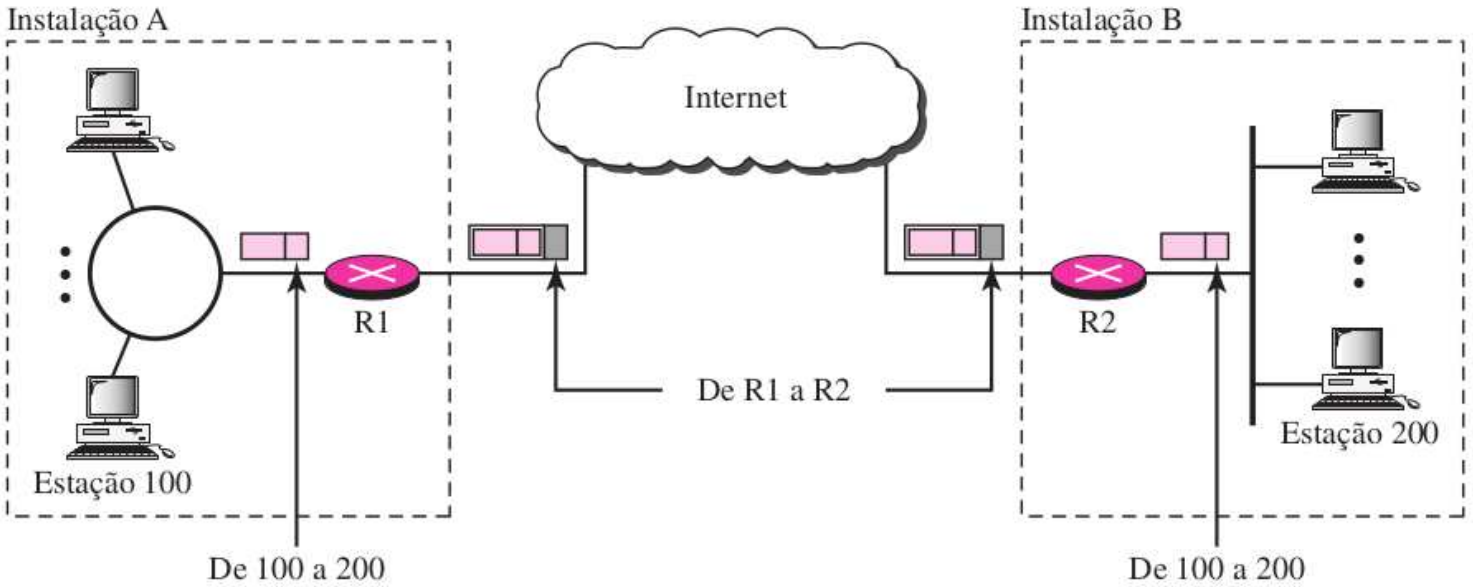
O TLS é uma iniciativa de padronização do IETF cujo objetivo é produzir uma versão padrão do SSL para Internet. TLS é muito semelhante à SSL. Entrentanto, apresentou como diferença:

- Eliminou algumas vulnerabilidades de segurança e algoritmo obsoleto utilizados no SSL (Fortezza);
- Modificou o modo da geração das chaves de sessão;
- Acrescentou novos tipos de certificados digitais e métodos de integridade da mensagem.

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

VPN - *Virtual Private Network*

VPN é uma técnica que possibilita o uso de uma rede pública como a internet (meio inseguro) para transportar dados de modo seguro e sigiloso. Ela possui como objetivo garantir: a confidencialidade e integridade dos dados, não repúdio do emissor e autenticação da mensagem.



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

VPN

A VPN pode ser implementada por várias tecnologias, entre elas temos: PGP, SSL/TLS, SSH, IPSec, L2TP e PPTP. Entretanto, as duas técnicas mais populares de implementação de VPNs são a que utiliza o IPSec e o SSL/TLS.

Nas VPNs onde se exige alto volume de transações e baixa latência, é mais indicado o uso do IPSec pois ele apresenta uma maior eficiência. Quando precisamos de segurança apenas em uma aplicação específica é mais indicado as tecnologias SSL/TLS.

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

SSL/TLS – Implementações

Openswan é um exemplo de *software* livre que implementa o VPN com IPSec.

O OpenVPN é um exemplo de *software* livre, que utiliza TLS para criar túneis VPN. VPN com TLS é mais utilizada uma vez que a sua implementação costuma ser mais simples.

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

Dúvidas

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