Redes de Computadores

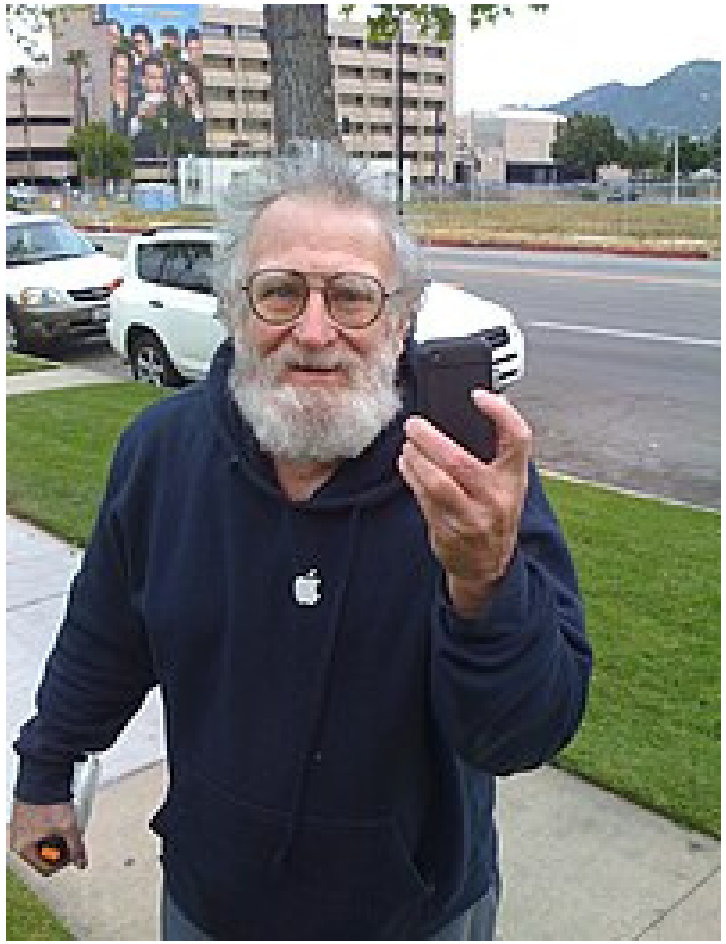
Marisangila Alves, MSc

marisangila.alves@pronton.me

Introdução a Segurança de Redes

Um pouco de história...

- Invasão de rede já existia antes da Internet.
- Rede de telefônia era alvo de ataques.
- John Draper.



Um pouco de história...

John Thomas Draper:

- Quem é John Draper:
  - Nascido em Las Vegas, em 11 de março de 1943.
  - Hacker e programador norte-americano.
- Criação do Conceito de "*Phreaking*":
  - Desenvolveu a técnica de *phreaking*, que consistia em manipular sistemas telefônicos para fazer ligações gratuitas.
  - Usou um apito de plástico (oferecido como brinde em um cereal) para reproduzir o tom de 2600 Hz.

Um pouco de história...

- O tom de 2600 Hz permitia acessar diretamente os satélites usados para chamadas de longa distância.
- Com isso, era possível fazer chamadas sem pagar pela ligação.
- O uso de *phreaking* por Draper forçou os Estados Unidos a alterar a sinalização de controle em seus sistemas de telefonia.
- Draper ficou conhecido como Capitão Crunch ou Crunchman.
- O apelido veio do Cap'n Crunch, mascote de um cereal, de onde ele encontrou o apito usado para *phreaking*.

Um pouco de história...

- Em 1972, Draper foi preso por fraude relacionada ao *phreaking*.
- Condenado a cinco anos de prisão.
- Durante os anos 1970, Draper ensinou suas habilidades de phone *phreaking* a dois jovens: **Steve Jobs e Steve Wozniak.**
- Jobs e Wozniak, mais tarde, fundaram a **Apple Computer.**
- Draper foi brevemente empregado pela Apple.
- Criou uma interface telefônica para o Apple II.

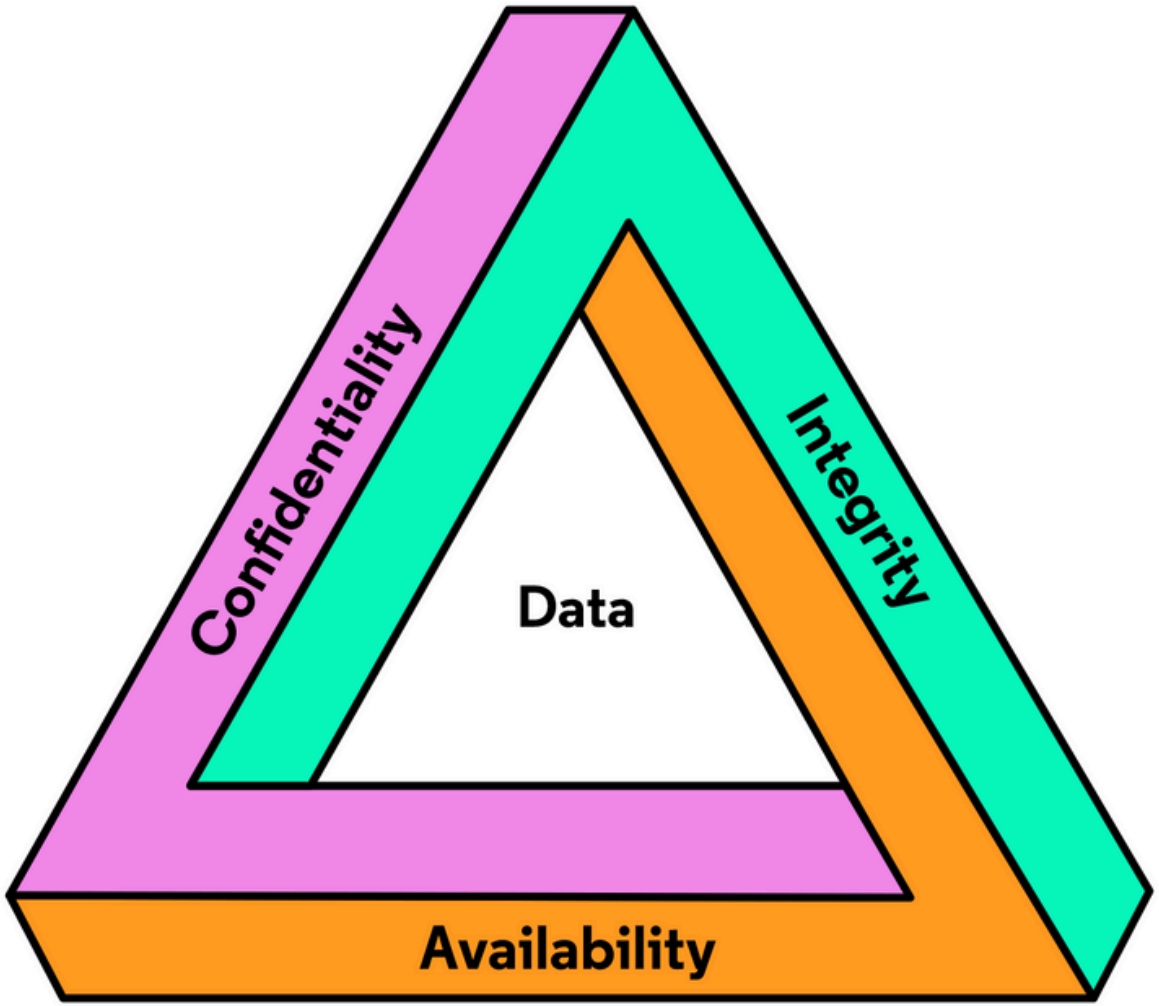
O que é

Cybersecurity é um conjunto de ferramentas, políticas, conceitos e salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e os recursos do usuário (ITU, 2009).

Em resumo ...

Cibersegurança é a proteção de **sistemas**, **dispositivos** físicos, **processos** organizacionais e **pessoas** contra ameaças, garantindo a segurança de **informações**.

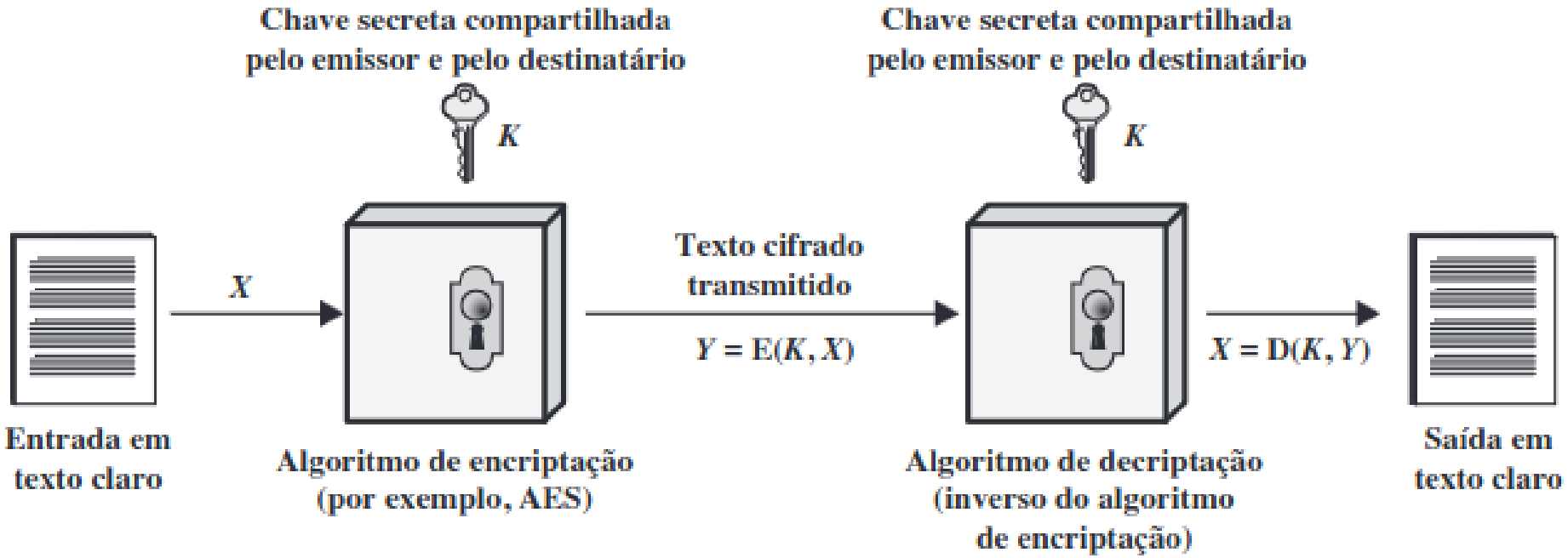
TRIADE CID



CONFIDENCIALIDADE

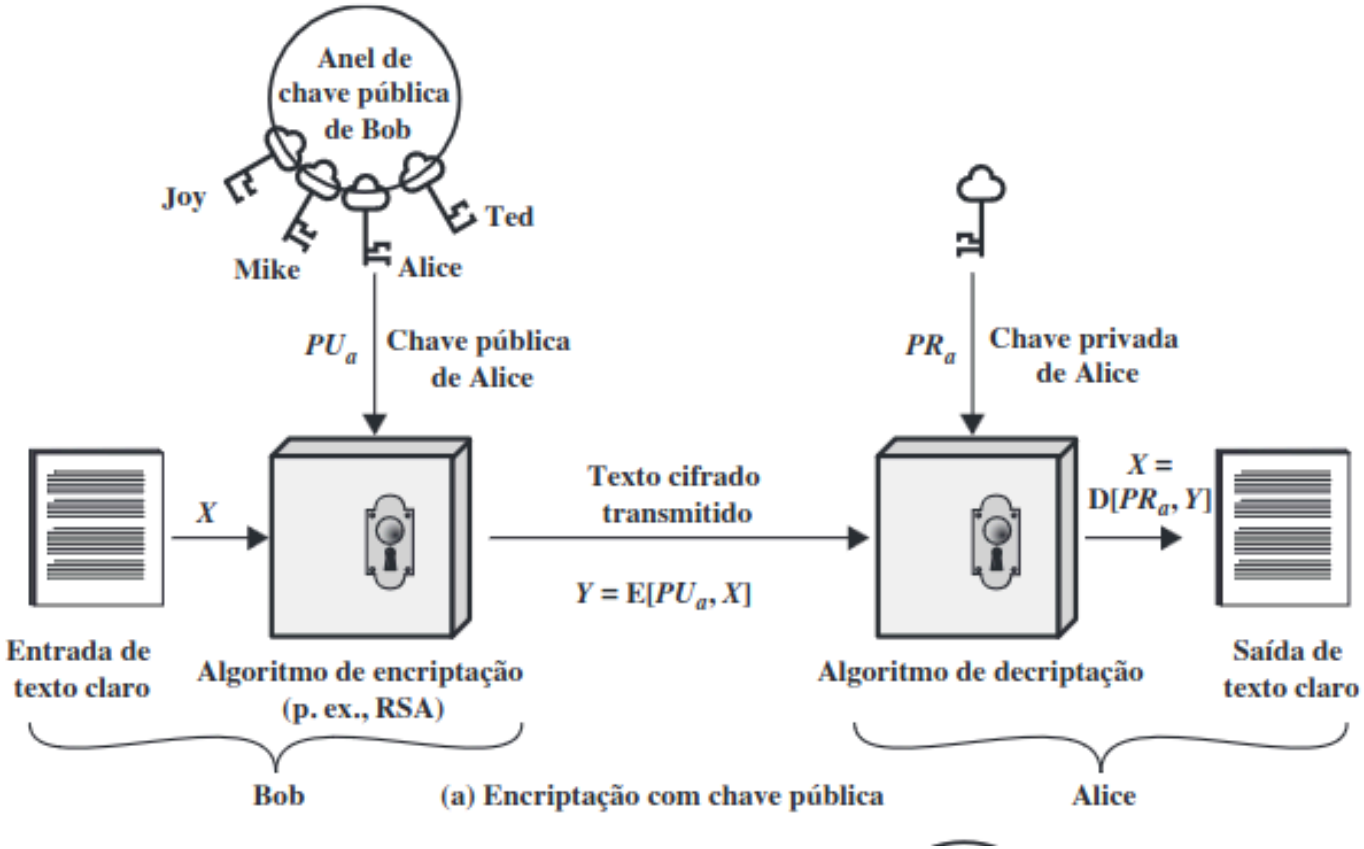
Confidencialidade em cibersegurança significa garantir que apenas indivíduos autorizados possam acessar informações sensíveis.

Criptografia Simétrica



Fonte: Stallings

Criptografia Assimétrica



Fonte: Stallings

CONFIDENCIALIDADE

- Criptografia de Dados;
- Controle de Acesso;
- VPN (*Virtual Private Network*);
- Segurança Física;
- Anonimização de Dados.

INTEGRIDADE

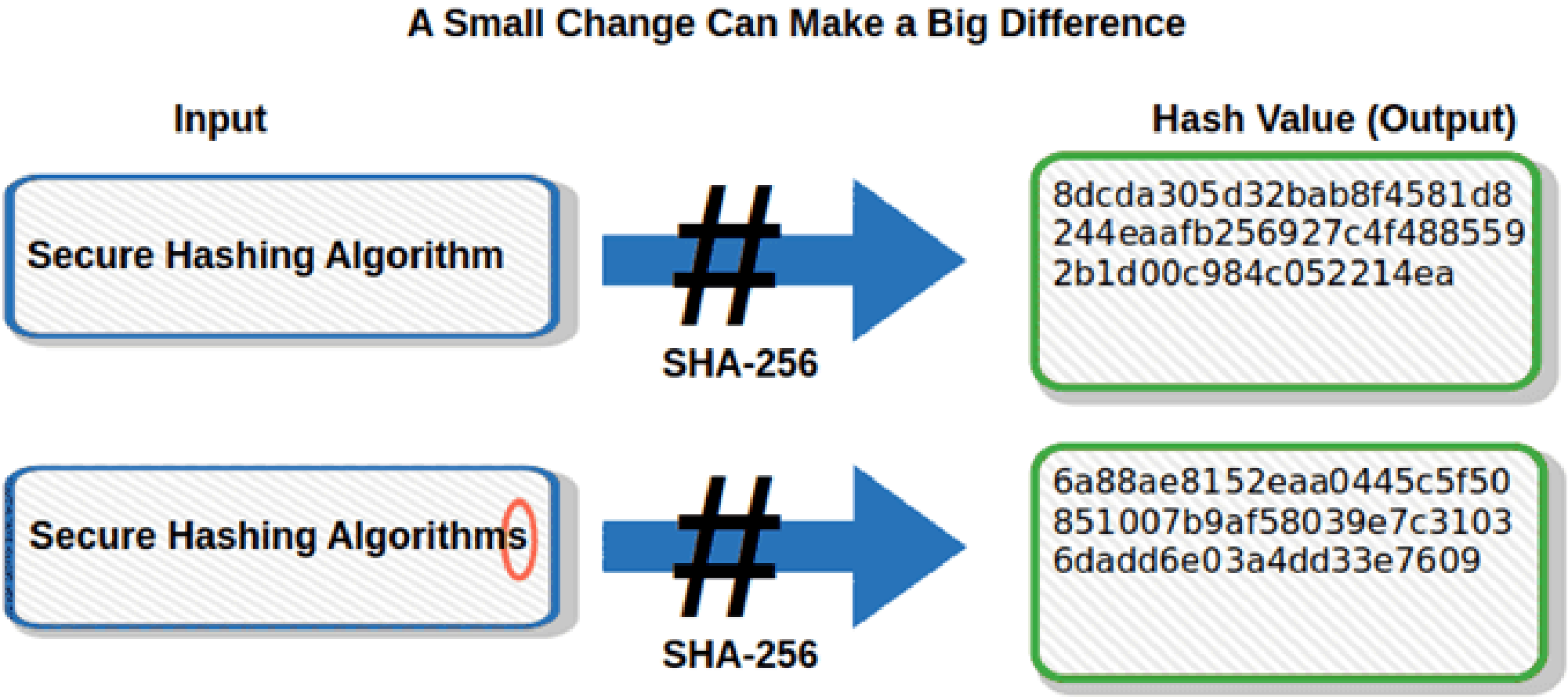
Integridade em cibersegurança envolve garantir que os dados e sistemas permaneçam completos, precisos e livres de alterações não autorizadas.

- Integridade de dados.
- Integridade de sistemas.

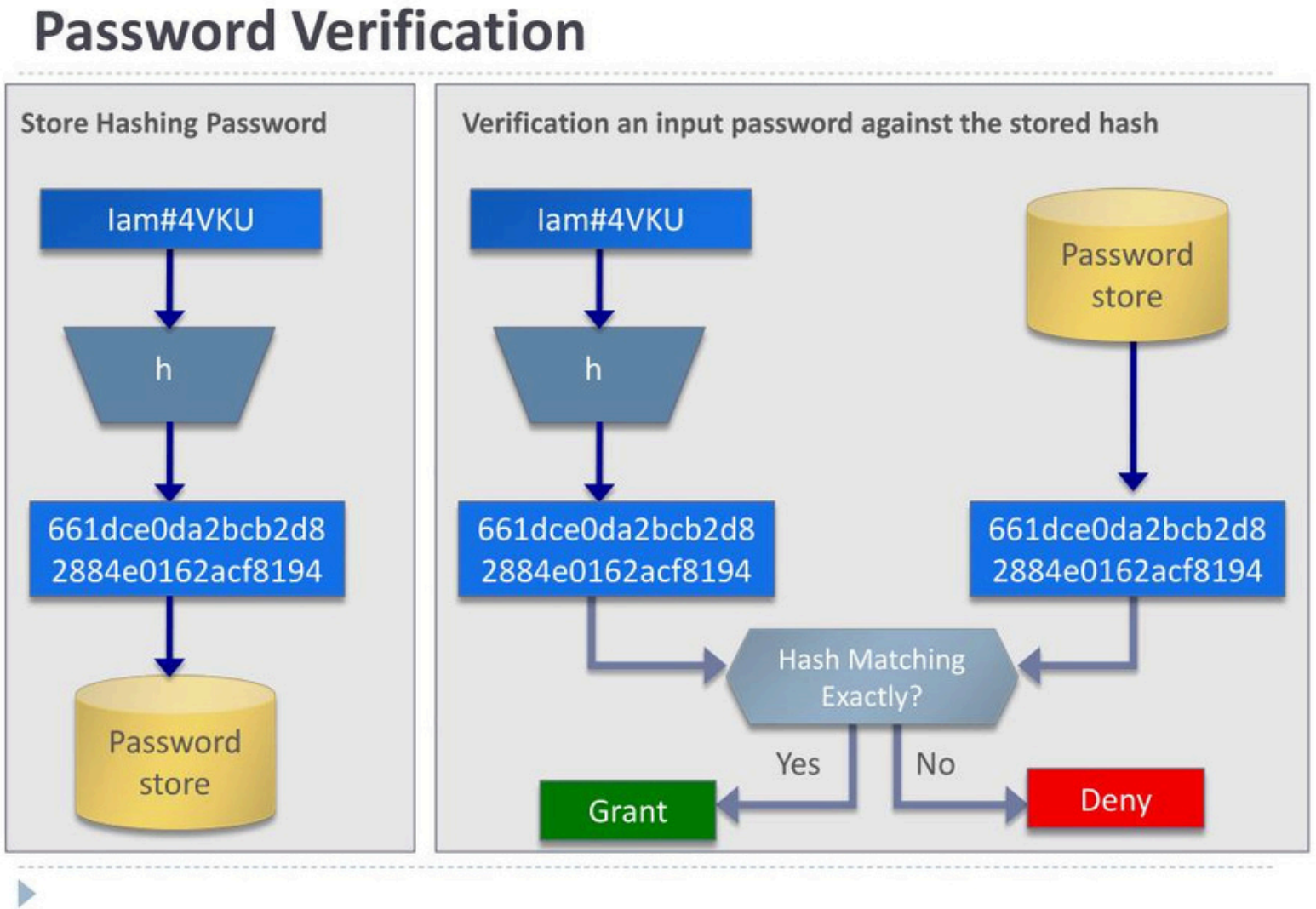
Hashing

Um hash garante integridade ao gerar um valor único e fixo para os dados, permitindo verificar se os dados foram alterados comparando o hash original com o recalculado.

Hashing


A Small Change Can Make a Big Difference
Input
Hash Value (Output)
Secure Hashing Algorithm
SHA-256
8dcda305d32bab8f4581d8
244eaafb256927c4f488559
2b1d00c984c052214ea
Secure Hashing Algorithms
SHA-256
6a88ae8152eaa0445c5f50
851007b9af58039e7c3103
6dadd6e03a4dd33e7609

Hashing


Password Verification
Store Hashing Password
Iam#4VKU
h
661dce0da2bcb2d8
2884e0162acf8194
Password
store
Verification an input password against the stored hash
Iam#4VKU
h
661dce0da2bcb2d8
2884e0162acf8194
Password
store
661dce0da2bcb2d8
2884e0162acf8194
Hash Matching
Exactly?
Yes
No
Grant
Deny

INTEGRIDADE

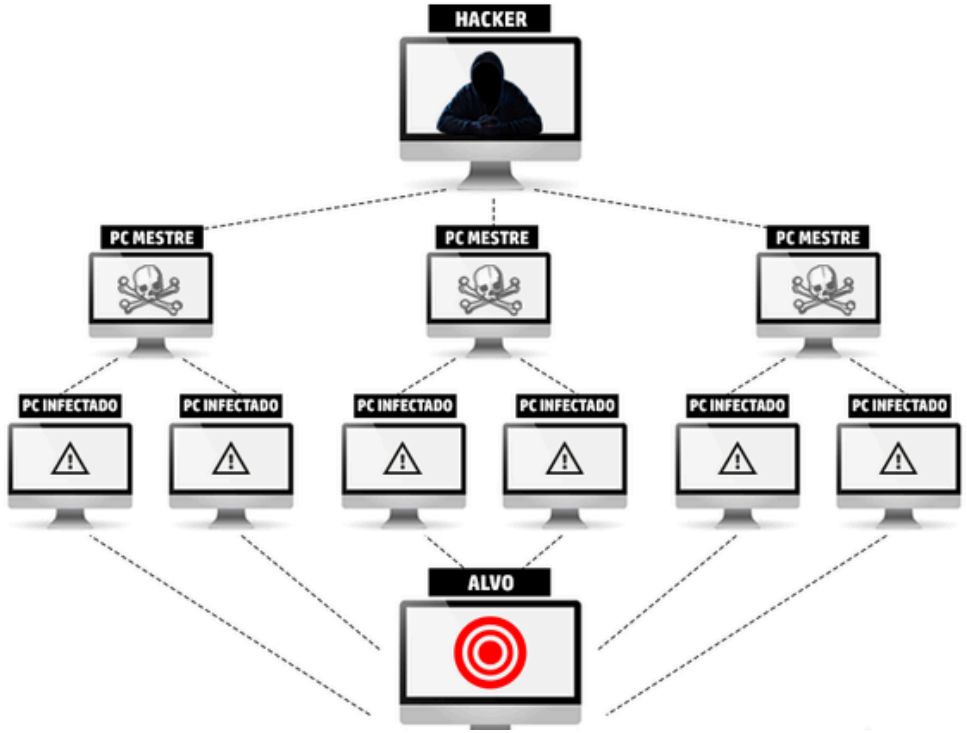
- Assinaturas Digitais;
- Controle de Acesso;
- *Checksums* e *Hashes* ;
- Arquivos de Log.

DISPONIBILIDADE

Disponibilidade em cibersegurança refere-se à garantia de que os sistemas e recursos digitais estejam sempre acessíveis e operacionais quando necessário, evitando interrupções não planejadas.

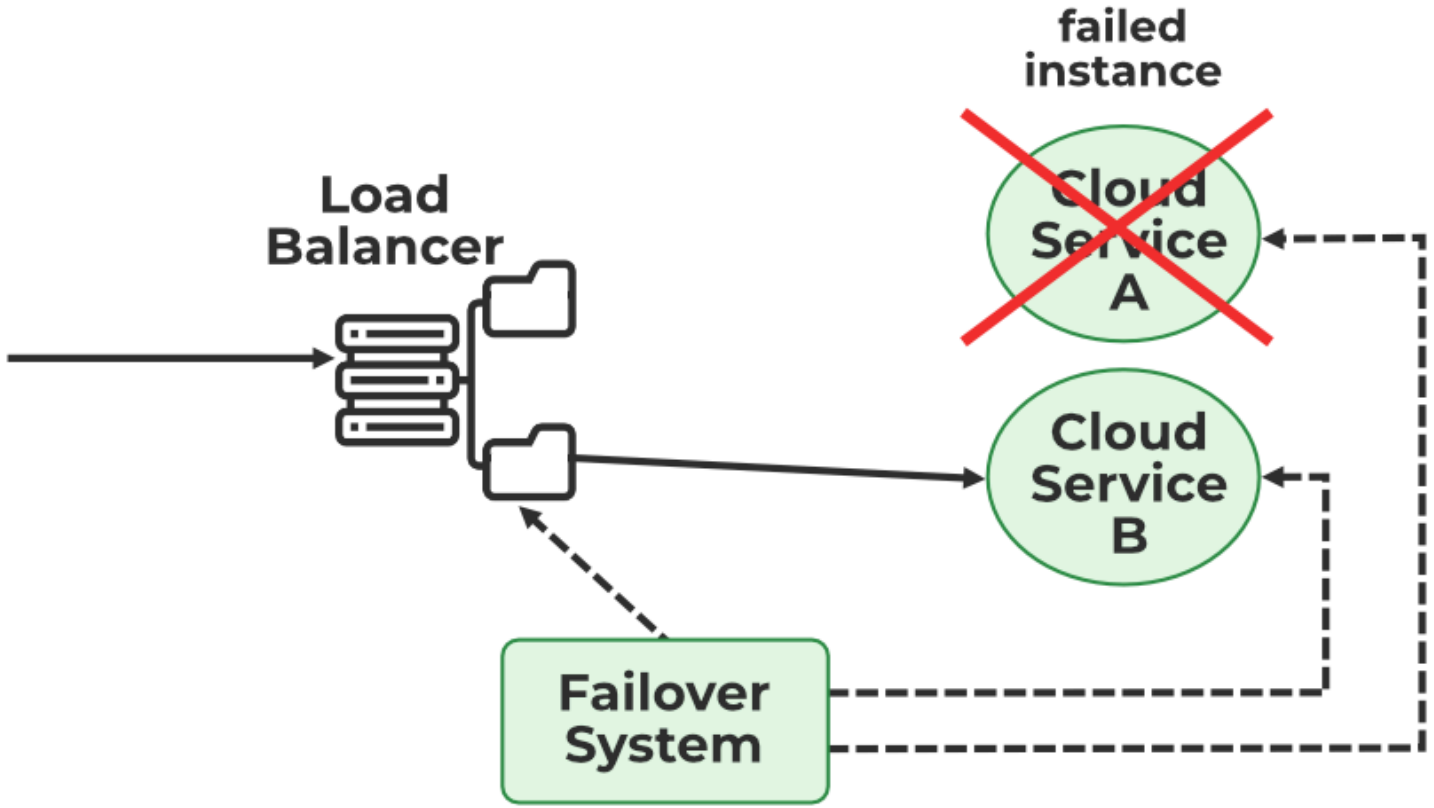
DDOS (*Distributed Denial of Service*)

- Negação de Serviço:
  - DOS (*Denial of Service*);
  - DDOS (*Distributed Denial of Service*).

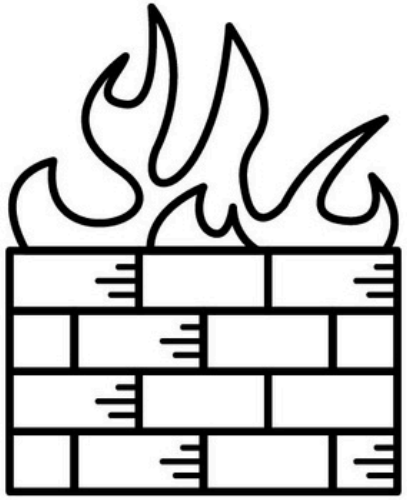


DISPONIBILIDADE

- Balanceamento de Carga;
- Servidores de *Backup (Failover)*.



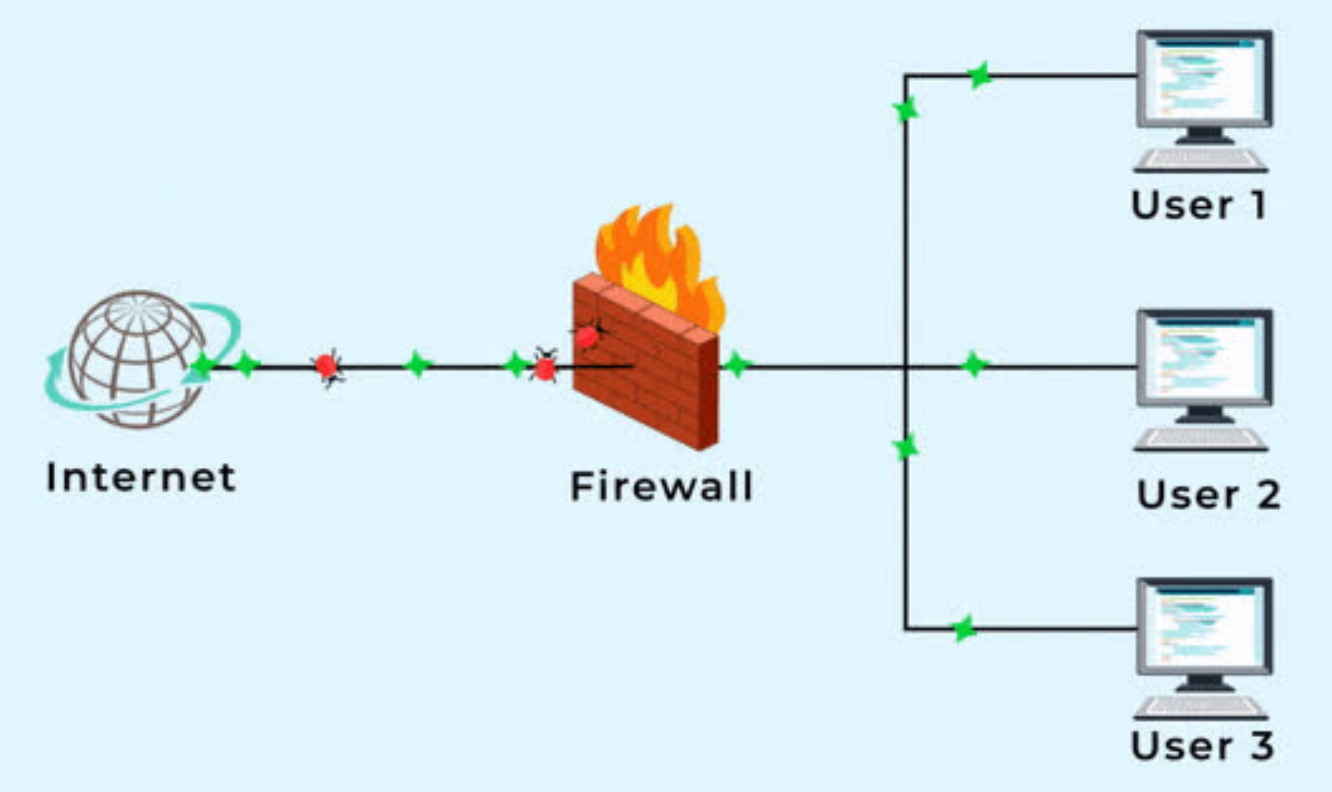
Firewalls



Definição

Os *firewalls* podem ser um meio efetivo de proteger um sistema local ou uma rede de sistemas contra ameaças à segurança baseadas em rede e, ao mesmo tempo, permitir acesso ao mundo exterior via redes de longa distância e Internet.

Firewall



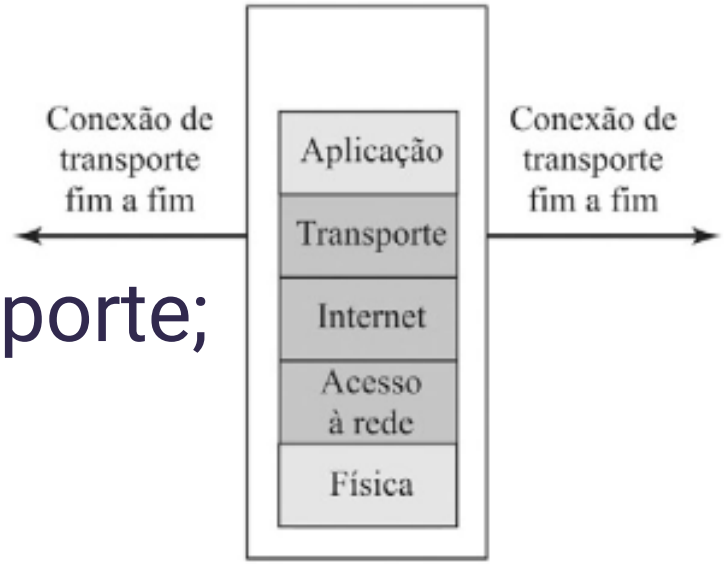
O termo "firewall" em inglês compara a função de evitar a propagação de acessos nocivos dentro de uma rede de computadores à de uma parede anti-chamas.

Metas de projeto de *Firewall*

- Todo tráfego deve passar pelo *firewall*;
- Somente tráfego autorizado;
- O *firewall* não é imune a infiltração.

Firewalls

- ***Firewall* de filtragem de pacotes:**
  - IP destino;
  - IP origem;
  - Endereço de nível de transporte;
  - Campo Protocolo;
  - Interface.



(b) Firewall de filtragem de pacotes

Firewalls

- ***Firewall* de filtragem de pacotes:**
  - Políticas:
    - **Padrão = descartar:** Aquilo que não é expressamente permitido é proibido.
    - **Padrão = transmitir:** Aquilo que não é expressamente proibido é permitido.

Firewalls

- **Padrão = descartar:**
  - Política mais restritiva.
  - Afeta a transparência do *firewall* para usuários da rede.
  - Pode ser usada em redes públicas, como universidades.

Firewalls

- Vantagem: simplicidade.
- Desvantagem: não pode filtrar outras camadas.
    - **Exemplo:** Por exemplo, um *firewall* de filtro de pacotes não é capaz de bloquear comandos específicos de aplicações; se um *firewall* de filtro de pacotes permitir determinada aplicação, todas as funções disponíveis dentro dessa aplicação serão permitidas.

ACL (*Access Control List*)

É uma lista de regras usadas para controlar o tráfego de entrada e saída em dispositivos de rede, como roteadores e *firewalls*.

ACL (*Access Control List*)

Cada regra define quais pacotes de dados são permitidos ou negados, com base em critérios como endereço IP de origem ou destino, protocolo, número de porta e outras informações da camada de rede.

ACL (*Access Control List*)

As regras definem se o tráfego deve ser permitido ou negado.

Principais critérios de filtragem:

- Endereço IP de origem e destino: Define de onde vem e para onde vai o pacote.
- Protocolos: Pode-se especificar protocolos como TCP, UDP, ICMP, etc.
- Portas: Filtragem com base em portas de origem e destino (como HTTP – porta 80, HTTPS – porta 443).
- Exemplo ACL:
  - Permitir que apenas o IP 192.168.1.10 acesse a rede:

```
access-list 1 permit 192.168.1.10 0.0.0.0
```

ACL (*Access Control List*)

Máscara curingas são utilizadas em ACLs.

- As máscaras coringas são o inverso de uma máscara de sub-rede tradicional.
- Ela especifica quais partes de um endereço IP devem ser consideradas na comparação e quais podem variar.
- **Máscara de Sub-rede vs. Máscara Curinga:**
  - A máscara de sub-rede usa o valor 1 para bits da rede (fixos) e 0 para bits do host (variáveis).
  - A máscara coringa faz o oposto: usa 0 para os bits que devem ser comparados e 1 para os bits que podem variar.

ACL (*Access Control List*)

- **Exemplo Prático:**
  - Suponha que você queira criar uma regra ACL que permita tráfego para qualquer endereço IP da faixa 192.168.1.0/24. A máscara coringa seria:
    - **Endereço IP da rede:** 192.168.1.0
    - **Máscara de rede:** 255.255.255.0
    - **Máscara Curinga:** 0.0.0.255

Isso significa que todos os bits dos três primeiros octetos (192.168.1) devem ser comparados exatamente, enquanto o último octeto pode variar de 0 a 255.

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

Firewalls

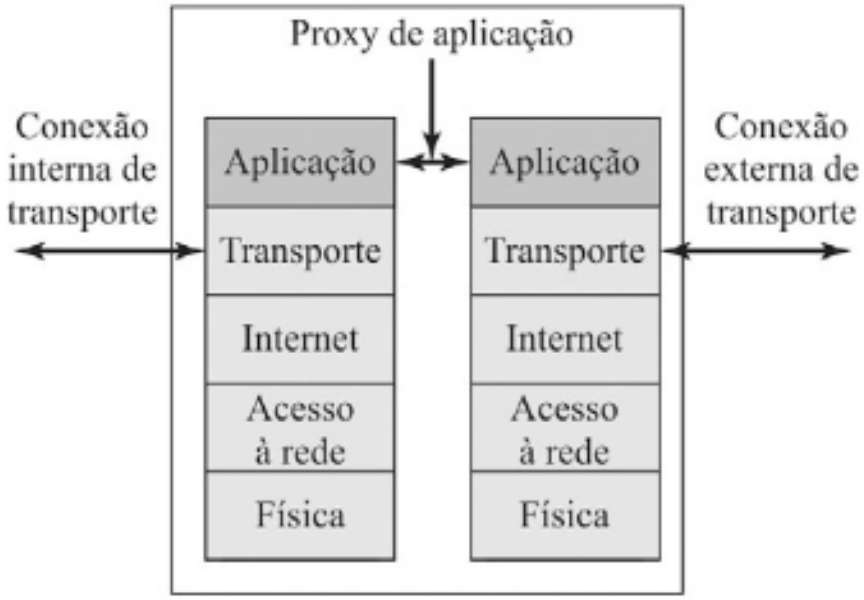
- **Ataques direcionados para *Firewall* de filtragem de pacotes:**
  - **Falsificação de endereço IP:** O intruso transmite pacotes que vêm de fora da rede com um campo de endereço IP de origem que contém o endereço de uma estação interna.
  - A contramedida é descartar pacotes cujo endereço de origem seja interno se esse pacote chegar a uma interface externa.

Firewalls

- **Ataques direcionados para *Firewall* de filtragem de pacotes:**
  - **Ataques de fragmentos minúsculos:** O atacante espera que o *firewall* de filtragem examine apenas o primeiro fragmento e que os fragmentos restantes passem.
  - Um ataque de fragmentos minúsculos pode ser derrotado pela imposição de uma regra que estabelece que o primeiro fragmento de um pacote deve conter uma quantidade mínima predefinida do cabeçalho de transporte.

Firewalls

- **Proxy de aplicação:**
  - Age como um retransmissor de tráfego no nível de aplicação. Um usuário contata o proxy usando uma aplicação TCP/IP.
  - Custo de processamento.
  - Aumento de atraso.

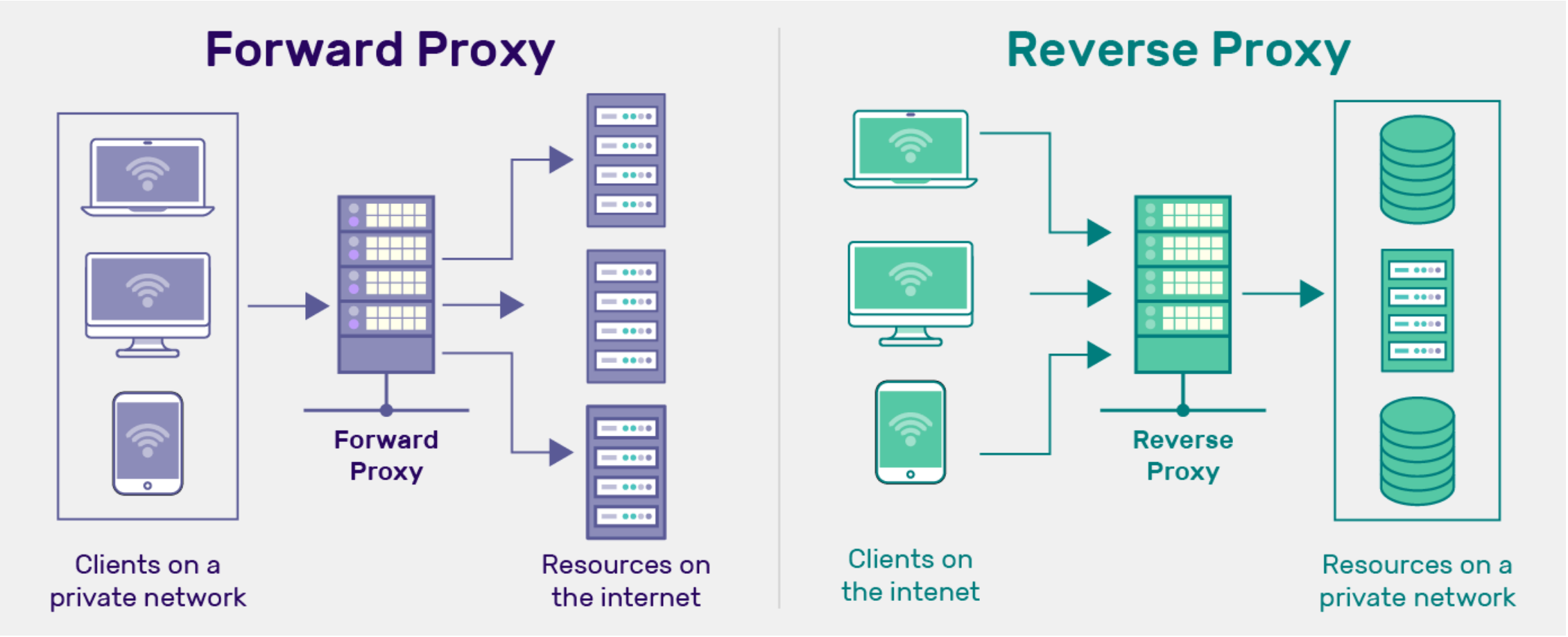


(d) Firewall do tipo proxy de aplicação

Proxy

Atua como um intermediário entre um usuário e a internet, que encaminha solicitações de acesso a recursos na web. Pode **filtrar, monitorar e modificar** o tráfego para melhorar a segurança, privacidade ou desempenho.

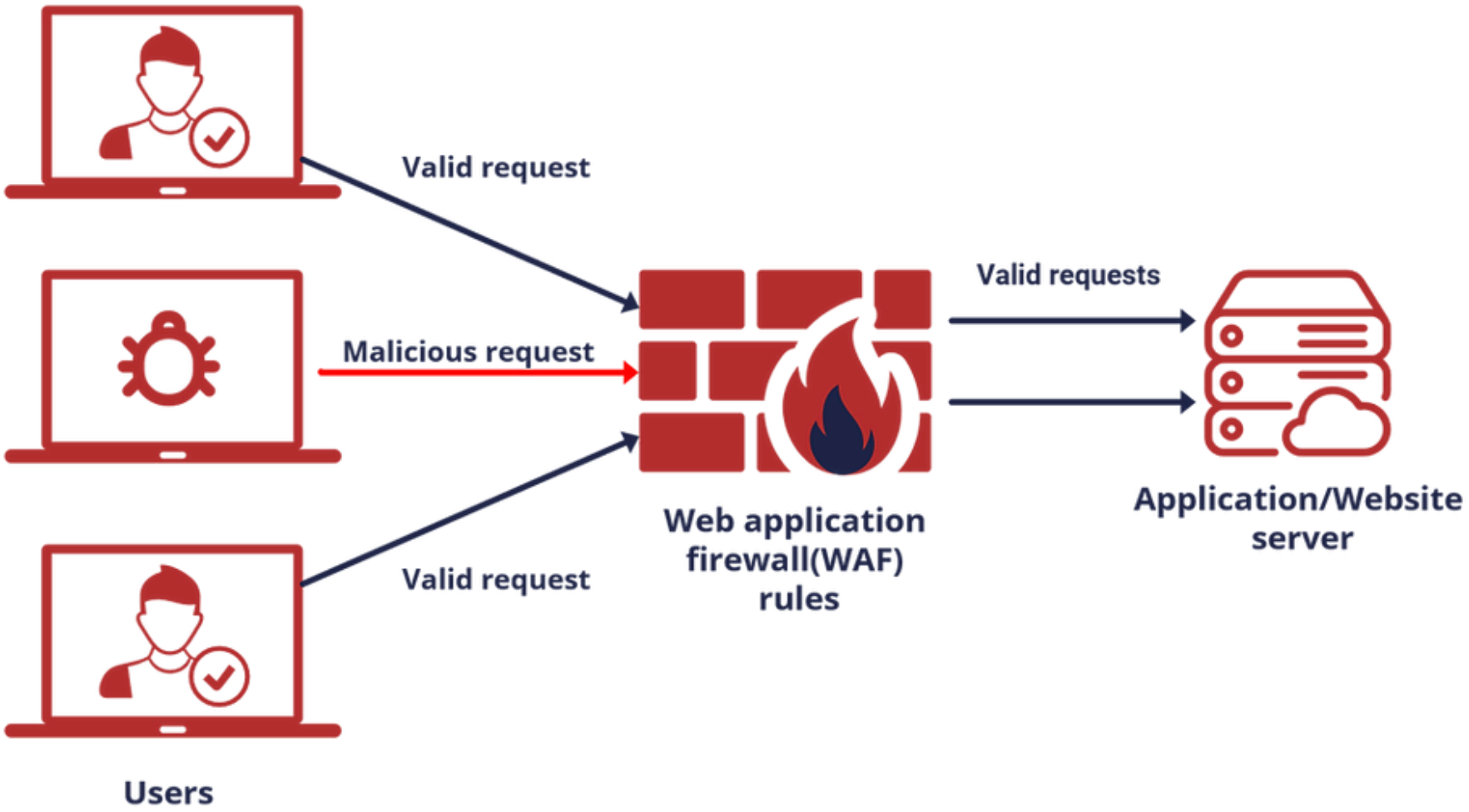
Proxy


Forward Proxy
Forward Proxy
Clients on a private network
Resources on the internet
Reverse Proxy
Reverse Proxy
Clients on the intenet
Resources on a private network

WAF (*Web Application Firewall*)

Enquanto um *firewall* tradicional protege a rede, um WAF foca especificamente na camada de aplicação, avaliando o comportamento das solicitações e respostas HTTP para garantir que não contenham código ou padrões maliciosos que possam comprometer a segurança da aplicação.

WAF (*Web Application Firewall*)



Implantação de *Firewalls*

- Máquina autônoma;
  - Open Source:
    - PfSense;
    - OPNsense;
    - IPFire;
    - ClearOS;
    - Comunidade Endian Firewall.
- Roteador;

Implantação de *Firewalls*

- Estação Bastião (servidor);
- Firewalls baseados em estação (autônomo);

Configuração de *Firewalls*

- **Redes DMZ (*Demilitarized Zone*):**
  - É uma sub-rede isolada que serve para adicionar uma camada extra de segurança entre a rede interna de uma organização e a internet, permitindo que serviços públicos sejam acessíveis externamente sem expor a rede interna.

Configuração de *Firewalls*

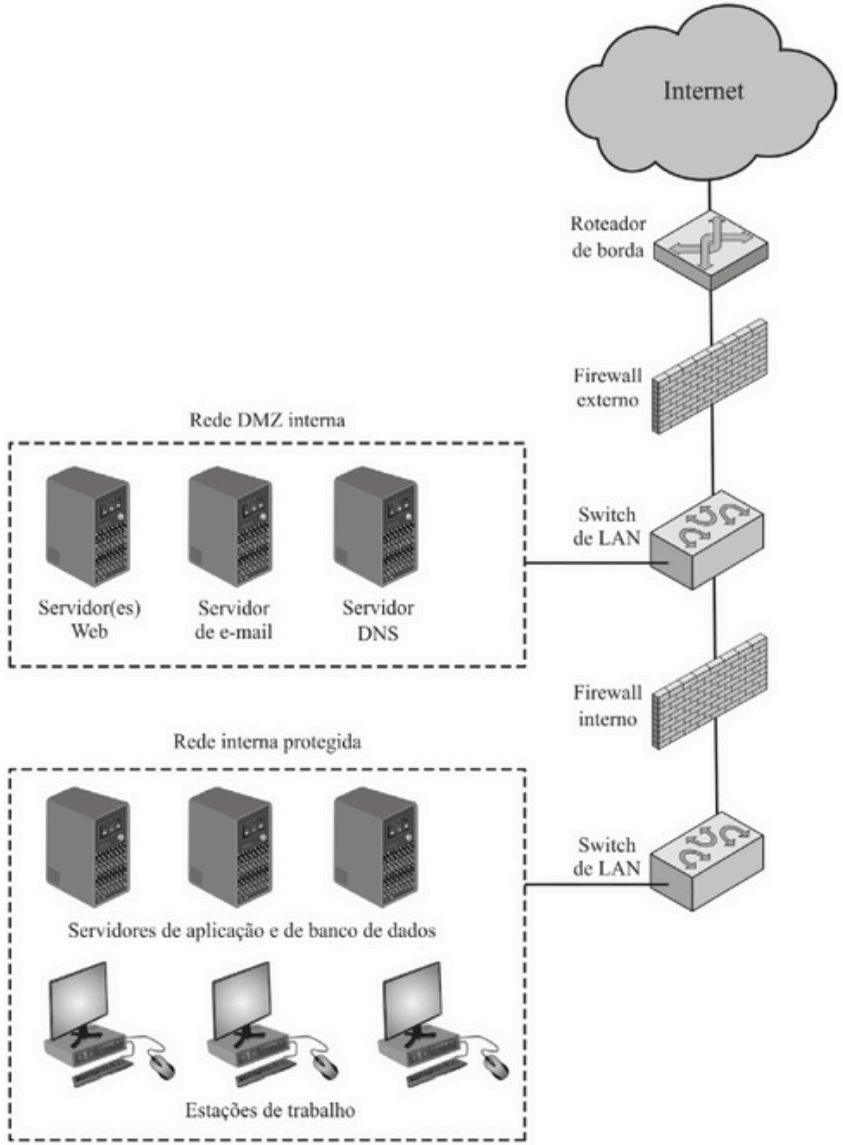


FIGURA 9.2 Exemplo de configuração de firewall.

VPN

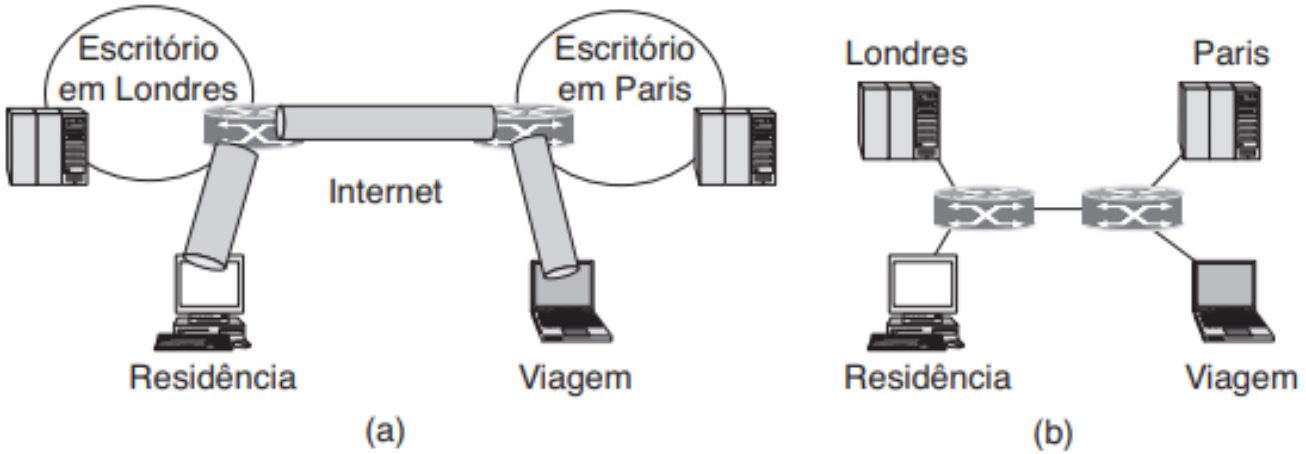
(Virtual Private Network)

Redes Privadas Virtuais (VPN)

Em essência, uma VPN consiste em um conjunto de computadores que se interconectam por meio de uma rede relativamente insegura e que faz uso de protocolos criptográficos e especiais para prover segurança.

O que é

Uma Rede Virtual Privada simula uma rede privada sobre a infraestrutura de uma rede pública.



Fonte: Tanenbaum, 2011.

VPN *(Virtual Private Network)*

Quando você se conecta a uma VPN, seu dispositivo estabelece uma conexão criptografada com um servidor VPN.

VPN *(Virtual Private Network)*

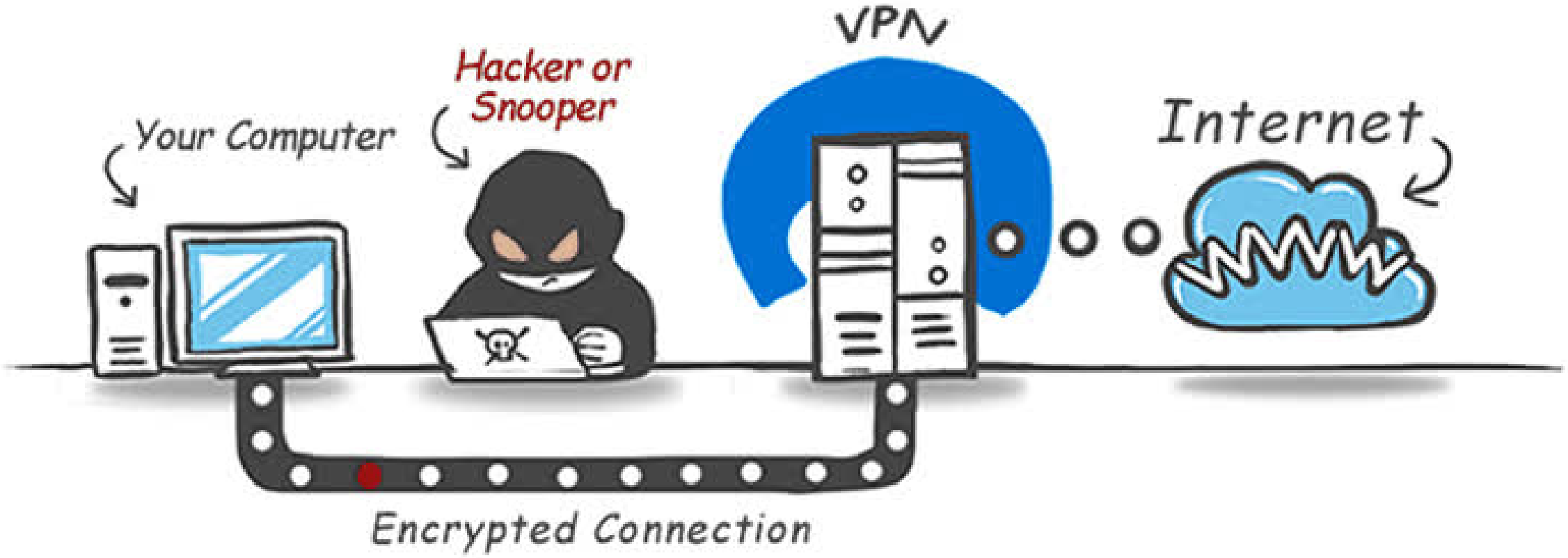
Exemplos de Implementação:

- VPN de Escritório Remoto: Funcionários que trabalham de casa podem usar IPsec para se conectar à rede da empresa. Ao iniciar a conexão, o IPsec estabelece uma comunicação segura, garantindo que todos os dados enviados e recebidos sejam criptografados e autenticados.
- Conexão entre Filiais: Uma empresa com várias filiais pode usar IPsec para interligar suas redes. Isso permite que as filiais compartilhem dados e recursos de forma segura, mesmo que a conexão seja feita através da Internet pública.

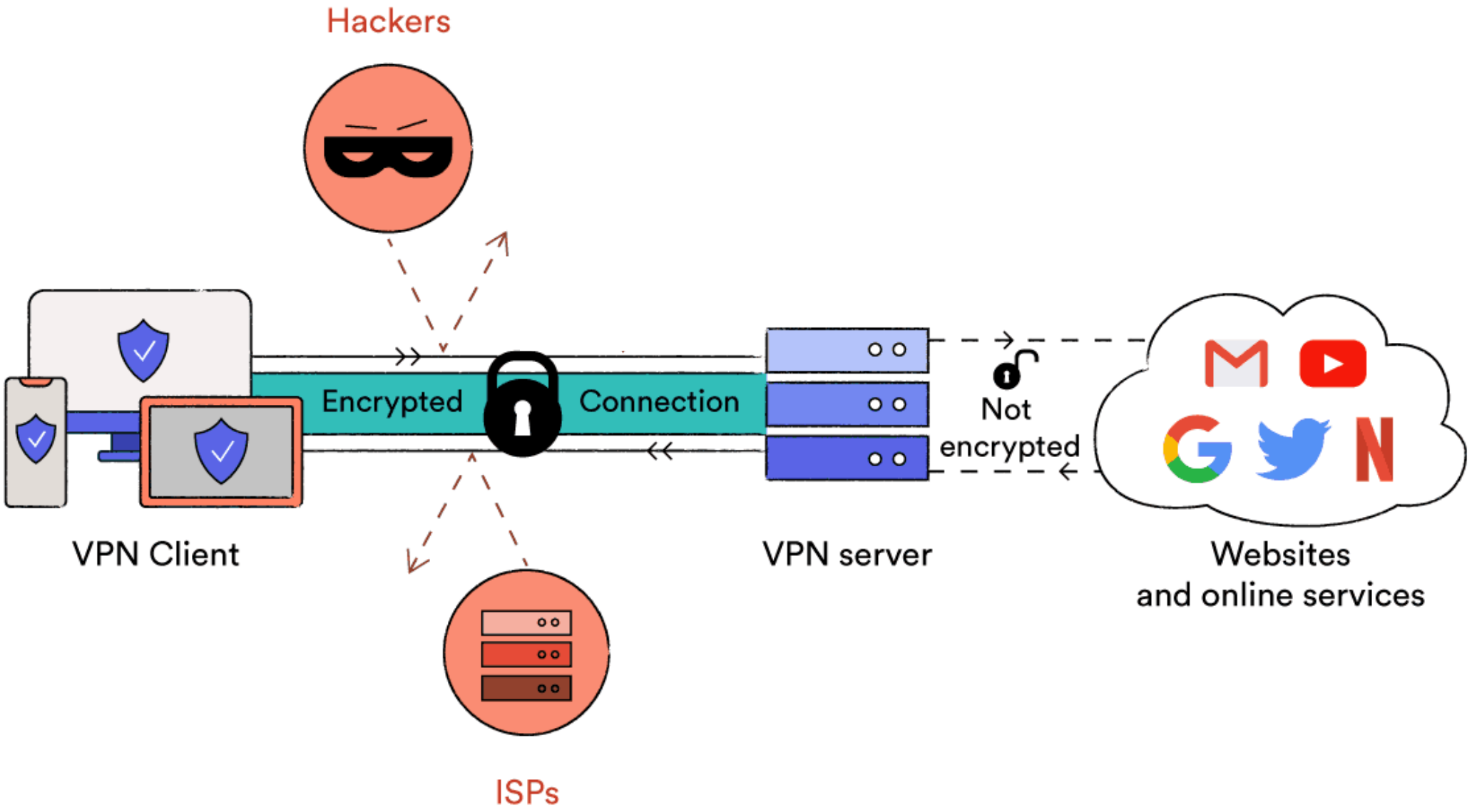
VPN - Rede Privada Virtual

Todas as informações que você envia e recebe são encapsuladas nessa conexão segura, tornando-as ilegíveis para qualquer pessoa que esteja tentando interceptá-las.

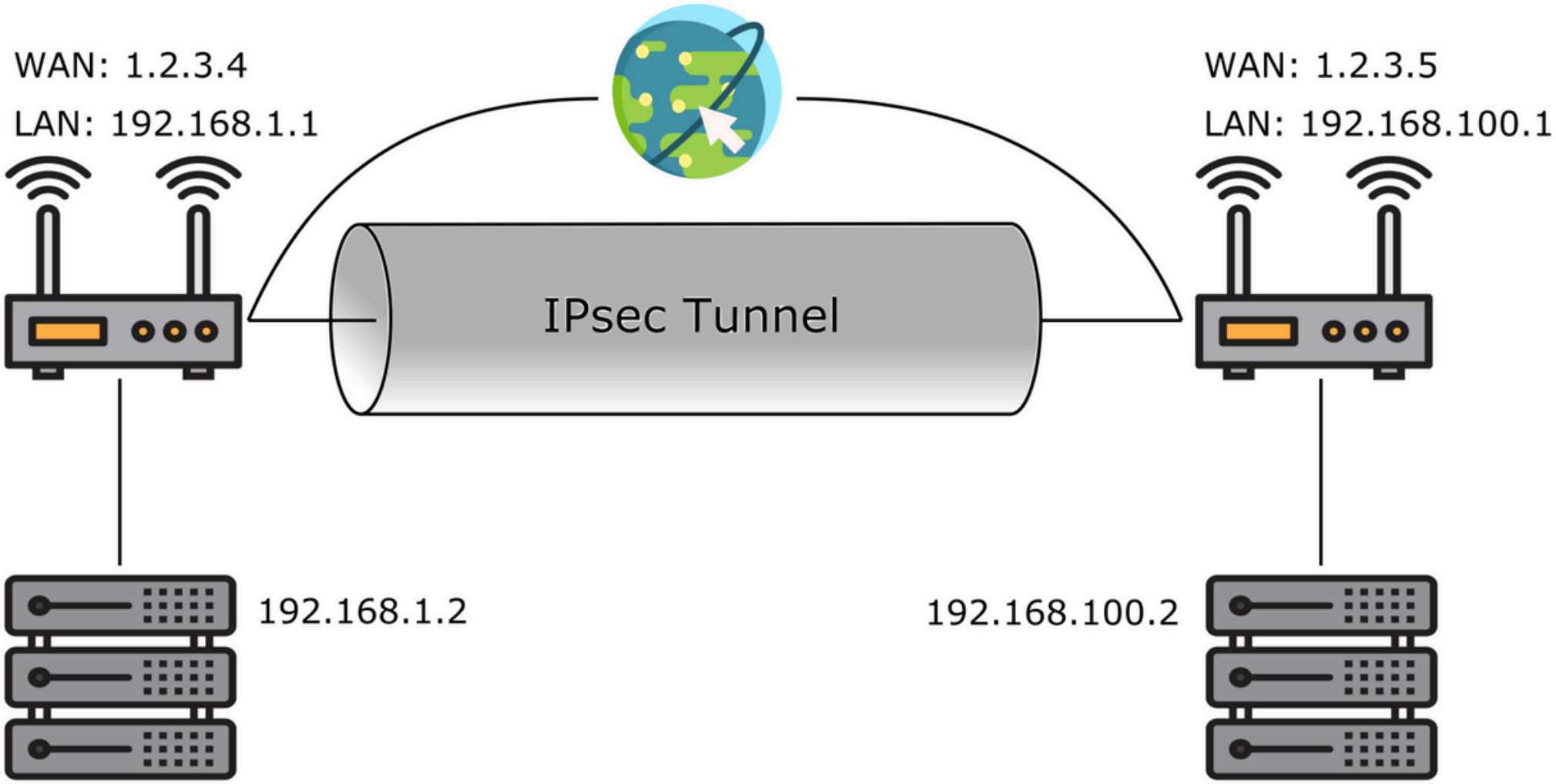
VPN - Rede Privada Virtual



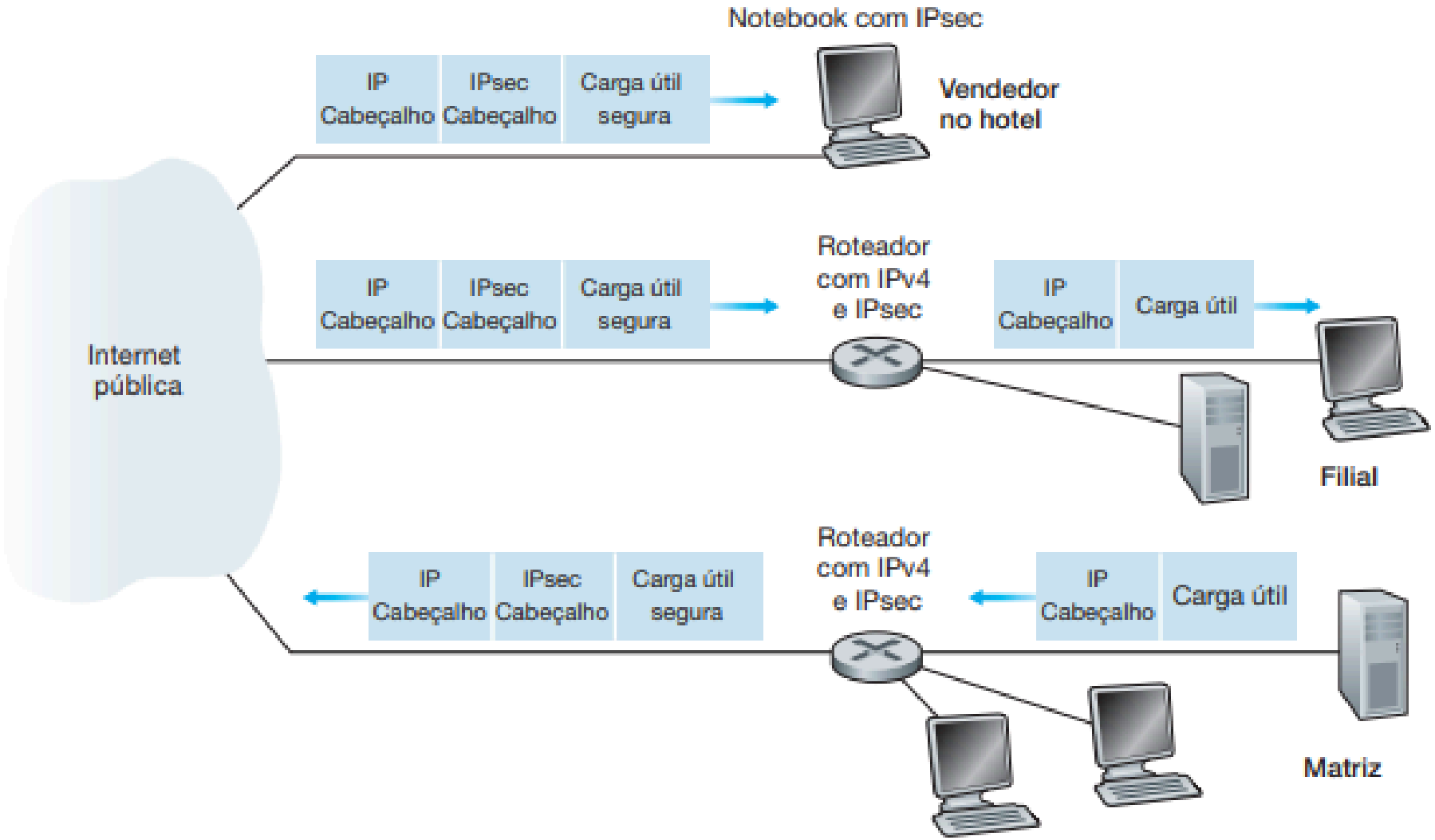
VPN - Rede Privada Virtual



VPN (*Virtual Private Network*)



VPN (*Virtual Private Network*)

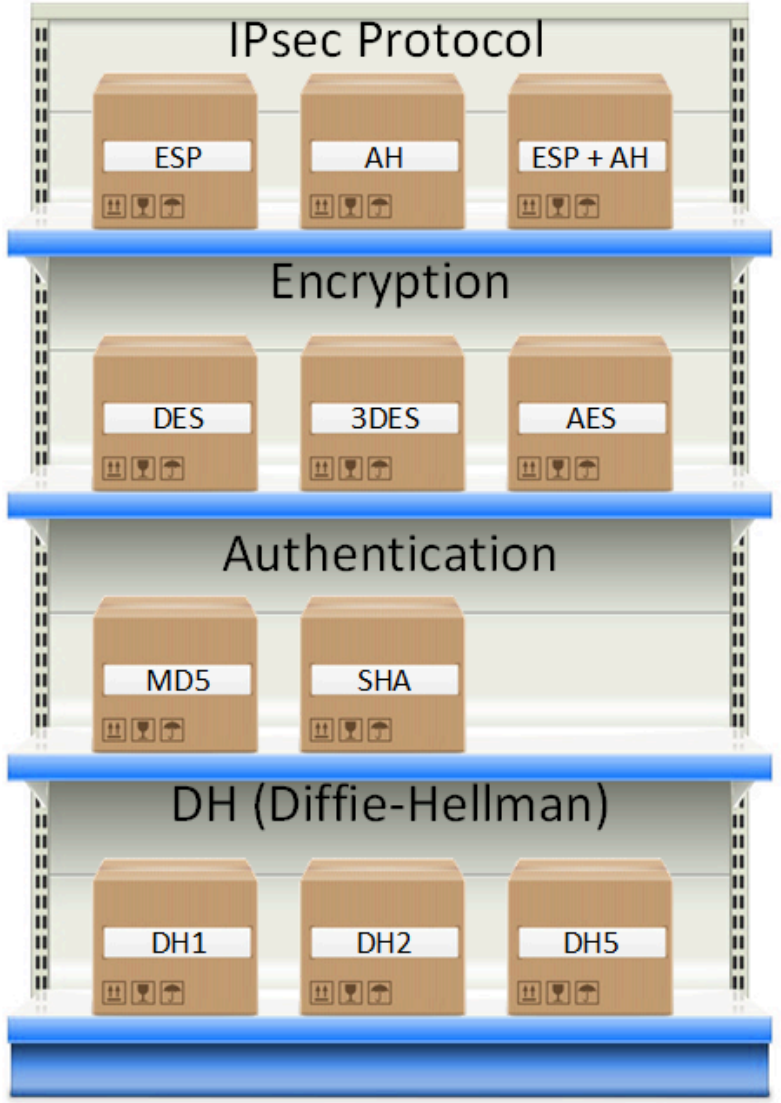


Principais Protocolos

- **L2F**
  - Protocolo de Encaminhamento de Camada 2
  - Desenvolvido pela CISCO
  - Pertence à Camada 2 (Enlace).
- **PPTP**
  - Protocolo de Tunelamento Ponto-a-Ponto
  - Desenvolvido por Ascend Communication, U.S. Robotics, 3Com Corporation, Microsoft Corporation, ECI Telematics
  - Pertence à Camada 2 (Enlace).
- **L2TP**
  - Cisco, PPTP Forum e IETF desenvolveram o Protocolo de Tunelamento de Camada 2 (L2TP), combinando L2F e PPTP
  - Pertence à Camada 2 (Enlace).
- **IPSec**
  - Desenvolvido pelo IETF (Internet Engineering Task Force)
  - Pertence à Camada 3 (Rede).

Internet Security Protocol (IPsec)

- Conjunto de padrões de segurança;
  - Confidencialidade;
  - Integridade;
  - Autenticação;
  - *Anti-replay;*

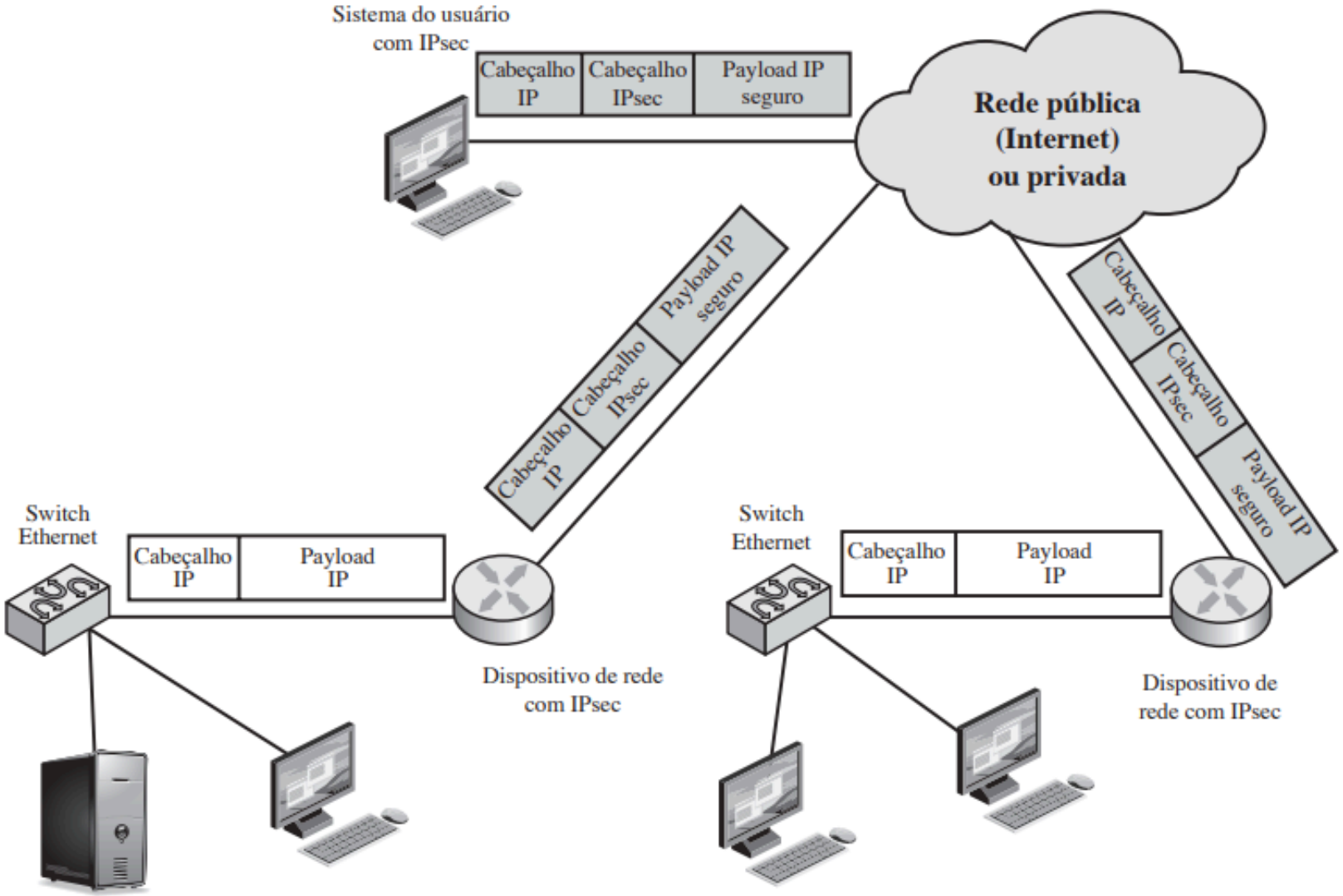


Aplicações do IPsec

- **Conectividade segura do escritório pela Internet:** Uma empresa pode usar IPSec para criar uma rede privada virtual segura através da Internet, reduzindo a necessidade de redes privadas dedicadas e economizando custos.

- **Acesso remoto seguro pela Internet:** Um usuário final pode acessar a rede de uma empresa de forma segura por meio de uma conexão local com um ISP usando IPSec quando estiver fora da empresa (em viagem, ou em sua casa).

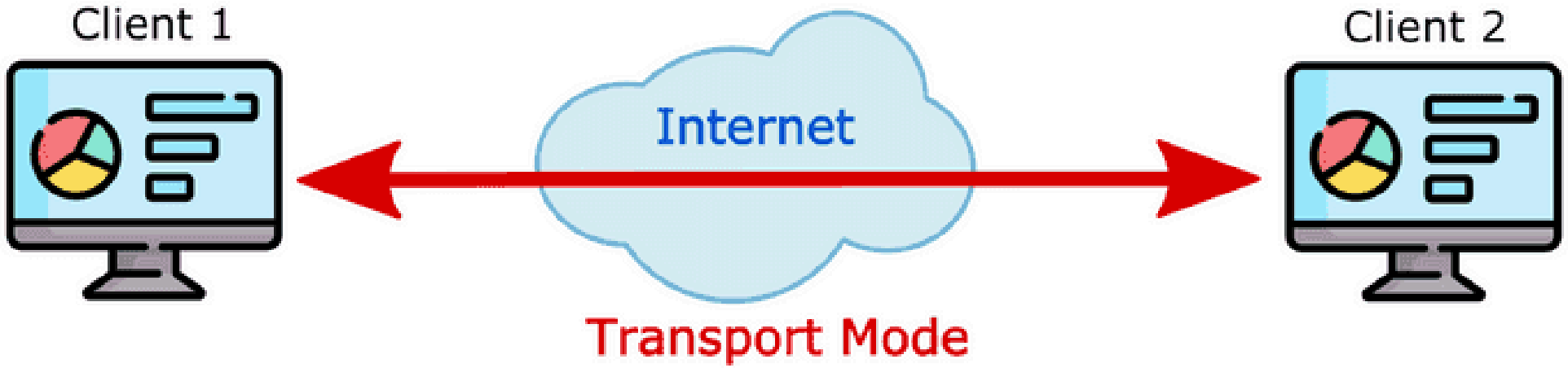
Aplicações do IPsec



Fonte: Tanenbaum, 2011.

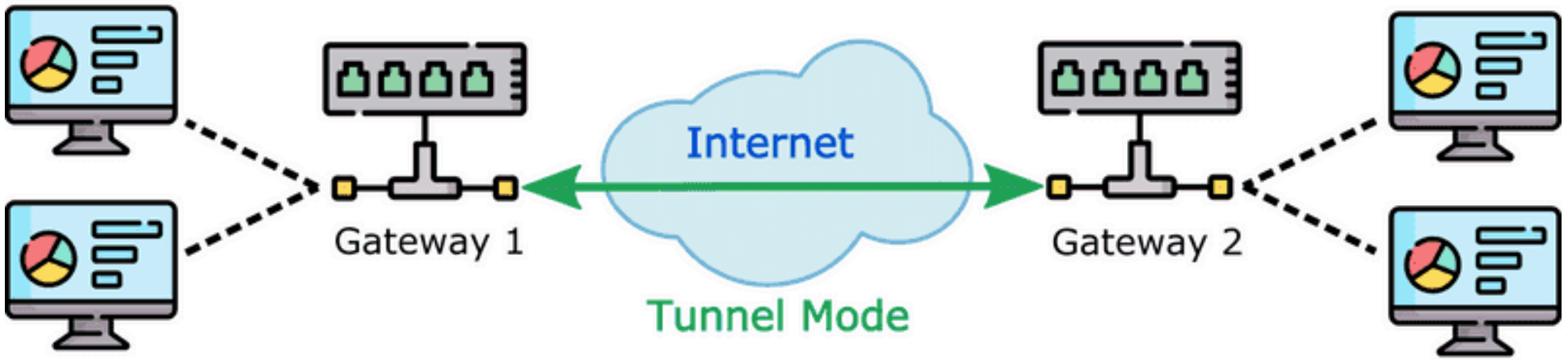
Modo transporte

- **Apenas a carga útil (*payload*) é criptografada.**
- **Necessário aplicação no *host*.**



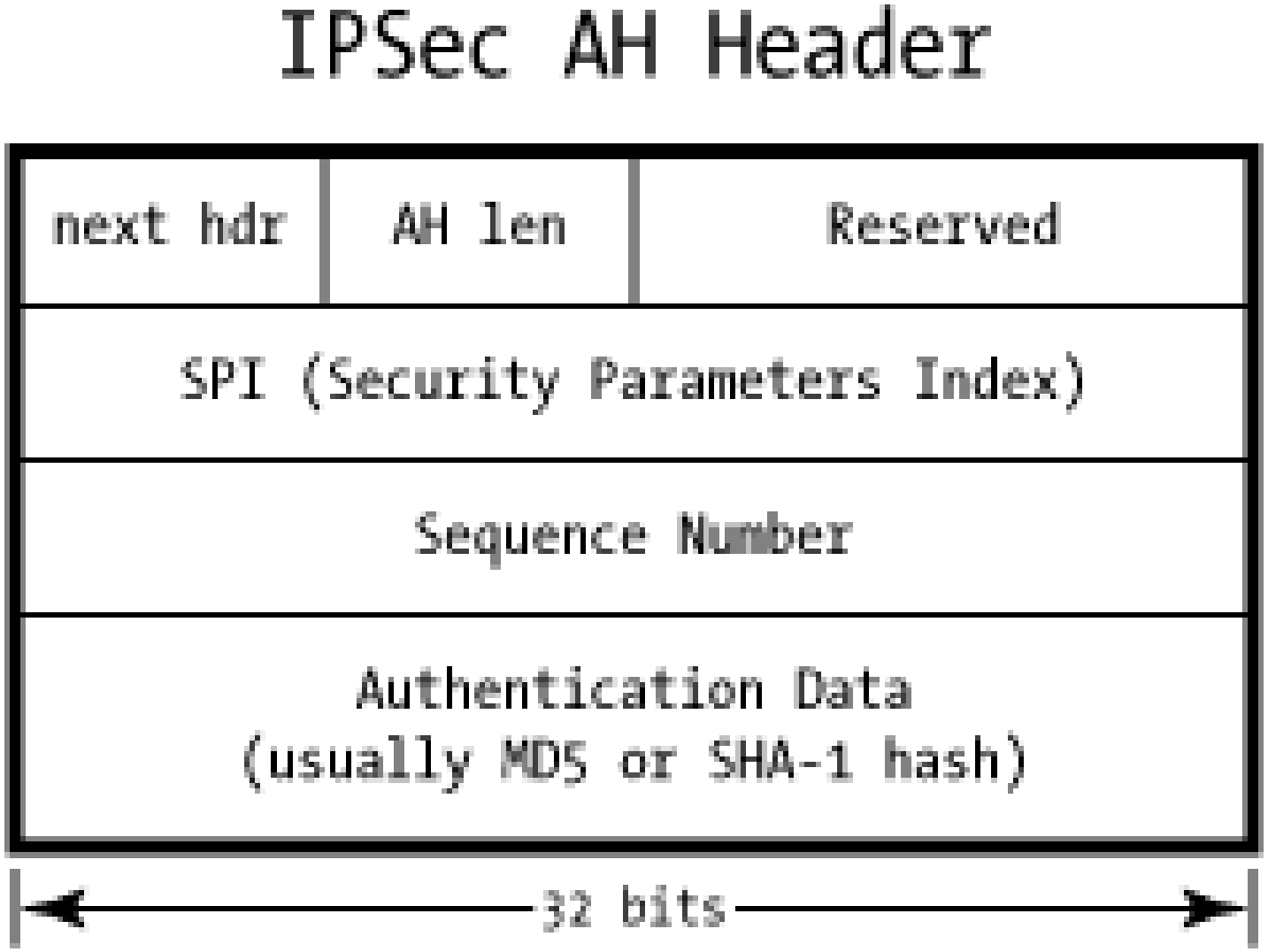
Modo túnel (tunelamento)

- **O cabeçalho e o *payload* são criptografados.**
- **Transparente ao usuário.**



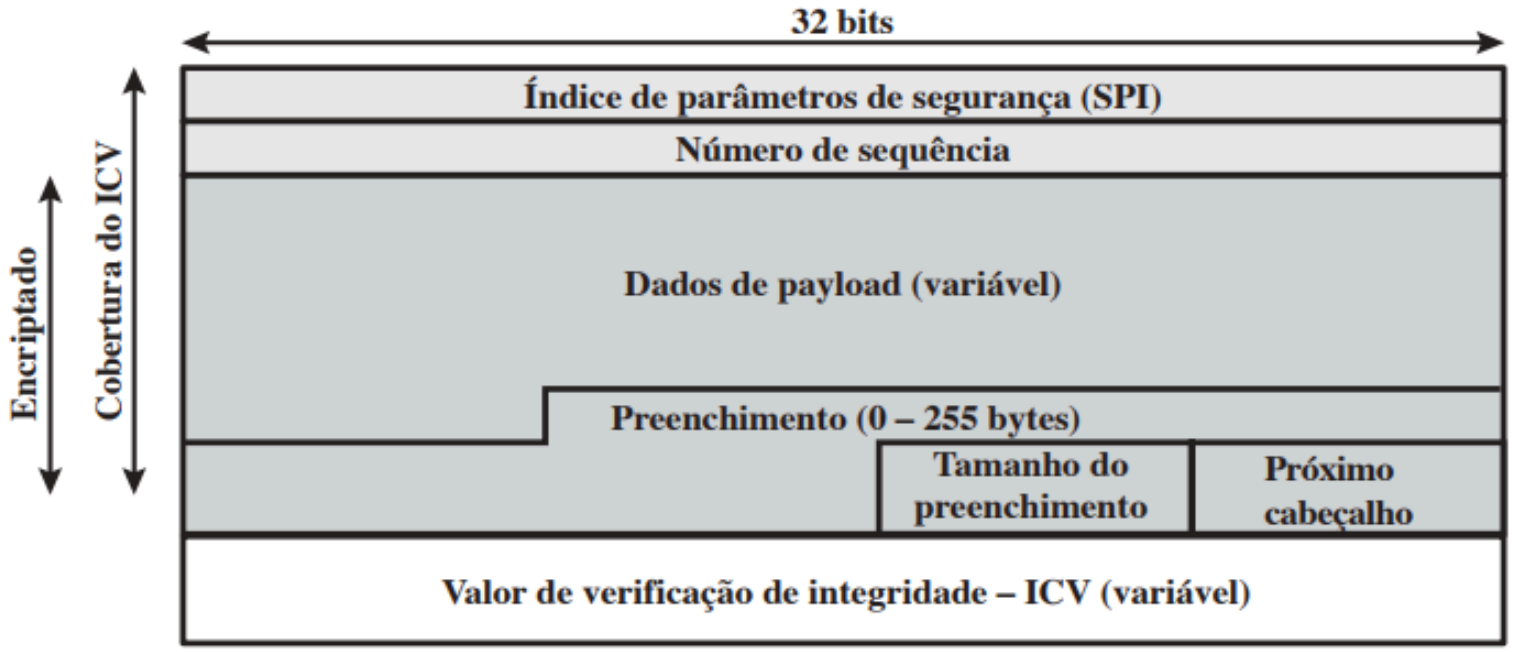
Authentication Header (AH)

Cabeçalho AH:



Encapsulating Security Payload (ESP)

Cabeçalho ESP:



(a) Formato de alto nível de um pacote ESP

Fonte: Stallings, 2015

Segurança em redes sem fio

Definição

- As redes wireless ou redes sem fio são um sistema de comunicação de dados extremamente flexível, que pode ser usado como uma extensão ou uma alternativa a redes locais (LANs cabeadas).

- É uma tecnologia que combina conectividade de dados com mobilidade através de tecnologia de radiofrequência (RF).

- A rede sem fio utiliza-se de ondas eletromagnéticas para transmitir e receber dados de seus dispositivos ou estações.

Alvos de ataque

- Dispositivos finais: um smartphone, um laptop, um tablet, um sensor sem fio, um dispositivo Bluetooth e etc.
- Pontos de Acesso: torres celulares, hotspots e etc.
- Meio de Transmissão: ondas de rádio.

Fonte: STALLINGS e BROWN, 2014.

Ameaças

- **Associação acidental:** A proximidade de LANs com e sem fio pode levar usuários a se conectarem inadvertidamente a redes vizinhas, expondo recursos da LAN.

- **Associação maliciosa:** Dispositivos configurados como pontos de acesso legítimos podem ser usados para roubar senhas e invadir redes com fio.

Ameaças

- **Redes ad hoc:** Conexões diretas entre computadores sem fio podem ser uma ameaça pela falta de controle central.

- **Redes não tradicionais:** Dispositivos como Bluetooth, leitores de códigos de barra e PDAs representam riscos de interceptação e falsificação.

- **Roubo de identidade (falsificação de MAC):** Interceptação de tráfego para obter endereços MAC privilegiados.

Ameaças

- **Ataques do tipo homem no meio:** Persuadir usuários e pontos de acesso a se comunicarem através de um intermediário, vulnerável em redes sem fio.

- **Negação de serviço (DoS):** Ataque que bombardeia pontos de acesso com mensagens para consumir recursos.

- **Injeção em rede:** Ataque que utiliza tráfego não filtrado para reconfigurar roteadores e switches e degradar o desempenho da rede.

Segurança de transmissões

- **Técnicas de ocultação de sinal:**
  - Ocultar (*Service Set Identifier* — SSID);
  - Reduzir a potência de sinal;
  - Nomes crípticos a SSIDs;
  - Pontos de acesso longe de janelas e paredes externas.
- **Criptografia.**

Segurança de rede sem fio

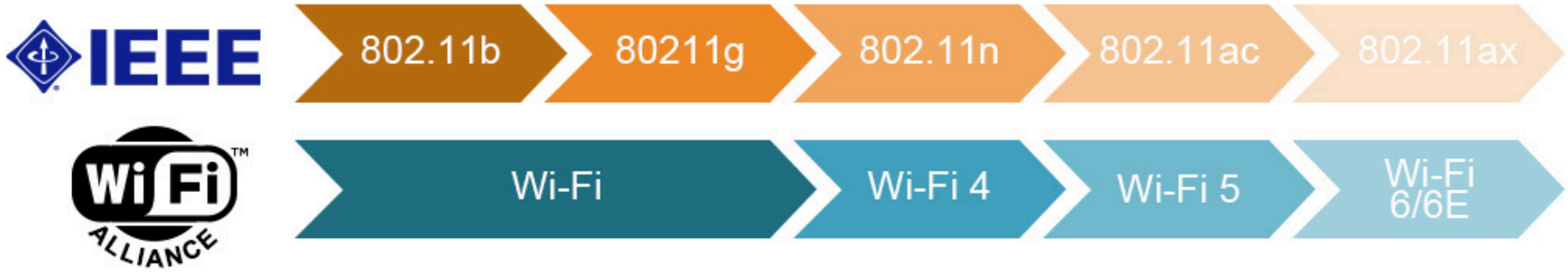
- Criptografia.
- Antivírus e firewall.
- Desligar a transmissão do identificador.
- Trocar o identificador padrão do roteador (IP).
- Mudar a senha de administrador do seu roteador.
- Um roteador pode ser configurado para comunicar-se somente com endereços MAC aprovados.
  - É claro que endereços MAC podem ser falsificados, portanto isso é apenas um dos elementos de uma estratégia de segurança.

Protocolos IEEE 802.11

- O IEEE 802 é um comitê que desenvolveu padrões para redes locais (LANs).
- Em 1990, o IEEE 802 Committee formou um novo grupo de trabalho, o IEEE 802.11, para desenvolver um protocolo para LANs sem fio (WLANs).

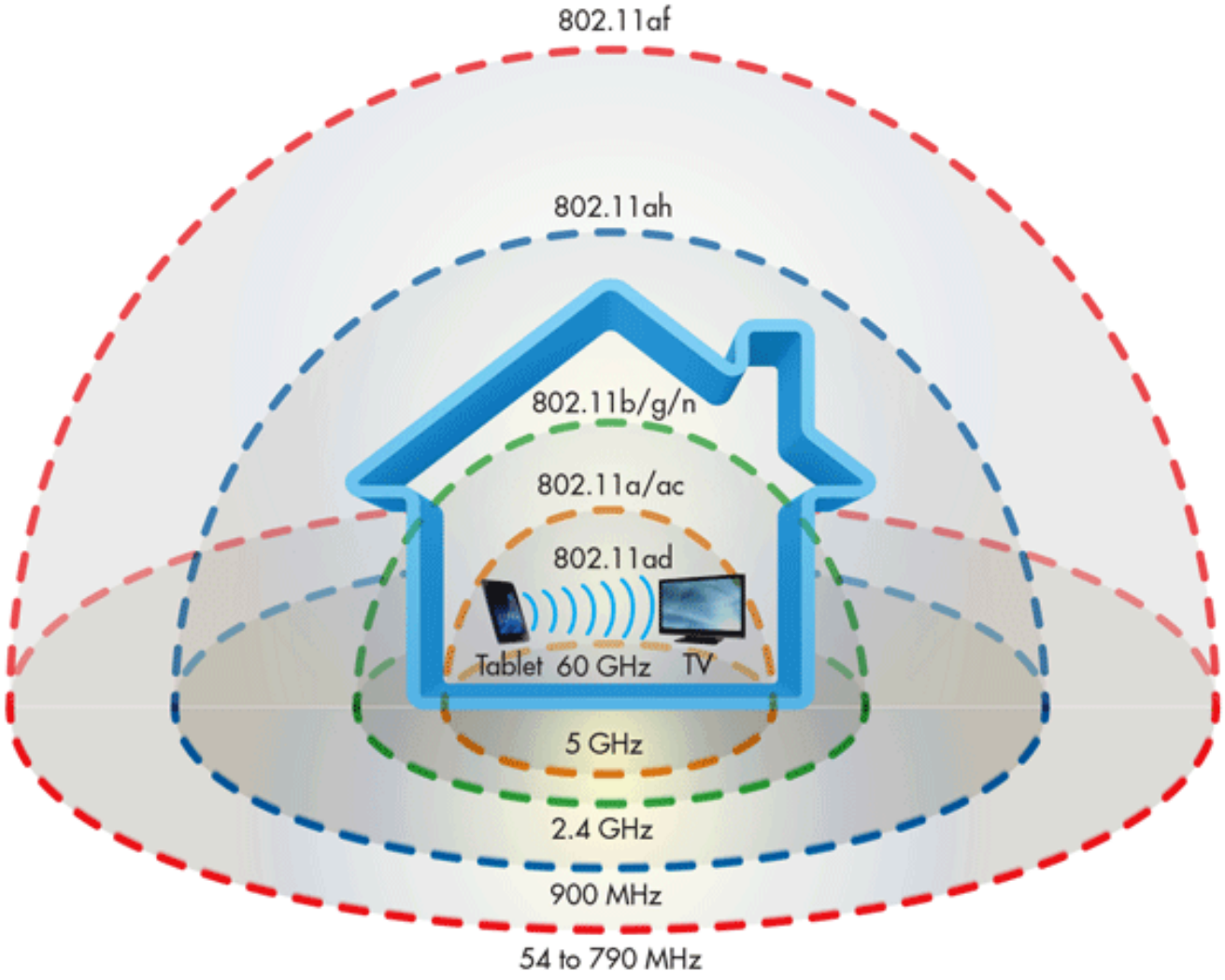
Protocolos IEEE 802.11

Certificação Aliança Wi-fi

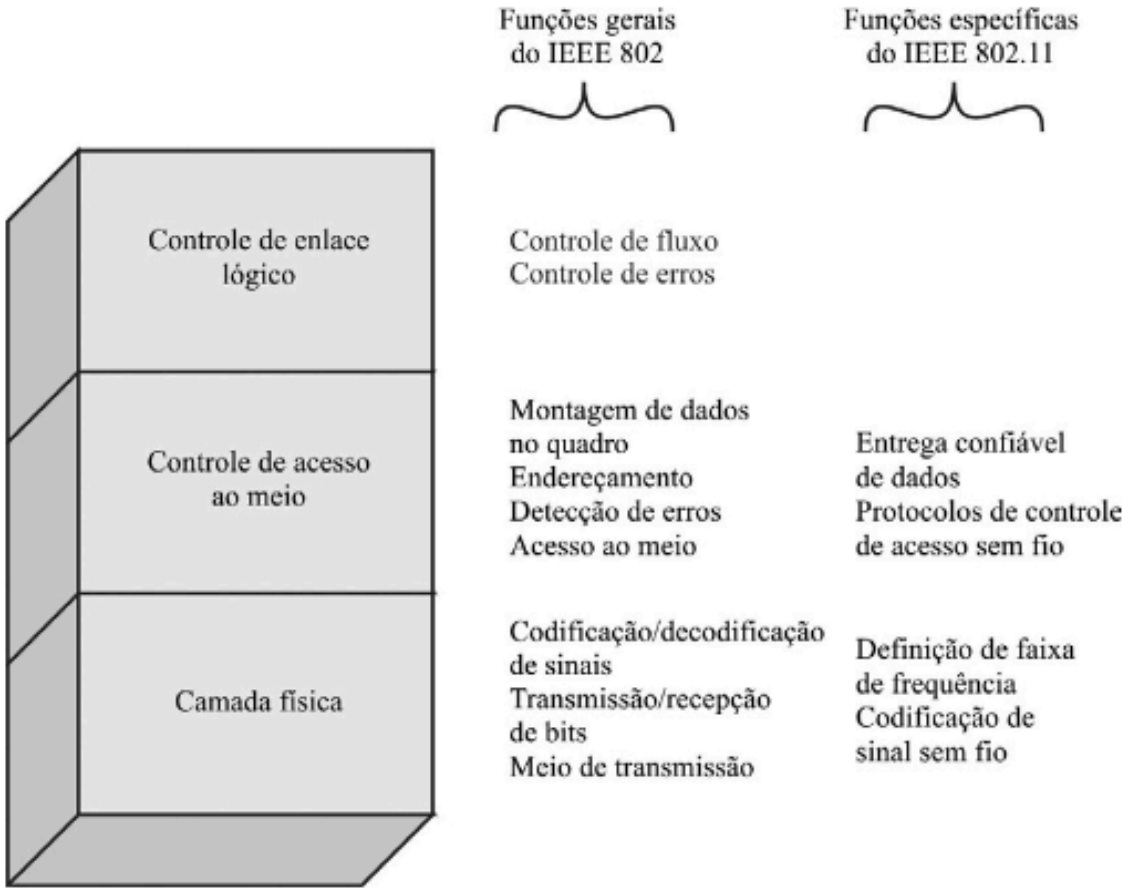


Rel.Year	1999	2007	2009	2013	2020
Freq.Band	2.4 GHz	2.4 GHz	2.4 + 5 GHz	5 GHz	2.4 + 5 + 6 GHz(6E)
Bandwidth	20 MHz	20 MHz	40 MHz	80 MHz,160 MHz	80 MHz,160 MHz

Protocolos IEEE 802.11



Arquitetura IEEE 802.11



Fonte: STALLINGS e BROWN, 2014.

Autenticação IEEE 802.11

	WEP	WPA	WPA2	WPA3
Full Form	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Release Year	1997	2003	2004	2018
Key Size	64 bit, 128 bit	128 bit	128 bit	128 bit, 256 bit
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP, AES-GCMP

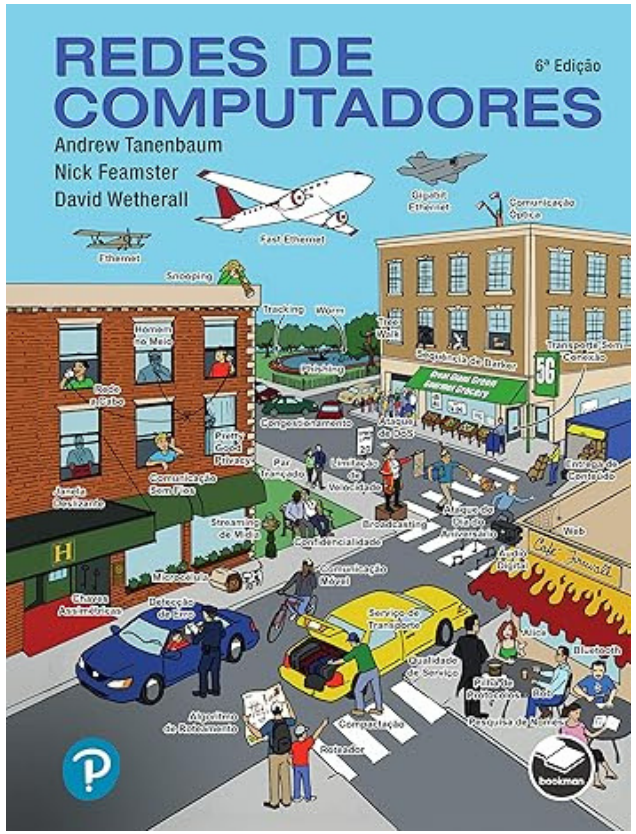
Autenticação IEEE 802.11

	WEP	WPA	WPA2	WPA3
Protocolo de criptografia	RC4	TKIP	AES	AES
Método de autenticação	CRC	PSK	PSK	SAE
Tamanho da chave	10, 26 ou 32 dígitos hexadecimais	8 a 64 caracteres	8 a 64 caracteres	8 a 64 caracteres
Dispositivos compatíveis/suporte	Alto	Alto	Alto	Baixo
Nível de segurança	Fraca	Média	Alta	Altíssima

Leitura Recomendada

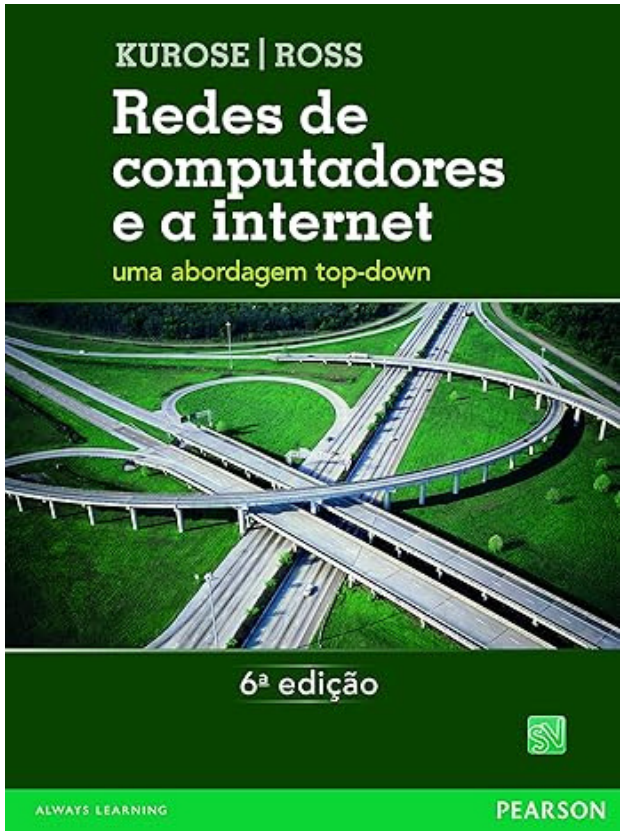
Capítulo 8 do livro:

Redes de Computadores

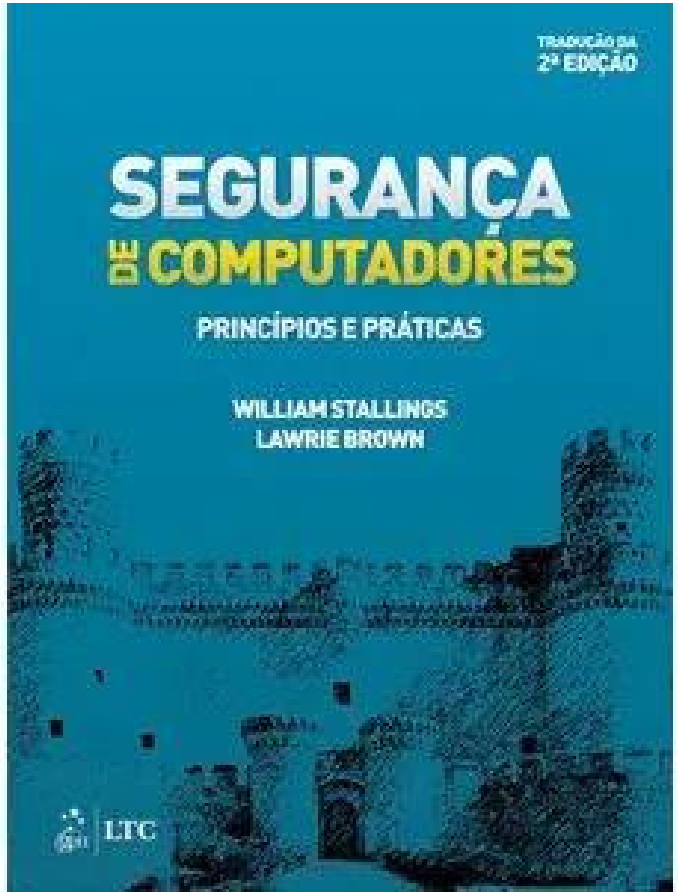


Capítulos 8 do livro:

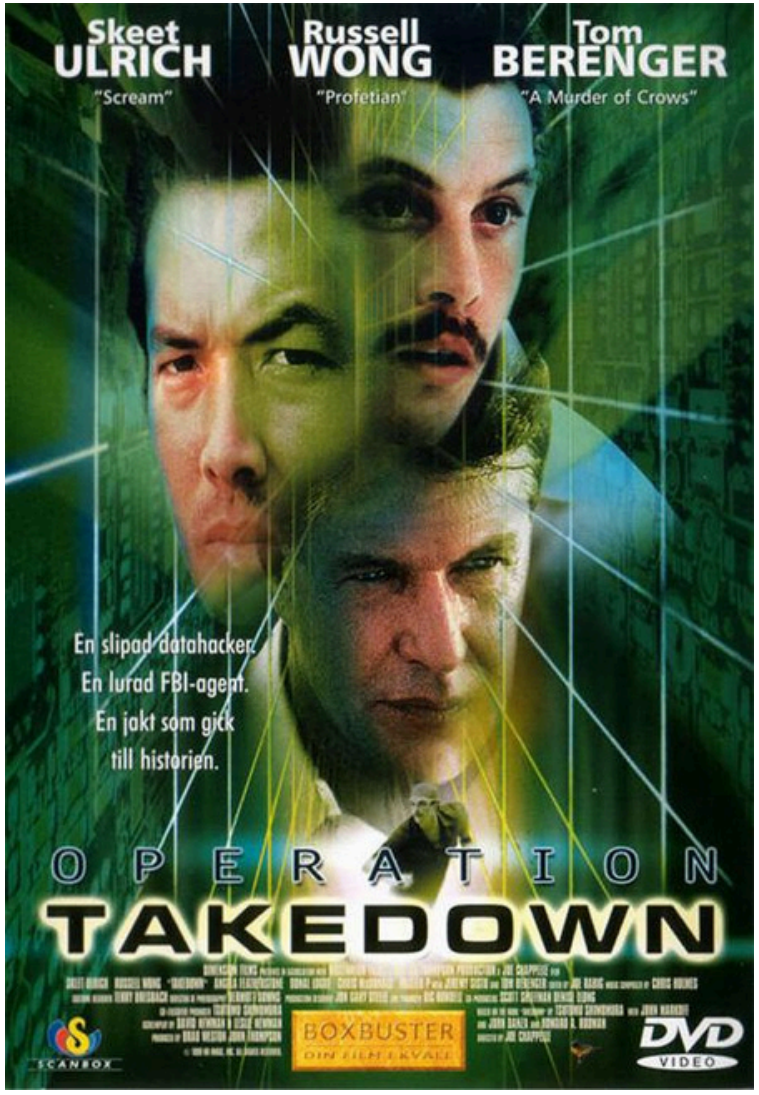
Redes de Computadores e a internet



Leitura Recomendada



Sugestão de Filme



Referências

WETHERALL, J.; TANENBAUM, A. S. Redes de Computadores. 6ª edição. Rio de Janeiro: Editora Campus, 2021.

KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet. 5ª edição. São Paulo: Person, 2021.

FOROUZAN, Behrouz A. Comunicação de dados e redes de computadores. 4ª edição. AMGH Editora, 2010.

INTERNET ENGINEERING TASK FORCE (IETF). RFCs. Disponível em: https://www.ietf.org/process/rfcs/. Acesso em: 22 out. 2024.

STALLINGS, William; BROWN, Lawrie. Segurança de computadores: princípios e práticas. Tradução de Arlete Simille Marques. 2º. ed., Rio de Janeiro: Elsevier, 2014.

STALLINGS, William; BROWN, Lawrie. Computer security: principles and practice. Pearson, 2015.

DE MORAES, ALEXANDRE FERNANDES. Redes sem fio: Instalação, Configuração e Segurança-Fundamentos. Saraiva Educação SA, 2010.

Redes de Computadores

Marisangila Alves, MSc

marisangila.alves@proton.me