Segurança na Internet

Roberto Sadao Yokoyama

UTFPR-CP

Setembro, 2016

Aula de hoje: [1]

[1] Slides baseados no material dos livros: Forouzan [1] e Stallings [2]

Introdução

- **Autenticação** de mensagens e **privacidade** aplicados às camadas de rede, de transporte e de aplicação do modelo Internet
  - IPSec
  - SSL (ou TLS)
  - PGP
- No geral são usados: MAC (*Message Authentication Code*) + Criptografia

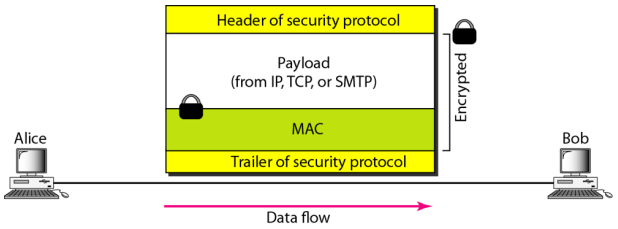


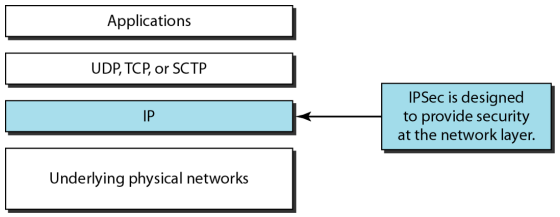
Figura : Estrutura comum dos três protocolos de segurança

IPSec (IPSecurity)

IPSec

é um conjunto de protocolos desenvolvidos pelo IETF para oferecer segurança para um pacote no nível da rede

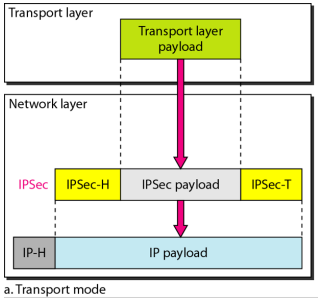
- Ajuda a criar pacotes **confidenciais** e **autenticados** para a camada IP
- Opera em dois modos: transporte ou túnel



IPSec

Modo de transporte:

- IPSec protege aquilo que é entregue da camada de transporte para a camada de rede (protege o payload da camada de rede).
- Não protege o cabeçalho IP. Nesse modo, o cabeçalho e o trailer IPSec são acrescentados às informações provenientes da camada de transporte
- Normalmente, é usado quando precisa de proteção fim-a-fim

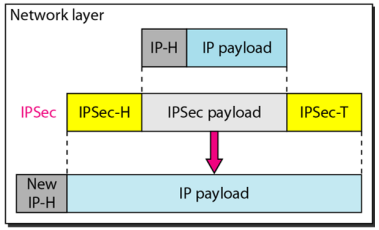


a. Transport mode

IPSec

Modo de túnel:

- IPSec protege o pacote IP inteiro, inclusive o cabeçalho
- Acrescenta um novo cabeçalho IP, com informações distintas do cabeçalho IP original
- Em geral, é usado entre dois roteadores, entre um host e um roteador ou entre um roteador e um host (quando o emissor ou o receptor não for um host)



b. Tunnel mode

IPSec

Os modos em ação:

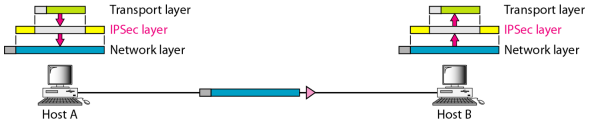


Figura : Modo transporte em ação

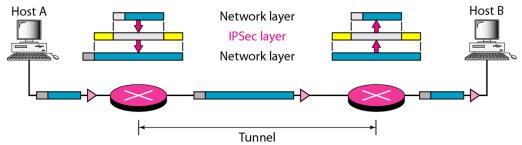


Figura : Modo túnel em ação

IPSec

Protocolos de segurança:

- IPSec define dois protocolos para oferecer autenticação e/ou criptografia para pacotes no nível IP:
  - AH (authentication header)
  - ESP (encapsulating security payload)

IPSec

AH (authentication header)

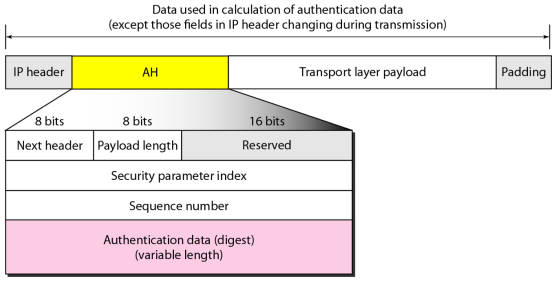
- autenticar o host de origem
- garantir a integridade do payload
  - usa uma função hash e uma chave simétrica para criar um resumo
  - o resumo é inserido no cabeçalho AH
  - o AH é colocado na posição posição apropriada
- Quando um datagrama IP transporta um cabeçalho de autenticação, o valor original do *campo de protocolo* é substituído pelo valor 51

O protocolo AH fornece autenticação de fonte e integridade de dados, mas não privacidade

IPSec

AH, etapas:

1. Cabeçalho AH é acrescentado ao payload com o campo dados de autenticação configurado em zero
2. Bits de preenchimento podem se acrescentados para tornar par o comprimento total
3. Hashing se baseia no pacote total. Com exceção dos campos IP que mudam o valor durante a transmissão
4. Os dados de autenticação dão inseridos no cabeçalho de autenticação
5. O cabeçalho IP é acrescentado após o valor campo de protocolo ser alterado para 51



IPSec

Cabeçalho AH:

- **Next header**: define o tipo de payload transportado pelo cabeçalho IP (TCP, UDP, ICMP ou OSPF)
- **Payload length**: comprimento do cabeçalho de autenticação
- **Security paramter index**: identificador de circuitos virtuais
- **Sequence number**: fornece informações de ordenação para uma sequencia datagramas
- **Authentication data**: é o resultado da aplicação de função hash a todo datagrama IP, exceto para campos que são modificados em trânsito (ex. TTL)

IPSec

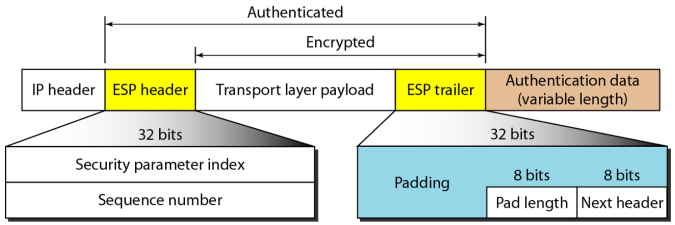
ESP (Encapsulation Security Payload):

- o ESP adiciona cabeçalho e trailer
- dados de autenticação acrescentados no final do pacote
- o valor do *campo protocolo* do IP é 50

O ESP oferece recursos de autenticação de fonte, integridade e privacidade

ESP, etapas:

1. é acrescentado um trailer ESP ao payload
2. o payload e o trailer são criptografados
3. é adicionado o cabeçalho ESP
4. o cabeçalho ESP, o payload e o trailer ESP são usados para criar os dados de autenticação
5. os dados de autenticação são acrescentados no final de trailer ESP
6. o cabeçalho IP é acrescentado após o valor do protocolo ser alterado para 50



Cabeçalho ESP:

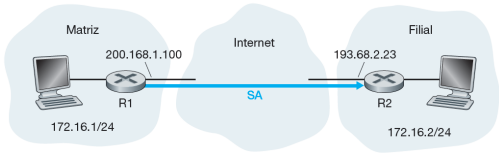
- **Security parameter index**: identificador de circuitos virtuais
- **Number of sequence**: fornece informação de ordenação
- **Padding**: preenchimento
- **Pad lenght**: comprimento de preenchimento
- **Next header**: define o tipo do payload
- **Authentication data**: é resultado da aplicação de um esquema de autenticação a partes do datagrama

Tabela : Serviços fornecidos pelo IPSec

Serviços	AH	ESP
Controle de acesso	Sim	Sim
Autenticação de mensagens (integridade)	Sim	Sim
Autenticação de entidades (autenticação de fontes de dados)	Sim	Sim
Confidencialidade	Não	Sim
Proteção de ataque de reprodução	Sim	Sim

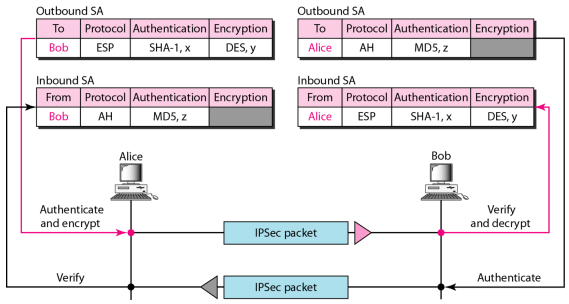
Associação de segurança (SA – security association): o IPSec precisa de conjunto de parâmetros de segurança antes de se tornar operacional. O estabelecimento dos parâmetros de segurança é realizado por meio da SA

- Um conjunto de parâmetros é estabelecido entre o emissor e determinado receptor na primeira vez que o emissor tiver um datagrama a ser enviado para esse receptor em particular
- O conjunto pode ser salvo para transmissão futura
- O IPSec transforma um protocolo sem estabelecimento de conexão, o IP, em um protocolo orientado a conexão (conexão lógica, denominada associação)
- Uma SA é uma conexão lógica simples; ou seja, ela é unidirecional do remetente ao destinatário.
- Se as duas entidades querem enviar datagramas seguros entre si, então duas SAs precisam ser estabelecidas, uma em cada direção.



IPSec

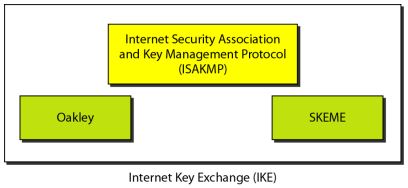
SA: exemplo simples



- **Banco de dados de associação de segurança** (SADB): um conjunto de SA armazenado em um BD
- **SPI** (Security paramter Index): diferencia uma SA da outra. Índice é definido por parâmetro+endereço_de_origem+endereço_de_destino+protocolo

IPSec

IKE (Internet Key Exchange): protocolo usado para criar as SA para o IPSec. É um procolo complexo baseado em três outros protocolos – Oakley, SKEME e ISAKMP.



Internet Key Exchange (IKE)

- **Oakley**: protocolo para troca de chaves baseado no Diffie-Hellman
- **SKEME**: é outro protocolo para troca de chaves, que usa criptografia de chave pública para autenticação de entidades em um protocolo de intercâmbio de chaves
- **ISAKMP**: implementa as trocas estabelecidas no IKE. Define vários pacotes, protocolos e parâmetros que possibilitam a ocorrência de trocas IKE em mensagens formatadas padronizadas para criar SAs.

VPN

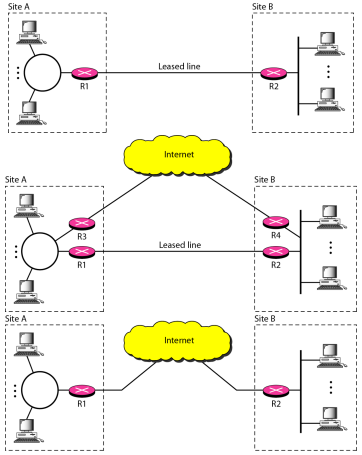
Virtual Private Network (VPN): as organizações usam a Internet para comunicação entre elas (ex. matriz e filial), mas precisam de privacidade em suas comunicações internas. O VPN usa o protocolo IPSec para aplicar segurança aos datagramas IP.

- **Redes privadas**: é para uso interno da organização, possibilita o acesso a recursos compartilhados e, ao mesmo tempo, fornece privacidade
- **Intranet**: rede privada (LAN), limitada aos usuários dentro da organização
- **Extranet**: uma intranet com alguns recursos acessíveis por usuários fora da organização sob controle do administrador de redes

VPN

Três formas de obter privacidade

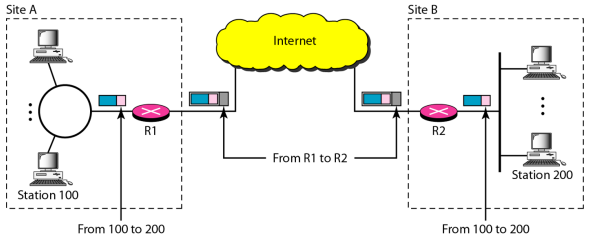
- Redes privadas
- Redes híbridas
- Redes Privadas Virtuais



VPN

Tecnologia VPN: usa o IPSec no modo túnel para fornecer autenticação, integridade e privacidade

- utiliza dois conjuntos de endereços
- rede pública (Internet) é responsável para transportar o pacote R1 a R2



Referências

[1] B. A. Forouzan. *Comunicação de Dados e Redes de Computadores*. McGrawHill e Bookman, 2008.

[2] W. Stallings and L. Brown. *Segurança de computadores – princípios e práticas*. Elsevier, 2014.