CS-045 · Network

VPNs

Encrypted tunnels that carry private traffic safely across untrusted networks.

Executive Summary

A virtual private network creates an encrypted tunnel that lets traffic travel privately across an untrusted network such as the public internet. VPNs are used to connect remote workers to an organization and to link entire sites together securely. They protect confidentiality and integrity in transit, but they are one control among many, not a complete security solution.

What It Is

A VPN, or virtual private network, extends a private network across a public one by wrapping traffic in an encrypted tunnel between two endpoints. There are two common patterns. A remote access VPN connects an individual user's device to an organization's network, so the user can reach internal resources as if they were on site. A site-to-site VPN connects two networks together, for example joining a branch office to a headquarters over the internet. VPNs rely on protocols that handle authentication, key exchange, and encryption, with IPsec and TLS-based VPNs among the most widely used. The result is that data moving between endpoints is protected from eavesdropping and tampering.

Why It Matters

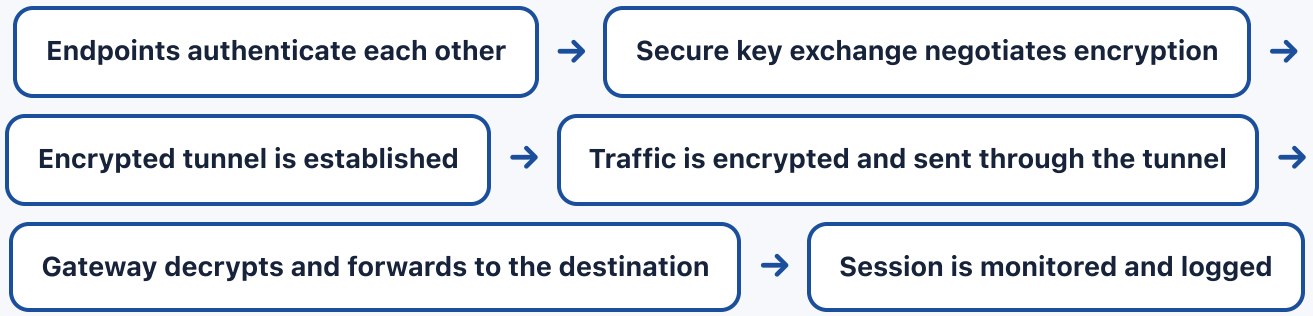
Sending sensitive traffic across networks you do not control, such as public Wi-Fi or the open internet, exposes it to interception. A VPN reduces that risk by encrypting the traffic so onlookers see only unreadable data. For organizations, VPNs enabled the shift to remote and hybrid work by giving distributed staff protected access to internal systems. At the same time, VPNs have become high-value targets: a compromised VPN can hand an attacker a foothold inside the network, so VPN gateways must be patched and protected with strong authentication.

Understanding both the benefits and the limits of VPNs is important for anyone securing modern access.

How It Works

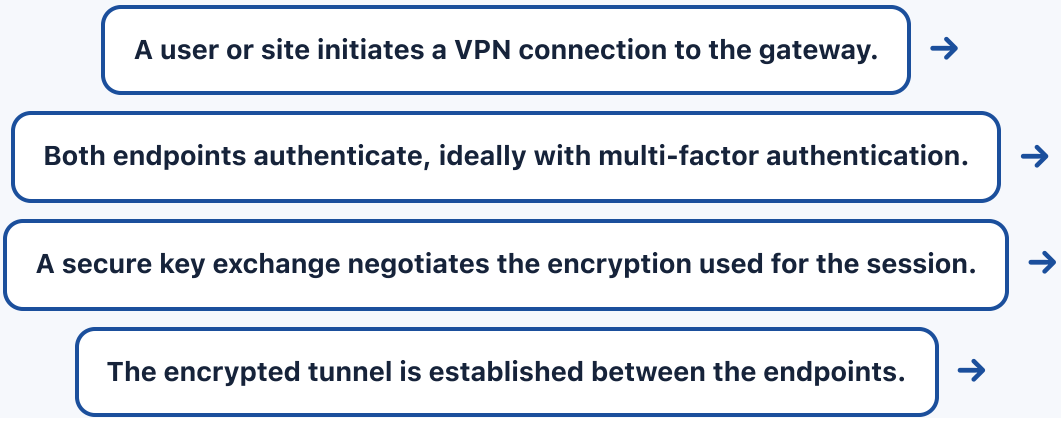
When a VPN connection is established, the two endpoints first authenticate each other, then negotiate encryption keys through a secure key exchange, and finally build the tunnel that carries encrypted traffic. In an IPsec VPN, this handshake and the encryption of packets follow the IPsec protocol suite. In a TLS-based VPN, the tunnel is built on the same transport security that protects websites. Once the tunnel is up, the client's traffic is encrypted, sent to the VPN gateway, decrypted, and forwarded to its destination, with replies returning the same way. Modern access designs increasingly pair or replace traditional VPNs with zero trust approaches that verify each request rather than granting broad network access after a single login.

Architecture Diagram



A VPN establishes trust, exchanges keys, and builds an encrypted tunnel so traffic crosses an untrusted network safely.

Visual Workflow



Traffic flows encrypted through the tunnel and is decrypted at the gateway. →

The gateway logs and monitors the session for anomalies.

Common Attacks

- Exploiting unpatched vulnerabilities in VPN gateway software
- Credential theft and brute force against VPN logins lacking strong authentication
- On-path attacks against weak or outdated VPN encryption
- Using a compromised VPN account as a foothold to move through the network
- Split-tunnel misconfigurations that expose the device to untrusted networks

Common Mistakes

- Leaving VPN gateways unpatched despite them being internet-facing
- Allowing VPN access with only a password and no multi-factor authentication
- Granting broad network access after login instead of least privilege
- Assuming a VPN alone makes a device or session fully secure
- Failing to monitor VPN logs for unusual access patterns

Best Practices

- Require multi-factor authentication for all VPN access
- Patch VPN gateways promptly because they are internet-facing targets
- Use current, strong encryption and disable outdated protocols
- Limit what an authenticated user can reach, following least privilege
- Log and monitor VPN sessions and consider a zero trust access model

Quick Checklist

- [x] Multi-factor authentication is enforced on all VPN logins
- [x] VPN gateway software is patched to a current, supported version

- [x] Only strong, current encryption protocols are enabled
- [x] Access after login is limited to what each role requires
- [x] VPN session logs are collected and monitored for anomalies

Recommended Tools

VPN gateway or concentrator
Terminates and manages encrypted tunnels for remote users or sites

IPsec or TLS VPN client
Establishes the encrypted tunnel from an endpoint device

Multi-factor authentication service
Adds a second factor to VPN login to resist credential theft

Zero trust access platform
Verifies each request rather than granting broad network access

Industry Standards

RFC 4301 (IPsec)
Defines the security architecture for the IPsec protocol suite

NIST SP 800-77
Guide to IPsec VPN deployment and configuration

NIST SP 800-207
Zero Trust Architecture, relevant to modern access models

Career Relevance

VPN deployment, hardening, and troubleshooting are common responsibilities for network security engineers and security engineers, while cloud security engineers connect environments with site-to-site tunnels and evaluate zero trust alternatives. SOC analysts investigate suspicious VPN logins as part of access monitoring. Because remote access is central to modern work, VPN knowledge is a practical skill across the roles that AI-Governance-Jobs.com serves.

Interview Questions

- What is the difference between a remote access VPN and a site-to-site VPN?
- How does a VPN establish an encrypted tunnel between two endpoints?
- Why are VPN gateways such attractive targets, and how do you protect them?
- What is split tunneling, and what are its trade-offs?
- How does a zero trust access model differ from a traditional VPN?

Related Certifications

CompTIA Security+ | **CompTIA Network+** | **Cisco CCNA Security**

Further Reading

- NIST SP 800-77: Guide to IPsec VPNs
- NIST SP 800-207: Zero Trust Architecture
- CISA: Selecting and Hardening Remote Access VPN Solutions

Key Takeaways

- A VPN builds an encrypted tunnel to protect traffic across untrusted networks.
- Remote access VPNs connect users; site-to-site VPNs connect whole networks.
- IPsec and TLS-based VPNs are the most widely used protocols.
- VPN gateways are high-value targets, so patching and MFA are essential.
- Zero trust models increasingly complement or replace broad VPN access.

FAQ

▶ **Does a VPN make me completely anonymous or secure?**

▶ **What is the difference between IPsec and TLS VPNs?**

▶ **Are VPNs being replaced by zero trust?**

Related Careers

RELATED ROLES

- Network Security Engineer
- Security Engineer
- Cloud Security Engineer

RELATED CERTIFICATIONS

- CompTIA Security+
- CompTIA Network+
- Cisco CCNA Security

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

- Career guides
- Role roadmaps
- Salary data
- Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **VPNs**
3. Go deeper: Firewalls
4. Go deeper: DNS Security
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

- CS-043 Firewalls
- CS-044 DNS Security
- CS-046 NAT
- CS-049 Proxy Servers
- CS-001 Cybersecurity