FortiGate Durcissement : Benchmark CIS et Guide 2026

> Le durcissement d'un FortiGate ne se limite pas à activer l'IPS et le pare-feu applicatif. Un firewall Fortinet mal configuré expose l'organisation à des vecteurs d'attaque documentés — des VPN SSL sans MFA aux comptes admin par défaut, en passant par les CVE critiques non patchées. Ce guide applique le CIS Benchmark FortiOS, le DISA STIG et les recommandations ANSSI pour vous fournir un référentiel de durcissement exhaustif et actionnable en 2026.

Le FortiGate de Fortinet est l'un des pare-feux NGFW les plus déployés en France et en Europe, particulièrement dans les PME, les ETI et les administrations publiques. Sa richesse fonctionnelle — inspection SSL, contrôle applicatif, SD-WAN, VPN IPsec et SSL, protection DNS, sandboxing FortiSandbox — en fait un composant central de la sécurité du SI. Mais cette richesse fonctionnelle est aussi son principal vecteur de risque : chaque fonctionnalité mal configurée ouvre une surface d'attaque potentielle. Les exemples ne manquent pas — la CVE-2024-21762 sur le SSL-VPN a permis l'exécution de code à distance sans authentification sur des millions d'appareils FortiGate exposés sur Internet, dont une proportion significative n'avait reçu aucun durcissement spécifique au-delà de la configuration par défaut. Ce guide compile les contrôles de sécurité issus du **CIS Benchmark FortiOS**, du **DISA STIG FortiGate** et des bonnes pratiques ANSSI pour constituer un référentiel de durcissement complet, priorisé, et directement exploitable par les RSSI, les intégrateurs réseau et les équipes SOC. Il couvre l'intégralité du cycle de vie de la configuration — de la gestion des comptes administrateurs à la politique de journalisation, en passant par le VPN, l'IPS, le filtrage applicatif et la segmentation réseau.

À RETENIR

⚡ À retenir — Durcissement FortiGate 2026

Le CIS Benchmark FortiOS v7.x définit 200+ contrôles répartis en niveaux L1 (essentiels, sans impact sur la disponibilité) et L2 (avancés, recommandés pour les environnements à haute sensibilité). Les trois vecteurs d'attaque les plus fréquemment exploités sur FortiGate sont : les interfaces d'administration exposées sur Internet sans MFA, les SSL-VPN non patchés (CVE-2024-21762, CVE-2023-27997), et les politiques de filtrage permissives avec inspection SSL désactivée. Un durcissement complet réduit de 70 à 85 % la surface d'attaque exploitable documentée dans les bulletins FortiGuard PSIRT.

Référentiels de durcissement FortiGate : CIS, DISA STIG et ANSSI

Trois référentiels font autorité pour le durcissement d'un FortiGate en environnement professionnel. Le **CIS Benchmark for FortiOS** (v7.2, publié par le Center for Internet Security) est le plus utilisé en Europe. Il définit deux profils : le niveau 1 regroupe les contrôles essentiels qui n'impactent pas la disponibilité et peuvent être appliqués immédiatement sur tout environnement de production ; le niveau 2 cible les déploiements à haute sensibilité (secteur financier, administration, opérateurs d'importance vitale) et inclut des contrôles plus restrictifs sur le chiffrement et l'authentification.

Le **DISA STIG FortiGate** (Security Technical Implementation Guide) est le référentiel utilisé par les administrations américaines et de plus en plus adopté par les OIV et OSE européens comme baseline technique. Il priorise les contrôles en catégories CAT I (critique, à corriger immédiatement), CAT II (haute sévérité) et CAT III (moyenne sévérité). Les contrôles CAT I incluent l'interdiction des mots de passe par défaut, la désactivation des services inutilisés (HTTP sur l'interface admin, Telnet, SNMP v1/v2), et la validation des certificats SSL pour le management.

L'**ANSSI** publie quant à elle des recommandations dans son guide "Sécurité des pare-feux" (version 2022) et dans le ReCyF 2026. Pour les organisations soumises à NIS 2, le mapping entre les contrôles FortiGate et les mesures de l'article 21 est disponible dans notre template de mapping ReCyF ANSSI. L'ANSSI recommande en particulier la segmentation stricte des zones d'administration, la journalisation centralisée sur un collecteur externe, et l'application systématique des patches dans un délai de 72h pour les vulnérabilités critiques.

Gestion des comptes administrateurs et authentification forte

La gestion des comptes admin est le premier contrôle CIS L1. Sur un FortiGate fraîchement déployé, le compte `admin` par défaut doit être renommé ou désactivé immédiatement — la simple connaissance de ce nom de compte facilite les attaques par force brute. Le CIS recommande de créer des comptes nominatifs distincts pour chaque administrateur, avec des profils de permissions correspondant au principe du moindre privilège : un administrateur réseau n'a pas besoin d'accéder à la configuration VPN, un opérateur de surveillance n'a besoin que d'un accès lecture aux logs.

L'authentification multifacteur (MFA) doit être activée sur toutes les interfaces d'administration. FortiGate intègre nativement FortiToken (TOTP) et supporte les solutions RADIUS avec challenge-response (FreeRADIUS, Microsoft NPS). La configuration CLI correspondante :

```
config system admin
    edit "admin-nominatif"
        set two-factor fortitoken
        set fortitoken "FTK0000000000"
        set email-to "admin@entreprise.fr"
    next
end
```

Les tentatives d'authentification échouées doivent déclencher un verrouillage progressif. Le CIS L1 recommande 3 tentatives maximum avant verrouillage de 5 minutes, avec alerte automatique. La gestion des mots de passe doit respecter une politique de complexité forte (16 caractères minimum, majuscules/minuscules/chiffres/caractères spéciaux) et une rotation tous les 90 jours maximum. Pour les environnements avec de nombreux administrateurs, l'intégration LDAP/

Active Directory avec des groupes de sécurité dédiés simplifie la gestion — consultez notre checklist de durcissement Active Directory pour sécuriser le backend d'authentification.

L'accès SSH à la CLI doit être restreint à une liste blanche d'adresses IP source, et RSA 4096 bits ou Ed25519 doit remplacer l'authentification par mot de passe. L'accès HTTPS à la WebUI doit utiliser TLS 1.2 minimum (TLS 1.3 recommandé) avec une suite de chiffrement conforme aux recommandations ANSSI A+.

Segmentation réseau, zones et interfaces

La segmentation réseau est le deuxième pilier du durcissement FortiGate. Le DISA STIG impose une séparation stricte des zones : WAN (untrust), LAN (trust), DMZ (semi-trust), Management (out-of-band). L'interface de management ne doit jamais être exposée sur la zone WAN — une exigence que beaucoup d'organisations négligent pour des raisons de commodité, au prix d'une exposition critique.

Les politiques de pare-feu doivent suivre le principe du refus par défaut (*deny all, allow by exception*). Chaque règle doit être documentée, datée, et associée à un propriétaire métier. Le CIS recommande un audit trimestriel des règles pour identifier les règles obsolètes (destination non joignable, service non utilisé depuis 90+ jours). Les zones VLAN doivent être configurées pour éviter le VLAN hopping : désactivation du DTP, ports non utilisés en mode access sur un VLAN noir.

Pour les environnements multi-sites, la micro-segmentation via VXLAN ou des Virtual Domains (VDOM) permet d'isoler les environnements de production, de développement et d'administration sur un même châssis physique. Chaque VDOM dispose de sa propre table de routage, de ses propres administrateurs, et de ses propres politiques — c'est l'architecture recommandée par Fortinet pour les déploiements MSP et les organisations avec plusieurs périmètres distincts.

Politiques UTM : IPS, App Control et Anti-Malware

L'inspection applicative (UTM) est la valeur ajoutée principale d'un NGFW par rapport à un pare-feu stateful classique. Sur FortiGate, le moteur UTM comprend le système de prévention d'intrusion (IPS), le contrôle applicatif (App Control), le filtrage web (Web Filter), l'anti-malware (AV), et le filtrage DNS. Chacun de ces profils doit être configuré explicitement — les profils par défaut sont insuffisants pour un environnement de production sécurisé.

Pour l'**IPS**, le CIS L1 recommande d'activer les signatures "critiques" et "hautes" en mode blocage, et les signatures "moyennes" en mode monitoring pendant 30 jours avant basculement en blocage. Les faux positifs doivent être analysés et les exceptions documentées. Le FortiGuard IPS est mis à jour plusieurs fois par jour — vérifiez que la mise à jour automatique des signatures est activée et que l'intervalle de vérification est inférieur à 1 heure.

L'**App Control** permet de bloquer les applications à risque (Tor, proxies anonymes, outils P2P non approuvés, applications de shadow IT) indépendamment du port utilisé. En 2026, les cas d'usage incluent le blocage des clients IA non approuvés (ChatGPT web sans DLP, Copilot non administré) et des outils de transfert de fichiers non chiffrés. Le moteur d'App Control FortiGuard identifie 5000+ applications par leurs empreintes comportementales, pas seulement par les ports.

Inspection SSL/TLS : Deep Packet Inspection et exceptions

L'inspection SSL (Deep Packet Inspection) est la fonctionnalité la plus impactante sur les performances et la plus délicate à configurer. Sans elle, 70 à 90 % du trafic réseau d'une organisation typique échappe à l'inspection UTM — les malwares et les exfiltrations de données se cachent dans le HTTPS chiffré. Avec elle, des problèmes de compatibilité apparaissent sur les applications utilisant du certificate pinning (banking apps, certains SaaS) ou des configurations TLS non standard.

La configuration recommandée pour 2026 : inspection SSL activée sur tous les profils UTM appliqués au trafic WAN, avec une liste d'exclusions pour les domaines bancaires,

gouvernementaux et les applications avec pinning connu. Le certificat CA utilisé pour l'interception doit être déployé sur tous les postes clients via une GPO Active Directory — sans cela, les utilisateurs verront des avertissements de certificat sur chaque site HTTPS inspecté.

Le DISA STIG impose que les suites de chiffrement TLS 1.0 et 1.1 soient désactivées sur toutes les interfaces FortiGate. La configuration CLI :

```
config system global
    set ssl-min-proto-version TLSv1-2
    set strong-crypto enable
end
```

VPN IPsec et SSL-VPN : durcissement et CVE critiques

Le VPN est la surface d'attaque la plus exploitée sur les FortiGate exposés sur Internet en 2024-2026. La **CVE-2024-21762** (CVSS 9.6) permettait une exécution de code à distance sans authentification sur le SSL-VPN FortiGate — elle a été massivement exploitée par des groupes APT dès sa divulgation. La **CVE-2023-27997** (CVSS 9.8) offrait un heap overflow pré-authentification. Ces deux CVE illustrent pourquoi le patching VPN doit être traité en urgence absolue.

Pour le **SSL-VPN**, les mesures de durcissement prioritaires sont : l'activation du MFA sur tous les comptes VPN, la restriction du SSL-VPN à des VLAN dédiés avec accès limité aux ressources nécessaires (principe du moindre privilège réseau), la désactivation du Split Tunneling si le contexte le permet, et la mise en place d'une politique de timeout de session agressive (8 heures maximum, déconnexion en cas d'inactivité de 30 minutes). Le portail SSL-VPN ne doit pas être exposé sur le port 443 par défaut — un port non standard réduit l'exposition aux scanners automatisés.

Pour le **VPN IPsec**, la cipher suite recommandée par l'ANSSI en 2026 pour les tunnels site-à-site est : IKEv2, AES-256-GCM, SHA-384, DH Group 20 (ECP384). Les configurations RSA 1024 bits, DES/3DES et MD5 doivent être explicitement désactivées. Le Dead Peer Detection (DPD) doit être activé pour détecter les tunnels défaillants et éviter les politiques orphelines. Pour

approfondir le durcissement de la messagerie électronique associée à votre périmètre FortiGate, consultez notre guide FortiMail durcissement antispam.

SD-WAN sécurisé : bonnes pratiques et vecteurs d'attaque

Le SD-WAN FortiGate est de plus en plus déployé pour remplacer les MPLS dans les architectures multi-sites. Sa surface d'attaque spécifique est souvent sous-estimée. Les principales vulnérabilités liées au SD-WAN mal configuré incluent : l'absence de chiffrement sur les liens SD-WAN (le SD-WAN route le trafic mais ne le chiffre pas par défaut — il faut coupler SD-WAN et IPsec overlay), l'exposition involontaire d'interfaces SD-WAN sur Internet, et la confiance implicite accordée aux liens secondaires (4G/LTE de secours) sans inspection UTM.

Le DISA STIG recommande que tout lien SD-WAN passant sur un réseau non maîtrisé (Internet, 4G) soit systématiquement chiffré via IPsec Overlay. La Health Check SD-WAN doit utiliser des probes HTTPS vers des serveurs internes contrôlés plutôt que des probes ICMP vers des serveurs publics, qui peuvent être manipulés pour forcer des changements de routage (attaque de type SD-WAN hijacking).

Journalisation FortiAnalyzer et rétention des logs

La journalisation centralisée est un prérequis de la détection d'incidents et de la conformité NIS 2. Sur FortiGate, les logs doivent être envoyés en temps réel vers un collecteur externe — FortiAnalyzer, Syslog, ou SIEM (Splunk, Elastic, Wazuh). La journalisation locale sur la mémoire flash du FortiGate est insuffisante : capacité limitée, rotation rapide, et perte des logs en cas de compromission du pare-feu.

Le CIS L1 impose la journalisation des événements suivants au minimum : authentifications réussies et échouées (admin et VPN), changements de configuration, sessions refusées par les politiques, alertes IPS et AV, événements système (redémarrage, mise à jour firmware). Le

niveau de log recommandé est "Information" pour les événements système et "Warning" pour les politiques UTM — le niveau "Debug" ne doit jamais être activé en production car il génère des volumes de logs qui saturent le stockage et peuvent faire tomber le service de journalisation.

La rétention des logs est fixée à 12 mois minimum par la directive NIS 2 (article 21, mesure 7). Un FortiAnalyzer dimension 500 Go suffit pour une organisation de 200 utilisateurs avec une politique de log complète. Pour les environnements plus grands, FortiAnalyzer Cloud ou un SIEM dédié est recommandé. Notre guide audit cybersécurité PME 2026 détaille les exigences de logging dans le contexte d'un audit PASSI.

Benchmark de performance FortiGate : UTM activé vs désactivé

Le choix du modèle FortiGate doit intégrer l'impact de l'UTM sur les performances. Les chiffres de débit annoncés par Fortinet dans les datasheets correspondent au mode pare-feu pur (stateful) sans inspection applicative. L'activation de l'ensemble des profils UTM réduit généralement le débit de 60 à 75 % par rapport aux valeurs nominales. Voici les données de performance UTM complètes pour les modèles les plus courants en 2026 :

Modèle	Débit FW pur	Débit UTM complet	Sessions concurrentes	Usage recommandé
FortiGate 40F	5 Gbps	600 Mbps	700 000	TPE, agences ≤25 users
FortiGate 60F	10 Gbps	1 Gbps	1 500 000	PME ≤50 users
FortiGate 100F	20 Gbps	2 Gbps	3 000 000	PME/ETI ≤200 users
FortiGate 200F	27 Gbps	3 Gbps	4 000 000	ETI ≤500 users
FortiGate 400F	65 Gbps	9.5 Gbps	8 000 000	Grande entreprise / datacenter

L'activation du SSL Inspection est le facteur d'impact le plus fort sur les performances : elle seule peut réduire de 30 % supplémentaires le débit UTM. Si votre lien Internet dépasse 80 % de la capacité UTM du modèle installé, envisagez un upgrade ou une décharge TLS dédiée. Le dimensionnement doit inclure une marge de 40 % pour les pics de trafic et les futures activations de fonctionnalités.

Tests de configuration CLI : commandes de vérification

La validation de la configuration est une étape obligatoire après chaque modification et lors des audits périodiques. FortiGate fournit un ensemble de commandes `diagnose` et `get` pour vérifier l'état réel de la configuration :

```
 # Vérifier les comptes admin et leur configuration MFA
get system admin

# Vérifier les services exposés sur les interfaces
get system interface

# Vérifier la version firmware et les patches appliqués
get system status

# Vérifier la configuration SSL-VPN
get vpn ssl settings

# Tester la résolution DNS et la connectivité FortiGuard
diagnose debug rating

# Vérifier les sessions actives et les politiques matchées
diagnose firewall iprope show

# Vérifier les logs en temps réel (mode debug)
diagnose log test
```

Ces commandes constituent la base d'un script d'audit de configuration automatisé. Pour une vérification de conformité CIS complète, des outils tiers comme **Nipper** (anciennement Nipper Studio) ou **FireMon** automatisent l'analyse de la configuration exportée et génèrent un rapport de

conformité mappé sur le CIS Benchmark. Notre guide de durcissement des environnements Windows complète cette approche pour sécuriser les endpoints du périmètre.

CIS Controls mappés aux fonctions FortiGate

Les CIS Controls v8 définissent 18 groupes de contrôles. Voici comment les fonctions FortiGate se mappent sur les contrôles les plus pertinents :

CIS Control 4 (Configuration sécurisée des actifs) → Durcissement admin, désactivation services inutilisés, politiques de passwords, CIS Benchmark FortiOS L1+L2

CIS Control 6 (Gestion des comptes) → Comptes nominatifs, MFA FortiToken, intégration LDAP, RBAC via profils admin

CIS Control 9 (Protection email et navigateurs) → FortiMail (antispam), App Control (bloque navigateurs non approuvés), Anti-Phishing FortiGuard

CIS Control 10 (Défenses contre les malwares) → AV FortiGuard en mode blocage, FortiSandbox pour l'analyse comportementale des fichiers suspects

CIS Control 12 (Gestion de l'infrastructure réseau) → Segmentation VLAN, VDOM, politiques de routage, SD-WAN sécurisé

CIS Control 13 (Surveillance et défense du réseau) → IPS en mode blocage, App Control, journalisation FortiAnalyzer, intégration SIEM

CIS Control 16 (Sécurité des applications) → SSL Inspection, WAF FortiWeb (si déployé en complément), filtrage URL FortiGuard

Pour les organisations NIS 2, ce mapping CIS Controls / FortiGate s'intègre dans la démarche de conformité documentée dans le ReCyF ANSSI. Un audit de configuration FortiGate réalisé par un prestataire PASSI qualifié peut valider ce mapping et constituer une preuve de diligence raisonnable lors d'un contrôle ANSSI. Notre guide d'audit cybersécurité PME détaille les étapes pour préparer et réussir un audit PASSI.

FAQ — Durcissement FortiGate

Quelle est la différence entre le CIS Benchmark FortiOS L1 et L2 ?

Le niveau L1 du CIS Benchmark FortiOS regroupe les contrôles de durcissement essentiels qui peuvent être appliqués sans perturber les services en production. Il couvre la gestion des comptes, la désactivation des services inutilisés, la configuration des mots de passe, et la journalisation basique. Le niveau L2 ajoute des contrôles plus restrictifs — chiffrement renforcé, contrôle applicatif étendu, inspection SSL complète, restriction des suites cryptographiques — qui peuvent nécessiter des ajustements sur certaines applications legacy. L'approche recommandée est d'implémenter L1 immédiatement sur tout l'environnement, puis de déployer L2 progressivement en commençant par les segments les plus sensibles (DMZ, accès administration).

Dois-je activer l'inspection SSL sur tout le trafic HTTPS sortant ?

L'activation de l'inspection SSL sur 100 % du trafic HTTPS est l'objectif cible, mais elle doit être déployée graduellement pour éviter les interruptions de service. Commencez par activer l'inspection en mode monitoring (sans blocage) pendant 2 à 4 semaines pour identifier les applications incompatibles (certificate pinning, TLS mutuels). Construisez une liste d'exclusions documentée pour ces applications, puis basculez en mode blocage. Les exclusions systématiques recommandées incluent les domaines bancaires (.fr des établissements financiers), les services gouvernementaux (impots.gouv.fr, ameli.fr) et les solutions de mise à jour système (Windows Update, WSUS). Sans inspection SSL, votre IPS, votre antimalware et votre contrôle applicatif sont aveugles sur la majorité du trafic web moderne.

Comment protéger le FortiGate contre les CVE critiques de type CVE-2024-21762 ?

Trois couches de protection complémentaires sont nécessaires. En premier lieu, le patching : la CVE-2024-21762 a été corrigée dans FortiOS 7.4.3, 7.2.6 et 7.0.13 — tout FortiGate en version antérieure reste vulnérable. Établissez un processus de veille sur les bulletins FortiGuard PSIRT et planifiez les maintenances dans un délai de 72h pour les CVE CVSS ≥9.0. En deuxième lieu,

la réduction de la surface d'exposition : si le SSL-VPN n'est pas utilisé, désactivez-le complètement (`set sslvpn-max-proto-ver` + désactivation du portail). En troisième lieu, la détection : FortiGuard IPS intègre des signatures pour détecter les tentatives d'exploitation des CVE FortiGate connues — vérifiez que les signatures sont à jour et en mode blocage. Les solutions de threat intelligence comme Shodan Monitor permettent également de détecter si votre FortiGate apparaît dans des scans d'exploitation actifs.

