Segurança Operacional

Tecnologias de Defesa - VPN

Gustavo Vilar

- Mini – CV
  - PPF / DPF – Papiloscopista Policial Federal
  - Pós-Graduado em Docência do Ensino Superior – UFRJ
  - Graduado em Ciência da Computação e Processamento de Dados – ASPER/PB
  - Aprovações: PRF 2002, PF 2004, MPU 2010, ABIN 2010

Gustavo Vilar

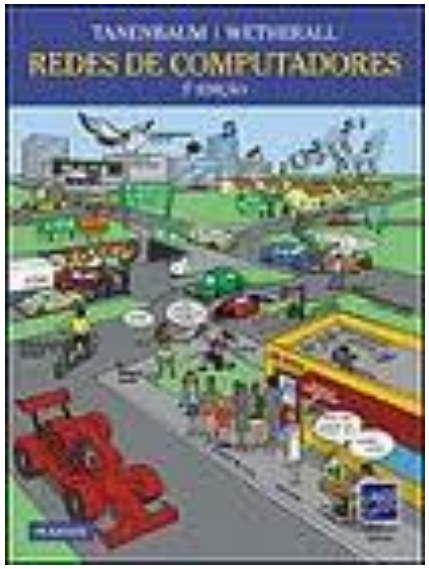
- Contatos:
  - gustavopintovilar@gmail.com
  - p3r1t0f3d3r4l@yahoo.com.br

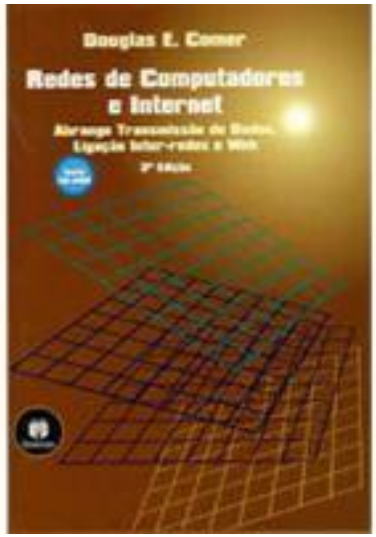
ITnerante

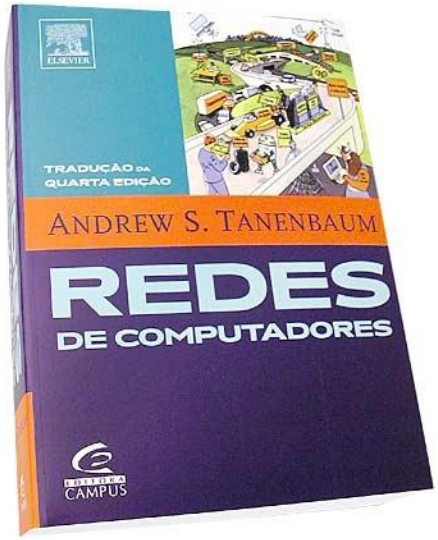
Escopo

- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais freqüentes.
- Abordar as metodologias de resolução de questões das principais bancas

Bibliografia



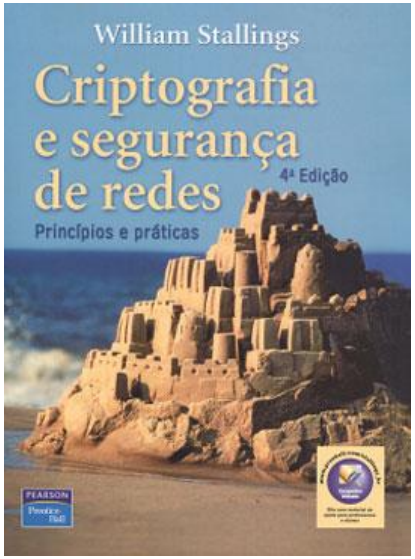




cespeUnB

Fundação Carlos Chagas

FUNDAÇÃO CESGRANRIO



ITnerante

VPN – Carga Horária

- 12 vídeo aulas (04h09m49s / 00h20m49s)
  - VPNs
    - Princípios
    - Montagem
    - Pontos de Implementação
    - Protocolos e Camadas
  - Primeira Bateria de Questões
  - Recomendações e Posicionamentos das VPNs
  - Protocolo IPSec
    - Introdução
    - Aspectos Relevantes
    - Cabeçalhos
    - Modos de Operação
  - Protocolo SSL/TLS
    - Aspectos relevantes
    - Funcionamento
    - Subprotocolos
  - Segunda Bateria de Questões

ITnerante

Algumas razões para VPN

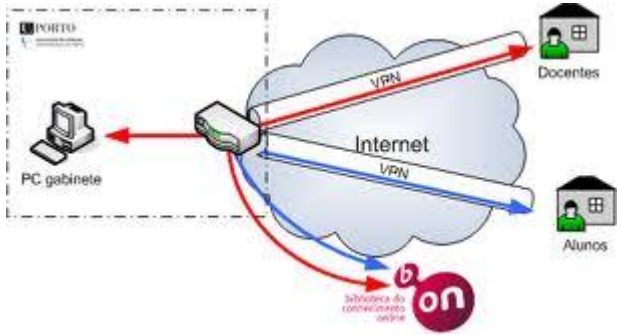
Conexões dedicadas custam caro

Aumento da complexidade de gerenciamento das conexões

Estrutura de acesso remoto mais complexa

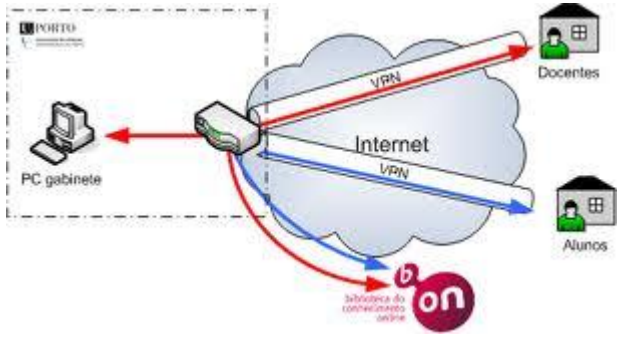
Embasamento VPN

- Uso de redes públicas para comunicação
- Virtual – Não requer circuitos alugados para interconectar sites
- Privada – Uso exclusivo de uma instituição. Tecnologia garante que a comunicação entre qualquer par de computadores permaneça oculta ou isolada de estranhos



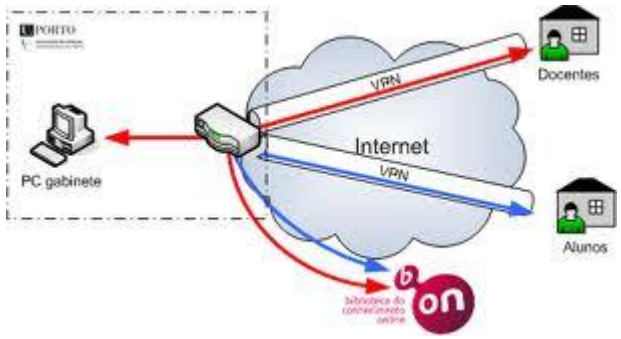
Embasamento VPN

- Usa o conceito de tunelamento para envio dos pacotes
  - Criptografia ou isolamento de tráfego num meio compartilhado
- Nas linhas dedicadas nenhum tráfego poderá vazar para fora das instalações da empresa, e os intrusos terão de grampear fisicamente as linhas para entrar ($$$)
- Diminuição do número de conexões e dos custos
  - Apenas uma conexão pública precisa ser gerenciada



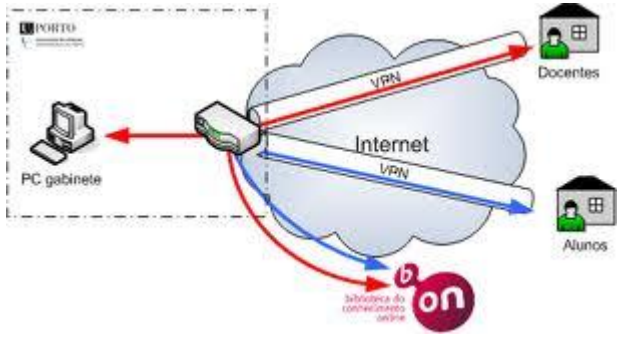
Embasamento VPN

- VPN implica em riscos
  - Confidencialidade
  - Integridade
  - Autenticidade
- Intranet VPN
  - Conecta departamentos e filiais de uma mesma organização
- Extranet VPN
  - Conecta parceiros comerciais



Embasamento VPN

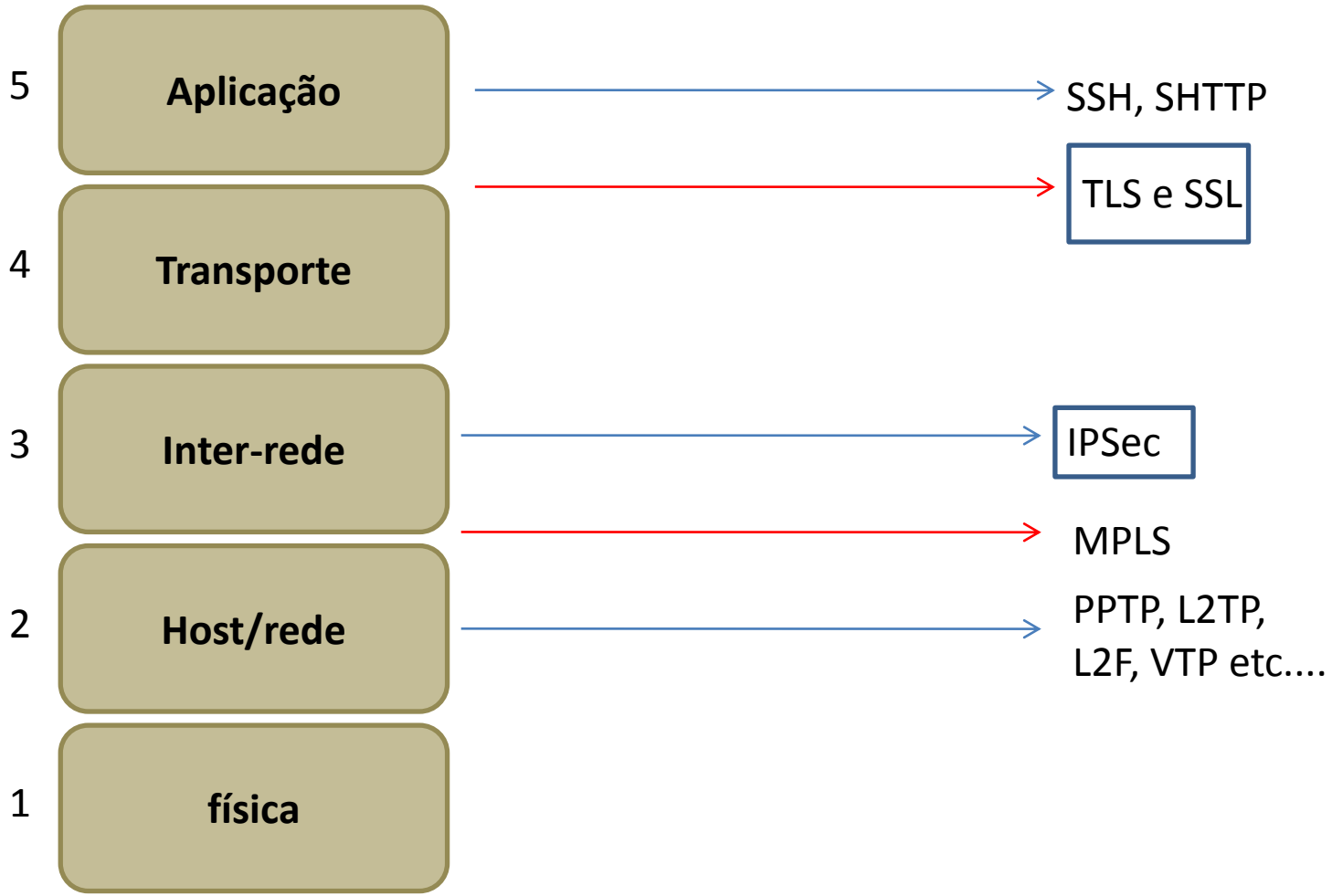
- Criptografia (C.I.A.)
- Tunelamento – Seja pela criptografia ou pelo isolamento de tráfego em um meio compartilhado
  - Pacotes dentro de outros pacotes. Mesmo protocolo ou protocolos distintos



Tipos de VPN

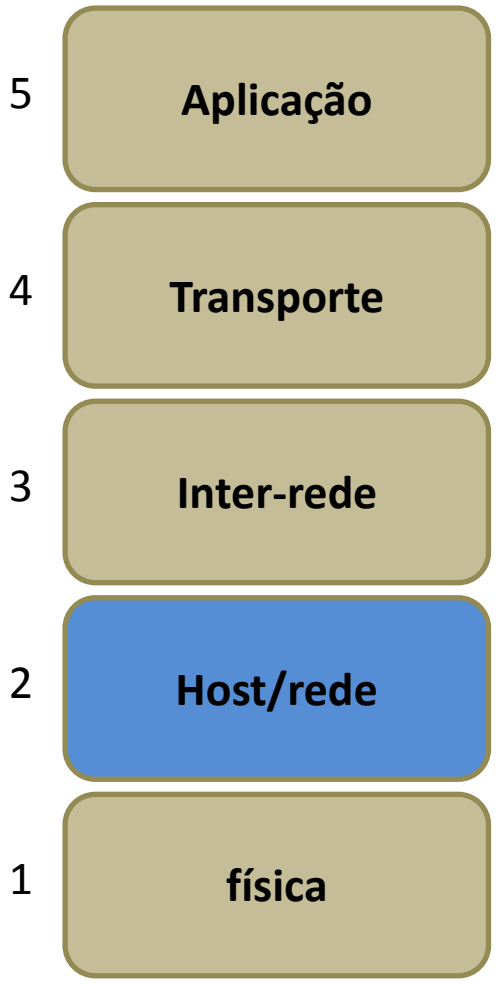
- Gateway-to-gateway VPN
  - Transparente para o usuário
  - Túneis iniciam e terminam nos gateways das organizações ou provedores VPN
- Client-to-gateway VPN
  - Túnel é iniciado no próprio equipamento do usuário
    - » requer software
    - » Uso de chave secreta
    - » permite uso de certificação digital
    - » Geralmente a autenticação é do aparelho e não do usuário
  - Necessidade de um software
  - Não é transparente
- Client-to-client
- Remote Access-VPN
  - Requer autenticação forte
  - É usado como forma alternativa de acesso remoto
  - Túnel inicia no cliente ou no provedor de acesso
  - PPP até o provedor

Protocolos VPN



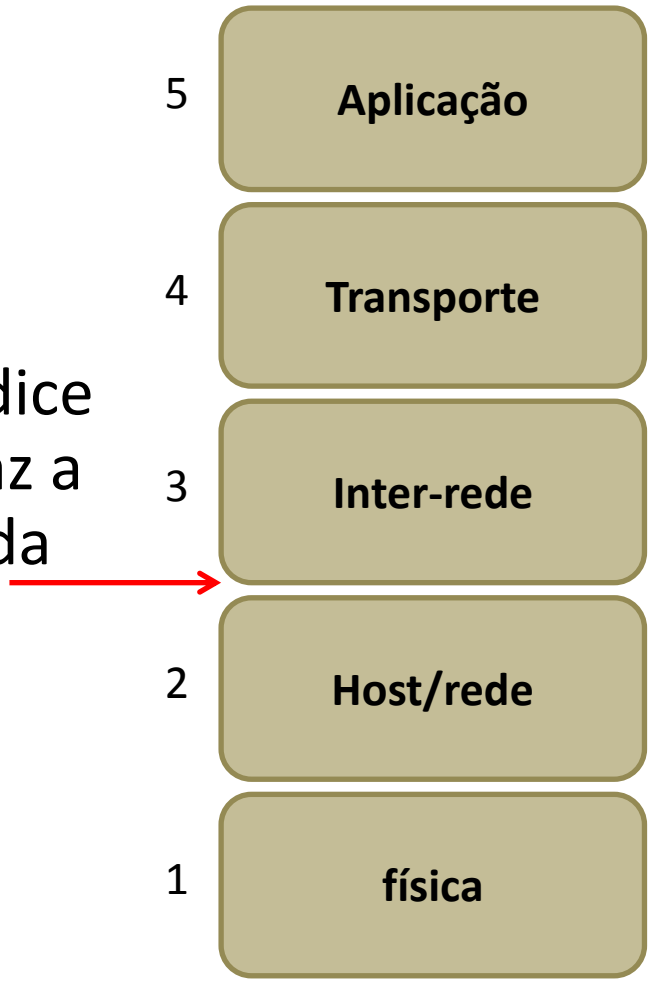
Camada 2

- Usado apenas para autenticação
- Tunelamento iniciado SEMPRE no equipamento do usuário
  - PPTP, L2F, L2TP, VTP
- Vantagens
  - Simplicidade
  - Compressão
  - Codificação completa
  - Inicialização BIDIRECIONAL do tráfego
- Desvantagens
  - Padronização em desenvolvimento
  - Pouca escalabilidade, segurança e confiabilidade
  - Impacto na fragmentação
- Indicado para
  - Indicados para acesso discado
  - Billing por volume de dados



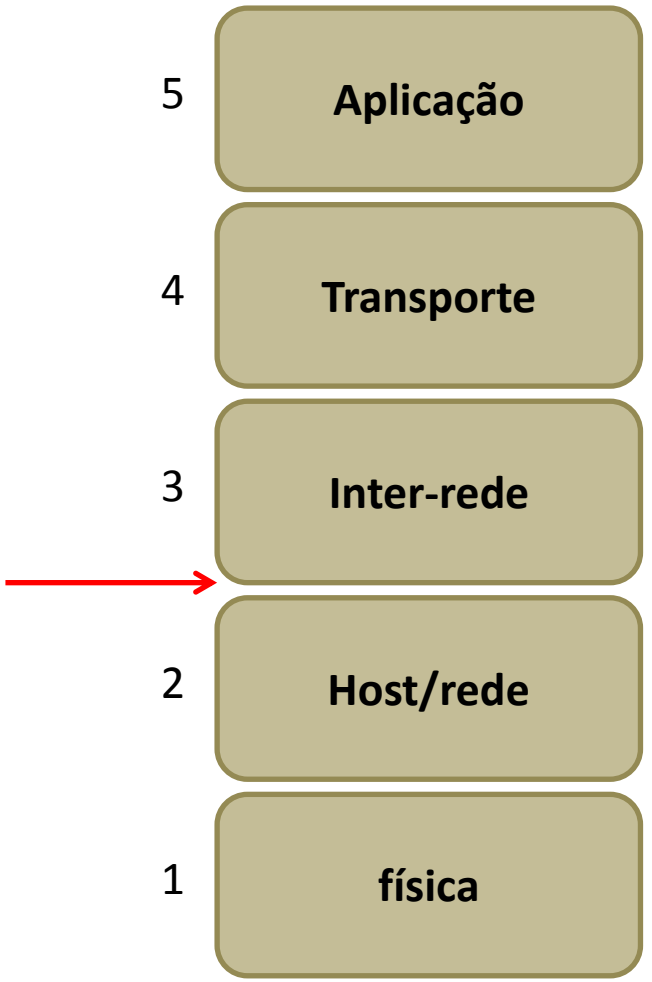
Camada “2.5”

- MPLS
  - Isolamento de tráfego
  - Está perigosamente perto da comutação por circuito
  - Transforma o rótulo em um índice para uma tabela interna que faz a descoberta da interface de saída correta, simplesmente uma questão de pesquisa interna
  - também conhecido como COMUTAÇÃO POR TAGS.



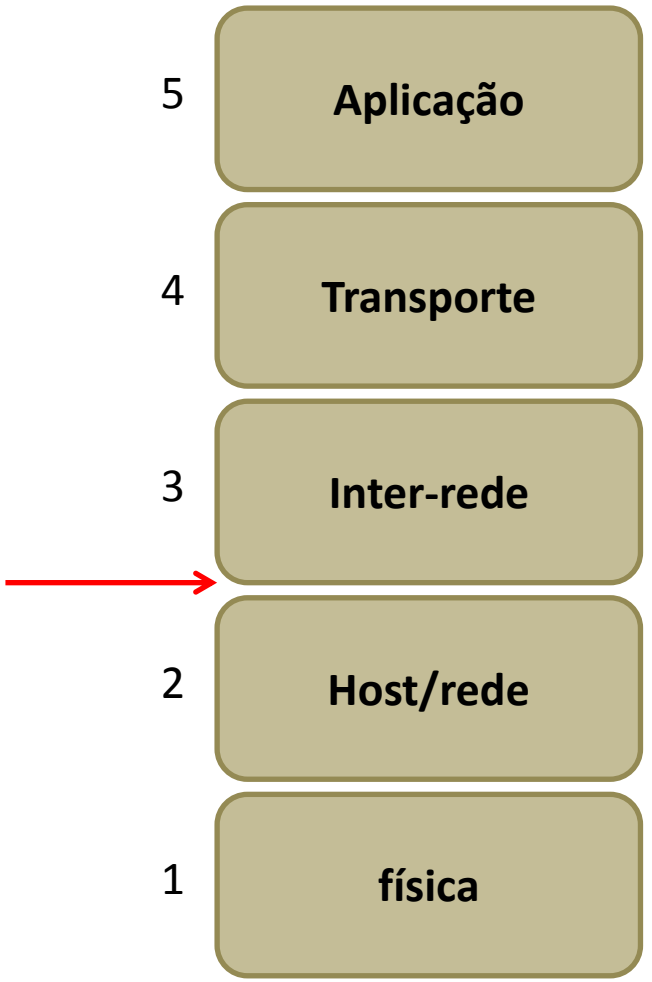
Camada “2.5”

- Rótulo
  - Só precisa ser válido por um salto
  - Troca de rótulo à medida que pacote passa de um roteador para outro
  - Rótulos atribuídos a fluxos ativos e recuperados quando terminados
  - Roteadores do core usam MPLS (comutação no lugar de pesquisa em tabelas de rotas)



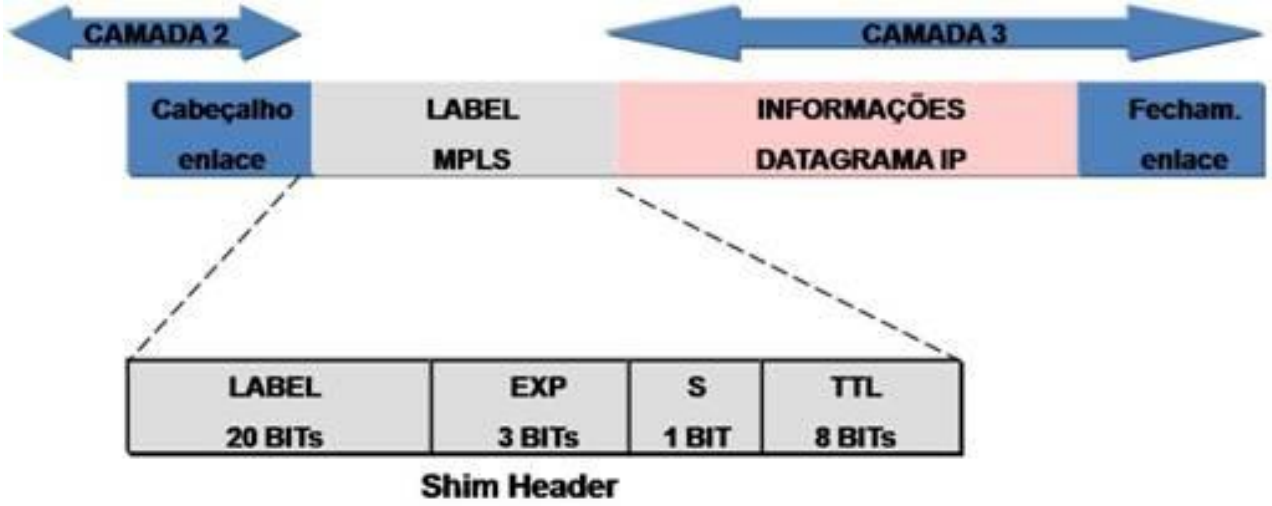
Camada “2.5”

- Vantagens
  - Baixo overhead no transporte do frame
  - Transparência para o usuário
- Desvantagens
  - Problemas com fragmentação
  - Violação de tamanhos máximos de frames (inserção e retirada via hardware – pilha de protocolos isenta)



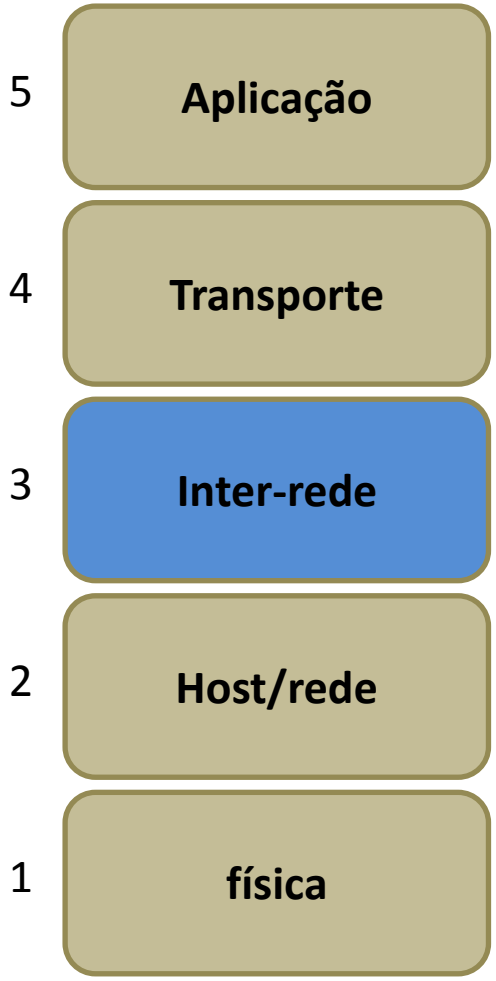
Camada “2.5”

- Cabeçalho MPLS fica depois do cabeçalho do frame
- Chamado de multiprotocolo pois pode ser usado com qualquer protocolo da camada 3
- 1 - Campo Label - que contém o valor da etiqueta para um determinado pacote;
- 2 - Campo EXP - informa a classe de serviço, define a prioridade dada ao pacote;
- 3 - Campo S - informa se há ou não empilhamento (stack) de etiquetas;
- 4 - Campo TTL - Time to Live - conta por quantos roteadores o pacote passou, procura evitar loops.



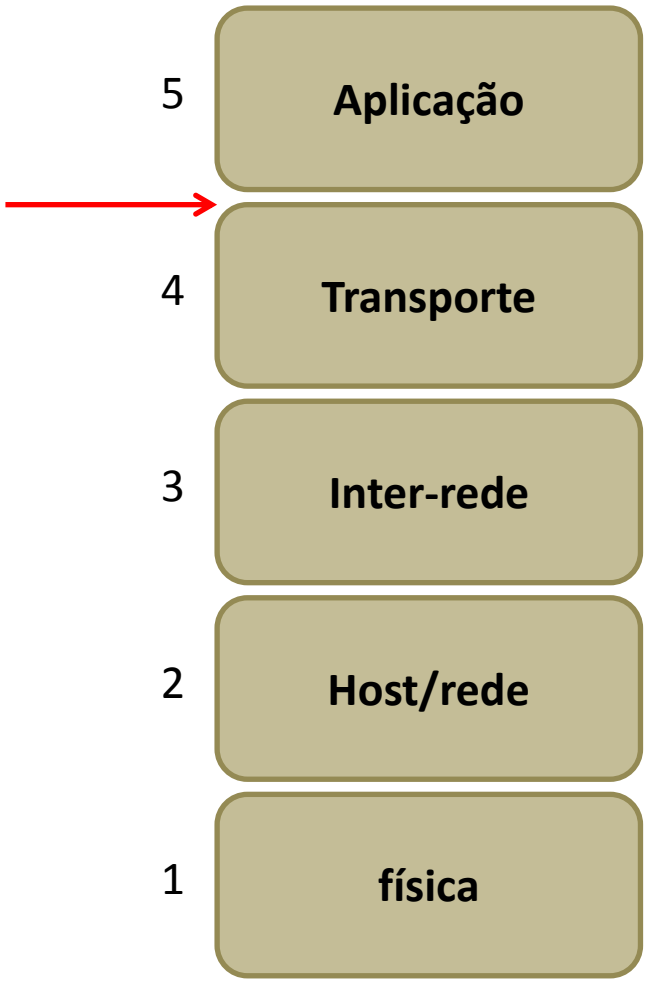
Camada 3

- IPSEC
  - Autenticação
  - Sigilo
  - Integridade
  - Padrão de fato das VPNs
- Mobile IP
- IPv6
- Vantagens
  - Escalabilidade
  - Segurança
  - Confiabilidade
- Desvantagens
  - Poucos fabricantes
  - desenvolvimento mais complexo



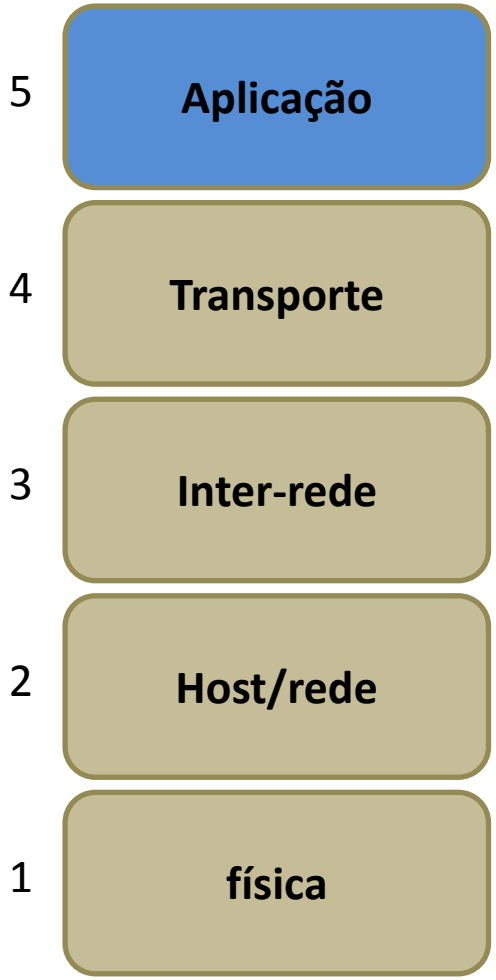
Camada 4.5

- SSL/TLS
  - Não está posicionado em uma camada específica, situando-se na “camada” de api socket
  - Solução adicional de segurança para os frágeis protocolos das camadas superiores.



Camada 5

- Camada 4
  - SSH
  - SHTTP (não confundir com HTTPS)
  - Etc.

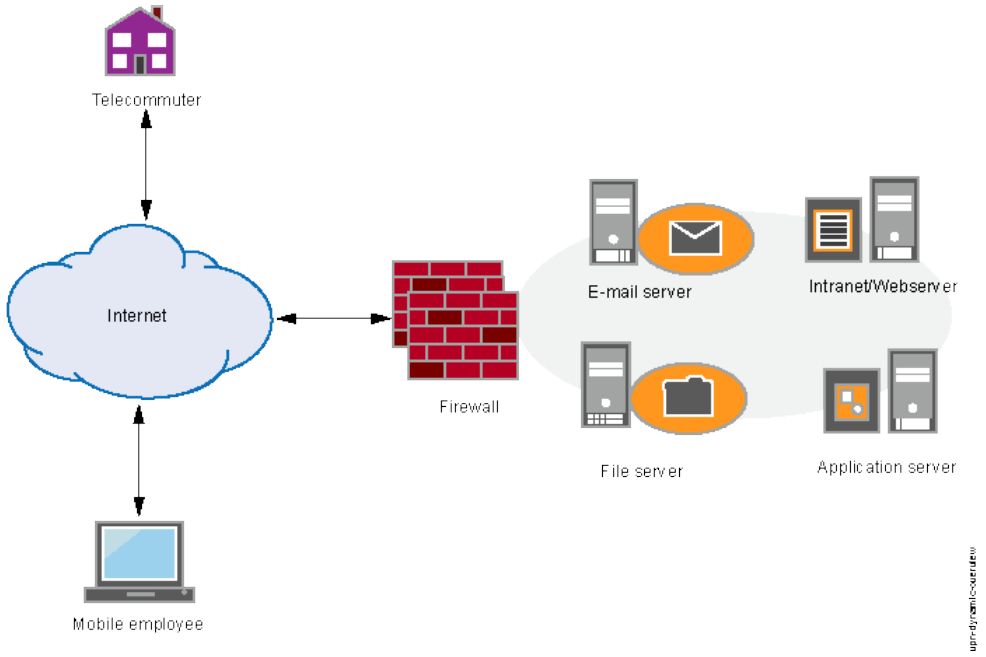


Motivações e Impedimentos

- Motivações para tunelamento na camada de aplicação
  - Usuário no controle
- Motivações para tunelamento ocorrer na camada de transporte
  - Suporte para todos os protocolos da camada superior
- Motivações para a tunelamento ocorrer na camada de rede
  - Compulsoriedade
- Motivações para o tunelamento NÃO ocorrer na camada de enlace
  - Fragilidade no processo de desenquadramento/reenquadramento

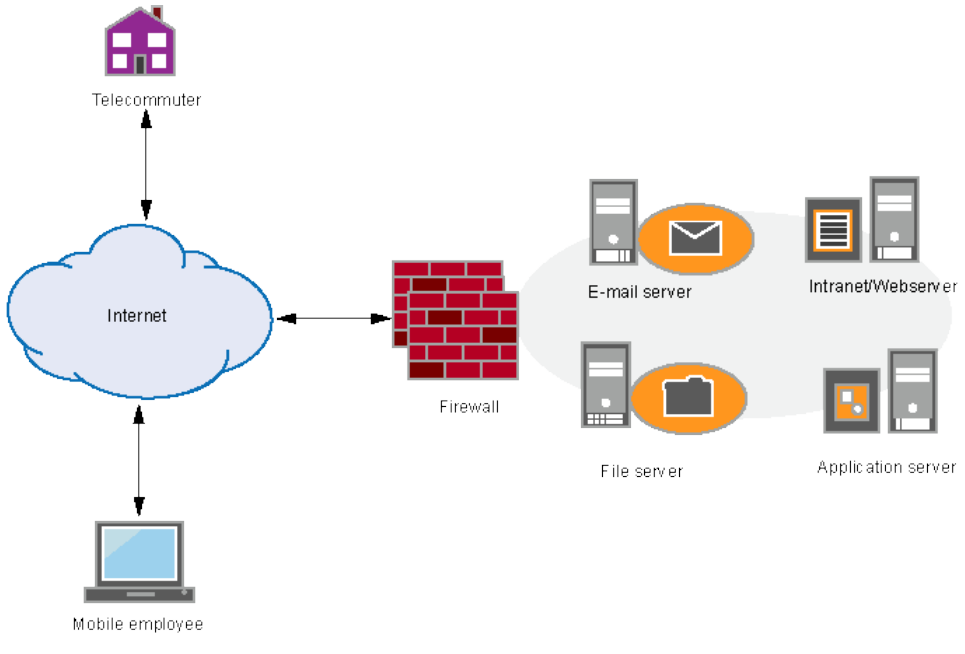
Posicionamento da VPN em relação ao Firewall

- Em frente ao firewall
  - Único ponto de falha
  - Riscos da indisponibilidade
  - Não é possível verificar se o gateway VPN foi ou não comprometido
  - VPN deve aceitar todo tipo de tráfego, criptografado ou não
  - Além de ponto terminal de VPN, deverá agir como gateway



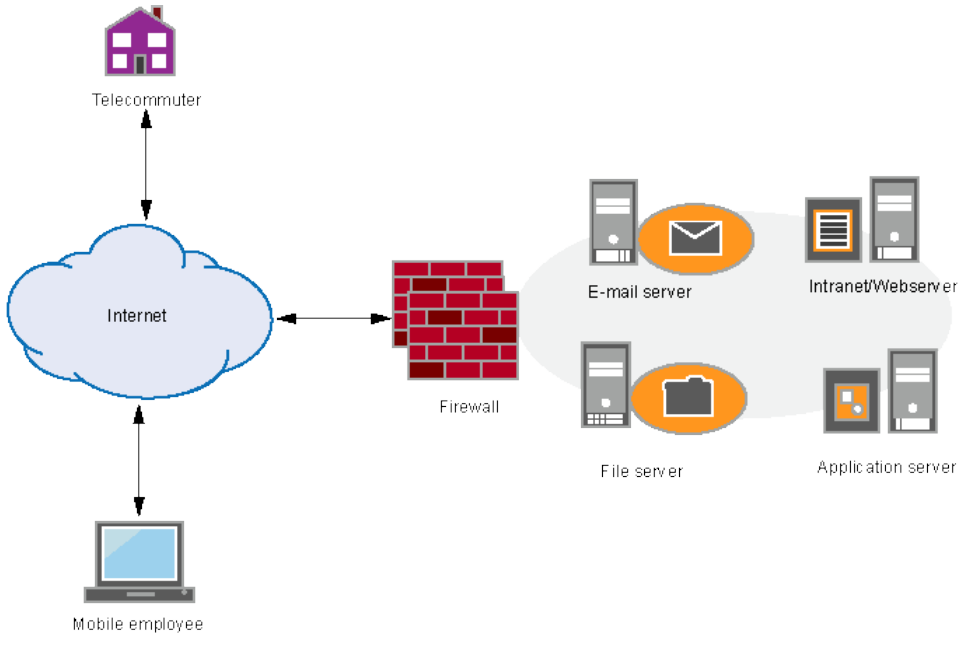
Posicionamento da VPN em relação ao Firewall

- No firewall
  - Único ponto de falha
  - Administração e gerenciamento simplificados
  - Falhas na implementação da VPN podem liberar acesso para controle do firewall ou das tabelas de filtragem ou de todas conexões



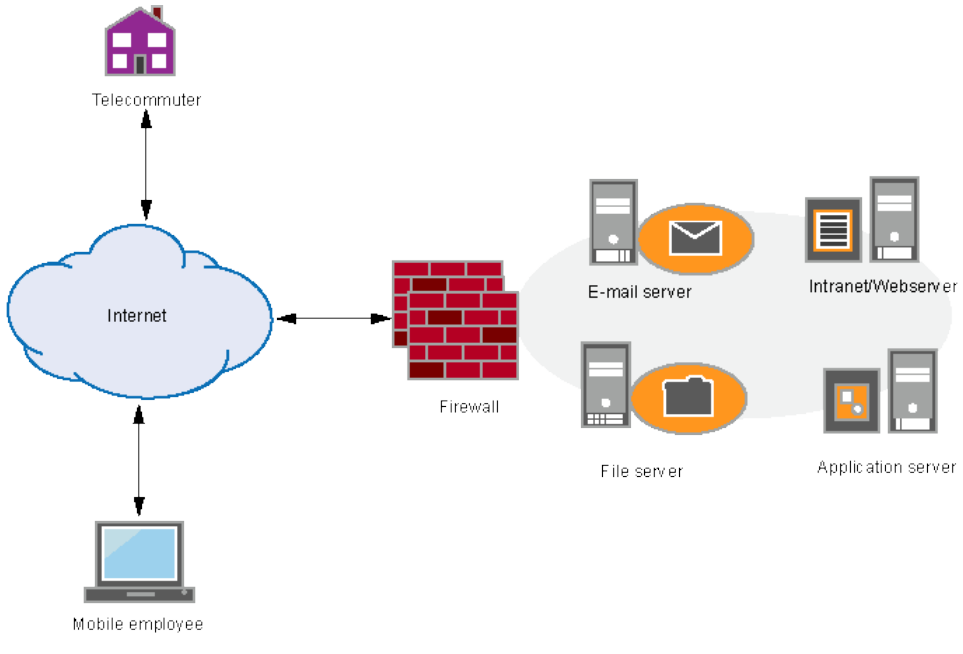
Posicionamento da VPN em relação ao Firewall

- Em interface dedicada do firewall
  - Mais indicada
  - Pacotes IPSEc são enviados para a VPN, que os decifra e devolve para o firewall
  - Firewall filtra estes pacotes segundo a política de segurança
  - Pacotes não criptografados são filtrados diretamente



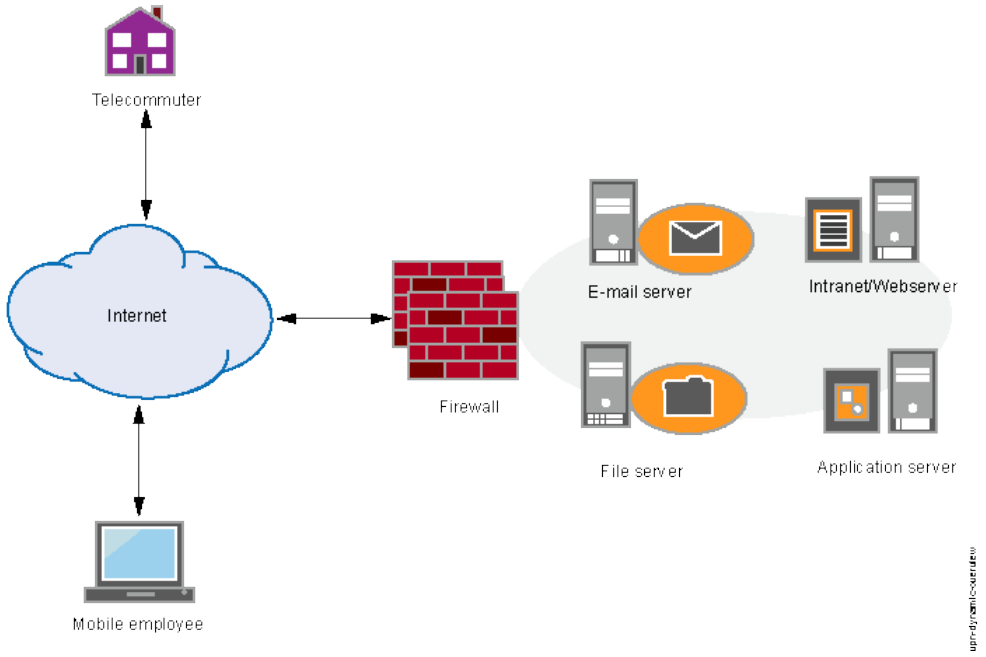
Posicionamento da VPN em relação ao Firewall

- Paralelo ao firewall
  - Elimina o único ponto de falha
  - Deixa a VPN à mercê de ataques vindos da internet
  - Oferece caminho alternativo para o hacker
  - Política de segurança do firewall não será aplicada à VPN



Posicionamento da VPN em relação ao Firewall

- Atrás do firewall
  - Firewall deve deixar passar todo tráfego cifrado para a VPN
  - Firewall deve permitir passagem dos pacotes com campo protocol com 50 ou 51, bem como porta 500 para IKE
  - Liberar as portas usadas pelos protocolos de camadas altas: 443, 22, etc...



Bateria de questões de aprendizagem

Virtual Private Network – Conceitos

ITnerante

TRT 24 – FCC 2011 – Analista Judiciário – Tecnologia da Informação

1. A tecnologia VPN proporciona, em termos de níveis de segurança:

a. autenticação do usuário, apenas.
b. criptografia, apenas.
c. autenticação dos dados e autenticação do usuário, apenas.
d. autenticação do usuário e criptografia, apenas.
e. autenticação do usuário, criptografia e autenticação dos dados

TRT 8 – FCC 2010 – Analista Judiciário – Tecnologia da Informação

2. O protocolo L2TP utilizado na implementação de VPNs atua na camada

a. Física.
b. Rede.
c. Enlace.
d. Transporte.
e. Aplicação.

INMETRO – CESPE 2010 – Pesquisador

3. Um mecanismo de controle de acesso a rede que melhore a segurança e diminua o risco de quebra da integridade e da confidencialidade das informações trafegadas nos acessos remotos consiste em

A. política de segurança da informação.
B. VPN (virtual private network) com IPSEC.
C. proxy.
D. servidor de logs dedicado.
E. autenticação centralizada em um serviço de diretório.

BASA – CESPE 2010 – ti – Segurança da Informação

4. Com relação a VPN, julgue os itens que se seguem.

[118] Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.

[119] Apesar de ser uma opção disponível, não se recomenda o uso de autenticação junto com cifração em VPNs, considerando a diminuição de desempenho.

[120] Preferencialmente, as VPNs são implementadas sobre protocolos de rede orientados à conexão como o TCP.

MPS – CESPE 2010 – Tecnologia da Informação

5. Julgue os itens que se seguem, relativos a aplicações web e conceitos de VPN (virtual private network).

[70] POP3 (post office protocol, versão 3) e IMAP4 (Internet mail access protocol, versão 4) são usados para baixar mensagens de um servidor de correio eletrônico.

[71] Uma VPN é uma rede privada porque é de uso exclusivo de uma organização ou empresa e é uma rede virtual porque ela não constitui uma WAN privada real (ou física).

[72] O FTP usa os serviços do TCP para estabelecer duas conexões, uma de controle e outra de dados, que utilizam as portas 21 e 22, respectivamente.

MPU – CESPE 2010 – Analista de Informática

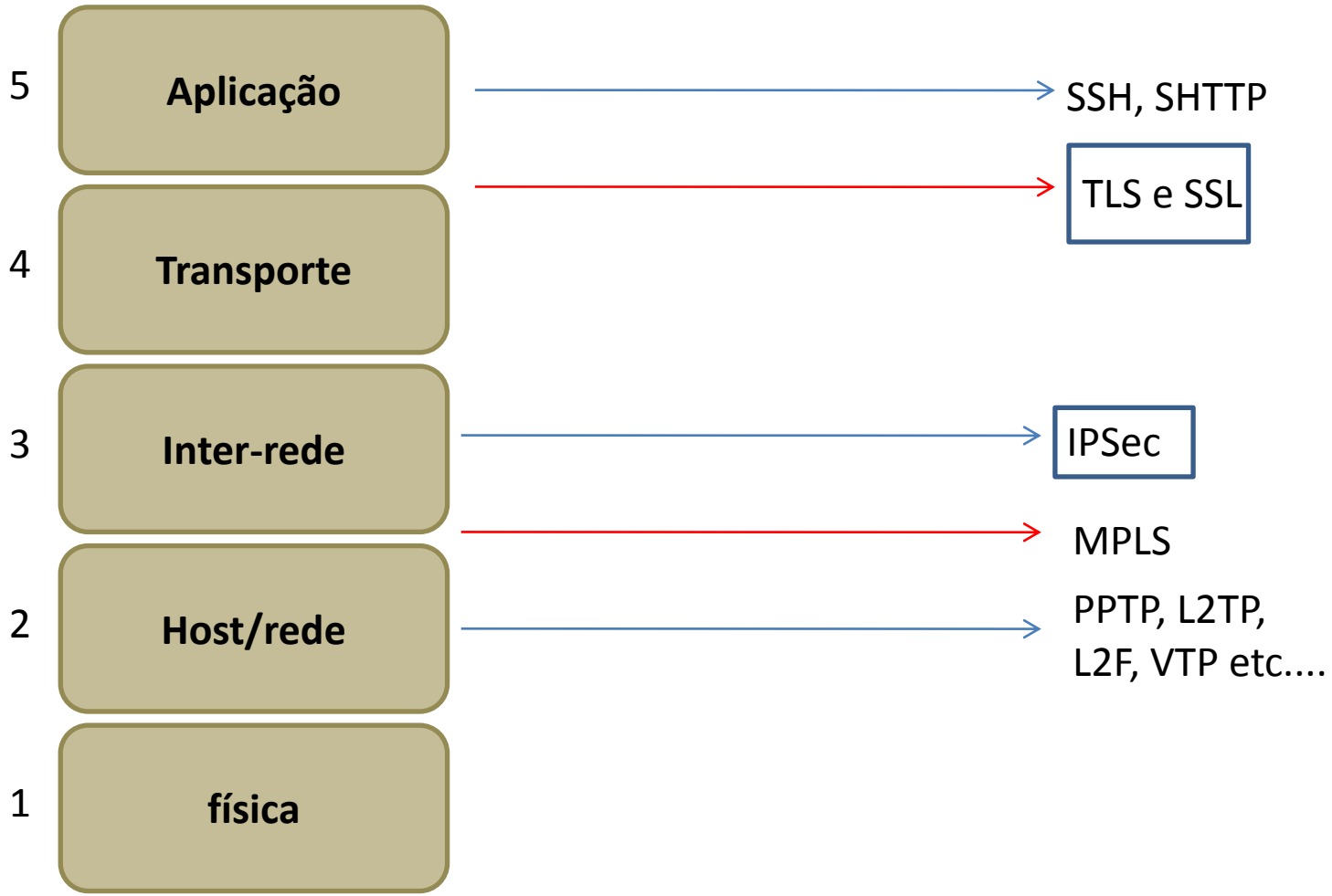
6. A respeito de segurança da informação, julgue os itens seguintes.

[136] A VPN pode ser uma alternativa para conexão remota de um usuário, via Internet, à rede privada de uma empresa, a partir de um provedor de acesso.

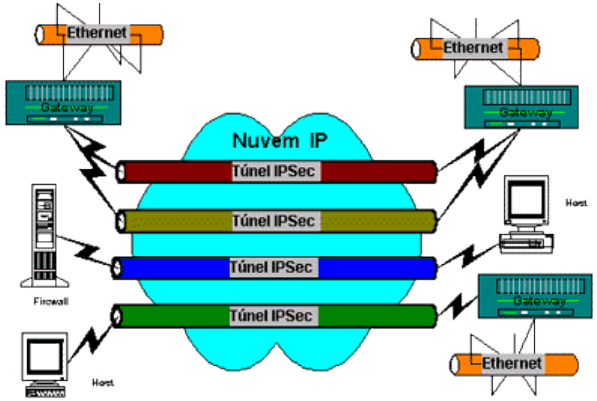
Gabarito

1. E
2. C
3. B
4. C, E, E
5. C, C, E
6. C

Protocolos VPN

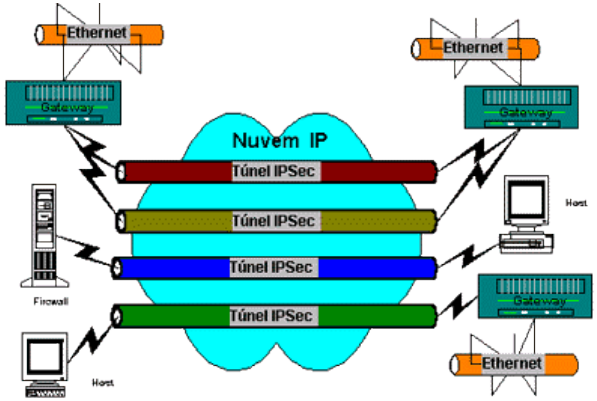


IPSec



- Padrão de fato das VPNs
- É parte majoritária do IPv6, opcional para o uso com IPv4
- Pré-requisito: o TCP/IP
- Provê
  - Confidencialidade (DES CBC)
    - Criptografia apenas para dados em trânsito
    - Criptografia simétrica por causa do desempenho
  - Integridade e autenticidade (HMAC + MD5 ou SHA-1)
    - Contra modificações não autorizadas, sejam elas acidentais ou intencionais

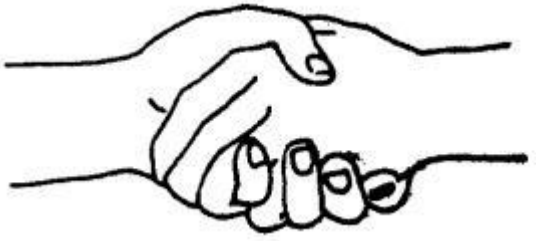
IPSec



- Por questões de interoperabilidade, qualquer implementação IPSec deve suportar
  - MD5 ou SHA-1
  - DES-CBC, Null Authentication Algorithm e Null Encryption Algorithm
- Independente de algoritmos específicos
- Não é um protocolo isolado pois oferece vários algoritmos de segurança
- Projeto prevê níveis de granularidades variados

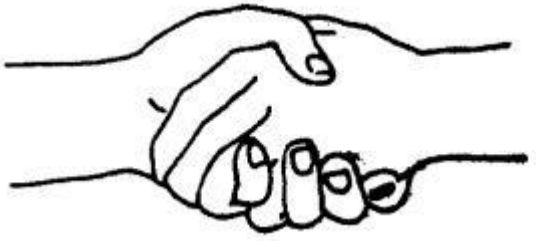
Associações de segurança

- IPSEC - Orientado a conexão
  - SA - Associação de segurança
- Conexão SIMPLEX entre dois pontos com identificador de segurança associado
  - Unidirecional
  - Para cada associação existem 2 SAs
  - Opções podem ser assimétricas
- Destino pode especificar o tempo de vida de uma SA e reusar o índice de parâmetros de segurança
  - Índice tem valor local no destino



Associações de segurança

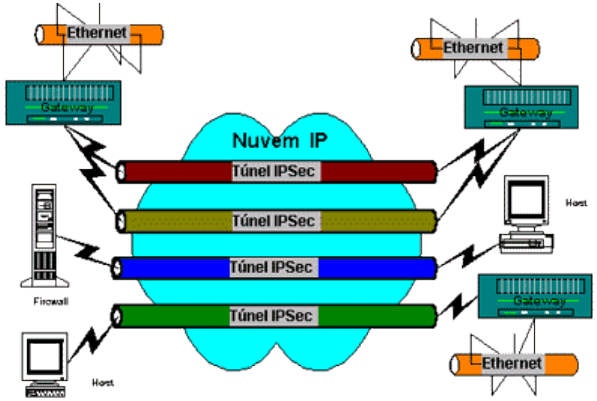
- Segurança na certificação digital e chaves
  - Canal seguro deve ser estabelecido antes da troca da chave ou de arquivo de configuração
  - Se não for possível, aconselha-se o uso de canais diferentes (telefone para chave / e-mail para arquivos de conf)
  - Roubo do equipamento do usuário
  - Roubo do disco rígido
  - Envio de aparelho para assistência técnica (arquivos config e chaves)



Associações de segurança

- Pode usar ESP ou AH mas não os 2
  - Para isso são necessários 2 Sas
- SA = Security parameter Index + IP de destino do pacote + AH ou ESP
  - SPI = 32 bits
  - AH ou ESP definido pelo identificador

IPSec

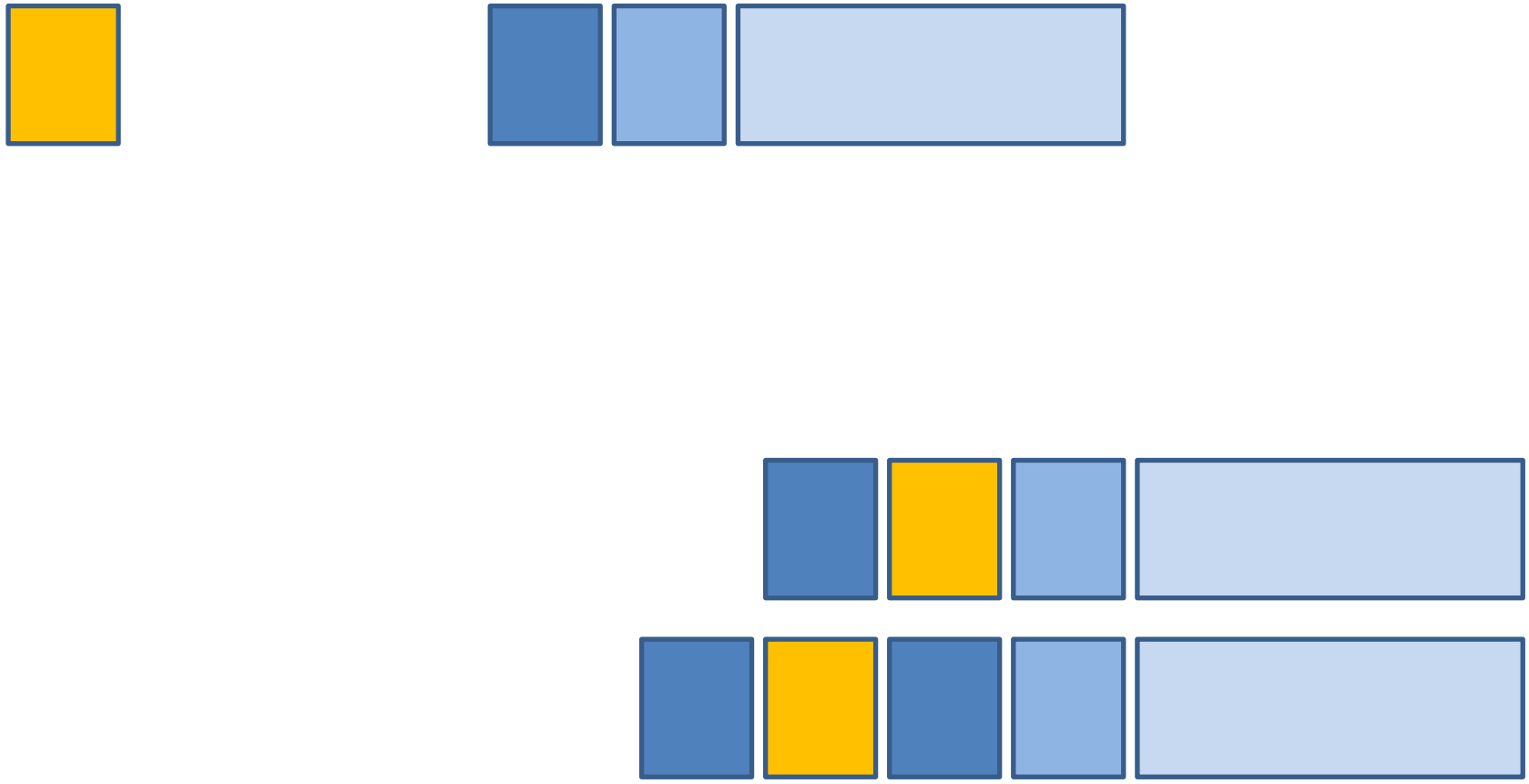


- Estabelecimento das chaves
  - Manual
  - Automático
    - OBS: IKE não é obrigatório, apenas recomendável
- Como os firewalls se destinam principalmente a questão da segurança, é natural fazer os túneis começarem e terminarem nos firewalls
- Projeto prevê níveis de granularidades variados
- Dividido em duas partes
  - Dois Cabeçalhos
  - ISAKMP (Internet Security Association and Key Management Protocol)

Cabeçalhos x Modos

- Cabeçalhos
  - ESP
  - AH
- Modos
  - Transporte
  - Túnel

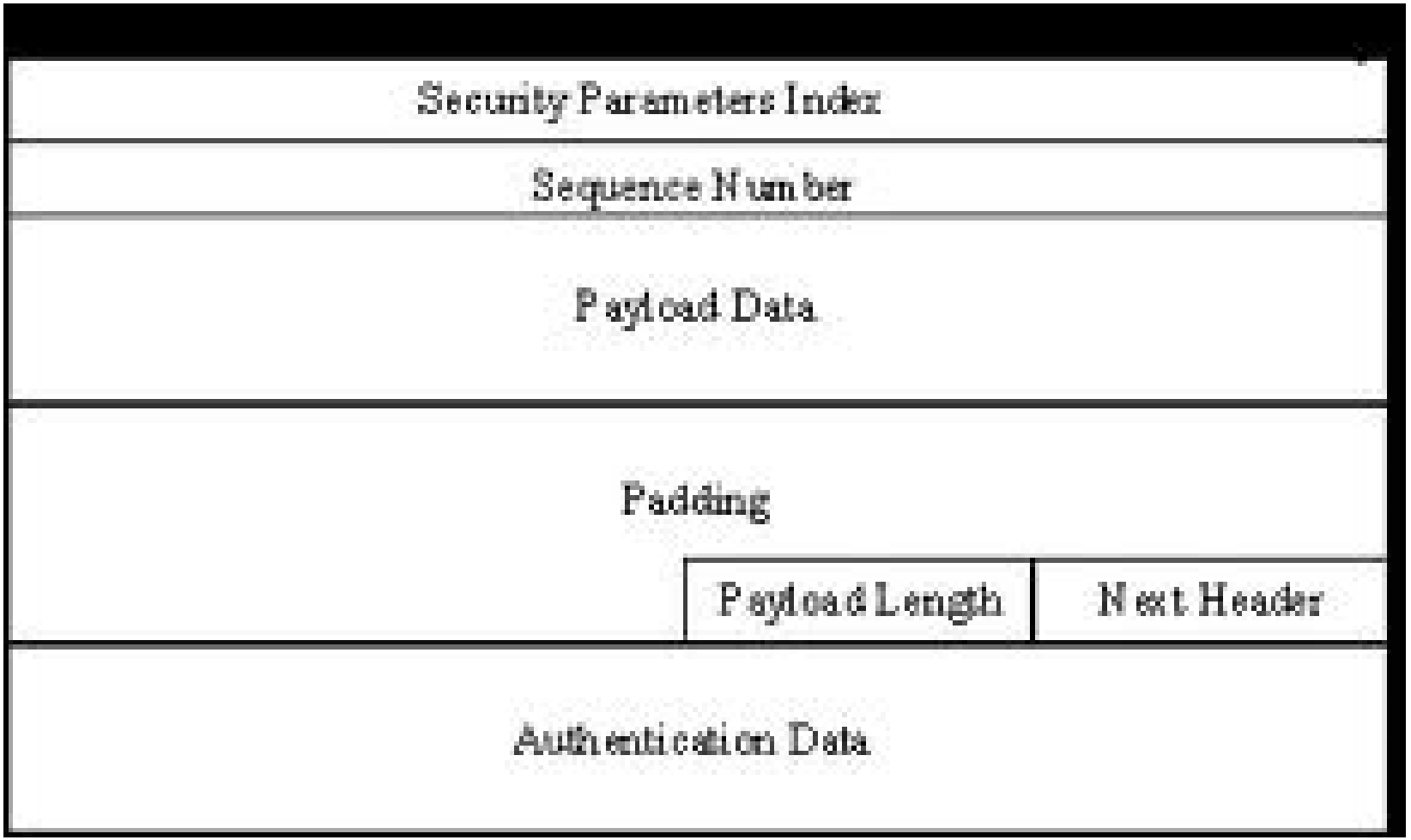
Cabeçalhos x Modos



Cabeçalhos - ESP

- Serve para autenticar e criptografar
  - Sigilo não engloba o cabeçalho nem os dados de autenticação
- Valor 50 no cabeçalho IP
- Autenticação OPCIONAL
- Integridade via HMAC
  - Chave compartilhada entra no cálculo da assinatura (Chave + hash)
  - Abrange os campos do cabeçalho que não se alteram
  - informação Incluída no trailler
    - Maior vantagem nas implementações em hardware
    - HMAC pode ser calculado a medida que os bits saem pela interface de rede e são acrescentados ao final
  - NÃO encapsula o cabeçalho IP mais externo

Cabeçalhos - ESP



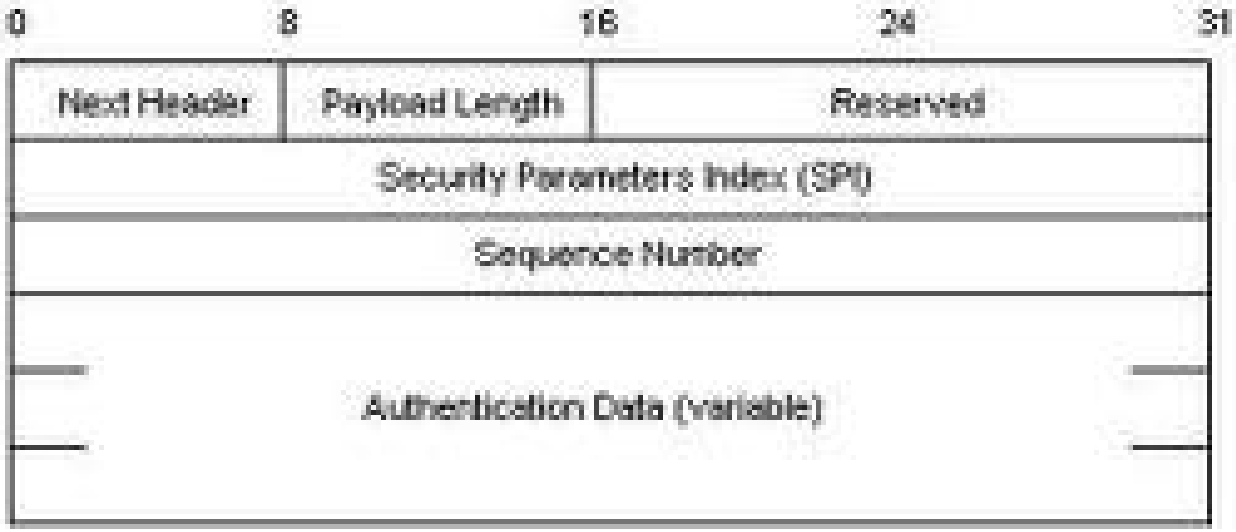
Suporte mínimo – ESP

- RFC 2406 impõe que deve haver suporte para
  - DES in CBC mode
  - HMAC with MD5
  - HMAC with SHA-1
  - NULL Authentication algorithm
  - NULL Encryption algorithm

Cabeçalhos - AH

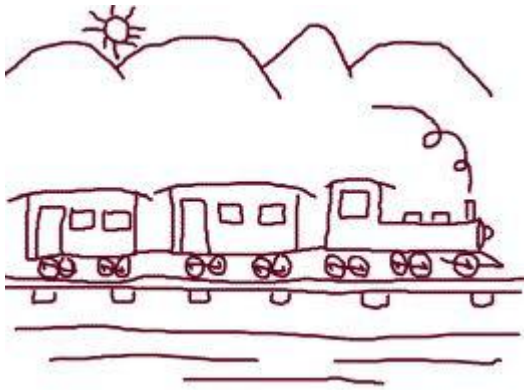
- Não oferece sigilo (SEM CRIPTOGRAFIA)
- Integridade via HMAC
  - Chave compartilhada entra no cálculo da assinatura (Chave + hash)
  - Abrange os campos do cabeçalho IP que não se alteram
  - informação Incluída no cabeçalho
  - Assinatura calculada ANTES do envio do pacote
- Serve basicamente para autenticar o remetente
  - Autenticação alcança o cabeçalho externo
- Valor 51 no cabeçalho IP

Cabeçalhos - AH

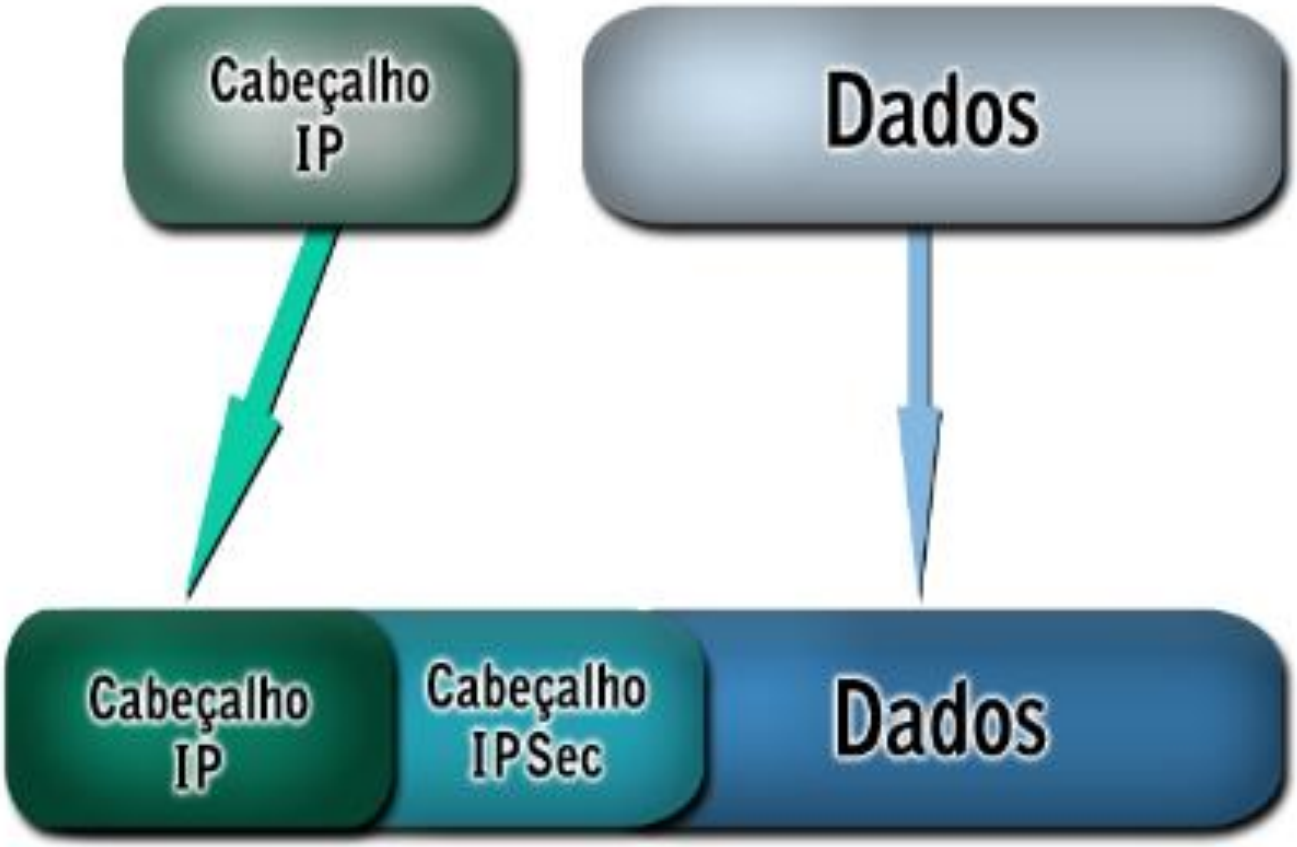


Modos de Operação - Transporte

- Transporte
  - Somente a mensagem (payload) é encapsulada
  - Usado para comunicações de host-a-host / fim-a-fim
  - Cabeçalho é posto entre cab IP original e transporte
  - Afeta pouco o tamanho do pacote
  - Campo Protocol do Ip é alterado para
    - 50 - ESP
    - 51 - AH
    - Valor substituído migra para o cabeçalho IPSec
  - Modo nativo



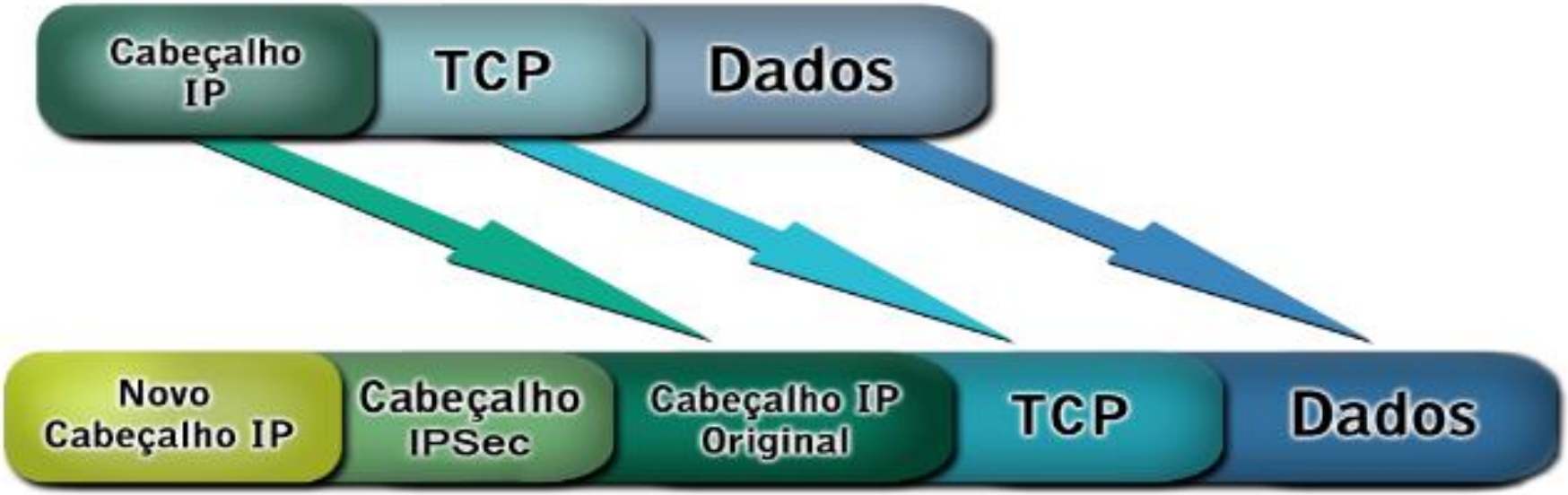
Modo Transporte



Modos de Operação - Túnel

- Pacote IP é encapsulado por inteiro
- Adição de novo cabeçalho IP
- Cabeçalho IPSEC é posto entre o novo cabeçalho e o cabeçalho Ip original
- Útil quando o túnel termina antes do destino final
  - Geralmente máquinas de gateway de segurança (firewall)
  - Ips de origem e destino são dos extremos do túnel, não dos hosts
- Útil na agregação de conexões TCP, diminuindo as informações para análise de tráfego
- Afeta bastante o tamanho do pacote pois acrescenta um novo cabeçalho IP
- Geralmente usado por gateways IPSec, que manipulam o tráfego IP por hosts que não aceitam IPSec
- Garante Confidencialidade do fluxo de tráfego
- Ips da origem e destino mascarados

Modo Túnel



VPN - Ataques / Vulnerabilidades

- Cliente VPN como gateway
  - Uma conexão do computador cliente conectado à internet e outra com o túnel IPSEc
  - Se o cliente tiver capacidade de roteamento os pacotes são redirecionados para o túnel IPSec
    - Nem todo SO suporta
  - Uso do source routing
- Controle da máquina do usuário
- Vírus e cavalos de Tróia
- Compartilhamento de arquivos do Windows
- Conexão ao aparelho via modem

ITnerante

SSL / TLS

- Inicialmente desenvolvido pela Netscape
  - Transações comerciais on-line
- Situa-se na camada de API socket, ou seja, entre a camada de transporte e de aplicação
  - Independe de protocolo de aplicação
  - Independe de protocolo de Transporte
- Permite autenticação mútua, sendo o lado servidor OBRIGATÓRIO e o lado cliente OPCIONAL
  - O cliente não é obrigado a ter um certificado digital válido, o servidor sim
- Negociação de algoritmos de criptografia que ambos lados admitam
  - Criptografia apenas para dados em trânsito
- SSL não foi adotado oficialmente pela IETF. Este instituto o tomou como base e construiu o TLS
- TLS e SSL usam a mesma porta e a maioria das implementações SSL admite TLS

SSL / TLS

- Constrói conexão segura incluindo:
  - Negociação de parâmetros entre cliente e servidor.
  - Autenticação mútua de cliente e servidor. (certificação digital)
  - Comunicação secreta. (criptografia simétrica)
  - Proteção da integridade dos dados. (hash)
- Representado pelo cadeado no browser
- Sessão SSL: Associação estabelecida entre um cliente e um servidor através de uma sequência de handshakes
  - Não confundir com conexão SSL
  - As conexões podem ser criadas com base um uma sessão já estabelecida, poupando um novo handshake
  - Cada sessão pode conter uma ou mais conexões
- O uso de HTTPS assegura uso de certificados digitais - pelo menos o lado servidor

Versões

- SSLv1
- SSLv2
- SSLv3 / TLS 1.0
  - versão predominante
  - Permite que qualquer das partes solicite novo handshake em qualquer momento da sessão (renegociação de chaves e cifragens)
  - Fornece compactação de dados (opcional)
  - mecanismo de Diffie-Hellman
  - uso de certificados Não-RSA
  - Capacidade de envio de cadeias de certificados (Push)

TLS x SSL – Não interoperam

- SSLv3
- Permite apenas conexões seguras
- começam com segurança e avançam diretamente para comunicações seguras

- TLSv1 (SSLv3.1)
- Permite conexões seguras e inseguras na mesma porta
- TLS primeiro começa com uma insegurança, e só muda para comunicações seguras após o handshake entre o cliente e o servidor ser bem sucedido
- TLS é mais extensível e provavelmente será mais amplamente apoiada no futuro com os padrões da Internet
- Para usuários que se conectam a um servidor de e-mail via POP ou IMAP, isso significa que o uso de TLS lhe permitirá optar por conexões seguras, mas facilmente mudar para conexões não seguras, se necessário, sem necessidade de alterar as portas. Isso não é possível com SSL

TLS x SSL – Curiosidades

- TLS Versão 1 teve sua quebra prometida em setembro 2011
  - Thai Duong e Juliano Rizzo
  - O TLS 1.0 é vulnerável
  - Até hoje não se ouviu falar no assunto
- TLS 1.1 e 1.2 não são suportados por praticamente nenhum navegador

Combinações tradicionais

- RC4 com chave de 128 bits e o MD5. (aplicações comuns de E-Comerce).
- AES ou DES triplo com 3 ch separadas (criptografia) e o SHA-1 (integridade) – op bancárias
- São 31, mas na prática apenas os citados acima

Subprotocolos

- Handshake Protocol
  - Constrói conexão segura incluindo:
    - Negociação de parâmetros entre cliente e servidor.
    - Autenticação mútua de cliente e servidor. (assinatura digital)
    - Comunicação secreta. (criptografia)
      - Chave para dados do cliente
      - Chave para dados do servidor
    - Proteção da integridade dos dados. (hash)
      - Chave para HMAC do cliente
      - Chave para HMAC do servidor
    - Handshake em qualquer momento, permitindo renegociação de chaves e cifragens

Handshake Protocol - Passos

1 - Cliente envia um número aleatório (nonce) e uma lista de cifras e métodos de compressão que estaria apto a negociar com o servidor (mensagem CLIENT_HELLO).

2 - Servidor retorna seu número aleatório (nonce) e a cifra e método de compressão selecionados (mensagem SERVER_HELLO).

3 - Servidor envia seu certificado, o qual conterá sua chave pública (SERVER_CERTIFICA TE). O tipo de certificado enviado dependerá da cipher suite negociada.

4 - Caso seja necessária a autenticação do cliente, o servidor envia um pedido de certificado ao cliente (mensagem CERTIFICATE_REQUEST) e sinaliza ao cliente que a fase de HELLO está finalizada (mensagem SERVER_HELLO_DONE). Servidor avisa ao cliente que agora é a vez dele.

5 - Cliente responde escolhendo ao acaso uma chave pré-mestre de 384 bits e envia ao servidor (codificada com a ch pública do servidor). a chave de sessão real usada para codificar os dados é derivada da chave pré-mestre combinada com ambos os nonces.

6 - Cliente informa ao servidor que deve passar para a nova cifra.

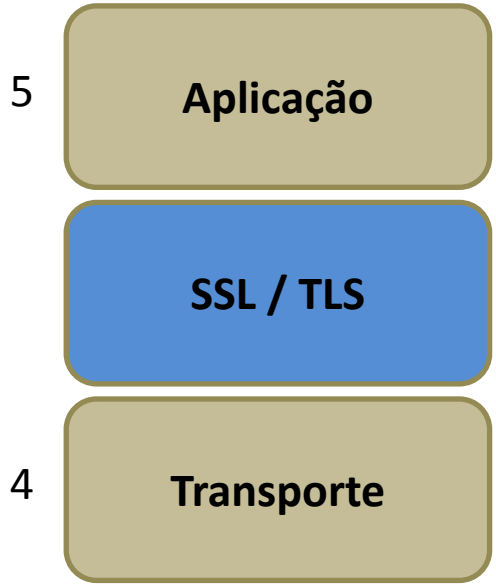
7 - Ambos os lados possuem agora as chaves de sessão a serem utilizadas. Uma última mensagem é enviada (mensagem FINISHED - já decifrada com os segredos negociados) por ambas as partes, checada (a fim de evitar ataques por espelhamento) e o processo de handshake é finalizado.

Subprotocolos

- Alert Protocol
  - Envia mensagens de alerta sobre erros ou avisos
    - Fatal
    - Warning
  - Evita ataques de truncamento (TCP FIN antecipado) com o alerta CLOSE_NOTIFY
  - Mensagens sobre status do certificado (revoked, expired, unknow)

- Record Protocol
  - Transferência de dados
  - Depois que a conexão segura é estabelecida, a principal tarefa da SSL é manipular a compactação e a criptografia

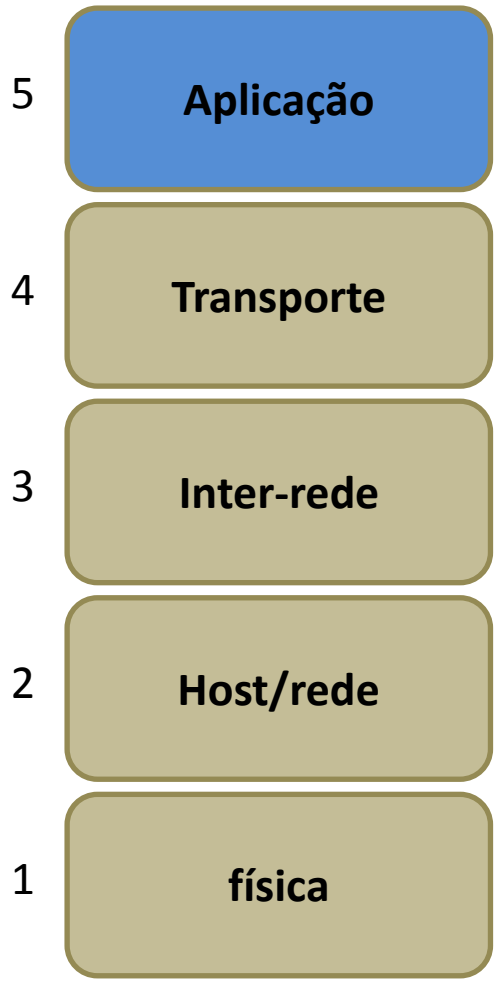
Raio-x do SSL / TLS



1. Divisão do fluxo da camada de aplicação em blocos de texto simples (registros) de no máximo 16K
2. OPCIONALMENTE há a compactação de dados
3. Cálculo de um MAC para cada registro
4. Encriptação dos Textos (criptografados ou não) com os respectivos MACs através do uso da chave de sessão. Tamanho Máximo do registro de 1024 bytes
5. Inserção de um cabeçalho SSL em cada registro

SSH – Secure Shell

- Protocolo da camada de aplicação
- Possibilita conexões remotas como o Telnet, só que de forma criptografada
- Muito usado em administração remota Unix like
- Interface de terminal
- Porta 22



Bateria de questões de aprendizagem

Virtual Private Network – MPLS, IPSec, SSL/TLS

ITnerante

CORREIOS – CESPE 2011 – Analista de Correios – Suporte a Sistemas

1. Acerca de algoritmos de criptografia e protocolos, julgue os itens subsecutivos

[97] O protocolo IPSEC possui a capacidade de esconder os endereços IPs internos, pois suporta o recurso chamado NAT (network address translation).

[98] Um servidor SSH (secure shell) que esteja rodando em um sistema operacional GNU/Linux suporta o algoritmo RSA para geração de chaves de autenticação, mas esse servidor falha caso se utilizem chaves ou o algoritmo DSA.

[99] O IPSEC é muito utilizado em conexões VPN (virtual private network), pois é capaz de validar a integridade e a confidencialidade das informações trafegadas na VPN, por meio da utilização do AH (autentication header) e do ESP (encapsulating security payload).

[100] O protocolo SSL, muito utilizado na camada física do protocolo TCP/IP, foi desenvolvido para a segurança entre aplicações

MPU – CESPE 2010 – Analista DE Informática – Suporte técnico

2. Acerca de VPN (virtual private network) e VPN-SSL (VPN secure sockets layer) e seus protocolos, julgue os itens subsequentes.

[143] Em redes VPNs-SSL, o protocolo SSL é usado tanto para a comunicação host a host quanto entre host e cliente. Em ambos os casos, o IPSec (Internet protocol security) provê serviço de encriptação dos dados transmitidos.

[144] Nas VPNs, antes de serem encapsulados dentro de outro, no processo de tunelamento, os pacotes são criptografados com o objetivo de torná-los indecifráveis, caso sejam interceptados maliciosamente durante o seu transporte.

TRT 23 – FCC 2011 – Analista Judiciário – Tecnologia da Informação

3. O protocolo de segurança IP, mais conhecido por IPSec, fornece dois modos de operação, a saber:

a. Autenticação e Encapsulamento.
b. Autenticação e Encriptação.
c. Encriptação e Chaveamento.
d. Chaveamento e Tunelamento.
e. Transporte e Tunelamento.

TRT 4 – FCC 2011 – Técnico Judiciário – Tecnologia da Informação

4. Em relação a ferramentas de segurança utilizadas em uma rede de computadores é INCORRETO afirmar:

a. O SSL (Secure Socket Layer) é executado entre a camada de transporte e de aplicação do TCP/IP.
b. IDS (Intrusion Detection System) refere-se a meios técnicos de descobrir a existência de acessos não autorizados em uma rede.
c. No modo túnel do IPSec (IP Security Protocol), um IDS pode verificar somente o cabeçalho do pacote.
d. No modo de transporte, o IPSec cuida da proteção ou autenticação somente da área de dados do pacote IP.
e. No modo túnel do IPSec, o pacote IP inteiro é criptografado e encapsulado.

TRT-RN – FCC 2011 – Analista Judiciário – Analista de Sistemas

5. O IPSec fornece uma função combinada de autenticação e criptografia denominada

a. Authentication Header.
b. Key Changing.
c. Header Encapsulating.
d. Encapsulating Security Payload.
e. Auto Encryption.

TRT 16 – FCC 2009 – Técnico Judiciário – Tecnologia da Informação

6. O protocolo de segurança IP (IPSec)

a. é obrigatório tanto no sistema de endereçamento IPv4 quanto no IPv6.
b. no modo transporte é usado para comunicações de host-a-rede e de host-a-host sobre a internet.
c. não pode ser usado protegendo os protocolos TCP e UDP.
d. não provê confidencialidade dos dados com o cabeçalho de autenticação (AH).
e. não provê integridade das mensagens com o Encapsulating Security Payload (ESP).

CORREIOS – CESPE 2011 – Analista de Correios – Engenharia de redes de comunicação

7. Algumas técnicas de construção de túneis, nas quais se adota o conceito de redes privadas, utilizam MPLS. Acerca dessas técnicas, julgue os itens a seguir

[86] Considera-se VPN MPLS uma tecnologia orientada a conexão, de acordo com os modelos comuns de VPN.

[87] Uma característica de funcionamento de túneis embasados em VPN MPLS é o isolamento do tráfego por VLAN, padrão IEEE 802.1Q, antes de o tráfego entrar no roteador.

[88] Uma VPN MPLS, por padrão, isola o tráfego, a fim de garantir que os dados transmitidos por meio de um túnel MPLS estejam cifrados.

[89] Uma vez que uma VPN MPLS pode ser vista como uma intranet privada, é possível a utilização de serviços IP, como o multicast.

Gabarito

1. E, E, C, E
2. E, E
3. E
4. C
5. D
6. D
7. E, E, E, C