

VPN SECURITY
& EXPOSURE.

VPN gateways are internet-facing, always-on, and rarely patched on schedule — **making them one of the most exploited entry points into corporate networks**. From split-tunneling misconfigurations to unpatched appliance CVEs, a poorly governed VPN becomes the front door attackers actually use.

- PATCH CADENCE
- SPLIT-TUNNEL CONTROL
- MFA ENFORCEMENT
- EXPOSURE SCANNING

01 THE MECHANISM

Encrypted Tunnel
Establishes an **encrypted point-to-point channel** between the remote device and the corporate network before any traffic is exchanged.

Authentication Gateway
Verifies user identity — ideally with **MFA** — before granting the tunnel any network access.

Access Scoping
Determines **full tunnel vs. split tunnel routing**, controlling how much of a device's traffic actually passes through the tunnel.

02 THE FLOW

The Connection Cycle PER SESSION

1

User initiates connection; the VPN gateway **presents its certificate** and negotiates encryption.

2

Credentials and MFA are verified before a session token is issued.

3

Traffic is routed per policy — **full tunnel, split tunnel, or app-specific rules**.

The Exposure Cycle ONGOING

1

Vendor discloses a **CVE affecting the appliance's** authentication or session-handling code.

2

Exploit code often appears within days, targeting unpatched internet-facing gateways.

3

Unpatched, exposed portals are **scanned and compromised faster** than most patch cycles can respond.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Appliance Patch Management	Keeps VPN gateway firmware and software current against disclosed CVEs.
Strong Authentication	Enforces MFA and blocks credential-stuffing against the VPN login portal.
Tunnel & Routing Policy	Governs split-tunneling, DNS leakage, and which traffic bypasses inspection.
External Exposure Monitoring	Continuously scans for exposed VPN portals, expired certs, and default configs.

04 REMOTE ACCESS APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Password-Only VPN Login	No	Credential stuffing and phishing bypass a single-factor login easily.
Full-Tunnel Without Segmentation	No	A compromised endpoint gets broad network reach once connected.
Patch-When-Convenient Cadence	No	Exploit code frequently appears within days of a VPN CVE disclosure.
Perimeter VPN Alone (No ZTNA)	No	Grants network-level trust rather than per-application, per-request access.
Combined VPN Governance (MFA + Patch SLA + Segmentation + Monitoring)	Yes	Closes the gaps that turn VPNs into the most exploited entry point.

VPN SECURITY.

PATCH · AUTHENTICATE · MONITOR

05

PROGRAM OPERATIONS

VPN appliances are some of the most-targeted internet-facing assets. Public CVE disclosures are followed almost immediately by mass scanning.

Split tunneling trades convenience for exposure. Traffic that bypasses the tunnel also bypasses corporate inspection and logging.

Patch SLAs must be shorter for edge devices. A gateway sitting on the internet has far less room for a slow patch cycle than an internal server.

Legacy VPN is a stepping stone, not an endpoint. Most zero trust roadmaps plan to retire broad-access VPN in favor of per-application ZTNA.

06

CONTROL MAPPING

CISA VPN SECURITY GUIDANCE

Federal guidance for **hardening and monitoring remote access infrastructure**.

NIST SP 800-77

Guide to **IPsec VPNs** covering architecture and configuration.

CIS CONTROLS V8.1

Network infrastructure management and secure remote access safeguards.

NIST CSF 2.0

Protect function coverage for remote access and boundary defense.

07

WHAT THIS DOES NOT SOLVE

Compromised endpoint devices

A VPN secures the tunnel, not a **malware-infected laptop** connecting through it.

Credential reuse across services

Stolen credentials from unrelated breaches still work if **MFA isn't enforced**.

Zero-day appliance vulnerabilities

Even a fully patched gateway can be hit by a **vulnerability with no available fix yet**.

Insider misuse of granted access

Legitimate VPN sessions can still be used to **exfiltrate data or move laterally**.

08

MYTHS VS. REALITY

MYTH	REALITY
"Our VPN is encrypted, so it's secure."	Encryption protects data in transit; it does nothing about the authentication, patch, or config layers .
MYTH	REALITY
"Split tunneling just improves speed."	It also carves out unmonitored traffic paths that bypass corporate inspection.
MYTH	REALITY
"We patch VPN appliances on our normal cycle."	Internet-facing edge devices need faster SLAs than internal systems .
MYTH	REALITY
"VPN and ZTNA are the same thing."	VPN grants network access; ZTNA grants scoped, per-application access .
MYTH	REALITY
"MFA on VPN is optional if the password is strong."	Password-only VPN logins remain a leading initial-access vector regardless of password strength.

09

SPEAK THE PROGRAM — KEY TERMS

VPN

An **encrypted tunnel** connecting a remote device to a private network over the internet.

SPLIT TUNNELING

Routing only some traffic through the VPN tunnel while **the rest travels the local network directly**.

ZTNA

Zero Trust Network Access — grants **per-application, identity-verified access** instead of broad network trust.

CREDENTIAL STUFFING

Using breached username/password pairs from other sites to **attempt login on a different service**.

ATTACK SURFACE

The sum of every exposed entry point an attacker could target, **including VPN portals**.

PATCH SLA

The **maximum time allowed** between a vulnerability disclosure and applying its fix.