# BENCHMARK DE DURCISSEMENT FORTIGATE FORTIOS 7.4.x 2026

## 🛡️ AYI NEDJIMI CONSULTANTS (ANC)

**Version :** 1.5 — Mai 2026 **Applicabilité :** Fortinet FortiGate toutes séries (FG-x00, FG-x00F, FG-1xxx, FG-2xxx, FG-3xxx, VM-Series) — FortiOS 7.4.0 et supérieur **Classification :** CONFIDENTIEL **Auteur :** AYI NEDJIMI Consultants — https://ayinedjimi-consultants.fr

---

## Conventions et niveaux de criticité

| NIVEAU | SIGNIFICATION |
|---|---|
| 🔴 **CRITIQUE** | Exploitable sans authentification, patch ou remédiation immédiat |
| 🟠 **ÉLEVÉ** | Risque élevé d'exploitation, action sous 72h |
| 🟡 **MOYEN** | Réduction significative de la surface d'attaque |
| 🟢 **L1** | Baseline CIS Level 1 — recommandé pour tous les environnements |
| 🔵 **L2** | CIS Level 2 — défense en profondeur, environnements sensibles |
| ⚪ **INFO** | Bonne pratique / observabilité / configuration opérationnelle |

**Format de chaque contrôle :** > **CIS Ref** | **MITRE** | **Niveau** > - Description du risque > - Impact potentiel > - Navigation interface GUI > - CLI de vérification > - Remédiation > - Valeur par défaut > - Critère de conformité

---

## Table des matières

## Top 10 Quick Wins — 80 % du risque en priorité

*Ces 10 actions couvrent la majorité des vecteurs d'attaque documentés sur FortiGate. Commencer ici avant toute autre configuration.*

| # | ACTION | DOMAINE | IMPACT | EFFORT |
|---|---|---|---|---|
| 1 | Mettre à jour FortiOS vers la dernière version stable GA | D1 | 🔴 CRITIQUE | Faible |
| 2 | Désactiver l'accès management (HTTPS/ SSH/HTTP/SNMP) depuis l'interface WAN | D3 | 🔴 CRITIQUE | Faible |
| 3 | Supprimer le compte admin par défaut et créer un compte nommé | D2 | 🔴 CRITIQUE | Faible |
| 4 | Activer la politique de mots de passe (min. 14 caractères) et le verrouillage | D2 | 🟠 ÉLEVÉ | Faible |
| 5 | Configurer les Trusted Hosts pour chaque compte administrateur | D2 | 🟠 ÉLEVÉ | Faible |
| 6 | Activer les profils IPS et Antivirus sur toutes les politiques de trafic | D5 | 🟠 ÉLEVÉ | Moyen |
| 7 | Activer la journalisation vers un SIEM externe (syslog chiffré ou FortiAnalyzer) | D10 | 🟠 ÉLEVÉ | Moyen |
| 8 | Désactiver les clés TLS statiques ( `ssl-` | D1 | 🟡 MOYEN | Faible |

| # | ACTION | DOMAINE | IMPACT | EFFORT |
|---|---|---|---|---|
| | `static-key-ciphers disable`) | | | |
| 9 | Activer le Security Fabric et connecter FortiAnalyzer | D6 | 🟡 MOYEN | Moyen |
| 10 | Configurer TLS 1.2 minimum pour SSL-VPN et désactiver SSLv3/TLS 1.0 | D7 | 🟡 MOYEN | Faible |

# Domaine 1 — Gestion du firmware et mises à jour

***Objectif :*** *Maintenir FortiOS à jour pour éliminer les vulnérabilités connues exploitées activement. Les équipements FortiGate sont parmi les équipements réseau les plus ciblés par les attaquants étatiques et cybercriminels (CISA KEV 2023-2026 : CVE-2023-27997, CVE-2022-40684, CVE-2024-21762, CVE-2026-24858, CVE-2025-59718/59719).*

---

## Contrôle 1.1 — Firmware FortiOS à jour

***CIS Ref :*** *2.1.6* | ***MITRE :*** *T1190, T1601* | ***Niveau :*** 🔴 *CRITIQUE*

**Description du risque**

Les versions obsolètes de FortiOS exposent l'organisation à des vulnérabilités critiques activement exploitées dans la nature. Fortinet publie régulièrement des mises à jour correctives incluant des patches de sécurité. En 2025-2026, plusieurs CVE critiques ont été exploitées massivement et ajoutées au catalogue CISA KEV (Known Exploited Vulnerabilities) :

| CVE | CVSS | DESCRIPTION | STATUT |
|---|---|---|---|
| **CVE-2026-24858** | 9.8 | Contournement d'authentification via SAML SSO — exploitation active, CISA KEV Déc 2025 | 🔴 Actif |
| **CVE-2025-59718** | 9.8 | FortiCloud SSO bypass via messages SAML forgés — intrusions actives depuis Déc 12, 2025 | 🔴 Actif |
| **CVE-2025-59719** | 9.8 | Variante FortiCloud SSO bypass (campagne couplée CVE-2025-59718) | 🔴 Actif |
| **CVE-2024-21762** | 9.6 | SSL-VPN out-of-bounds write permettant RCE pré-authentification — CISA KEV | 🔴 Actif |
| **CVE-2023-27997** | 9.8 | Heap overflow SSL-VPN pré-authentification (RCE sans credentials) | 🟠 Patchée |
| **CVE-2022-40684** | 9.8 | Contournement d'authentification via API REST — exploitée massivement | 🟠 Patchée |

***Note CISA (Avril 2025) :*** *Même après l'application des patches, des attaquants peuvent avoir déposé des backdoors persistantes (symlinks, comptes cachés). Se référer à la section Réponse à Incident pour la vérification post-compromission.*

**Pattern d'attaque documenté :** Le SSL-VPN et l'interface de gestion exposée sont les deux vecteurs d'entrée initiaux documentés dans la quasi-totalité des incidents FortiGate recensés par le PSIRT Fortinet et les agences gouvernementales (CISA, ANSSI, CERT-EU).

**Impact potentiel**

- Compromission complète du pare-feu sans authentification (CVE-2026-24858, CVE-2024-21762)
- Accès non autorisé au réseau interne via mouvement latéral
- Exfiltration massive de données sensibles et de configurations
- Déploiement de backdoors persistantes par des groupes APT (symlinks SSL-VPN, comptes admin cachés)
- Prise de contrôle de l'ensemble de la politique de sécurité réseau

**Navigation**

```
Dashboard > Status > System Information > Firmware Version
→ System > Fabric Management > FortiGate
→ Clic droit sur le FortiGate > Upgrade
→ Sélectionner la dernière version GA stable
→ Confirmer l'upgrade (prévoir une fenêtre de maintenance)
```

**CLI de vérification**

```
get system status
```

Vérifier le champ `Version` dans la sortie. Comparer avec la version GA la plus récente sur https://docs.fortinet.com/upgrade-tool

```
FGT1 # get system status
...
Version: FortiGate-200F v7.4.8,build2900,260101 (GA)
...
```

**Remédiation**

1. Vérifier le chemin d'upgrade recommandé sur https://docs.fortinet.com/upgrade-tool
2. Exporter la configuration avant toute mise à jour : `execute backup config ftp <ip> <fichier>`
3. Télécharger le firmware depuis https://support.fortinet.com > Firmware Download
4. Planifier la mise à jour en fenêtre de maintenance (redémarrage requis)
5. En GUI : System > Fabric Management > clic droit sur le FortiGate > Upgrade
6. Vérifier le fonctionnement post-upgrade et comparer les configurations
7. Consulter https://www.fortiguard.com/psirt?product=FortiOS pour les CVE actives
8. Après patch : vérifier les indicateurs post-exploitation (voir section Réponse à Incident)

> ***FortiOS 7.4.8+ :*** *Le hachage des mots de passe administrateurs utilise désormais PBKDF2 (remplace SHA256 simple). Recommandé pour les environnements sensibles.*

**Valeur par défaut :** Le firmware livré correspond à la version installée en usine. Il n'existe pas de mise à jour automatique du firmware OS.

**Critère de conformité :** FortiOS ≥ dernière version GA stable publiée. Délai maximum de déploiement des patches critiques (CVSS ≥ 9.0) : 72 heures. Patches élevés : 30 jours. Vérifier l'absence de CVE actives référencées dans CISA KEV (https://www.cisa.gov/known-exploited-vulnerabilities-catalog).

---

## Contrôle 1.2 — Désactiver les clés TLS statiques et renforcer la cryptographie

***CIS Ref :*** *2.1.8* | ***MITRE :*** *T1557, T1600* | ***Niveau :*** 🔵 *L2*

### Description du risque

Par défaut, `ssl-static-key-ciphers` est activé sur FortiOS. Les chiffrements à clé statique (RSA key exchange) ne garantissent pas la confidentialité persistante (Perfect Forward Secrecy). Si la clé privée du serveur est compromise, l'ensemble des sessions TLS passées peuvent être déchiffrées. Cette configuration permet à un attaquant ayant enregistré du trafic chiffré de le déchiffrer a posteriori.

De plus, le paramètre `dh-params` contrôle la taille des paramètres Diffie-Hellman utilisés lors des échanges de clés. Une taille insuffisante (< 2048 bits) expose aux attaques Logjam. La recommandation Fortinet pour les environnements sensibles est 8192 bits.

### Impact potentiel

- Déchiffrement rétroactif de toutes les sessions TLS d'administration
- Exposition des credentials administrateurs et des configurations
- Attaques de type man-in-the-middle facilitées (T1557)
- Affaiblissement actif du chiffrement via downgrade (T1600)
- Non-conformité avec les exigences ANSSI/PCI-DSS sur la confidentialité persistante

### Navigation

```
System > Settings
→ Section "Administration Settings"
→ Vérifier que "SSL Static Key Ciphers" n'est pas activé
(Option non disponible en GUI standard — configuration CLI uniquement)
```

### CLI de vérification

```
config system global
    get
```

Vérifier que `ssl-static-key-ciphers` est positionné à `disable`, `strong-crypto` à `enable` et `dh-params` à une valeur ≥ 2048.

### Remédiation

```
# Désactiver les clés TLS statiques (activer PFS)
config system global
    set ssl-static-key-ciphers disable
end

# Renforcement cryptographique complet (recommandé Fortinet 7.4)
config system global
    set strong-crypto enable
    set ssl-static-key-ciphers disable
    set dh-params 8192
end
```

> ***Note :*** `strong-crypto enable` *est activé par défaut sur FortiOS 7.4, mais sa présence doit être vérifiée sur les équipements migrés depuis une version antérieure.* `dh-params 8192` *peut avoir un léger impact sur les performances pour les modèles d'entrée de gamme.*

**Valeur par défaut :** `ssl-static-key-ciphers` est **activé** par défaut sur FortiOS 7.4.x. `strong-crypto` est activé par défaut. `dh-params` : 2048 par défaut.

**Critère de conformité :** `ssl-static-key-ciphers : disable`, `strong-crypto : enable`, `dh-params` ≥ 2048 (8192 recommandé pour environnements sensibles) dans la sortie de `get system global`.

---

## Contrôle 1.3 — Activer les mises à jour automatiques FortiGuard

> ***CIS Ref :*** *2.1.6 (étendu)* | ***MITRE :*** *T1190, T1203* | ***Niveau :*** 🟢 *L1*

### Description du risque

Les signatures FortiGuard (IPS, Antivirus, Web Filter, Application Control) doivent être maintenues à jour pour détecter et bloquer les menaces les plus récentes. Un équipement avec des signatures obsolètes laisse passer des exploits et malwares connus. FortiGuard publie des mises à jour plusieurs fois par jour pour les nouvelles menaces. FortiOS 7.4 introduit également les **alertes FortiGuard database** pour notifier les administrateurs lorsque les signatures sont anormalement dépassées.

### Impact potentiel

- Propagation de malwares récents non détectés par des signatures obsolètes
- Exploits zero-day connus non bloqués par l'IPS
- Compromission de postes internes via trafic web non filtré
- Non-conformité avec les SLA de protection des contrats FortiCare
- Absence de détection si les bases FortiGuard sont plus anciennes que 24h (alerte recommandée)

### Navigation

```
System > FortiGuard
→ Section "AntiVirus & IPS Updates"
→ "Scheduled Updates" : activer
→ "Update Frequency" : sélectionner "Every 1 hour" (recommandé)
→ "Accept Push Updates from FortiGuard" : activer
→ Apply
```

**CLI de vérification**

```
show system autoupdate schedule
show system autoupdate tunneling
get system autoupdate status
diagnose autoupdate status
```

**Remédiation**

```
config system autoupdate schedule
    set status enable
    set frequency every
    set time 00:00
end

config system autoupdate push-update
    set status enable
end
```

Vérifier la connectivité FortiGuard et forcer une mise à jour immédiate :

```
execute update-now
diagnose autoupdate status
```

Pour activer les alertes FortiGuard sur signatures obsolètes (FortiOS 7.4) :

```
config system fortiguard
    set update-server-location automatic
    set auto-firmware-upgrade disable
end
```

**Valeur par défaut :** Les mises à jour automatiques sont activées par défaut mais la fréquence peut être trop basse selon les configurations d'usine.

**Critère de conformité :** Mises à jour FortiGuard activées avec une fréquence ≤ 1 heure. Date des dernières signatures IPS/AV : moins de 24 heures. `Push updates` activé.

---

## Contrôle 1.4 — Désactiver l'auto-installation USB et sécurité physique

***CIS Ref :*** *2.1.7* | ***MITRE :*** *T1091, T1195* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Par défaut, FortiOS permet l'installation automatique de firmware et de configurations depuis une clé USB connectée au port USB physique de l'équipement. Cette fonctionnalité, conçue pour faciliter le déploiement initial, représente un vecteur d'attaque physique critique en production. Un attaquant ayant accès physique à l'équipement peut charger un firmware malveillant ou une configuration de porte dérobée sans authentification.

La sécurité physique est un prérequis fondamental documenté par Fortinet dans son guide de durcissement officiel : le FortiGate doit être installé dans une salle serveurs verrouillée avec contrôle d'accès physique (badge, biométrie). Les ports réseau inutilisés doivent être protégés par du contrôle d'accès 802.1x.

**Impact potentiel**

- Installation d'un firmware trojanisé par accès physique non autorisé
- Écrasement de la configuration de sécurité par une version backdoorée
- Compromission totale sans laisser de traces dans les logs d'authentification
- Vecteur d'attaque utilisé dans des scénarios d'espionnage industriel (T1195)

**Navigation**

```
(Non disponible en GUI — configuration CLI uniquement)
```

**CLI de vérification**

```
config system auto-install
    get
```

Vérifier que `auto-install-config` et `auto-install-image` sont tous deux à `disable`.

**Remédiation**

```
# Désactiver l'auto-installation depuis USB
config system auto-install
    set auto-install-config disable
    set auto-install-image disable
end
```

**Mesures complémentaires de sécurité physique (hors CLI) :**

- Installer le FortiGate dans une baie verrouillée en salle serveurs avec accès contrôlé
- Activer le contrôle d'accès 802.1x sur les ports réseau physiques non utilisés
- Désactiver ou obstruer physiquement les ports USB inutilisés si possible
- Documenter et tracer tous les accès physiques à l'équipement

**FortiGate avec TPM (Trusted Platform Module) :**

Sur les modèles FortiGate équipés d'un TPM, il est recommandé de stocker le mot de passe de chiffrement maître (master encryption key) sur le TPM pour une protection renforcée des données de configuration chiffrées :

```
config system global
    set private-data-encryption enable
end
```

> *Sur les modèles avec TPM, cette commande lie le chiffrement au matériel — la configuration ne peut pas être déchiffrée sur un autre équipement FortiGate.*

**Valeur par défaut :** `auto-install` est **activé** par défaut (auto-install-config : enable, auto-install-image : enable). `private-data-encryption` : disable par défaut.

**Critère de conformité :** `auto-install-config : disable` ET `auto-install-image : disable` dans la sortie de `config system auto-install / get`. Accès physique à l'équipement documenté et restreint.

---

# Domaine 2 — Authentification et accès administrateur

> ***Objectif :*** *Protéger l'accès administrateur au FortiGate contre les attaques par credential stuffing, brute force et l'utilisation de comptes par défaut. L'accès administrateur non sécurisé est le vecteur initial d'attaque le plus fréquent sur les équipements FortiGate selon le PSIRT Fortinet.*

---

## Contrôle 2.1 — Supprimer le compte admin par défaut

> ***CIS Ref :*** *2.4.1* | ***MITRE :*** *T1078* | ***Niveau :*** 🔴 *CRITIQUE*

**Description du risque**

Le compte `admin` avec mot de passe vide (ou trivial) est présent sur tout FortiGate livré en usine. Ce compte est universellement connu des attaquants et est systématiquement testé lors de scans automatisés. Des campagnes d'exploitation massive ciblent les FortiGate exposés en utilisant ces credentials par défaut. La CVE-2022-40684 (contournement d'authentification) permettait de modifier le mot de passe de l'admin via l'API REST sans s'authentifier.

**Impact potentiel**

- Accès administrateur complet sans effort de la part de l'attaquant
- Modification immédiate de toutes les politiques de sécurité
- Exfiltration de la configuration complète incluant clés VPN et certificats
- Pivot vers l'infrastructure interne via création de règles permissives

**Navigation**

```
System > Administrators
→ Créer un nouvel administrateur avec nom spécifique (ex: adm-prenom)
→ Attribuer le profil "super_admin"
→ Configurer le mot de passe (≥ 14 caractères, complexe)
→ Configurer les Trusted Hosts
→ Sauvegarder
→ Se connecter avec le nouveau compte et vérifier l'accès
→ Revenir dans System > Administrators
→ Sélectionner le compte "admin" > Delete
```

**CLI de vérification**

```
show system admin
```

Vérifier l'absence du compte `admin` dans la liste. Aucune entrée avec `set name "admin"` ne doit apparaître.

**Remédiation**

```
config system admin
    edit "adm-votreprenom"
        set password <mot_de_passe_fort>
        set accprofile "super_admin"
        set trusthost1 <IP_réseau_management>/32
        set vdom "root"
    next
end
```

Puis, après connexion avec le nouveau compte :

```
config system admin
    delete "admin"
end
```

**Valeur par défaut :** Compte `admin` avec mot de passe vide présent à la livraison de l'équipement.

**Critère de conformité :** Aucun compte nommé `admin` dans `show system admin`. Tous les comptes administrateurs ont un nom nominatif ou fonctionnel distinct.

---

## Contrôle 2.2 — Politique de mots de passe administrateur avec hachage fort

***CIS Ref :*** *2.2.1* | ***MITRE :*** *T1110* | ***Niveau :*** 🟢 *L1*

**Description du risque**

Sans politique de mots de passe active, les administrateurs peuvent définir des mots de passe triviaux (vides, courts, non complexes) qui sont vulnérables aux attaques par dictionnaire et brute force. FortiOS 7.4 permet d'imposer une longueur minimale, la présence de caractères complexes et d'appliquer la politique aux mots de passe administrateurs et aux clés pré-partagées IPsec.

**Hachage des mots de passe :** Depuis FortiOS 7.4, les mots de passe administrateurs sont hachés avec SHA256. À partir de FortiOS **7.4.8**, le hachage utilise **PBKDF2** (Password-Based Key Derivation Function 2) qui est résistant aux attaques par dictionnaire accélérées par GPU. Il est fortement recommandé de migrer vers cette version pour les environnements sensibles.

**Impact potentiel**

- Compromission de comptes administrateurs par brute force ou dictionnaire
- Accès non autorisé avec modification des politiques de sécurité
- Pivot réseau complet depuis le FortiGate compromis
- Si hachage faible : crackage hors-ligne des hashs exfiltrés lors d'une compromission

**Navigation**

```
System > Settings
→ Section "Password Policy"
→ "Password scope" : Both (admin passwords + IPsec PSK)
→ "Minimum length" : 14
→ Cocher "Must contain upper-case letter"
→ Cocher "Must contain lower-case letter"
→ Cocher "Must contain number"
→ Cocher "Must contain non-alphanumeric"
→ Apply
```

**CLI de vérification**

```
get system password-policy
```

Vérifier : `status : enable`, `minimum-length : 14`, `apply-to : admin-password ipsec-preshared-key`.

**Remédiation**

```
config system password-policy
    set status enable
    set apply-to admin-password ipsec-preshared-key
    set minimum-length 14
    set must-contain upper-case-letter lower-case-letter number non-alphanumeric
    set change-4-characters enable
end
```

Configurer également le verrouillage sur tentatives échouées et le chiffrement des données privées :

```
config system global
    set admin-lockout-threshold 3
    set admin-lockout-duration 900
    set private-data-encryption enable
end
```

> ***Chiffrement des données privées :*** *`private-data-encryption enable` chiffre les mots de passe et données sensibles stockés dans la configuration (clés PSK, mots de passe SNMP, etc.) avec un algorithme AES. Sur FortiGate avec TPM, la clé de chiffrement est liée au matériel.*

**Valeur par défaut :** Politique de mots de passe **désactivée** par défaut (`set status disable`). Seuil de verrouillage : 3 tentatives, durée de verrouillage : 60 secondes. `private-data-encryption` : disable.

**Critère de conformité :** `status : enable`, `minimum-length : 14`, `must-contain` avec les 4 classes de caractères. Lockout threshold ≤ 3, lockout duration ≥ 900 secondes. `private-data-encryption : enable`. FortiOS ≥ 7.4.8 pour PBKDF2 dans les environnements sensibles.

---

## Contrôle 2.3 — Trusted Hosts pour tous les administrateurs

***CIS Ref :*** *2.4.2* | ***MITRE :*** *T1078, T1133* | ***Niveau :*** 🟠 *ÉLEVÉ*

### Description du risque

Sans restriction par adresse IP source (Trusted Hosts), un attaquant ayant obtenu des credentials administrateurs peut se connecter depuis n'importe quelle adresse IP du monde. La restriction par Trusted Hosts est un contrôle compensatoire critique qui limite considérablement la fenêtre d'exploitation même en cas de compromission de credentials.

### Impact potentiel

- Connexion administrative depuis des IP non autorisées (VPN pirate, Tor, pays tiers)
- Exploitation de credentials volés depuis n'importe quel point d'Internet
- Attaques de type credential stuffing difficilement détectables sans restriction IP

### Navigation

```
System > Administrators
→ Éditer chaque compte administrateur
→ Section "Trusted Hosts"
→ Trusted Host 1 : <IP_station_admin>/32 ou <sous-réseau_management>/24
→ Trusted Host 2 : <IP_secondaire_si_applicable>/32
→ OK
```

### CLI de vérification

```
show system admin
```

Vérifier que chaque entrée `edit` contient `set trusthost1` avec une IP/masque restrictif. L'absence de `trusthost` signifie que l'accès est autorisé depuis n'importe quelle IP (0.0.0.0/0.0.0.0).

### Remédiation

```
config system admin
    edit "adm-votreprenom"
        set trusthost1 192.168.10.10 255.255.255.255
        set trusthost2 10.0.100.0 255.255.255.0
        set trusthost3 0.0.0.0 0.0.0.0
    next
end
```

*Note : `trusthost3 0.0.0.0 0.0.0.0` n'est utilisé que si un troisième hôte de confiance spécifique est nécessaire. Ne pas laisser `0.0.0.0 0.0.0.0` comme seule valeur de Trusted Host.*

**Valeur par défaut :** Aucune restriction par adresse IP source — accès depuis toute adresse IP.

**Critère de conformité :** Chaque compte administrateur possède au moins un `trusthost` configuré avec une adresse IP ou sous-réseau restrictif (pas `0.0.0.0/0`).

---

## Contrôle 2.4 — Idle timeout administrateur ≤ 10 minutes

***CIS Ref :*** *2.4.4* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

### Description du risque

Une session administrative laissée ouverte sans activité représente une fenêtre d'attaque critique. Un poste de travail non verrouillé avec une session FortiGate active permet à toute personne physiquement présente de modifier la configuration. Ce risque est particulièrement important dans les datacenters et salles techniques avec accès mutualisé.

### Impact potentiel

- Accès non autorisé à une session administrative active
- Modification de la politique de sécurité par un tiers non autorisé
- Insertion de backdoors difficiles à détecter a posteriori

### Navigation

```
System > Settings
→ Section "Administration Settings"
→ "Idle Timeout" : 10 (minutes)
→ Apply
```

### CLI de vérification

```
get system global | grep admintimeout
```

La valeur doit être ≤ 10.

### Remédiation

```
config system global
    set admintimeout 10
end
```

**Valeur par défaut :** 5 minutes selon la documentation FortiOS 7.4. Certaines configurations d'usine peuvent avoir une valeur plus élevée.

**Critère de conformité :** `admintimeout` ≤ 10 minutes dans `get system global`.

---

## Contrôle 2.5 — Canaux d'accès administrateur chiffrés uniquement

***CIS Ref :*** *2.4.5* | ***MITRE :*** *T1557, T1040* | ***Niveau :*** 🟢 *L1*

### Description du risque

L'accès administrateur via HTTP (port 80) ou Telnet transmet les credentials et l'intégralité de la session en clair sur le réseau. Ces protocoles sont vulnérables aux attaques d'écoute passive (packet sniffing) et aux attaques de type man-in-the-middle. Seuls HTTPS et SSH doivent être autorisés pour l'administration. Pour les transferts de fichiers (sauvegardes, firmware), utiliser **SCP** (Secure Copy Protocol) à la place de FTP ou TFTP qui transmettent les données en clair.

### Impact potentiel

- Interception des credentials administrateurs en clair sur le réseau
- Capture complète de la session administrative par un attaquant sur le même réseau
- Attaques MITM permettant la modification de commandes en transit
- Interception des sauvegardes de configuration via FTP/TFTP non chiffré

### Navigation

```
System > Settings
→ Section "Administration Settings"
→ "HTTPS" : activer (port 443 ou port personnalisé ≥ 1024)
→ "HTTP Redirect" : activer (redirige HTTP vers HTTPS)
→ "HTTP" : désactiver ou rediriger uniquement
→ "Telnet" : désactiver
→ "SSH" : activer (port 22 ou port personnalisé)
→ Apply
```

### CLI de vérification

```
get system global | grep admin-
```

Vérifier : `admin-https : enable`, `admin-telnet : disable`, `admin-http : disable` (ou redirect uniquement).

### Remédiation

```
config system global
    set admin-https enable
    set admin-https-redirect enable
    set admin-telnet disable
    set admin-ssh enable
    set admin-http disable
    set admin-https-ssl-versions tlsv1-2 tlsv1-3
    set admin-ssh-port 22
end
```

Utiliser SCP pour les sauvegardes de configuration :

```
# Sauvegarde via SCP (à la place de FTP/TFTP)
execute backup config scp <ip_serveur_scp> <chemin_fichier> <utilisateur>

# Vérification que SCP est utilisable
diagnose debug application sshd -1
```

**Valeur par défaut :** HTTPS activé, HTTP activé (redirection par défaut en 7.4), Telnet désactivé, SSH activé.

**Critère de conformité :** `admin-telnet : disable`, `admin-http : disable` (ou redirect-only), `admin-https : enable`. Aucun protocole en clair actif sur les interfaces de management. SCP utilisé pour tous les transferts de fichiers administratifs.

---

## Contrôle 2.6 — SNMPv3 uniquement — désactiver v1/v2c

***CIS Ref :*** *2.3.1* | ***MITRE :*** *T1040, T1562* | ***Niveau :*** 🟢 *L1*

### Description du risque

SNMPv1 et SNMPv2c transmettent les données de monitoring, y compris les community strings, en clair. Ces versions sont vulnérables aux attaques par écoute passive permettant de récupérer les community strings, utilisables ensuite pour lire ou écrire la configuration de l'équipement. CVE classiques : SNMP Read Community String Information Disclosure. SNMPv3 ajoute l'authentification et le chiffrement des échanges.

### Impact potentiel

- Récupération des community strings en clair et accès en lecture à toute la MIB
- Extraction d'informations sur la topologie réseau, les interfaces et les routes
- Modification de la configuration via SNMP Write si la community est devinée

### Navigation

```
System > SNMP
→ Section "SNMP Agent" : activer
→ Supprimer toutes les communautés SNMPv1/v2c existantes
→ Section "SNMPv3" : créer un utilisateur
→ Security Level : Authentication and Privacy
→ Authentication Protocol : SHA256
→ Privacy Protocol : AES256
→ Configurer les Hosts autorisés
→ Apply
```

### CLI de vérification

```
config system snmp community
    show
```

La liste doit être vide (aucune communauté v1/v2c).

```
config system snmp user
    show
```

Au moins un utilisateur SNMPv3 doit être configuré avec `security-level auth-priv`.

**Remédiation**

Supprimer les communautés v1/v2c existantes (ici l'ID 1 correspond à "public") :

```
config system snmp community
    delete 1
end
```

Créer un utilisateur SNMPv3 avec chiffrement :

```
config system snmp sysinfo
    set status enable
end

config system snmp user
    edit "snmpv3_monitoring"
        set security-level auth-priv
        set auth-proto sha256
        set auth-pwd <mot_de_passe_auth_fort>
        set priv-proto aes256
        set priv-pwd <mot_de_passe_priv_fort>
        set notify-hosts <IP_serveur_SNMP>
    next
end
```

**Valeur par défaut :** Aucune communauté SNMP ni utilisateur SNMPv3 configurés par défaut. SNMP Agent désactivé.

**Critère de conformité :** `config system snmp community / show` retourne vide. Au moins un utilisateur SNMPv3 avec `security-level auth-priv`, `auth-proto sha256`, `priv-proto aes256`.

---

## Contrôle 2.7 — Bannières de connexion pré/post-login

***CIS Ref :*** *2.1.1, 2.1.2* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

**Description du risque**

L'absence de bannière légale avant la connexion peut affaiblir les poursuites judiciaires contre des accès non autorisés. Une bannière correctement rédigée constitue un avertissement légal explicite, génère un consentement à la surveillance et diminue la capacité d'un défendant à invoquer l'ignorance. Elle informe également les utilisateurs légitimes de leurs obligations.

**Impact potentiel**

- Fragilisation des procédures judiciaires en cas de compromission

- Absence de notification légale sur la surveillance du système
- Non-conformité avec certains référentiels réglementaires (ISO 27001, PCI-DSS)

**Navigation**

```
System > Replacement Messages
→ Extended View (coin supérieur droit)
→ "Pre-login Disclaimer Message" : éditer
→ Saisir le texte de la bannière légale
→ Save

System > Replacement Messages
→ "Post-login Disclaimer Message" : éditer
→ Saisir le texte MOTD
→ Save
```

Activer les bannières :

```
System > Settings
→ "Pre-login Banner" : enable
→ "Post-login Banner" : enable
→ Apply
```

**CLI de vérification**

```
get system global | grep login-banner
```

Vérifier : `pre-login-banner : enable`, `post-login-banner : enable`.

**Remédiation**

```
config system global
    set pre-login-banner enable
    set post-login-banner enable
end
```

Exemple de bannière légale :

```
config system replacemsg admin "pre_admin-disclaimer"
    set header "none"
    set buffer "AVERTISSEMENT : Ce système est un équipement informatique privé.
    Tout accès non autorisé est strictement interdit et susceptible de poursuites.
    L'utilisation de ce système implique le consentement à la surveillance."
end
```

**Valeur par défaut :** `pre-login-banner : disable`, `post-login-banner : disable`. Texte par défaut présent mais non affiché.

**Critère de conformité :** `pre-login-banner : enable` ET `post-login-banner : enable`. Texte de bannière approuvé par le service juridique de l'organisation.

---

## Contrôle 2.8 — Authentification multi-facteurs (MFA) pour les admins

***CIS Ref :*** *2.4.1 (étendu)* | ***MITRE :*** *T1078, T1110* | ***Niveau :*** 🟠 *ÉLEVÉ*

### Description du risque

Un mot de passe seul, même complexe, peut être compromis par phishing, keylogger, ou violation de données. L'authentification multi-facteurs (MFA) via FortiToken (hardware ou mobile) ou via FortiAuthenticator (RADIUS, LDAP, SAML) élimine la majorité des attaques par credential stuffing. **MITRE T1078 (Valid Accounts) — le MFA est la mitigation primaire recommandée.** Fortinet recommande : - **FortiToken Mobile** (application TOTP) : solution la plus simple pour les petits déploiements - **FortiToken Hardware** : token physique TOTP pour les environnements haute sécurité (FIPS, environnements sans smartphone) - **FortiAuthenticator** : solution entreprise centralisant le MFA via RADIUS, LDAP et SAML pour des centaines d'administrateurs et utilisateurs VPN

### Impact potentiel

- Compromission totale d'un compte admin par credential stuffing ou phishing (T1078)
- Accès non autorisé malgré un mot de passe fort si celui-ci est divulgué
- Prise de contrôle du FortiGate suite à une violation de base de données d'identités
- Sans MFA : les CVE de type authentication bypass (CVE-2022-40684) ont pu être combinées avec des credentials volés

### Navigation

```
System > Administrators
→ Éditer le compte administrateur cible
→ Section "Two-factor Authentication"
→ "Two-factor Authentication" : activer
→ Sélectionner : FortiToken Mobile, FortiToken Hardware, ou RADIUS (FortiAuthenticator)
→ Si FortiToken Mobile : saisir l'adresse email pour l'activation du token
→ OK

System > FortiTokens (pour vérifier les tokens enregistrés)
→ Import > FortiToken Mobile : scanner le QR code sur l'app FortiToken
```

### CLI de vérification

```
# Vérifier les tokens actifs
show system fortitoken

# Vérifier le MFA par compte
show system admin | grep -e "two-factor" -e "fortitoken" -e "email-to"
```

Vérifier la présence de `set two-factor fortitoken` ou `set two-factor email` pour chaque compte admin avec accès en écriture.

### Remédiation

**Option 1 — FortiToken Mobile** (après enregistrement du token dans `System > FortiTokens`) :

```
config system admin
    edit "adm-votreprenom"
        set two-factor fortitoken
        set fortitoken "<serial_token_fortitoken_mobile>"
        set email-to "<admin@domaine.fr>"
    next
end
```

**Option 2 — FortiToken Hardware** (token physique, numéro de série sur le token) :

```
config system admin
    edit "adm-securite"
        set two-factor fortitoken
        set fortitoken "<serial_token_hardware>"
    next
end
```

**Option 3 — FortiAuthenticator RADIUS** (pour déploiements entreprise) :

```
# Étape 1 : Configurer le serveur RADIUS FortiAuthenticator
config user radius
    edit "fortiauth-mfa"
        set server "<IP_FortiAuthenticator>"
        set secret "<shared_secret_radius>"
        set auth-type auto
        set radius-port 1812
    next
end

# Étape 2 : Activer le MFA RADIUS sur le compte admin
config system admin
    edit "adm-votreprenom"
        set two-factor radius
        set radius-server "fortiauth-mfa"
    next
end
```

**Option 4 — FortiAuthenticator LDAP avec SAML** (pour SSO entreprise) :

```
# FortiAuthenticator agit comme IdP SAML — configurer via l'interface FortiAuthenticator
# Sur FortiGate : activer SAML avec FortiAuthenticator comme IdP
config system saml
    set status enable
    set role service-provider
    set idp-cert "<cert_fortiauth_idp>"
    set idp-single-sign-on-url "https://<IP_FortiAuth>/saml-idp/..."
end
```

> ***Note FortiAuthenticator :*** *FortiAuthenticator supporte les méthodes MFA suivantes : FortiToken (TOTP), SMS, Email OTP, FIDO2/WebAuthn, et intégration avec des IdP tiers (Okta, Azure AD, etc.). Recommandé pour les organisations avec plus de 10 administrateurs.*

**Valeur par défaut :** MFA désactivée par défaut sur tous les comptes.

**Critère de conformité :** Tous les comptes administrateurs avec accès `super_admin` ou accès en écriture ont `two-factor` activé. Les comptes d'accès `read-only` sont exemptés si l'organisation l'accepte avec justification documentée. Pour les environnements sensibles : FortiToken Hardware ou FortiAuthenticator avec TOTP recommandés.

---

# Domaine 3 — Sécurisation de l'interface de gestion

***Objectif :*** *Restreindre l'exposition de l'interface de gestion du FortiGate au strict nécessaire. L'accès management depuis Internet est le vecteur initial d'exploitation documenté dans la majorité des incidents FortiGate recensés par le PSIRT et CISA. Les CVE-2026-24858 et CVE-2025-59718/59719 (SAML SSO bypass) rappellent que les mécanismes d'authentification déléguée constituent une surface d'attaque critique.*

---

## Contrôle 3.1 — Désactiver l'accès management depuis l'interface WAN

***CIS Ref :*** *1.3* | ***MITRE :*** *T1190, T1133* | ***Niveau :*** 🔴 *CRITIQUE*

**Description du risque**

Exposer les services de gestion (HTTPS, HTTP, SSH, SNMP, Telnet, ping) sur l'interface WAN expose directement le FortiGate à tous les scanners et attaquants d'Internet. Les vulnérabilités d'authentification FortiGate (CVE-2022-40684, CVE-2023-27997, CVE-2024-21762, CVE-2026-24858) ont été massivement exploitées sur des équipements avec management WAN accessible. Les scans Shodan identifient en temps réel les FortiGate exposés avec leur version de firmware.

**Impact potentiel**

- Exploitation directe depuis Internet de vulnérabilités d'authentification (CVE CISA KEV)
- Scan et énumération de l'équipement par des outils automatisés
- Attaques par brute force sur les credentials administrateurs
- Compromission complète du périmètre de sécurité réseau

**Navigation**

```
Network > Interfaces
→ Sélectionner l'interface WAN (généralement "wan1" ou "port1")
→ Éditer
→ Section "Administrative Access"
→ Décocher : HTTPS, HTTP, SSH, SNMP, Telnet, FMG-Access, Ping
→ Ne conserver que ce qui est strictement nécessaire pour le trafic utilisateur
→ OK
```

**CLI de vérification**

```
show system interface
```

Pour l'interface WAN : `set allowaccess` ne doit contenir aucun des services management (https, http, ssh, snmp, telnet, ping, radius-acct).

**Remédiation**

```
config system interface
    edit "wan1"
        set allowaccess ping
    next
end
```

> *Note : Remplacer “wan1” par le nom réel de votre interface WAN. Le `ping` peut être retiré également pour une sécurité maximale. N’utiliser que `set allowaccess` vide ou `set allowaccess none` si aucun accès management n’est nécessaire depuis le WAN.*

```
config system interface
    edit "wan1"
        unselect allowaccess https http ssh snmp telnet ping radius-acct
    next
end
```

**Valeur par défaut :** Variable selon le modèle. Sur certains modèles, HTTPS et Ping sont activés par défaut sur l’interface WAN.

**Critère de conformité :** `allowaccess` sur l’interface WAN ne contient pas `https`, `http`, `ssh`, `snmp`, `telnet`. L’accès management doit transiter par une interface dédiée ou un VLAN de gestion.

---

## Contrôle 3.2 — Restreindre les protocoles d’accès management

> ***CIS Ref :** 2.4.5, 2.4.7 | **MITRE :** T1040 | **Niveau :** 🟢 L1*

**Description du risque**

Sur l’interface de management dédiée, seuls HTTPS (TLS ≥ 1.2) et SSH doivent être autorisés. Les ports par défaut (443, 22) sont connus et scannés. Changer les ports administratifs sur des valeurs non standard réduit l’exposition aux scans automatisés, bien que cette mesure soit insuffisante seule (security by obscurity limitée).

**Impact potentiel**

- Exposition aux scans automatisés sur les ports 443/22 standards
- Interception de trafic management en clair si HTTP ou Telnet est activé

**Navigation**

```
System > Settings
→ Section "Administration Settings"
→ "HTTPS Port" : valeur personnalisée (ex: 8443) — optionnel
→ "SSH Port" : valeur personnalisée (ex: 2222) — optionnel
→ "HTTP Redirect to HTTPS" : activer
→ Apply
```

**CLI de vérification**

```
get system global | grep admin-port
```

**Remédiation**

```
config system global
    set admin-port 80
    set admin-https-redirect enable
    set admin-sport 8443
    set admin-ssh-port 2222
end
```

**Valeur par défaut :** HTTPS port 443, SSH port 22, HTTP port 80.

**Critère de conformité :** Telnet désactivé, HTTP désactivé ou redirigé uniquement vers HTTPS. Ports management documentés et inclus dans la matrice de flux de l'organisation.

---

## Contrôle 3.3 — Certificat TLS valide pour l'administration HTTPS

> ***CIS Ref :*** *2.4.5 (étendu)* | ***MITRE :*** *T1557* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

Le certificat auto-signé par défaut de FortiGate génère des alertes de sécurité dans les navigateurs et n'offre pas de garantie d'authenticité. Les administrateurs habitués à ignorer les alertes de certificat deviennent vulnérables aux attaques MITM. Un certificat signé par une PKI d'entreprise ou une CA publique reconnue garantit l'authenticité du FortiGate et prévient les attaques de substitution.

**Impact potentiel**

- Attaques MITM non détectées si les administrateurs ignorent les alertes TLS
- Phishing des credentials administrateurs via un faux portail FortiGate
- Non-conformité avec les politiques PKI de l'organisation

**Navigation**

```
System > Certificates
→ Import > Local Certificate
→ Importer le certificat PKCS12 ou le couple certificat/clé privée
→ System > Settings
→ "HTTPS Server Certificate" : sélectionner le certificat importé
→ Apply
```

**CLI de vérification**

```
show system global | grep admin-server-cert
get system certificate local
```

**Remédiation**

```
config system global
    set admin-server-cert "<nom_du_certificat>"
end
```

**Valeur par défaut :** Certificat auto-signé Fortinet_Factory livré avec l'équipement.

**Critère de conformité :** Certificat d'administration signé par la PKI de l'organisation ou une CA reconnue. Date d'expiration > 30 jours. Correspondance FQDN entre le CN/SAN du certificat et l'URL d'administration.

---

## Contrôle 3.4 — Local-in Policies : restriction d'accès management et journalisation

***CIS Ref :*** *2.4.6* | ***MITRE :*** *T1078, T1190, T1602.002* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Les Trusted Hosts sur les comptes administrateurs filtrent par compte, mais les Local-in Policies permettent de bloquer le trafic vers le FortiGate lui-même au niveau du pare-feu, indépendamment du compte utilisé. Cette double couche garantit qu'aucune tentative de connexion ne peut atteindre le démon d'administration depuis des adresses non autorisées.

**La journalisation des Local-in Policies** est un mécanisme forensique essentiel : elle permet de tracer toutes les tentatives d'accès au plan de contrôle du FortiGate (T1602.002 — Network Device Configuration Dump) même quand elles sont bloquées. Sans cette journalisation, les tentatives d'accès refusées sont invisibles.

**Impact potentiel**

- Connexions administratives depuis des IP non répertoriées dans les Trusted Hosts individuels
- Contournement des restrictions per-compte via des comptes créés sans Trusted Hosts
- Exposition des services d'administration à des scans et tentatives de brute force
- Impossibilité de détecter les tentatives de scan/exploitation sans journalisation Local-in

**Navigation**

```
Policy & Objects > Local In Policy
→ Create New
→ Incoming Interface : <interface_management>
→ Source Address : <objet_IP_réseau_management>
→ Destination Address : all
→ Service : HTTPS, SSH (services d'administration)
→ Action : ACCEPT
→ Log Allowed Traffic : activer
→ Créer une règle DENY all en dessous avec logging activé
→ Apply
```

**CLI de vérification**

```
show firewall local-in-policy
```

Vérifier la présence de règles avec `set logtraffic all` sur les règles DENY.

**Remédiation**

```
config firewall address
    edit "net_management"
        set subnet 192.168.100.0 255.255.255.0
    next
end

config firewall local-in-policy
    edit 1
        set intf "mgmt"
        set srcaddr "net_management"
        set dstaddr "all"
        set action accept
        set service "HTTPS" "SSH"
        set schedule "always"
        set logtraffic all
    next
    edit 2
        set intf "mgmt"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set service "ALL"
        set schedule "always"
        set logtraffic all
    next
end
```

> ***Journalisation forensique :*** *Activer `set logtraffic all` sur les règles DENY des Local-in Policies permet de détecter les scans et tentatives d'exploitation des interfaces de gestion, même les tentatives bloquées. Ces logs sont précieux pour l'investigation et la corrélation SIEM.*

**Valeur par défaut :** Aucune Local-in Policy configurée — tout le trafic vers le FortiGate est accepté sur les interfaces avec `allowaccess` activé. Aucune journalisation des accès refusés.

**Critère de conformité :** Au moins une Local-in Policy restreignant l'accès HTTPS/SSH au sous-réseau de management. Règle DENY-ALL en fin de liste pour les interfaces de management. `logtraffic all` activé sur les règles DENY pour la traçabilité forensique.

---

### Contrôle 3.5 — Version TLS minimum TLS 1.2 pour le management

> ***CIS Ref :*** *2.1.10* | ***MITRE :*** *T1557* | ***Niveau :*** 🟢 *L1*

**Description du risque**

TLS 1.0 et TLS 1.1 sont des protocoles dépréciés avec des vulnérabilités connues (POODLE, BEAST, CRIME). Leur utilisation pour l'accès administratif expose les sessions HTTPS à des attaques de downgrade et de déchiffrement. TLS 1.3 est actuellement le protocole le plus sécurisé et doit être activé en priorité. TLS 1.2 reste le minimum acceptable.

**Impact potentiel**

- Attaques de downgrade TLS permettant d'utiliser des algorithmes faibles
- Déchiffrement de sessions administratives via exploitation de vulnérabilités TLS < 1.2
- Non-conformité PCI-DSS (qui exige TLS 1.2 minimum depuis 2018)

**Navigation**

```
System > Settings
→ Section "Administration Settings"
→ "Minimum TLS Version" : TLS 1.2 (recommandé : TLS 1.3)
→ Apply
```

**CLI de vérification**

```
get system global | grep admin-https-ssl-versions
```

Valeur attendue : `tlsv1-2` ou `tlsv1-3` (ou les deux).

**Remédiation**

```
config system global
    set admin-https-ssl-versions tlsv1-2 tlsv1-3
end
```

Pour n'autoriser que TLS 1.3 (environnements les plus sensibles) :

```
config system global
    set admin-https-ssl-versions tlsv1-3
end
```

**Valeur par défaut :** FortiOS 7.x : TLS 1.2 et 1.3 activés. FortiOS 6.x : TLS 1.1, 1.2 et 1.3 activés.

**Critère de conformité :** `admin-https-ssl-versions` ne contient pas `tlsv1-0` ni `tlsv1-1`. Valeur minimale : `tlsv1-2`. Recommandé : `tlsv1-3` uniquement pour les environnements sensibles.

---

## Contrôle 3.6 — Durcissement SAML/SSO et authentification déléguée

***CIS Ref :*** *(best practice étendue)* | ***MITRE :*** *T1078, T1606* | ***Niveau :*** 🔴 *CRITIQUE*

### Description du risque

Les CVE-2026-24858, CVE-2025-59718 et CVE-2025-59719 (CVSS 9.8 chacune, CISA KEV) démontrent que l'authentification SAML SSO sur FortiGate constitue une surface d'attaque critique. Ces vulnérabilités permettent à un attaquant non authentifié de contourner complètement l'authentification en forgeant des messages SAML malformés ou en exploitant des failles dans la validation du SSO FortiCloud.

Si le SAML/SSO n'est pas utilisé dans votre environnement, il doit être désactivé. S'il est utilisé, la chaîne de certificats IdP doit être vérifiée rigoureusement et les versions FortiOS affectées doivent être patchées immédiatement.

**CVE détaillées :**

| CVE | DESCRIPTION | CISA KEV | REMÉDIATION |
|---|---|---|---|
| CVE-2026-24858 | Auth bypass via SAML SSO — exploitation active depuis Déc 2025 | Oui (Déc 2025) | Patch FortiOS immédiat |
| CVE-2025-59718 | FortiCloud SSO bypass via SAML forgé — campagne active | Oui | Patch + vérification IdP |
| CVE-2025-59719 | Variante SSO bypass (couplée CVE-2025-59718) | Oui | Patch + audit des logs SSO |

### Impact potentiel

- Accès administrateur complet sans authentification valide (bypass total)
- Compromission par des acteurs étatiques qui ont activement exploité ces vulnérabilités
- Persistance difficile à détecter si l'attaquant a créé des comptes supplémentaires
- Mouvement latéral immédiat vers l'ensemble du réseau géré par le FortiGate

### Navigation

```
System > Settings
→ Section "SAML Single Sign-On"
→ Si SAML non utilisé : désactiver complètement
→ Si SAML utilisé : vérifier la configuration IdP et les certificats
→ Apply
```

**CLI de vérification**

```
# Vérifier si SAML/SSO est activé
get system saml
show system saml

# Vérifier les administrateurs SAML
show system admin | grep saml

# Vérifier la configuration FortiCloud SSO
show system fortiguard | grep sso
```

**Remédiation**

Si SAML/SSO n'est pas utilisé (recommandé si non requis) :

```
config system saml
    set status disable
end
```

Si SAML est requis, vérifier et renforcer la configuration :

```
config system saml
    set status enable
    set role service-provider
    set cert "<certificat_sp_dedié>"
    set idp-cert "<certificat_idp_verifie>"
    set idp-entity-id "<entity_id_exact>"
    set idp-single-sign-on-url "<url_idp_https>"
    set default-login-page normal
end
```

**Vérification de la chaîne de certificats IdP :**

```
# Lister les certificats CA de confiance
show vpn certificate ca

# Vérifier la validité du certificat IdP importé
diagnose vpn certificate list
```

**Mesures complémentaires :** - Appliquer le patch FortiOS corrigeant CVE-2026-24858 et CVE-2025-59718/59719 immédiatement - Si SAML était activé sur une version vulnérable : auditer les comptes administrateurs créés (backdoors possibles) - Activer les alertes sur les événements d'authentification SAML dans les logs

**Valeur par défaut :** SAML désactivé par défaut sur les nouvelles installations.

**Critère de conformité :** SAML désactivé si non utilisé ( `status : disable` ). Si activé : certificat IdP valide et vérifié, version FortiOS non affectée par CVE-2026-24858 et CVE-2025-59718/59719. Audit des comptes admin après toute exposition à une version vulnérable.

---

## Contrôle 3.7 — Restrictions géographiques et ISDB pour l'accès management

> ***CIS Ref :*** *(best practice communauté Fortinet)* | ***MITRE :*** *T1078, T1190* | ***Niveau :*** 🔵 *L2*

### Description du risque

L'Internet Service Database (ISDB) de FortiGuard permet de restreindre l'accès management aux seuls pays ou régions géographiques légitimes pour l'organisation. Cette restriction géographique via les objets GeoIP bloque automatiquement les tentatives de connexion depuis des pays où l'organisation n'a aucune présence opérationnelle, réduisant significativement l'exposition aux campagnes d'attaque globales.

### Impact potentiel

- Réduction de 80 à 95 % des tentatives de brute force et de scan sur l'interface de management
- Blocage automatique des campagnes d'exploitation FortiGate depuis des pays tiers
- Contexte forensique amélioré : toute connexion depuis un pays non autorisé est une anomalie

### Navigation

```
Policy & Objects > Local In Policy
→ Créer une règle avec la source géographique restreinte
→ Source : objet GeoIP (ex: France uniquement)
→ Destination : interface management
→ Service : HTTPS, SSH
→ Action : ACCEPT (avant la règle DENY all)
```

### CLI de vérification

```
show firewall local-in-policy
show firewall address | grep ipcountry
```

### Remédiation

```
# Créer un objet géographique (ex: France)
config firewall address
    edit "geo-france"
        set type ipmask
        set country "FR"
    next
end

config firewall local-in-policy
    edit 1
        set intf "mgmt"
        set srcaddr "geo-france"
        set dstaddr "all"
        set action accept
        set service "HTTPS" "SSH"
        set schedule "always"
        set logtraffic all
    next
    edit 2
        set intf "mgmt"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set service "ALL"
        set schedule "always"
        set logtraffic all
    next
end
```

**Valeur par défaut :** Aucune restriction géographique configurée par défaut.

**Critère de conformité :** Local-in Policy géographique configurée pour limiter l'accès management aux pays où l'organisation dispose de présences légitimes. Journalisation activée sur les règles de blocage géographique.

---

## Contrôle 3.8 — Durcissement de l'API REST FortiGate

***CIS Ref :*** *(best practice Fortinet)* | ***MITRE :*** *T1078.003, T1552* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

L'API REST FortiGate permet d'automatiser la gestion de la configuration, les requêtes de monitoring et les modifications de politiques via des appels HTTP/HTTPS authentifiés par des tokens. Un token API compromis ou mal protégé confère les mêmes privilèges que le compte administrateur associé — sans requérir de session interactive et donc sans déclencher les alertes de connexion habituelles. La CVE-2022-40684 (auth bypass CVSS 9.8) exploitait précisément l'API REST pour contourner l'authentification complète. Un token exposé dans un script ou un dépôt de code peut permettre une compromission silencieuse et persistante.

**Risques spécifiques à l'API REST :**

| RISQUE | DESCRIPTION | MITRE |
|---|---|---|
| Token API en clair dans un script | Exposition de credentials dans du code source | T1552 (Unsecured Credentials) |
| API accessible depuis n'importe quelle IP | Token utilisable depuis Internet si volé | T1078.003 (Local Accounts) |
| Compte API avec droits super_admin | Même compromission que la console admin | T1078.003 |
| Pas de rotation des tokens | Token valide indéfiniment après exfiltration | T1552 |
| API activée sur interface WAN | Surface d'attaque directement exposée | T1190 |

**Impact potentiel**

- Modification silencieuse de politiques de sécurité via l'API sans alerte de connexion GUI
- Exfiltration de la configuration complète (clés VPN, certificats, comptes) via appels API
- Persistance d'accès par un token compromis non détecté pendant des mois
- Escalade de privilèges si un compte API de monitoring dispose de droits excessifs

**Navigation**

```
System > Administrators
→ Create New > REST API Admin
→ Administrator Profile : "api-read-only" (ou profil minimal requis)
→ Trusted Hosts : OBLIGATOIRE — saisir uniquement les IP des systèmes d'automatisation
→ "PKI Group" : optionnel pour authentification par certificat
→ "Comments" : documenter la finalité du token
→ OK
→ Copier le token généré dans un coffre-fort de mots de passe (affiché une seule fois)
```

**CLI de vérification**

```
# Lister tous les comptes API configurés
show system api-user

# Vérifier les Trusted Hosts de chaque compte API
show system api-user | grep -e "name" -e "trusthost" -e "accprofile"

# Vérifier que l'API n'est pas accessible depuis les interfaces WAN
show system interface wan1 | grep allowaccess
# "api-access" ne doit pas apparaître
```

**Remédiation**

**Étape 1 — Créer un compte API dédié avec droits minimaux :**

```
# Créer un profil de droits restreint pour le monitoring API (lecture seule)
config system accprofile
    edit "api-monitoring-readonly"
        set secfabgrp read
        set ftviewgrp read
        set authgrp read
        set sysgrp read
        set netgrp read
        set loggrp read
        set fwgrp read
        set vpngrp none
        set utmgrp read
        set wanoptgrp none
        set wifi read
    next
end

# Créer le compte API avec Trusted Hosts restrictifs
config system api-user
    edit "api-monitoring-siem"
        set comments "Compte API lecture seule pour SIEM - rotation trimestrielle"
        set accprofile "api-monitoring-readonly"
        set vdom "root"
        config trusthost
            edit 1
                set ipv4-trusthost 10.100.50.10 255.255.255.255
                # IP du serveur SIEM uniquement
            next
            edit 2
                set ipv4-trusthost 10.100.50.11 255.255.255.255
                # IP du serveur d'automatisation secondaire
            next
        end
    next
end
```

**Étape 2 — Générer et stocker le token API de manière sécurisée :**

```
# Générer un nouveau token API (via GUI : System > Administrators > api-monitoring-siem >
Generate API Token)
# Le token n'est affiché qu'une seule fois — le stocker immédiatement dans CyberArk /
HashiCorp Vault

# Vérifier les tokens existants (les tokens ne sont pas lisibles en clair après création)
diagnose test application httpsd 1
```

**Étape 3 — Désactiver l'API si non utilisée sur les interfaces exposées :**

```
# Sur les interfaces WAN et production, s'assurer que l'accès API n'est pas activé
config system interface
    edit "wan1"
        # Vérifier que "api-access" n'est pas dans allowaccess
        show | grep allowaccess
    next
end

# Si l'API REST est entièrement inutilisée, la désactiver globalement
config system global
    set admin-https-redirect enable
    # Il n'existe pas de désactivation globale de l'API REST en FortiOS 7.4
    # La protection se fait par Trusted Hosts + profil minimal + Local-in Policy
end

# Bloquer l'accès à l'API depuis les réseaux non autorisés via Local-in Policy
config firewall local-in-policy
    edit 5
        set name "block-api-non-autorise"
        set intf "mgmt"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set service "HTTPS"
        set schedule "always"
        set logtraffic all
        set comments "Bloquer l'API depuis les IP non autorisées (complément Trusted Hosts)"
    next
end
```

**Étape 4 — Surveiller les accès API via les logs :**

```
# Activer la journalisation des accès API
config log eventfilter
    set admin enable
    # Les appels API apparaissent dans les logs admin avec le champ "api"
end

# Consulter les logs d'accès API récents
execute log filter category 0
execute log filter field action "api"
execute log display
```

**Politique de rotation des tokens API :**

| FRÉQUENCE | CONTEXTE | ACTION |
|---|---|---|
| Trimestrielle | Rotation normale | Générer un nouveau token, mettre à jour les scripts, révoquer l'ancien |
| Immédiate | Départ d'un membre de l'équipe | Révoquer et régénérer tous les tokens connus du collaborateur |

| FRÉQUENCE | CONTEXTE | ACTION |
|---|---|---|
| Immédiate | Suspicion de compromission | Révoquer le token, auditer les appels API récents dans les logs |
| Après chaque audit | Conformité | Documenter la rotation dans le journal de sécurité |

> ***Bonne pratique — jamais de credentials admin via l'API :*** *Ne jamais utiliser les credentials d'un compte administrateur humain (`admin-prenom`) pour les appels API. Toujours utiliser un compte `api-user` dédié. Les comptes API dédiés n'ont pas de session GUI et leurs activités sont distinctement identifiables dans les logs.*

**Valeur par défaut :** Aucun compte API REST configuré par défaut. La fonctionnalité est disponible mais désactivée (aucun token existant) à la livraison.

**Critère de conformité :** Tous les comptes `api-user` ont au moins un `trusthost` configuré avec une IP ou sous-réseau restrictif. Profil de droits minimal (lecture seule si monitoring seulement, pas de super_admin). Tokens stockés dans un coffre-fort de mots de passe. Rotation trimestrielle documentée. Aucun accès API depuis les interfaces WAN. Logs des accès API activés et transmis vers le SIEM. `show system api-user` ne retourne aucun compte sans trusthost configuré.

---

# Domaine 4 — Politiques de sécurité et objets

***Objectif :*** *S'assurer que la politique de sécurité du FortiGate respecte le principe du moindre privilège, bloque le trafic malveillant connu et journalise l'ensemble des flux pour permettre la détection et l'investigation.*

---

## Contrôle 4.1 — Blocage du trafic intra-zone

***CIS Ref :*** *1.2* | ***MITRE :*** *T1021* | ***Niveau :*** 🟢 *L1*

### Description du risque

Par défaut, FortiOS autorise le trafic entre interfaces appartenant à la même zone réseau. Cette configuration permet à un attaquant ayant compromis un équipement de se déplacer latéralement vers d'autres équipements sur le même segment sans traverser de règle de filtrage. Le blocage intra-zone force tout le trafic inter-hôtes à passer par les politiques de sécurité du FortiGate.

### Impact potentiel

- Mouvement latéral non détecté entre équipements du même sous-réseau
- Propagation de malwares et de ransomwares sans restriction inter-VLAN
- Impossibilité de détecter et bloquer les scans internes

### Navigation

```
Network > Interfaces
→ Sélectionner la zone concernée (ex: DMZ, LAN)
→ Éditer
→ "Block intra-zone traffic" : activer
→ OK
```

### CLI de vérification

```
config system zone
    edit "DMZ"
        show full
```

Vérifier : `set intrazone deny`.

### Remédiation

```
config system zone
    edit "DMZ"
        set intrazone deny
    next
    edit "LAN"
        set intrazone deny
    next
end
```

**Valeur par défaut :** Le trafic intra-zone est **bloqué** par défaut à la création d'une zone (`intrazone deny` est la valeur par défaut documentée dans le CIS).

**Critère de conformité :** `intrazone deny` configuré sur toutes les zones contenant plusieurs interfaces. Vérifier avec `show system zone`.

---

## Contrôle 4.2 — Interdire les règles avec service "ALL"

***CIS Ref :*** *3.2* | ***MITRE :*** *T1048, T1071* | ***Niveau :*** 🟠 *ÉLEVÉ*

### Description du risque

Une règle firewall utilisant le service "ALL" autorise tous les ports et protocoles entre la source et la destination, contournant entièrement le filtrage par port. Cette pratique courante lors de dépannages est souvent oubliée en production et crée des chemins d'exfiltration et de communication C2 non contrôlés. Le CIS Benchmark FortiGate 7.4.x recommande explicitement l'interdiction du service "ALL" dans les politiques.

### Impact potentiel

- Exfiltration de données sur des ports non standards (T1048)
- Communication C2 via protocoles tunnelés (DNS, ICMP, HTTP) non bloqués
- Contournement complet des profils de sécurité qui filtrent par protocole

### Navigation

```
Policy & Objects > Firewall Policy
→ Parcourir toutes les règles
→ Identifier les règles avec "Service : ALL"
→ Éditer chaque règle
→ Remplacer "ALL" par les services explicitement requis
→ OK
```

### CLI de vérification

```
show firewall policy | grep -f service
```

Rechercher les occurrences de `set service "ALL"`.

### Remédiation

Pour chaque règle utilisant ALL :

```
config firewall policy
    edit <id_politique>
        set service "HTTP" "HTTPS" "DNS"
        (remplacer par les services réellement nécessaires)
    next
end
```

**Valeur par défaut :** Les règles créées via l'assistant FortiGate utilisent parfois "ALL" par défaut.

**Critère de conformité :** Aucune règle de politique de sécurité active ne contient `service "ALL"` sauf exception documentée et justifiée. Audit trimestriel des politiques recommandé.

---

## Contrôle 4.3 — Bloquer le trafic vers les serveurs Tor, malveillants et scanners via ISDB

***CIS Ref :*** *3.3* | ***MITRE :*** *T1090, T1041* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

FortiGuard maintient des listes d'adresses IP associées à des nœuds Tor, des serveurs malveillants connus et des outils de scan via l'**Internet Service Database (ISDB)**. L'ISDB est une base dynamique mise à jour en continu par FortiGuard qui contient des milliers de services et d'adresses IP catégorisés. Bloquer explicitement ce trafic via l'ISDB empêche les communications avec des infrastructures C2 connues et l'exfiltration via Tor, sans nécessiter de maintenance manuelle de listes noires.

**Impact potentiel**

- Communication de malwares avec des serveurs C2 connus non bloquée
- Exfiltration de données via Tor ou proxies anonymes
- Propagation d'infections depuis des hôtes compromis vers des serveurs malveillants

**Navigation**

```
Policy & Objects > Firewall Policy
→ Create New
→ Incoming Interface : LAN (ou toutes interfaces internes)
→ Outgoing Interface : WAN
→ Source : all
→ Destination : Fortinet-Malicious.Server, Tor-Exit.Node (ISDB objects)
→ Service : ALL
→ Action : DENY
→ Logging : All Sessions
→ Positionner AVANT les règles permissives
→ OK
```

**CLI de vérification**

```
show firewall policy
```

Vérifier la présence d'une règle avec `set internet-service-src` ou `set internet-service` faisant référence aux objets Fortinet-Malicious et Tor.

**Remédiation**

```
config firewall policy
    edit 1
        set name "BLOCK-Tor-Malicious"
        set srcintf "LAN"
        set dstintf "WAN"
        set srcaddr "all"
        set internet-service enable
        set internet-service-id 65646 65647
        set action deny
        set schedule "always"
        set logtraffic all
        set comments "Bloc Tor et serveurs malveillants FortiGuard ISDB"
    next
end
```

**Valeur par défaut :** Aucun blocage ISDB configuré par défaut.

**Critère de conformité :** Règle de blocage ISDB pour Tor, serveurs malveillants et scanners présente et positionnée avant les règles permissives. Mise à jour ISDB activée (via `execute update-now`).

---

## Contrôle 4.4 — Journalisation activée sur toutes les politiques

> ***CIS Ref :*** *3.4* | ***MITRE :*** *T1562.004* | ***Niveau :*** 🟢 *L1*

**Description du risque**

Sans journalisation sur les politiques de sécurité, les flux autorisés ou bloqués ne sont pas tracés, rendant impossible la détection d'incidents, l'investigation forensique et la conformité réglementaire. La journalisation doit être activée sur l'ensemble des règles, y compris les règles d'autorisation, pour assurer la visibilité complète du trafic réseau.

**Impact potentiel**

- Impossibilité de détecter des compromissions actives sans journalisation du trafic
- Investigation forensique impossible en cas d'incident de sécurité
- Non-conformité avec les exigences réglementaires (PCI-DSS, ISO 27001, RGPD)

**Navigation**

```
Policy & Objects > Firewall Policy
→ Éditer chaque politique
→ Section "Logging Options"
→ "Log Allowed Traffic" : All Sessions (ou Security Events minimum)
→ "Log Violation Traffic" : activer
→ OK
```

**CLI de vérification**

```
show firewall policy | grep logtraffic
```

Toutes les politiques doivent avoir `set logtraffic all` ou `set logtraffic utm`.

**Remédiation**

Pour activer la journalisation sur toutes les politiques existantes :

```
config firewall policy
    edit <id>
        set logtraffic all
        set logtraffic-start enable
    next
end
```

**Valeur par défaut :** `logtraffic utm` par défaut sur les nouvelles politiques (uniquement les événements UTM, pas tous les flux).

**Critère de conformité :** Toutes les politiques actives ont `logtraffic all` ou `logtraffic utm` avec `logtraffic-start enable`. Aucune politique sans journalisation.

---

## Contrôle 4.5 — Nettoyage des règles inutilisées

***CIS Ref :*** *3.1* | ***MITRE :*** *T1562* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

Les règles non utilisées depuis plus de 90 jours représentent une surface d'attaque passive. Elles peuvent autoriser des flux résiduels non nécessaires, compliquer l'audit de la politique de sécurité et masquer des backdoors. FortiGate permet d'identifier les règles non utilisées via le compteur de sessions et la date de dernière correspondance.

**Impact potentiel**

- Flux résiduels non nécessaires qui élargissent la surface d'attaque
- Politique de sécurité opaque rendant difficile l'audit de conformité
- Règles orphelines potentiellement créées par des attaquants lors d'une compromission antérieure

**Navigation**

```
Policy & Objects > Firewall Policy
→ Activer la colonne "Last Used"
→ Trier par "Last Used" (ascendant)
→ Identifier les règles sans activité depuis > 90 jours
→ Vérifier la nécessité opérationnelle avec les équipes réseau
→ Désactiver, puis supprimer après confirmation
```

**CLI de vérification**

```
diagnose firewall iprope show 100004 <id_policy>
```

Ou pour un audit global :

```
show firewall policy
```

Vérifier les politiques avec `set status disable` ou commentaires marqués comme obsolètes.

**Remédiation**

```
config firewall policy
    edit <id_politique_inutilisee>
        set status disable
    next
end
```

Après validation (30 jours de monitoring) :

```
config firewall policy
    delete <id_politique_inutilisee>
end
```

**Valeur par défaut :** Aucune gestion automatique des règles inutilisées.

**Critère de conformité :** Processus de revue trimestrielle des politiques documenté. Aucune règle inactive depuis plus de 90 jours sans justification documentée.

---

## Contrôle 4.6 — Virtual Patching via Local-in Policies

***CIS Ref :*** *(best practice FortiOS 7.4)* | ***MITRE :*** *T1190, T1133* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

Lorsqu'un patch firmware n'est pas immédiatement déployable (contraintes opérationnelles, tests de régression, fenêtres de maintenance planifiées), FortiOS 7.4 permet le **Virtual Patching** : créer des Local-in Policies ou des règles IPS ciblées qui bloquent le vecteur d'exploitation d'une CVE spécifique sans mise à jour du firmware. Cette approche est documentée par Fortinet comme mesure compensatoire temporaire.

**Impact potentiel**

- Exposition à des CVE critiques non patchées pendant la période de déploiement du patch
- Exploitation de la fenêtre entre la publication d'un advisory PSIRT et le déploiement du patch

**Navigation**

```
Security Profiles > Intrusion Prevention
→ Créer une signature personnalisée ciblant la CVE spécifique
→ Ou utiliser une Local-in Policy pour bloquer les IP sources connues d'exploitation

Policy & Objects > Local In Policy
→ Créer des règles de blocage ciblées sur les vecteurs d'exploitation connus
```

**CLI de vérification**

```
show firewall local-in-policy
show ips sensor | grep custom
```

**Remédiation**

Exemple de virtual patch pour bloquer l'accès SAML depuis Internet (compensation CVE-2026-24858) :

```
# Bloquer l'accès au endpoint SAML depuis des IP non autorisées
config firewall local-in-policy
    edit 10
        set intf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set service "HTTPS"
        set url-filter "/remote/saml"
        set schedule "always"
        set logtraffic all
        set comments "Virtual patch CVE-2026-24858 - temporaire"
    next
end
```

> ***Important :*** *Le virtual patching est une mesure compensatoire temporaire. Le patch firmware officiel Fortinet reste la remédiation définitive obligatoire.*

**Valeur par défaut :** Aucun virtual patch configuré par défaut.

**Critère de conformité :** Pour toute CVE critique non patchée depuis plus de 72h : mesure compensatoire documentée et active. Plan de déploiement du patch défini avec date cible. Retrait du virtual patch après application du patch officiel.

---

## Contrôle 4.7 — Zero Trust Quick Start : checklist de déploiement initial

***CIS Ref :*** *6.7, 12.2 (CIS Controls v8)* | ***MITRE :*** *T1078, T1133, T1021* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Le modèle Zero Trust (ZT) repose sur le principe “ne jamais faire confiance, toujours vérifier” — aucun utilisateur, terminal ou flux n’est implicitement autorisé même à l’intérieur du périmètre réseau. FortiOS 7.4 fournit l’ensemble des briques nécessaires à une architecture Zero Trust native : ZTNA, FortiClient EMS, Security Fabric, User-ID et profils de sécurité. La non-application du modèle Zero Trust laisse subsister des règles permissives “any→any” qui constituent les vecteurs de mouvement latéral les plus exploités dans les incidents modernes.

**Prérequis :** FortiGate FortiOS 7.4+, FortiClient EMS v7.0+, licences Security Fabric.

**Checklist Zero Trust Quick Start pour FortiGate**

| ÉTAPE | ACTION | CONTRÔLE ASSOCIÉ | PRIORITÉ |
|---|---|---|---|
| 1 | Supprimer **toutes** les règles avec source/destination/service “any” non justifiées | 4.2 | 🔴 CRITIQUE |
| 2 | Activer l’authentification User-ID sur toutes les règles — identifier l’utilisateur associé à chaque flux | 2.8 | 🟠 ÉLEVÉ |
| 3 | Appliquer des profils de sécurité (IPS, AV, DNS Filter, Web Filter) sur **100 %** des règles ACCEPT | 5.1–5.5 | 🟠 ÉLEVÉ |
| 4 | Segmenter le réseau en zones distinctes : Users / Servers / IoT / Management / DMZ | 9.4 | 🟠 ÉLEVÉ |
| 5 | Déployer FortiClient EMS pour la vérification de posture des terminaux | 7.7 | 🔵 L2 |
| 6 | Activer ZTNA pour l’accès applicatif | 7.6 | 🔵 L2 |

| ÉTAPE | ACTION | CONTRÔLE ASSOCIÉ | PRIORITÉ |
|---|---|---|---|
| | — remplacer le SSL-VPN par ZTNA | | |
| 7 | Connecter les équipements au Security Fabric pour une visibilité unifiée | 6.1 | 🟡 MOYEN |
| 8 | Vérifier le Security Rating ≥ 80/100 comme indicateur de maturité ZT | 6.3 | ⚪ INFO |

**Impact potentiel si le modèle Zero Trust n'est pas appliqué**

- Mouvement latéral non contrôlé dans les zones LAN suite à une compromission initiale (T1021)
- Accès distant non conditionné à la posture du terminal (T1133)
- Règles permissives "any→any" créant des chemins d'exfiltration non contrôlés (T1048)

**CLI de vérification — audit Zero Trust rapide**

```
# Vérifier les règles avec source "all" ou destination "all" sur trafic interne
show firewall policy | grep -e srcaddr -e dstaddr
# Toute règle avec "all" en interne doit avoir une justification documentée

# Vérifier que 100 % des règles ACCEPT ont un profil IPS
show firewall policy | grep -e "ips-sensor" -e action
# Chaque "set action accept" doit être suivi de "set ips-sensor"

# Vérifier l'activation du User-ID (authentification)
show firewall policy | grep identity-based

# Vérifier le statut du Security Rating Zero Trust
diagnose security-rating result | grep -e "Zero Trust" -e FAIL -e WARN
```

**Remédiation — actions prioritaires Zero Trust**

```
# 1. Activer l'authentification User-ID sur les règles d'accès critiques
config firewall policy
    edit <id_politique_critique>
        set identity-based enable
        set auth-cert "<certificat_ssl>"
    next
end

# 2. Vérifier et remplacer toutes les règles "any" par des objets spécifiques
# Identifier toutes les politiques avec source "all" et trafic interne
show firewall policy | grep -B5 -A5 "srcaddr.*all"

# 3. Planifier le Security Rating pour valider la posture ZT
execute security-rating run
diagnose security-rating result | grep FAIL
```

> ***Indicateur de maturité Zero Trust FortiGate :*** *Un score Security Rating ≥ 80/100 avec zéro défaillance “Critical” dans la catégorie Coverage (profils de sécurité) est le proxy le plus rapide pour évaluer l’avancement du déploiement Zero Trust. Voir Contrôle 6.3.*

**Valeur par défaut :** Règles permissives créées par défaut dans les assistants FortiGate. Aucune vérification de posture ZT activée par défaut.

**Critère de conformité :** Aucune règle “any→any” active sans profil de sécurité associé. Security Rating ≥ 80/100. FortiClient EMS connecté avec tags de conformité appliqués (Contrôle 7.7). ZTNA configuré pour au moins les accès applicatifs critiques (Contrôle 7.6). Revue Zero Trust trimestrielle documentée.

---

# Domaine 5 — Profils de sécurité (IPS, AV, Web, App)

> ***Objectif :*** *Activer et configurer correctement tous les profils de sécurité UTM/NGFW sur les politiques de trafic pour détecter et bloquer les menaces connues. Les profils de sécurité non appliqués ou mal configurés sont l'une des principales causes d'incidents sur les équipements FortiGate avec licences UTM.*

---

## Contrôle 5.1 — Profil IPS en mode protection avec détection Botnet

> ***CIS Ref :*** *4.1.1, 4.1.2* | ***MITRE :*** *T1190, T1203* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Le profil IPS FortiGate en mode "monitor" seul ne bloque pas les exploits — il les journalise seulement. En mode "protection" avec les signatures critiques et élevées en action "block", l'IPS devient un contrôle actif contre les exploits connus. La détection Botnet dans l'IPS identifie les communications C2 sortantes des hôtes compromis.

**Impact potentiel**

- Exploitation réussie d'équipements internes via des vulnérabilités connues non bloquées
- Communication C2 de malwares non détectée sans détection Botnet activée
- Mouvement latéral facilité par des exploits réseau non bloqués

**Navigation**

```
Security Profiles > Intrusion Prevention
→ Create New ou éditer le profil existant
→ "IPS Signatures and Filters" :
   - Signatures Critiques : Action = Block, Logging = Enable
   - Signatures Élevées : Action = Block, Logging = Enable
   - Signatures Moyennes : Action = Monitor, Logging = Enable
→ "Botnet C&C" : Enable (Scan Outgoing Connections to Botnet Sites)
→ OK
→ Appliquer le profil à toutes les politiques concernées
```

**CLI de vérification**

```
show ips sensor
```

Vérifier que le profil IPS appliqué contient `set action block` pour les signatures critiques et élevées. Vérifier `set scan-botnet-connections block` ou `monitor`.

**Remédiation**

```
config ips sensor
    edit "protection-strict"
        set block-malicious-url enable
        set scan-botnet-connections block
        config entries
            edit 1
                set severity critical high
                set action block
                set log enable
            next
            edit 2
                set severity medium
                set action monitor
                set log enable
            next
        end
    next
end
```

Appliquer le profil aux politiques :

```
config firewall policy
    edit <id>
        set ips-sensor "protection-strict"
    next
end
```

**Valeur par défaut :** Profil IPS “default” créé mais non appliqué aux politiques. Action : monitor pour toutes sévérités.

**Critère de conformité :** Profil IPS en action “block” pour les signatures critiques et élevées appliqué à toutes les politiques couvrant le trafic Internet. Détection Botnet en mode block.

---

## Contrôle 5.2 — Profil Antivirus avec mises à jour et sandbox FortiGuard

***CIS Ref :*** *4.2.1 à 4.2.6* | ***MITRE :*** *T1204, T1566* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Un profil Antivirus mal configuré (protocoles non couverts, scan incomplet, heuristique désactivée) laisse passer des malwares connus et inconnus. FortiOS 7.4 propose l’analyse heuristique AI/ML, la base de données Outbreak Prevention et l’intégration avec FortiGuard AI-Based Sandbox (inline CDR) pour les fichiers Office et PDF. Ces fonctionnalités doivent toutes être activées.

**Impact potentiel**

- Infection de postes internes par des malwares non détectés dans les téléchargements
- Propagation de ransomwares via des pièces jointes email non analysées
- Exfiltration via des malwares de type stealer non détectés sans heuristique

**Navigation**

```
Security Profiles > AntiVirus
→ Create New ou éditer le profil existant
→ "Inspection Mode" : Full Scan
→ Activer pour tous protocoles : HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, POP3, POP3S, FTP,
FTPS
→ "Heuristic" : Enable (Quarantine ou Block)
→ "AI/ML-based Malware Detection" : Enable
→ "Grayware" : Enable
→ "Outbreak Prevention" : Enable
→ "FortiGuard AI-Based Sandbox" : Submit (pour les fichiers suspects)
→ OK
```

**CLI de vérification**

```
show antivirus profile
```

Vérifier l'activation des protocoles et des options heuristiques.

**Remédiation**

```
config antivirus profile
    edit "av-complet"
        set comment "Profil AV complet avec sandbox"
        config http
            set options scan
            set outbreak-prevention enabled
        end
        config ftp
            set options scan
        end
        config smtp
            set options scan
        end
        config imap
            set options scan
        end
        set analytics-bl-filetype enable
        set analytics-wl-filetype enable
        set fortiai enable
        set fortindr enable
        set fortisandbox enable
        set fortisandbox-mode inline
    next
end
```

**Valeur par défaut :** Profil Antivirus "default" créé avec scan HTTP basique. Sandbox, heuristique et Outbreak Prevention désactivés.

**Critère de conformité :** Profil AV activé sur tous les protocoles (HTTP, FTP, SMTP, IMAP). Heuristique, Outbreak Prevention et Sandbox (si licence disponible) activés. Profil appliqué à toutes les politiques couvrant le trafic utilisateur.

## Contrôle 5.3 — DNS Filter — blocage des domaines malveillants, C2 et Botnet

***CIS Ref :*** *4.3.1, 4.3.2, 4.3.3* | ***MITRE :*** *T1071.004, T1568, T1071.003* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Le DNS Filter FortiGuard bloque les résolutions DNS vers des domaines malveillants, serveurs C2 et sites de phishing en temps réel. FortiOS 7.4 apporte des fonctionnalités avancées critiques : - **Blocage Botnet C&C FortiGuard** : redirection des requêtes DNS vers des serveurs C2 connus vers un sinkhole FortiGuard - **External IP blocklist** : blocage des domaines issus de listes noires externes FortiGuard - **FortiGuard DNS over HTTPS/TLS** : le DNS Filtering intercepte également les requêtes DoH/DoT des clients malveillants - **Redirect botnet C&C requests to FortiGuard** : les requêtes vers des C2 sont redirigées vers un sinkhole plutôt que simplement bloquées, permettant la détection des hôtes infectés

Cette couche est complémentaire à l'IPS et à l'AV — elle constitue souvent le **premier** mécanisme de détection des malwares qui tentent de joindre leur C2, avant même qu'une connexion TCP ne soit établie.

**Impact potentiel**

- Communication C2 de malwares via DNS non bloquée sans DNS Filter (T1071.004)
- Phishing et téléchargement de payloads depuis des domaines malveillants connus
- Exfiltration de données via DNS tunneling (T1071.004) : encodage de données dans les requêtes DNS
- Résolution de domaines DGA (Domain Generation Algorithm) par des malwares modernes sans détection
- Ransomwares modernes utilisant le DNS pour le C2 principal : non détectés sans DNS Filter

**Navigation**

```
Security Profiles > DNS Filter
→ Create New
→ "FortiGuard Category Based Filter" : activer
→ Catégories malveillantes (Botnet C&C, Malware, Phishing, Spam) : Block
→ "Block DNS Requests to Known Botnet C&C" : activer → Redirect to FortiGuard
→ "External IP blocklist" : activer
→ "Log All DNS Queries and Responses" : activer
→ OK
→ Appliquer le profil aux politiques concernées
```

**CLI de vérification**

```
show dnsfilter profile
```

Vérifier la présence de `set block-botnet enable`, `set external-ip-blocklist enable` et du log DNS activé.

**Remédiation**

```
config dnsfilter profile
    edit "dns-strict-fortigate"
        set comment "Filtrage DNS strict FortiGuard — blocage C2/Botnet/Phishing"
        set block-botnet enable
        set external-ip-blocklist enable
        set log-all-domain enable
        config ftgd-dns
            config filters
                edit 26
                    set category 26
                    set action block
                    # Catégorie 26 : Malware
                next
                edit 61
                    set category 61
                    set action block
                    # Catégorie 61 : Phishing
                next
                edit 64
                    set category 64
                    set action block
                    # Catégorie 64 : Botnet C&C
                next
                edit 83
                    set category 83
                    set action block
                    # Catégorie 83 : Spam
                next
            end
        end
    next
end
```

Appliquer le profil aux politiques de trafic interne :

```
config firewall policy
    edit <id_politique_interne>
        set dnsfilter-profile "dns-strict-fortigate"
    next
end
```

> ***Complément — FortiGuard Filtering sur le DNS du FortiGate lui-même :*** *En plus du profil DNS Filter pour le trafic client, il est recommandé de configurer le FortiGate pour utiliser les serveurs DNS FortiGuard avec filtrage activé pour ses propres résolutions :*

```
config system dns
    set primary 208.91.112.53
    set secondary 208.91.112.52
    # DNS FortiGuard avec filtrage intégré
end
```

**Valeur par défaut :** Aucun profil DNS Filter actif par défaut.

**Critère de conformité :** Profil DNS Filter avec blocage des catégories Botnet C&C (64), Malware (26), Phishing (61) appliqué à toutes les politiques couvrant le trafic interne vers Internet. `block-botnet enable`, `external-ip-blocklist enable`. Journalisation de toutes les requêtes DNS activée.

---

## Contrôle 5.4 — Web Filter — blocage des catégories à risque

> ***CIS Ref :*** *4.4.1* | ***MITRE :*** *T1566, T1204* | ***Niveau :*** 🟡 *MOYEN*

### Description du risque

Le filtrage web par catégories FortiGuard permet de bloquer l'accès aux sites malveillants, de phishing, aux proxies anonymes et aux contenus non autorisés. Sans filtrage web actif, les utilisateurs peuvent visiter des sites distribuant des malwares ou des pages de phishing ciblant les credentials d'entreprise.

### Impact potentiel

- Téléchargement involontaire de malwares depuis des sites compromis
- Phishing des credentials d'entreprise depuis des sites imitateurs
- Utilisation de proxies anonymes pour contourner les politiques de sécurité

### Navigation

```
Security Profiles > Web Filter
→ Create New
→ "FortiGuard Category Based Filter" : activer
→ Catégories Malicious Websites, Phishing, Proxy Avoidance : Block
→ Catégories Hacking, Spyware : Block
→ "URL Filter" : ajouter des listes noires spécifiques si nécessaire
→ "Search Engines" : SafeSearch activer (optionnel)
→ OK
```

### CLI de vérification

```
show webfilter profile
```

### Remédiation

```
config webfilter profile
    edit "wf-entreprise"
        set comment "Filtrage web entreprise"
        config ftgd-wf
            config filters
                edit 1
                    set category 62
                    set action block
                next
                edit 2
                    set category 26
                    set action block
                next
                edit 3
                    set category 61
                    set action block
                next
            end
        end
        set log-all-url enable
        set web-filter-activex-log enable
        set web-filter-command-block-log enable
    next
end
```

**Valeur par défaut :** Aucun profil Web Filter actif. FortiGuard Web Filtering nécessite une licence.

**Critère de conformité :** Profil Web Filter actif avec blocage des catégories à risque. Journalisation des URL activée. Profil appliqué aux politiques d'accès Internet des utilisateurs.

---

## Contrôle 5.5 — Application Control — bloquer P2P et proxies anonymes

***CIS Ref :*** *4.5.1 à 4.5.4* | ***MITRE :*** *T1090, T1048* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

Les applications P2P (BitTorrent, eMule), les proxies anonymes (Tor Browser, Ultrasurf, Psiphon) et les applications à haut risque peuvent être utilisées pour exfiltrer des données, contourner les politiques de sécurité ou accéder à des ressources non autorisées. L'Application Control identifie ces applications indépendamment du port et du protocole utilisé.

**Impact potentiel**

- Exfiltration de données via applications P2P ou tunnels chiffrés
- Contournement des politiques de filtrage web et réseau via proxies anonymes
- Utilisation de ressources réseau pour des activités non autorisées (torrents, streaming)

**Navigation**

```
Security Profiles > Application Control
→ Create New
→ Catégories "P2P" : Block
→ Catégories "Proxy" : Block
→ Applications à risque élevé : Block
→ "Log all application traffic" : activer
→ OK
```

**CLI de vérification**

```
show application list
```

**Remédiation**

```
config application list
    edit "appctrl-strict"
        set comment "Contrôle applicatif strict"
        set unknown-application-action pass
        config entries
            edit 1
                set category 11
                set action block
                set log enable
            next
            edit 2
                set category 23
                set action block
                set log enable
            next
        end
    next
end
```

**Valeur par défaut :** Aucun profil Application Control actif par défaut.

**Critère de conformité :** Profil Application Control avec blocage des catégories P2P et Proxy appliqué aux politiques Internet. Journalisation de tout le trafic applicatif activée.

---

## Contrôle 5.6 — Data Loss Prevention (DLP)

***CIS Ref :*** *(best practice étendue)* | ***MITRE :*** *T1048, T1041* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Sans profil DLP, des données sensibles (numéros de carte bancaire, numéros de sécurité sociale, données médicales, propriété intellectuelle) peuvent être exfiltrées via des canaux web, email ou FTP sans détection. Le DLP FortiGate inspecte le contenu des flux pour détecter des patterns de données sensibles définis par des expressions régulières ou des archives de fingerprints.

**Impact potentiel**

- Exfiltration de données confidentielles en dehors du périmètre contrôlé
- Violation réglementaire (RGPD, PCI-DSS, HIPAA) par divulgation non contrôlée
- Compromission de la propriété intellectuelle de l'organisation

**Navigation**

```
Security Profiles > Data Loss Prevention
→ DLP Sensor > Create New
→ Ajouter des filtres : Credit Card Number, Social Security Number (si applicable)
→ Action : Block ou Quarantine (selon politique)
→ Log : activer
→ OK
→ Appliquer aux politiques concernées
```

**CLI de vérification**

```
show dlp sensor
```

**Remédiation**

```
config dlp sensor
    edit "dlp-financier"
        set comment "DLP données financières"
        config filter
            edit 1
                set name "cartes-bancaires"
                set type credit-card
                set action block
                set log enable
            next
        end
    next
end
```

**Valeur par défaut :** Aucun profil DLP actif par défaut.

**Critère de conformité :** Profil DLP défini et appliqué aux flux sortants HTTP/HTTPS/SMTP pour les utilisateurs manipulant des données sensibles. Revue trimestrielle des alertes DLP.

---

## Contrôle 5.7 — ANSSI : Double-barrière et isolation des zones critiques

***CIS Ref :*** *(ANSSI — Recommandations pare-feux)* | ***MITRE :*** *T1021, T1190* | ***Niveau :*** 🔵 *L2*

**Description du risque**

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) recommande explicitement dans son guide "Recommandations pour choisir des pare-feux maîtrisés" le principe de **double-barrière** : déployer au minimum deux équipements de filtrage en cascade, de constructeurs différents (diversification technologique), pour les zones hébergeant des systèmes critiques. Cette architecture empêche qu'une vulnérabilité affectant un constructeur unique compromette simultanément toutes les barrières de filtrage.

**Principe ANSSI fondamental :** "Tout ce qui n'est pas explicitement autorisé est interdit" — implémentation stricte du default-deny sur toutes les zones.

**Recommandations ANSSI complémentaires :** - Équipements de filtrage **dédiés** à la fonction sécurité réseau (pas de multifonction avec téléphonie, etc.) - Réseau de gestion **dédié et physiquement séparé** du réseau de production - Pas d'accès management depuis les réseaux de production ou Internet - Sécurité physique : baie verrouillée, contrôle d'accès documenté - **TLS 1.3 ou TLS 1.2 avec suites ECDHE exclusivement** (équivalent mode paranoïaque FortiGate)

**Impact potentiel**

- Compromission totale de la segmentation réseau si une seule barrière de filtrage est contournée
- Attaques supply chain sur le firmware d'un constructeur unique affectant toutes les barrières
- Mouvement latéral sans obstacles vers les systèmes critiques

**Navigation**

```
(Architecture et politique — configuration externe au FortiGate)
→ Vérifier la présence d'un second pare-feu en cascade devant ou derrière le FortiGate
→ Network > Interfaces > Vérifier l'existence d'une interface MGMT dédiée
→ Policy & Objects > Firewall Policy > Vérifier la politique implicit deny en fin de liste
```

**CLI de vérification**

```
# Vérifier l'interface de gestion dédiée
show system interface | grep -A 5 mgmt

# Vérifier la politique implicite (default deny)
config system settings
    get | grep implicit
# Valeur attendue : implicit-allow disable (default deny)

# Vérifier les suites TLS ECDHE pour le management
config system global
    get | grep -e ssl-static -e strong-crypto

# Vérifier que l'admin est accessible uniquement depuis l'interface MGMT
show system interface wan1 | grep allowaccess
```

**Remédiation**

```
# 1. Activer le default-deny implicite (refus par défaut)
config system settings
    set implicit-allow-dns disable
end

# 2. Forcer les suites ECDHE uniquement (recommandation ANSSI TLS strict)
config system global
    set ssl-static-key-ciphers disable
    set strong-crypto enable
    set dh-params 8192
    set admin-https-ssl-versions tlsv1-2 tlsv1-3
end

# 3. Dédier une interface de gestion séparée
config system interface
    edit "mgmt"
        set allowaccess https ssh
        set dedicated-to management
    next
end

# 4. Supprimer tout accès management des interfaces WAN et production
config system interface
    edit "wan1"
        set allowaccess none
    next
    edit "internal"
        set allowaccess none
    next
end
```

> ***Architecture double-barrière recommandée ANSSI :*** *Internet → [Pare-feu 1 (constructeur A)] → DMZ filtrage → [Pare-feu 2 FortiGate] → LAN critique. Le pare-feu frontal peut être d'un autre constructeur (ex: OPNsense, pfSense, ou équipement opérateur). Cette diversification garantit qu'une CVE critique sur un constructeur n'expose pas directement le LAN.*

**Valeur par défaut :** Interface MGMT disponible mais non forcément dédiée. Politique implicite configurable.

**Critère de conformité :** Interface MGMT physiquement dédiée et séparée du réseau de production. Politique implicite default-deny sur toutes les zones. TLS 1.2+ avec ECDHE exclusivement ( `ssl-static-key-ciphers disable` ). Architecture double-barrière documentée pour les zones critiques. Référence : ANSSI — Recommandations pour choisir des pare-feux maîtrisés.

---

# Domaine 6 — Security Fabric et FortiGuard

***Objectif :*** *Activer et configurer le Security Fabric Fortinet pour une visibilité centralisée, une réponse coordonnée et une évaluation continue de la posture de sécurité via le Security Rating. Sécuriser les relations de confiance du Security Fabric pour prévenir les escalades de privilèges documentées.*

---

## Contrôle 6.1 — Activer et configurer le Security Fabric avec upstream sécurisé

***CIS Ref :*** *5.2.1* | ***MITRE :*** *T1562, T1548* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

Sans Security Fabric activé et configuré, le FortiGate opère en isolation sans visibilité sur l'ensemble des équipements Fortinet du réseau. Le Security Fabric permet la corrélation d'événements entre FortiGate, FortiSwitch, FortiAP, FortiClient et FortiAnalyzer.

**Risque d'escalade de privilèges via Security Fabric (Fortinet Advisory 2025) :** Un administrateur authentifié disposant de la permission Security Fabric peut escalader ses privilèges vers super-admin en connectant le FortiGate à un FortiGate upstream malveillant ou contrôlé par un attaquant. Ce vecteur a été documenté dans plusieurs incidents réels. L'IP upstream doit être strictement restreinte aux FortiGate légitimes.

**Impact potentiel**

- Absence de visibilité sur les compromissions traversant plusieurs équipements réseau
- Impossibilité de quarantaine automatique des hôtes compromis
- Délai de détection accru sans corrélation centralisée des événements
- **Escalade de privilèges** : admin Security Fabric → super-admin via FortiGate upstream malveillant

**Navigation**

```
Security Fabric > Fabric Connectors > Security Fabric Setup
→ "Enable Security Fabric" : activer
→ "Role" : Root FortiGate (ou Downstream selon la topologie)
→ "FortiAnalyzer Logging" : configurer avec l'IP de FortiAnalyzer
→ "Upstream FortiGate IP" : configurer uniquement l'IP du FortiGate root légitime
→ Apply
```

**CLI de vérification**

```
show system csf
```

Vérifier : `set status enable`, `set upstream-ip` configuré sur l'IP du FortiGate root légitime (pas `0.0.0.0`), `set fabric-object-unification default`.

**Remédiation**

```
config system csf
    set status enable
    set upstream-ip <IP_FortiGate_Root_Légitime>
    set group-name "fabric-principal"
    set group-password <mot_de_passe_fabric>
    set forticloud-account-enforcement enable
    set fabric-object-unification default
end
```

> ***Restriction upstream critique :*** *Ne jamais laisser* `upstream-ip 0.0.0.0` *sur un FortiGate downstream en production. Cette valeur autoriserait la connexion à n'importe quel FortiGate upstream, permettant une escalade de privilèges. Configurer l'IP exacte du FortiGate root légitime.*

**FortiAnalyzer — vérification d'autorisation Fabric :**

```
# Sur FortiAnalyzer, activer la vérification du certificat d'autorisation Fabric
config system csf
    set authorization-request-type certificate
    set certificate <certificat_fabric>
end
```

**Valeur par défaut :** Security Fabric désactivé par défaut. `upstream-ip : 0.0.0.0` si non configuré.

**Critère de conformité :** Security Fabric activé et tous les FortiGate du réseau connectés. `upstream-ip` configuré sur l'IP exacte du FortiGate root légitime (pas 0.0.0.0). FortiAnalyzer avec vérification de certificat Fabric activée.

---

## Contrôle 6.2 — Quarantaine automatique des hôtes compromis

> ***CIS Ref :*** *5.1.1* | ***MITRE :*** *T1562, T1078* | ***Niveau :*** 🔵 *L2*

**Description du risque**

La quarantaine automatique via le Security Fabric (Compromised Host Quarantine) permet d'isoler en temps réel les hôtes détectés comme compromis (via IOC FortiGuard, IPS, Antivirus ou FortiEDR) sans intervention manuelle. Sans cette fonctionnalité, un hôte compromis continue de communiquer avec des serveurs C2 et de se propager latéralement pendant la durée de l'investigation.

**Impact potentiel**

- Propagation continue d'un malware depuis un hôte compromis non isolé
- Exfiltration continue de données pendant la durée de l'investigation manuelle
- Mouvement latéral vers d'autres systèmes pendant la fenêtre de réponse

**Navigation**

```
Security Fabric > Automation > Create New
→ Trigger : "Compromised Host" (FortiGuard IOC)
→ Action : "Quarantine Device" (via FortiSwitch ou FortiNAC)
→ Enable
→ Apply
```

**CLI de vérification**

```
show system automation-action
show system automation-trigger
```

**Remédiation**

```
config system automation-trigger
    edit "compromised-host-trigger"
        set event-type ioc
    next
end

config system automation-action
    edit "quarantine-action"
        set action-type quarantine-forticlient
    next
end

config system automation-stitch
    edit "quarantine-compromised"
        set trigger "compromised-host-trigger"
        set action "quarantine-action"
        set status enable
    next
end
```

**Valeur par défaut :** Aucune automatisation de quarantaine configurée par défaut.

**Critère de conformité :** Au moins une automation stitch configurée pour isoler automatiquement les hôtes détectés comme compromis par FortiGuard IOC ou IPS.

---

## Contrôle 6.3 — Security Rating et CSPM activés

***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1562* | ***Niveau :*** ⚪ *INFO*

**Description du risque**

Le **Security Rating** (CSPM — Cloud Security Posture Management) de FortiGate évalue en continu la configuration de l'équipement et de tout le Security Fabric contre les best practices Fortinet, les contrôles CIS et les recommandations réglementaires. Sans évaluation continue, les dérives de configuration (admin sans MFA ajouté post-durcissement, règle permissive ajoutée en urgence, etc.) peuvent introduire des vulnérabilités non détectées pendant des mois.

**FortiOS 7.4 — Fonctionnalités Security Rating clés :** - **Tableau de bord de conformité** : score 0-100 avec comparaison aux pairs du secteur (peer comparison) - **4 catégories d'évaluation** : Audit, Configuration, Coverage (couverture des profils), Optimization - **Contrôles critiques automatisés** : détection des comptes admin sans 2FA, interfaces ouvertes, politiques SSL faibles, versions TLS obsolètes - **Rapport planifié** : génération automatique de rapports PDF/CSV pour les audits de conformité - **Peer comparison** : comparer son score à la médiane des organisations du même secteur d'activité - **CSPM CLI** : `diagnose system csf check` pour vérification en ligne de commande

**Contrôles critiques vérifiés automatiquement (checks les plus importants) :**

| CONTRÔLE SECURITY RATING | CATÉGORIE | CRITICITÉ | IMPACT SI ÉCHOUÉ |
|---|---|---|---|
| Comptes admin sans MFA (2FA) | Audit | **Critique** | Accès admin sans second facteur — T1078 |
| Interfaces management exposées sur Internet | Audit | **Critique** | Attack surface WAN directe |
| Pas de profil IPS sur les politiques | Coverage | **Élevé** | Exploits réseau non bloqués |
| Configuration TLS SSL-VPN faible | Configuration | **Élevé** | Downgrade TLS possible — T1557 |
| Logs désactivés ou non transmis | Audit | **Élevé** | Visibilité nulle — T1562.006 |
| Règles firewall sans logging | Audit | **Moyen** | Investigation forensique impossible |
| Mises à jour FortiGuard > 24h | Coverage | **Élevé** | Signatures IPS/AV obsolètes |
| Compte admin "admin" par défaut présent | Audit | **Critique** | Compte universel connu des attaquants |
| Trusted Hosts non configurés | Audit | **Élevé** | Accès admin depuis toute IP |
| Security Fabric non activé | Configuration | **Moyen** | Pas de visibilité centralisée |

### Impact potentiel

- Dérive de configuration non détectée introduisant des vulnérabilités
- Absence de référentiel objectif pour évaluer la posture de sécurité
- Conformité difficile à mesurer sans outil automatisé
- Score bas = indicateur d'exposition accrue documenté par Fortinet

### Navigation

```
Security Fabric > Security Rating
→ "Run Now" pour une évaluation immédiate
→ Onglet "Security Posture" : score global et détail par catégorie
→ Onglet "Audit" : contrôles d'audit de compte et d'accès
→ Onglet "Configuration" : contrôles de configuration protocoles et chiffrement
→ Onglet "Coverage" : profils de sécurité appliqués aux politiques
→ Onglet "Optimization" : politiques inutilisées, règles redondantes
→ Cliquer sur chaque défaillance pour accéder au guide de remédiation intégré
→ "Schedule" : configurer une évaluation automatique quotidienne
→ "Peer Comparison" : comparer son score à la médiane du secteur
→ "Report" : générer un rapport PDF/CSV pour les audits de conformité
```

**CLI de vérification**

```
# Résumé du Security Rating
diagnose security-rating summary

# Vérification CSPM complète (Security Fabric Check)
diagnose system csf check

# Lister tous les contrôles échoués
diagnose security-rating result | grep FAIL

# Lister les contrôles échoués par catégorie
diagnose security-rating result | grep -e FAIL -e WARN

# Vérifier la dernière date d'évaluation
diagnose security-rating status

# Afficher le score détaillé par catégorie
diagnose security-rating result
```

**Remédiation**

1. Activer et planifier le Security Rating en évaluation quotidienne automatique : `config system security-rating` → `set status enable` → `set schedule daily` → `set time 02:00` → `end`
2. Forcer une évaluation immédiate pour obtenir un état initial : `execute security-rating run`, puis consulter avec `diagnose security-rating summary` et `diagnose security-rating result | grep FAIL`
3. Corriger en priorité toutes les défaillances catégorisées “Critical” (comptes admin sans MFA, interfaces management exposées WAN, compte “admin” par défaut présent) avant d’adresser les défaillances “High”
4. Exporter un rapport PDF/CSV de base depuis Security Fabric > Security Rating > Report pour archivage et référence d’audit initial (ISO 27001, PCI-DSS)
5. Mettre en place un suivi hebdomadaire : alerter si le score diminue de plus de 5 points entre deux évaluations consécutives ; viser un score cible ≥ 80/100
6. Si FortiManager est déployé, centraliser les scores de tous les FortiGate du parc depuis FortiManager > Security Fabric > Security Rating pour une vue agrégée de la posture

**Valeur par défaut :** Security Rating disponible mais non planifié automatiquement. La commande `diagnose system csf check` est disponible sans configuration préalable.

**Critère de conformité :** Score Security Rating ≥ 80/100. Toutes les défaillances “Critical” et “High” corrigées. Évaluation planifiée quotidiennement ( `config system security-rating` ). Rapport PDF/CSV exporté et archivé mensuellement pour les audits. `diagnose system csf check` sans erreur critique. Peer comparison documenté dans le rapport de sécurité annuel.

---

## Contrôle 6.4 — Tests de pénétration et évaluation sécurité périodique

***CIS Ref :*** *(best practice communauté Fortinet)* | ***MITRE :*** *T1190* | ***Niveau :*** 🔵 *L2*

**Description du risque**

La communauté Fortinet et les référentiels de sécurité recommandent des tests de pénétration annuels (ou après chaque changement majeur) sur les équipements FortiGate exposés. Ces tests permettent de valider l’efficacité des contrôles de sécurité configurés et de détecter des dérives ou des vulnérabilités non couvertes par les configurations de durcissement standard.

**Impact potentiel**

- Contrôles de sécurité configurés mais non testés dans un contexte d’attaque réel
- Vulnérabilités de configuration non détectées par les audits de configuration statiques
- Non-conformité avec PCI-DSS Req 11.4 (penetration testing)

**Navigation**

```
(Processus externe — non configurable via l'interface FortiGate)
```

**Remédiation**

Processus recommandé : 1. Planifier un test de pénétration annuel par un prestataire qualifié (PASSI en France) 2. Inclure dans le scope : interfaces de management, SSL-VPN, politiques de sécurité 3. Tester les CVE récentes non encore patchées en environnement de pré-prod 4. Valider les contrôles compensatoires (virtual patching, Local-in Policies) 5. Documenter les résultats et les plans de remédiation

**Valeur par défaut :** Aucun processus de test automatisé intégré à FortiGate.

**Critère de conformité :** Test de pénétration réalisé au minimum une fois par an et après tout changement majeur d’infrastructure. Résultats documentés et plans de remédiation suivis.

---

## Contrôle 6.5 — Flux de threat intelligence externes (STIX/TAXII, FortiGuard IOC, ETF)

***CIS Ref :*** *(best practice FortiOS 7.4)* | ***MITRE :*** *T1071, T1566, T1090* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Les flux de threat intelligence externe (External Threat Feeds — ETF) permettent d'enrichir la protection du FortiGate avec des indicateurs de compromission (IOC) provenant de sources tierces : listes d'IP malveillantes, domaines C2, URLs de phishing. Intégrés via les connecteurs Security Fabric, ces flux sont automatiquement utilisés dans les politiques de filtrage et les profils de sécurité. Le standard **STIX/TAXII** (Structured Threat Information Expression / Trusted Automated eXchange of Indicator Information) est le protocole de référence pour l'échange automatisé de threat intelligence inter-organisations.

**FortiGuard IOC Service :** FortiGuard propose nativement un service de Threat Intelligence avec des IOC mis à jour en continu. Les **External Connectors** (Security Fabric > External Connectors) permettent d'ajouter des sources supplémentaires pour couvrir des secteurs spécifiques (finance, santé, industrie) non couverts par FortiGuard seul.

**Types de threat feeds supportés par FortiOS 7.4 :**

| TYPE | DESCRIPTION | UTILISATION DANS FORTIGATE |
|---|---|---|
| `ip` | Liste d'adresses IP malveillantes | Blocage dans les politiques firewall |
| `domain` | Domaines C2 et phishing | DNS Filter + blocage politique |
| `url` | URLs malveillantes complètes | Web Filter + URL blocklist |
| `malware-hash` | Empreintes de fichiers malveillants | Antivirus (file hash blacklist) |

**Impact potentiel**

- Communications C2 vers des IP non référencées dans FortiGuard mais connues d'autres CTI (T1071)
- Phishing via des domaines récents non encore indexés par FortiGuard (T1566)
- Accès à des proxies anonymes non couverts par les bases FortiGuard standard (T1090)
- Absence de protection secteur-spécifique sans flux de threat intelligence dédiés

**Navigation**

```
Security Fabric > External Connectors
→ Create New
→ Type : "Threat Feeds" (IP Address, Domain Name, URL, ou Malware Hash)
→ Nom : identifier le flux (ex: "CTI-IP-Malveillantes")
→ URI de la ressource : URL du flux (texte brut, une entrée par ligne)
→ Refresh rate : 60 minutes (recommandé)
→ Certificate verification : activer si flux HTTPS
→ OK

Security Profiles > Web Filter (ou DNS Filter)
→ Ajouter le flux de threat intelligence comme source de blocage
```

**CLI de vérification**

```
# Lister les ressources externes configurées
show system external-resource

# Vérifier le statut de mise à jour des flux
diagnose external-resource refresh status

# Tester l'accès au flux
diagnose test application urlfilter 2
```

**Remédiation**

```
# Configurer un flux de threat intelligence IP (liste d'IP malveillantes)
config system external-resource
    edit "threat-feed-ip-malveillants"
        set type ip
        set resource "https://threat-feed.example.com/blocklist-ip.txt"
        set refresh-rate 60
        set status enable
        set username "<user_si_auth_requise>"
        set password "<password_si_auth_requise>"
    next
    edit "threat-feed-domaines-c2"
        set type domain
        set resource "https://threat-feed.example.com/c2-domains.txt"
        set refresh-rate 60
        set status enable
    next
    edit "threat-feed-urls-phishing"
        set type url
        set resource "https://threat-feed.example.com/phishing-urls.txt"
        set refresh-rate 60
        set status enable
    next
end
```

**Utilisation des flux dans les politiques de sécurité :**

```
# Utiliser un flux IP dans une politique firewall (blocage)
config firewall policy
    edit <id_policy_blocage_threat>
        set name "BLOCK-Threat-Intelligence-IPs"
        set srcintf "LAN"
        set dstintf "WAN"
        set srcaddr "all"
        set dstaddr "<nom_du_flux_ip_externe>"
        set action deny
        set schedule "always"
        set logtraffic all
        set comments "Blocage IPs threat intelligence externe"
    next
end

# Utiliser un flux de domaines dans DNS Filter
config dnsfilter profile
    edit "dns-strict-fortigate"
        set external-ip-blocklist enable
        # Le flux de domaines externe est automatiquement intégré
    next
end
```

**Sources de threat intelligence recommandées :**

| SOURCE | TYPE | URL / DESCRIPTION |
|---|---|---|
| FortiGuard IOC | IP/Domain/URL | Intégré nativement — Security Fabric > FortiGuard |
| Emerging Threats | IP/Rules | `https://rules.emergingthreats.net/blockrules/` |
| MISP (interne) | STIX/TAXII | Plateforme threat intel open-source |
| CERT nationaux | Divers | CERT-FR, CERT-EU — partage sectoriel |
| CIRCL.lu | STIX/TAXII | `https://www.circl.lu/services/misp-malware-ioc/` |

**Intégration STIX/TAXII (FortiSIEM / FortiAnalyzer ↔ MISP) :**

```
FortiAnalyzer → [STIX/TAXII API] → MISP / ISACs → enrichissement IOC → FortiGate External Connectors
```

> ***MITRE T1071 (Application Layer Protocol) :*** *Les flux de threat intelligence permettent de détecter les communications C2 qui utilisent des protocoles applicatifs légitimes (HTTP/HTTPS) pour se camoufler. En intégrant des listes C2 à jour dans les External Connectors, le FortiGate peut bloquer ces communications même quand les domaines/IPs sont très récents.*

**Valeur par défaut :** Aucun External Connector de threat intelligence configuré par défaut. FortiGuard IOC est disponible mais nécessite une licence FortiGuard Threat Intelligence Service.

**Critère de conformité :** Au moins un flux de threat intelligence externe (IP et/ou domaine) configuré via External Connectors avec refresh ≤ 60 minutes. Flux FortiGuard IOC activé (licence). Flux appliqués dans les politiques de blocage firewall et DNS Filter. Revue mensuelle des flux actifs et de leur taux de correspondance.

---

# Domaine 7 — VPN (IPsec, SSL-VPN et ZTNA)

> ***Objectif :*** *Sécuriser les accès distants via SSL-VPN et IPsec en imposant des protocoles forts, le MFA et en éliminant les configurations héritées vulnérables. Le SSL-VPN FortiGate a été la cible principale de plusieurs vulnérabilités critiques exploitées massivement en 2023-2026 (CVE-2023-27997, CVE-2024-21762, pattern d'attaque documenté par CISA et PSIRT Fortinet).*

---

## Contrôle 7.1 — SSL-VPN : TLS 1.2 minimum, désactiver SSLv3/TLS 1.0

> ***CIS Ref :*** *6.1.2* | ***MITRE :*** *T1133, T1557* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Le SSL-VPN FortiGate avec SSLv3 ou TLS 1.0 activés est vulnérable aux attaques POODLE et BEAST permettant le déchiffrement des sessions VPN. Ces protocoles obsolètes doivent être désactivés.

**CVE critiques ciblant le SSL-VPN FortiGate :**

| CVE | CVSS | DESCRIPTION | ACTION |
|---|---|---|---|
| **CVE-2023-27997** | 9.8 | Heap overflow dans le daemon SSL-VPN — RCE pré-authentification | Patch immédiat |
| **CVE-2024-21762** | 9.6 | Out-of-bounds write dans SSL-VPN — RCE pré-authentification — CISA KEV | Patch immédiat |

Ces CVE ont été exploitées massivement par des acteurs étatiques et des groupes de ransomware. Limiter les versions TLS réduit la surface d'attaque cryptographique, mais le patch firmware reste la remédiation principale.

**Impact potentiel**

- Déchiffrement de sessions VPN via attaques de downgrade sur TLS 1.0
- RCE pré-authentification via CVE-2023-27997 et CVE-2024-21762 (sans credentials requis)
- Compromission des credentials utilisateurs transitant par le VPN
- Installation de backdoors persistantes après exploitation initiale

**Navigation**

```
VPN > SSL-VPN Settings
→ Section "Tunnel Mode Client Settings"
→ "Cipher Suites" : désélectionner les suites faibles
→ "SSL/TLS Version" : TLS 1.2 minimum
→ Apply
```

**CLI de vérification**

```
show vpn ssl settings | grep tlsv
```

Vérifier la présence de `tlsv1-2` ou `tlsv1-3` et l'absence de `sslv3`, `tlsv1-0`, `tlsv1-1`.

**Remédiation**

```
config vpn ssl settings
    set tlsv1-0 disable
    set tlsv1-1 disable
    set tlsv1-2 enable
    set tlsv1-3 enable
    set algorithm high
    set banned-cipher RC4 3DES MD5
end
```

> ***Recommandation post-CVE-2024-21762 :*** *Si l'équipement était exposé avec une version vulnérable, réaliser un audit complet des comptes d'accès SSL-VPN et vérifier les symlinks dans les répertoires SSL-VPN (technique de persistance documentée par CISA Avril 2025 — voir section Réponse à Incident).*

**Valeur par défaut :** TLS 1.2 et 1.3 activés par défaut sur FortiOS 7.4. TLS 1.0 et 1.1 désactivés par défaut. Vérifier sur les équipements migrés depuis une version antérieure.

**Critère de conformité :** `tlsv1-0 : disable`, `tlsv1-1 : disable`, `sslv3 : disable`. `tlsv1-2 : enable` minimum. `algorithm : high` ou `strong`. Version FortiOS non affectée par CVE-2023-27997 et CVE-2024-21762.

---

## Contrôle 7.2 — IPsec : IKEv2 uniquement, pas de mode agressif

> ***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1133, T1040* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

IKEv1 en mode agressif est vulnérable à la divulgation du hash de la PSK (Preshared Key) qui peut être cracké hors ligne. IKEv1 présente de nombreuses vulnérabilités de sécurité par rapport à IKEv2. IKEv2 intègre nativement la protection contre les attaques par dictionnaire, le support de l'EAP pour l'authentification et une meilleure gestion des renouvellements de clés.

**Impact potentiel**

- Récupération de la PSK IPsec par capture du handshake IKEv1 en mode agressif
- Compromission de tous les tunnels IPsec utilisant la PSK divulguée
- Attaques man-in-the-middle sur les négociations IKEv1 (T1557)

**Navigation**

```
VPN > IPsec Wizard (ou éditer un tunnel existant)
→ Phase 1 : "IKE Version" : 2
→ Mode : Main (désactiver Aggressive)
→ Encryption : AES256GCM ou AES256
→ Authentication : SHA256 minimum (SHA384 recommandé)
→ DH Group : 14, 19, 20 ou 21
→ Perfect Forward Secrecy : activer
→ OK
```

**CLI de vérification**

```
show vpn ipsec phase1-interface
```

Vérifier : `set ike-version 2`, absence de `set aggressive-mode enable`.

**Remédiation**

```
config vpn ipsec phase1-interface
    edit "vpn-site-a"
        set ike-version 2
        set proposal aes256gcm-prfsha256 aes256-sha256
        set dhgrp 14 19 20
        set peertype any
    next
end

config vpn ipsec phase2-interface
    edit "vpn-site-a-p2"
        set phase1name "vpn-site-a"
        set proposal aes256gcm aes256-sha256
        set dhgrp 14 19 20
        set pfs enable
        set keylifeseconds 3600
    next
end
```

**Authentification OSPF MD5 pour le routage sur tunnels IPsec :**

```
# Si OSPF est utilisé sur les interfaces IPsec, activer l'authentification MD5
config router ospf
    config ospf-interface
        edit "intf-vpn"
            set authentication md5
            set md5-keys 1 <clé_md5_forte>
        next
    end
end
```

**Valeur par défaut :** IKEv1 utilisé par défaut dans les anciens tunnels. IKEv2 disponible et recommandé.

**Critère de conformité :** Tous les tunnels IPsec utilisent IKEv2. Aucun tunnel en mode agressif IKEv1. PFS activé sur toutes les phase 2. Algorithmes : AES256+ et SHA256+. OSPF avec authentification MD5 si utilisé sur tunnels.

## Contrôle 7.3 — Certificat signé pour le portail SSL-VPN

***CIS Ref :*** *6.1.1* | ***MITRE :*** *T1557, T1133* | ***Niveau :*** 🟢 *L1*

**Description du risque**

Le portail SSL-VPN avec un certificat auto-signé ou expiré peut être substitué par un portail de phishing indiscernable. Les utilisateurs VPN qui ont l'habitude d'ignorer les alertes de certificat sont des cibles privilégiées pour le credential harvesting. Un certificat signé par une CA de confiance garantit l'authenticité du portail VPN.

**Impact potentiel**

- Phishing des credentials VPN via faux portail SSL-VPN identique
- Attaque MITM interceptant les credentials et sessions VPN
- Compromission massive des comptes utilisateurs VPN

**Navigation**

```
VPN > SSL-VPN Settings
→ "Server Certificate" : sélectionner le certificat signé importé
→ (Le certificat doit être importé préalablement dans System > Certificates)
→ Apply
```

**CLI de vérification**

```
show vpn ssl settings | grep servercert
```

**Remédiation**

```
config vpn ssl settings
    set servercert "<nom_certificat_signe>"
end
```

**Valeur par défaut :** Certificat auto-signé Fortinet_Factory utilisé par défaut.

**Critère de conformité :** Certificat SSL-VPN signé par une CA reconnue (publique ou PKI d'entreprise). FQDN du certificat correspondant à l'URL du portail VPN. Date d'expiration > 30 jours.

## Contrôle 7.4 — MFA obligatoire pour les utilisateurs SSL-VPN

***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1133, T1078* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Le SSL-VPN sans MFA est vulnérable aux attaques par credential stuffing et au phishing des mots de passe. FortiGate supporte FortiToken (TOTP), SMS, email et intégration RADIUS/LDAP avec MFA pour les utilisateurs VPN. L'activation du MFA rend inopérantes les attaques par credential stuffing même en cas de compromission de bases de mots de passe.

**Impact potentiel**

- Accès VPN non autorisé via credentials volés par phishing ou credential stuffing
- Connexion persistante d'un attaquant au réseau interne via VPN compromis
- Escalade de privilèges depuis le réseau interne après connexion VPN non autorisée

**Navigation**

```
User & Authentication > User Definition
→ Éditer les utilisateurs VPN
→ "Two-factor Authentication" : Enable
→ Sélectionner FortiToken Mobile ou méthode Email
→ OK

VPN > SSL-VPN Portals
→ Éditer le portail
→ "User Group" : s'assurer que le groupe d'utilisateurs VPN a MFA activé
```

**CLI de vérification**

```
show user local
show user group
```

Vérifier la présence de `set two-factor fortitoken` ou `set two-factor email` sur les utilisateurs VPN.

**Remédiation**

```
config user local
    edit "utilisateur-vpn"
        set type password
        set two-factor fortitoken
        set fortitoken "<serial_token>"
        set email-to "<email@domaine.fr>"
    next
end
```

**Valeur par défaut :** MFA désactivé pour les utilisateurs VPN par défaut.

**Critère de conformité :** 100 % des utilisateurs ayant accès au SSL-VPN ont le MFA activé (FortiToken, RADIUS MFA, ou équivalent). Aucun accès VPN possible avec mot de passe seul.

---

### Contrôle 7.5 — Split tunneling restrictif pour SSL-VPN

***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1090, T1048* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Le split tunneling non restreint permet aux utilisateurs VPN de faire transiter simultanément du trafic via le VPN (vers les ressources internes) et directement vers Internet depuis leur poste. Un poste compromis connecté en VPN peut ainsi servir de pivot vers le réseau interne tout en ayant un accès Internet non contrôlé. La configuration recommandée utilise soit le full tunnel, soit un split tunnel avec liste blanche stricte des destinations autorisées.

**Impact potentiel**

- Pivot réseau depuis un poste compromis connecté en VPN vers le réseau interne
- Exfiltration de données internes via le trafic Internet non tunnelisé
- Contournement des contrôles de sécurité réseau pour le trafic Internet du poste distant

**Navigation**

```
VPN > SSL-VPN Portals
→ Éditer le portail
→ "Tunnel Mode" : activer
→ "Split Tunneling" : Disabled (Full Tunnel recommandé) ou "Enabled Based on Policy
Destination"
→ Si split tunnel nécessaire : "Routing Address" = IP/subnets autorisés uniquement
→ OK
```

**CLI de vérification**

```
show vpn ssl web portal
```

Vérifier : `set split-tunneling disable` (full tunnel) ou configuration de `split-tunneling-routing-address` avec liste restrictive.

**Remédiation**

Full tunnel (recommandé) :

```
config vpn ssl web portal
    edit "portal-vpn"
        set tunnel-mode enable
        set split-tunneling disable
    next
end
```

**Valeur par défaut :** Split tunneling désactivé sur les nouvelles installations (full tunnel par défaut).

**Critère de conformité :** Split tunneling désactivé (full tunnel) ou, si activé, liste blanche restrictive documentée limitant le trafic tunnelisé aux seules destinations internes nécessaires.

---

### Contrôle 7.6 — ZTNA (Zero Trust Network Access) — alternative supérieure au SSL-VPN

***CIS Ref :*** *(best practice FortiOS 7.4)* | ***MITRE :*** *T1133* | ***Niveau :*** 🔵 *L2*

**Description du risque**

FortiOS 7.4 introduit le **ZTNA (Zero Trust Network Access)** comme alternative plus sécurisée au SSL-VPN traditionnel. Contrairement au SSL-VPN qui accorde un accès large au réseau une fois authentifié, le ZTNA applique le **principe du moindre privilège à chaque application** : l'accès est accordé uniquement après vérification simultanée de l'identité, de l'état de santé du terminal et du contexte de connexion.

**MITRE T1133 (External Remote Services) :** Le ZTNA fournit un contrôle supérieur au SSL-VPN contre les abus d'accès distant — chaque accès applicatif est vérifié indépendamment, une compromission de credentials ne donne pas accès à l'ensemble du réseau.

**Comparaison SSL-VPN vs ZTNA FortiOS 7.4 :**

| CRITÈRE | SSL-VPN | ZTNA FORTIGATE |
|---|---|---|
| Accès réseau | Large (tunnel IP) | Applicatif uniquement |
| Vérification terminal | Limitée | FortiClient EMS posture check |
| Granularité | Par groupe/portail | Par application et par règle |
| Exposition réseau | Élevée (IP routable) | Nulle (proxy applicatif) |
| Protocoles supportés | IP/TCP générique | HTTP, SSH, RDP, SMB, FTP, TCP |
| Migration guide | — | FortiOS 7.4 SSL-VPN → ZTNA |

**Prérequis ZTNA FortiOS 7.4 :** - FortiClient EMS v7.0+ ou FortiClient EMS Cloud (gestion des postures) - FortiClient v7.0+ sur les terminaux (agent léger obligatoire) - Certificats TLS pour le ZTNA Application Gateway

**Impact potentiel si ZTNA non déployé (SSL-VPN seul) :**

- Compromission d'un credential SSL-VPN = accès réseau complet (T1133)
- Absence de vérification de la posture du terminal (antivirus à jour ? chiffrement disque ?)
- Mouvement latéral facilité depuis un poste compromis connecté en VPN

**Navigation**

```
VPN > ZTNA > ZTNA Rules
→ Create New (règle d'accès par application)
→ ZTNA Server : sélectionner le serveur ZTNA configuré
→ Source : groupe utilisateurs / tags de posture FortiEMS
→ Destination : application cible (URL, IP:port)
→ Action : Accept (avec vérification posture)
→ OK

User & Authentication > ZTNA > ZTNA Servers
→ Create New
→ Type : HTTPS Proxy ou TCP Forwarding
→ Server IP : IP du serveur applicatif interne
→ Server Port : port applicatif
→ Certificate : certificat TLS du serveur ZTNA
→ OK
```

**CLI de vérification**

```
# Vérifier la configuration du ZTNA Traffic Forward Proxy
show firewall ztna-traffic-forward-proxy

# Vérifier les serveurs ZTNA configurés
show firewall ztna-server

# Vérifier les règles ZTNA
show firewall policy | grep ztna

# Vérifier la connexion FortiClient EMS
show endpoint-control server
diagnose endpoint-control client-status list
```

**Remédiation**

1. Déployer FortiClient EMS v7.0+ et enrôler les terminaux ; sur FortiGate, connecter l'EMS via Security Fabric > Fabric Connectors > FortiClient EMS et vérifier avec `diagnose endpoint-control server status`
2. Créer le serveur ZTNA Application Gateway : `config firewall ztna-server` → `edit "ztna-webapp"` → `set type http` → `set vip "<IP_publique>"` → `set ssl-min-proto-version TLSv1-2` → `set ssl-certificate "<cert_ztna>"` → configurer `realservers` avec l'IP et le port du serveur interne → `end`
3. Créer les règles ZTNA applicatives avec vérification de posture : `config firewall ztna-traffic-forward-proxy` → conditionner l'accès avec `set ztna-ems-tag "FortiClient-Compliant"` → `set logtraffic all` → `end`
4. Inventorier les groupes d'accès SSL-VPN existants (`show vpn ssl web portal`), créer une règle ZTNA équivalente par application SSL-VPN, puis basculer les utilisateurs pilotes vers ZTNA par groupes
5. Après validation complète de la migration, désactiver le SSL-VPN : `config vpn ssl settings` → `set status disable` → `end`
6. Vérifier le bon fonctionnement avec `show firewall ztna-server`, `diagnose endpoint-control client-status list` et s'assurer que `set logtraffic all` est actif sur toutes les règles ZTNA

**Valeur par défaut :** ZTNA non configuré par défaut. SSL-VPN reste la solution VPN par défaut sur les nouvelles installations FortiOS 7.4.

**Critère de conformité :** Pour les nouveaux déploiements : ZTNA préféré au SSL-VPN. Pour les migrations : plan de migration SSL-VPN → ZTNA documenté avec délai. Tags de posture FortiEMS configurés et appliqués. Accès ZTNA limité aux seuls terminaux conformes (`ztna-ems-tag` configuré sur toutes les règles). Journalisation activée sur toutes les règles ZTNA.

---

## Contrôle 7.7 — Conformité endpoint via FortiClient EMS (Zero Trust posture check)

***CIS Ref :*** *(best practice FortiOS 7.4 + ZTNA)* | ***MITRE :*** *T1078* | ***Niveau :*** 🔵 *L2*

### Description du risque

Un accès réseau accordé à un utilisateur avec des credentials valides ne garantit pas que le terminal utilisé est sûr. Un poste non patché, sans antivirus à jour, sans chiffrement de disque ou exécutant des logiciels interdits représente un vecteur d'intrusion même si les credentials sont légitimes. **MITRE T1078 (Valid Accounts) :** FortiClient EMS permet de bloquer l'accès réseau même à des utilisateurs authentifiés si leur terminal n'est pas conforme à la politique de sécurité de l'organisation.

FortiClient EMS (Endpoint Management Server) collecte la posture de chaque terminal et transmet des **tags de conformité** au FortiGate. Ces tags sont ensuite utilisés dans les politiques de pare-feu et les règles ZTNA pour conditionner l'accès à l'état réel du poste.

**Critères de conformité endpoint typiques vérifiés par FortiClient EMS :**

| CRITÈRE | DESCRIPTION | IMPACT SI NON CONFORME |
|---|---|---|
| Niveau de patch OS | Windows/macOS à jour (dernières mises à jour critiques) | Accès refusé ou réseau de remédiation |
| Antivirus installé et à jour | Agent AV actif, signatures < 24h | Quarantaine automatique |
| Chiffrement disque actif | BitLocker (Windows) ou FileVault (macOS) | Accès données sensibles refusé |
| Absence de logiciels interdits | Pas de Tor Browser, TeamViewer non autorisé, etc. | Alerte + blocage accès |
| FortiClient version | Agent EMS à jour | Mise à jour forcée avant accès |
| Statut pare-feu local | Pare-feu hôte activé | Accès conditionné |

### Impact potentiel si EMS non déployé

- Accès réseau accordé à des postes non patchés exploitables comme vecteurs de rebond (T1078)
- Propagation de malwares depuis des postes sans AV à jour vers le réseau interne
- Non-conformité avec les exigences ZTNA : le ZTNA sans vérification de posture est partiel
- Absence de visibilité sur l'état réel des terminaux accédant aux ressources critiques

**Navigation**

```
Security Fabric > Fabric Connectors
→ Create New
→ Type : "FortiClient EMS"
→ EMS Server : <IP_ou_FQDN_FortiClient_EMS>
→ Port : 8013 (par défaut)
→ "Verify Certificate" : activer
→ Authorize (approuver la connexion côté EMS)
→ Apply

Security Fabric > Fabric Connectors > FortiClient EMS
→ Section "Endpoint Tags" : vérifier les tags de conformité remontés
```

**CLI de vérification**

```
# Vérifier la connexion FortiClient EMS
show endpoint-control server

# Vérifier le statut de la connexion EMS
diagnose endpoint-control server status

# Lister les terminaux enregistrés et leurs tags de conformité
diagnose endpoint-control registration list

# Vérifier les tags de conformité disponibles
show endpoint-control fctems
diagnose user fortiems list
```

**Remédiation**

1. Connecter FortiClient EMS au FortiGate : `config endpoint-control fctems` → `edit 1` → `set name "EMS-Production"` → `set server "<IP_EMS>"` → `set https-port 8013` → `set status enable` → `set pull-tags enable` → `set pull-vulnerabilities enable` → `set certificate-fingerprint "<fingerprint>"` → `end`
2. Activer la synchronisation des enregistrements FortiClient et vérifier les tags de conformité remontés : `diagnose endpoint-control server status` (doit afficher “connected”) puis `diagnose user fortiems list`
3. Définir dans FortiClient EMS les critères de conformité : niveau de patch OS (Windows Update), antivirus actif et signatures < 24h, chiffrement disque (BitLocker/FileVault), pare-feu hôte activé ; attribuer des tags “Compliant” / “Non-Compliant” selon les résultats
4. Appliquer les tags EMS dans les politiques firewall d’accès aux ressources critiques : `config firewall policy` → `edit <id>` → `set ztna-ems-tag "EMS-Compliant-Tag"` → `set logtraffic all` → `end` — seuls les terminaux conformes pourront accéder aux ressources
5. Créer une politique de redirection pour les terminaux non conformes vers un VLAN de remédiation (portail de mise à jour / helpdesk) avec `set logtraffic all` pour traçabilité
6. Vérifier l’ensemble du déploiement avec `diagnose endpoint-control registration list` (liste tous les terminaux enregistrés et leurs tags) et `diagnose endpoint-control client-status list`

**Valeur par défaut :** Aucune connexion FortiClient EMS configurée par défaut. Le check de posture EMS est désactivé.

**Critère de conformité :** FortiClient EMS connecté et synchronisé ( `diagnose endpoint-control server status` = connected). Tags de conformité configurés dans FortiClient EMS avec les critères de l'organisation (patch niveau OS, AV, chiffrement disque). Tags de conformité EMS appliqués dans les politiques d'accès aux ressources critiques. Portail de remédiation configuré pour les terminaux non conformes. Journalisation des accès conditionnés activée.

---

# Domaine 8 — Inspection SSL/TLS

> ***Objectif :*** *Configurer l'inspection SSL/TLS pour détecter les menaces cachées dans le trafic chiffré, qui représente désormais plus de 90 % du trafic Internet. Une inspection SSL correctement configurée avec un certificat CA dédié est essentielle pour l'efficacité des profils IPS, AV et Web Filter.*

---

## Contrôle 8.1 — Profil d'inspection SSL en deep inspection (full)

> ***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1573, T1048, T1557* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

Sans inspection SSL/TLS profonde, l'IPS, l'Antivirus et le Web Filter ne voient que les métadonnées des connexions HTTPS — ils ne peuvent pas inspecter le contenu des requêtes et réponses chiffrées. La majorité des malwares modernes et des canaux C2 utilisent HTTPS pour se camoufler dans le trafic légitime. L'inspection SSL déchiffre, inspecte et rechiffre le trafic à la volée.

Les **gaps d'inspection SSL** (T1557) constituent un angle mort significatif : sans deep inspection, les attaques man-in-the-middle via HTTPS, les tunnels chiffrés et l'exfiltration DNS over HTTPS ne peuvent pas être détectés.

**Impact potentiel**

- Malwares téléchargés en HTTPS non détectés par l'AV sans inspection SSL
- Communications C2 en HTTPS non bloquées par l'IPS sans inspection
- Exfiltration de données chiffrées non détectée par le DLP
- Attaques adversary-in-the-middle (T1557) non visibles sans inspection profonde

**Navigation**

```
Security Profiles > SSL/SSH Inspection
→ Sélectionner ou créer un profil "deep-inspection"
→ "SSL Inspection Mode" : Full SSL Inspection (Deep Inspection)
→ "CA Certificate" : sélectionner le certificat CA dédié (voir contrôle 8.2)
→ "Inspect All Ports" : activer ou spécifier les ports HTTPS (443, 8443)
→ "SSL Protocol Versions" : TLS 1.0 minimum désactivé
→ OK
→ Appliquer le profil aux politiques concernées
```

**CLI de vérification**

```
show firewall ssl-ssh-profile
```

Vérifier : `set inspect-all enable` ou configuration des ports HTTPS.

**Remédiation**

```
config firewall ssl-ssh-profile
    edit "deep-inspection-custom"
        set comment "Inspection SSL profonde"
        set caname "<CA_inspection>"
        set untrusted-caname "<CA_inspection>"
        config https
            set ports 443 8443
            set status deep-inspection
        end
        config imaps
            set ports 993
            set status deep-inspection
        end
        config pop3s
            set ports 995
            set status deep-inspection
        end
        config smtps
            set ports 465
            set status deep-inspection
        end
        set ssl-anomalies-log enable
        set ssl-exemptions-log enable
    next
end
```

**Valeur par défaut :** Profil “certificate-inspection” (vérification du certificat seulement, pas d’inspection du contenu) utilisé par défaut.

**Critère de conformité :** Profil deep-inspection appliqué aux politiques couvrant le trafic Internet utilisateur. Taux d’exemptions documenté et < 5 % du trafic total.

---

## Contrôle 8.2 — Certificat CA dédié pour l’inspection SSL

***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1557* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

L’inspection SSL nécessite un certificat CA dont la clé privée est utilisée pour re-signer les certificats des serveurs inspectés. Utiliser le certificat CA Fortinet par défaut expose la clé à un risque partagé entre tous les équipements FortiGate dans le monde. Un CA dédié, généré par la PKI de l’organisation, garantit que la clé privée est unique et sous contrôle exclusif.

**Impact potentiel**

- Risque de compromission si la clé CA d’inspection Fortinet par défaut est divulguée
- Impossibilité de distinguer le trafic inspecté du trafic légitime sans CA dédié
- Non-conformité avec les politiques PKI d’entreprise

**Navigation**

```
System > Certificates > Create/Import > CA Certificate
→ Generate (si génération locale) ou Import (si PKI externe)
→ Nommer le certificat (ex: "CA-SSL-Inspection-[orgname]")
→ Valeur de durée : 3 à 5 ans maximum
→ Distribuer le certificat CA aux navigateurs des utilisateurs (via GPO Active Directory)
```

**CLI de vérification**

```
show vpn certificate ca
show system certificate ca
```

**Remédiation**

Générer un CA dédié depuis FortiGate :

```
config vpn certificate local
    edit "CA-inspection"
        set comments "CA dédié pour inspection SSL - [orgname]"
    next
end
```

Ou importer un CA signé par la PKI d'entreprise.

**Valeur par défaut :** CA Fortinet par défaut ("Fortinet_CA_SSL") utilisé pour l'inspection.

**Critère de conformité :** CA d'inspection SSL distinct du CA Fortinet par défaut. Clé privée protégée. Certificate déployé dans les magasins de certificats des postes via GPO.

---

## Contrôle 8.3 — Exemptions SSL limitées et documentées

***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1048* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Les exemptions d'inspection SSL (certificat-pinning, banking, santé) sont nécessaires mais doivent être strictement limitées et revues régulièrement. Un excès d'exemptions (catégories entières, domaines génériques) crée des angles morts dans l'inspection et peut être exploité par des malwares qui s'hébergent sur des domaines exemptés.

**Impact potentiel**

- Téléchargement de malwares depuis des domaines exemptés non inspectés
- Communications C2 non détectées via des domaines dans des catégories exemptées
- Exfiltration de données via des canaux SSL non inspectés

**Navigation**

```
Security Profiles > SSL/SSH Inspection
→ Éditer le profil deep-inspection
→ Section "SSL Exemptions"
→ N'exempter que les destinations spécifiques nécessaires (pas de catégories entières)
→ Documenter chaque exemption avec une justification métier
→ Activer "Log SSL Exemptions"
```

**CLI de vérification**

```
show firewall ssl-ssh-profile | grep exempt
```

Vérifier que la liste d'exemptions est minimale et documentée.

**Remédiation**

Limiter les exemptions à des FQDN ou adresses IP spécifiques :

```
config firewall ssl-ssh-profile
    edit "deep-inspection-custom"
        config ssl-exempt
            edit 1
                set type fortiguard-category
                set fortiguard-category 100
                (Finance et banking — si nécessaire opérationnellement)
            next
        end
    next
end
```

**Valeur par défaut :** Exemptions par défaut pour les catégories banking, santé et quelques domaines connus.

**Critère de conformité :** Liste d'exemptions documentée et revue trimestriellement. Aucune catégorie entière exemptée sans justification. Log des exemptions activé.

---

## Contrôle 8.4 — Gestion du cycle de vie des certificats (OCSP, CRL, expiration)

***CIS Ref :*** *(best practice PKI)* | ***MITRE :*** *T1553, T1557* | ***Niveau :*** 🟢 *L1*

**Description du risque**

Les certificats TLS utilisés par le FortiGate pour l'administration HTTPS, le portail SSL-VPN, l'inspection SSL et le Security Fabric doivent être gérés activement sur l'ensemble de leur cycle de vie. Un certificat expiré dégrade la confiance (alertes navigateur, rupture des connexions automatisées) ; un certificat révoqué non détecté crée un vecteur d'attaque MITM (T1557). L'absence de vérification de révocation (OCSP/CRL) permet à un attaquant disposant d'un certificat volé mais révoqué de se faire passer pour un serveur légitime.

**MITRE T1553 (Subvert Trust Controls) :** Un attaquant peut tenter d'utiliser un certificat compromis ou auto-signé pour intercepter le trafic. La vérification OCSP et les CRL garantissent que seuls les certificats valides et non révoqués sont acceptés.

**Types de certificats à gérer sur FortiGate :**

| TYPE | UTILISATION | CONTRÔLE CLÉ |
|---|---|---|
| Certificat management HTTPS | Authentification de l'interface admin | Signé par CA reconnue, non expiré |
| Certificat portail SSL-VPN | Authentification du portail VPN | Signé par CA publique, FQDN correct |
| CA d'inspection SSL | Re-signature des certificats inspectés | CA dédiée, déployée sur les postes |
| Certificats Security Fabric | Authentification entre membres Fabric | Émis par CA Fortinet ou PKI interne |
| Certificats ZTNA | Authentification du ZTNA Gateway | Signé par CA reconnue |

**Impact potentiel**

- Certificat management expiré = interruption des accès administrateurs et des automatisations API (T1499)
- Certificat révoqué non détecté = attaque MITM silencieuse sur le trafic administratif (T1557)
- Certificat auto-signé par défaut = les administrateurs ignorent les alertes TLS (habituation dangereuse)
- Absence de monitoring d'expiration = découverte de l'expiration en urgence opérationnelle

**Navigation**

```
System > Certificates
→ Vérifier les dates d'expiration de tous les certificats locaux
→ Importer > Local Certificate : importer un certificat signé PKI
→ "Certificate Details" : vérifier CN/SAN, CA émettrice, validité

System > Settings
→ "HTTPS Server Certificate" : sélectionner le certificat management importé
→ Apply

VPN > SSL-VPN Settings
→ "Server Certificate" : sélectionner le certificat VPN importé
```

**CLI de vérification**

```
# Lister tous les certificats locaux et leurs dates d'expiration
get vpn certificate local

# Vérifier les détails d'un certificat spécifique
diagnose vpn certificate check-cert <nom_certificat>

# Vérifier les CA de confiance configurées
show vpn certificate ca

# Vérifier les CRL configurées
show vpn certificate crl

# Vérifier la configuration OCSP
show vpn certificate setting | grep ocsp

# Vérifier les certificats proches de l'expiration (< 30 jours)
diagnose sys certificate list | grep -e expire -e valid
```

**Remédiation**

1. Importer le certificat management signé par la PKI de l'organisation (GUI : System > Certificates > Import > Local Certificate > PKCS12), puis l'assigner à l'interface HTTPS admin : `config system global` → `set admin-server-cert "<nom_certificat>"` → `end`
2. Activer la vérification OCSP pour rejeter les certificats révoqués : `config vpn certificate setting` → `set ocsp-status enable` → `set ocsp-option must` → `end` ; vérifier avec `show vpn certificate setting | grep ocsp`
3. Importer et configurer la CRL de la PKI interne : `config vpn certificate crl` → `edit "CRL-PKI-Interne"` → `set http-url "http://pki.company.com/crl/root.crl"` → `set update-vdom "root"` → `end` ; vérifier avec `show vpn certificate crl`
4. S'assurer qu'aucun certificat n'est proche de l'expiration : `get vpn certificate local | grep -e "name" -e "expire"` et `diagnose vpn certificate check-cert <nom_certificat>` — planifier le renouvellement 60 jours avant expiration
5. Documenter dans un tableau de suivi l'ensemble des certificats (management HTTPS, SSL-VPN, CA inspection SSL, Security Fabric) avec leur date d'expiration, CA émettrice et date de renouvellement prévue
6. Mettre en place une alerte automatique sur les événements "certificate expiry warning" dans FortiAnalyzer ou le SIEM, et intégrer la vérification mensuelle dans le processus de supervision ( `diagnose sys certificate list | grep -e expire -e valid` )

**Valeur par défaut :** Certificat auto-signé Fortinet_Factory pour le management et le VPN. OCSP désactivé par défaut. Aucune CRL configurée par défaut.

**Critère de conformité :** Certificat management HTTPS signé par la PKI de l'organisation (pas le certificat Fortinet_Factory). Certificat SSL-VPN signé par une CA reconnue. OCSP activé ( `set ocsp-status enable` ). CRL configurée pour la PKI interne si applicable. Aucun certificat expiré ou expirant dans moins de 30 jours. Processus de monitoring d'expiration documenté et automatisé (alerte 60j avant). `diagnose vpn certificate check-cert` sans erreur sur tous les certificats critiques.

---

# Domaine 9 — Paramètres réseau et segmentation

> ***Objectif :*** *Configurer les paramètres réseau fondamentaux du FortiGate (DNS, NTP, IPv6, zones) pour assurer la précision des logs, la sécurité des communications réseau et une segmentation efficace limitant le mouvement latéral.*

---

## Contrôle 9.1 — DNS sécurisé configuré

> ***CIS Ref :*** *1.1* | ***MITRE :*** *T1071.004* | ***Niveau :*** 🟢 *L1*

**Description du risque**

Le FortiGate utilise le DNS pour la résolution des FQDN dans les politiques, les mises à jour FortiGuard, les connexions Security Fabric et les profils de sécurité. L'utilisation de serveurs DNS non sécurisés ou par défaut expose l'équipement à des attaques d'empoisonnement DNS (DNS spoofing) qui peuvent rediriger les mises à jour FortiGuard vers des serveurs malveillants ou compromettre la résolution des noms dans les politiques de sécurité.

**Impact potentiel**

- Empoisonnement DNS redirigeant les mises à jour FortiGuard vers des serveurs malveillants
- Contournement du filtrage DNS via des résolveurs alternatifs non contrôlés
- Résolution incorrecte des FQDN dans les politiques de sécurité

**Navigation**

```
Network > DNS
→ DNS Type : "Specify"
→ Primary DNS Server : <IP_DNS_interne_ou_FortiGuard>
→ Secondary DNS Server : <IP_DNS_secondaire>
→ "Fortiguard DDNS" : optionnel selon besoin
→ Apply
```

**CLI de vérification**

```
config system dns
    show
```

Vérifier la présence d'un serveur DNS primaire et secondaire configurés explicitement.

**Remédiation**

```
config system dns
    set primary 8.8.8.8
    set secondary 8.8.4.4
    set protocol cleartext dot
    set ssl-certificate "Fortinet_Factory"
    set server-hostname "dns.google"
end
```

Pour DNS over TLS (DoT) vers FortiGuard :

```
config system dns
    set protocol dot
    set primary 96.45.45.45
    set secondary 96.45.46.46
end
```

**Valeur par défaut :** DNS primaire : 96.45.45.45 (FortiGuard), secondaire : 96.45.46.46 (FortiGuard).

**Critère de conformité :** Serveurs DNS primaire et secondaire configurés avec des serveurs connus et de confiance. DNS over TLS (DoT) activé si FortiGuard DNS est utilisé.

---

### Contrôle 9.2 — NTP authentifié configuré

***CIS Ref :*** *2.1.4* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

**Description du risque**

L'heure correcte du FortiGate est critique pour la validité des certificats TLS (vérification de plage de validité), la cohérence des timestamps dans les logs (corrélation SIEM), et le bon fonctionnement des politiques basées sur des plannings. Un temps incorrect peut invalider des certificats valides ou rendre des logs inutilisables en investigation forensique. **L'authentification NTP** empêche les attaques de manipulation de l'heure (NTP spoofing) qui pourraient invalider des certificats ou perturber la corrélation des logs.

**Impact potentiel**

- Invalidation des certificats TLS si l'heure système est incorrecte
- Logs avec timestamps incohérents rendant l'investigation forensique impossible
- Contournement des politiques basées sur des plannings horaires
- Attaque NTP spoofing modifiant l'heure du système pour invalider des certificats VPN

**Navigation**

```
System > Settings
→ Section "System Time"
→ "NTP Server" : Specify
→ Saisir les serveurs NTP (pool.ntp.org, time.cloudflare.com)
→ "Sync Now"
→ Apply
```

**CLI de vérification**

```
show system ntp
diagnose sys ntp status
```

Vérifier `synchronized: yes` et la liste des serveurs NTP configurés.

**Remédiation**

```
# Configuration NTP avec authentification complète
# MITRE T1070 (Indicator Removal) : timestamps corrects = forensique fiable
config system ntp
    set ntpsync enable
    set type custom
    set syncinterval 60
    config ntpserver
        edit 1
            set server "pool.ntp.org"
            set ntpv3 enable
            set authentication enable
            set key-id 1
            set key "<clé_ntp_partagée_forte>"
        next
        edit 2
            set server "time.cloudflare.com"
            set ntpv3 enable
            set authentication enable
            set key-id 2
            set key "<clé_ntp_secondaire>"
        next
        edit 3
            set server "<serveur_ntp_interne>"
            set ntpv3 enable
            set authentication enable
            set key-id 3
            set key "<clé_ntp_interne>"
        next
    end
end
```

> ***NTP Authentication — pourquoi critique (MITRE T1070) :*** *Un attaquant capable de manipuler l'heure du FortiGate peut invalider des certificats TLS (en renvoyant la date en dehors de la plage de validité), perturber les politiques basées sur des plannings, et rendre inutilisable la corrélation forensique des logs (Indicator Removal via timestamp manipulation). L'authentification NTP avec des clés partagées garantit que seuls les serveurs NTP légitimes peuvent synchroniser l'heure.*

**Configurer le fuseau horaire correct :**

```
config system global
    set timezone 28
    # 28 = Europe/Paris (UTC+1/+2 selon heure d'été)
    # Lister les timezones : execute time ?
end
```

**Vérification post-configuration :**

```
# Vérifier la synchronisation NTP
diagnose sys ntp status
# Valeur attendue : synchronized: yes, stratum: 2 ou 3

# Vérifier l'heure courante
get system status | grep time
execute time
```

**Valeur par défaut :** NTP FortiGuard configuré par défaut (ntp1.fortiguard.com, ntp2.fortiguard.com). Authentification NTP désactivée par défaut.

**Critère de conformité :** Au moins 2 serveurs NTP configurés (dont un serveur NTP interne si disponible). `synchronized: yes` dans `diagnose sys ntp status`. Authentification NTP activée avec clés partagées. Fuseau horaire correct configuré (`set timezone`). Déviation maximale tolérée : ≤ 1 seconde par rapport à la source NTP de référence.

---

## Contrôle 9.3 — IPv6 désactivé si non utilisé

> ***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1190* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Si IPv6 n'est pas utilisé dans l'environnement, le laisser activé sur le FortiGate expose des interfaces réseau supplémentaires potentiellement non couvertes par les politiques de sécurité IPv4. Des scans et des exploits IPv6 spécifiques (CVE liées à l'implémentation IPv6 de FortiOS) peuvent cibler des équipements avec IPv6 activé mais non configuré ni filtré.

**Impact potentiel**

- Exposition à des vulnérabilités spécifiques à l'implémentation IPv6 de FortiOS

- Tunnels IPv6 non filtrés permettant de contourner les politiques IPv4
- Surface d'attaque élargie sans bénéfice opérationnel

**Navigation**

```
System > Settings
→ "IPv6 Support" : désactiver si IPv6 non utilisé
→ Redémarrage requis
→ Apply
```

**CLI de vérification**

```
get system global | grep ipv6
```

Vérifier : `ipv6-accept-ra : disable` et `ipv6-allow-anycast-probe : disable`.

**Remédiation**

Si IPv6 non utilisé :

```
config system global
    set ipv6-allow-anycast-probe disable
    set ipv6-allow-local-in-silent-drop enable
end
```

Sur les interfaces :

```
config system interface
    edit "wan1"
        set ip6 disable
    next
end
```

**Valeur par défaut :** IPv6 activé par défaut sur FortiOS 7.4.

**Critère de conformité :** IPv6 désactivé sur toutes les interfaces si l'organisation n'utilise pas IPv6. Exception documentée si IPv6 est requis opérationnellement.

---

## Contrôle 9.4 — Segmentation zones LAN/WAN/DMZ

***CIS Ref :*** *(best practice)* | ***MITRE :*** *T1021* | ***Niveau :*** 🟢 *L1*

**Description du risque**

Sans segmentation en zones distinctes (LAN, WAN, DMZ, MGMT), tout le trafic entre les différents segments réseau peut circuler sans contrôle. La segmentation force tout le trafic inter-zone à traverser les politiques de sécurité du FortiGate, permettant l'inspection, le filtrage et la journalisation. La DMZ doit isoler les serveurs exposés pour limiter l'impact en cas de compromission.

**Impact potentiel**

- Propagation d'une compromission depuis la DMZ vers le LAN sans contrôle
- Mouvement latéral facilité par l'absence de segmentation entre VLAN
- Impossibilité d'appliquer des politiques de sécurité différenciées par zone

**Navigation**

```
Network > Interfaces
→ Créer des zones : LAN, WAN, DMZ, MGMT
→ Assigner les interfaces aux zones appropriées
→ Activer "Block intra-zone traffic" pour LAN et DMZ
→ Définir les politiques inter-zones dans Policy & Objects > Firewall Policy
```

**CLI de vérification**

```
show system zone
show system interface | grep zone
```

**Remédiation**

```
config system zone
    edit "LAN"
        set intrazone deny
        set interface "internal1" "internal2"
    next
    edit "DMZ"
        set intrazone deny
        set interface "dmz"
    next
    edit "MGMT"
        set intrazone deny
        set interface "mgmt"
    next
end
```

**Valeur par défaut :** Zones non configurées sur les nouveaux équipements. Configuration dépendante du modèle FortiGate.

**Critère de conformité :** Au minimum 3 zones définies (LAN, WAN, DMZ). `intrazone deny` sur LAN et DMZ. Politiques de flux inter-zones documentées et minimales (moindre privilège).

---

## Contrôle 9.5 — Protection DoS hardware (ASIC NP6/NP7)

***CIS Ref :*** *(best practice Fortinet)* | ***MITRE :*** *T1498* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

Les FortiGate équipés de processeurs NP6 ou NP7 (Network Processor) peuvent décharger la protection contre les attaques DoS/DDoS sur le matériel, sans impacter les performances du CPU. Cette protection hardware ASIC permet de traiter et bloquer des millions de paquets d'attaque DoS par seconde sans dégradation du service légitime. Les attaques de type Network Denial of Service (T1498) sont fréquemment utilisées pour masquer des tentatives d'intrusion ou pour impacter la disponibilité des services critiques.

**Types d'attaques protégées par offloading NP6/NP7 :** - `tcp_syn_flood` : Flooding SYN TCP (attaque la plus courante) — seuil recommandé : 2000/s - `tcp_port_scan` : Scans de ports TCP — seuil recommandé : 1000/s - `tcp_src_session` / `tcp_dst_session` : Limite de sessions par IP source/destination — seuil : 5000 - `ip_src_session` / `ip_dst_session` : Limite de sessions IP globale par source/destination — seuil : 5000

**Bonne pratique — Déploiement en deux phases :** 1. **Phase 1 — MONITOR** : activer en mode `monitor` (sans blocage) pendant 1-2 semaines pour établir la baseline de trafic légitime et identifier les seuils appropriés 2. **Phase 2 — BLOCK** : passer en mode `block` une fois les seuils calibrés selon le profil de trafic réel

**Impact potentiel**

- Saturation du CPU FortiGate par des attaques DoS volumétriques
- Interruption du service de filtrage réseau pendant une attaque DoS
- Utilisation d'une attaque DoS comme leurre pendant une intrusion simultanée (T1498)

**Navigation**

```
Policy & Objects > DoS Policy
→ Create New
→ Interface : WAN (puis répliquer sur autres interfaces exposées)
→ Source Address : all
→ Destination Address : all
→ Service : ALL
→ Activer les anomalies une par une avec leurs seuils
→ Commencer avec l'action "Monitor" puis passer à "Block" après baseline
→ Apply
```

**CLI de vérification**

```
# Vérifier la politique DoS configurée
show firewall DoS-policy

# Vérifier les anomalies détectées sur NP6 (hardware offloading)
diagnose npu np6 anomaly list

# Vérifier les statistiques d'anomalies en temps réel
diagnose npu np6 anomaly stats 0

# Vérifier si les FortiGate dispose d'un NP7 (modèles récents)
diagnose npu np7 anomaly list
```

**Remédiation**

**Phase 1 — Mode MONITOR (baseline, à déployer en premier) :**

```
config firewall DoS-policy
    edit 1
        set name "dos-baseline-wan"
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set status enable
        config anomaly
            edit "tcp_syn_flood"
                set status enable
                set log enable
                set action monitor
                set threshold 2000
            next
            edit "tcp_port_scan"
                set status enable
                set log enable
                set action monitor
                set threshold 1000
            next
            edit "tcp_src_session"
                set status enable
                set log enable
                set action monitor
                set threshold 5000
            next
            edit "tcp_dst_session"
                set status enable
                set log enable
                set action monitor
                set threshold 5000
            next
            edit "ip_src_session"
                set status enable
                set log enable
                set action monitor
                set threshold 5000
            next
            edit "ip_dst_session"
                set status enable
                set log enable
                set action monitor
                set threshold 5000
            next
        end
    next
end
```

**Phase 2 — Mode BLOCK (après calibration des seuils) :**

```
config firewall DoS-policy
    edit 1
        set name "dos-protection-wan"
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set status enable
        config anomaly
            edit "tcp_syn_flood"
                set status enable
                set log enable
                set action block
                set threshold 2000
            next
            edit "tcp_port_scan"
                set status enable
                set log enable
                set action block
                set threshold 1000
            next
            edit "tcp_src_session"
                set status enable
                set log enable
                set action block
                set threshold 5000
            next
            edit "tcp_dst_session"
                set status enable
                set log enable
                set action block
                set threshold 5000
            next
            edit "ip_src_session"
                set status enable
                set log enable
                set action block
                set threshold 5000
            next
            edit "ip_dst_session"
                set status enable
                set log enable
                set action block
                set threshold 5000
            next
        end
    next
end
```

**Activer l’offloading ASIC NP6/NP7 pour le DoS hardware :**

```
config system npu
    set ipsec-ob-np-sel auto
    config fp-anomaly
        set tcp-syn-flood-drop enable
        set tcp-port-scan-drop enable
        set ip-src-session-drop enable
    end
end
```

> ***Note :*** *Les seuils fournis (2000/s, 1000/s, 5000) sont des valeurs de départ recommandées par Fortinet. Ajuster selon le profil de trafic légitime de l'organisation après la phase de monitoring. Un seuil trop bas peut bloquer du trafic légitime.*

**Valeur par défaut :** Protection DoS non configurée par défaut. Les processeurs NP6/NP7 sont disponibles mais leurs fonctionnalités DoS doivent être activées explicitement.

**Critère de conformité :** Politique DoS configurée sur l'interface WAN avec protection contre tcp_syn_flood, tcp_port_scan, tcp_src_session, tcp_dst_session, ip_src_session et ip_dst_session. Phase monitor réalisée avant activation du blocage. Seuils documentés et revus trimestriellement. Journalisation activée sur toutes les anomalies.

---

## Contrôle 9.6 — Authentification des protocoles de routage (OSPF/BGP)

> ***CIS Ref :*** *(best practice NIST SP 800-41)* | ***MITRE :*** *T1599* | ***Niveau :*** 🔵 *L2*

**Description du risque**

Si le FortiGate participe à un routage dynamique (OSPF, BGP, RIP), les échanges de topologie réseau entre routeurs doivent être authentifiés pour prévenir l'injection de routes malveillantes. Un attaquant ayant accès au même segment réseau qu'une interface OSPF ou BGP peut injecter de fausses annonces de routes pour : - Rediriger le trafic vers ses propres équipements (man-in-the-middle) - Créer des routes "black hole" pour une attaque DoS - Exfiltrer du trafic en le redirigant vers un équipement sous son contrôle

**MITRE T1599 (Network Boundary Bridging) :** La manipulation des tables de routage peut permettre de contourner les segmentations réseau et les périmètres de sécurité en redirigeant le trafic.

**Impact potentiel**

- Redirection du trafic légitime vers des équipements malveillants (T1599)
- Contournement des politiques de filtrage réseau par manipulation des routes
- Déni de service réseau par injection de routes invalides ou black-hole
- Espionnage du trafic inter-sites via redirection de routes BGP

**Navigation**

```
Network > Routing > OSPF
→ "Authentication" : activer pour chaque interface OSPF
→ Authentication Type : MD5 (ou SHA-256 si disponible)
→ Key ID et Password : configurer

Network > Routing > BGP
→ "BGP Peers" : éditer chaque peer
→ "Password" : activer et configurer un mot de passe BGP
```

**CLI de vérification**

```
# Vérifier l'authentification OSPF
show router ospf | grep authentication

# Vérifier les passwords BGP (apparaissent obfusqués)
show router bgp | grep -e password -e neighbor

# Vérifier les voisins OSPF établis
get router info ospf neighbor

# Vérifier les sessions BGP établies
get router info bgp summary
```

**Remédiation**

**OSPF avec authentification MD5 :**

```
config router ospf
    set router-id <IP_router_id>
    config ospf-interface
        edit "interface-lan"
            set interface "internal"
            set authentication md5
            config md5-keys
                edit 1
                    set key "<clé_md5_forte_ospf>"
                next
            end
        next
        edit "interface-dmz"
            set interface "dmz"
            set authentication md5
            config md5-keys
                edit 1
                    set key "<clé_md5_forte_ospf_dmz>"
                next
            end
        next
    end
    config area
        edit 0.0.0.0
            set type regular
        next
    end
end
```

**BGP avec authentification par password :**

```
config router bgp
    set as <votre_AS_number>
    config neighbor
        edit "<IP_peer_BGP>"
            set password "<mot_de_passe_bgp_fort>"
            set remote-as <AS_peer>
            set activate enable
        next
    end
end
```

**RIP avec authentification MD5 (si RIPv2 utilisé) :**

```
config router rip
    config interface
        edit "internal"
            set auth-mode md5
            config auth-md5
                edit 1
                    set key-string "<clé_md5_rip>"
                next
            end
        next
    end
end
```

> ***OSPF sur tunnels IPsec :*** *Si OSPF est utilisé pour annoncer des routes via des tunnels IPsec site-à-site, l'authentification OSPF MD5 doit être configurée sur les interfaces virtuelles IPsec (voire redondante avec la protection IPsec elle-même — défense en profondeur). Référence : Contrôle 7.2.*

**Valeur par défaut :** Aucune authentification configurée sur OSPF/BGP/RIP par défaut. Routage dynamique non activé par défaut.

**Critère de conformité :** Authentification MD5 (minimum) activée sur toutes les interfaces OSPF participantes. Password BGP configuré sur tous les peers BGP. Si RIPv2 utilisé : authentification MD5 activée. Clés de routage distinctes des mots de passe administrateurs. Rotation des clés planifiée (annuelle minimum).

---

## Contrôle 9.7 — High Availability (HA) hardening

> ***CIS Ref :*** *(best practice Fortinet)* | ***MITRE :*** *T1499, T1200* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Le mode High Availability (Active-Passive ou Active-Active) du FortiGate assure la continuité de service en cas de défaillance d'un nœud, mais introduit des vecteurs d'attaque spécifiques si mal configuré. Le trafic de heartbeat HA non authentifié peut être exploité pour injecter un nœud HA malveillant dans le cluster (**MITRE T1200 — Hardware Additions**), accédant à l'ensemble de la configuration et du trafic inspecté. Un cluster HA non sécurisé peut également être déstabilisé par un attaquant générant des défaillances artificielles du heartbeat pour provoquer des basculements répétés (**MITRE T1499 — Service Denial**).

**Vecteurs d'attaque HA spécifiques :**

| VECTEUR | DESCRIPTION | MITRE |
|---|---|---|
| Injection de nœud HA malveillant | FortiGate attaquant se connecte comme membre du cluster | T1200 |
| Usurpation heartbeat sans authentification | Messages VRRP-like forgés déstabilisant le cluster | T1499 |
| Sniffing heartbeat en clair | | T1040 |

| VECTEUR | DESCRIPTION | MITRE |
|---|---|---|
| | Synchronisation de session interceptée sur le réseau heartbeat | |
| Flapping (pre-emption) non contrôlé | Basculements répétés causant des interruptions de service | T1499 |
| Interface heartbeat partagée avec le trafic de données | Compromission d'un VLAN de données peut affecter le HA | T1200 |

**Impact potentiel**

- Injection d'un nœud HA non autorisé accédant à toute la configuration (clés VPN, comptes admin, politiques)
- Basculements répétés du cluster causant des interruptions de service réseau
- Déchiffrement du trafic de synchronisation de sessions (tables de connexion, état du pare-feu)
- Non-disponibilité du service de sécurité réseau pendant les basculements non maîtrisés

**Navigation**

```
System > HA
→ "Mode" : Active-Passive (recommandé) ou Active-Active
→ "Group ID" : identifiant unique du cluster (1-255)
→ "Group Name" : nom distinctif du cluster
→ "Password" : OBLIGATOIRE — mot de passe fort pour authentifier le heartbeat
→ "Heartbeat Interface(s)" : sélectionner les interfaces DÉDIÉES au heartbeat HA
→ "Override" : Disable (prévenir le flapping)
→ "Session Pickup" : Enable (pour l'Active-Passive — continuité de sessions)
→ "Monitor Interfaces" : sélectionner les interfaces à surveiller pour le failover
→ Apply
```

**CLI de vérification**

```
# Vérifier la configuration HA complète
show system ha

# Vérifier le statut HA en temps réel
get system ha status

# Vérifier les checksums de synchronisation entre membres
diagnose sys ha checksum show

# Afficher le statut détaillé par virtual cluster
diagnose sys ha dump-by-vcluster

# Vérifier la synchronisation des sessions
diagnose sys ha status
```

**Remédiation**

**Configuration HA sécurisée (mode Active-Passive recommandé) :**

```
config system ha
    set group-id 1
    set group-name "FW-HA-PROD"
    set mode a-p
    # a-p = Active-Passive (recommandé) / a-a = Active-Active
    set password <mot_de_passe_ha_fort_min16_car>
    # CRITIQUE : ce mot de passe authentifie les membres du cluster
    # Un cluster sans mot de passe accepte n'importe quel membre
    set hbdev "port3" 50 "port4" 50
    # Interfaces DÉDIÉES au heartbeat HA — priorités 50
    # Ne jamais partager avec les interfaces de données
    set priority 200
    # Priorité plus haute = membre préféré comme master
    set override disable
    # Désactiver la pre-emption — prévient les basculements répétés (flapping)
    # après retour du master d'origine
    set session-sync-dev "port4"
    # Interface dédiée à la synchronisation des tables de session
    set monitor "port1" "port2"
    # Interfaces à surveiller pour déclencher un failover
    # Si port1 OU port2 tombe, le cluster bascule
    set ha-uptime-diff-margin 300
    # Marge de temps d'uptime pour éviter les basculements sur différences mineures
    set link-failed-signal enable
    # Signaler immédiatement les pannes de liens monitorés
end
```

**Configuration réseau du heartbeat HA :**

```
# Les interfaces heartbeat HA doivent être sur un VLAN ou segment DÉDIÉ
# Ne jamais connecter les interfaces heartbeat sur le réseau de production
# Recommandation : câble direct ou switch dédié HA (pas sur le même switch que les données)

# Vérifier que les interfaces heartbeat n'ont pas de politique de sécurité traversante
show system interface port3 | grep allowaccess
# Les interfaces HA ne doivent avoir aucun allowaccess (aucun service admin)

# Vérifier que les interfaces heartbeat ne sont pas dans des zones de sécurité
show system zone
```

**Vérification post-configuration HA :**

```
# 1. Vérifier que les deux membres sont synchronisés
get system ha status
# Chercher : "Primary" et "Secondary" avec statuts "in-sync"

# 2. Vérifier l'absence de désynchronisation de configuration
diagnose sys ha checksum show
# Les checksums doivent être identiques entre Primary et Secondary

# 3. Tester le failover (en fenêtre de maintenance)
# Sur le membre Primary, simuler une panne d'interface monitorée
# puis vérifier que le Secondary prend le rôle Primary

# 4. Vérifier la synchronisation des tables de session
diagnose sys session full-stat

# 5. Accéder au membre Secondary pour vérification
execute ha manage 1 admin
# (0 = primary, 1+ = secondary)
```

**Gestion des mises à jour firmware en HA (staggered upgrade) :**

```
# Procédure de mise à jour sans interruption de service
# 1. Se connecter au cluster (interface virtuelle HA)
# 2. Accéder au membre Secondary via :
execute ha manage 0 admin

# 3. Mettre à jour le Secondary en premier
execute restore image ftp <image_fortiOS> <ip_ftp>

# 4. Après redémarrage du Secondary et synchronisation HA :
#    Déclencher un failover manuel pour que le Secondary devienne Primary
execute ha failover

# 5. Mettre à jour l'ancien Primary (maintenant Secondary)
execute ha manage 1 admin
execute restore image ftp <image_fortiOS> <ip_ftp>
```

**Valeur par défaut :** HA désactivé par défaut. Si configuré sans mot de passe : cluster ouvert à toute injection de nœud. `override` activé par défaut (pre-emption) — source de flapping.

**Critère de conformité :** `set password` configuré avec un mot de passe fort (≥ 16 caractères) dans `config system ha`. `set override disable` pour prévenir le flapping. Interfaces heartbeat physiquement dédiées (pas partagées avec le trafic de données). `set monitor` configuré sur les interfaces critiques (WAN, LAN). `diagnose sys ha checksum show` retourne des checksums identiques entre les membres. Procédure de mise à jour staggered documentée.

---

## Contrôle 9.8 — Sécurisation SD-WAN

***CIS Ref :*** *(best practice FortiOS 7.4)* | ***MITRE :*** *T1599* | ***Niveau :*** 🔵 *L2*

### Description du risque

FortiOS 7.4 intègre nativement le SD-WAN permettant de router dynamiquement le trafic sur plusieurs liens WAN selon des règles de qualité de service. Sans durcissement, les politiques SD-WAN peuvent créer des chemins de routage qui contournent les profils de sécurité applicables au trafic WAN standard. **MITRE T1599 (Network Boundary Bridging) :** si une règle SD-WAN route du trafic applicatif sur un lien WAN de secours non inspecté ou vers une destination imprévue, des données sensibles peuvent transiter hors du périmètre contrôlé. L'identification des applications dans SD-WAN doit reposer sur les signatures FortiGuard (couche 7) et non uniquement sur les ports, pour éviter le contournement par des applications légitimes abusées par des attaquants.

**Risques SD-WAN spécifiques :**

| RISQUE | DESCRIPTION | MITRE |
|---|---|---|
| Règle SD-WAN sans profil de sécurité | Trafic routé sans IPS/AV sur le lien SD-WAN sélectionné | T1599 |
| Application steering sur ports seuls | Bypass possible en changeant de port | T1599 |
| Lien dégradé toujours utilisé | Routage sur lien instable augmentant les risques | T1499 |
| Règle implicite SD-WAN ouverte | Catch-all routing non loggué vers n'importe quel lien | T1562 |
| Health check non sécurisé | Probes HTTP en clair permettant le spoofing des résultats | T1557 |

### Impact potentiel

- Trafic malveillant routé sur un lien SD-WAN secondaire échappant à l'inspection du lien principal
- Application steering basé uniquement sur les ports contourné par des malwares utilisant des ports HTTP/HTTPS
- Routage de trafic sensible sur un lien Internet de secours moins protégé
- Absence de logging sur la règle SD-WAN implicite masquant les flux non maîtrisés

### Navigation

```
Network > SD-WAN > SD-WAN Rules
→ Pour chaque règle : vérifier que des profils de sécurité sont appliqués
  (Les profils de sécurité s'appliquent via les politiques firewall qui utilisent SD-WAN)
→ "Mode" : Best Quality ou Lowest Cost avec SLA définie
→ "Health Check" : configurer pour chaque lien WAN SD-WAN
→ "Application" : utiliser les signatures FortiGuard (pas uniquement les ports)
→ Règle implicite : Action = Deny ou Log avec logging activé

Policy & Objects > Firewall Policy
→ S'assurer que les politiques couvrant le trafic SD-WAN ont les profils de sécurité activés
```

### CLI de vérification

```
# Vérifier la configuration SD-WAN globale
show system sdwan

# Vérifier les règles SD-WAN
show system sdwan rules

# Vérifier les membres (liens WAN) du SD-WAN
show system sdwan members

# Vérifier les health checks configurés
show system sdwan health-check

# Vérifier les SLA performance (qualité de lien)
diagnose sys sdwan health-check

# Vérifier le statut des membres SD-WAN
diagnose sys sdwan member
```

**Remédiation**

1. Configurer un health check HTTPS par lien WAN (protocole HTTPS plus difficile à usurper que ping) : `config system sdwan` → `config health-check` → `edit "HC-WAN1"` → `set server "connectivity-check.fortigate.com"` → `set protocol https` → `set failtime 3` → `set recoverytime 5` → `set members 1` → `end` ; répéter pour chaque lien WAN
2. Créer des règles SD-WAN avec steering applicatif FortiGuard couche 7 (pas uniquement les ports) : `config system sdwan` → `config service` → `set mode best-quality` → `set health-check "HC-WAN1" "HC-WAN2"` → `set application-list "appctrl-sdwan"` avec seuils SLA documentés (latency-threshold, jitter-threshold, packetloss-threshold) → `end`
3. S'assurer que les politiques firewall couvrant l'interface SD-WAN virtuelle ( `virtual-wan-link` ) activent les profils de sécurité complets : `set utm-status enable` → `set ips-sensor "protection-strict"` → `set av-profile "av-complet"` → `set webfilter-profile "wf-entreprise"` → `set ssl-ssh-profile "deep-inspection-custom"` → `set logtraffic all`
4. Activer le logging de la politique implicite SD-WAN pour tracer tous les flux non maîtrisés : `config log setting` → `set fwpolicy-implicit-log enable` → `end`
5. Vérifier l'état des membres SD-WAN et l'absence de lien dégradé utilisé activement : `diagnose sys sdwan member` et `diagnose sys sdwan health-check` — documenter les seuils SLA dans la politique de sécurité
6. Contrôler l'ensemble de la configuration avec `show system sdwan rules` pour vérifier que chaque règle référence un health check et non uniquement des ports, et que la règle catch-all a `logtraffic all` activé

**Valeur par défaut :** SD-WAN désactivé par défaut. Si activé, aucun health check configuré, aucun profil de sécurité imposé sur les règles SD-WAN par défaut.

**Critère de conformité :** Health checks configurés sur tous les membres SD-WAN avec seuils SLA documentés. Politiques firewall couvrant `virtual-wan-link` avec IPS, AV, Web Filter et DNS Filter activés (mêmes profils que les politiques WAN classiques). Application steering basé sur les signatures FortiGuard (pas ports seuls). Règle implicite SD-WAN avec logging activé. `diagnose sys sdwan member` ne retourne aucun lien en état "down" utilisé pour le routage actif.

---

# Domaine 10 — Journalisation et supervision SIEM

***Objectif :*** *Configurer la journalisation complète vers un SIEM externe ou FortiAnalyzer pour permettre la détection des incidents, l'investigation forensique et la conformité réglementaire. Les logs doivent être transmis de manière chiffrée et conservés au minimum 90 jours.*

---

## Contrôle 10.1 — Journalisation événements activée (Event Logging)

***CIS Ref :*** *7.1.1* | ***MITRE :*** *T1562.006* | ***Niveau :*** 🟢 *L1*

### Description du risque

Sans journalisation des événements système activée, les connexions administratives, les modifications de configuration, les échecs d'authentification et les événements système critiques ne sont pas tracés. Ces logs sont indispensables pour détecter les intrusions, les modifications non autorisées et pour les audits de conformité.

### Impact potentiel

- Modifications de configuration non tracées permettant des backdoors persistantes
- Impossibilité de détecter les tentatives de brute force sur les comptes administrateurs
- Non-conformité réglementaire sur les exigences de traçabilité des accès privilégiés

### Navigation

```
Log & Report > Log Settings
→ Section "Event Logging"
→ Activer : System Activity Events, User Activity Events, Router Events
→ "Security Rating Events" : activer
→ Apply
```

### CLI de vérification

```
show log setting
```

Vérifier : `event enable`, `security-rating enable`, `system enable`.

### Remédiation

```
config log setting
    set fwpolicy-implicit-log enable
    set fwpolicy6-implicit-log enable
    set log-user-in-upper enable
    set brief-traffic-format disable
end
```

Activer l'ensemble des catégories de logs — **tous les types doivent être activés** pour une couverture forensique complète :

```
config log eventfilter
    set event enable
    set system enable
    set vpn enable
    set user enable
    set router enable
    set wan-opt enable
    set wireless-activity enable
    set ha enable
    set compliance-check enable
    set endpoint enable
    set admin enable
    set dhcp enable
    set wanopt enable
    set network enable
    set security-rating enable
end
```

***Couverture complète des catégories de logs FortiOS 7.4 :***

| CATÉGORIE | DESCRIPTION | PERTINENCE SÉCURITÉ |
|---|---|---|
| `system` | *Événements système (démarrage, redémarrage, pannes)* | *Détection d'indisponibilité suspecte* |
| `admin` | *Connexions, modifications de config par les admins* | ***CRITIQUE** — traçabilité accès privilégiés* |
| `user` | *Authentifications utilisateurs (FSSO, RADIUS, LDAP)* | *Détection des compromissions de comptes* |
| `vpn` | *Connexions/déconnexions VPN, tunnels IPsec* | *Accès distants non autorisés* |
| `router` | *Changements de routage, adjacences OSPF/BGP* | *Manipulation des tables de routage* |
| `ha` | *Événements High Availability (failover, sync)* | *Détection des interruptions de service HA* |
| `compliance-check` | *Résultats des vérifications de conformité* | *Audit de posture continue* |
| `endpoint` | *Activité FortiClient/ZTNA sur les terminaux* | *Posture des équipements accédant au réseau* |
| `dhcp` | *Attribution d'adresses IP DHCP* | *Inventaire et détection de rogues devices* |
| `network` | *Événements réseau (ARP, spanning tree, etc.)* | *Détection d'anomalies réseau basses couches* |
| `wireless-activity` | *Événements Wi-Fi FortiAP* | *Détection de rogue AP et connexions Wi-Fi* |
| `wan-opt` / `wanopt` | *Optimisation WAN* | *Analyse des performances et anomalies WAN* |
| `security-rating` | *Résultats Security Rating CSPM* | *Suivi continu de la posture de sécurité* |

**Vérifier les logs traffic (séparé des event logs) :**

```
# Vérifier la journalisation du trafic (forward, local, sniffer)
show log setting
# Valeurs attendues :
# fwpolicy-implicit-log : enable
# local-in-allow : enable
# local-in-deny-unicast : enable
# local-in-deny-broadcast : enable
# local-out : enable
```

**Valeur par défaut :** Journalisation des événements partiellement activée selon le profil d'usine. De nombreuses catégories (`admin`, `ha`, `dhcp`, `compliance-check`) sont désactivées par défaut.

**Critère de conformité :** Toutes les catégories d'événements activées dans `config log eventfilter`. Journalisation des politiques implicites (`fwpolicy-implicit-log enable`). Logs traffic (`local-in-allow`, `local-in-deny-unicast`) activés. **MITRE T1562.006** (Indicator Blocking — disable logging) : la désactivation des logs est un indicateur de compromission active. **MITRE T1070.002** (Clear Linux or Mac System Logs) : activer l'envoi vers un SIEM externe pour que la suppression locale ne détruise pas les preuves.

---

## Contrôle 10.2 — Syslog vers SIEM externe chiffré en format CEF (TCP/TLS fiable)

***CIS Ref :*** *7.2.1, 7.3.2* | ***MITRE :*** *T1562.006, T1070.002, T1005* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

Les logs stockés uniquement sur le FortiGate local peuvent être effacés ou modifiés par un attaquant ayant compromis l'équipement (**MITRE T1070.002** — Clear System Logs). La transmission vers un SIEM externe garantit la préservation des preuves forensiques (**MITRE T1005** — Data from Local System : risque d'exfiltration des logs si non centralisés). L'utilisation de syslog en clair UDP 514 expose les logs à l'interception et à la modification. Le syslog chiffré via TLS (port 6514) en mode TCP fiable garantit l'intégrité, la confidentialité et la livraison des messages.

**Format CEF (Common Event Format) :** Le format CEF est le standard de l'industrie pour l'intégration avec les SIEM (Splunk, QRadar, Elastic/Kibana, ArcSight). Il permet le parsing automatique sans configuration manuelle sur le SIEM.

**Impact potentiel**

- Effacement des preuves d'intrusion par un attaquant ayant accès au FortiGate (T1070.002)
- Interception et modification des logs en transit si non chiffrés (T1557)
- Investigation forensique impossible sans logs centralisés préservés
- Exfiltration de logs sensibles si transmis en clair sur le réseau (T1005)

**Navigation**

```
Log & Report > Log Settings
→ Section "Remote Logging and Archiving"
→ "Send Logs to Syslog" : activer
→ IP/FQDN : <IP_SIEM>
→ Port : 6514 (TCP/TLS — recommandé)
→ "Reliable Logging" (TCP) : activer
→ "Log Format" : CEF (pour intégration SIEM automatique)
→ Source IP : <IP_interface_management_FortiGate>
→ Apply
```

**CLI de vérification**

```
show log syslogd setting
```

Vérifier : `status : enable`, `server : <IP_SIEM>`, `reliable : enable`, `enc-algorithm : high`, `format : cef`, `mode : reliable`.

**Remédiation**

```
# Configuration syslog TCP/TLS chiffré avec format CEF pour intégration SIEM
config log syslogd setting
    set status enable
    set server "siem.company.com"
    set reliable enable
    set port 6514
    set enc-algorithm high
    set certificate "<cert_TLS_SIEM>"
    set mode reliable
    set facility local7
    set format cef
end
```

Configurer le filtre pour s'assurer que TOUTES les catégories critiques sont transmises :

```
config log syslogd filter
    set severity information
    set forward-traffic enable
    set local-traffic enable
    set multicast-traffic enable
    set sniffer-traffic disable
    set anomaly enable
    set voip enable
    set dns enable
    set ssh enable
end
```

**Catégories minimum à transmettre vers le SIEM :**

| CATÉGORIE | IMPORTANCE SIEM | TYPE DE LOGS |
|---|---|---|
| `forward-traffic enable` | **Critique** | Tous les flux réseau inspectés |

| CATÉGORIE | IMPORTANCE SIEM | TYPE DE LOGS |
|---|---|---|
| `local-traffic enable` | **Critique** | Trafic vers/depuis le FortiGate lui-même |
| `anomaly enable` | **Critique** | Événements IPS/DoS |
| `dns enable` | Élevé | Requêtes DNS (détection C2) |
| `ssh enable` | Élevé | Sessions SSH administratives |
| `voip enable` | Moyen | Trafic VoIP (si applicable) |

**Pour les environnements avec plusieurs SIEM ou redondance (syslogd2, syslogd3) :**

```
# Second syslog server (redondance ou SIEM secondaire)
config log syslogd2 setting
    set status enable
    set server "<IP_SIEM_secondaire>"
    set reliable enable
    set port 6514
    set enc-algorithm high
    set mode reliable
    set format cef
end
```

**Vérification de la connectivité et des logs envoyés :**

```
# Tester l'envoi de logs vers le syslog configuré
diagnose log test

# Vérifier les statistiques d'envoi
diagnose test application syslogd 3

# Vérifier les erreurs de connexion syslog
diagnose log test
```

**Valeur par défaut :** Syslog désactivé par défaut. Format `default` (non CEF). Mode `udp` (non fiable).

**Critère de conformité :** Syslog activé vers au moins un SIEM externe avec `reliable enable` (TCP), `enc-algorithm high` (TLS), `format cef` (pour parsing SIEM automatique). Logs de trafic (forward, local), événements UTM, DNS et anomalies tous transmis. Port 6514 (TLS) utilisé. **MITRE T1562.006** mitigé : logs non éliminables localement car centralisés sur SIEM externe. **MITRE T1070.002** mitigé : toute tentative de suppression de logs sur le FortiGate ne détruit pas les preuves déjà envoyées.

---

### Contrôle 10.3 — Transfert fiable et chiffré vers FortiAnalyzer avec authentification par certificat

***CIS Ref :*** *7.2.1, 7.3.1* | ***MITRE :*** *T1562.006, T1070.002* | ***Niveau :*** 🟡 *MOYEN*

**Description du risque**

FortiAnalyzer offre une journalisation centralisée, une corrélation d'événements et des rapports de conformité intégrés pour les environnements Fortinet. La transmission vers FortiAnalyzer est chiffrée nativement et fiable via TCP. Sans FortiAnalyzer, la visibilité sur l'ensemble du Security Fabric est limitée et la corrélation inter-équipements impossible. L'utilisation du mode UDP syslog standard est déconseillée car les paquets peuvent être perdus sans notification — le mode `reliable` (TCP) garantit la livraison et détecte les interruptions de connexion.

**Pipeline recommandé :** FortiGate → FortiAnalyzer → FortiSIEM (pour corrélation étendue multi-sources).

**Impact potentiel**

- Perte de logs en transit si UDP utilisé (pas de confirmation de réception)
- Absence de corrélation des événements entre FortiGate et autres équipements Fortinet (T1562.006)
- Rapports de conformité manuels chronophages sans FortiAnalyzer
- Investigation forensique complexe sans timeline centralisée des événements (T1070.002)

**Navigation**

```
Security Fabric > Fabric Connectors > Logging & Analytics
→ FortiAnalyzer : activer
→ IP/FQDN : <IP_FortiAnalyzer>
→ "Upload Option" : Real Time
→ "Reliable" : activer (TCP)
→ "Encrypt Log Transmission" : activer (TLS)
→ Validate connection
→ Apply
```

**CLI de vérification**

```
show log fortianalyzer setting
```

Vérifier : `status : enable`, `server : <IP_FortiAnalyzer>`, `reliable : enable`, `enc-algorithm : high`, `ssl-min-proto-version : TLSv1-2`.

```
# Tester la connexion FortiAnalyzer
diagnose log test
execute log fortianalyzer-test

# Vérifier le statut de la connexion en temps réel
diagnose test application fmgd 5
```

**Remédiation**

```
config log fortianalyzer setting
    set status enable
    set server "192.168.1.100"
    set reliable enable
    set enc-algorithm high
    set ssl-min-proto-version tlsv1-2
    set certificate "FortiGate_CA"
    set conn-timeout 10
    set monitor-keepalive-period 5
    set monitor-failure-retry-period 5
    set upload-option realtime
    set source-ip "<IP_mgmt_FortiGate>"
end
```

**Paramètres de surveillance de la connexion :**

| PARAMÈTRE | VALEUR RECOMMANDÉE | DESCRIPTION |
|---|---|---|
| `conn-timeout` | 10 | Timeout de connexion initiale (secondes) |
| `monitor-keepalive-period` | 5 | Fréquence des pings de maintien de connexion |
| `monitor-failure-retry-period` | 5 | Délai de ré-essai après échec de connexion |
| `reliable` | enable | Mode TCP avec accusé de réception |
| `enc-algorithm` | high | Algorithmes TLS haut niveau uniquement |

**Vérifications diagnostiques complémentaires :**

```
# Vérifier que les logs partent bien vers FortiAnalyzer
execute log filter device fortianalyzer
execute log display

# Vérifier les statistiques d'envoi par équipement
diagnose log device list

# Tester l'envoi d'un log de test
diagnose log test
```

**Valeur par défaut :** FortiAnalyzer désactivé par défaut. Mode UDP. Pas d'authentification par certificat.

**Critère de conformité :** FortiAnalyzer configuré et connexion validée ( `diagnose log test` sans erreur). Transmission chiffrée TLS ( `enc-algorithm high` , `ssl-min-proto-version tlsv1-2` ). Mode `reliable enable` (TCP). Authentification par certificat ( `certificate` configuré). Upload mode : `realtime` . **MITRE T1070.002** mitigé : logs préservés sur FortiAnalyzer même si le FortiGate est compromis et ses logs locaux supprimés.

## Contrôle 10.4 — Rétention des logs ≥ 90 jours

***CIS Ref :*** *(best practice réglementaire)* | ***MITRE :*** *T1562.006* | ***Niveau :*** 🟢 *L1*

**Description du risque**

La plupart des réglementations (PCI-DSS, ISO 27001, RGPD, DORA, NIS2) imposent une conservation des logs de sécurité d'au minimum 90 jours en ligne et 1 an en archive. Sans politique de rétention configurée, les logs peuvent être écrasés prématurément, rendant impossible l'investigation d'incidents découverts tardivement (average dwell time des APT : 21-197 jours).

**Impact potentiel**

- Impossibilité d'investiguer des incidents découverts après purge des logs
- Non-conformité réglementaire avec PCI-DSS Req 10.7, ISO 27001, NIS2
- Perte de preuves judiciaires en cas de cyberattaque

**Navigation**

```
Log & Report > Log Settings
→ Configurer la rétention sur FortiAnalyzer (recommandé) : ≥ 90 jours
→ Sur FortiGate local : Dashboard > System Resources > Disk Usage
→ Activer le disque local si disponible pour buffer temporaire
```

**CLI de vérification**

Sur FortiAnalyzer :

```
diagnose fortianalyzer list
```

Sur FortiGate :

```
diagnose log test
show log disk setting
```

**Remédiation**

```
config log disk setting
    set status enable
    set ips-archive enable
    set max-log-file-size 100
    set roll-day sunday
    set roll-time 00:00
    set upload enable
    set upload-destination ftp
end
```

Configurer la rétention sur le SIEM/FortiAnalyzer selon la politique de l'organisation (≥ 90 jours actifs, ≥ 365 jours archive).

**Valeur par défaut :** Pas de disque local sur la plupart des modèles. Rétention dépendante de la capacité de stockage disponible.

**Critère de conformité :** Rétention des logs ≥ 90 jours en ligne sur le SIEM ou FortiAnalyzer. Archivage ≥ 365 jours. Politique de rétention documentée et alignée avec les exigences réglementaires applicables.

---

## Contrôle 10.5 — Alertes sur événements critiques

***CIS Ref :*** *7.1.1 (étendu)* | ***MITRE :*** *T1562* | ***Niveau :*** 🟡 *MOYEN*

### Description du risque

Sans alertes automatiques sur les événements critiques (connexions administratives, modifications de politiques, tentatives de brute force, déclenchements IPS critiques), les équipes de sécurité ne sont pas notifiées en temps réel des incidents potentiels. Le temps de détection moyen d'une compromission sans alertes automatisées est de plusieurs semaines.

### Impact potentiel

- Compromissions non détectées pendant de longues périodes sans alertes
- Modifications de configuration non autorisées passant inaperçues
- Absence de réponse à incident en temps réel

### Navigation

```
Log & Report > Alert E-mail
→ "Enable Alert E-mail" : activer
→ Serveur SMTP : configurer
→ Seuils d'alerte :
   - IPS Critical : Enable
   - Login Failure : Enable (threshold : 3)
   - Admin Login : Enable
   - Config Change : Enable
→ Apply
```

### CLI de vérification

```
show alertemail setting
```

### Remédiation

```
config alertemail setting
    set username "<adm_email>"
    set mailto1 "<soc@domaine.fr>"
    set filter-mode category
    set IPS-logs enable
    set firewall-authentication-failure-logs enable
    set ha-logs enable
    set admin-login-logs enable
    set configuration-changes-logs enable
    set critical-interval 1
    set warning-interval 15
end
```

**Valeur par défaut :** Alertes email désactivées par défaut.

**Critère de conformité :** Alertes configurées pour les événements IPS critiques, échecs d'authentification admin (seuil ≤ 3), modifications de configuration. Destination vers le SOC ou l'équipe sécurité. Délai d'alerte ≤ 5 minutes pour les événements critiques.

---

## Contrôle 10.6 — Durcissement FortiAnalyzer (lockout, TLS, position réseau, sécurité des comptes)

***CIS Ref :*** *7.3.1 (étendu)* | ***MITRE :*** *T1562.006, T1070.002, T1005* | ***Niveau :*** 🟠 *ÉLEVÉ*

**Description du risque**

FortiAnalyzer est un composant de sécurité critique — sa compromission équivaut à la perte de toute la forensique de logs. Un FortiAnalyzer non durci (comptes par défaut, TLS faible, exposé directement sur le réseau) représente un point de défaillance catastrophique : un attaquant qui le compromet peut effacer toutes les preuves de son intrusion (**MITRE T1070.002** — Clear Linux or Mac System Logs) et exfiltrer l'intégralité de l'historique des événements réseau (**MITRE T1005** — Data from Local System).

***AVERTISSEMENT CRITIQUE — FortiAnalyzer 5.4.0+ :*** *Il n'existe* ***pas de mécanisme de récupération de mot de passe*** *sur FortiAnalyzer 5.4.0 et supérieur. En cas de perte du mot de passe administrateur, la seule option est une réinitialisation d'usine (perte de toutes les données). Documenter les mots de passe de manière sécurisée dans un coffre-fort de mots de passe (CyberArk, HashiCorp Vault, Bitwarden Enterprise) immédiatement après la configuration initiale.*

**Impact potentiel**

- Compromission du FortiAnalyzer = effacement de toutes les preuves d'intrusion sur l'infrastructure Fortinet (T1070.002)
- Exfiltration de l'intégralité des logs réseau historiques par un attaquant (T1005)
- Désactivation ou altération silencieuse de la journalisation sans que le FortiGate ne le détecte (T1562.006)
- Perte irrémédiable de l'accès administrateur si le mot de passe est oublié (absence de récupération)

### Position réseau recommandée

> *Le FortiAnalyzer **doit être placé derrière un FortiGate** pour bénéficier de sa protection. Ne jamais exposer l'interface de gestion FortiAnalyzer directement sur Internet ou sur un segment réseau non filtré. Le FortiGate protégeant le FortiAnalyzer doit avoir les profils **IPS** et **Antivirus** activés sur les politiques couvrant le trafic FortiAnalyzer.*

### Navigation (FortiAnalyzer GUI)

```
System > Settings
→ "Login Security" :
   → "Admin lockout threshold" : 2
   → "Admin lockout duration" : 120 secondes
→ "Encryption Settings" :
   → "SSL Protocol" : TLS 1.2
   → "Encryption Level" : High
→ Apply

System > Admin > Password Policy
→ "Minimum length" : 14
→ "Complexity" : Upper + Lower + Number + Special
→ "Password expiry" : 90 jours
→ Apply

System > NTP
→ Configurer au moins 2 serveurs NTP
→ Synchroniser avec les mêmes serveurs que le FortiGate
→ Fuseau horaire identique à celui du FortiGate
```

### CLI de vérification (FortiAnalyzer)

```
# Vérifier le lockout administrateur
config system global
    get | grep admin-lockout
# Valeurs attendues : admin-lockout-threshold: 2, admin-lockout-duration: 120

# Vérifier le niveau TLS
config system global
    get | grep -e enc-algorithm -e ssl-protocol -e fgfm-ssl

# Vérifier la politique de mots de passe
config system admin
    show | grep -e password -e expire
```

### Remédiation

1. Durcir le lockout administrateur sur FortiAnalyzer : `config system global` → `set admin-lockout-threshold 2` → `set admin-lockout-duration 120` → `end` ; vérifier avec `config system global` → `get | grep admin-lockout`

2. Forcer TLS 1.2 sur tous les protocoles de communication FortiAnalyzer : `config system global` → `set enc-algorithm high` → `set fgfm-ssl-protocol tlsv1.2` → `set oftp-ssl-protocol tlsv1.2` → `set ssl-protocol tlsv1.2` → `set ssl-low-encryption disable` → `end`
3. Activer la politique de mots de passe administrateur : `config system password-policy` → `set status enable` → `set minimum-length 14` → `set must-contain upper-case-letter lower-case-letter number non-alphanumeric` → `set expire-status enable` → `set expire-day 90` → `end`
4. Créer des comptes administrateurs nominatifs avec MFA et Trusted Hosts : `config system admin user` → `edit "adm-prenom-nom"` → `set trusthost1 <IP_station>/32` → `set two-factor-auth enable` → `end` ; désactiver ou supprimer le compte “admin” par défaut après avoir créé un compte administrateur de secours documenté
5. Placer le FortiAnalyzer derrière un FortiGate avec profils IPS et AV activés sur les politiques couvrant son trafic ; ne jamais exposer son interface de management sur Internet ou un segment non filtré
6. Documenter immédiatement le mot de passe administrateur dans un coffre-fort sécurisé (CyberArk, HashiCorp Vault, Bitwarden Enterprise) — aucune récupération n’est possible sur FortiAnalyzer 5.4.0+ en cas de perte

**Valeur par défaut :** `admin-lockout-threshold : 3` (non 2), `admin-lockout-duration : 60` secondes. Niveau TLS non forcé à `high` par défaut. Politique de mots de passe non activée par défaut.

**Critère de conformité :** `admin-lockout-threshold : 2`, `admin-lockout-duration : 120`. TLS 1.2 minimum sur tous les protocoles (`enc-algorithm high`, `ssl-low-encryption disable`). Comptes administrateurs nominatifs avec MFA. Politique de mots de passe activée (min. 14 car., expiration 90 jours). FortiAnalyzer derrière un FortiGate avec IPS et AV activés. Documentation de récupération des mots de passe dans un coffre-fort sécurisé.

---

### Contrôle 10.7 — Pipeline de threat intelligence et journalisation pipeline FortiGate → SIEM complet

***CIS Ref :*** *7.3.2 (étendu)* | ***MITRE :*** *T1562.006, T1070.002* | ***Niveau :*** 🔵 *L2*

**Description du risque**

La mise en place d’un pipeline de journalisation complet FortiGate → FortiAnalyzer → SIEM avec des flux de threat intelligence intégrés permet de corréler automatiquement les événements réseau avec des indicateurs de compromission (IOC) en temps réel. Sans ce pipeline, la détection d’intrusions sophistiquées repose sur une analyse manuelle des logs, insuffisante face aux APT modernes.

**Architecture de pipeline recommandée :**

```
Internet
    ↓
[FortiGate]
    ├─→ [logs TCP/TLS] → FortiAnalyzer → FortiSIEM
    ├─→ [syslog CEF TLS:6514] → Splunk / QRadar / Elastic
    └─→ [STIX/TAXII + IOC] → FortiGuard / threat feeds externes
```

**Impact potentiel**

- Absence de corrélation entre événements réseau et IOC connus sans pipeline intégré
- Détection tardive d'APT sans threat intelligence temps réel
- Logs fragmentés sur plusieurs systèmes sans timeline cohérente pour l'investigation

**Navigation**

```
Log & Report > Log Settings
→ Configurer à la fois FortiAnalyzer ET Syslog (SIEM) pour redondance
→ Security Fabric > External Connectors
→ Ajouter des flux de threat intelligence externes
```

**Remédiation — Configuration complète du pipeline**

**Étape 1 — Configurer la transmission FortiAnalyzer (principal) :**

```
config log fortianalyzer setting
    set status enable
    set server "<IP_FortiAnalyzer>"
    set reliable enable
    set enc-algorithm high
    set ssl-min-proto-version tlsv1-2
    set certificate "FortiGate_CA"
    set conn-timeout 10
    set monitor-keepalive-period 5
    set monitor-failure-retry-period 5
    set upload-option realtime
end
```

**Étape 2 — Configurer le syslog CEF vers SIEM (en parallèle) :**

```
config log syslogd setting
    set status enable
    set server "siem.company.com"
    set reliable enable
    set port 6514
    set enc-algorithm high
    set certificate "<cert_SIEM>"
    set mode reliable
    set facility local7
    set format cef
end
```

**Étape 3 — Vérifier que toutes les catégories de logs sont transmises :**

```
# Vérifier le filtre de logs FortiAnalyzer
config log fortianalyzer filter
    set severity information
    set forward-traffic enable
    set local-traffic enable
    set multicast-traffic enable
    set sniffer-traffic disable
    set anomaly enable
    set voip enable
    set dns enable
    set ssh enable
end

# Vérifier le filtre de logs Syslog
config log syslogd filter
    set severity information
    set forward-traffic enable
    set local-traffic enable
    set anomaly enable
    set dns enable
end
```

**Étape 4 — Tests de validation du pipeline :**

```
# Test envoi de log vers FortiAnalyzer
diagnose log test

# Vérifier la liste des équipements connectés à FortiAnalyzer
execute log filter device fortianalyzer

# Test envoi vers syslogd
diagnose test application syslogd 3

# Vérifier le statut FMGD (processus de communication FortiAnalyzer)
diagnose test application fmgd 5
```

**Valeur par défaut :** Ni FortiAnalyzer ni syslog configurés par défaut. Aucun pipeline de threat intelligence intégré par défaut.

**Critère de conformité :** FortiAnalyzer ET syslog SIEM configurés en parallèle (redondance). Format CEF activé pour le syslog SIEM. Toutes les catégories critiques (forward-traffic, local-traffic, anomaly, dns) transmises vers les deux destinations. Tests de validation `diagnose log test` réussis. Pipeline documenté dans l'architecture de sécurité de l'organisation.

---

# Réponse à incident

## Indicateurs de compromission FortiGate

| INDICATEUR | SIGNIFICATION | ACTION IMMÉDIATE |
|---|---|---|
| Connexions administratives depuis des IP inconnues | Accès non autorisé ou credential compromis | Bloquer l'IP source via Local-in Policy, révoquer la session, changer tous les mots de passe |
| Modification de politiques de sécurité non planifiée | Manipulation de configuration (backdoor) | Restaurer la sauvegarde, audit complet des changements, investigation forensique |
| Logs IPS : détection d'exploits FortiOS (CVE récents) | Tentative d'exploitation du FortiGate lui-même | Isoler l'équipement, appliquer le patch immédiatement, analyser les IOC |
| Trafic sortant vers des IP de la liste CISA KEV | Hôte interne compromis communicant avec C2 | Isoler l'hôte via Security Fabric Quarantine, analyser le poste avec EDR |
| SSL-VPN : authentifications multiples depuis des IP distantes | Credential stuffing ou phishing VPN | Forcer MFA, bloquer les IP sources, analyser les logs VPN |
| Augmentation anormale du volume de logs IPS | Scan interne ou propagation de malware | Identifier la source, isoler le segment concerné, analyser les hôtes suspects |
| Suppression ou désactivation de règles de journalisation | Tentative d'effacement de traces post-compromission | Restaurer la configuration, considérer l'équipement comme compromis |
| Comptes administrateurs créés sans planification | Backdoor administrative créée par un attaquant | Supprimer le compte, revue complète de la configuration, analyse forensique |
| Authentifications SAML/SSO inhabituelles ou depuis des IP inconnues | Exploitation possible de CVE-2026-24858 ou CVE-2025-59718/59719 | Désactiver SAML, patcher immédiatement, auditer tous les comptes admin |
| Symlinks dans les répertoires SSL-VPN ( `/data/etc/ssl/` ) | Technique de persistance post-exploitation documentée CISA Avril 2025 | Supprimer les symlinks, réinitialiser FortiOS, considérer la compromission confirmée |
| Processus inconnus dans `diagnose sys top` | Implant ou backdoor potentiel sur le FortiGate | Isoler l'équipement, contacter PSIRT Fortinet, démarrer investigation forensique |

## Vérification post-exploitation — Advisory CISA Avril 2025

> ***Contexte :*** *En Avril 2025, Fortinet et CISA ont publié un advisory conjoint documentant une nouvelle technique de persistance post-exploitation. Même après l'application d'un patch corrective d'une CVE connue, des attaquants peuvent avoir déposé des backdoors persistantes. Cette vérification doit être effectuée sur tout FortiGate ayant été exposé avec une version vulnérable.*

### Étape 1 : Vérifier les comptes administrateurs non autorisés

```
# Lister tous les comptes administrateurs
show system admin

# Vérifier les comptes avec des profils élevés
show system admin | grep -e "accprofile" -e "super_admin"

# Rechercher les comptes créés récemment (comparer avec la liste approuvée)
diagnose sys admin list
```

**Indicateur de compromission :** Tout compte administrateur non répertorié dans la liste approuvée de l'organisation.

### Étape 2 : Vérifier les symlinks de persistance SSL-VPN

```
# Vérifier les fichiers dans les répertoires SSL-VPN
diagnose sys mount | grep ssl

# Lister les fichiers dans le répertoire webroot SSL-VPN
execute ls /data/etc/ssl/
execute ls /var/www/sslvpn/

# Rechercher les symlinks suspects (liens symboliques non attendus)
diagnose sys mount list
```

**Indicateur de compromission :** Présence de fichiers ou symlinks inattendus dans les répertoires SSL-VPN, notamment des liens vers `/` (racine du système de fichiers), permettant à un attaquant d'accéder à l'ensemble du système de fichiers via le portail SSL-VPN.

### Étape 3 : Analyser les logs SSL-VPN pour les authentifications anormales

```
# Filtrer les logs d'authentification SSL-VPN
execute log filter category 1
execute log filter field user
execute log display

# Rechercher les authentifications depuis des IP inhabituelles
diagnose log test
execute log fortianalyzer-test

# Analyser les sessions SSL-VPN actives et passées
diagnose vpn ssl list
diagnose vpn ssl statistics
```

**Indicateur de compromission :** Authentifications depuis des IP inconnues, des horaires inhabituels, ou des volumes anormaux de tentatives.

### Étape 4 : Vérifier les processus et l'intégrité du système

```
# Lister les processus en cours d'exécution
diagnose sys top

# Vérifier la consommation CPU/mémoire anormale
diagnose hardware deviceinfo disk
diagnose sys memory status

# Vérifier les connexions réseau actives depuis le FortiGate lui-même
diagnose ip address list
diagnose netlink neighbor list
```

**Indicateur de compromission :** Processus inconnus dans `diagnose sys top`, connexions sortantes vers des IP non attendues, consommation CPU anormale au repos.

### Étape 5 : Commandes forensiques avancées

```
# Vérifier les tâches planifiées (potential backdoor persistence)
show system automation-stitch
show system automation-trigger

# Vérifier les scripts personnalisés
show system replacemsg

# Extraire les logs pour analyse externe
execute log filter start-line 1
execute log filter max-checklines 1000
execute log display

# Vérifier l'intégrité des politiques critiques
show firewall policy
show vpn ssl settings
show system admin
show system global
```

---

## Commandes de Threat Hunting FortiGate

*Ces commandes permettent une investigation forensique active sur le FortiGate pour détecter des activités malveillantes en cours ou des traces d'exploitation passée. À utiliser dans le cadre d'une réponse à incident ou d'une chasse aux menaces proactive.*

### Identification des transferts de données suspects (exfiltration potentielle)

```
# Identifier les grands transferts de données depuis une IP suspecte
execute log filter field srcip <ip_suspecte>
execute log filter field action accept
execute log display

# Analyser les volumes par session (flux > 100 MB sortants)
diagnose sys session list | grep -e proto -e bytes
```

### Audit des connexions administratives récentes

```
# Vérifier les connexions administratives des dernières 24 heures
execute log filter field logid 0100032003
execute log filter time-period one-day
execute log display
# LogID 0100032003 = événements d'authentification admin
```

### Analyse des connexions sortantes inhabituelles depuis le FortiGate lui-même

```
# Inspecter en temps réel le trafic vers une IP externe suspecte
diagnose sniffer packet any "host <ip_externe_suspecte>" 4
# Le chiffre "4" = niveau de verbosité (4 = avec headers IP et TCP complets)
```

### Détection des modifications de configuration non autorisées

```
# Vérifier le statut de synchronisation de la configuration
diagnose debug fscd stats

# Vérifier si la configuration a été modifiée récemment
get system config-status
# Inspecter le checksum de configuration et la date de dernière modification
```

### Identification des flux à haute bande passante (canaux d'exfiltration)

```
# Lister les interfaces et leurs statistiques de trafic
diagnose netlink ifconfig list

# Vérifier les routes actives (routes injectées suspectes)
diagnose ip route list
```

### Audit des sessions VPN actives (connexions anormales)

```
# Lister tous les tunnels IPsec actifs (vérifier les peers inattendus)
diagnose vpn tunnel list

# Résumé des tunnels IPsec par statut
get vpn ipsec tunnel summary

# Lister les sessions SSL-VPN actives (IP source, utilisateur, durée)
diagnose vpn ssl list
```

### Vérification de la communication FortiGuard (intégrité des mises à jour)

```
# Lister les serveurs FortiGuard Distribution Service configurés
diagnose fdsv2 svr list

# Vérifier les informations de service FortiGuard
diagnose fdsv2 service-info
# Détecter une redirection des mises à jour vers un serveur malveillant
```

### Corrélation SIEM — requêtes de chasse recommandées

| REQUÊTE | OBJECTIF | SOURCE LOG |
|---|---|---|
| | Admin depuis IP non autorisée | Event logs |

| REQUÊTE | OBJECTIF | SOURCE LOG |
|---|---|---|
| `logid=0100032003 AND srcip NOT IN [subnet_management]` | | |
| `logid=0100032001 AND status=failed` | Tentatives de connexion admin échouées | Event logs |
| `action=accept AND bytes_sent > 100000000` | Transferts > 100 Mo (exfiltration) | Traffic logs |
| `utm-subtype=botnet-c2 OR dns_category=64` | Communication C2 détectée | UTM/DNS logs |
| `type=event AND subtype=vpn AND action=ssl-new-con` | Nouvelles sessions SSL-VPN | VPN event logs |
| `type=traffic AND srcip=<FortiGate_IP>` | Trafic sortant depuis le FW lui-même | Local traffic |
| `type=event AND subtype=system AND action=config-change` | Modifications de configuration | System event logs |

## Procédure d'isolation d'urgence FortiGate

```
# 1. Capturer l'état courant avant toute intervention
execute backup config ftp <ip_ftp_securise> <nom_fichier_backup>
get system status
show full-configuration

# 2. Identifier les sessions administratives actives suspectes
get system session-list | grep admin
diagnose sys session list

# 3. Terminer les sessions suspectes
diagnose sys session clear
execute disconnect-admin-session <session_id>

# 4. Bloquer les accès depuis des IP suspectes via Local-in Policy
config firewall local-in-policy
    edit 999
        set intf "any"
        set srcaddr "<IP_suspecte>"
        set dstaddr "all"
        set action deny
        set schedule "always"
        set service "ALL"
    next
end

# 5. Changer tous les mots de passe administrateurs immédiatement
config system admin
    edit "<nom_admin>"
        set password <nouveau_mot_de_passe_fort>
    next
end

# 6. Extraire les logs pour investigation forensique
execute log fortianalyzer-test
diagnose log test
execute log display

# 7. Vérifier l'intégrité des politiques de sécurité critiques
show firewall policy
show vpn ipsec phase1-interface
show vpn ssl settings

# 8. Vérifier les comptes administrateurs (présence de backdoors)
show system admin

# 9. Vérifier les symlinks SSL-VPN (technique de persistance CISA Avril 2025)
execute ls /data/etc/ssl/
diagnose sys mount list

# 10. Notifier le SOC et déclencher la procédure de réponse à incident
# Contact CERT Fortinet : psirt@fortinet.com
# CISA : https://www.cisa.gov/report
```

## Checklist de réponse rapide (15 premières minutes)

- ☐ Documenter l'heure de détection et la nature de l'incident
- ☐ Capturer la configuration et les logs avant toute modification
- ☐ Identifier si le FortiGate lui-même est compromis ou s'il détecte une compromission réseau
- ☐ Notifier le RSSI et le SOC
- ☐ Isoler les systèmes internes suspects via Security Fabric Quarantine
- ☐ **Vérifier les comptes administrateurs** (backdoors éventuelles — créés par l'attaquant)
- ☐ **Vérifier les symlinks dans les répertoires SSL-VPN** (persistance post-exploitation CISA Avril 2025)
- ☐ **Analyser les logs SSL-VPN** pour des authentifications anormales (IP inconnues, horaires inhabituels)
- ☐ **Vérifier les processus actifs** avec `diagnose sys top` (implants potentiels)
- ☐ Appliquer les patches disponibles si l'incident implique une CVE connue
- ☐ Désactiver SAML/SSO si CVE-2026-24858 ou CVE-2025-59718/59719 potentiellement exploitées
- ☐ Conserver les preuves (logs, captures, configurations) pour l'investigation
- ☐ Contacter PSIRT Fortinet si compromission confirmée (psirt@fortinet.com)

## Références


- Fortinet PSIRT — Security Advisories
- Fortinet Hardening Guide FortiOS 7.4
- CIS Benchmark for FortiGate 7.4.x v1.0.1
- MITRE ATT&CK — Network Devices
- ANSSI — Recommandations pour choisir des pare-feux maîtrisés
- ANSSI — Recommandations de sécurité pour l'architecture d'un SI
- CISA Known Exploited Vulnerabilities — FortiGate
- CISA Advisory AA25-087A — FortiGate Post-Exploitation (Avril 2025)
- NIST SP 800-41 Rev. 1 — Guidelines on Firewalls and Firewall Policy
- Fortinet Documentation FortiOS 7.4
- Fortinet CLI Reference FortiOS 7.4
- Fortinet Upgrade Tool
- PCI-DSS v4.0 — Requirement 10 (Logging)
- NIS2 Directive — Article 21 (Cybersecurity measures)
- DORA — Digital Operational Resilience Act (Règlement UE 2022/2554, en vigueur janvier 2025) — Art.9 : gestion des risques TIC (hardening pare-feu) ; Art.10 : continuité opérationnelle numérique (HA hardening) ; Art.11 : gestion des incidents (journalisation/SIEM)

- CVE-2026-24858 — NVD NIST
- CVE-2024-21762 — NVD NIST
- CVE-2023-27997 — NVD NIST
- Fortinet Community — Hardening Best Practices

---

## ANNEXE — Checklists de vérification rapide

*Checklists condensées pour audit terrain et conformité. Chaque ligne = un contrôle actionnable vérifiable en moins de 2 minutes.*

### Domaine 1 — Firmware et mises à jour

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 1.1 | FortiOS à jour (dernière version GA) — aucune CVE CISA KEV active | 🔴 CRITIQUE | `get system status` | ☐ |
| 1.2 | Clés TLS statiques désactivées, strong-crypto enable, dh-params ≥ 2048 | 🔵 L2 | `get system global \| grep -e ssl-static -e strong-crypto -e dh-params` | ☐ |
| 1.3 | Mises à jour FortiGuard automatiques ≤ 1h | 🟢 L1 | `show system autoupdate schedule` | ☐ |
| 1.4 | Auto-install USB désactivé + private-data-encryption enable | 🔵 L2 | `config system auto-install / get` | ☐ |

### Domaine 2 — Authentification et accès administrateur

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 2.1 | Compte “admin” par défaut supprimé | 🔴 CRITIQUE | `show system admin` | ☐ |

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 2.2 | Politique de mots de passe activée (min 14 car.) + private-data-encryption | 🟢 L1 | `get system password-policy` | ☐ |
| 2.3 | Trusted Hosts configurés pour tous les admins | 🟠 ÉLEVÉ | `show system admin` | ☐ |
| 2.4 | Idle timeout ≤ 10 minutes | 🟢 L1 | `get system global \| grep admintimeout` | ☐ |
| 2.5 | Telnet et HTTP désactivés — SCP pour transferts | 🟢 L1 | `get system global \| grep admin-` | ☐ |
| 2.6 | SNMPv3 uniquement (pas de v1/v2c) | 🟢 L1 | `config system snmp community / show` | ☐ |
| 2.7 | Bannières pré/post-login activées | 🟢 L1 | `get system global \| grep login-banner` | ☐ |
| 2.8 | MFA activé pour tous les admins (FortiToken/ FortiAuthenticator) | 🟠 ÉLEVÉ | `show system admin \| grep two-factor` | ☐ |

## Domaine 3 — Interface de gestion

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 3.1 | Aucun accès management sur interface WAN | 🔴 CRITIQUE | `show system interface wan1` | ☐ |
| 3.2 | Telnet désactivé sur toutes les interfaces | 🟢 L1 | `show system interface` | ☐ |
| 3.3 | Certificat TLS valide pour HTTPS admin | 🟡 MOYEN | `get system global \| grep admin-server-cert` | ☐ |
| 3.4 | Local-in Policies management avec journalisation forensique | 🟠 ÉLEVÉ | `show firewall local-in-policy` | ☐ |
| 3.5 | | 🟢 L1 | `get system global \| grep ssl-versions` | ☐ |

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| | TLS 1.2+ uniquement pour management | | | |
| 3.6 | SAML/SSO désactivé si non utilisé — CVE-2026-24858 patchée | 🔴 CRITIQUE | `get system saml` | ☐ |
| 3.7 | Restrictions géographiques GeoIP pour management | 🔵 L2 | `show firewall local-in-policy` | ☐ |
| 3.8 | REST API : comptes dédiés, trusted hosts, profil minimal, rotation trimestrielle | 🟠 ÉLEVÉ | `show system api-user` | ☐ |

## Domaine 4 — Politiques de sécurité

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 4.1 | Intra-zone traffic bloqué | 🟢 L1 | `show system zone` | ☐ |
| 4.2 | Aucune règle avec service “ALL” | 🟠 ÉLEVÉ | `show firewall policy \| grep service` | ☐ |
| 4.3 | Blocage ISDB Tor/Malicious activé | 🟠 ÉLEVÉ | `show firewall policy` | ☐ |
| 4.4 | Journalisation activée sur toutes les politiques | 🟢 L1 | `show firewall policy \| grep logtraffic` | ☐ |
| 4.5 | Revue des règles inutilisées (< 90j) | 🟡 MOYEN | Audit manuel dans Policy & Objects | ☐ |
| 4.6 | Virtual Patching pour CVE non patchées | 🟡 MOYEN | `show firewall local-in-policy` | ☐ |
| 4.7 | Zero Trust Quick Start : aucune règle | 🔵 L2 | `show firewall policy \| grep srcaddr` + `diagnose security-rating result` | ☐ |

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| | any→any, User-ID, profils 100%, zones segmentées, Score SR ≥ 80 | | | |

## Domaine 5 — Profils de sécurité

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 5.1 | Profil IPS en mode block pour critiques/élevés | 🟠 ÉLEVÉ | `show ips sensor` | ☐ |
| 5.2 | Profil AV avec heuristique et Outbreak Prevention | 🟠 ÉLEVÉ | `show antivirus profile` | ☐ |
| 5.3 | DNS Filter FortiGuard — blocage C2/Botnet/Phishing + block-botnet enable | 🟠 ÉLEVÉ | `show dnsfilter profile` | ☐ |
| 5.4 | Web Filter avec blocage catégories malveillantes | 🟡 MOYEN | `show webfilter profile` | ☐ |
| 5.5 | App Control — P2P et proxies bloqués | 🟡 MOYEN | `show application list` | ☐ |
| 5.6 | DLP configuré pour données sensibles | 🔵 L2 | `show dlp sensor` | ☐ |
| 5.7 | ANSSI double-barrière : interface MGMT dédiée + default-deny + ECDHE seul | 🔵 L2 | `show system interface mgmt` + `get system settings` | ☐ |

## Domaine 6 — Security Fabric et FortiGuard

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 6.1 | Security Fabric activé — upstream-ip restrictif (pas 0.0.0.0) | 🟡 MOYEN | `show system csf` | ☐ |
| 6.2 | Quarantaine automatique hôtes compromis | 🔵 L2 | `show system automation-stitch` | ☐ |
| 6.3 | Security Rating ≥ 80/100, planifié quotidiennement, rapport mensuel PDF/CSV | ⚪ INFO | `diagnose security-rating summary` + `diagnose system csf check` | ☐ |
| 6.4 | Test de pénétration annuel planifié | 🔵 L2 | Processus documenté | ☐ |
| 6.5 | Flux threat intelligence externes (IP/domaine) via External Connectors, refresh ≤ 60 min | 🔵 L2 | `show system external-resource` | ☐ |

## Domaine 7 — VPN

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 7.1 | SSL-VPN : TLS 1.2+ uniquement — CVE-2023-27997 et CVE-2024-21762 patchées | 🟠 ÉLEVÉ | `show vpn ssl settings \| grep tlsv` | ☐ |
| 7.2 | IPsec : IKEv2 uniquement, pas de mode agressif | 🟠 ÉLEVÉ | `show vpn ipsec phase1-interface` | ☐ |
| 7.3 | Certificat signé pour portail SSL-VPN | 🟢 L1 | `show vpn ssl settings \| grep servercert` | ☐ |
| 7.4 | MFA obligatoire pour utilisateurs VPN | 🟠 ÉLEVÉ | `show user local \| grep two-factor` | ☐ |

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 7.5 | Split tunneling restreint ou désactivé | 🔵 L2 | `show vpn ssl web portal` | ☐ |
| 7.6 | ZTNA déployé ou plan migration SSL-VPN→ZTNA documenté + tags posture EMS | 🔵 L2 | `show firewall ztna-server` + `show endpoint-control server` | ☐ |
| 7.7 | FortiClient EMS connecté — tags conformité (OS patch, AV, BitLocker) dans politiques | 🔵 L2 | `show endpoint-control fctems` + `diagnose endpoint-control server status` | ☐ |

## Domaine 8 — Inspection SSL/TLS et certificats

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 8.1 | Deep inspection activée et appliquée | 🟡 MOYEN | `show firewall ssl-ssh-profile` | ☐ |
| 8.2 | CA d'inspection dédié (non Fortinet par défaut) | 🟡 MOYEN | `show system certificate ca` | ☐ |
| 8.3 | Exemptions SSL documentées et minimales | 🔵 L2 | `show firewall ssl-ssh-profile \| grep exempt` | ☐ |
| 8.4 | Certificats management/VPN signés PKI, OCSP activé, CRL configurée, monitoring expiration | 🟢 L1 | `get vpn certificate local` + `show vpn certificate setting \| grep ocsp` | ☐ |

## Domaine 9 — Réseau, segmentation et HA

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 9.1 | DNS de confiance configuré (DoT activé) | 🟢 L1 | `show system dns` | ☐ |
| 9.2 | NTP authentifié configuré — 2+ serveurs, auth enable (anti T1070) | 🟢 L1 | `diagnose sys ntp status` | ☐ |
| 9.3 | IPv6 désactivé si non utilisé | 🔵 L2 | `get system global \| grep ipv6` | ☐ |
| 9.4 | Zones LAN/WAN/DMZ segmentées | 🟢 L1 | `show system zone` | ☐ |
| 9.5 | Protection DoS ASIC (NP6/NP7) — phase monitor puis block, 6 anomalies | 🟡 MOYEN | `show firewall DoS-policy` | ☐ |
| 9.6 | OSPF/BGP : authentification MD5 sur toutes les interfaces routage dynamique | 🔵 L2 | `show router ospf \| grep auth` | ☐ |
| 9.7 | HA : mot de passe heartbeat, interfaces dédiées, override disable, interfaces monitorées | 🟠 ÉLEVÉ | `show system ha` + `get system ha status` | ☐ |
| 9.8 | SD-WAN : profils sécurité sur politiques virtual-wan-link, health checks SLA, logging implicite | 🔵 L2 | `show system sdwan` + `diagnose sys sdwan member` | ☐ |

## Domaine 10 — Journalisation et SIEM

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| 10.1 | Event Logging activé — toutes catégories (system, admin, user, VPN, HA, DHCP, compliance) | 🟢 L1 | `show log eventfilter` | ☐ |
| 10.2 | Syslog CEF vers SIEM externe — TCP/TLS port 6514, mode reliable, format cef | 🟠 ÉLEVÉ | `show log syslogd setting` | ☐ |
| 10.3 | FortiAnalyzer configuré — TLS, mode reliable, certificat auth, keepalive | 🟡 MOYEN | `show log fortianalyzer setting` | ☐ |
| 10.4 | Rétention logs ≥ 90 jours en ligne, ≥ 365 jours archive | 🟢 L1 | Vérifier sur SIEM/FortiAnalyzer | ☐ |
| 10.5 | Alertes critiques configurées (SOC) | 🟡 MOYEN | `show alertemail setting` | ☐ |
| 10.6 | FortiAnalyzer durci — lockout 2 essais / 120s, TLS 1.2 high, comptes nominatifs MFA, derrière FortiGate | 🟠 ÉLEVÉ | Sur FortiAnalyzer : `config system global / get` | ☐ |
| 10.7 | Pipeline logs complet FortiGate → FortiAnalyzer + SIEM (CEF) validé | 🔵 L2 | `diagnose log test` + `diagnose test application fmgd 5` | ☐ |

| # | CONTRÔLE | NIVEAU | COMMANDE DE VÉRIFICATION | STATUT |
|---|---|---|---|---|
| | ( `diagnose log test` ) | | | |

## Checklist Réponse à Incident — Vérification Post-Exploitation (CISA Avril 2025)

| # | VÉRIFICATION | COMMANDE | INDICATEUR DE COMPROMISSION |
|---|---|---|---|
| RI.1 | Comptes admin non autorisés | `show system admin` | Comptes non répertoriés dans la liste approuvée |
| RI.2 | Symlinks SSL-VPN persistants | `execute ls /data/etc/ssl/` | Liens symboliques inattendus |
| RI.3 | Authentifications SSL-VPN anormales | `diagnose vpn ssl list` | IP inconnues, horaires inhabituels |
| RI.4 | Processus inconnus | `diagnose sys top` | Processus non standard ou consommation CPU anormale |
| RI.5 | Automation backdoor | `show system automation-stitch` | Stitch non planifiés ou modifiés |
| RI.6 | Config SAML suspecte | `get system saml` | SAML activé avec IdP inconnu |
| RI.7 | Sessions admin actives | `diagnose sys session list` | Sessions depuis IP non autorisées |

## Tableau récapitulatif par domaine

| DOMAINE | CONTRÔLES | CRITIQUE | ÉLEVÉ | MOYEN | L1 | L2 | INFO |
|---|---|---|---|---|---|---|---|
| D1 — Firmware | 4 | 1 | 0 | 0 | 1 | 2 | 0 |
| D2 — Auth | 8 | 2 | 2 | 0 | 3 | 0 | 1 |
| D3 — Interface mgmt + API | 8 | 2 | 2 | 1 | 2 | 2 | 0 |
| D4 — Politiques + ZT | 7 | 0 | 2 | 2 | 2 | 1 | 0 |
| | 7 | 0 | 3 | 2 | 0 | 2 | 0 |

| DOMAINE | CONTRÔLES | CRITIQUE | ÉLEVÉ | MOYEN | L1 | L2 | INFO |
|---|---|---|---|---|---|---|---|
| D5 — Profils UTM | | | | | | | |
| D6 — Security Fabric | 5 | 0 | 0 | 1 | 0 | 3 | 1 |
| D7 — VPN + ZTNA + EMS | 7 | 0 | 3 | 0 | 1 | 3 | 0 |
| D8 — SSL/ TLS + Certificats | 4 | 0 | 0 | 2 | 1 | 1 | 0 |
| D9 — Réseau + HA + SD-WAN | 8 | 0 | 1 | 1 | 2 | 4 | 0 |
| D10 — Logs/ SIEM | 7 | 0 | 3 | 2 | 2 | 1 | 0 |
| **TOTAL** | **65** | **5** | **16** | **11** | **14** | **19** | **2** |

***Note :*** *7 contrôles de vérification forensique (RI.1 à RI.7) dans la section Réponse à Incident ne sont pas comptés dans les domaines principaux. Total contrôles avec RI forensiques :* ***72****. Ce total de 65 contrôles principaux numérotés est enrichi sur 5 passages depuis la version initiale. Ajouts du cinquième passage (version 1.5) : contrôle 4.7 Zero Trust Quick Start, commandes de threat hunting (section Réponse à Incident), tableau de conformité multi-référentiels (CIS Controls v8, NIS2 Art.21, ISO 27001:2022, PCI DSS v4, RGPD Art.32, DORA Art.9). Les métadonnées ITEMS (83) incluent les contrôles de l'ANNEXE RI, les contrôles du tableau de conformité et plusieurs contrôles CIS L1/L2 sous-jacents enrichis dans chaque domaine.*

## Mapping MITRE ATT&CK complet

| TECHNIQUE | ID | CONTRÔLES COUVRANTS |
|---|---|---|
| Exploit Public-Facing Application | T1190 | 1.1, 3.1, 4.6, 6.4, 9.5 |
| Valid Accounts | T1078 | 2.1, 2.3, 2.8, 3.4, 3.6, **7.7** |
| Local Accounts (API tokens) | **T1078.003** | **3.8** |
| Brute Force | T1110 | 2.2, 2.4, 2.8 |
| External Remote Services | T1133 | 2.3, 7.1, 7.4, **7.6** |
| Adversary-in-the-Middle | T1557 | 1.2, 2.5, 3.3, 8.1, **8.4** |

| TECHNIQUE | ID | CONTRÔLES COUVRANTS |
|---|---|---|
| Subvert Trust Controls | **T1553** | **8.4** |
| Unsecured Credentials | **T1552** | **3.8** |
| Weaken Encryption | T1600 | 1.2, **5.7** |
| Modify System Image | T1601 | 1.1, 1.4 |
| Network Device Config Dump | T1602.002 | 3.4 |
| Network Denial of Service | T1498 | **9.5** |
| Service Denial (HA disruption) | **T1499** | **9.7** |
| Hardware Additions (rogue HA node) | **T1200** | **9.7** |
| Impair Defenses | T1562 | 6.1, 10.1, 10.5 |
| Indicator Blocking (disable logging) | **T1562.006** | **10.1, 10.2, 10.6** |
| Exfiltration over Web Service | T1048 | 4.2, 5.6, 8.3 |
| Application Layer Protocol (DNS) | T1071.004 | **5.3**, 9.1 |
| Application Layer Protocol (C2) | T1071 | **6.5** |
| Forge Web Credentials | T1606 | 3.6 |
| Lateral Movement | T1021 | 4.1, 9.4 |
| Command and Control | T1090 | 4.3, 5.5 |
| Indicator Removal (timestamps) | T1070 | **9.2** |
| Clear Linux or Mac System Logs | **T1070.002** | **10.2, 10.3, 10.6** |
| Data from Local System (log exfil) | **T1005** | **10.2, 10.6** |
| Network Boundary Bridging | T1599 | **9.6, 9.8** |
| Phishing | T1566 | **6.5**, 5.3, 5.4 |

## Tableau de correspondance avec les référentiels de conformité

*Ce tableau met en correspondance les principaux contrôles FortiGate avec les référentiels réglementaires et de sécurité applicables aux organisations françaises et européennes. Utiliser ce tableau pour justifier les contrôles implémentés lors d'audits de conformité.*

### Abréviations des référentiels

| RÉFÉRENTIEL | DESCRIPTION | APPLICABILITÉ |
|---|---|---|
| **CIS Controls v8** | Center for Internet Security Controls version 8 | Toutes organisations |
| **NIS2 Art.21** | Directive NIS2 (EU 2022/2555) — Mesures de gestion des risques | Opérateurs essentiels/importants UE |
| **ISO 27001:2022** | Annexe A — Contrôles de sécurité de l'information | Organisations certifiées ISO 27001 |
| **PCI DSS v4** | Payment Card Industry Data Security Standard v4.0 | Organisations traitant des paiements par carte |
| **RGPD Art.32** | Règlement Général sur la Protection des Données — Mesures techniques | Toutes organisations traitant données personnelles UE |
| **DORA Art.9** | Digital Operational Resilience Act (EU 2022/2554) — ICT Risk Management | Entités financières UE (en vigueur janvier 2025) |

### Table de correspondance contrôles FortiGate — référentiels

| CONTRÔLE FORTIGATE | N° CONTRÔLE | CIS CONTROLS V8 | NIS2 ART.21 | ISO 27001:2022 | PCI DSS V4 | RGPD ART.32 | DORA ART.9 |
|---|---|---|---|---|---|---|---|
| Mise à jour firmware FortiOS | 1.1 | CIS 7.3 | ✓ | A.8.8 | Req 6.3.3 | ✓ | ✓ |
| Clés TLS statiques / PFS | 1.2 | CIS 3.10 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |
| Mises à jour FortiGuard | 1.3 | CIS 7.3 | ✓ | A.8.8 | Req 6.3.3 | ✓ | ✓ |
| Auto-install USB désactivé | 1.4 | CIS 4.6 | ✓ | A.8.1 | Req 12.3 | ✓ | — |
| Suppression compte admin défaut | 2.1 | CIS 5.3 | ✓ | A.9.2.3 | Req 8.2.2 | ✓ | ✓ |
| Politique mots de passe | 2.2 | CIS 5.2 | ✓ | A.9.4.3 | Req 8.3.6 | ✓ | ✓ |
| Trusted Hosts administrateurs | 2.3 | CIS 12.2 | ✓ | A.8.15 | Req 1.3.2 | ✓ | ✓ |
| Idle timeout ≤ 10 min | 2.4 | CIS 4.3 | ✓ | A.9.4.2 | Req 8.2.8 | ✓ | ✓ |
| Protocoles d'accès chiffrés | 2.5 | CIS 3.10 | ✓ | A.8.24 | Req 2.2.7 | ✓ | ✓ |

| CONTRÔLE FORTIGATE | N° CONTRÔLE | CIS CONTROLS V8 | NIS2 ART.21 | ISO 27001:2022 | PCI DSS V4 | RGPD ART.32 | DORA ART.9 |
|---|---|---|---|---|---|---|---|
| SNMPv3 uniquement | 2.6 | CIS 12.3 | ✓ | A.8.21 | Req 2.2.1 | ✓ | ✓ |
| Bannière de connexion | 2.7 | CIS 4.1 | ✓ | A.6.2.1 | Req 12.9 | ✓ | ✓ |
| MFA administrateurs | 2.8 | CIS 6.3 | ✓ | A.9.4.2 | Req 8.4.2 | ✓ | ✓ |
| Désactivation accès management WAN | 3.1 | CIS 12.2 | ✓ | A.8.20 | Req 1.3.2 | ✓ | ✓ |
| Restriction protocoles management | 3.2 | CIS 4.1 | ✓ | A.9.4.2 | Req 2.2.7 | ✓ | ✓ |
| Certificat TLS HTTPS admin | 3.3 | CIS 3.10 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |
| Trusted Hosts + Local-in Policy | 3.4 | CIS 12.2 | ✓ | A.8.15 | Req 1.3.2 | ✓ | ✓ |
| TLS 1.2+ pour management | 3.5 | CIS 3.10 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |
| Durcissement SAML/SSO | 3.6 | CIS 5.6 | ✓ | A.9.4.2 | Req 8.2.2 | ✓ | ✓ |
| Restrictions géographiques GeoIP | 3.7 | CIS 12.2 | ✓ | A.8.20 | Req 1.3.2 | ✓ | — |
| REST API hardening | 3.8 | CIS 5.3 | ✓ | A.9.2.3 | Req 8.2.2 | ✓ | ✓ |
| Blocage intra-zone | 4.1 | CIS 12.2 | ✓ | A.8.22 | Req 1.3.1 | ✓ | ✓ |
| Interdire service “ALL” | 4.2 | CIS 12.2 | ✓ | A.8.20 | Req 1.3.1 | ✓ | ✓ |
| Blocage ISDB Tor/Malicious | 4.3 | CIS 9.2 | ✓ | A.8.23 | Req 1.3.3 | ✓ | ✓ |
| Journalisation toutes politiques | 4.4 | CIS 8.5 | ✓ | A.8.15 | Req 10.2 | ✓ | ✓ |
| Nettoyage règles inutilisées | 4.5 | CIS 12.2 | ✓ | A.8.20 | Req 1.2.7 | ✓ | — |
| Virtual Patching | 4.6 | CIS 7.4 | ✓ | A.8.8 | | ✓ | ✓ |

| CONTRÔLE FORTIGATE | N° CONTRÔLE | CIS CONTROLS V8 | NIS2 ART.21 | ISO 27001:2022 | PCI DSS V4 | RGPD ART.32 | DORA ART.9 |
|---|---|---|---|---|---|---|---|
| | | | | | Req 6.3.3 | | |
| Zero Trust Quick Start | 4.7 | CIS 6.7 | ✓ | A.8.18 | Req 8.4.1 | ✓ | ✓ |
| Profil IPS en mode protection | 5.1 | CIS 13.4 | ✓ | A.8.16 | Req 6.4.1 | ✓ | ✓ |
| Profil AV (tous protocoles) | 5.2 | CIS 10.1 | ✓ | A.8.7 | Req 5.2.1 | ✓ | ✓ |
| DNS Filter (C2/ Botnet block) | 5.3 | CIS 9.2 | ✓ | A.8.23 | Req 1.3.3 | ✓ | ✓ |
| Web Filter catégories à risque | 5.4 | CIS 9.3 | ✓ | A.8.23 | Req 6.4.1 | ✓ | ✓ |
| Application Control P2P/ Proxy | 5.5 | CIS 2.5 | ✓ | A.8.28 | Req 6.4.1 | ✓ | ✓ |
| Data Loss Prevention (DLP) | 5.6 | CIS 3.14 | ✓ | A.8.12 | Req 3.4 | ✓ | ✓ |
| ANSSI double-barrière | 5.7 | CIS 12.2 | ✓ | A.8.22 | Req 1.3.1 | ✓ | ✓ |
| Security Fabric | 6.1 | CIS 13.1 | ✓ | A.8.16 | Req 10.7 | ✓ | ✓ |
| Quarantaine automatique | 6.2 | CIS 13.2 | ✓ | A.8.16 | Req 12.10 | ✓ | ✓ |
| Security Rating CSPM | 6.3 | CIS 1.1 | ✓ | A.5.36 | Req 12.3 | ✓ | ✓ |
| Tests de pénétration | 6.4 | CIS 18.1 | ✓ | A.8.8 | Req 11.4 | ✓ | ✓ |
| Flux threat intelligence | 6.5 | CIS 17.5 | ✓ | A.8.16 | Req 12.3 | ✓ | ✓ |
| SSL-VPN TLS 1.2+ | 7.1 | CIS 12.6 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |
| VPN IPsec IKEv2 | 7.2 | CIS 12.6 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |
| Certificat SSL-VPN signé | 7.3 | CIS 3.10 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |

| CONTRÔLE FORTIGATE | N° CONTRÔLE | CIS CONTROLS V8 | NIS2 ART.21 | ISO 27001:2022 | PCI DSS V4 | RGPD ART.32 | DORA ART.9 |
|---|---|---|---|---|---|---|---|
| MFA utilisateurs VPN | 7.4 | CIS 6.3 | ✓ | A.9.4.2 | Req 8.4.2 | ✓ | ✓ |
| Split tunneling restrictif | 7.5 | CIS 12.7 | ✓ | A.8.20 | Req 1.3.1 | ✓ | ✓ |
| ZTNA | 7.6 | CIS 6.7 | ✓ | A.8.18 | Req 8.4.1 | ✓ | ✓ |
| FortiClient EMS posture | 7.7 | CIS 6.5 | ✓ | A.8.19 | Req 12.3 | ✓ | ✓ |
| SSL/TLS Inspection deep | 8.1 | CIS 13.10 | ✓ | A.8.16 | Req 4.2.1 | ✓ | ✓ |
| CA dédié inspection SSL | 8.2 | CIS 3.10 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |
| Exemptions SSL limitées | 8.3 | CIS 13.10 | ✓ | A.8.16 | Req 4.2.1 | ✓ | ✓ |
| OCSP/CRL/ expiration certificats | 8.4 | CIS 3.10 | ✓ | A.8.24 | Req 4.2.1 | ✓ | ✓ |
| DNS sécurisé/ DoT | 9.1 | CIS 9.1 | ✓ | A.8.23 | Req 10.6.1 | ✓ | ✓ |
| NTP authentifié | 9.2 | CIS 8.4 | ✓ | A.8.17 | Req 10.6.1 | ✓ | ✓ |
| IPv6 désactivé si inutilisé | 9.3 | CIS 12.4 | ✓ | A.8.20 | Req 1.3.1 | — | — |
| Segmentation LAN/WAN/DMZ | 9.4 | CIS 12.2 | ✓ | A.8.22 | Req 1.3.1 | ✓ | ✓ |
| Protection DoS ASIC NP6/NP7 | 9.5 | CIS 13.9 | ✓ | A.8.16 | Req 6.4.2 | ✓ | ✓ |
| Auth routage OSPF/BGP | 9.6 | CIS 12.2 | ✓ | A.8.21 | Req 1.3.2 | ✓ | ✓ |
| HA hardening | 9.7 | CIS 11.3 | ✓ | A.17.2.1 | Req 12.4 | ✓ | ✓ |
| SD-WAN security | 9.8 | CIS 12.6 | ✓ | A.8.20 | Req 1.3.1 | ✓ | ✓ |
| Event Logging complet | 10.1 | CIS 8.2 | ✓ | A.8.15 | Req 10.2 | ✓ | ✓ |
| Syslog SIEM chiffré CEF | 10.2 | CIS 8.9 | ✓ | A.8.15 | Req 10.3 | ✓ | ✓ |

| CONTRÔLE FORTIGATE | N° CONTRÔLE | CIS CONTROLS V8 | NIS2 ART.21 | ISO 27001:2022 | PCI DSS V4 | RGPD ART.32 | DORA ART.9 |
|---|---|---|---|---|---|---|---|
| FortiAnalyzer chiffré fiable | 10.3 | CIS 8.9 | ✓ | A.8.15 | Req 10.3 | ✓ | ✓ |
| Rétention logs ≥ 90 jours | 10.4 | CIS 8.3 | ✓ | A.8.15 | Req 10.7 | ✓ | ✓ |
| Alertes événements critiques | 10.5 | CIS 8.11 | ✓ | A.8.16 | Req 12.10 | ✓ | ✓ |
| FortiAnalyzer hardening | 10.6 | CIS 8.9 | ✓ | A.8.15 | Req 10.3 | ✓ | ✓ |
| Pipeline threat intel/logs complet | 10.7 | CIS 17.5 | ✓ | A.8.16 | Req 12.3 | ✓ | ✓ |

### Note sur l'applicabilité DORA (Règlement UE 2022/2554)

> ***DORA — Digital Operational Resilience Act*** *est entré en vigueur le* ***17 janvier 2025****. Il s'applique aux entités financières de l'Union Européenne : banques, assurances, gestionnaires d'actifs, plateformes de négociation, et à leurs prestataires TIC tiers. Les contrôles FortiGate contribuent directement à :*
>
> - ***Article 9 — Gestion des risques TIC :*** *Le hardening du pare-feu (contrôles 1.1 à 9.8) constitue une mesure de protection et de prévention requise par l'Art.9(2).*
> - ***Article 10 — Continuité des activités :*** *Le HA hardening (contrôle 9.7) et la protection DoS (9.5) adressent les exigences de continuité opérationnelle numérique.*
> - ***Article 11 — Réponse et rétablissement :*** *La journalisation SIEM (contrôles 10.1–10.7), les alertes (10.5) et les procédures de réponse à incident documentées dans ce guide répondent aux exigences de gestion et de notification des incidents TIC.*
> - ***Article 28 — Risques liés aux tiers TIC :*** *La sécurisation des accès VPN et ZTNA (contrôles 7.1–7.7) couvre le risque de concentration sur des prestataires externes.*

### Note sur NIS2 Article 21 (Directive UE 2022/2555)

> *La Directive NIS2, transposée en droit français par la loi n° 2023-703 du 1er août 2023, impose aux opérateurs essentiels et importants des mesures de sécurité proportionnées aux risques. L'****Article 21*** *liste explicitement les mesures requises incluant : la sécurité des réseaux (contrôles D1–D9), la gestion des accès (D2–D3), la continuité (D9), la gestion des incidents (D10) et la sécurité de la chaîne d'approvisionnement. Ce benchmark couvre l'ensemble de ces exigences pour les équipements FortiGate.*

*Document généré par AYI NEDJIMI Consultants — https://ayinedjimi-consultants.fr Version 1.5 — Mai 2026 — Cinquième passage d'enrichissement : tableau de conformité multi-référentiels (CIS Controls v8, NIS2 Art.21, ISO 27001:2022, PCI DSS v4, RGPD Art.32, DORA Art.9), commandes forensiques de threat hunting (identification exfiltration, audit connexions admin, VPN, surveillance FortiGuard), contrôle 4.7 Zero Trust Quick Start, note DORA Art.9/10/11, note NIS2 Art.21. Version 1.4 — Quatrième passage d'enrichissement : REST API hardening (3.8 : tokens dédiés, trusted hosts, rotation trimestrielle), FortiClient EMS endpoint compliance (7.7 : posture check Zero Trust, tags conformité), gestion cycle de vie certificats (8.4 : OCSP/CRL, monitoring expiration), High Availability hardening (9.7 : mot de passe heartbeat, interfaces dédiées, override disable, checksums HA), SD-WAN security (9.8 : profils sécurité sur virtual-wan-link, health checks SLA, logging implicite), nouveaux mappings MITRE T1499/T1200/T1553/T1552/T1078.003/T1599 Basé sur le CIS FortiGate 7.4.x Benchmark v1.0.1 (janvier 2026) Sources : Fortinet PSIRT, CISA KEV, ANSSI, MITRE ATT&CK v15, NIST SP 800-41, CIS Controls v8, NIS2/DORA EUR-Lex Classification : CONFIDENTIEL — Usage interne uniquement*