Marisangila Alves, MSc
marisangila.alves@udesc.br
marisangila.com.br

UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA
JOINVILLE
CENTRO DE CIÊNCIAS TECNOLÓGICAS

UDESC
Universidade do Estado de Santa Catarina

2026/1

Segurança da Informação

Rede Privada Virtual

Sumário

Introdução

O que é?

Uma rede Virtual Privada **simula** uma rede privada sobre a infraestrtura de uma rede pública.

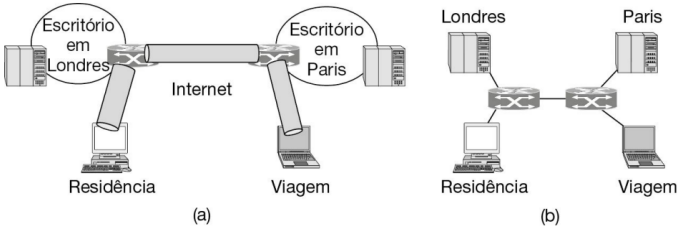


Figura: Rede Privada Virtual (Kurose; Ross, 2021).

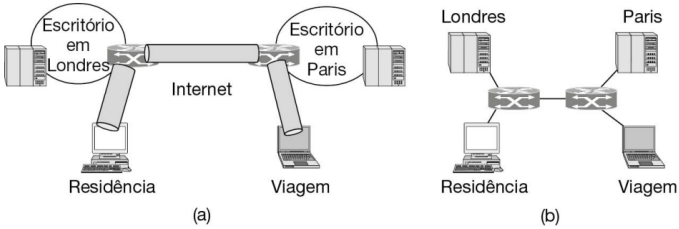


Figura: Rede Privada Virtual (TANENBAUM, 2004).

- VPN (Virtual Private Network) cria um túnel seguro sobre redes públicas (como a Internet).
- Permite que dados sejam transmitidos de forma confidencial, como se estivesse em uma rede privada.
- Usos comuns:
  - Acesso remoto corporativo (*Home Office*);
  - Conexão entre matriz e filiais (*Site-to-Site*);
  - Proteção em redes Wi-Fi públicas;
  - Integração com parceiros (Extranet VPN);
  - Privacidade e anonimização de IP (VPN comercial);
  - Acesso remoto a dispositivos e servidores (SSH, bancos de dados);
  - *Bypass* de geolocalização[1].

[1] O uso de VPN para contornar geolocalização pode violar termos de serviço e, dependendo da finalidade e da legislação local, pode ter implicações legais. A ilegalidade não está na VPN em si, mas no uso que se faz dela.

- **VPN de acesso remoto:** usuário acessa a rede corporativa de forma segura.
- **VPN site-a-site:** conecta redes inteiras entre filiais:
  - Intranet: Conexão entre LANs da mesma instituição.
  - Extranet: Conexão entre LANs de parceiros comerciais.

Principais Protocolos de VPN I

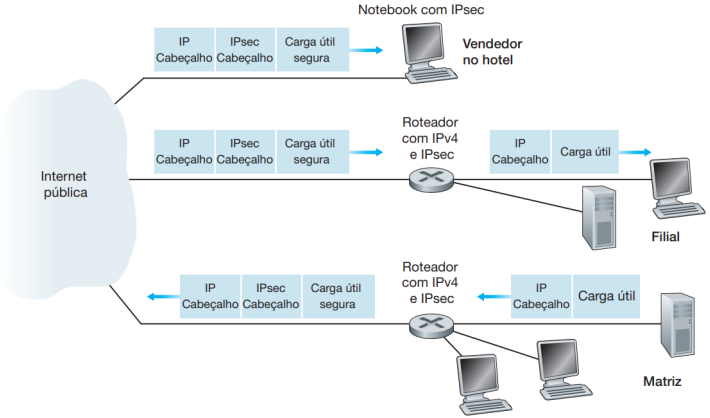
Prot.	OSI	Descrição / Uso	Desenv.
PPTP	L2	Tunelamento baseado em PPP. Usa GRE. Criptografia MPPE.	Microsoft
L2TP	L2	Tunelamento camada 2. Sem criptografia nativa. Usado com IPsec.	Cisco / MS
IPsec	L3	Autenticação e criptografia IP (AH, ESP, IKE). Site-to-Site e remoto.	IETF
GRE	L3	Encapsulamento genérico. Sem criptografia.	Cisco
OpenVPN	L3/L2	Baseada em TLS. Modo TUN ou TAP.	OpenVPN Inc.
WireGuard	L3	VPN moderna. Curve25519 + ChaCha20. Alto desempenho.	Donenfeld
SSL VPN	L4/L7	Baseada em TLS. Túnel completo ou portal web.	IETF
MPLS	L2.5/L3	VPN de operadora com isolamento por rótulos.	IETF
SSH	L7	Tunelamento de portas. Não é VPN nativa.	IETF

IP Security

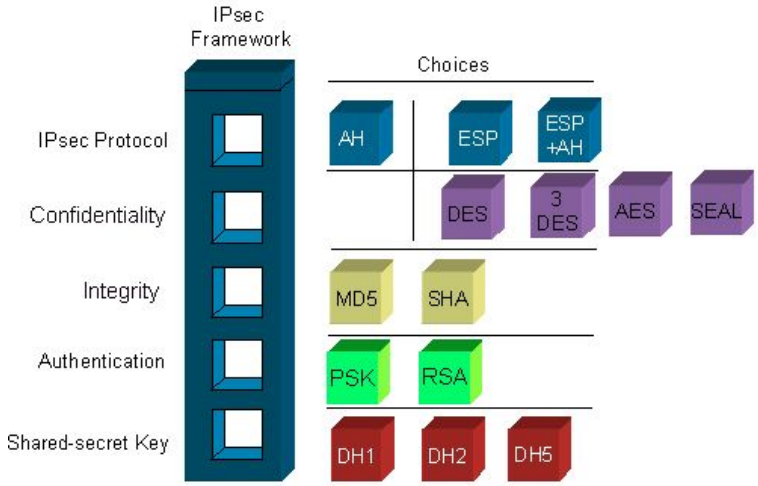
- Segurança em nível de rede (IP).
- Modos de operação:
  - Transporte: protege apenas o *payload*
  - Túnel: protege todo o pacote IP
- Protocolos principais:

- **RFC 4301**: Security Architecture for the Internet Protocol (define a arquitetura geral do IPsec).
- **RFC 6071**: IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap (guia e organização das RFCs do IPsec).
- **RFC 2406**: IP Encapsulating Security Payload (ESP).
- **RFC 2407**: The Internet IP Security Domain of Interpretation for ISAKMP.
- **RFC 2408**: Internet Security Association and Key Management Protocol (ISAKMP).
- **RFC 2409**: The Internet Key Exchange (IKE).

Conjuntos de Protocolos II



Conjuntos de Protocolos III



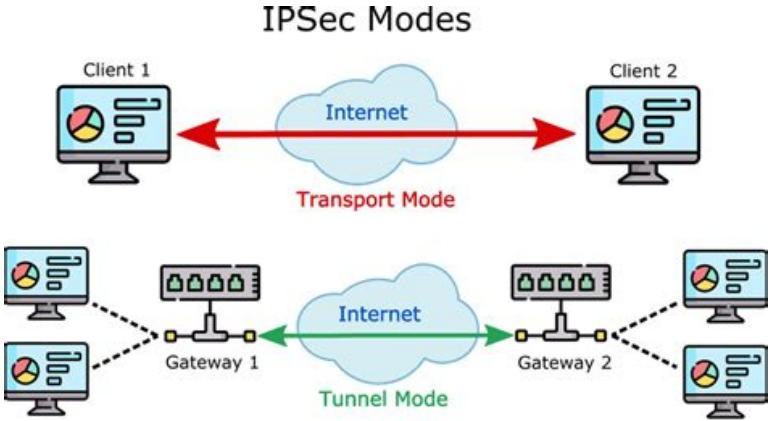
Modo Transporte

No modo transporte, o IPsec mantém o cabeçalho IP original e protege apenas o payload do pacote (como o segmento TCP/UDP e os dados).

Modo Túnel

É criado um novo cabeçalho IP externo, enquanto o pacote IP original inteiro (cabeçalho + dados) fica encapsulado e protegido dentro do túnel.

VPN — © 2026 ALVES, M.


IPSec Modes
Client 1
Internet
Client 2
Transport Mode
Internet
Gateway 1
Gateway 2
Tunnel Mode

ESP (*Encapsulating Security Payload*)

É o protocolo do IPsec que fornece criptografia, integridade, autenticação e proteção contra replay para os dados transportados.

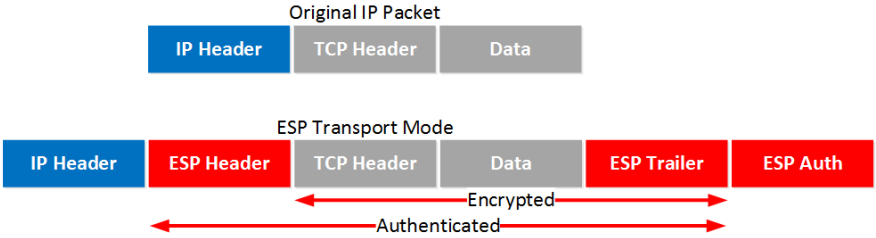


Figura: IP sec com ESP em modo transporte.

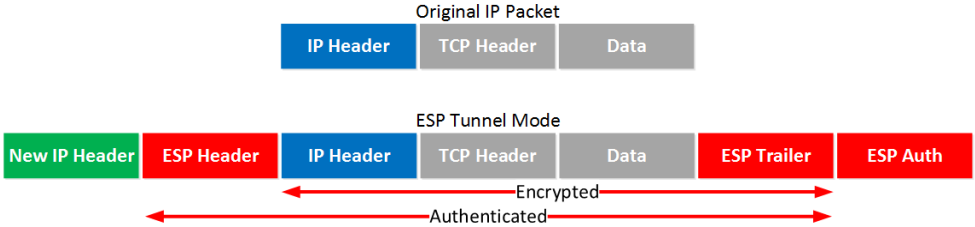


Figura: IP sec com ESP em modo túnel.

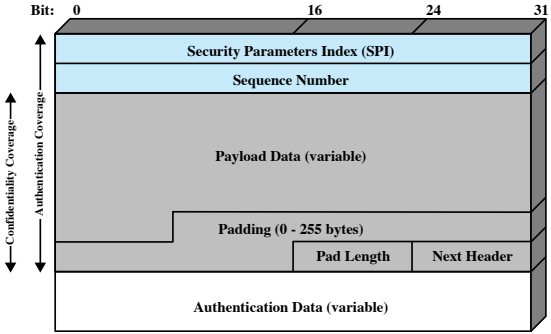


Figure 21.5 IPSec ESP Format

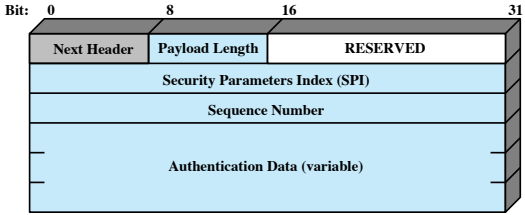


Figure 21.4 IPSec Authentication Header

VPN — © 2026 ALVES, M.

AH (*Authentication Header*)

É o protocolo do IPsec que fornece autenticação e integridade do pacote IP, mas não oferece criptografia dos dados.

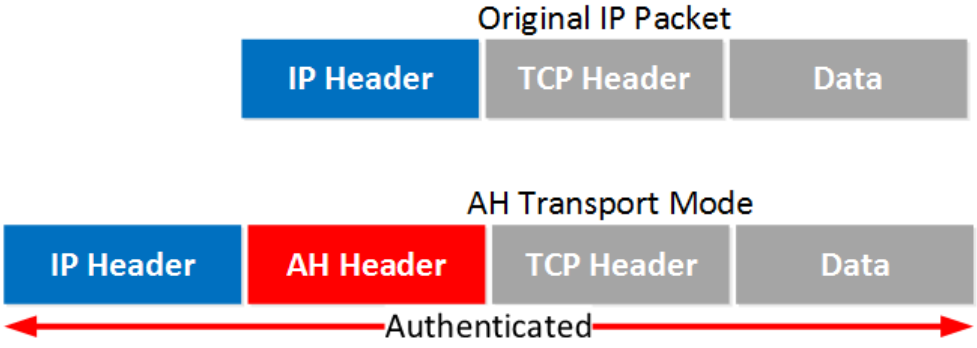


Figura: IP sec com AH em modo transporte.

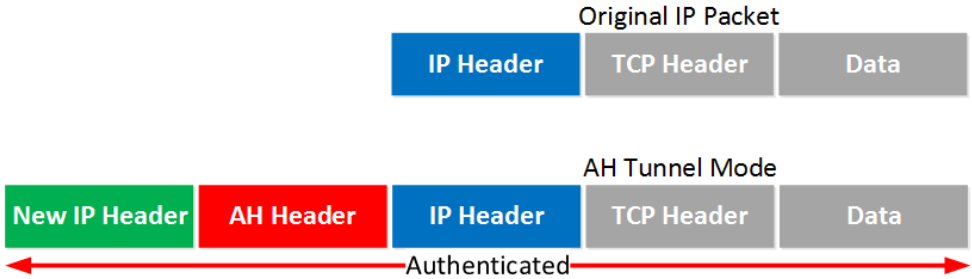
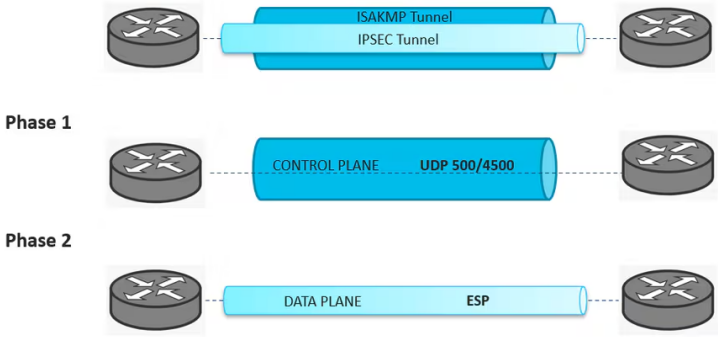


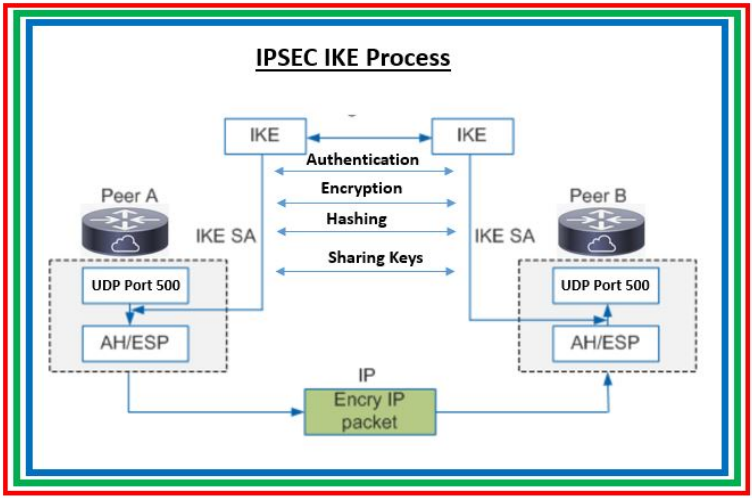
Figura: IP sec com AH em modo túnel.

- **ISAKMP (Internet Security Association and Key Management Protocol):**
  - É um framework que define a estrutura para negociar e gerenciar Associações de Segurança (Security Associations – SAs)[2].
  - Define o formato das mensagens e como os parâmetros de segurança são trocados.
  - Não define algoritmos; apenas organiza a negociação.
  - É utilizado pelo IKE para estabelecer túneis IPsec.
- **Fase 1: Estabelecimento do Canal Seguro:**
  - Troca de chaves utilizando Diffie-Hellman.
  - Autenticação das partes.
  - Criação da Security Association do IKE (SA IKE).
- **Fase 2: Estabelecimento do Túnel IPsec:**
  - Definição do protocolo de proteção (ESP ou AH).
  - Definição dos algoritmos de criptografia e integridade.
  - Definição das redes ou tráfego que será protegido.
  - Criação da Security Association do IPsec (SA IPsec).



[2]Um conjunto de parâmetros que define como a comunicação será protegida. SA funciona como um "contrato de segurança" entre dois dispositivos.

- **O que é o IKE (Internet Key Exchange):**
  - Protocolo responsável por negociar e estabelecer as chaves criptográficas do IPsec.
  - Implementa o gerenciamento de Security Associations (SAs).
  - Realiza autenticação entre os pares (certificados, PSK, etc.).
  - Executa a troca segura de chaves (Diffie-Hellman).
  - Define quais algoritmos criptográficos serão utilizados (AES, SHA, etc.).


IPSEC IKE Process
IKE
IKE
Authentication
Encryption
Hashing
Sharing Keys
Peer A
Peer B
IKE SA
IKE SA
UDP Port 500
UDP Port 500
AH/ESP
AH/ESP
IP
Encry IP packet

SSL/TLS

Atenção!

O SSL não é um protocolo único, mas sim duas camadas de protocolos.

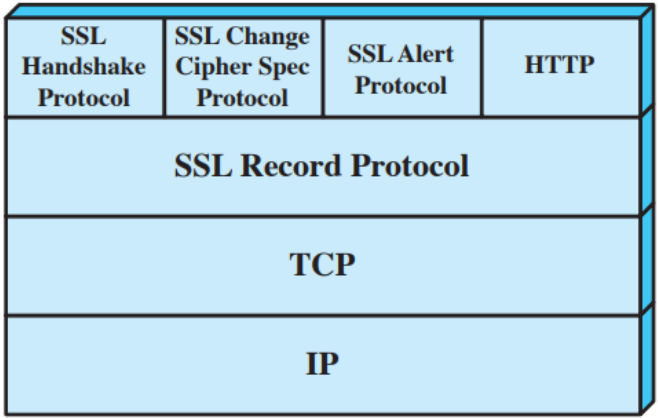


Figura: Cabeçalho SSL (STALLINGS; BROWN, 2015).

Protocolo / Conceito	Função Resumida
SSL Record Protocol	Camada base do SSL; provê **confidencialidade** (cifração simétrica) e **integridade** (MAC); fragmenta, comprime (opcional) e encapsula dados.
Handshake Protocol	Realiza **autenticação**, **negociação de algoritmos** e **estabelecimento de chaves**; cria a **sessão SSL**.
Change Cipher Spec Protocol	Envia mensagem única (valor 1) para ativar a **CipherSpec** negociada, movendo o estado pendente para o atual.
Alert Protocol	Envia alertas de erro ou evento: **warning** ou **fatal**; alertas fatais encerram a conexão.
Sessão SSL	Associação segura contendo **parâmetros criptográficos** compartilhados; pode ser reutilizada, evitando renegociação.
Conexão SSL	Canal temporário e seguro; usa parâmetros da sessão; uma sessão pode ter **múltiplas conexões**.

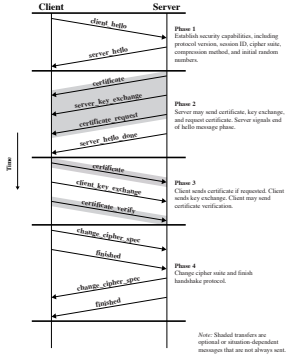


Figure 21.3 Handshake Protocol Action

Figura: Procolo de Apresentação (STALLINGS; BROWN, 2015).

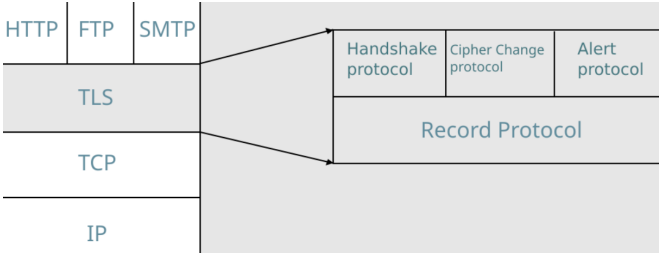


Figura: TLS

VPN — © 2026 ALVES, M.

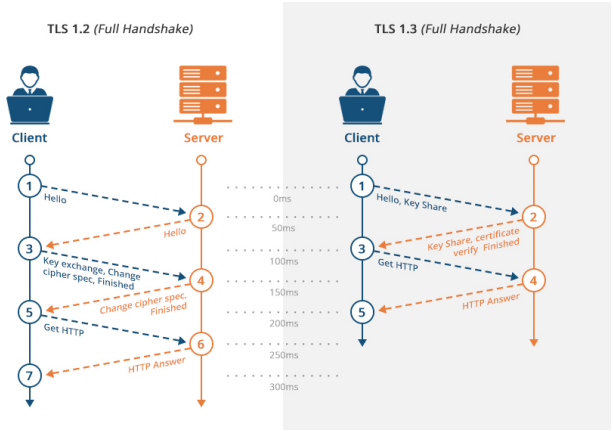


Figura: TLS 1.2 vs TLS 1.3

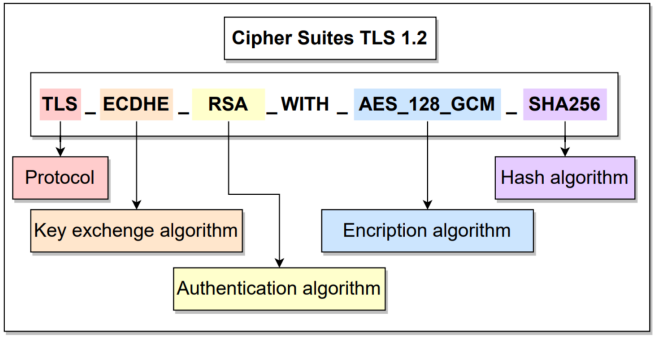


Figura: Cipher Suite

VPN — © 2026 ALVES, M.

SSH

- Secure Shell (SSH) é um protocolo para comunicações de rede seguras.
- Foi projetado para ser relativamente simples e pouco dispendioso de ser implementado.
- O SSH foi desenvolvido para substituir o TELNET, oferecendo comunicação criptografada.
- Suporta:
  - Conexão remota;
  - Transferência segura de arquivos (SCP).

VPN — © 2026 ALVES, M.

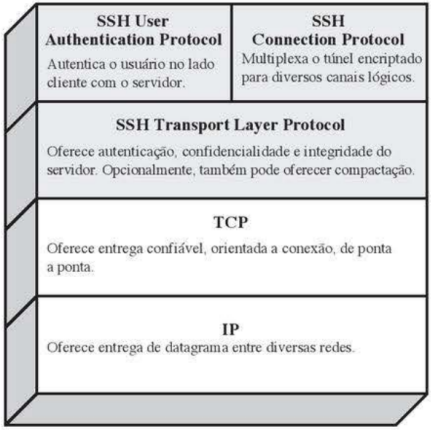


Figura: Pilha de Protocolos SSH (Stallings, 2020).

- Autenticação do usuário:
  - Baseada em senha
    - O usuário informa nome de usuário e senha
    - A senha é enviada criptografada com a chave pública do servidor
  - Baseada em chave pública (RSA)
    - O servidor mantém uma cópia da chave pública do usuário

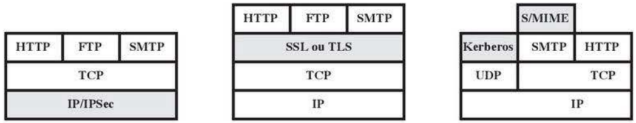
VPN — © 2026 ALVES, M.

```
# Conectar a um servidor remoto
ssh usuario@servidor.com

# Transferir arquivo seguro
scp arquivo.txt usuario@servidor.com:/destino/
```

VPN — © 2026 ALVES, M.

	SSH	**SSL/TLS**
Sigla	Secure Shell	Secure Socket Layer / Transport Layer Security
Protocolo/Porta TCP	TCP/22	TCP/443
Uso principal	Envio seguro de comandos em um servidor remoto	Comunicação segura entre dois hosts (ex.: navegador e servidor web)
Opções de autenticação	Usuário/senha, chaves SSH ou ambos	Normalmente utiliza certificados digitais X.509 para autenticação do cliente e do servidor
Baseado em	Túneis de rede criptografados	Certificados digitais
Tipo de protocolo	Protocolo de acesso remoto	Protocolo de segurança criptográfica
Objetivo	Reduzir ameaças de segurança no login e acesso remoto a servidores	Garantir transmissão segura entre servidor web e navegador cliente



Níveis de segurança na pilha TCP/IP (STALLINGS; BROWN, 2015).

Segurança na Pilha TCP/IP

A pilha TCP/IP apresenta múltiplos níveis de segurança distribuídos entre suas camadas, contemplando desde mecanismos na camada de enlace, como VPNs de camada 2 (ex.: L2TP), passando pela proteção na camada de rede com IPsec, pela segurança na camada de transporte com TLS, até soluções na camada de aplicação como SSH e HTTPS, além de protocolos específicos como S/MIME para proteção de e-mails, Kerberos para autenticação centralizada e DNSSEC para garantir a integridade e autenticidade das consultas ao DNS.

Capítulo 17 e 20 (Stallings, 2020)

VPN — © 2026 ALVES, M.

Bibliografia

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 8. ed. São Paulo: Pearson, 2021.

STALLINGS, William. **Cryptography and Network Security: Principles and Practice**. 8. ed. [*S. l.*]: Pearson, 2020.

STALLINGS, William; BROWN, Lawrie. **Computer security: principles and practice**. 1. ed. São Paulo: Pearson Prentice Hall, 2015. p. 492. ISBN 9788576051190.

TANENBAUM, Andrew S. **Computer Networks**. 4. ed. New Jersey: Prentice Hall, 2004. p. 813.

Estes slides estão protegidos por uma licença Creative Commons

Este modelo foi adaptado de Maxime Chupin.

Marisangila Alves, MSc
marisangila.alves@udesc.br
marisangila.com.br

UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA
JOINVILLE
CENTRO DE CIÊNCIAS TECNOLÓGICAS

UDESC
Universidade do Estado de Santa Catarina

2026/1

Segurança da Informação

Rede Privada Virtual