VPN

- Virtual Private Network (VPN) é uma conexão segura baseada em criptografia
- O objetivo é transportar informação sensível através de uma rede insegura (Internet)
- VPNs combinam tecnologias de criptografia, autenticação e tunelamento
- É interessante para interligar pontos distantes de uma organização através da Internet

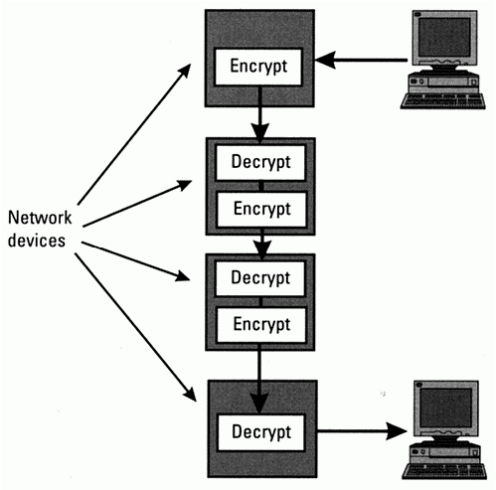
Nível de segurança de uma VPN

- O nível de segurança de uma VPN depende da camada onde a segurança é aplicada
- Os cabeçalhos dos pacotes abaixo da camada protegida não estão seguros
- Essa informação pode ser usada para planejar um ataque
- Quanto mais alta a camada protegida, mais informação pode ser obtida por "grampos"

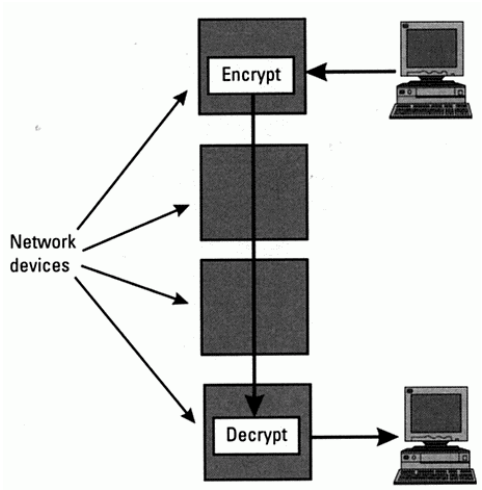
Nível de segurança de uma VPN

- Exemplo: segurança a nível de rede não protege o número IP (informação de tráfego)
- Se a camada criptografada for a de transporte, um sniffer pode identificar qual serviço está sendo usado:
  - WWW (consulta a páginas)
  - SMTP (envio de emails)
  - DNS (consulta de nomes)

Tipos de VPN: Nodo-a-Nodo



Tipos de VPN: Fim-a-Fim



Protocolos de VPN

- Existem diversos protocolos de VPN:
  - PPTP (Point to Point Tunneling Protocol)
  - L2TP (Layer 2 Tunneling Protocol)
  - CIPE
  - IPSec (Internet Protocol Security)
  - SOCKS
  - SSL / TLS (Secure Socket Layer / Transport Layer Security)
  - SSH + PPP (Secure Shell + Peer-to-Peer Protocol)

PPTP

- Point to Point Tunneling Protocol: Microsoft
- PPTP é usado em máquinas NT e faz VPN nodo-a-nodo
- A criptografia é feita na camada de enlace
- O PPTP é basicamente uma extensão do PPP
- A segurança do PPTP é baseada no algoritmo MD4 (Message Digest 4): fraca
- Está disponível somente em Windows NT, 98 e Linux

PPTP

- O PPTP não é um algoritmo seguro porque o algoritmo MD4 foi quebrado e provado não ser unidirecional
- Existem programas hacker que conseguem descobrir o tráfego de uma VPN PPTP
- Apesar de tudo, é um dos tipos mais difundidos porque foi um dos primeiros protocolos disponíveis

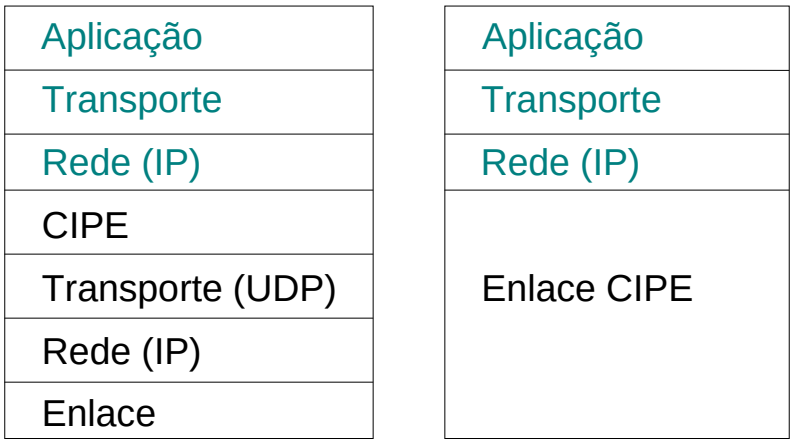
L2TP

- L2TP combina o protocolo Cisco Layer-Two Forwarding com PPTP
- Também é uma extensão do PPP
- Só pode ser usado em VPN nodo-a-nodo devido a aplicação na camada de enlace
- Para funcionar fim-a-fim, todos os nós da rede (roteadores) precisam suportar L2TP

CIPE

- O protocolo CIPE é diferente, porque utiliza como enlace o protocolo UDP
- É um protocolo fim-a-fim
- O CIPE usa o algoritmo IDEA (64 bits) ou Blowfish (128 bits) para criptografar o IP
- Porém o overhead do CIPE é maior do que os mostrados anteriormente

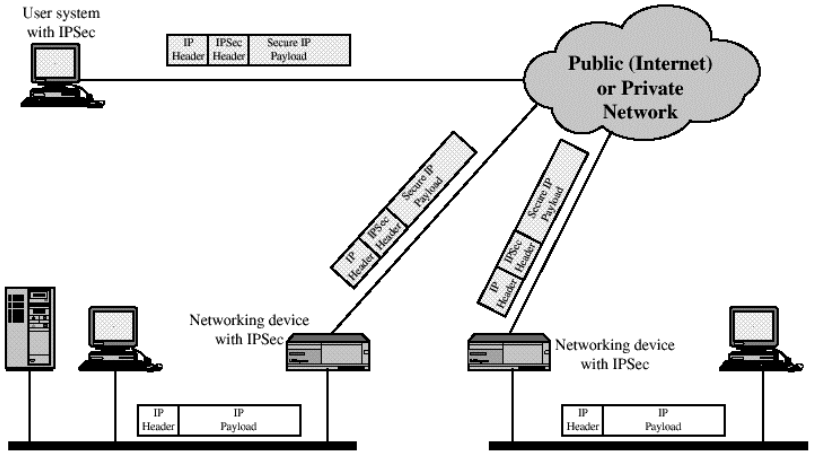
CIPE



IPSec

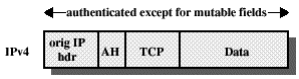
- O IPSec está em desenvolvimento pelo IETF
- O IPSec utiliza criptografia a nível de rede (acima dos protocolos de enlace)
- Suporta dois modos de operação:
  - Modo de Transporte
  - Modo de Túnel
- Serviços:
  - Autenticação: AH (Authentication Header)
  - Criptografia: ESP (Encapsulating Security Payload)

IPSec

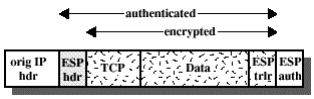


IPSec

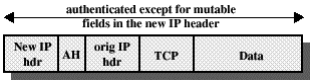
- Transporte
  - AH



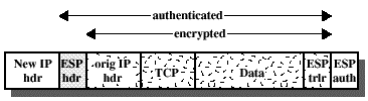
  - ESP



- Túnel
  - AH



  - ESP



IPSec - Modo de Transporte

- No modo de transporte somente o payload do pacote IP é criptografado
- Portanto é um protocolo fim-a-fim
- Porém está sujeito a análise de tráfego em função dos dados do cabeçalho do IP estarem disponíveis

IPSec - Modo de Túnel

- No modo de túnel o IPSec criptografa também o cabeçalho do IP
- Portanto é node-to-node e ambos os lados deve suportar IPSec
- Porém protege contra análise de tráfego
- É mais seguro que o modo de transporte, porém menos flexível

SOCKS

- SOCKS é usado para tráfego TCP através de um proxy de IP
- É compatível com quase todas as aplicações TCP e provê serviços rudimentares de firewall como NAT
- O serviço de NAT (Network Address Translator) mantém secreto o número IP de máquinas internas

SOCKS

- Apesar de funcionar a nível de transporte, evita análise de tráfego porque o endereço IP é mascarado pelo NAT
- Ao ser enviado para a Internet, o número IP original é substituído por outro temporário
- Porém só pode ser utilizado em um ambiente de proxy

SSL - Secure Socket Layer

- SSL é o protocolo usado para consultas a páginas seguras na Web
- Utiliza autenticação e criptografia de chave pública e de chave secreta
- Não é considerado um protocolo de VPN, por comunicar somente duas entidades
- Porém pode ser usado como base para uma VPN baseada no serviço de SSH + PPP

SSH + PPP

- SSH é um protocolo usado para acesso remoto de forma segura
- É usado para substituir o Telnet
- Utiliza o SSL para estabelecer um canal de comunicação seguro e usa o protocolo do Telnet sobre esse canal seguro
- A VPN é criada usando o SSH para transportar pacotes PPP

SSH

- O SSH cria um terminal remoto virtual seguro utilizando o SSL (ou TLS):

Telnet
TCP
IP

Telnet SSH
SSL ou TLS
TCP
IP

SSH + PPP

Aplicação
Transporte
Rede
PPP
Telnet SSH
SSL (ou TLS)
TCP
IP

- O protocolo de VPN SSH + PPP insere muito overhead na comunicação
- Porém é simples de ser implementado

Conclusão

- VPNs são essenciais para a utilização da Internet como meio de transmissão de dados sensíveis
- A segurança de uma VPN vem dos algoritmos escolhidos e da segurança das senhas
- VPNs podem ser implementadas em hardware (roteadores) ou software (Windows NT)