

Resumo do que vimos em Segurança da Comunicação

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais TI pos, Moss

- Firewall
 - Firewall de pacotes sem estado
 - Firewall de pacotes com estado
 - Gateways de Aplicação





Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

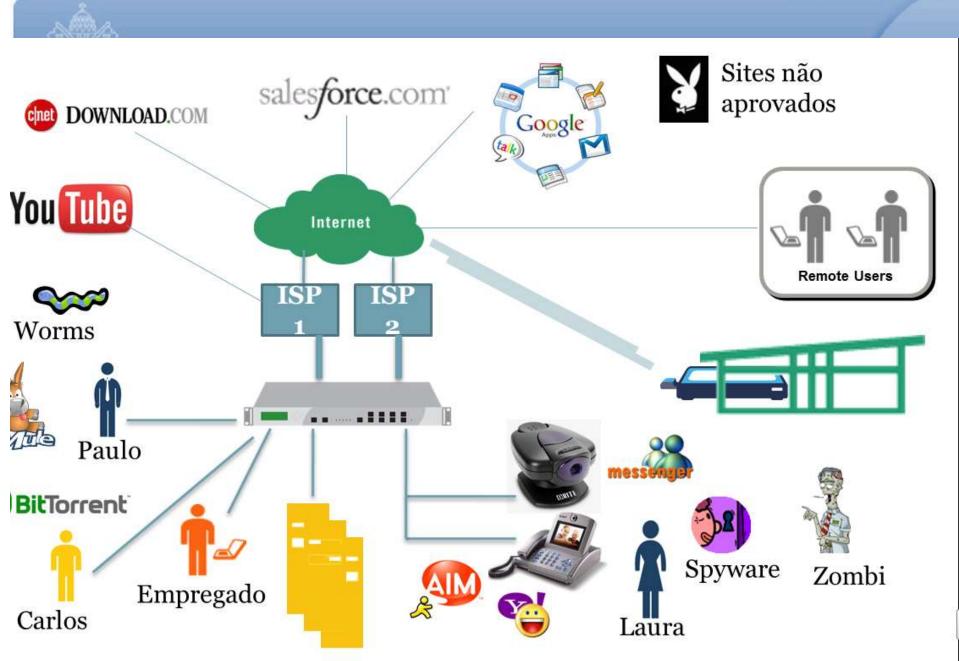
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais UTM (Unified Threat Management)

- Gerenciador Unificado de Ameaças: Como o próprio nome diz agrega várias funções de segurança da rede em um único equipamento com o objetivo de simplificar a administração do ambiente.





Serviços

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

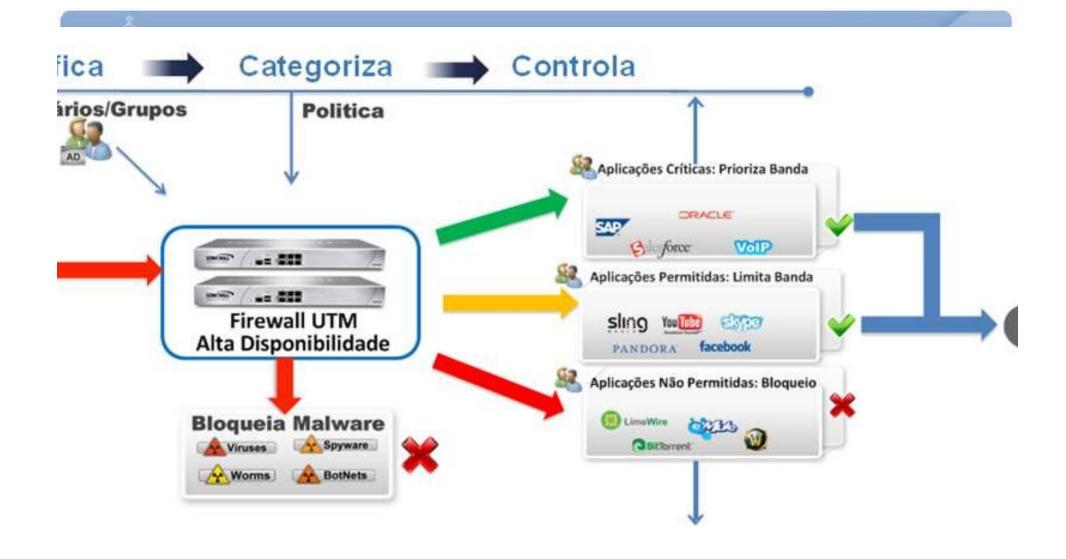
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seq. da WEB

- Firewall
- VPN
- Balanceamento de Carga e redundância de link;
- Priorização de largura de banda;
- IPS Sistema de Detecção contra intrusos
- Gateway Antivírus;
- Filtro de Conteúdo;



Seg. da WEB

Questões Sociais

ES 14BACKDOOR
15DDOS 33DNS
T >35FINGER
15Instant
IAP 16INFO
44MS-SQL 24MSIMEDIA 6MYSQL
P 20RACLE
21POP2 4POP3
ICES 13SCAN
17TELNET
3WEB-ATTACKS
EB-CLIENT



Inspeção em tempo real





Questoes Sociais



Checagem de tráfego WEB

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

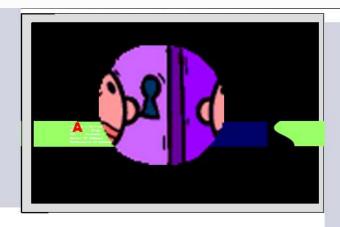
Seg. de Correio

Seq. da WEB

Questões Sociais

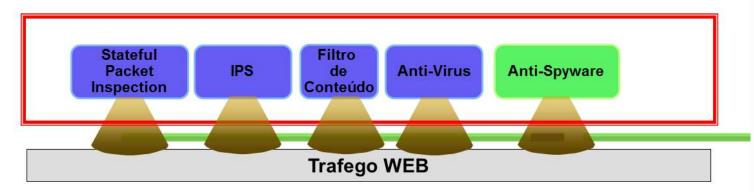
Bases

ATTACK-RESPONSES 14BACKDOOR
58BAD-TRAFFIC 15DDOS 33DNS
19DOS 18EXPLOIT >35FINGER
13FTP 50ICMP 115Instant
Messenger 25IMAP 16INFO
7Miscellaneous 44MS-SQL 24MSSQL/SMB 19MULTIMEDIA 6MYSQL
2NETBIOS 25NNTP 20RACLE
25P2P 51POLICY 21POP2 4POP3
18RPC 124RSERVICES 13SCAN
25SMTP 23SNMP 17TELNET
14TFTP 9VIRUS 3WEB-ATTACKS
47WEB-CGI 312WEB-CLIENT





Spyware encontrado e bloqueado





Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

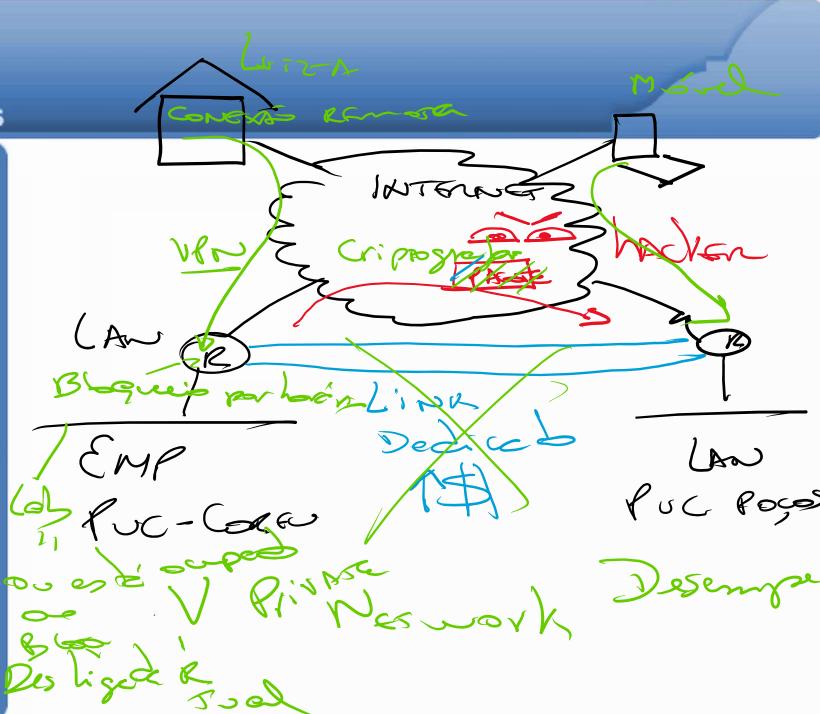
Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio 🔾 🕓

Seg. da WEB





VPNs – Virtual Private Networks (1)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

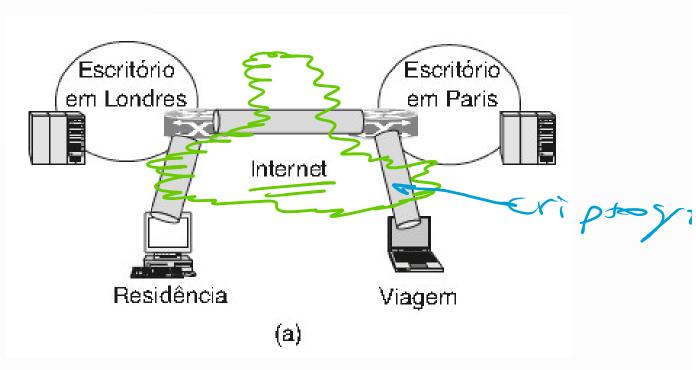
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seq. da WEB

Questões Sociais



Uma rede privada virtual (VPN).



VPNs – Virtual Private Networks (2)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

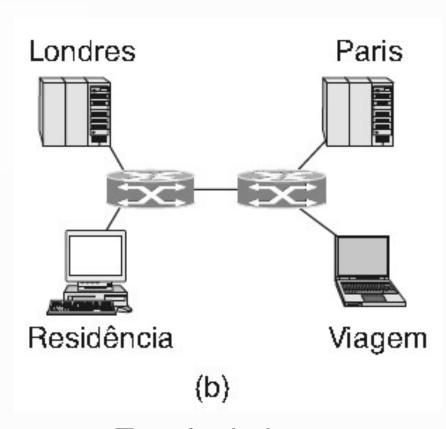
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Topologia interna.



Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

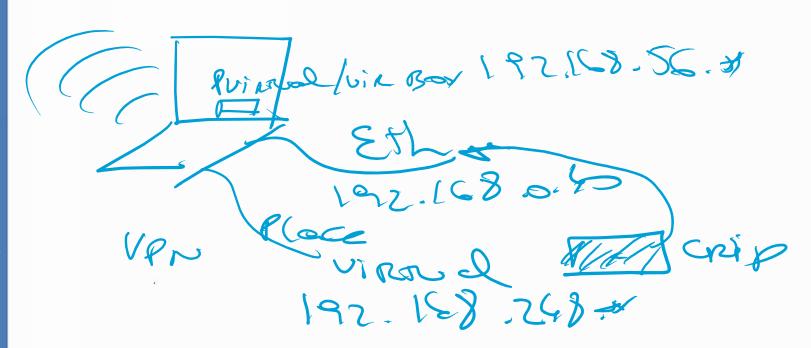
Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB





VPNs – Virtual Private Networks (3)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

- O tunelamento pode ser voluntário
 (estabelecido pelo próprio usuário)
 ou compulsório (o usuário não sabe
 que está passando por um túnel)
- O tunelamento e a criptografia garantem a segurança dos dados mas não podem garantir tempos de resposta e taxas de transmissão.



Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

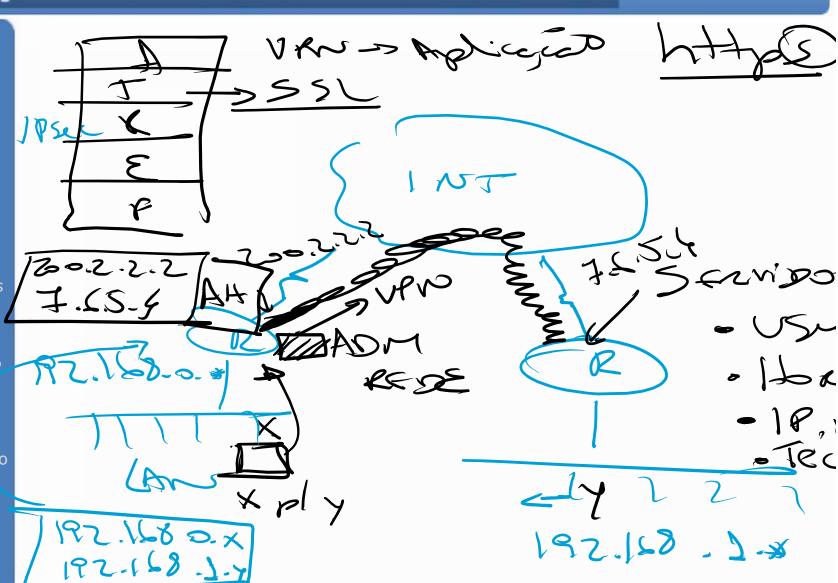
Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB





VPNs – Virtual Private Networks (4)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seq. da WEB

Questões Sociais

Requisitos Básicos

- Autenticação de Usuários
 - Autenticar o usuário e permitir o acesso apenas de usuários autorizados.
 - Auditar qualquer tentativa de acesso, autorizado ou não.
- Gerenciamento de Endereços
 - Não divulgar os endereços internos da rede, utilizando endereços externos fictícios.
- Criptografia de Dados
 - Manter a privacidade dos dados na rede pública.



VPNs – Virtual Private Networks (5)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seq. da WEB

- Tunelamento na Camada de Enlace:
 - PPTP (Point-to-Point Tunneling) da Microsoft permite que o tráfego IP, IPX e NetBEUI sejam criptografados e encapsulados para serem enviados através de redes IP privadas ou públicas.
 - <u>L2TP</u> (*Layer 2 Tunneling Protocol*) da IETF permite que o tráfego IP, IPX e NetBEUI sejam criptografados e enviados através de canais de comunicação de datagrama ponto a ponto tais como IP, X25, Frame Relay ou ATM.
 - <u>L2F</u> (*Layer 2 Forwarding*) da Cisco é utilizada para VPNs discadas.
 - CIPE Empilha tudo dentro de um pacote UDP.



VPNs – Virtual Private Networks (6)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

- Tunelamento na Camada de Rede
 - IPsec
- Tunelamento na Camada Transporte
 - SOCKS é usado para tráfego TCP através de um proxy.
 - SOCKS com serviço de NAT
 - SSL (Secure Socket Layer)
 - SSH abertura de uma sessão remota a um computador que irá trafegar como sendo seu proxy



Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

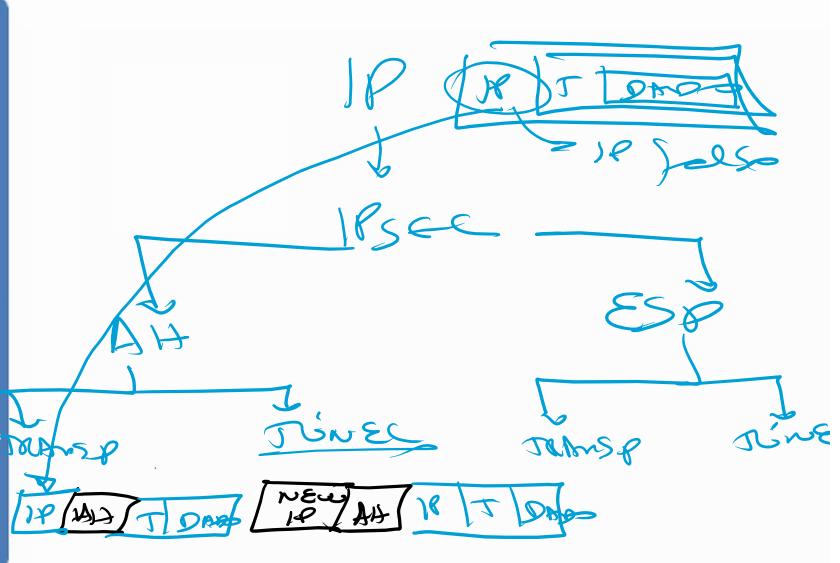
Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB





IPsec (1)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

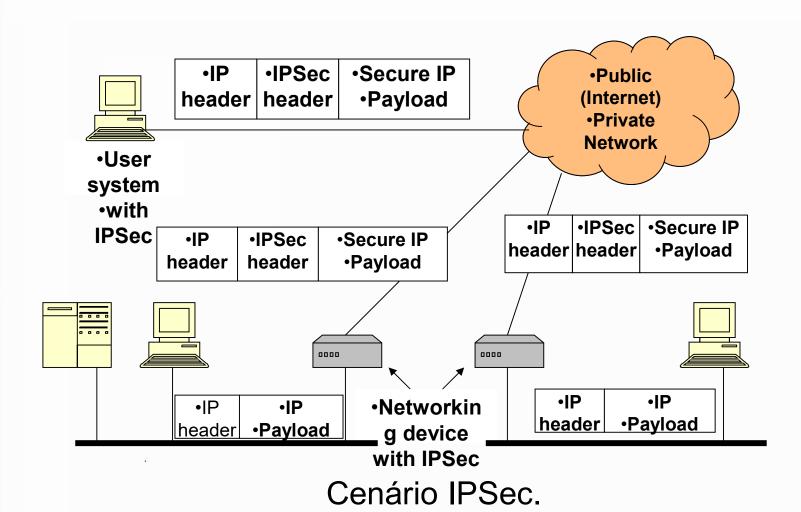
Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB





IPsec (2)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

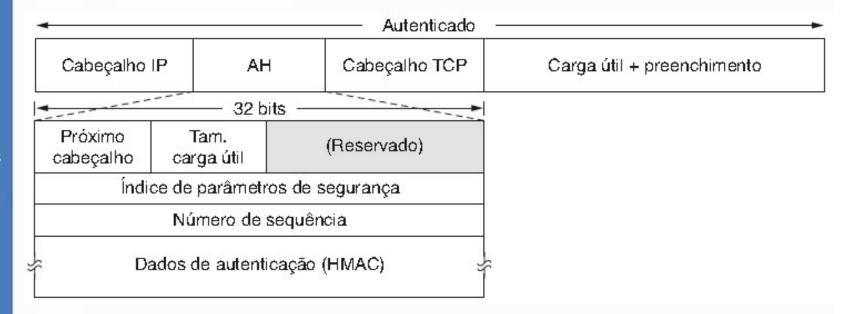
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Cabeçalho de autenticação IPsec em modo de transporte para o IPv4.



IPsec (3)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

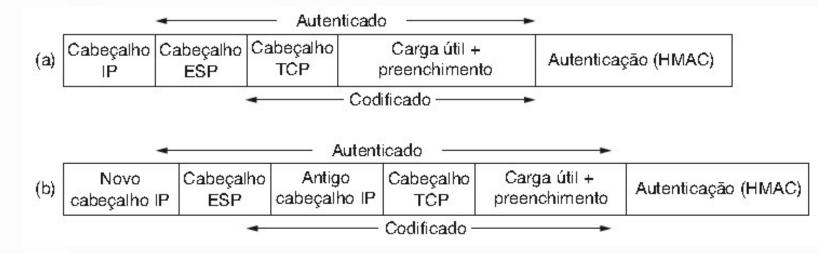
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



(a) ESP em modo de transporte. (b) ESP em modo túnel.



IPsec (4)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

• Modos de Operação

- Modo Transporte
 - Criptografa apenas a carga útil do pacote IP (protocolo fim-a-fim).
 - O cabeçalho é transmitido em texto plano (inseguro).
- Modo Túnel
 - Criptografa também o cabeçalho IP (protocolo nó-a-nó).
 - Mais seguro e menos flexível que o modo transporte



VPNs – Virtual Private Networks (7)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

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 Server, Linux, etc)