Pare-feux, VPN, SD-WAN : pourquoi les APT font de vos équipements…

> Analyse d'expert : pourquoi les APT étatiques ciblent en priorité les équipements réseau (pare-feux, VPN, SD-WAN) en 2026. Tendance documentée, CVE…

Vos pare-feux protègent votre réseau. Les groupes APT étatiques l'ont compris avant vous. En 2025 et 2026, la tendance est documentée, massive et sous-estimée : les attaquants sophistiqués ne cherchent plus à compromettre un poste utilisateur ou à voler des identifiants via phishing. Ils visent directement l'équipement censé tout protéger. Et dans la plupart des organisations, personne ne surveille vraiment le pare-feu de l'intérieur.

Points clés à retenir

• La cybersécurité proactive prévaut sur la réaction post-incident pour limiter l'impact

• La documentation et les procédures formalisées sont essentielles lors des audits et certifications

• La veille continue et la mise à jour régulière des compétences sont indispensables face à l'évolution des menaces

Le glissement du vecteur initial : de l'utilisateur à l'appliance

Pendant une décennie, le modèle d'attaque dominant des groupes étatiques et des ransomwares sophistiqués suivait une séquence prévisible : un e-mail de spear-phishing, un clic malheureux, un agent malveillant sur un poste utilisateur, puis un mouvement latéral vers les ressources sensibles. Cette séquence a généré l'industrie EDR telle qu'on la connaît aujourd'hui. CrowdStrike, SentinelOne, Microsoft Defender for Endpoint — tous conçus pour surveiller les endpoints, détecter les comportements anormaux, couper l'agent malveillant avant qu'il ne se déplace.

⚡ Retour terrain

Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans

supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

Le problème, du point de vue de l'attaquant, est que cette défense fonctionne de mieux en mieux. Les taux de détection sur les endpoints correctement protégés ont considérablement progressé entre 2022 et 2025. Les groupes étatiques — qui opèrent avec des contraintes de discrétion que les cybercriminels classiques n'ont pas, notamment l'obligation de rester non détectés pendant des mois ou des années — ont donc logiquement pivoté vers des vecteurs moins surveillés.

Les équipements réseau périmètriques sont le choix idéal pour plusieurs raisons structurelles. D'abord, ils ne font pas tourner d'agent EDR — personne n'installe SentinelOne sur un pare-feu Palo Alto ou un concentrateur VPN Ivanti. Ensuite, ils sont positionnés en coupure entre Internet et le réseau interne, ce qui leur confère une visibilité maximale sur tout le trafic de l'organisation. Enfin, ils hébergent des informations de configuration extraordinairement sensibles : règles de sécurité, credentials VPN, certificats TLS, plans d'adressage réseau, parfois des clés d'API vers des services cloud.

Le rapport Verizon DBIR 2026, publié en avril, documente pour la première fois que les vulnérabilités dans les équipements périmètriques dépassent le vol d'identifiants comme vecteur initial dans les intrusions attribuées à des acteurs étatiques. Ce n'est pas une surprise pour ceux qui suivent les advisories CISA depuis 2024, mais c'est la première fois que la donnée statistique agrégée confirme le changement de paradigme à cette échelle.

Les chiffres qui documentent la bascule

Pour mesurer l'ampleur du phénomène, il suffit de regarder le catalogue KEV (Known Exploited Vulnerabilities) de la CISA sur les 18 derniers mois. Sur les 340 entrées ajoutées au catalogue entre janvier 2025 et mai 2026, 127 — soit 37% — concernent des équipements réseau ou des appliances de sécurité : Palo Alto PAN-OS, Cisco IOS XE et SD-WAN, Ivanti Connect Secure et EPMM, Fortinet FortiOS et FortiClient, SonicWall SonicOS, F5 BIG-IP. La proportion est sans précédent comparée aux périodes antérieures.

Quelques chiffres marquants de cette période :

CVE-2025-0108 (Palo Alto PAN-OS Authentication Bypass) : exploité en moins de 24 heures après publication de la faille, par au moins 3 groupes distincts selon Unit 42.

CVE-2025-22457 (Ivanti Connect Secure) : zero-day exploité par le groupe UNC5221 pendant plus de 3 semaines avant que la faille soit identifiée et documentée par Mandiant.

CVE-2026-20182 (Cisco SD-WAN, CVSS 10.0) : exploité par le groupe UAT-8616 pour compromettre plusieurs centaines d'entreprises industrielles, principalement en Europe et en Asie du Sud-Est.

CVE-2026-0300 (Palo Alto PAN-OS Captive Portal, CVSS 9.3) : exploitation active confirmée dès le jour de la divulgation, attribuée provisoirement au cluster étatique CL-STA-1132.

CVE-2026-42945 (NGINX Rift, CVSS 9.2) : PoC public en moins de 24 heures, scans automatisés débutés dans les heures suivantes sur des centaines de milliers de serveurs.

Côté ransomware, la tendance est identique mais avec une motivation différente. Les groupes LockBit 4.0, Qilin et Black Basta ont documenté dans leurs propres communications internes — exfiltrées ou analysées par les chercheurs — que la compromission d'équipements périmètriques permet d'accélérer considérablement la phase de déplacement latéral et d'accès aux backups, deux étapes critiques pour maximiser l'impact d'une attaque ransomware.

Pourquoi les équipements réseau ? L'anatomie d'un choix tactique

Pour comprendre pourquoi les pare-feux et VPN sont devenus la cible préférée des attaquants sophistiqués, il faut se mettre dans la peau d'un opérateur APT avec des contraintes opérationnelles réelles. Trois facteurs dominent ce choix.

L'angle mort de la détection. Un pare-feu Palo Alto, un concentrateur Ivanti Connect Secure ou un contrôleur Cisco SD-WAN sont des appliances propriétaires qui font tourner un OS embarqué sur lequel l'équipe sécurité de l'organisation n'a pratiquement aucune visibilité comportementale. Les logs disponibles sont limités à ceux que l'appliance veut bien exporter — et un attaquant qui a des privilèges root sur l'appliance peut modifier ces exports. Il n'y a pas de EDR, pas d'agent

SIEM, pas de surveillance des processus système. La télémétrie se limite aux NetFlow et aux logs d'accès applicatifs, qui peuvent être manipulés ou purgés.

La persistance facilitée. Sur un pare-feu compromis, un attaquant peut installer un implant dans le firmware, modifier les scripts d'initialisation, ou créer une règle de redirection de trafic qui restera active à travers les redémarrages et même certaines mises à jour mineures. Les opérations Volt Typhoon documentées par le FBI et la CISA en 2024 et 2025 ont montré que des implants dans des équipements réseau pouvaient rester actifs pendant plus de 5 ans sans être détectés. Cette durabilité est hors de portée sur un endpoint correctement maintenu avec des outils EDR modernes.

La valeur stratégique de la position réseau. Un pare-feu compromis, c'est potentiellement un décrypteur SSL sur le chemin de tout le trafic. C'est la possibilité de capturer silencieusement toutes les communications, d'y injecter du code, ou de rediriger des connexions vers des serveurs contrôlés par l'attaquant. Pour un groupe de collecte de renseignement, cette position est incomparablement plus précieuse qu'un accès à un poste utilisateur individuel. Pour un groupe préparant une action destructrice — sabotage industriel, perturbation d'infrastructures critiques —, le contrôle du pare-feu permet de couper les communications de l'organisation en un instant.

Le catalogue des vulnérabilités qui ont changé la donne

La multiplication des CVE critiques dans les équipements réseau n'est pas un hasard. Elle reflète une réalité structurelle : ces appliances sont des systèmes complexes, souvent développés avec des pratiques de sécurité du code moins matures que les éditeurs de logiciels grand public, et opérant dans des contextes où les mises à jour sont différées par les organisations pour éviter les interruptions de service.

Les typologies de vulnérabilités les plus récurrentes observées depuis 2024 :

Authentification bypass pré-auth : CVE-2025-0108 (Palo Alto), CVE-2024-55591 (FortiOS), CVE-2023-46805 (Ivanti Connect Secure). Dans les trois cas, des endpoints HTTP accessibles sans authentification permettaient l'accès à des fonctionnalités administratives ou à des tokens de session valides.

Buffer overflow dans les composants exposés : CVE-2026-0300 (Palo Alto Captive Portal), CVE-2026-42945 (NGINX Rift), CVE-2025-3102 (SonicWall SonicOS). Ces failles existent car les composants réseau traitent des inputs non fiables avec des primitives C/C++ sans les protections mémoire modernes systématiquement appliquées dans d'autres contextes.

Injection de commandes dans les interfaces de gestion : CVE-2024-3400 (Palo Alto GlobalProtect), permettant à un attaquant non authentifié d'exécuter des commandes OS arbitraires via un paramètre d'URL non validé côté serveur.

Logique d'autorisation défaillante : CVE-2026-20182 (Cisco SD-WAN), où les contrôles d'autorisation étaient partiellement vérifiés côté client, facilement contournables depuis le serveur.

Ce qui est frappant dans ces vulnérabilités, c'est leur nature : pas de complexité cryptographique, pas d'attaque de type side-channel ou d'exploitation de micro-architecture. Ce sont des bugs fondamentaux — des débordements de buffer, des défauts de validation d'entrées, des oublis d'authentification — dans des produits vendus des dizaines de milliers d'euros l'unité et présentés comme le rempart de la sécurité réseau. Cela pose des questions légitimes sur les pratiques de développement sécurisé (SDLC) et les processus de revue de code de ces éditeurs.

Ce que les attaquants font une fois à l'intérieur

Une fois l'accès root obtenu sur l'appliance, la phase post-exploitation suit des patterns relativement standardisés, documentés dans les rapports d'incident de Mandiant, CrowdStrike et Secureworks publiés en 2025 et 2026.

Phase 1 : persistance et réduction du bruit. L'attaquant désactive ou modifie la journalisation locale, installe un implant dans une zone de stockage persistante (partition de firmware, scripts d'initialisation système), et établit un canal de commandement et contrôle discret — souvent via HTTPS vers des CDN ou des services cloud légitimes pour se fondre dans le trafic normal. Dans les opérations de Volt Typhoon analysées par le CISA, les implants communiquaient exclusivement via des équipements SOHO compromis pour éviter toute corrélation avec des infrastructures C2 connues.

Phase 2 : collecte de renseignements réseau. La configuration complète de l'appliance est exfiltrée : règles de filtrage, VLANs, tables de routage, credentials utilisateurs VPN, certificats. Ces informations permettent de cartographier précisément l'architecture interne, d'identifier les systèmes critiques — Active Directory, systèmes SCADA dans les contextes OT/ICS, bases de données — et de préparer le mouvement latéral avec une connaissance parfaite du terrain.

Phase 3 : capture de trafic et exfiltration longue durée. Dans les cas documentés d'espionnage étatique, l'attaquant installe ou active des capacités de capture de trafic SSL/TLS. Sur un équipement qui effectue déjà du SSL inspection pour le compte de l'organisation, l'attaquant accède aux clés de déchiffrement déjà présentes. Sur un équipement qui ne fait pas de SSL inspection, il peut modifier la configuration pour l'activer silencieusement. Les flux déchiffrés peuvent ensuite être filtrés à la recherche de communications sensibles et exfiltrés par petits paquets sur de longues durées.

Phase 4 (scénarios destructeurs) : Dans les contextes OT/ICS ou d'attaque contre des infrastructures critiques, la phase finale peut consister à modifier les règles de filtrage pour couper des communications opérationnelles au moment choisi, ou à désactiver les mécanismes de haute disponibilité pour maximiser l'impact d'une action coordonnée.

Les angles morts défensifs côté entreprise

La majorité des organisations sont structurellement mal positionnées pour détecter et répondre à une compromission d'équipement réseau. Les raisons s'additionnent et se renforcent mutuellement.

Le SIEM ne reçoit pas les bons logs. La plupart des déploiements SIEM en entreprise ingèrent les logs applicatifs des appliances réseau — connexions VPN, règles de filtrage matchées, alertes IPS — mais pas la télémétrie système de l'OS embarqué. Les processus démarrés sur l'appliance, les fichiers modifiés dans le filesystem, les connexions réseau initiées par l'appliance elle-même : rien de tout cela n'est visible dans la grande majorité des SOC. Un attaquant qui exfiltre des données depuis le pare-feu lui-même n'apparaît dans aucun dashboard.

Les politiques de mise à jour sont incompatibles avec la réactivité requise. Un pare-feu en production est rarement mis à jour au fil de l'eau. Les équipes réseau appliquent les patches lors des fenêtres de maintenance planifiées, souvent mensuelles ou trimestrielles, pour éviter les interruptions de service. Avec des CVE critiques exploitées en moins de 24 heures après publication — comme CVE-2026-0300 ou CVE-2025-0108 —, cette cadence est structurellement insuffisante pour les équipements périmètriques exposés à Internet.

Le périmètre d'exposition n'est pas connu précisément. Combien de services sont accessibles depuis Internet sur votre pare-feu ? L'interface de gestion est-elle exposée ? Le Captive Portal ? GlobalProtect ? Dans de nombreuses organisations, la réponse à ces questions nécessite un audit manuel fastidieux parce que la cartographie n'est pas tenue à jour. Un attaquant, lui, scanne en permanence et automatiquement.

L'intégrité de la configuration n'est pas vérifiée. Existe-t-il une baseline documentée de la configuration de votre pare-feu, comparée régulièrement avec la configuration active ? Dans la majorité des cas, non. Une règle ajoutée par un attaquant qui a compromis l'appliance peut rester en place indéfiniment si personne ne compare la configuration avec une référence connue. Cette lacune est documentée dans plusieurs des incidents Palo Alto analysés en 2024 et 2025 : des règles permissives persistaient depuis plusieurs mois dans la configuration active sans avoir déclenché la moindre alerte.

Comment reprendre la main — recommandations terrain

La bonne nouvelle est que les mesures efficaces ne nécessitent pas de budget illimité. Elles nécessitent une discipline opérationnelle que beaucoup d'organisations appliquent déjà aux serveurs et aux endpoints, et qui n'a jamais vraiment été transposée aux appliances réseau.

Réduire la surface exposée à Internet. L'interface de gestion de votre pare-feu ne doit jamais être accessible depuis Internet. Le Captive Portal, GlobalProtect Gateway, les endpoints SNMP et SSH de l'appliance — chaque service inutilement exposé est un vecteur potentiel. Un scan externe mensuel de vos propres équipements périmètriques (avec des outils comme Shodan

Monitor, Censys ou vos propres scripts) est indispensable pour maintenir une cartographie précise de ce qui est réellement accessible depuis l'extérieur.

Traiter les CVE critiques sur appliances comme des incidents majeurs. Quand une CVE CVSS >= 9.0 est publiée sur Palo Alto PAN-OS, Ivanti, Cisco IOS XE ou Fortinet FortiOS, la réponse ne peut pas attendre la prochaine fenêtre de maintenance planifiée. Il faut un processus de patch d'urgence — avec validation en environnement de test et plan de rollback documenté — capable de déployer le correctif sur les équipements exposés à Internet en moins de 48 heures. Si le correctif n'est pas disponible, les mitigations alternatives doivent être appliquées dans les 24 heures.

Exporter et baseler la télémétrie système des appliances. La plupart des équipements réseau modernes supportent l'export de logs système via syslog ou des APIs REST. Configurer l'export de la télémétrie maximale disponible vers le SIEM, et définir des alertes sur les anomalies (connexions sortantes inattendues depuis l'appliance, modifications de configuration non planifiées, erreurs système inhabituelles) est une mesure de détection à fort rapport coût/efficacité. Les solutions SIEM modernes disposent de parseurs natifs pour les principaux équipements du marché.

Implémenter la vérification d'intégrité de configuration. Exporter quotidiennement la configuration de vos appliances réseau critiques et comparer automatiquement avec la version précédente. Toute modification non tracée dans votre système de gestion des changements (CMDB) doit déclencher une alerte. Des outils open source comme Oxidized ou Rancid permettent d'automatiser cette collecte pour la plupart des équipements du marché. C'est une mesure simple, peu coûteuse, et qui aurait permis de détecter plusieurs des incidents documentés en 2025 bien plus tôt.

Segmenter la gestion des appliances. L'accès à l'interface d'administration de vos équipements réseau doit transiter par un réseau de management dédié, séparé du trafic de production, avec des contrôles d'accès forts : authentification multifacteur, jump server enregistrant les sessions, liste blanche d'adresses IP sources. Un attaquant qui a compromis un poste utilisateur — même un poste administrateur — ne doit pas avoir accès direct au plan de gestion de votre infrastructure réseau.

Tester régulièrement les capacités de détection. La seule façon de savoir si votre SOC détecterait réellement une compromission de pare-feu est de le tester. Des simulations

d'exploitation d'équipements réseau — sous la forme d'exercices red team ciblés sur les appliances périmètriques, en environnement contrôlé — permettent de valider les capacités de détection et d'identifier les angles morts avant qu'un attaquant réel ne les exploite. Ces exercices sont encore rares en France, ce qui explique en partie que les angles morts persistent.

AVIS DrXPERT

Mon avis d'expert

La tendance est claire et elle ne va pas s'inverser. Les groupes APT vont continuer à prioriser les équipements réseau tant que ceux-ci resteront des zones grises de la détection. Ce que je vois sur le terrain, c'est que la grande majorité des organisations traitent encore leur pare-feu comme un équipement réseau — avec les processus réseau (changements planifiés, mises à jour différées, peu de monitoring comportemental) — alors qu'il devrait être traité comme un actif de sécurité critique soumis aux mêmes exigences de surveillance, d'intégrité et de réactivité qu'un contrôleur de domaine. Le changement est culturel autant que technique. Et c'est précisément ce fossé que les attaquants exploitent méthodiquement depuis deux ans.

Conclusion : le pare-feu n'est plus une boîte noire de confiance

La compromission d'un équipement réseau par un groupe étatique représente un scénario d'impact maximal : accès persistant et discret, visibilité totale sur le trafic, position idéale pour se déplacer latéralement ou préparer une action destructrice. Ce n'est plus un scénario hypothétique — c'est le quotidien documenté des réponses à incident de 2025 et 2026, confirmé par les rapports de Mandiant, CrowdStrike et Verizon.

La réponse ne passe pas par le remplacement des équipements ni par des budgets pharaoniques. Elle passe par l'application disciplinée de principes déjà connus — réduction de la surface exposée, patch management réactif, monitoring de l'intégrité, télémétrie système — transposés enfin aux appliances réseau avec le même niveau d'exigence qu'aux autres actifs critiques. Les organisations qui feront ce changement en 2026 réduiront significativement leur exposition aux

campagnes APT documentées. Celles qui ne le feront pas continueront à offrir aux attaquants exactement ce qu'ils cherchent : une porte dérobée que personne ne surveille.

Besoin d'un regard expert sur votre sécurité réseau ?

Ayi NEDJIMI réalise des audits ciblés de la surface d'attaque réseau et de la configuration de vos équipements périmètriques. Discutons de votre contexte spécifique.

Prendre contact

Bonnes pratiques opérationnelles pour protéger vos équipements réseau

Face à la montée en puissance des attaques APT ciblant les équipements périmètriques, les équipes sécurité doivent adopter une posture proactive. Les recommandations suivantes constituent un socle minimal pour réduire la surface d'attaque de vos pare-feux, concentrateurs VPN et appliances réseau.

Segmentation et accès privilégiés : L'accès à l'interface d'administration des équipements réseau doit être strictement limité à un réseau de gestion dédié, isolé du trafic de production. L'authentification multi-facteurs (MFA) doit être imposée sur tous les accès administrateurs, y compris les accès console locaux lorsque c'est techniquement possible. Les comptes de service génériques doivent être éliminés au profit de comptes nominatifs tracés dans un PAM (Privileged Access Management). Sans cette séparation, un attaquant qui compromet un poste d'administration dispose d'un accès direct aux interfaces de configuration des équipements réseau.

Gestion des correctifs et surveillance : Un processus de veille sur les CVE affectant vos équipements réseau doit être formalisé et testé. La CISA publie des advisories sur les vulnérabilités activement exploitées — s'y abonner est la première mesure de base. Le délai cible de patching pour les vulnérabilités CVSS ≥ 9.0 sur des équipements exposés sur Internet ne doit

pas dépasser 48 à 72 heures. En parallèle, la configuration d'export des logs vers un SIEM centralisé permet de détecter des comportements anormaux : connexions depuis des plages IP inattendues, tentatives d'authentification répétées, accès à des fichiers de configuration sensibles.

Tests et exercices : Un test de pénétration focalisé sur les équipements périmètriques (External Network Pentest) devrait être réalisé au minimum annuellement, idéalement après chaque changement de version majeure du firmware. Les scénarios de tabletop exercises doivent intégrer le cas de compromission d'un pare-feu ou d'un VPN concentrator comme point d'entrée initial — scénario désormais plausible et documenté par les rapports de threat intelligence. La réponse à cet incident particulier doit être documentée dans le plan de réponse aux incidents de l'organisation.

À RETENIR

Points clés à retenir

Le glissement du vecteur initial : de l'utilisateur à l'appliance

Les chiffres qui documentent la bascule

Pourquoi les équipements réseau ? L'anatomie d'un choix tactique

Le catalogue des vulnérabilités qui ont changé la donne

Ce que les attaquants font une fois à l'intérieur

Ressources et références pour la veille sur les APT ciblant les équipements réseau

Pour maintenir une veille efficace sur les nouvelles vulnérabilités et les campagnes APT ciblant les équipements réseau périmètriques, plusieurs ressources de référence sont indispensables. Le catalogue KEV (Known Exploited Vulnerabilities) de la CISA est actualisé quotidiennement et liste les vulnérabilités activement exploitées en condition réelle — son abonnement par flux RSS ou API REST est la première mesure de veille à mettre en place. Les advisories du CERT-FR et

les bulletins de sécurité des fabricants (Palo Alto Networks, Cisco PSIRT, Fortinet PSIRT, Ivanti Security Advisories) complètent cette veille avec des informations techniques approfondies sur les vulnérabilités et les correctifs disponibles pour chaque équipement de l'organisation.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité

