Edge devices: would you know if your firewall or VPN had been broken into?

This month, take every edge device's management interface off the internet and send its logs to a system the device can't erase, and replace anything past end of support within 12 months. When a flaw in one is exploited, assume the device is compromised: collect evidence, reset or rebuild it and rotate every credential it held, because a patch doesn't remove an attacker who is already in.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.1**

Written for

IT and network teams running firewalls, VPN gateways, routers, load balancers, file-transfer appliances and other internet-facing devices, in organizations of any size

Latest version

sheets.einblick.dev/edge-devices/

If you only do five things

1. **Know every device that faces the internet.** List each firewall, VPN gateway, router, load balancer and file-transfer appliance with its software version and end-of-support date, and scan your address ranges for the ones nobody listed. CISA, the FBI and the NCSC urge every organization to keep that inventory[1].
2. **Take management interfaces off the internet.** Allow admin access only from a dedicated management network[3] or a short list of trusted addresses. The BSI found that firewall operators were hit less often, even by zero-days, when management access was restricted to trusted sources[4].
3. **Put strong MFA on every login the device accepts.** Require phishing-resistant MFA for admin access[3] and the strongest MFA the VPN supports for every user, as the passkeys and MFA sheet describes. VPN access made up 44% of the connection types in the initial access broker offers Verizon analyzed[5].
4. **Send the logs somewhere the device can't erase.** Forward detailed logs to a central system and alert on admin logins, configuration changes and hardware changes[3]. Keep them for at least 12 months, as Mandiant advises for network devices' admin logs: BRICKSTORM intrusions averaged 393 days of dwell time[6].
5. **Replace devices before support ends.** An unsupported device won't get the fix for the next exploited flaw. Budget each replacement a year before its end-of-support date, and add compensating controls for any you can't remove in time[3].

Check a device after an exploited flaw

Collect evidence first, patch within the patching sheet's deadlines, then check every device the flaw could reach before the patch.

1. **Capture evidence before you patch or reboot.** Before updating, store logs off the device and take a disk and memory snapshot, as CISA required for Cisco SD-WAN[8], and export the configuration. If you find signs of compromise, disconnect the device but keep it powered on[9].
2. **Don't trust a clean integrity check.** CISA warns that Ivanti's checker can miss attacker commands that run only in memory[11]. On FortiGates, a file link planted by attackers could survive patching[12].
3. **Look for new admin accounts and changed settings.** In attacks Fortinet disclosed in January 2026, attackers downloaded configurations and added local admins such as `audit` and `backup`[13]. Compare configurations and firmware hashes with your offline copies and the vendor's values[15].
4. **Reset or rebuild, then upgrade.** Follow the vendor's recovery steps, such as a factory reset or new virtual instance for Ivanti[11] or a reimage for Cisco Firepower[10]. Review any configuration you restore.
5. **Rotate every secret the device held.** Reset the domain, admin and local account passwords, reissue stored certificates and replace API keys and license server credentials[11]. End live sessions too, as Citrix's `kill` commands did after CVE-2025-5777[14].
6. **Hunt behind the device.** Check what the device's accounts and VPN users did in directory, server and cloud logs since the first known exploitation. Attackers can use access they set up months or years later[4].

Harden what stays exposed

- **Switch off what you don't use.** Disable unused ports, protocols and features, including management protocols[15,4]. FortiGates that had never enabled SSL-VPN weren't affected by the file-link persistence[12].
- **Use only encrypted management.** Allow SSH, HTTPS and SNMPv3, and block outbound connections from the management interface except to your AAA, syslog and telemetry collectors[15].
- **Turn off vendor cloud logins you don't need.** A FortiCloud single sign-on bypass let attackers into FortiGates that had it enabled[13]. If you keep such a feature, log and review every use.
- **Give the device as few secrets as possible.** Bind it to the directory with a dedicated low-privilege account over LDAPS. Attackers use the devices' own packet capture to collect plaintext credentials[6].

What to demand from vendors

- **An end-of-support date before you buy.** From 11 December 2027, the EU Cyber Resilience Act requires manufacturers of new products to state it at the time of purchase[17]. Put it in the contract.
- **Logs and evidence built in.** Ask for TLS-protected remote logging, a record of admin actions and a supported way to collect memory and disk, as the NCSC specifies for network devices[16].
- **A way to prove the device is clean.** Ask for an integrity tool and a recovery procedure that removes persistence. On Cisco Firepower, neither a reboot nor the patch did[9].
- **Secure management out of the box.** Phishing-resistant MFA for admins and no management interface on the internet by default. Canada's Cyber Centre says customers should demand that vendors harden devices to secure management interfaces[3].

- **Keep it away from the core.** Zones, firewall rules and admin paths are in the network segmentation sheet.

What changed in 2026

- **CISA set deadlines for end-of-support edge devices.** BOD 26-02 of February 2026 gives US federal civilian agencies 12 to 18 months to remove them[2]; CISA, the FBI and the NCSC urge everyone to follow it[1].
- **Patches and reboots didn't clear Cisco firewalls.** In April 2026, CISA had federal civilian agencies hard-reset them[9]; Cisco advises reimaging[10].
- **Ivanti's checker can miss in-memory attacks.** In October 2026, CISA warned that it may not detect exploitation of CVE-2026-104935 in Connect Secure, and that confirming it takes network and memory forensics. Connect Secure 22.8 reaches end of life on 31 January 2027[11].

What you can skip

- **Country blocking as your main defense.** Attackers route through covert networks of compromised routers that can be rapidly reshaped[18]. Treat geo-blocks and static blocklists as noise filters, not protection.
- **A clean perimeter pen test as proof of safety.** Google counted 14 zero-days in edge devices in 2025 and thinks that undercounts[7]. No test finds next month's flaw.
- **Ripping out the VPN in a hurry.** The NCSC advises keeping it until other controls give the same protection[19]. A ZTNA connector or cloud gateway is an edge device too, so inventory, harden and log it the same way.

Mistakes that cost the most

- **Marking a device patched on a still-vulnerable version.** CISA found agencies doing this with Cisco firewalls[9]. Check the fixed releases.
- **Restoring the attacker's configuration.** A post-compromise backup can bring back their admin accounts, so Fortinet and Cisco say to treat all configuration as compromised[12,10]. Restore a checked backup or rebuild.
- **Overlooking small and remote devices.** Verizon found 45,000 to 50,000 end-of-life cellular modems with an exposed management interface in 2025, and saw such devices reused as attack proxies[5].

What this looks like at your size

Small team, no security staff

- Ask your IT provider to list every internet-facing device with its end-of-support date, and replace any past it.
- Get free exposure alerts from Shadowserver[20]. In Germany, CERT-Bund alerts the operator of your IP range[22]; UK-based organizations can join NCSC Early Warning[21].
- Check that the firewall's admin page is reachable only from inside and that VPN users need MFA.

Growing, with IT or security staff

- Forward firewall and VPN logs to your SIEM or log service, keep 12 months and alert on admin logins and configuration changes.
- Write a one-page compromise check per vendor: integrity tool, evidence to collect, reset steps and credentials to rotate.
- Add end-of-support dates to the asset inventory and budget replacements a year ahead.

Enterprise or regulated

- Manage devices only over an out-of-band network from dedicated admin workstations[3].
- Score vendors against the NCSC's forensic and monitoring specification in procurement[16].
- Use BOD 26-02's timelines as your benchmark and keep an incident response retainer that covers appliance forensics.

Version history

5 Nov 2026, version 1.1	Reviewed for company readers: added CERT-Bund's reports for German network operators and limited NCSC Early Warning to UK-based organizations.

Sources

1. Reducing the Attack Surface for End-of-Support Edge Devices. CISA, FBI and NCSC (UK), 5 Feb 2026. cisa.gov
2. BOD 26-02: Mitigating Risk From End-of-Support Edge Devices. CISA, 5 Feb 2026. cisa.gov
3. Security considerations for edge devices (ITSM.80.101). Canadian Centre for Cyber Security, Feb 2025. cyber.gc.ca
4. The State of IT Security in Germany 2025: Vulnerabilities in perimeter systems. BSI, 11 Nov 2025. medien.bsi.bund.de
5. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
6. M-Trends 2026 Executive Edition. Google Cloud (Mandiant), Mar 2026. services.google.com
7. Look What You Made Us Patch: 2025 Zero-Days in Review. Google Threat Intelligence Group, 5 Mar 2026. cloud.google.com
8. V1: ED 26-03: Mitigate Vulnerabilities in Cisco SD-WAN Systems. CISA, 11 Mar 2026. cisa.gov
9. ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices (with V1 and implementation note). CISA, updated 23 Apr 2026. cisa.gov
10. Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense. Cisco PSIRT, updated 19 May 2026. sec.cloudapps.cisco.com
11. CISA Urges Patching Newly Exploited Vulnerabilities in Ivanti Connect Secure. CISA, updated 30 Oct 2026. cisa.gov
12. Analysis of Threat Actor Activity. Fortinet PSIRT, 10 Apr 2025. fortinet.com
13. FG-IR-26-060: Administrative FortiCloud SSO authentication bypass. Fortinet PSIRT, 27 Jan 2026. fortiguard.com
14. NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-5349 and CVE-2025-5777 (CTX693420). Citrix, revised 20 Jul 2026. support.citrix.com
15. Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System (AA25-239A). NSA, CISA, FBI and international partners, updated 3 Sep 2025. cisa.gov
16. Guidance on digital forensics and protective monitoring specifications for producers of network devices and appliances. NCSC (UK), 4 Feb 2025. ncsc.gov.uk
17. Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 13(19), 69 and 71. EUR-Lex, 2024. eur-lex.europa.eu
18. Executive Summary: Defending against China-nexus covert networks of compromised devices. NCSC (UK), 23 Apr 2026. ncsc.gov.uk
19. Zero trust migration: How will I know if I can remove my VPN?. NCSC (UK), reviewed 16 Jan 2026. ncsc.gov.uk
20. Subscribe to Reports. Shadowserver Foundation, checked 3 Nov 2026. shadowserver.org
21. Early Warning. NCSC (UK), checked 3 Nov 2026. ncsc.gov.uk
22. CERT-Bund Reports. BSI, checked 5 Nov 2026. bsi.bund.de