BENCHMARK DE DURCISSEMENT PALO ALTO NGFW 2026

🔥 AYI NEDJIMI CONSULTANTS (ANC)

Version : 4.1 — Mai 2026 **Applicabilité :** Palo Alto PA-Series, VM-Series — PAN-OS 10.x, 11.x, 12.x
Classification : CONFIDENTIEL **Auteur :** AYI NEDJIMI Consultants — https://ayinedjimi-consultants.fr

---

Conventions et niveaux de criticité

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

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

Table des matières

1. Domaine 1 — Gestion du firmware et mises à jour
2. Domaine 2 — Authentification et accès administrateur
3. Domaine 3 — Sécurisation de l'interface de gestion
4. Domaine 4 — Zones et politiques de sécurité
5. Domaine 5 — App-ID et User-ID
6. Domaine 6 — Threat Prevention et WildFire
7. Domaine 7 — VPN et accès distant (GlobalProtect)
8. Domaine 8 — Décryptage SSL/TLS

9. Domaine 9 — Segmentation, NAT et Haute Disponibilité
10. Domaine 10 — Journalisation et supervision SIEM
- Réponse à incident
- Références
- ANNEXE — Checklists de vérification rapide

Top 10 Quick Wins — 80% du risque en priorité

Ces 10 actions couvrent la majorité des vecteurs d'attaque documentés. Commencer ici.

#	ACTION	DOMAINE	IMPACT	EFFORT
1	**CVE-2026-0300** — Patcher PAN-OS ou désactiver Response Pages sur les interfaces WAN immédiatement	D5	🔴 CRITIQUE	Très faible
2	Mettre à jour PAN-OS vers la dernière version stable	D1	🔴 CRITIQUE	Faible
3	Désactiver l'accès SSH/HTTPS depuis l'interface WAN	D3	🔴 CRITIQUE	Faible
4	Activer MFA pour tous les comptes admin	D2	🔴 CRITIQUE	Moyen
5	Désactiver les services inutiles (Telnet, HTTP, SNMPv1/v2)	D3	🟠 ÉLEVÉ	Faible
6	Activer Threat Prevention sur toutes les politiques	D6	🟠 ÉLEVÉ	Moyen
7	Configurer WildFire pour l'analyse de tous les fichiers	D6	🟠 ÉLEVÉ	Faible
8	Restreindre l'accès admin par plage IP autorisée	D3	🟠 ÉLEVÉ	Faible
9	Activer le décryptage SSL/TLS outbound (Forward Proxy)	D8	🟡 MOYEN	Élevé

#	ACTION	DOMAINE	IMPACT	EFFORT
10	Configurer la journalisation Syslog vers un SIEM externe	D10	🟡 MOYEN	Moyen

Domaine 1 — Gestion du firmware et mises à jour

Objectif : *Maintenir PAN-OS, les signatures de contenu dynamique et la synchronisation HA à jour pour éliminer les vulnérabilités connues exploitées activement. Les failles critiques comme CVE-2024-3400 (CVSS 10.0, GlobalProtect RCE) démontrent l'impératif de patching rapide sur les NGFW Palo Alto. L'Integrity Measurement Architecture (IMA) garantit en complément l'intégrité des binaires PAN-OS contre les modifications malveillantes.*

Contrôle 1.1 — Mise à jour PAN-OS vers la dernière version stable

CIS Ref : *4.x / Device Setup* | ***MITRE :*** *T1190* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Les versions obsolètes de PAN-OS exposent l'organisation à des vulnérabilités critiques activement exploitées. En 2024, CVE-2024-3400 (score CVSS 10.0) a permis l'exécution de code arbitraire via GlobalProtect sans authentification. CVE-2022-0028 et CVE-2021-3064 sont également dans le catalogue CISA KEV. Les attaquants scannent massivement les versions exposées en moins de 24h après publication d'un PoC.

Impact potentiel

- Compromission totale du firewall sans authentification
- Pivot vers le réseau interne depuis l'interface de gestion
- Exfiltration silencieuse de la configuration complète (clés, certificats, politiques)
- Utilisation du firewall comme relais d'attaque (T1090)

Navigation

```
Device > Software > Check Now
→ Identifier la dernière version stable du train de maintenance (ex : 11.1.x)
→ Cliquer sur "Download" puis "Install"
→ Cocher "Reboot device after install" si fenêtre de maintenance planifiée
```

CLI de vérification

```
show system info | match sw-version
show system info | match uptime
request system software check
show system software status
```

Remédiation

1. Exporter la configuration courante avant toute mise à jour : `Device > Setup > Operations > Export Named Configuration Snapshot`
2. Vérifier les release notes pour les breaking changes (notamment changements de comportement App-ID)
3. Planifier la mise à jour en fenêtre de maintenance (hors heures de production)
4. En environnement HA : mettre à jour le membre passif en premier, basculer, puis mettre à jour l'ancien actif
5. Valider le fonctionnement des politiques critiques post-update
6. Documenter la version installée et la date dans le registre de changements ITSM
7. **Vérification d'intégrité des images PAN-OS :** Les mises à jour PAN-OS sont signées numériquement par Palo Alto Networks. La vérification de signature est automatique lors du téléchargement depuis `Device > Software > Check Now`. Pour une vérification manuelle complémentaire, comparer le hash SHA-256 de l'image téléchargée avec le hash publié sur `support.paloaltonetworks.com` avant installation.
8. **Vérification post-installation (IMA) :** Après chaque mise à jour majeure, exécuter `request system software verify` pour valider l'intégrité des binaires installés par l'Integrity Measurement Architecture (IMA).
9. **Protection anti-rollback :** PAN-OS intègre une protection native contre le downgrade vers des versions présentant des vulnérabilités connues. Ne jamais contourner cette protection. Consulter le PSIRT avant tout rollback planifié.

Valeur par défaut : Version installée en usine — aucune mise à jour automatique activée par défaut. Vérification de signature des images activée automatiquement lors du téléchargement.

Critère de conformité : PAN-OS dans le train de maintenance supporté, version ≤ 30 jours après la date de publication pour les correctifs CVSS ≥ 9.0. Aucun CVE du catalogue CISA KEV non corrigé. Hash SHA-256 des images PAN-OS vérifié avant installation sur les systèmes critiques. `request system software verify` exécuté après chaque mise à jour majeure.

Contrôle 1.2 — Sauvegardes automatiques de la configuration

> ***CIS Ref :*** *Device Setup > Operations* | ***MITRE :*** *T1490* | ***Niveau :*** 🟢 *L1*

Description du risque

L'absence de sauvegardes régulières de la configuration expose l'organisation à une perte totale de la politique de sécurité en cas d'incident, de mise à jour défaillante, ou d'effacement malveillant. Un attaquant ayant compromis un compte admin peut effacer la configuration pour masquer ses traces ou provoquer une indisponibilité prolongée.

Impact potentiel

- Indisponibilité totale du périmètre réseau (RTO non maîtrisé)
- Perte irréversible de la politique de sécurité complète
- Obligation de reconfiguration manuelle depuis zéro
- Non-conformité réglementaire (PCI-DSS req. 10, ISO 27001 A.12.3)

Navigation

```
Device > Setup > Operations > Export Named Configuration Snapshot
→ Nommer le snapshot avec la date (ex : config-AAAA-MM-JJ)
→ Télécharger le fichier .xml sur un stockage hors-bande sécurisé

Pour automatisation via Panorama :
Panorama > Device Deployment > Config Backups
→ Configurer la fréquence et le nombre de révisions conservées
```

CLI de vérification

```
show config saved
show config list
```

Remédiation

1. Configurer un script de sauvegarde automatique quotidienne via l'API REST PAN-OS :

   ```
   curl -k "https://<MGMT-IP>/api/?type=export&category=configuration&key=<API-KEY>" -o
   config-$(date +%Y%m%d).xml
   ```

2. Stocker les sauvegardes dans un espace hors-bande chiffré (S3 avec SSE-KMS, NAS dédié isolé)
3. Conserver au minimum 30 versions (rotation quotidienne sur 30 jours)
4. Tester la restauration complète trimestriellement en environnement de lab
5. Chiffrer les fichiers de sauvegarde (ils contiennent les clés maître et certificats)
6. Documenter la procédure de restauration dans le PCA/PRA

Valeur par défaut : Aucune sauvegarde automatique configurée. La configuration locale est conservée sur le disque du firewall uniquement.

Critère de conformité : Sauvegarde automatique ≤ 24h, stockage hors-bande chiffré, test de restauration documenté dans les 90 derniers jours, au moins 30 versions conservées.

Contrôle 1.3 — Mises à jour des contenus dynamiques (signatures)

CIS Ref : *4.1, 4.2 (Dynamic Updates)* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

Les bases de signatures Antivirus, Applications & Threats, et WildFire doivent être mises à jour régulièrement. Des signatures obsolètes permettent à des malwares connus de passer inaperçus. Palo Alto publie des mises à jour Antivirus toutes les 24h et des mises à jour WildFire toutes les 5 minutes.

Impact potentiel

- Malwares connus non détectés par les profils de sécurité

- Nouvelles applications non reconnues par App-ID (trafic traité comme inconnu)
- Exploits récents non bloqués par Vulnerability Protection
- Degradation silencieuse de la posture de sécurité

Navigation

```
Device > Dynamic Updates
→ Antivirus : cliquer sur l'engrenage, définir Schedule = "Hourly", action = "Download and Install"
→ Applications and Threats : définir Schedule = "Daily" à 01:00, action = "Download and Install"
→ WildFire Updates : définir Schedule = "Real Time" (ou Every 5 Minutes)
→ Cliquer "Check Now" pour forcer une mise à jour immédiate
```

CLI de vérification

```
show system info | match threat-version
show system info | match app-version
show system info | match av-version
show system info | match wildfire-version
request content upgrade check
```

Remédiation

1. Activer les mises à jour automatiques Antivirus : toutes les heures
2. Activer les mises à jour Applications & Threats : quotidiennes à heure creuse
3. Activer les mises à jour WildFire : en temps réel (nécessite licence WildFire)
4. Cocher “Disable new apps in content update” en production si validation préalable souhaitée
5. Configurer une alerte si la mise à jour échoue (via log System, severity = High)
6. Vérifier que le firewall a accès à `updates.paloaltonetworks.com` en TCP/443 depuis l’interface de gestion

Valeur par défaut : Aucune planification automatique configurée. Les mises à jour doivent être déclenchées manuellement.

Critère de conformité : Signatures Antivirus datant de moins de 25h, Applications & Threats datant de moins de 8 jours, WildFire datant de moins de 1h. Planification automatique configurée et validée.

Contrôle 1.4 — Synchronisation firmware en environnement HA

CIS Ref : *3.1, 3.2, 3.3 (High Availability)* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

En environnement HA (haute disponibilité), une désynchronisation de version PAN-OS entre les membres actif et passif crée une fenêtre de vulnérabilité lors d’un basculement. Le membre passif peut exécuter une version plus ancienne avec des vulnérabilités connues, exposant l’organisation lors d’un failover planifié ou non planifié.

Impact potentiel

- Le membre passif prend le relais avec une version vulnérable lors d'un failover
- Comportement imprévisible des politiques entre versions différentes
- Non-conformité audit : les deux membres doivent être en conformité simultanément
- Risque d'exploitation pendant la fenêtre de basculement

Navigation

```
Device > High Availability > General
→ Vérifier "HA State" : Active / Passive
→ Vérifier "Sync Status" : Configuration Synchronized

Device > High Availability > Link and Path Monitoring
→ Activer Link Monitoring et Path Monitoring

Pour vérifier les versions :
Device > Software (sur chaque membre)
```

CLI de vérification

```
show high-availability state
show high-availability all
show high-availability transitions
```

Remédiation

1. Mettre à jour le membre passif en premier : `Device > Software > Install` (sur le passif)
2. Vérifier la synchronisation : `show high-availability state` doit afficher "synchronized"
3. Effectuer un basculement contrôlé : `request high-availability state suspend` (sur l'actif)
4. Mettre à jour l'ancien actif (maintenant passif)
5. Vérifier que les deux membres ont la même version et sont synchronisés
6. Activer le monitoring de chemin (path monitoring) vers une IP critique pour détecter les pannes

Valeur par défaut : La synchronisation automatique de version n'est pas native ; chaque membre doit être mis à jour manuellement dans l'ordre correct.

Critère de conformité : Les deux membres HA ont la même version PAN-OS. Statut HA = "synchronized". Link Monitoring et Path Monitoring activés.

Contrôle 1.5 — Integrity Measurement Architecture (IMA) et Secure Boot

> ***CIS Ref :*** *Device Setup / System Integrity* | ***MITRE :*** *T1601 (Modify System Image)* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

L'Integrity Measurement Architecture (IMA) est un mécanisme de sécurité natif à PAN-OS qui s'exécute en mode enforcement par défaut sur les plateformes supportées. IMA mesure et vérifie l'intégrité de chaque binaire avant son exécution : seuls les binaires signés cryptographiquement par Palo Alto Networks peuvent s'exécuter. Cette protection contre-carre directement la technique MITRE ATT&CK T1601 (Modify System Image), utilisée par des acteurs APT pour modifier le firmware ou les binaires PAN-OS afin d'établir une persistance indétectable.

CVE-2024-3400 (CVSS 10.0) et d'autres exploits récents ont démontré que des attaquants cherchent à modifier les binaires PAN-OS après exploitation initiale. Sans IMA, ces modifications persistent après redémarrage.

Impact potentiel

- Persistance d'un implant malveillant dans les binaires PAN-OS après compromission initiale (T1601)
- Exécution de malwares non signés sur le data plane ou le management plane
- Impossibilité de détecter la modification post-exploitation sans vérification d'intégrité
- Compromission persistante survivant aux mises à jour de signatures antivirus

Navigation

```
Device > Setup > Management > System Settings
→ Vérifier "Secure Boot" : Enabled (plateformes matérielles supportées)

Pour vérifier l'état IMA :
Device > Troubleshooting > System Information
→ IMA Status : Enforcing

CLI :
show system ima-status
show system boot-mode
```

CLI de vérification

```
show system ima-status
show system software status
request system software verify
show system boot-mode
debug system ima show
```

Remédiation

1. Vérifier que l'IMA est en mode Enforcing : `show system ima-status` doit afficher "enforcing"
2. Sur les plateformes matérielles PA-Series : activer Secure Boot dans les paramètres BIOS/UEFI du châssis si désactivé
3. Ne jamais utiliser `debug system ima disable` sauf directive explicite de Palo Alto PSIRT pour un cas de support — documenter toute désactivation temporaire
4. Après tout incident de sécurité suspectant une compromission : exécuter `request system software verify` pour valider l'intégrité des binaires installés
5. S'assurer que les mises à jour PAN-OS sont téléchargées uniquement depuis `updates.paloaltonetworks.com` (binaires signés)

6. Utiliser le **Best Practice Assessment (BPA)** tool (`https://bpa.paloaltonetworks.com/`) ou **AIOps for NGFW** (via Panorama) pour évaluer automatiquement la conformité de la posture de sécurité, incluant l'état IMA
7. En cas d'alerte IMA (binaire non autorisé détecté) : isoler immédiatement le firewall, ouvrir un ticket Palo Alto PSIRT, restaurer depuis une sauvegarde saine

Valeur par défaut : IMA actif en mode Enforcing par défaut sur PAN-OS 10.x et 11.x. Secure Boot dépend de la plateforme matérielle.

Critère de conformité : IMA en mode Enforcing. Secure Boot activé sur toutes les plateformes matérielles supportées. Aucune désactivation IMA non documentée. Vérification d'intégrité exécutée après chaque mise à jour majeure et après tout incident.

Domaine 2 — Authentification et accès administrateur

> ***Objectif :*** *Protéger les comptes administrateurs contre la compromission par force brute, credential stuffing, et vol de session. La compromission d'un compte admin sur un NGFW donne accès à l'ensemble du périmètre réseau.*

Contrôle 2.1 — Authentification multi-facteurs (MFA) pour les administrateurs

> ***CIS Ref :*** *1.4 (Authentication Settings)* | ***MITRE :*** *T1078* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

L'authentification par simple mot de passe pour les administrateurs du firewall est insuffisante face aux attaques de credential stuffing, phishing et brute force. Les attaquants ciblent en priorité les comptes d'administration des équipements réseau pour obtenir un accès persistant et invisible. CVE-2024-3400 a été exploité en combinaison avec des credentials volés pour établir des backdoors.

Impact potentiel

- Compromission de l'interface de gestion par un attaquant externe ou interne
- Modification silencieuse des politiques de sécurité (ouverture de ports, désactivation du filtrage)
- Création de comptes admin backdoor persistants
- Exfiltration de la configuration complète incluant les clés privées VPN

Navigation

```
Device > Authentication Profile > Add
→ Name : MFA-Admin-Profile
→ Type : RADIUS / SAML / Kerberos (selon infrastructure IdP)
→ Onglet "Multi Factor Auth" : cocher "Enable Additional Authentication Factors"
→ Sélectionner le profil MFA (Duo, Okta, Azure AD MFA)

Device > Administrators > [compte admin]
→ Authentication Profile : sélectionner MFA-Admin-Profile

Device > Setup > Management > Authentication Settings
→ Authentication Profile : sélectionner MFA-Admin-Profile
```

CLI de vérification

```
show admins
show authentication profile
show config running | xpath /config/mgt-config/users/entry | match authentication-profile
```

Remédiation

1. Déployer un profil d'authentification RADIUS pointant vers un serveur MFA (Duo Security, Okta, RSA SecurID)
2. Lier ce profil à tous les comptes administrateurs locaux et aux groupes LDAP/AD admin
3. Configurer une méthode de secours (breakglass account) avec certificat matériel (YubiKey)
4. Tester la connexion MFA depuis un poste d'administration avant de pousser en production
5. Documenter la procédure de récupération en cas de panne du serveur MFA

Valeur par défaut : Authentification par mot de passe local uniquement. MFA non configuré par défaut.

Critère de conformité : MFA actif sur 100% des comptes administrateurs. Aucun compte admin ne peut se connecter avec mot de passe seul (sauf compte breakglass documenté et sous contrôle PAM).

Contrôle 2.2 — Politique de mots de passe renforcée

> ***CIS Ref :*** *1.3.1 à 1.3.10 (Minimum Password Requirements)* | ***MITRE :*** *T1110* | ***Niveau :*** 🟢 *L1*

Description du risque

Des mots de passe faibles ou réutilisés permettent les attaques par dictionnaire et brute force. Le CIS Benchmark PAN-OS 11 définit des exigences précises : complexité activée, longueur minimale 12 caractères, au moins 1 majuscule, 1 minuscule, 1 chiffre, 1 caractère spécial, rotation tous les 90 jours, historique de 24 mots de passe, différence d'au moins 3 caractères entre anciens et nouveaux mots de passe.

Impact potentiel

- Compromission de comptes admin par attaque dictionnaire ou brute force
- Réutilisation de mots de passe compromis depuis d'autres services (credential stuffing)
- Accès persistant par un attaquant ayant deviné un mot de passe simple

Navigation

```
Device > Setup > Management > Minimum Password Complexity
→ Cocher "Enabled"
→ Minimum Length : 12
→ Minimum Uppercase Letters : 1
→ Minimum Lowercase Letters : 1
→ Minimum Numeric Letters : 1
→ Minimum Special Characters : 1
→ Required Password Change Period (days) : 90
→ New Password Differs By Characters : 3
→ Prevent Password Reuse Limit : 24
```

CLI de vérification

```
show config running | xpath /config/mgt-config/password-complexity
show admins
show config running | xpath /config/mgt-config/users
```

Remédiation

1. Naviguer vers `Device > Setup > Management > Minimum Password Complexity` et cocher “Enabled”
2. Configurer tous les paramètres selon les valeurs CIS ci-dessus
3. Supprimer tout profil de mot de passe permissif sous `Device > Password Profiles`
4. Forcer le changement de mot de passe à la prochaine connexion pour tous les comptes
5. Vérifier qu’aucun compte n’utilise le mot de passe par défaut `admin`

Valeur par défaut : Complexity désactivée. Mot de passe par défaut `admin` / `admin`.

Critère de conformité : Complexity = enabled, longueur ≥ 12, tous les critères de caractères activés, rotation ≤ 90 jours, historique ≥ 24. Aucun profil de mot de passe permissif existant (`Device > Password Profiles` = vide).

Contrôle 2.3 — Verrouillage de compte après tentatives échouées

> ***CIS Ref :*** *1.4.2 (Failed Attempts & Lockout Time)* | ***MITRE :*** *T1110* | ***Niveau :*** 🟢 *L1*

Description du risque

Sans mécanisme de verrouillage, un attaquant peut effectuer un nombre illimité de tentatives de connexion (brute force). Les interfaces de gestion Palo Alto exposées sur Internet sont régulièrement ciblées par des scans automatisés testant des milliers de combinaisons credentials/mots de passe.

Impact potentiel

- Compromission de comptes admin par attaque brute force non détectée
- Exposition prolongée sans alerte en cas d’attaque lente (low & slow brute force)
- Violation des exigences PCI-DSS (req. 8.3.4 : verrouillage après 6 tentatives max)

Navigation

```
Device > Authentication Profile > [profil admin] > Advanced
→ Failed Attempts : 5
→ Lockout Time (minutes) : 30

Device > Setup > Management > Authentication Settings
→ Failed Attempts : 5
→ Lockout Time : 30
```

CLI de vérification

```
show config running | xpath /config/mgt-config/authentication-profile
show authentication profile name <nom-profil>
```

Remédiation

1. Dans le profil d'authentification admin : définir `Failed Attempts = 5` et `Lockout Time = 30 minutes`
2. Appliquer ces paramètres à tous les profils d'authentification utilisés pour la gestion
3. Configurer une alerte Syslog/SNMP sur l'événement de verrouillage (auth-lockout)
4. Définir une procédure de déverrouillage manuel par l'équipe N+1 (PAM/change control)

Valeur par défaut : Failed Attempts = 0 (désactivé), pas de verrouillage automatique.

Critère de conformité : Failed Attempts ≤ 5, Lockout Time ≥ 30 minutes, appliqué à tous les profils d'authentification admin.

Contrôle 2.4 — Timeout de session administrateur

> ***CIS Ref :*** *1.4.1 (Idle Timeout)* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

Description du risque

Une session administrateur laissée ouverte sans activité permet à un attaquant ayant accès physique ou réseau à la station de travail d'effectuer des modifications non autorisées. Les sessions Web UI et CLI doivent se déconnecter automatiquement après une période d'inactivité.

Impact potentiel

- Session admin hijacking depuis un poste non verrouillé (T1563 — Remote Service Session Hijacking)
- Modifications non autorisées par un tiers ayant accès au poste d'un administrateur
- Non-conformité PCI-DSS (req. 8.2.8 : timeout ≤ 15 minutes d'inactivité)

Navigation

```
Device > Setup > Management > General Settings
→ Idle Timeout (minutes) : 10

Pour les administrateurs individuels :
Device > Administrators > [compte] > General
→ Authentication Profile : vérifier que le profil avec idle timeout est appliqué
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/setting/management | match
idle-timeout
show admins
```

Remédiation

1. Définir `Idle Timeout = 10 minutes` dans `Device > Setup > Management > General Settings`
2. Vérifier que ce timeout s'applique aux sessions HTTPS (Web UI) et SSH (CLI)
3. Communiquer la procédure aux administrateurs (reconnexion MFA requise après timeout)

Valeur par défaut : Idle Timeout = 0 (pas de déconnexion automatique).

Critère de conformité : Idle Timeout ≤ 10 minutes configuré globalement. Applicable à toutes les sessions UI et CLI.

Contrôle 2.5 — RBAC et suppression du compte admin par défaut

> ***CIS Ref :*** *Device Administrators* | ***MITRE :*** *T1078* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Le compte `admin` par défaut de PAN-OS est connu universellement. Sa présence avec des droits Super User constitue une cible évidente pour les attaquants. Le RBAC (Role-Based Access Control) doit limiter les privilèges au strict nécessaire selon le principe du moindre privilège.

Impact potentiel

- Exploitation du compte par défaut avec mot de passe usine non changé
- Accès Super User non audité par des opérateurs ne nécessitant que des droits lecture
- Impossibilité de tracer les actions par individu si un compte générique est partagé

Navigation

```
Device > Administrators > Add
→ Créer des comptes nominatifs avec rôles appropriés

Device > Admin Roles > Add
→ Créer des rôles personnalisés (Read-Only, Operator, Security-Admin)

Device > Administrators > admin
→ Changer le mot de passe ou désactiver le compte si un compte admin nominatif existe
→ Idéalement : renommer ou recréer avec un nom non générique
```

CLI de vérification

```
show admins all
show config running | xpath /config/mgt-config/users
show config running | xpath /config/mgt-config/users/entry[@name='admin']
```

Remédiation

1. Créer des comptes administrateurs nominatifs avec un profil de rôle approprié
2. Assigner le rôle minimal nécessaire : `Device Admin` pour les opérations courantes, `Super User` uniquement pour la configuration structurelle

3. Désactiver ou changer le mot de passe du compte `admin` par défaut si conservation nécessaire (breakglass)
4. Créer un compte breakglass avec un mot de passe complexe stocké dans un coffre-fort (CyberArk, HashiCorp Vault) — accès audité
5. Documenter les rôles et permissions dans la matrice RBAC de l'organisation

Valeur par défaut : Compte `admin` avec rôle Super User et mot de passe `admin` à la livraison.

Critère de conformité : Aucun compte partagé actif. Compte `admin` par défaut désactivé ou avec mot de passe changé et accès MFA. Tous les comptes ont un rôle RBAC défini selon le principe du moindre privilège.

Contrôle 2.6 — Authentification par certificat pour SSH

> ***CIS Ref :*** *1.2 (Management Interface Settings)* | ***MITRE :*** *T1110* | ***Niveau :*** 🔵 *L2*

Description du risque

L'authentification SSH par mot de passe est vulnérable aux attaques brute force. L'authentification par certificat (clé publique/privée) est cryptographiquement plus robuste et élimine le risque de devinette de mot de passe sur l'accès CLI.

Impact potentiel

- Brute force SSH non protégé si le verrouillage de compte n'est pas fonctionnel
- Interception du mot de passe sur le réseau de gestion non chiffré (bien que SSH chiffre le transport, le hash peut être attaqué hors ligne)

Navigation

```
Device > Administrators > [compte admin] > SSH Keys
→ Import : coller la clé publique SSH de l'administrateur (format OpenSSH)
→ Type : RSA 4096 bits ou Ed25519

Device > Setup > Management > Authentication Settings
→ Désactiver "Allow password authentication for SSH" si tous les admins ont des clés
```

CLI de vérification

```
show config running | xpath /config/mgt-config/users/entry/ssh-public-key
```

Remédiation

1. Générer une paire de clés SSH pour chaque administrateur (RSA 4096 ou Ed25519)
2. Importer la clé publique dans le profil de chaque administrateur
3. Tester la connexion SSH par certificat avant de désactiver l'authentification par mot de passe SSH
4. Stocker les clés privées dans un gestionnaire de clés sécurisé (PAM)

Valeur par défaut : Authentification par mot de passe SSH activée. Pas de clé SSH configurée.

Critère de conformité : Clé SSH (RSA ≥ 2048 bits ou Ed25519) importée pour tous les comptes admin ayant accès CLI. Authentification par mot de passe SSH désactivée si possible.

Domaine 3 — Sécurisation de l'interface de gestion (management)

Objectif : *Réduire la surface d'attaque de l'interface de gestion en limitant les protocoles autorisés, les adresses IP sources, et les services exposés. L'interface de gestion est la cible principale des attaquants ciblant les NGFW. Les CVE les plus critiques de 2024-2025 (CVE-2024-3400, CVE-2025-0108, CVE-2024-9474) ont toutes été exploitées via l'interface de gestion exposée — une configuration stricte de ce domaine est le contrôle de sécurité le plus impactant.*

Contrôle 3.1 — Restriction des adresses IP autorisées pour la gestion

CIS Ref : *1.2.1, 1.2.2 (Permitted IP Addresses)* | ***MITRE :*** *T1078* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Sans restriction d'adresses IP sources, l'interface de gestion est accessible depuis n'importe quel réseau, y compris Internet. Les scans Shodan identifient quotidiennement des interfaces de gestion Palo Alto exposées. Les trois CVE critiques les plus récentes illustrent l'impératif absolu de cette restriction :

- **CVE-2024-3400** (CVSS 10.0, CISA KEV) : OS command injection via GlobalProtect — exploitation de masse depuis Internet contre des interfaces exposées
- **CVE-2025-0108** : Authentication bypass sur l'interface de gestion PAN-OS — permet l'accès administrateur sans credentials
- **CVE-2024-9474** : Privilege escalation via l'interface de gestion — permet à un utilisateur à faibles privilèges d'obtenir les droits root

Ces trois vulnérabilités partagent un vecteur commun : l'interface de gestion accessible sans restriction réseau. La guidance CISA recommande explicitement de limiter l'interface de gestion à des réseaux internes dédiés ou un jump box sécurisé.

Impact potentiel

- Exposition de l'interface de gestion aux attaques internet-facing
- Exploitation des vulnérabilités 0-day avant disponibilité des patches (T1190)
- Brute force non limité géographiquement
- Compromission complète du firewall via CVE-2025-0108 (auth bypass) sans credentials valides

Navigation

```
Device > Setup > Interfaces > Management
→ "Permitted IP Addresses" : ajouter uniquement les plages IP légitimes
   (ex : 10.0.100.0/24 — VLAN de gestion dédié)

Pour les profils de gestion d'interface :
Network > Network Profiles > Interface Mgmt > [profil]
→ "Permitted IP Addresses" : idem

Device > Setup > Management > Management Interface Settings
→ Cocher uniquement HTTPS et SSH
→ Décocher HTTP, Telnet, SNMP (si SNMP géré séparément)
```

CLI de vérification

```
show interface management
show config running | xpath /config/devices/entry/deviceconfig/system/permitted-ip
show config running | xpath /config/devices/entry/deviceconfig/system | match service
```

Remédiation

1. Définir les plages IP autorisées dans `Device > Setup > Interfaces > Management > Permitted IP Addresses`
2. Utiliser un VLAN de gestion dédié et isolé (out-of-band management si possible) — recommandation CISA
3. Appliquer les mêmes restrictions sur tous les profils Interface Management `Network > Network Profiles > Interface Mgmt`
4. Ne jamais autoriser des plages `0.0.0.0/0` ou `any`
5. Si un accès distant à l'interface de gestion est nécessaire : exiger le passage par un VPN gateway ou un jump box sécurisé avec MFA — ne jamais exposer directement sur Internet
6. Configurer des ACLs de management VLAN au niveau des switches upstream pour un deuxième niveau de protection
7. Vérifier l'absence d'exposition via `curl -k https://<IP-MGMT>/` depuis une IP externe — si accessible, traiter comme incident immédiat

Valeur par défaut : Aucune restriction d'IP. Toutes les adresses sources autorisées par défaut.

Critère de conformité : `Permitted IP Addresses` configuré avec des plages spécifiques sur l'interface de management et tous les profils d'interface management. Aucune règle `any` ou `0.0.0.0/0`. Interface de gestion inaccessible depuis la zone untrust/Internet.

Contrôle 3.2 — Désactivation des protocoles de gestion non sécurisés

CIS Ref : *1.2.3, 1.2.4 (HTTP and Telnet disabled)* | ***MITRE :*** *T1040* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

HTTP et Telnet transmettent les credentials en clair. Même sur un réseau interne, un attaquant ayant réalisé un pivot réseau peut capturer les sessions d'administration. Ces protocoles ne doivent jamais être actifs sur un équipement de sécurité.

Impact potentiel

- Capture de credentials admin en clair sur le réseau de gestion
- Session hijacking d'une connexion HTTP active
- Violation des exigences PCI-DSS (req. 2.2.7 : tous les accès administrateurs non-console chiffrés)

Navigation

```
Device > Setup > Interfaces > Management
→ Décocher "HTTP"
→ Décocher "Telnet"
→ Laisser cochés : HTTPS, SSH uniquement

Network > Network Profiles > Interface Mgmt > [tous les profils]
→ Décocher HTTP et Telnet sur tous les profils
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/system | match service
show interface management
```

Remédiation

1. Décocher HTTP et Telnet dans `Device > Setup > Interfaces > Management`
2. Répéter pour tous les profils `Network > Network Profiles > Interface Mgmt`
3. Vérifier qu'HTTPS utilise TLS 1.2 minimum (contrôle 3.4)
4. Tester que la connexion HTTP redirige vers HTTPS ou est refusée après la modification

Valeur par défaut : HTTP et Telnet désactivés par défaut sur les versions récentes de PAN-OS. Vérifier les configurations héritées (upgrades depuis versions anciennes).

Critère de conformité : HTTP = désactivé, Telnet = désactivé sur l'interface de management et tous les profils Interface Mgmt. Seuls HTTPS et SSH autorisés.

Contrôle 3.3 — SNMPv3 exclusivement (désactivation SNMPv1/v2c)

CIS Ref : *1.5.1 (V3 for SNMP polling)* | ***MITRE :*** *T1040, T1602 (Data from Configuration Repository)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

SNMPv1 et SNMPv2c utilisent des community strings en clair (typiquement "public" ou "private") transmises sans chiffrement ni authentification forte. Un attaquant sur le réseau de gestion peut capturer la community string et interroger ou même modifier la configuration SNMP. SNMPv3 fournit authentification (SHA) et chiffrement (AES).

La technique MITRE ATT&CK **T1602 — Data from Configuration Repository** couvre précisément l'exfiltration de configuration réseau via des requêtes SNMP MIB dump. Un attaquant utilisant SNMPv2c avec la community string "public" (souvent active par défaut) peut extraire l'intégralité de la table de routage, les interfaces, les voisins BGP/OSPF et les paramètres de configuration sans aucune authentification forte. Cette technique est activement utilisée dans les campagnes APT ciblant les équipements réseau.

Impact potentiel

- Énumération complète de la configuration réseau via SNMP GET sans authentification (community "public") — T1602
- Modification de configuration via SNMP SET si write community string capturée
- Reconnaissance réseau facilitée (topologie, interfaces, routes, voisins BGP)
- Extraction des MIB SNMP révélant les tunnels VPN, les politiques NAT et la structure des zones

Navigation

```
Device > Setup > Operations > SNMP Setup
→ Version : V3
→ Configurer un utilisateur SNMPv3 avec :
   - Security Level : authPriv (authentification + chiffrement)
   - Auth Protocol : SHA
   - Priv Protocol : AES-128 ou AES-256

Device > Server Profiles > SNMP Trap
→ Version : V3 (pour les traps sortants)
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/system/snmp-setting
show snmp stats
```

Remédiation

1. Désactiver SNMPv1 et SNMPv2c si actifs
2. Configurer SNMPv3 avec `authPriv` : SHA pour l'authentification, AES-128 minimum pour le chiffrement
3. Définir des utilisateurs SNMPv3 avec des mots de passe forts (≥ 16 caractères)
4. Restreindre les requêtes SNMP aux adresses IP des serveurs de supervision autorisés (contrôle T1602 : empêcher les interrogations SNMP depuis des sources non autorisées)
5. Utiliser SNMPv3 pour les traps également (`Device > Server Profiles > SNMP Trap`)
6. Tester périodiquement depuis une IP non autorisée que les requêtes SNMPv1/v2 sont refusées

Valeur par défaut : SNMP désactivé par défaut. Si activé, la version par défaut peut être SNMPv2c sur des configurations héritées.

Critère de conformité : Si SNMP est utilisé, uniquement SNMPv3 avec niveau de sécurité `authPriv`. SNMPv1 et SNMPv2c désactivés. Restriction par adresse IP source sur les requêtes SNMP.

Contrôle 3.4 — TLS 1.2 minimum pour l'interface HTTPS de gestion

CIS Ref : *1.2.5 (Valid Certificate for Browser-Based Admin)* | ***MITRE :*** *T1040, T1600 (Weaken Encryption)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

TLS 1.0 et 1.1 présentent des vulnérabilités connues (POODLE, BEAST, SWEET32). L'interface de gestion HTTPS doit forcer TLS 1.2 ou supérieur. De plus, un certificat auto-signé ou expiré expose les administrateurs aux attaques Man-in-the-Middle lors de la connexion à la Web UI.

La technique MITRE ATT&CK **T1600 — Weaken Encryption** correspond aux attaques de downgrade TLS qui forcent une connexion sécurisée à utiliser une version ou suite cryptographique vulnérable. Sans configuration explicite de la version TLS minimum, un attaquant en position MITM peut négocier TLS 1.0 avec les suites RC4 ou DES, permettant le déchiffrement de la session administrative.

Impact potentiel

- Downgrade TLS permettant le déchiffrement de sessions admin (T1600)
- Attaque MITM si le certificat n'est pas validé par une CA de confiance
- Non-conformité PCI-DSS (req. 6.4.3 : TLS fort requis pour tous les accès admin)

Navigation

```
Device > Setup > Management > SSL/TLS Service Profile
→ Créer un profil : Min Version = TLSv1.2, Max Version = TLSv1.3
→ Sélectionner un certificat valide signé par une CA interne ou publique

Device > Setup > Management > General Settings
→ SSL/TLS Service Profile : sélectionner le profil créé
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/system/ssl-tls-service-
profile
show sslmgr-store
```

Remédiation

1. Créer un profil SSL/TLS : `Device > Setup > Management > SSL/TLS Service Profile > Add`
2. Définir Min Protocol Version = TLSv1.2, Max = TLSv1.3
3. Importer un certificat de gestion signé par la CA interne de l'organisation
4. Lier ce profil à l'interface HTTPS de gestion
5. Vérifier avec un scanner TLS (testssl.sh, Qualys SSL Labs pour les interfaces exposées) que TLS 1.0/1.1 sont refusés

Valeur par défaut : Certificat auto-signé généré à l'installation. Version TLS minimale non restreinte sur les configurations héritées.

Critère de conformité : TLS minimum = TLSv1.2. Certificat signé par une CA de confiance (non auto-signé). TLS 1.0 et 1.1 désactivés.

Contrôle 3.5 — Bannière de connexion légale

CIS Ref : *1.1.2 (Login Banner)* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

Description du risque

L'absence de bannière légale sur l'interface de connexion peut affaiblir la position juridique de l'organisation en cas de poursuite contre un accès non autorisé. La bannière avertit les utilisateurs non autorisés et constitue une preuve de mise en garde préalable.

Impact potentiel

- Fragilisation juridique en l'absence d'avertissement explicite d'accès restreint
- Non-conformité avec certaines réglementations sectorielles (FISMA, NIS2)

Navigation

```
Device > Setup > Management > General Settings
→ Login Banner : saisir le texte de la bannière légale
Exemple :
"ACCÈS RÉSERVÉ AU PERSONNEL AUTORISÉ. Toute connexion non autorisée est interdite
et fera l'objet de poursuites judiciaires. Les activités sont enregistrées et auditées."
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/system | match login-banner
```

Remédiation

1. Rédiger une bannière légale validée par le service juridique de l'organisation
2. La configurer dans `Device > Setup > Management > General Settings > Login Banner`
3. Inclure : avertissement d'accès restreint, mention d'enregistrement des activités, contact pour signalement

Valeur par défaut : Aucune bannière configurée.

Critère de conformité : Bannière légale présente, non vide, validée par le service juridique. Visible à la connexion HTTPS et SSH.

Contrôle 3.6 — Durcissement de l'API REST/XML PAN-OS

CIS Ref : *1.2 (Management Interface Settings)* | ***MITRE :*** *T1078.003 (Local Accounts — API key theft equivalent)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

PAN-OS expose deux interfaces de programmation : une **API XML** (historique, disponible sur toutes les versions) et une **API REST** (PAN-OS 9.0+). Ces interfaces permettent l'automatisation de la configuration, la récupération d'informations système et le déclenchement d'opérations administratives avec les mêmes droits que l'administrateur associé. Des clés API mal protégées, non tournées, ou trop larges constituent un vecteur d'accès permanent au firewall, sans les protections liées à la session interactive (timeout, MFA).

Des clés API codées en dur dans des scripts d'automatisation, des dépôts Git, ou des fichiers de configuration constituent un risque majeur de fuite. Un attaquant obtenant une clé API active peut accéder au firewall sans déclencher les alertes d'authentification MFA habituelles.

Impact potentiel

- Accès administrateur au firewall via clé API volée ou exposée sans déclenchement de l'alerte MFA (T1078.003)
- Exfiltration de la configuration complète (clés VPN, certificats, politiques) via l'API XML
- Modification silencieuse des règles de sécurité via des scripts automatisés non contrôlés
- Persistance post-exploitation : création de backdoors via l'API après une compromission initiale
- Mouvement latéral si la clé API est partagée entre plusieurs environnements

Navigation

```
-- Génération de clés API par application (pas par credential admin) --
Device > Administrators > [admin] > Generate API Key
→ Utiliser un compte administrateur dédié à l'automatisation (ex : svc-api-noc)
→ JAMAIS utiliser le compte admin principal pour générer des clés API
→ Assigner un rôle RBAC minimal au compte de service API

-- Restriction des clés API par IP source --
Policies > Security (Local-in Policy)
→ Créer une Local-in Policy restreignant les connexions HTTPS (API) aux IP des systèmes
d'automatisation autorisés
→ Source : IP des systèmes d'automatisation (SIEM, Ansible, Terraform, scripts NOC)
→ Destination : interface de gestion (IP mgmt)
→ Application : ssl
→ Action : Allow
→ Toute autre source → Deny

-- Vérification des clés API actives --
Device > Administrators > [compte service API] > API Key
→ Régénérer la clé trimestriellement
→ Invalider les clés non utilisées depuis > 90 jours

-- Désactivation de l'API si non utilisée --
Device > Setup > Management > Management Interface Settings
→ Décocher "Enable API" si l'API n'est pas utilisée pour l'automatisation
→ Cette option désactive l'accès API REST et XML complètement

-- REST API avec OAuth (PAN-OS 9.0+) --
Device > Setup > Management > Enable REST API
→ Préférer l'authentification OAuth pour les intégrations REST modernes
→ Configurer des clients OAuth avec des scopes limités au minimum nécessaire

CLI :
set deviceconfig system management interface api enabled no
```

CLI de vérification

```
# Vérifier si l'API est activée
show config running | xpath /config/devices/entry/deviceconfig/system | match "api"

# Vérifier les clés API actives et les comptes de service
show admins all
show config running | xpath /config/mgt-config/users | match "api"

# Tester l'accessibilité de l'API depuis une IP autorisée
# (depuis le système d'automatisation)
curl -k "https://<MGMT-IP>/api/?type=op&cmd=<show><system><info></info></system></
show>&key=<API-KEY>"

# Vérifier les logs d'accès API
show log system subtype api
```

Remédiation

1. **Compte de service dédié :** Créer un compte administrateur spécifique à chaque application consommatrice d'API (ex : `svc-api-ansible`, `svc-api-siem`) avec le rôle RBAC minimal nécessaire. Ne jamais partager de clé API entre applications.
2. **Génération de clés par application :** Générer une clé API distincte par compte de service dans `Device > Administrators > [admin] > Generate API Key`. Documenter chaque clé dans le gestionnaire de secrets de l'organisation (CyberArk, HashiCorp Vault).
3. **Restriction IP source :** Configurer des Local-in Policies restreignant les requêtes API aux seules IP des systèmes d'automatisation autorisés. Bloquer les requêtes API depuis toute autre source.
4. **Rotation trimestrielle des clés :** Programmer la rotation des clés API tous les 90 jours maximum. La rotation ne nécessite pas de redémarrage du firewall — planifier dans le gestionnaire de changements.
5. **Désactivation si inutilisée :** Si l'automatisation via API n'est pas utilisée, désactiver l'API complètement dans `Device > Setup > Management > Management Interface Settings`.
6. **Inventaire des clés :** Maintenir un registre des clés API actives, de leurs propriétaires, applications et dates de création. Invalider immédiatement les clés dont le propriétaire n'est plus actif.
7. **Audit des logs API :** Configurer des alertes SIEM sur l'accès API en dehors des plages horaires d'automatisation définies (ex : accès API manuel à 3h du matin = anomalie).
8. **Ne jamais stocker les clés API en clair** dans des scripts, fichiers de configuration, dépôts Git, ou variables d'environnement non protégées — utiliser un gestionnaire de secrets.

Valeur par défaut : API XML activée par défaut. Aucune restriction IP source sur les requêtes API. Clés API non créées ni gérées par défaut.

Critère de conformité : Un compte de service dédié par application consommatrice d'API. Clés API rotées tous les 90 jours. Restriction IP source via Local-in Policy sur les requêtes API. API désactivée si inutilisée. Alertes SIEM sur accès API anormaux. Registre des clés actives maintenu et audité.

Domaine 4 — Zones et politiques de sécurité

Objectif : *Implémenter une politique de sécurité basée sur les zones (trust, untrust, DMZ) avec le principe du moindre privilège : tout trafic non explicitement autorisé doit être bloqué. Les règles permissives (any/any) sont le principal vecteur d'escalade de privilèges réseau. Utiliser le Policy Optimizer pour migrer des règles port-based vers des règles App-ID. Déployer des contrôles Kill Chain dès l'étape de reconnaissance (étape 1) pour détecter et bloquer les attaquants avant qu'ils n'atteignent les phases d'exploitation.*

Contrôle 4.1 — Règle de refus implicite par défaut (deny-all)

CIS Ref : *7 (Security Policies)* | ***MITRE :*** *T1071* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

PAN-OS dispose d'une règle de refus implicite en fin de politique, mais elle ne génère pas de logs par défaut. Sans règle de refus explicite avec logging, le trafic bloqué n'est pas visible dans les logs et les tentatives d'attaque passent inaperçues. Le CIS Benchmark exige que la règle de refus soit explicite et journalisée.

Impact potentiel

- Trafic bloqué non visible dans les logs : impossibilité de détecter les tentatives de reconnaissance
- Confusion sur ce qui est bloqué versus permis lors des audits
- Non-conformité avec les exigences de journalisation exhaustive (PCI-DSS req. 10.2)

Navigation

```
Policies > Security > Add (en bas de liste)
→ Name : Deny-All-Log
→ Source Zone : any
→ Destination Zone : any
→ Application : any
→ Service : any
→ Action : Deny
→ Profile Group : (aucun nécessaire)
→ Log at Session End : coché
→ Log Forwarding : profil Syslog SIEM

Policies > Security > Default Rules > intrazone-default
→ Action : Deny (au lieu de Allow)
→ Log at Session End : coché
```

CLI de vérification

```
show running security-policy
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules/
entry[@name='Deny-All-Log']
```

Remédiation

1. Créer une règle `Deny-All-Log` en dernière position de la politique de sécurité
2. Modifier la règle `intrazone-default` pour logger le trafic bloqué
3. Configurer le Log Forwarding Profile pour envoyer ces logs au SIEM
4. Vérifier que les logs de refus apparaissent bien dans `Monitor > Logs > Traffic`

Valeur par défaut : Règle de refus implicite présente mais sans logging. Règle intrazone-default = Allow (sans log).

Critère de conformité : Règle deny explicite en dernière position avec Log at Session End = enabled. Règle intrazone-default = Deny avec logging. Tous les logs de refus transmis au SIEM.

Contrôle 4.2 — Élimination des règles “any-any” et nettoyage de politique

> ***CIS Ref :*** *7.2 (Service setting of ANY), 7.1* | ***MITRE :*** *T1071* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les règles avec source = any, destination = any, service = any, ou application = any constituent des ouvertures massives dans la politique de sécurité. Ces règles existent souvent suite à des opérations de dépannage non nettoyées ou à une méconnaissance de PAN-OS. La règle `Service = ANY` désactive le contrôle de port et expose à des abus de protocoles (tunneling, port non standard).

Impact potentiel

- Trafic non autorisé passant par des ports non standard non détecté (T1599 — Network Boundary Bridging)
- Applications malveillantes utilisant des ports arbitraires contournant le filtrage
- Difficulté à identifier le périmètre autorisé lors des audits de sécurité

Recommandation Tufin : placer les règles bloquant le trafic malveillant en **tête de rulebase**, utiliser des règles spécifiques avant les règles générales pour éviter le rule shadowing, implémenter des groupes d’adresses et d’applications.

Navigation

```
Policies > Security
→ Filtrer les règles avec Service = "any" ou Application = "any"
→ Pour chaque règle identifiée : analyser le trafic légitime réel via
   Monitor > Logs > Traffic > filtrer par règle

Pour désactiver une règle suspecte :
→ Clic droit > Disable
→ Ou : supprimer après validation
```

CLI de vérification

```
show running security-policy
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match "service.*any"
show policy-hit-count vsys vsys1 rule-base security type pre-rulebase
```

Remédiation

1. Inventorier toutes les règles avec `Service = any` ou `Application = any`
2. Analyser les logs de trafic pour identifier le trafic légitime passant par ces règles
3. Réécrire chaque règle avec des applications et services spécifiques
4. Désactiver les règles inutilisées (0 hits sur 90 jours) avant suppression définitive
5. Planifier des revues de politique trimestrielles avec le **Policy Optimizer** (voir contrôle 4.5)
6. Implémenter des **Application Groups** et **Address Groups** pour simplifier la politique sans règles permissives

Valeur par défaut : Aucune règle pré-configurée (hors règles default). Les règles `any` sont créées par les administrateurs.

Critère de conformité : Aucune règle avec `Service = any` sur des flux Internet-facing. Applications explicitement nommées sur toutes les règles autorisant le trafic vers/depuis la zone untrust.

Contrôle 4.3 — Profils de sécurité attachés à toutes les règles permit

> ***CIS Ref :*** *6 (Security Profiles)* | ***MITRE :*** *T1059* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Une règle de sécurité qui autorise le trafic sans profil de sécurité attaché est aveugle aux menaces applicatives : malwares, exploits, URLs malveillantes. Tout trafic autorisé doit être inspecté par au moins un Security Profile Group incluant Anti-Virus, Anti-Spyware, Vulnerability Protection et URL Filtering.

Impact potentiel

- Malwares transitant dans les flux autorisés sans inspection
- Exploits passant dans les flux applicatifs légitimes (ex : CVE dans HTTP/HTTPS)
- Exfiltration de données via des protocoles autorisés non inspectés

Navigation

```
Objects > Security Profile Groups > Add
→ Créer un groupe "Strict-Security-Group" avec :
   - Antivirus Profile : profil configuré (contrôle 6.1)
   - Anti-Spyware Profile : profil configuré (contrôle 6.2)
   - Vulnerability Protection : profil configuré (contrôle 6.3)
   - URL Filtering : profil configuré (contrôle 6.5)
   - File Blocking : profil configuré
   - Data Filtering : profil configuré
   - WildFire Analysis : profil configuré (contrôle 6.4)

Policies > Security > [chaque règle permit]
→ Profile Group : Strict-Security-Group
```

CLI de vérification

```
show running security-policy
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
profile-setting
```

Remédiation

1. Créer un Security Profile Group consolidé dans `Objects > Security Profile Groups`
2. Attacher ce groupe à chaque règle de type `allow`
3. Vérifier avec `show running security-policy` qu'aucune règle permit n'a `profile-setting = none`
4. Exception documentée uniquement pour le trafic intrazone faible risque et validé

Valeur par défaut : Aucun profil de sécurité attaché aux règles par défaut.

Critère de conformité : 100% des règles de type Allow ont un Security Profile Group attaché incluant au minimum Anti-Virus, Anti-Spyware, Vulnerability Protection et URL Filtering.

Contrôle 4.4 — Threat Intelligence Feed et blocage des IoC connus

> ***CIS Ref :*** *7.3 (Threat Intelligence Sources)* | ***MITRE :*** *T1071* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

PAN-OS permet de configurer des External Dynamic Lists (EDL) pour bloquer automatiquement les IP et domaines malveillants connus depuis des flux de Threat Intelligence. Sans ces listes, des C2 (Command & Control) connus peuvent communiquer librement avec les hôtes internes.

Impact potentiel

- Communication non bloquée avec des serveurs C2 référencés dans les bases TI
- Exfiltration de données vers des IP malveillantes connues
- Propagation de malwares utilisant des domaines dans les blacklists publiques

Navigation

```
Objects > External Dynamic Lists > Add
→ Name : Palo-Alto-EDL-IP (ou Threat-Intel-IP)
→ Type : IP List
→ Source : https://edl.paloaltonetworks.com/premium/v50/base (PAN-DB)
   Ou sources tierces : Spamhaus, Emerging Threats, MISP
→ Check for updates : Every hour

Policies > Security > Add
→ Name : Block-ThreatIntel-IoC
→ Source/Destination : utiliser la EDL
→ Action : Deny
→ Position : avant les règles permit (en tête de rulebase)
```

CLI de vérification

```
show object external-dynamic-list all
show config running | xpath /config/devices/entry/vsys/entry/external-list
```

Remédiation

1. Créer des EDL pour les IP malveillantes, les domaines C2 et les hashes de malwares
2. Configurer l'actualisation horaire des listes
3. Créer des règles de sécurité bloquant le trafic vers/depuis les entrées EDL (en tête de politique)
4. Activer le DNS Sinkholing dans le profil Anti-Spyware (contrôle 6.2) pour les domaines malveillants
5. Configurer des notifications SIEM dédiées pour les hits sur les règles EDL (indicateurs de compromission actifs)

Valeur par défaut : Aucune EDL configurée. Pas de blocage automatique des IoC.

Critère de conformité : Au moins une EDL IP et une EDL domaine configurées avec actualisation ≤ 1h. Règles de blocage en tête de politique référençant ces listes.

Contrôle 4.5 — Policy Optimizer : migration App-ID et analyse de posture

> ***CIS Ref :*** *7.1 (Application Security Policies)* | ***MITRE :*** *T1071, T1599* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Le **Policy Optimizer** est un outil natif PAN-OS qui analyse automatiquement les règles de sécurité basées sur les ports et identifie les applications réellement utilisées dans ces flux. Sans Policy Optimizer, la migration des règles port-based vers App-ID est manuelle et difficile à maintenir dans le temps. Les règles port-based permettent le **Network Boundary Bridging** (T1599) — des applications non autorisées utilisant les mêmes ports que les applications légitimes pour contourner le filtrage.

Palo Alto recommande également d'utiliser le **Best Practice Assessment (BPA)** (`https://bpa.paloaltonetworks.com/`) pour mesurer l'usage du NGFW par rapport aux meilleures pratiques, et **AIOps for NGFW** (via Panorama) pour une évaluation continue automatisée.

Impact potentiel

- Applications malveillantes contournant le filtrage en utilisant des ports HTTP/HTTPS ouverts (T1599)
- Rule shadowing : une règle générale masque une règle spécifique, résultant en un comportement inattendu
- Règles obsolètes accumulées créant une surface d'attaque difficile à auditer
- Applications non autorisées (Tor, proxies) utilisant des ports ouverts

Navigation

```
Policies > Security > Policy Optimizer
→ Onglet "New App Viewer" : voir les nouvelles applications détectées depuis la dernière
analyse
→ Onglet "Unused Apps" : règles avec applications non utilisées depuis 90 jours
→ Onglet "No App Specified" : règles sans App-ID défini (règles port-based)

Pour chaque règle identifiée dans "No App Specified" :
→ Cliquer sur "Rule Usage" : voir les applications réellement vues dans ce flux
→ Cliquer sur "Optimize" : PAN-OS propose automatiquement les App-IDs correspondants
→ Valider et committer

Via BPA (Best Practice Assessment) :
→ Naviguer vers https://bpa.paloaltonetworks.com/
→ Exporter la configuration du firewall et analyser le rapport de conformité

Via AIOps for NGFW (Panorama) :
Panorama > AIOps > Best Practices
→ Consulter le score de conformité et les recommandations priorisées
```

CLI de vérification

```
show policy-hit-count vsys vsys1 rule-base security type pre-rulebase
show running security-policy
show application name <app-name>
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"application.*any"
```

Remédiation

1. Activer le Policy Optimizer dans `Policies > Security > Policy Optimizer`
2. Identifier toutes les règles dans l'onglet "No App Specified"
3. Pour chaque règle : analyser les applications détectées sur 30-90 jours de trafic réel
4. Utiliser la fonction "Optimize" pour convertir automatiquement les règles port-based en règles App-ID
5. Tester en mode shadow (Allow + Log) avant de supprimer la règle port-based originale
6. Exécuter régulièrement le BPA tool pour mesurer le progrès et identifier les nouvelles opportunités d'amélioration
7. Programmer des analyses mensuelles avec AIOps for NGFW si Panorama est déployé

8. Supprimer les règles avec 0 hits depuis > 90 jours après validation

Valeur par défaut : Policy Optimizer disponible mais non utilisé activement. Règles port-based créées par défaut lors de migrations depuis des firewalls legacy.

Critère de conformité : Aucune règle port-based avec `No App Specified` sur les flux Internet-facing. Analyse BPA effectuée dans les 90 derniers jours. Score de conformité BPA documenté.

Contrôle 4.6 — Profils de protection DoS et Zone Protection

> ***CIS Ref :*** *6.15, 6.16, 6.17, 6.18 (DoS Protection)* | ***MITRE :*** *T1498 (Network Denial of Service)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les attaques DoS volumétriques (T1498) et les attaques protocolaires (SYN flood, UDP flood) peuvent saturer les ressources du firewall et rendre indisponibles les services critiques. PAN-OS propose deux niveaux de protection complémentaires :

1. **Zone Protection Profiles** : protection au niveau des zones réseau (contrôle des floods entrant dans une zone)
2. **DoS Protection Profiles** : protection granulaire par règle/politique (contrôle par source, destination ou combinaison)

Ces contrôles permettent également de détecter les indicateurs CISA : les pics de trafic inhabituels et les patterns d'attaque DoS doivent générer des alertes SIEM immédiates.

Impact potentiel

- Saturation du firewall lors d'une attaque DDoS rendant l'ensemble des services indisponibles (T1498)
- Épuisement de la table des sessions empêchant les connexions légitimes
- Contournement de la protection par fragmentation IP ou attaques Layer 7

Navigation

```
-- Zone Protection Profile (protection par zone) --
Network > Network Profiles > Zone Protection > Add
→ Name : ZP-Untrust-DoS
→ Onglet "Flood Protection" :
   - SYN : Action = SYN Cookies, Alarm Rate = 10000, Activate = 20000, Maximum = 40000
   - ICMP : Action = Random Early Drop, Activate = 1000, Maximum = 5000
   - UDP : Action = Random Early Drop, Activate = 10000, Maximum = 20000
→ Onglet "Reconnaissance Protection" :
   - TCP Port Scan : block-ip (durée 3600s)
   - UDP Port Scan : block-ip
   - Host Sweep : block-ip

Network > Zones > [zone untrust]
→ Zone Protection Profile : ZP-Untrust-DoS

-- DoS Protection Profile (protection granulaire par règle) --
Objects > Security Profiles > DoS Protection > Add
→ Name : DoS-Protect-Critical-Servers
→ Type : Aggregate
→ SYN Flood : Action = SYN Cookies, Alarm Rate = 5000, Max Rate = 20000
→ UDP Flood : Action = Random Early Drop
→ ICMP Flood : Action = Random Early Drop

Policies > DoS Protection > Add
→ Name : DoS-Protect-DMZ-Servers
→ Source Zone : untrust
→ Destination Zone : dmz
→ Destination Address : IP des serveurs DMZ exposés
→ Action : Protect
→ DoS Profile : DoS-Protect-Critical-Servers
→ Log Forwarding : profil SIEM (notification sur dépassement de seuil)
```

CLI de vérification

```
show zone-protection zone untrust
show dos-protection policy
show config running | xpath /config/devices/entry/network/profiles/zone-protection-profile
show config running | xpath /config/devices/entry/vsys/entry/profiles/dos-protection
show counter global filter aspect zone-protection
```

Remédiation

1. Créer un Zone Protection Profile avec SYN Cookies pour la zone untrust
2. Créer des DoS Protection Profiles pour les serveurs DMZ exposés
3. Configurer des politiques DoS Protection couvrant les flux untrust → DMZ
4. Définir des seuils basés sur le trafic légitime observé (éviter les faux positifs)
5. Configurer des alertes SIEM sur les dépassements de seuil (indicateur d'attaque DoS en cours)
6. Valider que les logs DoS sont transmis au SIEM pour corrélation avec les indicateurs CISA

Valeur par défaut : Aucun Zone Protection Profile ni DoS Protection Profile configuré par défaut.

Critère de conformité : Zone Protection Profile avec SYN Cookies sur toutes les zones untrust. DoS Protection Profiles sur les serveurs DMZ exposés. Alertes SIEM configurées sur dépassement de seuil DoS.

Contrôle 4.7 — Kill Chain Étape 1 : Prévention de la reconnaissance via Zone Protection et Geo-IP

CIS Ref : *6.15, 6.19 (Zone Protection — Reconnaissance)* | ***MITRE :*** *T1595 (Active Scanning), T1590 (Gather Victim Network Information)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

La première étape du Kill Chain (Reconnaissance) consiste pour l'attaquant à cartographier le réseau cible : détection d'hôtes actifs (host sweeps), scan de ports TCP/UDP, fingerprinting OS et services. PAN-OS permet de détecter et bloquer ces activités directement au niveau du Zone Protection Profile. Le blocage des pays à haut risque via les External Dynamic Lists Geo-IP réduit significativement la surface d'attaque en éliminant les vecteurs d'attaque provenant de zones géographiques sans relation commerciale avec l'organisation.

Sans contrôles de reconnaissance, un attaquant peut cartographier silencieusement l'ensemble du périmètre réseau en quelques minutes, identifier les services exposés, et planifier son exploitation avec précision.

Impact potentiel

- Cartographie complète du périmètre réseau par un attaquant externe non détectée (T1595)
- Identification des versions de services via fingerprinting permettant le ciblage de CVE spécifiques
- Énumération des adresses IP actives facilitant les attaques ciblées (T1590)
- Volume élevé de sessions à faible payload : indicateur de scanning actif dans les logs

Navigation

```
-- Reconnaissance Protection dans le Zone Protection Profile --
Network > Network Profiles > Zone Protection > [ZP-Untrust-Strict] > Reconnaissance
Protection
→ TCP Port Scan :
   - Action : block-ip
   - Interval (sec) : 2
   - Threshold (ports) : 5
   - Block Duration (sec) : 3600
→ UDP Port Scan :
   - Action : block-ip
   - Interval (sec) : 10
   - Threshold (ports) : 10
   - Block Duration (sec) : 3600
→ Host Sweep :
   - Action : block-ip
   - Interval (sec) : 10
   - Threshold (hosts) : 5
   - Block Duration (sec) : 3600

IMPORTANT — Exception pour les outils de supervision internes :
→ Créer une règle d'exception avec Action = alert (non block) pour les IP des
   scanners internes légitimes (Nessus, Qualys, SIEM) afin d'éviter les faux positifs
→ Network > Network Profiles > Zone Protection > [profil] > Reconnaissance Protection
   → Exclude list : adresses IP des scanners légitimes

-- Blocage Geo-IP via External Dynamic Lists --
Objects > External Dynamic Lists > Add
→ Name : EDL-HighRisk-Countries
→ Type : IP List ou utiliser les Geo-IP régions PAN-DB
→ Ou : utiliser les régions Geo-IP natives PAN-OS :
   Policies > Security > Add
   → Name : Block-HighRisk-GeoIP
   → Source : Region > sélectionner les pays à haut risque sans relation commerciale
   → Action : Deny
   → Position : en tête de rulebase, avant les règles permit
   → Log at Session End : coché (pour analyse des tentatives bloquées)

-- Analyse des logs pour détection de scanning --
Monitor > Logs > Traffic
→ Filtrer : bytes <= 200 AND sessions-per-src-ip > 100
→ Sessions à volume élevé et faible payload = indicateur de scanning actif
→ Créer une règle SIEM : alert si sessions/IP/minute > 500 depuis la zone untrust
```

CLI de vérification

```
show zone-protection zone untrust
show config running | xpath /config/devices/entry/network/profiles/zone-protection-profile |
match reconnaissance
show counter global filter aspect zone-protection
show log threat | match "scan\|sweep"
```

Remédiation

1. Activer la Reconnaissance Protection dans tous les Zone Protection Profiles attachés aux zones externes (untrust, DMZ publiée)

2. Configurer les seuils : TCP Port Scan ≥ 5 ports en 2 secondes = block-ip, durée 1 heure
3. Configurer Host Sweep : ≥ 5 hôtes en 10 secondes = block-ip, durée 1 heure
4. **Exception critique :** ajouter les IP des scanners internes légitimes dans la liste d'exclusion avec action = alert (pas block) — sinon les outils de vulnerability assessment internes seront bloqués
5. Créer des règles de blocage Geo-IP pour les pays sans relation commerciale avec l'organisation, en tête de rulebase
6. Configurer une alerte SIEM sur les hits de reconnaissance (indicateur d'attaque en phase initiale)
7. Analyser régulièrement les logs de trafic pour les patterns de haute-fréquence/faible-volume (scanning lent non déclenché par les seuils)

Valeur par défaut : Reconnaissance Protection désactivée par défaut dans les Zone Protection Profiles. Aucun blocage Geo-IP configuré.

Critère de conformité : Reconnaissance Protection activée (TCP/UDP Port Scan + Host Sweep = block-ip) sur tous les Zone Protection Profiles des zones externes. Exception scanner interne configurée avec action = alert. Blocage Geo-IP configuré via EDL ou règles Geo-IP pour les pays à haut risque sans relation commerciale. Alertes SIEM sur hits de reconnaissance.

Domaine 5 — App-ID et User-ID

> ***Objectif :*** *Exploiter pleinement les capacités App-ID et User-ID de PAN-OS pour une politique de sécurité granulaire par application et par utilisateur, et non par port/protocole. Restreindre User-ID aux zones de confiance pour éviter l'exposition des informations d'identité. Bloquer explicitement les App-IDs "unknown" qui constituent le canal principal des C2 modernes.*

Contrôle 5.1 — App-ID activé sur toutes les politiques (aucune règle port-based)

> ***CIS Ref :*** *7.1 (Application Security Policies)* | ***MITRE :*** *T1071* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les règles basées sur les ports (service = tcp/80, tcp/443) ne distinguent pas les applications légitimes des applications malveillantes utilisant ces mêmes ports. App-ID identifie l'application réelle quelle que soit le port utilisé. Une règle permettant `service=tcp/443` autorise potentiellement des centaines d'applications différentes.

Impact potentiel

- Applications non autorisées transitant sur les ports ouverts (ex : Tor sur TCP/443)
- Tunneling d'applications dans des protocoles autorisés (SSH over HTTP, etc.)
- Impossibilité de contrôler la granularité applicative sans App-ID

Navigation

```
Policies > Security > [chaque règle]
→ Application : remplacer "any" par la liste d'applications spécifiques
→ Service : définir sur "application-default" (suit le port standard de l'application)

Objects > Applications > [application]
→ Vérifier les ports par défaut pour chaque application autorisée
```

CLI de vérification

```
show running security-policy
show application name <application>
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"application.*any"
```

Remédiation

1. Inventorier les applications légitimes utilisées dans chaque flux réseau
2. Remplacer `Application = any` par la liste nominative des applications nécessaires

3. Définir `Service = application-default` pour laisser App-ID gérer les ports
4. Activer `Application Exception` pour les applications utilisant des ports non standard avec justification documentée
5. Utiliser le Policy Optimizer (contrôle 4.5) pour identifier automatiquement les applications dans les règles port-based
6. Utiliser `App-ID Cloud Engine` pour obtenir des mises à jour App-ID en temps réel

Valeur par défaut : Les règles créées manuellement peuvent avoir `Application = any`. App-ID est actif par défaut mais n'est pas forcé dans la politique.

Critère de conformité : Aucune règle allow avec `Application = any` sur des flux Internet-facing. Service = `application-default` sur toutes les règles sauf exceptions documentées.

Contrôle 5.2 — User-ID restreint aux interfaces de confiance

> ***CIS Ref :*** *2.3, 2.4 (User-ID)* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

Description du risque

User-ID doit être activé uniquement sur les interfaces internes (zones trust). L'activer sur une interface untrust expose les mappages IP-utilisateur aux réseaux non approuvés et permet à un attaquant externe de cibler des comptes nominatifs en connaissant leurs adresses IP.

Impact potentiel

- Fuite des informations utilisateur (IP-to-username mapping) vers des zones non sécurisées
- Ciblage spécifique d'utilisateurs à hauts privilèges identifiés via User-ID
- Attaques d'usurpation d'identité utilisateur facilité par la connaissance des mappages

Navigation

```
Network > Interfaces > [interface interne] > Advanced > Other Info
→ User Identification ACL : Include List = réseaux internes uniquement
→ Exclure les réseaux sensibles (serveurs, zones DMZ)

Device > User Identification > User-ID Agents
→ Vérifier que l'agent n'est déployé que sur les contrôleurs de domaine internes

Device > Setup > User-ID > Network Access (Include / Exclude)
→ Include Networks : 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
→ Exclude Networks : sous-réseaux serveurs, DMZ, adresses IP de service
```

CLI de vérification

```
show user ip-user-mapping all
show user group-mapping state all
show config running | xpath /config/devices/entry/vsys/entry/user-id-agent
```

Remédiation

1. Désactiver User-ID sur toutes les interfaces untrust/DMZ
2. Définir explicitement `Include Networks` avec les sous-réseaux internes utilisateurs uniquement
3. Ajouter les sous-réseaux serveurs et de service dans `Exclude Networks` pour éviter les faux mappages
4. Désactiver le `WMI Probing` (contrôle 5.3) sauf besoin justifié

Valeur par défaut : User-ID désactivé par défaut. Si activé, aucune restriction réseau par défaut.

Critère de conformité : User-ID activé uniquement sur les interfaces internes (trust). Include/Exclude Networks configurés pour exclure les zones DMZ, untrust et les sous-réseaux serveurs.

Contrôle 5.3 — Désactivation du WMI Probing

> ***CIS Ref :*** *2.2 (WMI Probing disabled)* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

Description du risque

Le WMI Probing permet au firewall de sonder activement les machines Windows pour obtenir les informations de connexion utilisateur. Cette technique génère un trafic réseau WMI potentiellement intercepté et constitue une surface d'attaque supplémentaire. Les environnements modernes utilisent l'agent User-ID ou les redirecteurs de logs AD pour un mappage passif.

Impact potentiel

- Trafic WMI généré par le firewall pouvant être détecté et exploité
- Faux positifs dans les mappages si des machines WMI sont inaccessibles
- Exposition des credentials de service WMI si le compte utilisé est compromis

Navigation

```
Device > User Identification > Discovery
→ WMI Probing : décocher "Enable WMI Probing"

Ou dans la configuration User-ID Agent :
Device > User Identification > User-ID Agents > [agent] > WMI Probing
→ Désactiver
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/user-id-collector/setting |
match wmi
```

Remédiation

1. Désactiver WMI Probing dans `Device > User Identification > Discovery`
2. Utiliser à la place : User-ID Agent installé sur les DC, Syslog redistribution depuis les DC, ou LDAP Group Mapping passif

3. Documenter la méthode de mappage utilisateur alternative retenue

Valeur par défaut : WMI Probing désactivé par défaut.

Critère de conformité : WMI Probing = désactivé. Mappage utilisateur réalisé via méthode passive (agent, syslog redistribution).

Contrôle 5.4 — Restriction du compte de service User-ID Agent

CIS Ref : *2.5, 2.6, 2.7 (User-ID Agent permissions)* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

Description du risque

Le compte de service utilisé par l'agent User-ID pour lire les logs d'événements Active Directory doit avoir des droits minimaux. Un compte de service avec des droits administrateur de domaine ou des droits d'ouverture de session interactive constitue un vecteur d'escalade de privilèges si compromis.

Impact potentiel

- Compromission du compte de service donnant accès à l'ensemble de l'AD
- Utilisation du compte de service pour des connexions interactives non autorisées
- Mouvement latéral facilité si le compte a des droits excessifs

Navigation

```
Sur le contrôleur de domaine :
→ Créer un compte de service dédié (ex : svc_useridagent)
→ Droits requis uniquement : "Read" sur l'Observateur d'événements (Security logs)
→ Désactiver "Interactive logon" pour ce compte (GPO)
→ Désactiver "Remote access" pour ce compte

Sur le firewall :
Device > User Identification > User-ID Agents > [agent]
→ Server Credentials : utiliser le compte de service minimal
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/user-id-agent
show user user-id-agent statistics
```

Remédiation

1. Créer un compte de service AD dédié avec droits minimaux (lecture seule sur Security Event Log)
2. Désactiver la connexion interactive et l'accès distant pour ce compte via GPO
3. Configurer le compte dans l'agent User-ID
4. Vérifier que le compte n'est pas membre de groupes privilégiés (Admins du domaine, etc.)
5. Renouveler le mot de passe du compte de service tous les 90 jours (ou utiliser gMSA)

Valeur par défaut : Aucun compte de service configuré par défaut. L'administrateur doit le créer lors du déploiement.

Critère de conformité : Compte de service User-ID avec droits minimaux uniquement. Connexion interactive désactivée. Renouvellement de mot de passe ≤ 90 jours ou utilisation d'un gMSA.

Contrôle 5.5 — Prévention des évasions L4/L7 : blocage des App-ID "unknown"

> ***CIS Ref :*** *7.1 (App-ID), Best Practices L4/L7 Evasions* | ***MITRE :*** *T1071.001 (Web Protocols), T1572 (Protocol Tunneling), T1008 (Fallback Channels)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les attaquants utilisent systématiquement les protocoles non reconnus par App-ID — classifiés comme `unknown-tcp` et `unknown-udp` — pour établir leurs canaux C2 (Command & Control). Ces App-IDs "unknown" correspondent à des protocoles propriétaires, des applications personnalisées, ou des communications chiffrées non standard. Bloquer explicitement `unknown-tcp`, `unknown-udp` et `unknown-p2p` est la technique de blocage C2 la plus efficace car la grande majorité des C2 modernes (Cobalt Strike, Metasploit, outils APT) utilisent des protocoles non identifiés par App-ID.

Une règle `allow` sans App-ID explicite ou avec `application = any` permet à n'importe quel outil offensif de communiquer librement. La référence Palo Alto "Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions" documente en détail ces vecteurs d'attaque.

Impact potentiel

- Canaux C2 utilisant des protocoles inconnus transitant librement dans les règles génériques (T1071)
- Tunneling de protocoles dans des flux autorisés (T1572 — DNS over HTTPS, ICMP tunneling)
- Canaux de fallback C2 sur des protocoles non standard contournant les profils Anti-Spyware (T1008)
- Exfiltration de données via des protocoles propriétaires non inspectés

Navigation

```
-- Règle de blocage explicite des App-IDs unknown --
Policies > Security > Add
→ Name : Block-Unknown-AppIDs
→ Source Zone : any
→ Destination Zone : untrust (ou any pour couvrir tous les flux)
→ Application : unknown-tcp, unknown-udp, unknown-p2p
   (ajouter aussi : insufficient-data pour les sessions courtes non identifiées)
→ Service : any
→ Action : Deny
→ Log at Session End : coché
→ Log Forwarding : Forward-All-to-SIEM
→ Position : AVANT les règles d'autorisation générales

-- Vérification des règles without security profiles --
Policies > Security
→ Identifier toutes les règles "allow" sans Security Profile Group
→ Aucune règle allow ne doit exister sans profil de sécurité attaché
→ Si une règle allow est nécessaire sans profil : justification documentée obligatoire

-- Activation de l'inspection sur TOUTES les règles allow --
Policies > Security > [chaque règle allow]
→ Profile Setting > Group : sélectionner Security Profile Group "best-practice"
→ Aucune exception sauf trafic interne documenté à faible risque

-- Référence : Palo Alto Best Practices for L4/L7 Evasions --
→ https://docs.paloaltonetworks.com/best-practices/
→ Section : "Securing Your Network from Layer 4 and Layer 7 Evasions"
```

CLI de vérification

```
show running security-policy | match unknown
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"unknown"
show application name unknown-tcp
show application name unknown-udp
show log traffic app unknown-tcp
show log traffic app unknown-udp
```

Remédiation

1. Créer une règle de blocage explicite en tête de rulebase couvrant `unknown-tcp`, `unknown-udp`, `unknown-p2p`
2. Activer le logging sur cette règle et transmettre au SIEM — chaque hit est un indicateur de C2 potentiel
3. Vérifier qu'aucune règle `allow` n'existe avec `Application = any` sur les flux Internet (contrôle 5.1)
4. S'assurer que chaque règle `allow` a un Security Profile Group attaché — une règle allow sans profil est un angle mort de sécurité
5. Auditer les applications `unknown-tcp` dans les logs sur 30 jours pour identifier les faux positifs légitimes avant d'activer le blocage
6. Exception documentée : applications métier propriétaires utilisant des protocoles non reconnus — créer des App-ID personnalisés ou des exceptions spécifiques au-dessus de la règle de blocage
7. Activer l'App-ID Cloud Engine pour des mises à jour de signatures en temps réel

Valeur par défaut : Les applications `unknown-tcp` et `unknown-udp` sont autorisées si une règle `allow` générale existe. Aucun blocage explicite par défaut.

Critère de conformité : Règle de blocage explicite pour `unknown-tcp`, `unknown-udp`, `unknown-p2p` en position prioritaire dans la rulebase. Logging activé sur ces règles. Aucune règle allow Internet-facing sans Security Profile Group. Hits sur les règles “unknown” transmis au SIEM avec alerte configurée.

Contrôle 5.6 — CVE-2026-0300 : Zero-Day Authentication Portal (Captive Portal) — RCE sans authentification

CIS Ref : *CVE / PSIRT Advisory* | ***MITRE :*** *T1190 (Exploit Public-Facing Application), T1059 (Command Execution), T1078 (Valid Accounts — post-exploitation)* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

CVE-2026-0300 (CVSS 9.3 si portail exposé sur Internet, 8.7 si restreint à l’interne) est un buffer overflow critique dans le composant **User-ID™ Authentication Portal** (Captive Portal) de PAN-OS. Cette vulnérabilité permet à un attaquant **non authentifié** d’exécuter du code arbitraire avec les droits root via le réseau, sans aucune interaction utilisateur.

L’exploitation active a débuté le **9 avril 2026** avec une RCE confirmée le **16 avril 2026**. Au moment de sa publication, **67 serveurs vulnérables** étaient identifiables sur Shodan exposant les ports **6081** et **6082** (ports du Captive Portal). La vulnérabilité a été ajoutée au catalogue **CISA KEV** (Known Exploited Vulnerabilities) et fait l’objet d’un Threat Brief publié par **Palo Alto Unit 42**.

Chaîne d’exploitation observée : 1. Scan des ports 6081/6082 exposés sur Internet → identification des cibles vulnérables 2. Envoi d’une requête réseau malformée déclenchant le buffer overflow dans le Captive Portal 3. Obtention d’un shell root sur le firewall sans aucune authentification (T1190) 4. Post-exploitation : énumération Active Directory via le firewall compromis (T1078) 5. Déploiement des malwares **EarthWorm** et **ReverseSocks5** pour persistance et C2

Systèmes affectés : PA-Series et VM-Series sous PAN-OS 10.2, 11.1, 11.2, 12.1 (versions non patchées).

Impact potentiel

- Exécution de code arbitraire avec droits root sur le firewall sans aucun credential (T1190)
- Compromission totale du firewall et accès à toutes les zones réseau contrôlées
- Énumération de l’Active Directory depuis le firewall compromis (T1078 post-exploitation)
- Installation de malwares persistants (EarthWorm, ReverseSocks5) comme relais réseau
- Pivot réseau complet depuis le firewall vers les systèmes internes
- Détection difficile : l’exploitation initiale ne laisse aucune trace d’authentification dans les logs

Navigation — Mitigations (par ordre de priorité)

```
-- Mitigation 1 : Appliquer le patch immédiatement --
Device > Software > Check Now
→ Versions corrigées (disponibles du 13 au 28 mai 2026 selon le train) :
   - PAN-OS 12.1.4-h5 ou 12.1.7
   - PAN-OS 11.2.x (version fixée disponible)
   - PAN-OS 11.1.x (version fixée disponible)
   - PAN-OS 10.2.x (version fixée disponible)
→ Consulter https://security.paloaltonetworks.com/CVE-2026-0300 pour les versions exactes

-- Mitigation 2 (URGENTE si patch impossible) : Restreindre le Captive Portal aux zones
internes --
Network > Network Profiles > Interface Mgmt
→ Éditer CHAQUE profil attaché aux interfaces L3 exposées sur Internet/zones non fiables
→ Décocher "Response Pages" sur les profils des interfaces WAN/DMZ/untrust
→ NE JAMAIS exposer le Captive Portal (ports 6081/6082) vers Internet

-- Mitigation 3 : Désactiver les Response Pages sur les interfaces Internet-facing --
Network > Network Profiles > Interface Mgmt > [profil interface WAN]
→ Décocher "Response Pages"
→ Répéter pour TOUS les profils attachés aux interfaces untrust et DMZ publiques

-- Mitigation 4 : Désactiver le Captive Portal si non utilisé --
Device > User Identification > Captive Portal Settings
→ Décocher "Enable Captive Portal"
→ OU : restreindre à des zones internes de confiance uniquement

-- Mitigation 5 : Activer le Threat ID 510019 (patch virtuel) --
Requiert PAN-OS 11.1+ et licence Threat Prevention :
Objects > Security Profiles > Vulnerability Protection > [profil] > Exceptions
→ Rechercher Threat ID : 510019
→ Action : block-ip (source)
→ Packet Capture : extended-capture
→ Activer la signature comme patch virtuel jusqu'à disponibilité du patch logiciel
```

CLI de vérification

```
# Vérifier la version PAN-OS actuelle
show system info | match sw-version

# Vérifier si le Captive Portal est activé
show user interface all | match captive

# Vérifier les profils Interface Management pour les Response Pages
show config running | xpath /config/devices/entry/network/profiles/interface-management-
profile | match "response-pages"

# Identifier les interfaces avec des profils exposant des Response Pages
show interface all | match "response"

# Vérifier si des connexions actives sur les ports 6081/6082 existent
show session all filter destination-port 6081
show session all filter destination-port 6082

# Vérifier l'état du Captive Portal
show user captive-portal statistics
show config running | xpath /config/devices/entry/vsys/entry/captive-portal
```

Remédiation

1. **Action immédiate (< 4h)** : Appliquer les patches PAN-OS disponibles sur le site PSIRT. En HA : patcher le passif en premier.
2. **Si patch impossible immédiatement** : Désactiver les `Response Pages` dans tous les profils Interface Management des interfaces untrust/Internet-facing. Cette mitigation est **immédiate et sans impact sur les services**.
3. Désactiver complètement le Captive Portal (`Device > User Identification > Captive Portal Settings`) si cette fonctionnalité n'est pas utilisée — la désactivation est la mesure de mitigation la plus propre.
4. Si le Captive Portal est nécessaire : le restreindre **exclusivement aux zones internes de confiance** — jamais sur des interfaces Internet-facing.
5. Sur PAN-OS 11.1+ : activer le Threat ID 510019 dans le profil Vulnerability Protection pour une protection par signature.
6. Scanner l'ensemble du périmètre réseau pour identifier les services exposant les ports 6081/6082 (`nmap -p 6081,6082 <plage-WAN>` depuis un scanner externe).
7. Vérifier les logs de la période d'exposition (à partir du 9 avril 2026) pour des indicateurs de compromission : activité inhabituelle depuis le firewall, nouvelles connexions sortantes, modifications de configuration non planifiées.
8. Si une compromission est suspectée : isoler le firewall, ne pas redémarrer, contacter **Palo Alto PSIRT** en urgence et ouvrir un ticket de réponse aux incidents.

Valeur par défaut : Le Captive Portal peut être activé dans certaines configurations User-ID. Les profils Interface Management exposent par défaut les Response Pages si non modifiés.

Critère de conformité : PAN-OS mis à jour vers une version corrigée CVE-2026-0300. `Response Pages` = désactivé sur tous les profils Interface Management des interfaces untrust/Internet. Captive Portal restreint aux zones internes ou désactivé si inutilisé. Vérification Threat ID 510019 si PAN-OS 11.1+ non encore patché.

Contrôle 5.7 — Durcissement avancé User-ID : WMI Probing, Include/Exclude Lists et restriction Captive Portal

CIS Ref : *2.2, 2.3, 2.4 (User-ID Hardening)* | ***MITRE :*** *T1078 (Valid Accounts), T1557 (Adversary-in-the-Middle), T1190* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le composant User-ID est l'un des vecteurs d'attaque les plus sous-estimés des NGFW Palo Alto. Plusieurs risques combinés peuvent permettre à un attaquant d'empoisonner les mappages IP-utilisateur, de cibler des comptes à hauts privilèges, ou d'exploiter le Captive Portal (CVE-2026-0300). Les trois contrôles suivants sont interdépendants et doivent être appliqués ensemble :

Risque 1 — WMI Probing dans les réseaux haute sécurité : Le WMI Probing fait **confiance aux données retournées par les endpoints Windows**, sans validation d'intégrité. Un endpoint compromis (ou un attaquant contrôlant une machine) peut retourner de faux mappages IP-utilisateur, empoisonnant la base User-ID du firewall. Cela peut permettre à un attaquant de se faire passer pour un utilisateur privilégié dans les logs et de contourner les politiques User-ID.

Risque 2 — Include/Exclude Networks non configurés : Sans listes d'inclusion/exclusion explicites, User-ID peut tenter de mapper des IP de serveurs critiques, de contrôleurs de domaine, ou de réseaux invités — créant des faux positifs et une surface d'attaque élargie.

Risque 3 — Captive Portal exposé à des zones non sécurisées : Même sans CVE-2026-0300, exposer le Captive Portal à des zones non sécurisées constitue un vecteur d'attaque permanent. Le Captive Portal ne doit être accessible que depuis des zones internes de confiance.

Impact potentiel

- Empoisonnement des mappages User-ID par un endpoint malveillant via WMI (T1557)
- Ciblage de comptes utilisateurs à hauts privilèges identifiés via les mappages corrompus (T1078)
- Dépendance circulaire dangereuse si les contrôleurs de domaine sont inclus dans les réseaux User-ID
- Exposition du Captive Portal comme surface d'attaque permanente (T1190)
- Fuite des informations d'identité réseau vers des zones non autorisées

Navigation

```
-- 1. Désactiver WMI Probing dans les réseaux haute sécurité --
Device > User Identification > User Mapping
→ Section "Windows-based User ID Agent" > WMI Probing
→ Décocher "Enable WMI Probing"

CLI :
set deviceconfig setting user-id wmi-poll disable

Alternative recommandée (passive) :
→ Utiliser l'agent User-ID déployé sur les contrôleurs de domaine
→ Ou : redistribution Syslog des événements d'authentification Windows
→ Ou : LDAP Group Mapping (passif, sans probing)

-- 2. Configurer les listes Include/Exclude Networks --
Device > User Identification > User Mapping > Include/Exclude Networks

Section "INCLUDE" — Ajouter uniquement les réseaux des postes utilisateurs :
→ Exemple : 10.10.0.0/16 (postes utilisateurs uniquement)
→ Exemple : 172.16.50.0/24 (postes nomades)
→ NE PAS inclure les réseaux serveurs, DC, ou DMZ

Section "EXCLUDE" — Exclure explicitement les réseaux sensibles :
→ Sous-réseaux des contrôleurs de domaine (ex : 10.0.0.0/26)
→ Sous-réseaux des serveurs de monitoring (SIEM, Splunk, etc.)
→ Réseaux invités/WiFi invité
→ Segments DMZ
→ Adresses IP de service (imprimantes, téléphones IP, IoT)

CLI :
set user-id-include-exclude-network include <network/prefix>
set user-id-include-exclude-network exclude <network/prefix>

-- 3. Restreindre le Captive Portal aux zones internes uniquement --
(Si le Captive Portal doit rester actif)

Network > Network Profiles > Interface Mgmt > [profil WAN/untrust]
→ Décocher "Response Pages" sur tous les profils des interfaces Internet-facing

Device > User Identification > Captive Portal Settings
→ Vérifier que le Captive Portal n'est activé que sur les interfaces internes
→ Configurer "Inactivity Timer" et "Timer" avec des valeurs courtes (1-2h max)
→ Utiliser une méthode d'authentification forte (SAML/Kerberos, pas NTLM)

CLI pour vérifier les zones où le Captive Portal est actif :
show user captive-portal statistics
show config running | xpath /config/devices/entry/vsys/entry/captive-portal
```

CLI de vérification

```
# Vérifier l'état du WMI Probing
show config running | xpath /config/devices/entry/vsys/entry/user-id-collector/setting |
match wmi

# Vérifier les Include/Exclude Networks configurés
show config running | xpath /config/devices/entry/vsys/entry/user-id-include-exclude

# Vérifier les mappages utilisateur actifs (recherche d'anomalies)
show user ip-user-mapping all
show user ip-user-mapping ip <IP-suspecte>

# Vérifier la configuration du Captive Portal
show user captive-portal statistics
show config running | xpath /config/devices/entry/vsys/entry/captive-portal

# Vérifier les interfaces avec Response Pages activées
show config running | xpath /config/devices/entry/network/profiles/interface-management-
profile | match "response"
```

Remédiation

1. **Désactiver WMI Probing** dans `Device > User Identification > User Mapping` — utiliser à la place l'agent User-ID sur les DC (méthode passive plus sûre).
2. **Configurer les Include Networks** : inclure uniquement les sous-réseaux hébergeant des postes utilisateurs managés. Ne jamais inclure les réseaux serveurs ou les contrôleurs de domaine.
3. **Configurer les Exclude Networks** : exclure explicitement les DC (évite la dépendance circulaire AD↔Firewall), les serveurs de sécurité (SIEM, scanners), les réseaux invités, et les segments DMZ.
4. **Restreindre le Captive Portal** : désactiver `Response Pages` sur tous les profils Interface Management des interfaces Internet-facing (mesure critique pour CVE-2026-0300).
5. Si le Captive Portal est utilisé : forcer l'authentification SAML ou Kerberos (éviter NTLM qui est vulnérable au relay).
6. Auditer régulièrement les mappages User-ID avec `show user ip-user-mapping all` pour détecter des IP d'infrastructures (DC, SIEM) dans les mappages.
7. Documenter les réseaux inclus/exclus dans la matrice de segmentation réseau de l'organisation.

Valeur par défaut : WMI Probing peut être activé selon la configuration. Include/Exclude Networks non configurés par défaut (tous les réseaux traités). Captive Portal potentiellement actif sur toutes les interfaces.

Critère de conformité : WMI Probing désactivé dans les réseaux haute sécurité. Include Networks limités aux sous-réseaux postes utilisateurs. Contrôleurs de domaine et réseaux sensibles dans Exclude Networks. `Response Pages` désactivé sur tous les profils Interface Management des interfaces untrust. Méthode de mappage User-ID passive documentée.

Domaine 6 — Threat Prevention et WildFire

Objectif : *Déployer des profils de sécurité best-practice complets pour couvrir les étapes 5 (Installation) et 6 (C2) du Kill Chain. WildFire fournit une analyse sandbox pour les fichiers inconnus. Les profils Anti-Spyware avec DNS Sinkhole et le blocage des App-IDs "unknown" constituent les contrôles C2 les plus efficaces. Le blocage des fichiers PE et des archives chiffrées prévient l'installation de malwares. Ces profils doivent être regroupés dans un Security Profile Group "best-practice" et attachés à toutes les règles allow sans exception.*

Déploiement phasé recommandé (approche entreprise) : *Ne jamais passer directement en mode blocage sur un environnement de production inconnu. Le déploiement en 5 phases garantit une adoption sans rupture de service.*

Phase 1 — Planification (Semaine 0) : *Définir trois groupes de profils de sécurité :* `secure` *(blocage complet),* `alert-only` *(alerte uniquement, aucun blocage),* `secure-webservers` *(profil spécifique aux serveurs exposés). Identifier les exceptions prévisibles par zone et type de système.*

Phase 2 — Collecte de données (Semaines 1–4) : *Déployer les profils* `alert-only` *sur* ***toutes*** *les règles de sécurité. Collecter au moins 30 jours de télémétrie de menaces incluant les basculements HA et les événements spéciaux (déploiements, maintenances). Consulter* `Dashboard > Threat Activity` *pour identifier les patterns.*

Phase 3 — Analyse du risque : *Catégoriser les règles : (a) zéro hit de menace → candidats immédiats au durcissement ; (b) > 250 000 sessions avec < 0,01% de menaces → candidats sûrs ; (c) activité de menace significative → analyse manuelle requise par le propriétaire du système.*

Phase 4 — Durcissement sélectif : *Passer progressivement de* `alert-only` *à* `secure` *en commençant par les règles à faible risque. Documenter les exceptions approuvées par le responsable du système.*

Phase 5 — Standardisation : *Toutes les nouvelles règles reçoivent automatiquement le groupe* `secure`*. BPA/AIOps valide une couverture à 100%.*

Note de performance : *Threat Prevention entraîne une réduction de débit d'environ 50% — des benchmarks pré-déploiement sont indispensables sur les règles à haut débit avant activation du mode blocage.*

Contrôle 6.1 — Profil Antivirus best-practice : WildFire Inline ML et reset-both

CIS Ref : *6.1, 6.20 (Antivirus profiles)* | ***MITRE :*** *T1059, T1566* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le profil Antivirus par défaut utilise l'action `default` qui peut ne pas bloquer sur certains décodeurs. Le CIS Benchmark exige l'action `reset-both` (réinitialisation de la connexion côté client et serveur) sur tous les décodeurs sauf IMAP et POP3 (qui nécessitent `reset-client`). La fonctionnalité **WildFire Inline ML** (Machine Learning inline) détecte en temps réel les menaces sans soumettre à WildFire cloud — critique pour les menaces zero-day. Sur PAN-OS 10.0+, activer "Hold for WildFire Real Time Signature Lookup" retient les sessions suspectes jusqu'à réception de la signature, éliminant la fenêtre de vulnérabilité entre la détection et le blocage.

Impact potentiel

- Malwares transmis via HTTP, FTP, SMTP, SMB non bloqués si action = alert
- Contournement de l'inspection antivirus via des protocoles avec action permissive
- Ransomwares et chevaux de Troie transitant sans obstruction
- Fichiers malveillants zero-day non détectés sans WildFire Inline ML

Navigation

```
Objects > Security Profiles > Antivirus > Add
→ Name : AV-BestPractice

Onglet "Antivirus" — WildFire Signature Action (7 protocoles) :
→ FTP : reset-both
→ HTTP : reset-both
→ HTTP2 : reset-both
→ IMAP : reset-client
→ POP3 : reset-client
→ SMB : reset-both
→ SMTP : reset-both

Onglet "WildFire Inline ML" — WildFire Inline ML Action (7 protocoles) :
→ FTP : reset-both
→ HTTP : reset-both
→ HTTP2 : reset-both
→ IMAP : reset-client
→ POP3 : reset-client
→ SMB : reset-both
→ SMTP : reset-both

Onglet "Threat Exceptions" : vide (pas d'exceptions sauf cas documenté)

Options globales :
Device > Setup > WildFire
→ "Enable real-time signature lookup" : coché (globalement)
→ Dans le profil : "Hold for WildFire Real Time Signature Lookup" : activé

Navigation : Objects > Security Profiles > Antivirus > [profil] > WildFire Inline ML
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/profiles/virus
show antivirus-signature-version
show wildfire status
```

Remédiation

1. Créer un nouveau profil Antivirus `AV-BestPractice`
2. Configurer `reset-both` sur FTP, HTTP, HTTP2, SMB, SMTP dans la section WildFire Signature
3. Configurer `reset-client` sur IMAP et POP3 (les serveurs mail ne supportent pas reset-both)
4. Répliquer les mêmes actions dans la section WildFire Inline ML pour les 7 mêmes protocoles
5. Activer la recherche de signatures en temps réel globalement : `Device > Setup > WildFire > Enable real-time signature lookup`
6. Activer “Hold for WildFire Real Time Signature Lookup” dans le profil pour retenir les sessions suspectes
7. Attacher ce profil au Security Profile Group “best-practice” (contrôle 6.9)

Valeur par défaut : Profil Antivirus par défaut avec action `default` (variable selon le décodeur). WildFire Inline ML désactivé. Pas de “Hold” activé.

Critère de conformité : Profil Antivirus avec `reset-both` sur FTP/HTTP/HTTP2/SMB/SMTP et `reset-client` sur IMAP/POP3 dans les deux sections (WildFire Signature ET WildFire Inline ML). Real-time signature lookup global = activé. Profil attaché à toutes les règles allow. Signatures datant de moins de 25h.

Contrôle 6.2 — Profil Anti-Spyware best-practice : DNS Sinkhole et détection C2

> ***CIS Ref :*** *6.3, 6.4, 6.5 (Anti-Spyware)* | ***MITRE :*** *T1041, T1568 (Dynamic Resolution), T1071.004 (DNS)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le profil Anti-Spyware est le contrôle le plus critique pour la détection des communications C2 (Kill Chain étape 6). Il doit être activé sur **tout le trafic autorisé** sans exception. Le DNS Sinkhole redirige les requêtes DNS vers des domaines malveillants vers l’IP sinkhole de Palo Alto (`sinkhole.paloaltonetworks.com`), permettant l’identification immédiate des hôtes infectés — toute IP interne contactant l’IP sinkhole dans les logs est un indicateur de compromission (IoC) certifié.

La configuration recommandée des DNS Policies couvre les 5 catégories de domaines malveillants avec des niveaux de capture de paquets adaptés à la criticité.

Impact potentiel

- Communications C2 actives depuis des hôtes infectés non détectées sans Anti-Spyware
- Exfiltration de données via DNS tunneling (T1071.004)
- Persistance de malwares non détectés sans sinkholing
- Domaines C2 à rotation rapide (DGA) non bloqués sans signature Anti-Spyware à jour

Navigation

```
Objects > Security Profiles > Anti-Spyware > Add
→ Name : AntiSpyware-BestPractice

Onglet "Signature Policies" — Règles par sévérité :
→ Critical : Action = block-ip (source, durée 3600s) + extended-capture
→ High : Action = reset-both + single-packet capture
→ Medium : Action = reset-both + single-packet capture
→ Low : Action = default + single-packet capture
→ Informational : Action = default (pas de capture)

Règles "Brute Force" :
→ Action = reset-both + single-packet capture

Inline Cloud Analysis (Advanced Threat Prevention) :
→ Action = reset-both

Onglet "DNS Policies" — Configuration recommandée :
→ C2 Domains : Action = sinkhole + extended-capture, Severity = critical/high
→ Malware Domains : Action = sinkhole + single-packet, Severity = medium
→ Phishing Domains : Action = sinkhole + single-packet, Severity = medium/low
→ Parked Domains : Action = sinkhole + single-packet, Severity = low/informational
→ Grayware : Action = sinkhole + single-packet, Severity = informational
→ Dynamic DNS : Action = sinkhole + single-packet, Severity = low

DNS Sinkhole Settings (dans le profil) :
→ Enable Sinkhole : coché
→ IPv4 Sinkhole Address : sinkhole.paloaltonetworks.com (ou IP interne dédiée)
→ IPv6 Sinkhole Address : ::1

IMPORTANT : Autoriser le trafic DNS UNIQUEMENT vers les serveurs DNS sanctionnés :
Policies > Security > Add
→ Name : Allow-Sanctioned-DNS-Only
→ Application : dns
→ Destination : [IP des serveurs DNS internes autorisés]
→ Action : Allow (avec Anti-Spyware profile attaché)
→ Bloquer tout autre trafic DNS (dns vers any = Deny)

Navigation : Objects > Security Profiles > Anti-Spyware > [profil] > DNS Policies
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/profiles/spyware
show threat-signatures version
show dns-proxy all
```

Remédiation

1. Créer le profil `AntiSpyware-BestPractice` avec les sévérités configurées selon le tableau ci-dessus
2. Activer DNS Sinkholing avec l'IP par défaut `sinkhole.paloaltonetworks.com`
3. Configurer les 6 catégories de domaines dans DNS Policies avec les actions et captures appropriées
4. Créer une règle de sécurité forçant le DNS uniquement vers les serveurs DNS sanctionnés — bloquer tout autre trafic DNS
5. Créer une règle d'alerte sur le trafic vers l'IP sinkhole (hôte contactant le sinkhole = IoC immédiat)

6. Attacher ce profil à toutes les règles allow (pas uniquement Internet-facing mais ALL traffic)
7. Nécessite : licence Advanced Threat Prevention ou Threat Prevention

Valeur par défaut : Profil Anti-Spyware par défaut avec actions `default`. DNS Sinkholing désactivé. DNS Policies non configurées.

Critère de conformité : Profil Anti-Spyware avec block sur Critical (block-ip), reset-both sur High et Medium. DNS Sinkholing activé. Les 6 catégories de domaines configurées dans DNS Policies. Restriction DNS aux serveurs sanctionnés. Profil attaché à toutes les règles allow (tout le trafic). Alerte SIEM sur hits sinkhole.

Contrôle 6.3 — Profil Vulnerability Protection best-practice : inspection complète

CIS Ref : *6.6, 6.7 (Vulnerability Protection)* | ***MITRE :*** *T1190, T1203* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les exploits ciblant des vulnérabilités applicatives connues (Apache, Exchange, navigateurs) transitent dans des flux HTTP/HTTPS autorisés. Le profil Vulnerability Protection inspecte ce trafic et bloque les tentatives d'exploitation. Sans ce profil, les CVE critiques peuvent être exploitées même si le firewall autorise le trafic applicatif. L'**Inline Cloud Analysis** (Advanced Threat Prevention) complète la protection en détectant les exploits zero-day via analyse cloud en temps réel.

Impact potentiel

- Exploitation de CVE critiques dans les applications exposées (serveurs web, messagerie)
- Compromission d'hôtes internes via des exploits dans des flux autorisés
- Propagation de vers réseau exploitant des vulnérabilités connues (EternalBlue, etc.)

Navigation

```
Objects > Security Profiles > Vulnerability Protection > Add
→ Name : VulnProt-BestPractice

Règles par sévérité :
→ Critical :
   - Action : reset-both
   - Packet Capture : single-packet
   (ou block-ip source durée 300s pour les exploits actifs)

→ High :
   - Action : reset-both
   - Packet Capture : single-packet

→ Medium :
   - Action : default (reset ou alert selon la signature)
   - Packet Capture : single-packet

→ Low :
   - Action : default
   - Packet Capture : single-packet

→ Informational :
   - Action : default
   - Packet Capture : disable

Règles "Brute Force" :
→ Action : reset-both + single-packet capture

Onglet "Inline Cloud Analysis" (Advanced Threat Prevention requis) :
→ Action : reset-both

Onglet "Exceptions" :
→ CVE spécifiques en cours d'exploitation active (CISA KEV) : forcer block-ip si serveur non
patché
→ Créer des exceptions documentées pour réduire les faux positifs sur applications métier

Navigation : Objects > Security Profiles > Vulnerability Protection
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/profiles/vulnerability
show vulnerability-signature version
```

Remédiation

1. Créer `VulnProt-BestPractice` avec les actions par sévérité définies ci-dessus
2. Activer single-packet PCAP sur Critical, High et Medium pour forensique
3. Activer Inline Cloud Analysis si licence Advanced Threat Prevention disponible (action = reset-both)
4. Pour les CVE dans le catalogue CISA KEV non encore patchés : forcer block-ip dans les exceptions
5. Attacher le profil à toutes les règles allow (pas uniquement Internet-facing)

Valeur par défaut : Profil Vulnerability Protection avec action `default`. Pas de capture de paquets. Inline Cloud Analysis désactivé.

Critère de conformité : Profil VP avec reset-both sur Critical et High, single-packet PCAP sur Critical/High/Medium. Inline Cloud Analysis = reset-both si licence disponible. Profil attaché à toutes les règles allow. Signatures à jour (< 8 jours).

Contrôle 6.4 — Profil WildFire Analysis best-practice : tous fichiers bidirectionnel

CIS Ref : *5.1, 5.2, 5.3, 5.6 (WildFire)* | ***MITRE :*** *T1059, T1204* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

WildFire analyse les fichiers inconnus dans un environnement sandbox cloud pour détecter les malwares zero-day. Sans configuration optimale, seuls certains types de fichiers sont envoyés à WildFire et la taille maximale par défaut est trop basse. Le CIS Benchmark exige la maximisation des limites de taille et l'activation pour tous les types de fichiers dans les **deux directions** (upload ET download). Sur PAN-OS 10.0+ avec Advanced WildFire, les signatures sont livrées en temps réel (5 minutes vs 15-30 minutes).

Les fichiers de type PE (exécutables Windows), Adobe Flash/PDF, Microsoft Office, Java et APK Android représentent les vecteurs de malware les plus fréquents et doivent être prioritaires.

Impact potentiel

- Malwares zero-day non soumis à WildFire si types de fichiers non configurés
- Fichiers PE, PDF, Office malveillants passant sans analyse sandbox
- Délai de détection augmenté si les mises à jour WildFire ne sont pas en temps réel
- Exfiltration de fichiers sensibles en upload non inspectée

Navigation

```
Objects > Security Profiles > WildFire Analysis > Add
→ Name : WildFire-BestPractice

Règle principale :
→ Applications = any
→ File Types = any
→ Direction = both (upload ET download — critique pour détecter l'exfiltration)
→ Analysis = public-cloud (WildFire public) ou WF-500 (appliance privée)

Types de fichiers prioritaires (si granularité souhaitée) :
→ PE (Windows Executables) : forward, both directions
→ Adobe Flash, PDF : forward, both
→ Microsoft Office (doc, xls, ppt) : forward, both
→ Java (jar) : forward, both
→ Android APK : forward, both

Device > Setup > WildFire
→ WildFire Public Cloud : activé, server = wildfire.paloaltonetworks.com
→ Real-time WildFire (PAN-OS 10.0+, Advanced WildFire) : activé
→ Report Benign Files : Yes (pour enrichissement de la base)
→ Report Grayware Files : Yes

Device > Dynamic Updates > WildFire
→ Schedule : Real Time (nécessite licence WildFire)

Objects > Security Profiles > WildFire Analysis > [profil] > File Size Limits
→ PE : 10 MB
→ PDF : 1000 KB
→ MS Office : 2000 KB
→ APK : 30 MB

Alertes (Device > Log Settings > WildFire) :
→ Configurer email, SNMP ou syslog pour les verdicts malveillants

Exclusions :
→ Créer des règles d'exception au-DESSUS de la règle principale pour :
   - Serveurs Windows Update (éviter faux positifs sur PE Microsoft signés)
   - Serveurs de distribution logiciels internes légitimes
   → Action = no-forward pour ces sources/destinations

Navigation : Objects > Security Profiles > WildFire Analysis
```

CLI de vérification

```
show wildfire status
show wildfire statistics
show config running | xpath /config/devices/entry/vsys/entry/profiles/wildfire-analysis
show wildfire last-action
```

Remédiation

1. Créer le profil WildFire `WildFire-BestPractice` avec transmission de tous les types de fichiers dans les deux directions
2. Maximiser les limites de taille de fichiers dans `Device > Setup > WildFire`

3. Activer les mises à jour WildFire en temps réel (`Device > Dynamic Updates > WildFire > Real Time`)
4. Configurer les alertes pour les fichiers malveillants détectés via email/SNMP/syslog
5. Créer des règles d'exclusion **au-dessus** de la règle principale pour les serveurs de distribution légitimes
6. Attacher ce profil au Security Profile Group "best-practice" (contrôle 6.9)

Valeur par défaut : WildFire Analysis Profile vide. Limites de taille par défaut basses. Mises à jour non en temps réel. Direction = download uniquement.

Critère de conformité : Profil WildFire envoyant tous types de fichiers vers WildFire en direction both. Mises à jour signatures WildFire < 1h. Alertes configurées sur détection malware. Exclusions documentées et minimales.

Contrôle 6.5 — Profil URL Filtering best-practice : catégories BLOCK et HIGH-RISK

CIS Ref : *6.8, 6.9, 6.10, 6.12 (URL Filtering)* | ***MITRE :*** *T1071, T1566* | ***Niveau :*** 🟢 *L1*

Description du risque

Sans filtrage URL, les utilisateurs peuvent accéder à des sites de phishing, de malware-distribution, de C2 ou de contenu non autorisé. PAN-DB catégorise des milliards d'URLs. Le blocage des catégories malveillantes et à haut risque réduit significativement la surface d'attaque. L'option "Log Container Page Only" doit être désactivée pour une visibilité complète. La soumission de credentials d'entreprise sur des sites à haut risque doit être bloquée.

Impact potentiel

- Téléchargement de malwares depuis des sites de distribution
- Accès à des pages de phishing volant des credentials d'entreprise
- Communication avec des C2 via HTTP/HTTPS si domaines non bloqués
- Exfiltration via des proxies anonymiseurs et DNS chiffré

Navigation

```
Objects > Security Profiles > URL Filtering > Add
→ Name : URL-BestPractice

-- Catégories BLOCAGE OBLIGATOIRE (malveillantes) --
Action = block :
→ command-and-control
→ compromised-website
→ grayware
→ malware
→ phishing
→ ransomware
→ scanning-activity

-- Catégories BLOCAGE HAUT RISQUE --
Action = block :
→ dynamic-dns
→ encrypted-dns
→ hacking
→ insufficient-content
→ newly-registered-domains
→ not-resolved
→ parked
→ proxy-avoidance-and-anonymizers
→ unknown (ou alert si trop permissif en production)

-- Catégories ALERT (visibilité sans blocage) --
→ high-risk (si not blocking)
→ questionable

Onglet "Settings" :
→ Log Container Page Only : DÉSACTIVÉ (cocher pour loguer TOUTES les URLs individuelles)
→ Safe Search Enforcement : ACTIVÉ (Google, Bing, Yahoo, YouTube)
   Note : obligatoire pour les établissements d'enseignement recevant des fonds fédéraux
→ Hold Client Requests during Category Lookup : ACTIVÉ (sécurité maximale)
→ HTTP Header Logging : activé (User-Agent, Referer, X-Forwarded-For)

User Credential Submission :
→ Sur catégories malveillantes : Action = block
→ Sur catégories haut risque : Action = block
→ Activer "Log Credential Submissions" pour visibilité complète

Navigation : Objects > Security Profiles > URL Filtering
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/profiles/url-filtering
show url-filtering statistics
show url-cloud status
```

Remédiation

1. Activer PAN-DB dans `Device > Setup > Content-ID > URL Filtering`
2. Créer le profil `URL-BestPractice` avec toutes les catégories malveillantes en block
3. Ajouter les 8 catégories à haut risque en block

4. Désactiver “Log Container Page Only” pour une journalisation complète
5. Activer Safe Search Enforcement pour les environnements éducatifs ou corporate
6. Activer “Hold Client Requests during Category Lookup” pour une sécurité maximale (légère latence)
7. Bloquer la soumission de credentials sur les catégories malveillantes et à haut risque
8. Attacher le profil au Security Profile Group “best-practice”

Valeur par défaut : Aucun profil URL Filtering attaché. PAN-DB activé mais sans profil = pas de filtrage.

Critère de conformité : 7 catégories malveillantes bloquées. 8 catégories haut risque bloquées. Log Container Page Only = désactivé. Safe Search = activé. User Credential Submission = block sur catégories risquées. Profil attaché à toutes les règles allow vers Internet.

Contrôle 6.6 — Zone Protection Profile : SYN Cookies, flood et reconnaissance

> ***CIS Ref :*** *6.15, 6.16, 6.17, 6.18 (Zone Protection Profiles)* | ***MITRE :*** *T1499* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les attaques DDoS (SYN flood, UDP flood, ICMP flood) peuvent saturer les ressources du firewall et des serveurs exposés. Les Zone Protection Profiles permettent de limiter ces attaques avec des mécanismes comme les SYN Cookies (protection SYN flood sans état) et des seuils de taux pour chaque type de flood.

Impact potentiel

- Saturation des ressources du firewall lors d’une attaque DDoS
- Indisponibilité des services exposés (DoS effectif)
- Détournement du firewall lors d’une attaque de reconnaissance (port scan, OS fingerprinting)

Navigation

```
Network > Network Profiles > Zone Protection > Add
→ Name : ZP-Untrust-Strict

Onglet "Flood Protection" :
→ SYN : Action = SYN Cookies, Alarm Rate = 10000, Activate = 20000, Maximum = 40000
→ ICMP : Action = Random Early Drop, Activate = 1000, Maximum = 5000
→ UDP : Action = Random Early Drop, Activate = 10000, Maximum = 20000
→ ICMPv6 : Action = Random Early Drop

Onglet "Reconnaissance Protection" :
→ TCP Port Scan : action = block-ip (durée 3600s)
→ UDP Port Scan : action = block-ip
→ Host Sweep : action = block-ip

Onglet "Packet Based Attack Protection" :
→ IP Spoofing : block
→ TCP Split Handshake : block
→ Packet Too Large : block
→ Land Attack : block

Network > Zones > [zone untrust]
→ Zone Protection Profile : ZP-Untrust-Strict
```

CLI de vérification

```
show zone-protection zone untrust
show config running | xpath /config/devices/entry/network/profiles/zone-protection-profile
```

Remédiation

1. Créer un Zone Protection Profile pour la zone untrust avec SYN Cookies activés
2. Configurer les seuils de flood adaptés au trafic légitime observé
3. Activer la protection de reconnaissance (port scan, host sweep)
4. Appliquer le profil à la zone untrust
5. Créer un profil moins restrictif pour les zones internes (trust, DMZ) si nécessaire

Valeur par défaut : Aucun Zone Protection Profile configuré sur les zones par défaut.

Critère de conformité : Zone Protection Profile avec SYN Cookies activé attaché à toutes les zones untrust. Flood Protection configurée avec seuils définis. Reconnaissance Protection activée.

Contrôle 6.7 — Kill Chain Étape 5 : Profil File Blocking — prévention de l'installation

CIS Ref : *6.11, 6.12 (File Blocking)* | ***MITRE :*** *T1566.001 (Spearphishing Attachment), T1204.002 (User Execution — Malicious File), T1105 (Ingress Tool Transfer)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

L’étape 5 du Kill Chain (Installation) correspond au dépôt d’un malware sur le système cible. Les fichiers PE (exécutables Windows), les archives chiffrées, les fichiers HTA, LNK et les téléchargeurs constituent les vecteurs d’installation les plus courants. Le profil prédéfini **“strict”** de Palo Alto bloque un ensemble de types de fichiers dangereux dès la première mise en service.

Les archives chiffrées (encrypted-zip, encrypted-rar) sont particulièrement dangereuses car elles ne peuvent pas être inspectées par les moteurs antivirus et WildFire. Les fichiers PE dans des archives ZIP sont utilisés massivement dans les campagnes de phishing pour contourner les protections email.

Impact potentiel

- Installation de malwares via téléchargement d’exécutables (T1105 — Ingress Tool Transfer)
- Exécution accidentelle de fichiers LNK, HTA, SCR malveillants reçus par email (T1204.002)
- Contournement de l’inspection antivirus via archives chiffrées ou multi-encodées
- Distribution de ransomwares via fichiers PE ou scripts dans des archives

Navigation

```
-- Option 1 : Utiliser le profil prédéfini "strict" --
Objects > Security Profiles > File Blocking
→ Sélectionner le profil prédéfini "strict" (baseline recommandée)
→ Ce profil bloque : batch files, DLLs, Java classes, Windows PE, .hta, .lnk,
   .tar, BitTorrent, encrypted-zip, encrypted-rar, multilevel-encoded

-- Option 2 : Créer un profil personnalisé "FileBlock-BestPractice" --
Objects > Security Profiles > File Blocking > Add
→ Name : FileBlock-BestPractice

Règle 1 (BLOQUE — fichiers PE dangereux) :
→ Applications : any
→ File Types : pe, dll, cpl, ocx, sys, scr, drv, efi, fon, pif
→ Direction : both (upload ET download)
→ Action : block

Règle 2 (BLOQUE — PE dans archives ZIP) :
→ Applications : any
→ File Types : pe (embedded in zip)
→ Direction : download
→ Action : block

Règle 3 (BLOQUE — archives chiffrées) :
→ File Types : encrypted-zip, encrypted-rar
→ Direction : both
→ Action : block

Règle 4 (BLOQUE — exécuteurs à risque) :
→ File Types : hta, lnk, .tar, bittorrent, multlevel-encoded
→ Direction : both
→ Action : block

Règle 5 (ALERTE — autres types) :
→ File Types : any
→ Direction : both
→ Action : alert (visibilité sans blocage)

-- Exception au-DESSUS des règles de blocage --
Créer des règles d'exception spécifiques AVANT les règles de blocage :
→ Exception 1 : Source = Windows Update servers → Action = allow (PE Microsoft légitimes)
→ Exception 2 : Source = [serveurs distribution logiciels internes] → Action = allow
→ Ces exceptions doivent être positionnées EN TÊTE du profil (avant les règles de blocage)

Navigation : Objects > Security Profiles > File Blocking
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/profiles/file-blocking
show log threat subtype file-blocking
```

Remédiation

1. Utiliser le profil prédéfini “strict” comme baseline immédiate en production
2. Créer un profil personnalisé `FileBlock-BestPractice` pour un contrôle granulaire

3. Bloquer impérativement : PE, DLL, CPL, OCX, SYS, SCR, DRV, EFI, FON, PIF dans les deux directions
4. Bloquer les PE dans les archives ZIP — vecteur majeur de campagnes de phishing
5. Bloquer les archives chiffrées (encrypted-zip, encrypted-rar) — ne peuvent pas être inspectées
6. Bloquer HTA, LNK, TAR, BitTorrent, fichiers multi-encodés
7. Créer des règles d'exception **au-dessus** des règles de blocage pour Windows Update et les serveurs de distribution légitimes
8. Activer le logging (action = alert) sur tous les autres types de fichiers pour visibilité
9. Attacher ce profil au Security Profile Group "best-practice" (contrôle 6.9)

Valeur par défaut : Aucun profil File Blocking configuré ou attaché par défaut. Profil prédéfini "strict" disponible mais non attaché.

Critère de conformité : Profil File Blocking basé sur "strict" ou équivalent, bloquant PE/DLL/HTA/LNK/encrypted-zip/encrypted-rar dans les deux directions. Exceptions documentées et positionnées en tête du profil. Profil attaché à toutes les règles allow. Logging configuré sur tous les types de fichiers.

Contrôle 6.8 — Kill Chain Étape 6 : DNS Sinkholing — configuration pas-à-pas

> ***CIS Ref :*** *6.3, 6.4, 6.5 (Anti-Spyware — DNS Sinkhole)* | ***MITRE :*** *T1071.004 (DNS), T1568 (Dynamic Resolution), T1041 (Exfiltration Over C2 Channel)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le DNS Sinkholing est l'une des techniques de détection C2 les plus efficaces disponibles sur PAN-OS. Lorsqu'un hôte infecté tente de résoudre un domaine C2 malveillant, le firewall forge une réponse DNS pointant vers l'IP sinkhole (`sinkhole.paloaltonetworks.com` ou une IP interne dédiée). L'hôte infecté tente alors de contacter cette IP sinkhole — ce trafic est visible dans les logs Threat avec action = sinkhole, constituant un IoC certifié permettant l'identification immédiate de l'hôte compromis.

Sans DNS Sinkholing, les communications C2 via DNS passent souvent inaperçues. Les malwares modernes utilisent DGA (Domain Generation Algorithm) pour générer des milliers de domaines C2 — les signatures Anti-Spyware incluent ces patterns DGA.

Impact potentiel

- Communications C2 via DNS non détectées sans sinkholing (T1071.004)
- DNS tunneling permettant l'exfiltration de données en contournant le filtrage HTTP (T1041)
- Domaines DGA non bloqués permettant la persistance C2 même après blacklisting des domaines connus
- Hôtes infectés non identifiables sans le signal sinkhole dans les logs

Navigation

```
-- Configuration pas-à-pas du DNS Sinkholing --

Étape 1 : Modifier ou cloner le profil Anti-Spyware
Objects > Security Profiles > Anti-Spyware > [AntiSpyware-BestPractice]

Étape 2 : Vérifier la source de signatures DNS
Onglet "DNS Policies"
→ Signature Source : vérifier que "default-paloalto-dns" est présent et actif

Étape 3 : Configurer l'action sinkhole
→ Policy Action = "sinkhole"
→ Pour chaque catégorie (C2, Malware, Phishing, Grayware, etc.) :
   Action = sinkhole

Étape 4 : Activer la capture de paquets
→ Packet Capture : single-packet (pour la plupart des catégories)
→ Packet Capture : extended-capture (pour C2 Domains — forensique plus complète)

Étape 5 : DNS Sinkhole Settings dans le profil
Objects > Security Profiles > Anti-Spyware > [profil] > DNS Sinkhole Settings
→ Enable Sinkhole : coché
→ IPv4 Sinkhole IP : sinkhole.paloaltonetworks.com
   (ou IP interne dédiée, ex : 10.100.100.100, pour filtrer dans les règles de sécurité)
→ IPv6 Sinkhole IP : ::1

Étape 6 : Configurer la politique de sécurité pour la détection
Policies > Security > [règle applicable] > Actions
→ Log at Session Start : coché (pour détecter les tentatives C2 dès la connexion)
→ Profile Group : attacher AntiSpyware-BestPractice

Étape 7 : Vérifier les logs sinkhole
Monitor > Logs > Threat
→ Filtrer : (action eq sinkhole)
→ Chaque entrée = hôte interne infecté tentant de contacter un C2

Étape 8 (optionnel — sinkhole IP interne) :
Si utilisation d'une IP interne sinkhole :
→ Créer une règle de sécurité : Source = any, Destination = [sinkhole IP interne]
→ Action = Allow + Log at Session Start + Log Forwarding vers SIEM
→ Alerte SIEM P1 sur tout trafic vers cette IP = IoC immédiat

Licence requise : Advanced Threat Prevention ou Threat Prevention
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/profiles/spyware | match
sinkhole
show log threat | match sinkhole
show dns-proxy all
test security-policy-match application dns destination <IP-DNS-server>
```

Remédiation

1. S’assurer que le profil Anti-Spyware (contrôle 6.2) a le DNS Sinkholing activé

2. Vérifier que “default-paloalto-dns” est présent dans les sources de signatures DNS Policies
3. Configurer l’action sinkhole sur toutes les catégories de domaines malveillants
4. Activer la capture de paquets (single-packet minimum, extended pour les C2)
5. Configurer `Log at Session Start` dans les règles de sécurité pour détecter les tentatives dès l’initiation
6. Créer une alerte SIEM P1 sur l’action = sinkhole dans les logs Threat — réponse immédiate requise
7. Si sinkhole IP interne utilisée : créer une règle de détection dédiée permettant ce trafic avec logging complet
8. Former l’équipe SOC : chaque log sinkhole = hôte compromis à isoler

Valeur par défaut : DNS Sinkholing désactivé dans le profil Anti-Spyware par défaut. Aucune configuration DNS Policies.

Critère de conformité : DNS Sinkholing activé dans le profil Anti-Spyware. Source “default-paloalto-dns” configurée. Action sinkhole sur toutes les catégories de domaines malveillants. Log at Session Start activé sur les règles avec Anti-Spyware. Alerte SIEM P1 configurée sur logs action = sinkhole. Procédure SOC documentée pour la réponse aux alertes sinkhole.

Contrôle 6.9 — Security Profile Groups best-practice : “best-practice” et “default”

> ***CIS Ref :*** *6 (Security Profile Groups)* | ***MITRE :*** *T1059, T1566* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les Security Profile Groups permettent de regrouper tous les profils de sécurité (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, WildFire Analysis) en un seul objet attachable aux règles de sécurité. Sans groupes, chaque profil doit être attaché individuellement à chaque règle, augmentant le risque d’oubli et d’incohérence.

La création d’un groupe “best-practice” combinant tous les profils best-practice définis dans les contrôles 6.1 à 6.7 garantit qu’aucune règle allow n’est sans inspection complète. Le groupe “default” peut être utilisé pour l’attachement automatique aux nouvelles règles créées, évitant les règles sans profil.

Impact potentiel

- Règles allow sans profil de sécurité = angle mort de sécurité (aucune inspection des menaces)
- Incohérence des profils entre règles si attachés individuellement
- Nouvelles règles créées sans profil si pas de groupe “default” configuré

Navigation

```
-- Groupe "best-practice" --
Objects > Security Profile Groups > Add
→ Name : best-practice
→ Antivirus Profile : AV-BestPractice (contrôle 6.1)
→ Anti-Spyware Profile : AntiSpyware-BestPractice (contrôle 6.2)
→ Vulnerability Protection Profile : VulnProt-BestPractice (contrôle 6.3)
→ URL Filtering Profile : URL-BestPractice (contrôle 6.5)
→ File Blocking Profile : FileBlock-BestPractice (contrôle 6.7)
→ Data Filtering Profile : (si Data Loss Prevention configuré)
→ WildFire Analysis Profile : WildFire-BestPractice (contrôle 6.4)

-- Groupe "default" (pour nouvelles règles) --
Objects > Security Profile Groups > Add
→ Name : default
→ Mêmes profils que "best-practice" (ou profils légèrement moins restrictifs selon
l'environnement)
→ Ce groupe sera proposé automatiquement lors de la création de nouvelles règles

-- Attachement à toutes les politiques --
Policies > Security > [chaque règle allow]
→ Profile Setting : Group
→ Group Name : best-practice

VÉRIFICATION — Aucune règle allow sans profil :
show running security-policy
→ Vérifier qu'aucune ligne "profile-setting: none" n'apparaît pour des règles "allow"

CLI :
show security-profile-group
show config running | xpath /config/devices/entry/vsys/entry/profile-group
```

CLI de vérification

```
show security-profile-group
show config running | xpath /config/devices/entry/vsys/entry/profile-group
show running security-policy | match "profile-setting"
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"profile-setting"
```

Remédiation

1. Créer le groupe `best-practice` regroupant les 6 profils best-practice (AV + AS + VP + URL + FB + WildFire)
2. Créer le groupe `default` comme clone de `best-practice` pour les nouvelles règles
3. Attacher le groupe `best-practice` à **toutes** les règles allow existantes
4. Vérifier avec `show running security-policy` qu'aucune règle allow n'a `profile-setting = none`
5. Documenter dans la politique de sécurité que toute nouvelle règle allow **doit** avoir un Security Profile Group
6. Utiliser AIOps for NGFW ou BPA pour détecter automatiquement les règles sans profil

Valeur par défaut : Aucun Security Profile Group créé par défaut. Les règles créées manuellement n'ont aucun profil attaché.

Critère de conformité : Groupes `best-practice` et `default` créés. 100% des règles allow ont le groupe `best-practice` attaché. Aucune règle allow sans `profile-setting`. Vérification automatisée via BPA ou AIOps configurée.

Contrôle 6.10 — Profil Data Filtering (DLP) : prévention de l'exfiltration de données sensibles

CIS Ref : *6 (Security Profiles — Data Filtering)* | ***MITRE :*** *T1048 (Exfiltration Over Alternative Protocol), T1567 (Exfiltration Over Web Service), T1530 (Data from Cloud Storage)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le Data Filtering (DLP — Data Loss Prevention) dans PAN-OS permet de détecter et bloquer la transmission de données sensibles dans les flux réseau autorisés : numéros de cartes de crédit, numéros de sécurité sociale, IBAN, marqueurs de propriété intellectuelle, et en-têtes de documents classifiés. Sans profil Data Filtering, un attaquant ayant accès à un poste interne peut exfiltrer librement des données sensibles via HTTP/HTTPS, SMTP, FTP ou d'autres protocoles autorisés.

Les réglementations PCI-DSS (req. 4, 9, 12), RGPD (art. 25, 32), NIS2 et HIPAA imposent des contrôles sur la transmission de données sensibles. Le Data Filtering fournit une couche de contrôle technique complémentaire aux solutions DLP endpoint.

La direction **upload (sortante)** est la plus critique : c'est sur les flux sortants que l'exfiltration se produit. La direction download est utile pour détecter les données sensibles reçues de l'extérieur (ex : credentials en clair envoyés par un partenaire).

Impact potentiel

- Exfiltration de données de paiement (numéros CB, CVV) via des flux HTTP/SMTP apparemment légitimes (T1048)
- Upload de documents confidentiels vers des services cloud non autorisés (T1567 — Google Drive, Dropbox, OneDrive personnels)
- Fuite de données clients via un poste compromis ou un collaborateur malveillant
- Violation réglementaire détectable uniquement a posteriori sans contrôle technique préventif
- Exfiltration silencieuse de bases de données (numéros de compte, IBAN) via des protocoles de messagerie

Navigation

```
-- Étape 1 : Créer le profil Data Filtering --
Objects > Security Profiles > Data Filtering > Add
→ Name : DLP-BestPractice

-- Étape 2 : Ajouter des patterns prédéfinis de données sensibles --

Règle 1 — Données de paiement (PCI-DSS) :
→ Cliquer "Add" dans la section Data Patterns
→ Pattern Name : credit-card-numbers (pattern prédéfini PAN-OS)
→ Application : any
→ File Type : any (ou restreindre à : pdf, doc, docx, xls, xlsx, txt, html)
→ Direction : upload (exfiltration sortante — le plus critique)
→ Alert Threshold : 1 occurrence (pour les CB — tolérance zéro)
→ Block Threshold : 5 occurrences
→ Action : alert (1 occurrence), block-continue (5 occurrences)
→ Log Severity : high

Règle 2 — Numéros de sécurité sociale / SSN :
→ Pattern Name : social-security-numbers (pattern prédéfini)
→ Direction : upload
→ Alert Threshold : 1 | Block Threshold : 3
→ Action : alert / block

Règle 3 — IBAN et coordonnées bancaires :
→ Pattern Name : bank-account-numbers (pattern prédéfini)
→ Direction : upload
→ Alert Threshold : 1 | Block Threshold : 3
→ Action : alert / block-continue

Règle 4 — Marqueurs de documents internes (pattern personnalisé) :
Objects > Custom Objects > Data Patterns > Add
→ Name : Internal-Document-Markers
→ Pattern Type : Regular Expression
→ Pattern : CONFIDENTIEL|CLASSIFIÉ|ANC-INTERNAL|PROPRIETARY
→ (Adapter selon les marqueurs de classification utilisés par l'organisation)
→ Threshold : 1 occurrence → alert, 2 occurrences → block

Règle 5 — En-têtes de documents sensibles (fichiers Office/PDF) :
→ File Type : pdf, ms-word, ms-excel, ms-powerpoint
→ Direction : both
→ Action : alert (pour visibilité complète des flux documentaires)

-- Étape 3 : Options du profil Data Filtering --
Objects > Security Profiles > Data Filtering > [DLP-BestPractice] > Settings
→ Data Capture : cocher (capture du contenu correspondant pour forensique)
   ⚠ Attention : les données capturées peuvent contenir des PII — protéger l'accès au PCAP
→ Log Forwarding : profil SIEM

-- Étape 4 : Attacher le profil au Security Profile Group --
Objects > Security Profile Groups > [best-practice]
→ Data Filtering Profile : DLP-BestPractice

-- Étape 5 : Attacher aux règles critiques (upload vers Internet) --
Policies > Security > [règles trust → untrust avec action allow]
→ Profile Setting : Group > best-practice (inclut maintenant DLP-BestPractice)
```

```
Navigation complète :
Objects > Security Profiles > Data Filtering > Add
Objects > Custom Objects > Data Patterns > Add (pour patterns personnalisés)
```

CLI de vérification

```
# Vérifier la configuration du profil Data Filtering
show config running | xpath /config/devices/entry/vsys/entry/profiles/data-filtering

# Vérifier les patterns de données configurés
show config running | xpath /config/devices/entry/vsys/entry/profiles/data-objects

# Consulter les logs Data Filtering
show log data direction equal backward
show log data | match "credit-card"

# Vérifier l'attachement au Security Profile Group
show config running | xpath /config/devices/entry/vsys/entry/profile-group | match "data-
filtering"
```

Remédiation

1. Créer le profil `DLP-BestPractice` dans `Objects > Security Profiles > Data Filtering`
2. Ajouter les patterns prédéfinis PAN-OS : `credit-card-numbers`, `social-security-numbers`, `bank-account-numbers`
3. Créer des patterns personnalisés (`Objects > Custom Objects > Data Patterns`) pour les marqueurs de classification de l'organisation
4. Configurer les seuils d'alerte et de blocage : commencer en mode alerte uniquement pendant 30 jours pour identifier les faux positifs avant d'activer le blocage
5. Attacher le profil au Security Profile Group `best-practice` (contrôle 6.9) et au groupe `default`
6. Prioriser les règles de politique couvrant les flux **trust → untrust (Internet)** et **trust → DMZ upload**
7. Configurer des alertes SIEM dédiées sur les logs Data Filtering de sévérité High (chaque hit = exfiltration potentielle)
8. Documenter la procédure de traitement des alertes DLP dans le runbook SOC (faux positifs vs incidents réels)
9. Si des données PCI-DSS (numéros CB) apparaissent dans les logs Data Filtering : traiter comme incident PCI-DSS immédiat (notification QSA potentiellement requise)

Valeur par défaut : Aucun profil Data Filtering créé ni attaché par défaut. La fonctionnalité est disponible dans toutes les licences PAN-OS standard.

Critère de conformité : Profil Data Filtering configuré avec au minimum les patterns CB et SSN/IBAN. Profil attaché au Security Profile Group `best-practice`. Alertes SIEM configurées sur les hits DLP. Mode alert-only pendant 30 jours de baseline, puis blocage sur les seuils définis. Logs Data Filtering transmis au SIEM avec procédure SOC documentée.

Domaine 7 — VPN et accès distant (GlobalProtect)

Objectif : *Sécuriser les accès VPN distants avec GlobalProtect en utilisant des protocoles cryptographiques forts (IKEv2, AES-256, PFS), une authentification MFA, et la validation de la posture des endpoints. Sur PAN-OS 11.1+, déployer la protection post-quantique via les PPK RFC 8784 pour protéger les sessions VPN contre les menaces futures des ordinateurs quantiques. Le VPN est un vecteur d'attaque majeur ciblé par les APT.*

Contrôle 7.1 — IKEv2 avec chiffrements forts (AES-256, PFS)

CIS Ref : *1.6.3, 1.7.1 (VPN Settings)* | ***MITRE :*** *T1133* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

IKEv1 avec mode agressif est vulnérable à l'interception du hash d'authentification (offline crack). Les suites de chiffrement faibles (DES, 3DES, MD5, DH groupe 1/2) peuvent être cassées par des ressources de calcul modernes. IKEv2 avec Perfect Forward Secrecy (PFS) garantit que la compromission d'une clé de session ne compromet pas les sessions passées.

Impact potentiel

- Déchiffrement hors-ligne des sessions VPN capturées si chiffrement faible (T1600)
- Attaque Man-in-the-Middle sur les négociations IKEv1 mode agressif
- Compromission rétroactive de toutes les sessions passées sans PFS

Navigation

```
Network > IKE Crypto > Add
→ Name : IKEv2-Strong-Crypto
→ DH Group : group14 (2048-bit) minimum, group20 (384-bit ECDH) recommandé
→ Encryption : aes-256-cbc ou aes-256-gcm
→ Authentication : sha256 ou sha384
→ Key Lifetime : 8 heures

Network > IPSec Crypto > Add
→ Name : IPSec-Strong-Crypto
→ IPSec Protocol : ESP
→ Encryption : aes-256-gcm (authentifié) ou aes-256-cbc + sha256
→ DH Group (PFS) : group14 minimum (activer PFS obligatoirement)
→ Key Lifetime : 1 heure

Network > IKE Gateways > [gateway] > Advanced Options
→ IKE Version : IKEv2 only (désactiver IKEv1)
→ IKE Crypto Profile : IKEv2-Strong-Crypto
```

CLI de vérification

```
show vpn ike-sa
show vpn ipsec-sa
show config running | xpath /config/devices/entry/network/ike-crypto-profiles
show config running | xpath /config/devices/entry/network/ipsec-crypto-profiles
```

Remédiation

1. Créer les profils IKE Crypto et IPSec Crypto avec les paramètres forts
2. Désactiver IKEv1 sur toutes les gateways IKE
3. Activer PFS (DH Group) dans le profil IPSec Crypto
4. Migrer les tunnels existants vers les nouveaux profils
5. Vérifier la compatibilité des clients VPN avant migration

Valeur par défaut : Profils par défaut avec DES/3DES et SHA1. IKEv1 activé.

Critère de conformité : IKEv2 uniquement. AES-256 minimum. SHA-256 minimum. PFS activé avec DH groupe ≥ 14. IKEv1 désactivé.

Contrôle 7.2 — GlobalProtect avec MFA et validation de posture HIP

> ***CIS Ref :*** *1.7 (VPN Settings), Auth Profiles* | ***MITRE :*** *T1133, T1078* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

GlobalProtect sans MFA est vulnérable au credential stuffing. Sans validation de posture (HIP — Host Information Profile), des endpoints non conformes (sans antivirus, avec OS non patché, chiffrement désactivé) peuvent se connecter au VPN et introduire des menaces dans le réseau interne.

Impact potentiel

- Connexion VPN depuis des credentials volés sans second facteur
- Endpoints compromis ou non conformes accédant au réseau interne via VPN
- Propagation de malwares depuis des machines personnelles non gérées

Navigation

```
Network > GlobalProtect > Portals > [portail] > Agent > Authentication
→ Authentication Profile : profil MFA (RADIUS + OTP ou SAML)
→ Certificate Profile : pour validation certificat client

Network > GlobalProtect > Gateways > [gateway] > Authentication
→ Même profil MFA

Objects > GlobalProtect > HIP Profiles > Add
→ Name : HIP-Corporate-Compliant
→ Conditions :
   - Antivirus up-to-date (last update < 24h)
   - Disk Encryption enabled
   - OS Patched (last patch < 30 days)
   - Host Firewall enabled

Policies > Security
→ Ajouter condition HIP Profile aux règles d'accès VPN
```

CLI de vérification

```
show global-protect-gateway current-user
show global-protect-gateway hip-report
show config running | xpath /config/devices/entry/vsys/entry/hip-profiles
```

Remédiation

1. Configurer MFA dans le profil d'authentification GlobalProtect
2. Créer des profils HIP définissant les critères de conformité des endpoints
3. Créer des règles de sécurité conditionnées par le profil HIP (accès restreint si non conforme)
4. Implémenter une page de remédiation pour les endpoints non conformes

Valeur par défaut : Authentification par mot de passe uniquement. Aucun profil HIP configuré.

Critère de conformité : MFA obligatoire pour GlobalProtect. Profil HIP configuré avec au moins antivirus et chiffrement disque. Règles d'accès VPN conditionnées par HIP.

Contrôle 7.3 — Certificat VPN valide signé par une CA de confiance

> ***CIS Ref :*** *1.6.3 (Certificate for VPN)* | ***MITRE :*** *T1040* | ***Niveau :*** 🟢 *L1*

Description du risque

Un certificat auto-signé pour le portail GlobalProtect crée une alerte de sécurité côté client et expose les utilisateurs à des attaques MITM. Les utilisateurs habitués à ignorer les alertes de certificat sont particulièrement vulnérables aux portails phishing GlobalProtect.

Impact potentiel

- Attaque MITM sur le portail VPN : interception des credentials avant chiffrement
- Portail VPN phishing difficile à distinguer si les utilisateurs ignorent les alertes certificat

Navigation

```
Device > Certificate Management > Certificates > Import
→ Importer le certificat TLS signé par la CA interne de l'organisation
→ Ou utiliser un certificat Let's Encrypt / CA publique pour les portails accessibles depuis Internet

Network > GlobalProtect > Portals > [portail] > Authentication
→ SSL/TLS Service Profile : sélectionner un profil utilisant le certificat valide

Network > GlobalProtect > Gateways > [gateway] > Authentication
→ SSL/TLS Service Profile : idem
```

CLI de vérification

```
show config running | xpath /config/devices/entry/certificate
show config running | xpath /config/devices/entry/ssl-tls-service-profile
```

Remédiation

1. Obtenir un certificat TLS valide (CA interne pour clients internes, CA publique pour clients Internet)
2. Importer le certificat et la clé privée dans `Device > Certificate Management > Certificates`
3. Créer un profil SSL/TLS référençant ce certificat
4. Appliquer ce profil au portail et à la gateway GlobalProtect
5. Configurer une alerte de renouvellement 60 jours avant expiration

Valeur par défaut : Certificat auto-signé généré à l'installation.

Critère de conformité : Certificat signé par une CA de confiance (non auto-signé). Validité restante > 30 jours. FQDN du certificat correspondant à l'adresse du portail.

Contrôle 7.4 — VPN Post-Quantique : PPK RFC 8784 et Hybrid Key Exchange (PAN-OS 11.1+)

CIS Ref : *1.6.3, 1.7.1 (VPN Crypto)* | ***MITRE :*** *T1133, T1600 (Weaken Encryption)* | ***Niveau :*** 🔵 *L2*

Description du risque

Les ordinateurs quantiques à grande échelle, lorsqu'ils deviendront opérationnels, seront capables de casser les algorithmes à clé publique actuels (RSA, DH, ECDH) via l'algorithme de Shor. La menace "Harvest Now, Decrypt Later" (HNDL) est déjà réelle : des acteurs APT capturent aujourd'hui des sessions VPN chiffrées pour les déchiffrer ultérieurement avec des ordinateurs quantiques. Les organisations gérant des données à longue durée de vie (gouvernements, défense, santé, finance) doivent anticiper cette menace.

PAN-OS 11.1+ implémente deux approches de protection post-quantique standardisées par l'IETF :

RFC 8784 — Post-Quantum IKEv2 avec Pre-Shared Keys (PPK) : - Ajoute une couche de sécurité symétrique à IKEv2 en utilisant une clé pré-partagée post-quantique - La PPK est transmise hors-bande (out-of-band) ; seul le Key ID est échangé pendant la négociation IKEv2 - Résistant aux attaques quantiques car basé sur AES (résistant à l'algorithme de Grover) - Mode Mandatory : la négociation échoue si la PPK n'est pas supportée par les deux pairs

RFC 9242 et RFC 9370 — Hybrid Key Exchange : - Combine des mécanismes KEM (Key Encapsulation Mechanism) classiques (ECDH) avec des KEM post-quantiques (ex : CRYSTALS-Kyber) - Jusqu'à 7 mécanismes KEM additionnels configurables - Sécurité conditionnelle : si l'un des mécanismes est sûr, l'échange de clé est sûr

Impact potentiel

- Déchiffrement rétroactif des sessions VPN capturées aujourd'hui par des acteurs étatiques (T1600)
- Compromission des tunnels VPN protégeant des données classifiées ou sensibles
- Non-conformité avec les futures réglementations post-quantiques (ANSSI, BSI, NIST SP 800-208)

Navigation

```
-- Configuration RFC 8784 (PPK Post-Quantum) --
Network > IKE Gateways > [gateway] > Advanced Options > Post-Quantum PPK
→ Enable Post-Quantum Pre-Shared Key : coché
→ PPK ID : identifiant unique pour cette paire de PPK (transmis en clair, non secret)
→ PPK Value : clé pré-partagée post-quantique (≥ 256 bits d'entropie)
   ⚠ Distribuer la PPK uniquement hors-bande (canal séparé, sécurisé, jamais via IKE)
→ Negotiation Mode : Mandatory (recommandé — la négociation échoue sans PPK)
   Note : "Optional" accepte aussi des pairs sans PPK (moins sécurisé)

CLI :
set network ike gateway <name> protocol ikev2 ppk enable yes
set network ike gateway <name> protocol ikev2 ppk id <ppk-id>
set network ike gateway <name> protocol ikev2 ppk key <ppk-key>
set network ike gateway <name> protocol ikev2 ppk mode mandatory

-- Algorithmes recommandés résistants aux attaques quantiques --
Network > IKE Crypto > [profil IKEv2-Strong-Crypto]
→ Encryption : AES-256-GCM (résistant à l'algorithme de Grover)
→ Authentication : SHA-384 ou SHA-512 (longueur suffisante contre Grover)
→ DH Group : group20 (384-bit ECDH) ou group21 (521-bit ECDH) minimum

Network > IPSec Crypto > [profil IPSec-Strong-Crypto]
→ Encryption : AES-256-GCM (clé 256 bits — seuil recommandé pour résistance quantique)
→ DH Group (PFS) : group20 minimum

-- Vérification de la configuration --
```

CLI de vérification

```
show vpn ike-sa gateway <name>
show config running | xpath /config/devices/entry/network/ike-gateways/entry/protocol/ikev2/ppk
show config running | xpath /config/devices/entry/network/ike-crypto-profiles
show vpn flow name <tunnel-name>
debug ike global on info
```

Remédiation

1. Vérifier que PAN-OS est en version 11.1 ou supérieure pour le support PPK RFC 8784
2. Générer des PPK de haute entropie (≥ 256 bits) : utiliser un générateur cryptographique certifié (FIPS 140-2/3) ; ne jamais utiliser des PPK dérivées de mots de passe
3. Distribuer les PPK exclusivement hors-bande : échange physique, canal chiffré séparé, ou gestionnaire de secrets (HashiCorp Vault avec HSM)
4. Configurer chaque IKE Gateway avec son PPK et un PPK ID unique :

   ```
   Network > IKE Gateways > [gateway] > Advanced Options > Post-Quantum PPK
   → Enable, saisir le PPK ID et la PPK value
   → Negotiation Mode = Mandatory pour les pairs contrôlés
   ```

5. Commencer par le mode “Optional” pour tester la compatibilité, puis passer en “Mandatory”
6. Mettre à jour les profils IKE Crypto pour utiliser AES-256-GCM et DH groupe ≥ 20
7. Planifier la rotation des PPK (recommandation : renouvellement annuel ou après tout incident de sécurité)
8. Documenter l’architecture PPK : quels tunnels, quels PPK ID, quelle date d’expiration

Valeur par défaut : PPK désactivé. IKEv2 classique sans protection post-quantique.

Critère de conformité : Pour PAN-OS 11.1+ dans les environnements sensibles (gouvernement, défense, santé, finance) : PPK RFC 8784 activé en mode Mandatory sur tous les tunnels site-à-site critiques. AES-256 utilisé sur tous les tunnels. PPK distribuées hors-bande avec documentation de la procédure de rotation.

Domaine 8 — Décryptage SSL/TLS

> ***Objectif :*** *Inspecter le trafic chiffré (HTTPS, SMTPS, etc.) via SSL Forward Proxy (trafic sortant) et SSL Inbound Inspection (serveurs exposés entrants). Sans décryptage, 80%+ du trafic malveillant moderne utilisant HTTPS est invisible aux profils de sécurité.*

Contrôle 8.1 — SSL Forward Proxy pour le trafic Internet sortant

> ***CIS Ref :*** *8.1 (SSL Forward Proxy)* | ***MITRE :*** *T1048* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

La quasi-totalité du trafic Internet utilise HTTPS. Sans SSL Forward Proxy, les profils Antivirus, URL Filtering, WildFire et Anti-Spyware ne peuvent pas inspecter ce trafic chiffré. Les malwares modernes communiquent quasi-exclusivement via HTTPS pour contourner l'inspection réseau.

Impact potentiel

- Téléchargements de malwares en HTTPS non inspectés
- Communications C2 en HTTPS non détectées
- Exfiltration de données via HTTPS non visible dans les logs applicatifs

Navigation

```
Device > Certificate Management > Certificates > Add
→ Créer un certificat CA intermédiaire pour le décryptage SSL Forward Proxy
→ Nom : PA-SSL-FP-CA (Self-Signed CA ou signé par CA racine interne)
→ Marquer "Certificate Authority" dans les attributs

Policies > Decryption > Add
→ Name : Decrypt-Outbound-SSL
→ Source Zone : trust
→ Destination Zone : untrust
→ Type : SSL Forward Proxy
→ Profile : default (ou profil personnalisé)
→ SSL/TLS Protocol Settings : TLS 1.2 minimum

Device > Certificate Management > SSL/TLS Service Profile
→ Distribuer le certificat CA de décryptage aux endpoints via GPO/MDM
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/rulebase/decryption
show decryption-policy
show system setting ssl-decrypt certificate
```

Remédiation

1. Générer ou importer une CA de décryptage dédiée
2. Distribuer ce certificat CA aux clients via GPO/MDM (Windows : Autorités de certification racine de confiance)
3. Créer la politique de décryptage SSL Forward Proxy
4. Définir des exclusions pour les sites légitimes qui ne supportent pas le décryptage (banking, SSO, certificats épinglés)
5. Vérifier les logs de décryptage dans `Monitor > Logs > Decryption`

Valeur par défaut : Aucune politique de décryptage configurée.

Critère de conformité : Politique SSL Forward Proxy active pour le trafic Internet sortant. CA de décryptage distribuée sur les endpoints. Exclusions documentées et minimales.

Contrôle 8.2 — SSL Inbound Inspection pour les serveurs exposés

> ***CIS Ref :*** *8.2 (SSL Inbound Inspection)* | ***MITRE :*** *T1190* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Le trafic entrant vers les serveurs exposés (serveurs web, API, messagerie) est chiffré en TLS. Sans SSL Inbound Inspection, le firewall ne peut pas inspecter les exploits et malwares dans ces flux entrants. Cette inspection nécessite l'importation de la clé privée des serveurs exposés dans le firewall.

Impact potentiel

- Exploits applicatifs (SQLi, RCE, XXE) transmis en HTTPS non inspectés
- Uploads de webshells en HTTPS non détectés par le profil Vulnerability Protection
- Attaques vers serveurs DMZ passant à travers le firewall sans inspection

Navigation

```
Device > Certificate Management > Certificates > Import
→ Importer le certificat et la clé privée du serveur exposé

Policies > Decryption > Add
→ Name : Decrypt-Inbound-Server
→ Source Zone : untrust
→ Destination Zone : dmz
→ Destination Address : IP du serveur exposé
→ Service : https (TCP/443)
→ Type : SSL Inbound Inspection
→ Certificate : sélectionner le certificat importé
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/rulebase/decryption | match
"ssl-inbound"
show decryption-policy
```

Remédiation

1. Importer les certificats et clés privées des serveurs DMZ exposés
2. Créer une politique de décryptage Inbound par serveur
3. Vérifier que les profils de sécurité (Vulnerability Protection, Antivirus) inspectent bien le trafic déchiffré
4. Planifier le renouvellement des clés importées avant expiration

Valeur par défaut : Aucune politique SSL Inbound Inspection configurée.

Critère de conformité : SSL Inbound Inspection configurée pour tous les serveurs exposés sur HTTPS en zone DMZ. Politiques actives et loggées.

Contrôle 8.3 — Exclusions de décryptage documentées et minimales

> ***CIS Ref :*** *8.3 (Trusted Certificate for Decryption)* | ***MITRE :*** *T1048* | ***Niveau :*** 🟢 *L1*

Description du risque

Certains sites et applications ne supportent pas le décryptage SSL (certificat épinglé, HPKP, applications bancaires). Ces exclusions doivent être documentées, minimales et régulièrement révisées. Des exclusions excessives réduisent l'efficacité du décryptage et peuvent être exploitées par des attaquants pour contourner l'inspection.

Impact potentiel

- Abus des exclusions pour faire transiter du trafic malveillant vers des domaines exclus
- Exclusions héritées non révisées couvrant des domaines inutilement larges
- Contournement de l'inspection par des malwares se connectant à des domaines exclus

Navigation

```
Policies > Decryption > Add
→ Name : NoDecrypt-Exceptions
→ Type : SSL Exclusion (No Decrypt)
→ Destination URL Category : financial-services, health-and-medicine (si nécessaire)
→ Ou : Destination Address : IP spécifiques des sites à exclure
→ Action : No Decrypt
→ Positionner AVANT la règle de décryptage générale
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/rulebase/decryption | match
"no-decrypt"
show decryption-exclusion cache
```

Remédiation

1. Inventorier les sites nécessitant une exclusion (certificats épinglés, applications métier)
2. Créer des règles d'exclusion spécifiques par FQDN ou catégorie URL (non par plage IP large)
3. Documenter chaque exclusion avec justification et responsable
4. Réviser la liste des exclusions trimestriellement et supprimer les entrées obsolètes

Valeur par défaut : Aucune exclusion configurée (mais certaines catégories sont exclues dans les profils de décryptage par défaut).

Critère de conformité : Toutes les exclusions documentées. Révision trimestrielle effectuée. Aucune exclusion sur `any` ou plages d'adresses larges non justifiées.

Contrôle 8.4 — Gestion des certificats et PKI : CA dédiée, OCSP, SCEP et renouvellement automatisé

CIS Ref : *8.1 (SSL/TLS Profiles), Certificate Management* | ***MITRE :*** *T1553 (Subvert Trust Controls), T1557 (Adversary-in-the-Middle via cert compromise)* | ***Niveau :*** 🟢 *L1*

Description du risque

La gestion du cycle de vie des certificats sur PAN-OS couvre plusieurs surfaces d'attaque critiques : certificat auto-signé sur l'interface de gestion (vecteur MITM), CA de décryptage SSL mal configurée (compromission de la confiance des utilisateurs), certificats expirés créant des interruptions de service ou des avertissements de sécurité ignorés, et absence de mécanisme de révocation empêchant la réaction rapide en cas de compromission de clé.

La technique MITRE **T1553 (Subvert Trust Controls)** couvre les attaques visant à compromettre les autorités de certification pour injecter des certificats malveillants. Un attaquant ayant accès à la CA de décryptage SSL du firewall peut générer des certificats frauduleux pour toutes les destinations HTTPS inspectées. La technique **T1557 (Adversary-in-the-Middle)** via compromission de certificat permet l'interception silencieuse du trafic chiffré.

Impact potentiel

- Attaque MITM sur l'interface de gestion via certificat auto-signé non validé par les administrateurs (T1557)
- Compromission de la CA de décryptage SSL Forward Proxy permettant l'usurpation de n'importe quel site HTTPS
- Interruption de service lors de l'expiration de certificats non monitorés (portail VPN, interface de gestion)
- Impossibilité de révoquer rapidement un certificat compromis sans mécanisme OCSP/CRL configuré
- Non-conformité PCI-DSS (req. 4.2.1 : inventaire des certificats et gestion de leur cycle de vie)

Navigation

```
-- 1. Génération d'une CA dédiée pour SSL Forward Proxy --
Device > Certificate Management > Certificates > Generate
→ Certificate Name : PA-SSL-Inspection-CA
→ Common Name : PA SSL Inspection CA - [Nom Organisation]
→ Certificate Authority : cocher (rend ce certificat utilisable comme CA)
→ Key Type : RSA 2048 bits (minimum) ou ECDSA P-256 (recommandé pour la performance)
→ Digest : SHA-256 minimum
→ Validity (jours) : 1825 (5 ans maximum recommandé)
→ Signed by : CA racine interne de l'organisation (ou auto-signé si CA indépendante)
IMPORTANT : Cette CA est DISTINCTE du certificat de gestion du firewall

Exporter et distribuer aux endpoints :
→ Device > Certificate Management > Certificates > [PA-SSL-Inspection-CA] > Export
→ Distribuer via GPO (Windows) ou MDM (macOS, iOS, Android) vers les Trusted Root CAs
→ JAMAIS utiliser le certificat auto-signé du firewall comme CA SSL Inspection

-- 2. Certificat de gestion HTTPS signé par CA interne --
Device > Certificate Management > Certificates > Import
→ Importer un certificat TLS signé par la CA interne de l'organisation
→ CN ou SAN : FQDN de l'interface de gestion (ex : fw1-mgmt.example.com)
→ Key Type : RSA 2048+ ou ECDSA P-256
→ Valeur par défaut : auto-signé — à remplacer impérativement

Device > Certificate Management > SSL/TLS Service Profile > Add
→ Name : Mgmt-HTTPS-Profile
→ Certificate : [certificat CA-signé importé]
→ Min Protocol Version : TLSv1.2
→ Max Protocol Version : TLSv1.3

Device > Setup > Management > General Settings
→ SSL/TLS Service Profile : Mgmt-HTTPS-Profile

-- 3. Vérification OCSP et CRL (révocation de certificats) --
Device > Certificate Management > Certificates > [certificat] > OCSP Responder
→ OCSP Responder URL : URL du répondeur OCSP de la CA (ex : http://ocsp.example.com)
→ Enable : coché

Alternative CRL :
Device > Certificate Management > Certificate Profile > Add
→ Ajouter la CRL Distribution Point de la CA
→ CRL Update Interval : toutes les 24h maximum

-- 4. SCEP pour renouvellement automatisé des certificats --
Device > Certificate Management > SCEP > Add
→ Name : SCEP-Internal-CA
→ SCEP URL : URL du serveur SCEP de la CA interne (ex : https://ca.example.com/certsrv/
mscep/mscep.dll)
→ CA Identity : identifiant de la CA
→ Challenge Password : mot de passe de challenge SCEP (protégé dans le gestionnaire de
secrets)
→ Subject CN : $HOSTNAME (variable automatique pour le nom du firewall)
→ Certificate Expiry Days : 365 (1 an)
→ Renew Before (jours) : 30 (renouveler 30 jours avant expiration)

-- 5. Alertes d'expiration de certificats --
Device > Certificate Management > Certificates > [certificat] > Certificate Expiry Alert
```

```
→ Enable : coché
→ Alert Before Expiry (jours) : 60 (alerte 60 jours avant expiration)
→ Notification : Syslog vers SIEM + email admin

-- 6. Profil SSL/TLS pour les Portails VPN GlobalProtect --
Device > Certificate Management > SSL/TLS Service Profile > Add
→ Name : GP-Portal-TLS-Profile
→ Certificate : [certificat GP signé par CA publique ou CA interne]
→ Min Protocol Version : TLSv1.2
→ Forward Trust Certificate : PA-SSL-Inspection-CA
→ Forward Untrust Certificate : [certificat "Untrusted" avec page d'avertissement]

-- 7. Monitoring des certificats via CLI --
# Liste tous les certificats avec dates d'expiration
show certificate domain all | match "Expired\|Not Valid\|Valid"

# Vérifier un certificat spécifique
show certificate domain <nom-certificat>
```

CLI de vérification

```
# Lister tous les certificats et leur validité
show certificate domain all

# Vérifier les certificats proches de l'expiration (moins de 60 jours)
show certificate domain all | match "Not Valid"

# Vérifier l'état SSL/TLS du service de gestion
show config running | xpath /config/devices/entry/deviceconfig/system/ssl-tls-service-
profile

# Vérifier la configuration SCEP
show config running | xpath /config/devices/entry/deviceconfig/system/scep

# Vérifier les profils SSL/TLS existants
show sslmgr-store

# Vérifier l'état des profils de certificat
show config running | xpath /config/devices/entry/deviceconfig/system/certificate-profile
```

Remédiation

1. **Remplacer le certificat auto-signé de gestion :** Importer un certificat TLS signé par la CA interne de l'organisation pour l'interface de gestion HTTPS. Lier ce certificat dans un profil SSL/TLS assigné à `Device > Setup > Management > General Settings`.
2. **CA dédiée pour SSL Forward Proxy :** Générer une CA spécifique à l'inspection SSL (`PA-SSL-Inspection-CA`) avec une clé ECDSA P-256 ou RSA 2048+. Ne jamais utiliser le certificat de gestion du firewall comme CA SSL Inspection.
3. **Distribuer la CA SSL Inspection :** Déployer le certificat CA d'inspection via GPO (Windows) et MDM (macOS/mobile) dans les Trusted Root CAs de tous les endpoints managés. Sans cette étape, les utilisateurs reçoivent des avertissements de sécurité pour tout site HTTPS.

4. **Configurer OCSP ou CRL :** Activer la vérification de révocation sur tous les certificats de CA dans les profils de certificat. Utiliser OCSP si le répondeur est disponible (temps réel), sinon CRL avec intervalle de mise à jour ≤ 24h.
5. **Configurer SCEP pour le renouvellement automatique :** Si l'infrastructure CA de l'organisation supporte SCEP, configurer le renouvellement automatique 30 jours avant expiration. Cette automatisation élimine le risque d'expiration involontaire.
6. **Alertes d'expiration :** Activer les alertes d'expiration sur tous les certificats avec un délai d'alerte de 60 jours minimum. Envoyer ces alertes vers le SIEM pour traçabilité.
7. **Éviter les certificats wildcard :** Ne jamais utiliser de certificats wildcard (`*.example.com`) sur le firewall — le scope est trop large et la compromission d'une seule clé affecte tous les sous-domaines.
8. **Inventaire des certificats :** Maintenir un inventaire documenté de tous les certificats actifs (nom, usage, CA signataire, date d'expiration, responsable) mis à jour lors de chaque renouvellement.

Valeur par défaut : Certificat auto-signé généré à l'installation pour la gestion HTTPS. Pas de SCEP configuré. Pas d'alertes d'expiration activées. Pas de vérification OCSP/CRL.

Critère de conformité : Certificat de gestion HTTPS signé par CA interne (non auto-signé). CA SSL Forward Proxy dédiée et distincte du certificat de gestion. OCSP ou CRL configuré avec intervalle ≤ 24h. Alertes d'expiration activées avec préavis ≥ 60 jours. Aucun certificat expiré en production. SCEP configuré si infrastructure SCEP disponible. Inventaire des certificats documenté et à jour.

Domaine 9 — Segmentation, NAT et Haute Disponibilité

Objectif : *Implémenter une segmentation réseau stricte avec des zones distinctes (trust, untrust, DMZ, management) et contrôler le NAT pour éviter les fuites de routage et le hairpinning non contrôlé. La micro-segmentation limite le mouvement latéral en cas de compromission. Le durcissement de la Haute Disponibilité (HA) garantit la confidentialité et l'intégrité des communications entre les membres du cluster HA, et prévient les interruptions de service liées à une configuration HA non sécurisée.*

Contrôle 9.1 — Architecture de zones : trust, untrust, DMZ séparées

CIS Ref : *7.1 (Zone-based security policies)* | ***MITRE :*** *T1055* | ***Niveau :*** 🟢 *L1*

Description du risque

L'absence de segmentation par zones place tous les systèmes dans un réseau plat où un hôte compromis peut communiquer librement avec tous les autres. La séparation en zones (untrust = Internet, trust = LAN, DMZ = serveurs exposés, management = gestion) limite le rayon d'explosion d'une compromission.

Impact potentiel

- Mouvement latéral libre depuis un hôte compromis vers les systèmes critiques
- Serveurs exposés (DMZ) pouvant atteindre directement les serveurs internes en cas de compromission
- Trafic de gestion exposé aux mêmes risques que le trafic de production

Navigation

```
Network > Zones > Add
→ Zone Trust : interfaces LAN, Type = Layer3
→ Zone Untrust : interface WAN, Type = Layer3
→ Zone DMZ : interfaces serveurs exposés, Type = Layer3
→ Zone Management : interface mgmt, Type = Management (séparée physiquement si possible)

Policies > Security
→ Règle DMZ-to-Trust : Action = Deny (les serveurs DMZ ne peuvent pas initier vers le LAN)
→ Règle Trust-to-DMZ : Allow sur ports spécifiques uniquement
→ Règle Untrust-to-DMZ : Allow uniquement sur les ports publiés (80, 443, etc.)
```

CLI de vérification

```
show zone all
show interface all
show config running | xpath /config/devices/entry/network/vlan
```

Remédiation

1. Définir au minimum 4 zones : untrust, trust, DMZ, management
2. Vérifier que chaque zone est sur un VLAN/segment réseau distinct
3. Créer des règles inter-zones basées sur le principe du moindre privilège
4. Interdire toute communication DMZ-vers-Trust non explicitement autorisée
5. Isoler physiquement ou logiquement le réseau de management

Valeur par défaut : Zones untrust et trust créées par défaut. DMZ et management à créer.

Critère de conformité : Minimum 3 zones de sécurité distinctes (untrust, trust, DMZ). Règle deny DMZ-to-Trust implicite. Réseau de management isolé.

Contrôle 9.2 — Politique NAT sécurisée et anti-hairpinning

> ***CIS Ref :*** *Segmentation / NAT* | ***MITRE :*** *T1090* | ***Niveau :*** 🟢 *L1*

Description du risque

Une configuration NAT permissive peut créer du trafic hairpinning non maîtrisé (trafic interne sortant par Internet pour revenir en DMZ, contournant les règles de sécurité intra-zone). Les règles NAT mal configurées peuvent également exposer des services internes involontairement.

Impact potentiel

- Contournement des politiques de sécurité via hairpinning
- Exposition de services internes par des règles NAT trop permissives
- Reconnaissance interne facilitée par des règles de Source NAT incomplètes

Navigation

```
Policies > NAT > Add
→ NAT de source (SNAT) pour le trafic Internet sortant :
   Source Zone : trust, Destination Zone : untrust
   Source Address : réseaux internes
   Translation : Dynamic IP and Port (interface IP)

→ Pour les serveurs DMZ publiés (DNAT) :
   Source Zone : untrust, Destination Zone : untrust (hairpin via zone)
   Destination Address : IP publique
   Translated Address : IP DMZ du serveur

→ Vérifier l'absence de règles NAT avec Source = any sans restriction
```

CLI de vérification

```
show running nat-policy
show config running | xpath /config/devices/entry/vsys/entry/rulebase/nat
```

Remédiation

1. Auditer toutes les règles NAT existantes
2. Supprimer les règles NAT non utilisées ou trop permissives
3. Documenter chaque règle DNAT (publication de service) avec justification
4. Vérifier que les règles SNAT utilisent des plages IP sources explicites (pas `any`)
5. Tester que les flux hairpinning légitimes passent par les règles de sécurité appropriées

Valeur par défaut : Aucune règle NAT pré-configurée.

Critère de conformité : Toutes les règles NAT documentées. Aucune règle NAT avec source = any non justifiée. Revue trimestrielle des règles DNAT.

Contrôle 9.3 — Micro-segmentation et interdiction intrazone non contrôlée

> ***CIS Ref :*** *7.1 (Intrazone), Security Policy* | ***MITRE :*** *T1055* | ***Niveau :*** 🔵 *L2*

Description du risque

Par défaut, PAN-OS autorise le trafic intra-zone (entre interfaces de la même zone) sans inspection. Dans une zone trust plate, tous les hôtes peuvent communiquer entre eux sans restriction. La micro-segmentation via sous-zones ou tags dynamiques permet de limiter ces communications latérales.

Impact potentiel

- Mouvement latéral libre entre serveurs/postes de la même zone lors d'une compromission
- Propagation de ransomwares entre postes du même VLAN non détectée
- Compromission d'un poste utilisateur donnant accès à tous les postes du même segment

Navigation

```
Network > Zones > [zone trust] > Zone Protection
→ Activer un Zone Protection Profile même en intrazone

Policies > Security > Default Rules > intrazone-default
→ Action : Allow (par défaut) → à changer en Deny avec log si micro-segmentation stricte
→ Ou : créer des règles intrazone explicites pour les flux légitimes uniquement

Pour une micro-segmentation avancée :
Objects > Tags > Ajouter des tags dynamiques
Policies > Security > Source/Destination : utiliser Dynamic Address Groups
```

CLI de vérification

```
show running security-policy | match intrazone
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"intrazone"
```

Remédiation

1. Modifier la règle `intrazone-default` pour logger tout le trafic intra-zone
2. Dans les environnements sensibles : passer `intrazone-default` en Deny et créer des règles explicites
3. Utiliser les Dynamic Address Groups et tags pour segmenter dynamiquement les flux
4. Implémenter des sous-zones (ex : serveurs-db, serveurs-web, postes-utilisateurs) pour une granularité accrue

Valeur par défaut : Trafic intrazone = Allow sans log ni inspection.

Critère de conformité : Règle intrazone-default avec logging activé. Dans les zones sensibles (serveurs, DMZ) : intrazone-default = Deny. Flux intrazone légitimes documentés et explicitement autorisés.

Contrôle 9.4 — Architecture Zero Trust : microsegmentation, User-ID + App-ID + Device-ID sur toutes les politiques

> ***CIS Ref :*** *7.1 (Application Security Policies), Zero Trust Best Practices* | ***MITRE :*** *T1199 (Trusted Relationship), T1021 (Remote Services — Lateral Movement), T1078 (Valid Accounts)* | ***Niveau :*** 🔵 *L2*

Description du risque

L'approche traditionnelle de sécurité périmétrique ("faire confiance à ce qui est à l'intérieur du réseau") est fondamentalement insuffisante face aux menaces modernes. La compromission d'un seul hôte interne ou d'un accès VPN légitime donne accès à l'ensemble du réseau interne si aucune microsegmentation n'est en place. Le principe **Zero Trust** — "ne jamais faire confiance, toujours vérifier" — implémenté nativement dans PAN-OS via la combinaison App-ID + User-ID + Device-ID constitue le niveau de contrôle le plus avancé.

MITRE ATT&CK **T1199 (Trusted Relationship)** couvre précisément l'abus de relations de confiance implicites dans l'architecture réseau. Un attaquant comprenant une relation de confiance (ex : Panorama qui fait confiance à tous les firewalls managés, ou un VPN qui fait confiance au segment trust) peut se déplacer librement sans déclencher d'alerte.

Composants Zero Trust dans PAN-OS : - **App-ID** : Jamais `Application = any` — uniquement les applications explicitement nécessaires - **User-ID** : Authentification utilisateur requise pour tous les flux sensibles (pas uniquement l'IP source) - **Device-ID** : Identification et évaluation de la posture des équipements (via Cortex XDR) - **Microsegmentation** : Zones granulaires par catégorie de charge de travail (web, base de données, application, gestion)

Impact potentiel

- Mouvement latéral libre depuis un seul hôte compromis si pas de Zero Trust (T1021)
- Relation de confiance implicite exploitée pour accéder à des systèmes critiques sans contrôle d'identité (T1199)
- Escalade de privilèges réseau via des comptes de service ou des exceptions de politique non révisées (T1078)
- Compromission de Panorama donnant accès à tous les firewalls managés sans contrôle supplémentaire (T1199)

Navigation

```
-- 1. Principes d'implémentation Zero Trust : App-ID sur TOUTES les politiques --
Policies > Security > [toutes les règles]
→ Application : JAMAIS "any" — uniquement les applications nominatives nécessaires
→ Service : application-default (App-ID gère les ports)
→ Source/Destination User : spécifier le groupe AD ou l'utilisateur si User-ID est configuré
→ Exception documentée obligatoire pour toute règle any

-- 2. Microsegmentation : zones par catégorie de charge de travail --
Network > Zones > Add

Architecture de zones recommandée (Zero Trust) :
→ Zone untrust : Internet et WAN non maîtrisé
→ Zone dmz-web : serveurs web frontaux exposés (T1 — HTTPS uniquement entrant)
→ Zone dmz-app : serveurs d'application (T2 — communications inter-tiers strictes)
→ Zone dmz-db : serveurs de base de données (T3 — ports SQL uniquement depuis zone dmz-app)
→ Zone trust-users : postes utilisateurs (accès contrôlé vers les ressources métier)
→ Zone trust-servers : serveurs internes (accès depuis trust-users selon App-ID)
→ Zone management : infrastructure de gestion (accès restreint aux admins MFA)
→ Zone iot : équipements IoT/OT (isolation stricte — pas d'accès vers trust)

Politiques Zero Trust inter-zones (exemples) :
→ untrust → dmz-web : allow HTTPS/HTTP (App-ID ssl + web-browsing uniquement)
→ dmz-web → dmz-app : allow app-spécifique uniquement (ex : application custom)
→ dmz-app → dmz-db : allow sql-server / mysql / postgresql uniquement
→ dmz-db → trust-servers : DENY par défaut (les DB n'initient pas de connexions vers
l'interne)
→ trust-users → trust-servers : allow par User-ID + App-ID (jamais IP seule)
→ management → any : allow ssh/https uniquement, source restreinte aux postes d'admin

-- 3. User-ID requis sur toutes les règles sensibles --
Policies > Security > [règle sensible]
→ Source User : [groupe AD des utilisateurs autorisés] (pas "any")
→ Requiert : User-ID activé et mappages à jour (contrôles 5.2, 5.7)

-- 4. Intégration Cortex XDR pour Device-ID (posture endpoint) --
Device > Setup > Management > Cortex XDR Integration
→ Activer l'intégration pour la validation de posture des endpoints
→ Politique Zero Trust : accès conditionné à la posture de sécurité de l'endpoint
→ Endpoint non conforme → zone quarantaine automatique

-- 5. Validation continue : BPA et AIOps --
Via BPA (https://bpa.paloaltonetworks.com/) :
→ Mesurer le pourcentage de règles avec App-ID vs any
→ Mesurer le pourcentage de règles avec User-ID défini
→ Score Zero Trust Readiness (rapport BPA)

Via Panorama > AIOps > Best Practices :
→ Dashboard Zero Trust : score de conformité par domaine
→ Recommandations priorisées pour améliorer la posture Zero Trust
```

CLI de vérification

```
# Vérifier les règles sans App-ID (candidats à la remédiation Zero Trust)
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"application.*any"

# Vérifier les règles sans User-ID (amélioration Zero Trust)
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"source-user.*any"

# Lister les zones configurées
show zone all

# Vérifier le trafic intrazone (mouvement latéral potentiel)
show running security-policy | match intrazone

# Vérifier l'état User-ID sur chaque interface
show user interface all
```

Remédiation

1. **Audit de la politique existante** : utiliser le Policy Optimizer (contrôle 4.5) pour identifier toutes les règles avec `Application = any` — ces règles sont incompatibles avec Zero Trust.
2. **Définir la topologie de zones Zero Trust** : créer des zones granulaires par catégorie de charge de travail (web, app, db, users, management, IoT) selon le modèle ci-dessus.
3. **Implémenter la règle “never trust, always verify”** : chaque règle doit spécifier l’application, l’utilisateur (via User-ID) ET la zone source/destination.
4. **Microsegmentation inter-couches applicatives** : interdire tout flux direct entre la zone db et les zones utilisateurs — toujours passer par la zone app.
5. **Aucune règle intrazone non contrôlée** : modifier `intrazone-default` en Deny avec logging dans les zones sensibles (contrôle 9.3).
6. **Intégration Cortex XDR** (si disponible) : conditionner l’accès réseau à la posture de sécurité de l’endpoint via Device-ID.
7. **Principe du moindre privilège réseau** : pour chaque règle, documenter pourquoi cette application, cet utilisateur, et ce segment doivent communiquer — si aucune justification claire, la règle est un risque.
8. Mesurer la progression Zero Trust via le BPA tool trimestriellement et documenter l’évolution du score.

Valeur par défaut : PAN-OS permet la configuration Zero Trust mais ne l’impose pas. Les configurations par défaut sont souvent permissives (any, any, allow).

Critère de conformité : Moins de 5% de règles avec `Application = any` sur les flux inter-zones. Zones granulaires par catégorie de charge de travail documentées. User-ID configuré sur les règles d’accès aux ressources sensibles. Flux DB → utilisateurs = Deny par défaut. Score BPA Zero Trust Readiness documenté et en amélioration. Analyse Policy Optimizer effectuée dans les 90 derniers jours.

Contrôle 9.5 — Durcissement Haute Disponibilité (HA) : chiffrement, authentification et tests de basculement

CIS Ref : *3.1, 3.2, 3.3 (High Availability)* | ***MITRE :*** *T1499 (Endpoint Denial of Service — HA prevents SPOF), T1040 (Network Sniffing — HA link encryption)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le cluster Haute Disponibilité (HA) PAN-OS se compose de deux membres (Active/Passive ou Active/Active) communiquant via deux liens dédiés : - **HA1 (Control Link)** : synchronisation de l'état de la configuration et des sessions de gestion — trafic hautement sensible - **HA2 (Data Link)** : synchronisation des tables de sessions et du trafic en cours — trafic potentiellement volumineux

Par défaut, ces communications HA **ne sont pas chiffrées**, exposant les informations de configuration et de session à un attaquant en position d'écoute sur le réseau de gestion. Un attaquant ayant accès au segment réseau HA peut intercepter les paquets HA1 pour extraire des informations de configuration, ou injecter des paquets HA falsifiés pour provoquer un basculement non planifié (attaque de disponibilité).

La désactivation du pre-emption est une mesure de stabilité critique : si le pre-emption est activé, le retour automatique du membre actif après récupération provoque un double basculement non contrôlé, augmentant le risque d'interruption de service et d'inconsistance de session.

Impact potentiel

- Interception des communications HA1 révélant des informations de configuration sensibles (T1040)
- Injection de paquets HA falsifiés provoquant un basculement non planifié (T1499 — attaque de disponibilité)
- Absence d'authentification du lien HA permettant à un acteur non autorisé de rejoindre le cluster
- Double basculement provoqué par le pre-emption lors d'un retour actif — interruption de service
- Synchronisation HA défaillante non détectée : le membre passif ne peut pas prendre le relais correctement
- Utilisation de câbles HA partagés avec le trafic de production : contaminant les données de synchronisation

Navigation

```
-- 1. Activation du chiffrement HA1 (Control Link) --
Device > High Availability > General > Control Link (HA1)
→ Encryption Enabled : cocher
→ Ce chiffrement protège les paquets de synchronisation de configuration sur HA1

CLI :
set deviceconfig high-availability control-link encryption enable

-- 2. Activation du chiffrement HA2 (Data Link) --
Device > High Availability > General > Data Link (HA2)
→ HA2 Encryption Enabled : cocher
→ Protège la synchronisation des sessions sur HA2

CLI :
set deviceconfig high-availability session-synchronization ha2-encryption-enabled yes

-- 3. Configuration du mot de passe HA Group (authentification) --
Device > High Availability > General > Election Settings
→ Group Password : définir un mot de passe fort partagé entre les deux membres
→ Ce mot de passe authentifie les membres du cluster — évite l'ajout d'un tiers non autorisé

CLI :
set deviceconfig high-availability group 1 authentication-key <clé-partagée>

-- 4. Désactivation du Pre-emption (stabilité du cluster) --
Device > High Availability > General > Election Settings
→ Preemptive : décocher
→ Avec pre-emption désactivé : une fois le membre passif devenu actif, il reste actif
  jusqu'à une intervention manuelle ou un failover explicite
→ Évite le double basculement lors du retour de l'ancien actif

CLI :
set deviceconfig high-availability group 1 preemptive no

-- 5. Configuration du Link Monitoring et Path Monitoring --
Device > High Availability > Link and Path Monitoring
→ Link Monitoring : activer et sélectionner les interfaces critiques de production
   (le failover se déclenche si ces interfaces tombent)
→ Path Monitoring : activer avec des IP cibles critiques (default gateway, IP serveur clé)
   - IP à monitorer : IP de la gateway Internet, IP d'un serveur interne critique
   - Failure Condition : any (l'une quelconque des cibles inaccessible = failover)
→ HA Passive Link State : Auto
   (le membre passif maintient ses interfaces "up" pour un failover rapide)

CLI :
set deviceconfig high-availability group 1 monitoring link-monitoring enabled yes
set deviceconfig high-availability group 1 monitoring path-monitoring enabled yes

-- 6. Configuration physique des liens HA --
→ HA1 : interface physique dédiée sur le VLAN/réseau de gestion out-of-band
   JAMAIS partager le lien HA1 avec du trafic de production
→ HA2 : interface physique dédiée sur un VLAN isolé
   Débit suffisant pour la synchronisation des sessions (au moins 1 Gbps)
→ Câblage direct entre les deux membres si possible (évite les switches intermédiaires)
→ Règles de firewall upstream : autoriser uniquement le trafic HA entre les deux membres HA
   Bloquer tout autre trafic vers les interfaces HA
```

```
-- 7. Tests de basculement (procédure recommandée) --
# Test de failover contrôlé (sur le membre actif) :
request high-availability state suspend

# Vérifier que le membre passif est devenu actif :
show high-availability state  (sur l'ex-passif — doit indiquer Active)

# Remettre en service le membre suspendu :
request high-availability state functional

# Vérifier la synchronisation après test :
show high-availability state-synchronization
```

CLI de vérification

```
# Vérifier l'état général HA
show high-availability state
show high-availability all

# Vérifier l'état de synchronisation HA
show high-availability state-synchronization

# Vérifier les statistiques du lien HA1 (inclut infos chiffrement)
show high-availability control-link statistics

# Vérifier les statistiques du lien HA2
show high-availability data-link statistics

# Vérifier le nombre de transitions HA (indicateur d'instabilité)
show high-availability transitions

# Vérifier la configuration HA complète
show config running | xpath /config/devices/entry/deviceconfig/high-availability

# Vérifier les versions PAN-OS des deux membres
show system info | match sw-version  (exécuter sur chaque membre)
```

Remédiation

1. **Activer le chiffrement HA1 et HA2** : Dans `Device > High Availability > General`, activer l'encryption sur les deux liens. Cette activation est transparente et ne nécessite pas d'interruption de service si appliquée simultanément sur les deux membres.
2. **Configurer le HA Group Password** : Définir un mot de passe de groupe fort (≥ 20 caractères, stocké dans le gestionnaire de secrets) pour authentifier les membres du cluster.
3. **Désactiver le Pre-emption** : Décocher `Preemptive` dans les paramètres d'élection HA pour éviter les basculements automatiques non contrôlés lors du retour de l'actif.
4. **Activer Link Monitoring et Path Monitoring** : Configurer des interfaces et chemins critiques comme déclencheurs de failover. Tester les seuils sur l'environnement réel pour éviter les faux positifs.
5. **Interfaces HA dédiées** : Vérifier que les liens HA1 et HA2 utilisent des interfaces physiques dédiées, séparées du trafic de production. Documenter les connexions physiques HA dans le schéma réseau.
6. **Règles de filtrage sur les interfaces HA** : Configurer les switches en amont pour n'autoriser que le trafic HA entre les deux membres. Bloquer tout trafic vers les ports HA depuis d'autres sources.

7. **Synchronisation de version PAN-OS** : Vérifier que les deux membres HA ont **exactement la même version PAN-OS** avant de déployer les contrôles de sécurité. Un membre exécutant une version différente peut présenter un comportement imprévisible (contrôle 1.4).
8. **Tests de basculement réguliers** : Effectuer un test de failover contrôlé trimestriellement (`request high-availability state suspend`) pour valider que le membre passif peut prendre le relais correctement et que les politiques sont bien synchronisées.
9. **Alertes SIEM sur les transitions HA** : Configurer des alertes sur les événements de basculement HA dans les logs Système. Un basculement non planifié est un indicateur d'incident réseau ou d'attaque de disponibilité.

Valeur par défaut : Chiffrement HA1 et HA2 désactivés par défaut. Pas de HA Group Password. Pre-emption activé par défaut. Link Monitoring et Path Monitoring à configurer manuellement.

Critère de conformité : Chiffrement HA1 et HA2 activés. HA Group Password configuré et stocké dans le gestionnaire de secrets. Pre-emption désactivé. Link Monitoring et Path Monitoring configurés avec au moins une interface et un chemin. Interfaces HA dédiées (pas de partage avec le trafic de production). Test de basculement documenté dans les 90 derniers jours. Alertes SIEM configurées sur les transitions HA. Deux membres HA avec la même version PAN-OS.

Domaine 10 — Journalisation et supervision SIEM

Objectif : *Centraliser tous les logs PAN-OS vers un SIEM externe pour la détection des menaces, la conformité réglementaire et la réponse aux incidents. La guidance CISA recommande spécifiquement de surveiller les logs de firewall pour : les tentatives d'accès admin répétées et échouées, les changements inattendus de comptes utilisateurs, et les connexions sortantes inhabituelles depuis le firewall lui-même. Sans logs centralisés, les tentatives d'intrusion et les compromissions restent invisibles.*

Contrôle 10.1 — Serveur Syslog configuré pour tous les types de logs

CIS Ref : *1.1.1.1 (Syslog logging)* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

Sans journalisation distante, les logs sont uniquement stockés sur le disque local du firewall avec une rétention limitée. Un attaquant ayant compromis le firewall peut effacer les logs locaux. La centralisation vers un SIEM externe garantit la persistance, l'immuabilité et la corrélation des événements.

Impact potentiel

- Perte des logs lors d'un incident (saturation disque, attaque, défaillance matérielle)
- Impossibilité d'analyser rétrospectivement des incidents au-delà de la rétention locale
- Non-conformité avec PCI-DSS (req. 10.5), NIS2, RGPD (art. 33 — documentation incidents)

Navigation

```
Device > Server Profiles > Syslog > Add
→ Name : SIEM-Syslog-Profile
→ Syslog Server : IP du SIEM (ex : 10.0.200.50)
→ Transport : UDP/514 (ou TCP/514, ou SSL/6514 pour chiffrement)
→ Format : BSD (ou IETF pour RFC 5424)
→ Facility : LOG_USER ou LOG_LOCAL0

Device > Log Settings > System > Add
→ Name : System-to-SIEM
→ Filter : All Logs
→ Syslog : SIEM-Syslog-Profile

Device > Log Settings > Configuration > Add
→ Filter : All Logs, Syslog : SIEM-Syslog-Profile

Device > Log Settings > User-ID > Add
→ Filter : All Logs, Syslog : SIEM-Syslog-Profile

Device > Log Settings > HIP Match > Add
→ Filter : All Logs, Syslog : SIEM-Syslog-Profile

Device > Log Settings > IP-Tag > Add
→ Filter : All Logs, Syslog : SIEM-Syslog-Profile
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/setting/syslog
show log-settings
show logging-status
```

Remédiation

1. Créer le profil Syslog pointant vers le SIEM
2. Configurer les Log Settings pour System, Configuration, User-ID, HIP Match, IP-Tag avec filtre = All Logs
3. Configurer le Log Forwarding Profile pour Traffic, Threat et WildFire (voir contrôles suivants)
4. Si chiffrement nécessaire : utiliser TCP avec TLS (port 6514, profil SSL/TLS côté firewall)
5. Tester la réception des logs sur le SIEM avec `test log-forwarding`

Valeur par défaut : Aucun serveur Syslog configuré. Logs stockés uniquement en local.

Critère de conformité : Profil Syslog configuré vers un SIEM. Tous les types de logs système (System, Config, User-ID, HIP, IP-Tag) transmis avec filtre = All Logs.

Contrôle 10.2 — Log Forwarding Profile sur toutes les règles de sécurité

CIS Ref : *7.4 (Logging on default security policies), 1.1.1* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

Les logs de trafic (Traffic), de menaces (Threat) et WildFire sont générés au niveau des règles de sécurité. Un `Log Forwarding Profile` doit être attaché à chaque règle de sécurité pour transmettre ces logs au SIEM. Sans ce profil, les logs restent en local uniquement.

Impact potentiel

- Trafic autorisé et bloqué non visible dans le SIEM : impossibilité de détecter les attaques
- Absence de corrélation entre les événements firewall et les autres sources de sécurité
- Non-conformité audit : les flux réseau doivent être journalisés (PCI-DSS req. 10.2)

Navigation

```
Objects > Log Forwarding > Add
→ Name : Forward-All-to-SIEM
→ Traffic Logs : Syslog = SIEM-Syslog-Profile, Filter = All Logs
→ Threat Logs : Syslog = SIEM-Syslog-Profile, Filter = All Logs
→ WildFire Logs : Syslog = SIEM-Syslog-Profile, Filter = All Logs
→ URL Logs : Syslog = SIEM-Syslog-Profile, Filter = All Logs
→ Data Logs : Syslog = SIEM-Syslog-Profile, Filter = All Logs

Policies > Security > [chaque règle]
→ Log Setting : Forward-All-to-SIEM
→ Log at Session End : coché (ou Log at Session Start pour trafic à longue durée)
```

CLI de vérification

```
show config running | xpath /config/devices/entry/vsys/entry/log-settings
show config running | xpath /config/devices/entry/vsys/entry/rulebase/security/rules | match
"log-setting"
show running security-policy | match "log-forwarding"
```

Remédiation

1. Créer le Log Forwarding Profile `Forward-All-to-SIEM`
2. Attacher ce profil à toutes les règles de sécurité (permit et deny)
3. Activer `Log at Session End` sur toutes les règles
4. Pour les règles de refus avec trafic haute fréquence, filtrer si nécessaire pour éviter la saturation du SIEM

Valeur par défaut : Aucun Log Forwarding Profile attaché aux nouvelles règles. Log at Session End désactivé par défaut sur certaines règles.

Critère de conformité : 100% des règles de sécurité ont un Log Forwarding Profile configuré. Log at Session End activé. Traffic, Threat, WildFire, URL et Data logs transmis au SIEM.

Contrôle 10.3 — SNMPv3 traps pour les événements critiques

CIS Ref : *1.1.1.2 (SNMPv3 traps)* | ***MITRE :*** *T1562* | ***Niveau :*** 🔵 *L2*

Description du risque

Les traps SNMP permettent une notification en temps réel des événements critiques (défaillance d'interface, saturation CPU/mémoire, tentative de connexion échouée) vers le système de supervision réseau (NMS). Sans traps, ces événements ne sont visibles qu'en consultant manuellement les logs.

Impact potentiel

- Attaque DDoS saturant les ressources du firewall non détectée en temps réel
- Défaillance d'interface HA non alertée
- Tentatives de connexion admin répétées non notifiées à l'équipe SOC

Navigation

```
Device > Server Profiles > SNMP Trap > Add
→ Name : NMS-SNMP-Trap
→ Version : V3
→ Users : créer un utilisateur SNMPv3
   - Security Level : authPriv
   - Auth Password : (mot de passe fort ≥ 16 chars)
   - Priv Password : (mot de passe fort ≥ 16 chars)

Device > Log Settings > System > Add
→ Filter : severity = critical
→ SNMP Trap : NMS-SNMP-Trap
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/system/snmp-setting
show snmp stats
```

Remédiation

1. Créer le profil SNMP Trap V3 avec sécurité authPriv
2. Configurer des traps sur les événements System de sévérité Critical et High
3. Valider la réception des traps sur le NMS avec `test snmp-trap`
4. Intégrer les traps dans les tableaux de bord de supervision réseau (Zabbix, SolarWinds, PRTG)

Valeur par défaut : Aucun profil SNMP Trap configuré.

Critère de conformité : Si SNMP traps utilisés : SNMPv3 avec authPriv uniquement. Traps configurés pour les événements System de sévérité ≥ High.

Contrôle 10.4 — Rétention des logs et intégration Panorama

CIS Ref : *Device Setup, Log Settings* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

La rétention des logs sur le firewall local est limitée par la taille du disque. Les exigences réglementaires (PCI-DSS : 12 mois, NIS2 : 12 mois, RGPD : variable) imposent une rétention longue durée. Panorama centralise la gestion et les logs de multiples firewalls pour une vue unifiée.

Impact potentiel

- Perte des preuves forensiques lors d'investigations portant sur des événements anciens
- Non-conformité avec les obligations légales de conservation des logs
- Impossibilité de détecter des attaques APT (Advanced Persistent Threats) à faible signature sur le long terme

Navigation

```
Device > Setup > Management > Logging and Reporting Settings
→ Log Storage : vérifier l'espace disponible et configurer les quotas par type de log

Pour Panorama :
Device > Setup > Management > Panorama Settings
→ Panorama Servers : IP du serveur Panorama principal et secondaire
→ Mode : Managed Device

Sur Panorama :
Panorama > Managed Devices > [firewall]
→ Vérifier "Log Collection Group" pour la centralisation des logs
→ Configurer la rétention : ≥ 90 jours en ligne, archive ≥ 12 mois
```

CLI de vérification

```
show system disk-space
show log traffic start-time equal last-30-days | match count
show panorama-status
```

Remédiation

1. Configurer les quotas de log locaux pour maximiser la rétention sur disque
2. Intégrer le firewall dans Panorama si disponible
3. Configurer l'archivage long terme des logs vers stockage externe (NFS, S3) via Panorama
4. Documenter la politique de rétention des logs conformément aux obligations réglementaires applicables

Valeur par défaut : Rétention limitée à la capacité du disque local. Pas d'intégration Panorama par défaut.

Critère de conformité : Logs Traffic et Threat conservés ≥ 90 jours accessible en ligne. Archive ≥ 12 mois pour les environnements soumis à PCI-DSS/NIS2. Intégration Panorama si plusieurs firewalls.

Contrôle 10.5 — Activation de la journalisation haute charge DP (High DP Load)

CIS Ref : *1.1.3 (Enable Log on High DP Load)* | ***MITRE :*** *T1499* | ***Niveau :*** ⚪ *INFO*

Description du risque

Lorsque le Data Plane (DP) du firewall est sous forte charge, certains logs peuvent être abandonnés silencieusement. L'option "Enable Log on High DP Load" garantit que les événements de sécurité sont loggés même lors d'attaques volumétriques qui saturent les ressources de traitement.

Impact potentiel

- Perte de logs pendant une attaque DDoS active, précisément au moment où les logs sont le plus nécessaires
- Impossibilité de reconstituer la chronologie d'une attaque volumétrique

Navigation

```
Device > Setup > Management > Logging and Reporting Settings
→ "Enable Log on High DP Load" : cocher

Ou :
Device > Setup > Management > General Settings
→ Log on High DP Load : Enabled
```

CLI de vérification

```
show config running | xpath /config/devices/entry/deviceconfig/setting/logging | match
"high-dp-load"
show system statistics application
```

Remédiation

1. Activer "Enable Log on High DP Load" dans les paramètres de logging
2. Surveiller l'utilisation CPU/mémoire du DP régulièrement
3. Configurer une alerte SNMP/Syslog si l'utilisation DP dépasse 80%

Valeur par défaut : Désactivé par défaut sur les versions antérieures à PAN-OS 11.x. Vérifier la valeur effective.

Critère de conformité : Log on High DP Load = Enabled.

Contrôle 10.6 — Surveillance des IoC spécifiques recommandés par la CISA

CIS Ref : *1.1.1 (Log Monitoring)* | ***MITRE :*** *T1078, T1562, T1498* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

La CISA recommande aux organisations de surveiller activement trois catégories spécifiques d'indicateurs dans les logs des firewalls réseau, qui sont précurseurs ou indicateurs de compromission active :

1. **Tentatives d'accès admin répétées et échouées** — indicateur d'attaque brute force ou de credential stuffing ciblant l'interface de gestion
2. **Changements inattendus de comptes utilisateurs** — un attaquant ayant obtenu un accès admin crée souvent un compte backdoor ou modifie les permissions

3. **Connexions sortantes inhabituelles depuis le firewall lui-même** — le firewall lui-même ne devrait initier des connexions sortantes que vers les serveurs de mise à jour, DNS, NTP, et Syslog/SIEM définis ; toute autre connexion sortante est suspecte

Ces indicateurs sont directement liés aux CVE récentes : CVE-2025-0108 (auth bypass) et CVE-2024-9474 (privilege escalation) permettent précisément à un attaquant de créer des comptes backdoor et d'établir des connexions sortantes de commande et contrôle depuis le firewall.

Impact potentiel

- Compromission non détectée via CVE-2025-0108 ou CVE-2024-9474 en l'absence de surveillance des changements de comptes
- Persistance d'un implant C2 sur le firewall non détecté si les connexions sortantes du firewall ne sont pas monitorées
- Attaque brute force réussie non détectée faute de corrélation des tentatives d'authentification échouées

Navigation

```
-- Alertes SIEM recommandées par la CISA --

1. Tentatives d'authentification admin échouées :
Monitor > Logs > System
→ Filtrer : subtype = auth, severity = medium, description match "failed"
→ Créer alerte SIEM : > 5 échecs depuis la même IP en < 5 minutes

2. Changements de configuration de comptes :
Monitor > Logs > Configuration
→ Filtrer : description match "admin" ou "user" ou "role"
→ Créer alerte SIEM : tout changement de compte hors fenêtre de maintenance

3. Connexions sortantes depuis le firewall (trafic initié par le MGT plane) :
Monitor > Logs > System
→ Surveiller les connexions vers des IP non référencées dans le profil de gestion
→ Comparer avec la liste autorisée : update servers, DNS, NTP, SIEM, Panorama

-- Configuration des alertes dans le profil Log Forwarding --
Device > Log Settings > System > [profil SIEM]
→ Filter : severity match "high" OR "critical"
→ Forwarding : SIEM-Syslog-Profile

-- Requêtes SIEM recommandées --
# Brute force admin
source=paloalto log_type=system subtype=auth status=failure
| stats count by src_ip
| where count > 5

# Modification de compte
source=paloalto log_type=config
| search description="*admin*" OR description="*user*"

# Connexions sortantes inattendues depuis IP de gestion
source=paloalto log_type=traffic
| where src_ip=<MGT-IP> AND dst_ip NOT IN [update-servers, dns, ntp, siem]
```

CLI de vérification

```
show log system direction equal backward
show log config direction equal backward | match "admin\|user\|role"
show admins
show session all filter application ssl source <MGT-IP>
```

Remédiation

1. Créer des règles d'alerte SIEM pour les trois indicateurs CISA : auth failures, compte changes, connexions sortantes anormales
2. Définir la liste des connexions sortantes légitimes du firewall (baselines) :
   - `updates.paloaltonetworks.com`, `wildfire.paloaltonetworks.com` — mises à jour
   - Serveurs DNS internes
   - Serveurs NTP
   - Serveurs SIEM/Syslog
   - Panorama (si déployé)
3. Configurer des alertes P1 pour tout changement de compte admin hors fenêtre de maintenance planifiée
4. Configurer des alertes P2 pour les pics de tentatives d'authentification échouées (> 5 en 5 minutes depuis une même IP)
5. Configurer des alertes P1 pour toute connexion sortante initiée depuis l'IP de gestion vers une destination non listée
6. Intégrer ces règles dans le runbook SOC avec procédures d'escalade documentées

Valeur par défaut : Aucune alerte SIEM spécifique configurée. Logs de système transmis sans filtrage ni corrélation.

Critère de conformité : Règles d'alerte SIEM configurées pour les trois indicateurs CISA. Baselines de connexions sortantes légitimes documentées. Runbook SOC incluant la procédure pour chaque alerte. Test des alertes effectué dans les 30 derniers jours.

Contrôle 10.7 — Durcissement Panorama : gestionnaire centralisé sécurisé

CIS Ref : *Panorama Administration Best Practices* | ***MITRE :*** *T1199 (Trusted Relationship), T1078 (Valid Accounts), T1562 (Impair Defenses)* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Panorama est la **plateforme de gestion centralisée** de tous les firewalls Palo Alto d'une organisation. Par conception, un firewall managé fait **confiance implicite** à Panorama : une configuration poussée depuis Panorama est appliquée sans validation sur tous les firewalls managés simultanément. **La compromission de Panorama équivaut à la compromission de l'ensemble du parc de firewalls.**

MITRE ATT&CK **T1199 (Trusted Relationship)** couvre précisément ce vecteur : un attaquant compromettant Panorama peut pousser des politiques malveillantes (ouverture de portes dérobées, désactivation du filtrage, exfiltration de configurations incluant les clés VPN) sur tous les firewalls en quelques secondes, depuis un seul point.

Panorama doit être durci avec le même niveau d'exigence que les firewalls eux-mêmes, en appliquant tous les contrôles des domaines D1 à D3 sur la plateforme Panorama. Les spécificités Panorama sont documentées ci-dessous.

Impact potentiel

- Compromission de Panorama = compromission simultanée de TOUS les firewalls managés (T1199)
- Push de politiques malveillantes sur l'ensemble du parc (ouverture de ports, désactivation du filtrage, T1562)
- Exfiltration de la configuration complète de tous les firewalls (clés VPN, certificats, politiques)
- Création de comptes backdoor sur tous les firewalls via un seul commit Panorama (T1078)
- Suppression de logs ou modification des profils de journalisation sur tout le parc
- Désactivation coordonnée de Threat Prevention sur toutes les règles en un commit

Navigation

```
-- 1. Isolation réseau de Panorama (priorité absolue) --
→ Panorama doit TOUJOURS être sur un VLAN de gestion dédié et isolé
→ JAMAIS exposer l'interface de gestion Panorama sur Internet
→ Accès à Panorama uniquement via jump box / bastion avec MFA
→ VLAN Panorama séparé des VLAN de production et de l'infrastructure managée
→ ACLs sur les switches upstream : seuls les firewalls managés et les jump boxes autorisés à
contacter Panorama

-- 2. Vérifier la connexion entre les firewalls et Panorama --
Sur chaque firewall managé (CLI) :
show panorama-status
→ Vérifier : "Connected", "Synchronized"
→ La connexion se fait sur TCP/3978 entre Panorama et le Management Plane du firewall

-- 3. MFA et RBAC sur Panorama --
(Panorama Web UI — identique au firewall)
Panorama > Administrators > Add
→ Comptes nominatifs uniquement — JAMAIS de compte partagé
→ Authentication Profile : MFA obligatoire (identique au contrôle 2.1)
→ Rôles : Device Group and Template Admin (accès restreint par périmètre)

Panorama > Admin Roles > Add
→ Rôles granulaires par groupe de firewalls (Device Groups)
→ Opérateurs : accès lecture seule sur leurs firewalls uniquement
→ Ingénieurs sécurité : accès modification sur leur périmètre uniquement
→ Super Admins : maximum 2 personnes, accès tracé, sous PAM

-- 4. Restriction des IP sources autorisées --
Panorama > Setup > Interfaces > Management
→ Permitted IP Addresses : uniquement les postes d'administration et jump boxes autorisés

-- 5. Panorama HA pour la haute disponibilité --
Panorama > High Availability > General
→ Configurer la HA en mode Active/Passive entre deux appliances M-Series
→ Vérifier la synchronisation : show high-availability state (sur Panorama)
→ HA Panorama garantit la continuité de la gestion centralisée

-- 6. Log Collectors redondants --
Panorama > Managed Collectors > Add
→ Configurer au minimum deux Log Collectors (redondance)
→ Chaque firewall envoie ses logs aux deux Log Collectors
→ Rétention : ≥ 90 jours en ligne sur les Log Collectors

-- 7. Certificats de gestion valides sur Panorama --
Panorama > Certificate Management > Certificates
→ Importer un certificat TLS signé par la CA interne
→ Profil SSL/TLS : TLS 1.2 minimum, certificat non auto-signé

-- 8. NTP et temps synchronisés --
Panorama > Setup > Services > NTP
→ NTP Servers : synchronisés avec les mêmes sources que les firewalls
→ Obligatoire pour la corrélation temporelle des logs

-- 9. Accès Panorama audité et alerté --
Panorama > Log Settings > System > Add
→ Filter : All Logs
```

```
→ Syslog : profil SIEM
→ Alertes SIEM sur : connexions admin, commits Panorama, modifications de Device Groups
```

CLI de vérification (depuis un firewall managé)

```
# Vérifier la connexion Panorama depuis un firewall
show panorama-status

# Vérifier que le firewall reçoit bien des configurations de Panorama
show config pushed-shared-policy
show config pushed-template

# Vérifier les admins actifs sur Panorama
# (Exécuter sur Panorama directement)
show admins all
show config running | xpath /config/mgt-config/users
```

CLI de vérification (sur Panorama)

```
# Vérifier la HA Panorama
show high-availability state
show high-availability all

# Vérifier l'état de tous les firewalls managés
show devices all
show devices connected

# Vérifier les Log Collectors
show log-collector all
show log-collector-group all

# Vérifier les admins actifs
show admins all

# Vérifier la version de Panorama
show system info | match sw-version
```

Remédiation

1. **Isolation réseau absolue** : placer Panorama sur un VLAN de gestion dédié, isolé des VLAN de production. Aucun accès direct depuis Internet. Accès uniquement via jump box avec MFA.
2. **MFA sur tous les comptes Panorama** : appliquer le même niveau d'exigence que pour les firewalls (contrôle 2.1). Aucun compte sans MFA ne doit exister.
3. **RBAC granulaire par Device Group** : limiter les droits de chaque administrateur aux firewalls dont il est responsable. Interdire les droits Super Admin non justifiés.
4. **Panorama HA** : déployer une paire M-Series en Active/Passive pour garantir la continuité de la gestion. Un Panorama unique est un SPOF critique.
5. **Log Collectors redondants** : configurer au moins deux Log Collectors avec une rétention ≥ 90 jours. Les logs Panorama sont essentiels pour les investigations forensiques.
6. **Certificats valides** : remplacer le certificat auto-signé par un certificat CA interne. TLS 1.2 minimum.

7. **Alertes SIEM sur commits Panorama** : chaque commit Panorama (push de configuration sur les firewalls) doit générer une alerte SIEM. Un commit hors fenêtre de maintenance planifiée est un indicateur de compromission immédiat.
8. **Restreindre les Permitted IP Addresses** sur l'interface de gestion Panorama : uniquement les jump boxes et bastions d'administration autorisés.
9. **Vérification régulière des appareils connectés** : `show devices all` doit correspondre exactement à l'inventaire des firewalls autorisés — tout appareil inconnu est une anomalie critique.
10. **Mettre à jour Panorama** : appliquer les mêmes politiques de patching que pour PAN-OS (contrôle 1.1) — les vulnérabilités PAN-OS s'appliquent également à Panorama.

Valeur par défaut : Panorama est livré avec un compte `admin` par défaut, sans MFA, sans restriction d'IP, sans HA. Doit être durci avant mise en production.

Critère de conformité : Interface de gestion Panorama inaccessible depuis Internet. MFA actif sur 100% des comptes Panorama. RBAC par Device Group configuré. Panorama HA Active/Passive configuré. Deux Log Collectors redondants. Certificat TLS signé par CA interne. Alertes SIEM configurées sur les commits Panorama et les connexions admin. Permitted IP Addresses restreints aux jump boxes autorisés. `show devices all` = inventaire certifié.

Réponse à incident

Indicateurs de compromission (IoC) spécifiques Palo Alto

INDICATEUR	SIGNIFICATION	ACTION IMMÉDIATE
Trafic entrant sur ports 6081 ou 6082 depuis la zone untrust (CVE-2026-0300)	Tentative d'exploitation du buffer overflow Captive Portal — RCE potentielle sans auth	Bloquer immédiatement les ports 6081/6082 en entrée, désactiver Response Pages, vérifier si exploitation réussie (sessions root anormales), contacter Palo Alto PSIRT
Connexions sortantes inattendues depuis le firewall vers des IP externes inconnues (post-CVE-2026-0300)	Potentielle RCE réussie — malware EarthWorm ou ReverseSocks5 actif	Isoler le firewall, investigation forensique, patch CVE-2026-0300 en urgence, contacter PSIRT
Activité d'énumération AD depuis l'IP du firewall (logs AD / SIEM)	Post-exploitation CVE-2026-0300 — accès root sur le firewall, reconnaissance AD en cours	Isoler le firewall, bloquer les connexions sortantes, forensique complète, notification DPO si données personnelles
Connexions admin hors plage horaire (logs System)	Accès non autorisé ou credential volé	Bloquer IP source, révoquer session, notification RSSI
Modification de politique non planifiée (logs Config)	Manipulation de configuration — accès compromis	Restaurer sauvegarde, audit complet des changements, investigation forensique
Alerte GlobalProtect depuis IP hors pays d'exploitation	Connexion VPN depuis localisation suspecte	Bloquer le compte, forcer re-auth MFA, vérifier les activités récentes

INDICATEUR	SIGNIFICATION	ACTION IMMÉDIATE
Trafic vers IP sinkhole User-ID (logs Threat)	Hôte interne infecté tentant de contacter un C2	Isoler l'hôte, analyse malware, scan antivirus complet
Tentatives de connexion admin multiples échouées	Attaque brute force en cours	Bloquer IP source, vérifier verrouillage compte actif, alerter SOC
Pic de trafic DNS inhabituel vers domaines aléatoires	DNS tunneling / exfiltration via DNS	Analyser les requêtes DNS, activer capture réseau, contacter équipe réponse incidents
Logs WildFire : verdict malveillant sur un fichier	Fichier malveillant téléchargé par un utilisateur	Isoler le poste utilisateur, bloquer le hash dans la politique, notifier endpoint
Modification des règles NAT publiées (logs Config)	Potentielle porte dérobée réseau créée	Restaurer la configuration, audit complet, notification d'incident
Accès à l'interface de gestion depuis la zone untrust	Configuration incorrecte ou attaque active	Vérifier les règles de gestion, bloquer immédiatement, analyser les logs
Hausse soudaine CPU DP > 90% sans trafic légitime justifiant	Attaque DDoS ou exploitation en cours (T1498)	Activer Zone Protection, rate limiting, contacter l'opérateur réseau upstream
Nouveau compte admin créé hors procédure (logs Config)	Backdoor post-exploitation — CVE-2024-9474 ou CVE-2025-0108	Désactiver immédiatement le compte, investigation forensique complète, contacter Palo Alto PSIRT
Alerte IMA : binaire non signé détecté	Tentative de modification des binaires PAN-OS (T1601)	Isoler le firewall, ne pas redémarrer, contacter Palo Alto PSIRT en urgence
Connexion sortante depuis l'IP de gestion vers IP inconnue	C2 depuis le firewall compromis	Bloquer la connexion, isoler le firewall, investigation forensique, contacter CERT
Requête SNMP depuis IP non autorisée (logs Threat)	Tentative d'énumération de configuration réseau (T1602)	Bloquer l'IP source, vérifier configuration SNMPv3, audit des restrictions d'accès SNMP
Log Threat action = sinkhole depuis hôte interne	Hôte infecté tentant de joindre un domaine C2	Isoler l'hôte immédiatement, analyse forensique, vérifier propagation réseau
Blocage File Blocking sur PE ou archive chiffrée	Tentative de téléchargement d'un malware (Kill Chain étape 5)	Analyser la source, vérifier l'hôte demandeur, alerter l'équipe endpoint
Blocage unknown-tcp/ unknown-udp dans les logs Traffic	Tentative de C2 via protocole inconnu (Kill Chain étape 6)	Analyser la destination, bloquer l'IP, vérifier l'hôte source
Hits sur règle Geo-IP blocage depuis pays à haut risque	Tentative de connexion depuis zone géographique interdite	Analyser la nature du trafic, vérifier si VPN utilisé comme rebond
Commit Panorama hors fenêtre de maintenance planifiée (logs Panorama / SIEM)	Modification de configuration non autorisée sur l'ensemble du parc — possible compromission Panorama (T1199)	Bloquer l'accès Panorama, auditer tous les changements depuis le dernier commit légitime, vérifier les comptes admin Panorama

INDICATEUR	SIGNIFICATION	ACTION IMMÉDIATE
Hits logs Data Filtering sur patterns CB/SSN/IBAN en direction upload	Exfiltration de données sensibles — incident PCI-DSS ou RGPD potentiel	Bloquer la session, identifier le poste source, alerter DPO/RSSI, initier la procédure de notification d'incident réglementaire
Nouvel équipement inconnu dans `show devices all` sur Panorama	Firewall non autorisé connecté à Panorama — vecteur d'intrusion possible (T1199)	Déconnecter l'équipement inconnu, auditer les Device Groups, vérifier les certificats d'authentification Panorama
Basculement HA non planifié (`show high-availability transitions` augmente hors maintenance)	Attaque de disponibilité, défaillance réseau, ou manipulation des liens HA (T1499)	Analyser les logs système HA, vérifier la stabilité des interfaces de monitoring, vérifier l'absence d'injection de paquets HA
Désynchronisation HA persistante (`show high-availability state-synchronization` = Not Synchronized)	Configuration ou session hors-sync : le passif ne peut pas prendre le relais correctement	Forcer la synchronisation, vérifier les liens HA2, investiguer la cause de la désynchronisation
Certificat expiré sur l'interface de gestion ou le portail VPN (alerte navigateur ou échec TLS client)	Absence de monitoring du cycle de vie des certificats — risque MITM si les utilisateurs ignorent les alertes	Renouveler immédiatement le certificat, enquêter sur les accès pendant la période d'expiration
Accès API REST/XML depuis une IP non autorisée (logs System subtype=api depuis IP hors whitelist)	Clé API volée ou exposée — accès admin sans MFA depuis une source non contrôlée (T1078.003)	Invalider immédiatement la clé API compromise, auditer les opérations effectuées, vérifier les configurations modifiées

Procédure d'isolation d'urgence

```
# 1. Capturer l'état courant (avant toute modification)
show running security-policy
show running nat-policy
show system info
show high-availability state
show admins

# 2. Exporter les logs d'audit des configurations récentes
show config audit diff
show log config direction equal backward

# 3. Identifier les sessions suspectes actives
show session all filter source <IP-suspecte>
show session all filter destination <IP-suspecte>
show user ip-user-mapping ip <IP-suspecte>

# 4. Bloquer une IP source suspecte en urgence
# Via création de règle deny en tête de politique ou via EDL dynamique
set config devices entry[name='localhost.localdomain'] vsys entry[name='vsys1'] address
entry[name='BLOCK-IP'] ip-netmask <IP-SUSPECTE>/32

# 5. Révoquer toutes les sessions admin actives si compromission confirmée
clear session all filter type management

# 6. Forcer la déconnexion des tunnels VPN suspects
clear global-protect-gateway current-user name <username>

# 7. Extraire les logs pour investigation forensique
tftp export log traffic start-time equal <AAAA/MM/JJ@HH:MM:SS> end-time equal <AAAA/MM/
JJ@HH:MM:SS> to <IP-TFTP>
tftp export log threat start-time equal <AAAA/MM/JJ@HH:MM:SS> end-time equal <AAAA/MM/
JJ@HH:MM:SS> to <IP-TFTP>

# 8. Vérifier l'intégrité du système (IMA)
show system software status
request system software verify
show system ima-status

# 9. En cas de compromission avérée : isoler le firewall
# Désactiver les interfaces non essentielles et contacter Palo Alto PSIRT
```

Commandes forensiques avancées

Requêtes de threat hunting et d'investigation post-incident à exécuter depuis la CLI PAN-OS ou via SSH sur l'interface de gestion. Ces commandes sont non-intrusives (lecture seule) et peuvent être exécutées en production sans risque d'interruption de service.

```
# Identifier les connexions sortantes anormales depuis le firewall lui-même
show routing fib | match "0.0.0.0"
debug dataplane packet-diag set filter match source <firewall-mgmt-ip>

# Lister toutes les sessions actives vers des IPs suspectes
show session all filter source <suspicious-ip>
show session all filter destination <suspicious-ip>

# Vérifier les comptes administrateurs actifs et leurs permissions
show admins
show admin-locks

# Auditer les règles modifiées récemment
show config diff running candidate
show log system direction equal forward subtype equal config

# Identifier le trafic vers les ports 6081/6082 (CVE-2026-0300)
show session all filter destination-port 6081
show session all filter destination-port 6082

# Vérifier l'état IMA (intégrité des binaires)
show system ima-status

# Analyser les logs WildFire pour des fichiers malveillants récents
show wildfire statistics
show log wildfire direction equal forward

# Vérifier les certificats expirés ou proches de l'expiration
show certificate domain all | match "days"

# Contrôler l'état HA
show high-availability state
show high-availability state-synchronization

# Surveiller les accès API non autorisés
show log system direction equal forward subtype equal general | match "api"
```

Plan de réponse aux incidents — niveaux d'escalade

NIVEAU	DÉCLENCHEUR	RESPONSABLE	DÉLAI DE RÉPONSE
P1 — CRITIQUE	Compromission confirmée du firewall, backdoor détecté, alerte IMA, log sinkhole C2 actif, exploitation CVE-2026-0300 suspectée (trafic ports 6081/6082 entrant depuis Internet)	RSSI + CERT interne + Palo Alto PSIRT	15 minutes
P2 — ÉLEVÉ	Credential admin compromis, règle malveillante détectée,	RSSI + Équipe réseau sécurité	1 heure

NIVEAU	DÉCLENCHEUR	RESPONSABLE	DÉLAI DE RÉPONSE
	CVE-2025-0108 ou CVE-2024-9474 ou CVE-2026-0300 exploité, blocage PE malveillant répété, malware EarthWorm/ ReverseSocks5 détecté		
P3 — MOYEN	Hôte infecté détecté via sinkhole, WildFire alerte, connexion sortante anormale du firewall, hit File Blocking sur archive chiffrée	SOC L2 + Équipe endpoint	4 heures
P4 — FAIBLE	Tentative brute force bloquée, scan SNMP depuis IP non autorisée, scan de reconnaissance détecté (Zone Protection hit), blocage Geo-IP, basculement HA non planifié, alerte expiration certificat < 30 jours, accès API depuis IP non whitelistée	SOC L1	24 heures

Références

- Palo Alto Networks PSIRT — Avis de sécurité
- CIS Benchmark for Palo Alto Firewall 11 v1.2.0
- MITRE ATT&CK — Network Devices Matrix
- ANSSI — Recommandations de sécurité pour les pare-feux de nouvelle génération
- CISA Known Exploited Vulnerabilities — Palo Alto
- CISA Hardening Guidance for Network Devices
- NIST SP 800-41 Rev. 1 — Guidelines on Firewalls and Firewall Policy
- Palo Alto Networks — PAN-OS 11.x Administrator’s Guide
- Palo Alto Networks — Best Practice Assessment (BPA)
- Palo Alto Networks — Best Practices Guide
- Palo Alto Networks — Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions
- Palo Alto Networks — AIOps for NGFW
- CERT-EU — Security Guidance for Palo Alto
- CVE-2026-0300 — PAN-OS User-ID Authentication Portal Buffer Overflow RCE (CVSS 9.3, CISA KEV, exploitation active avril-mai 2026)
- Palo Alto Unit 42 Threat Brief — CVE-2026-0300 Active Exploitation Analysis

- CERT-EU Advisory — CVE-2026-0300 Palo Alto NGFW Zero-Day Authentication Portal
- CVE-2024-3400 — GlobalProtect RCE (CVSS 10.0, CISA KEV)
- CVE-2025-0108 — PAN-OS Management Interface Authentication Bypass
- CVE-2024-9474 — PAN-OS Privilege Escalation via Management Interface
- RFC 8784 — Mixing Preshared Keys in IKEv2 for Post-quantum Security
- RFC 9242 — Intermediate Exchange in IKEv2
- RFC 9370 — Multiple Key Exchanges in IKEv2
- NIST SP 800-208 — Recommendation for Stateful Hash-Based Signature Schemes
- Palo Alto Networks — Panorama Administrator's Guide
- Palo Alto Networks — User-ID Technology Overview and Best Practices
- Palo Alto Networks — Zero Trust Architecture with NGFW
- Palo Alto Networks — Data Loss Prevention (DLP) Best Practices
- Palo Alto Networks — High Availability Administrator's Guide
- Palo Alto Networks — Certificate Management Guide
- Palo Alto Networks — XML API Usage Guide
- Palo Alto Networks — REST API Reference
- RFC 8894 — Simple Certificate Enrollment Protocol (SCEP)
- NIST SP 800-57 — Recommendation for Key Management
- DORA — Règlement (UE) 2022/2554 — Digital Operational Resilience Act (Art. 9 : ICT Risk Management, Art. 10 : Continuité, Art. 11 : Réponse et Rétablissement) — En vigueur depuis le 17 janvier 2025
- NIS2 — Directive (UE) 2022/2555 — Art. 21 : Mesures de gestion des risques de cybersécurité (durcissement firewall, gestion des incidents, continuité d'activité)

ANNEXE — Checklists de vérification rapide

Checklists condensées pour audit terrain et conformité. Chaque ligne = un contrôle actionnable.
Légende : ☐ = à vérifier | ✅ = conforme | ❌ = non conforme | N/A = non applicable

Domaine 1 — Firmware et mises à jour

#	CONTRÔLE	NIVEAU	STATUT
1.1	PAN-OS dans un train de maintenance supporté, patch < 30 jours pour CVSS ≥ 9.0	🔴 CRITIQUE	☐
1.2	Sauvegardes automatiques ≤ 24h, stockage hors-bande chiffré, test restauration < 90 jours	🟢 L1	☐

#	CONTRÔLE	NIVEAU	STATUT
1.3	Signatures Antivirus < 25h, Applications & Threats < 8 jours, WildFire < 1h	🟢 L1	☐
1.4	En HA : même version PAN-OS sur les deux membres, statut synchronized	🟢 L1	☐
1.5	IMA en mode Enforcing (`show system ima-status`), Secure Boot activé sur plateformes matérielles	🔴 CRITIQUE	☐

Domaine 2 — Authentification et accès administrateur

#	CONTRÔLE	NIVEAU	STATUT
2.1	MFA actif sur 100% des comptes admin (RADIUS, SAML, ou OTP)	🔴 CRITIQUE	☐
2.2	Complexity activée : longueur ≥ 12, 1 majuscule, 1 minuscule, 1 chiffre, 1 spécial	🟢 L1	☐
2.3	Verrouillage après ≤ 5 tentatives échouées, durée ≥ 30 minutes	🟢 L1	☐
2.4	Idle Timeout ≤ 10 minutes configuré globalement	🟢 L1	☐
2.5	Compte admin par défaut désactivé, comptes nominatifs avec RBAC minimal	🔴 CRITIQUE	☐
2.6	Authentification SSH par certificat configurée pour les admins CLI	🔵 L2	☐

Domaine 3 — Interface de gestion

#	CONTRÔLE	NIVEAU	STATUT
3.1	Permitted IP Addresses configuré sur interface mgmt et tous les profils Interface Mgmt — interface non accessible depuis untrust/ Internet	🔴 CRITIQUE	☐
3.2	HTTP et Telnet désactivés sur interface mgmt et tous les profils	🔴 CRITIQUE	☐
3.3	Si SNMP : SNMPv3 authPriv uniquement, SNMPv1/v2c	🟠 ÉLEVÉ	☐

#	CONTRÔLE	NIVEAU	STATUT
	désactivés, restriction IP source (anti-T1602)		
3.4	TLS 1.2 minimum pour HTTPS, certificat signé par CA de confiance, anti-downgrade (anti-T1600)	🟠 ÉLEVÉ	☐
3.5	Bannière légale configurée	🟢 L1	☐
3.6	API REST/XML : compte de service dédié par application, clés rotées tous les 90 jours, restriction IP source via Local-in Policy, API désactivée si inutilisée, alertes SIEM sur accès anormaux	🟠 ÉLEVÉ	☐

Domaine 4 — Zones et politiques de sécurité

#	CONTRÔLE	NIVEAU	STATUT
4.1	Règle deny explicite en dernière position avec logging. Intrazone-default = deny avec log	🔴 CRITIQUE	☐
4.2	Aucune règle allow avec Service = any sur flux Internet-facing, règles de blocage en tête de rulebase	🟠 ÉLEVÉ	☐
4.3	Security Profile Group (AV + AS + VP + URLFilter + WF) attaché à 100% des règles allow	🟠 ÉLEVÉ	☐
4.4	External Dynamic Lists (EDL) configurées et mises à jour toutes les heures	🟠 ÉLEVÉ	☐
4.5	Policy Optimizer utilisé — aucune règle “No App Specified” sur flux Internet-facing, BPA < 90 jours	🟡 MOYEN	☐
4.6	DoS Protection Profiles configurés pour serveurs DMZ, alertes SIEM sur dépassement de seuil	🟠 ÉLEVÉ	☐
4.7	Kill Chain Étape 1 — Zone Protection Reconnaissance Protection activée (TCP/UDP Port Scan + Host Sweep = block-ip), exception scanners internes = alert, blocage Geo-IP pays à haut risque	🟠 ÉLEVÉ	☐

Domaine 5 — App-ID et User-ID

#	CONTRÔLE	NIVEAU	STATUT
5.1	Aucune règle allow avec Application = any sur flux Internet-facing	🟠 ÉLEVÉ	☐
5.2	User-ID activé uniquement sur interfaces trust internes, Include/ Exclude Networks configurés	🟢 L1	☐
5.3	WMI Probing désactivé	🟢 L1	☐
5.4	Compte de service User-ID Agent avec droits minimaux, connexion interactive désactivée	🟢 L1	☐
5.5	Règle de blocage explicite pour unknown-tcp, unknown-udp, unknown-p2p — logging activé et alerte SIEM configurée	🟠 ÉLEVÉ	☐
5.6	**CVE-2026-0300** — PAN-OS patché vers version corrigée OU Response Pages désactivées sur tous les profils Interface Mgmt des interfaces WAN/untrust. Captive Portal restreint aux zones internes ou désactivé. Threat ID 510019 activé si PAN-OS 11.1+ non patché	🔴 CRITIQUE	☐
5.7	Durcissement User-ID avancé : WMI Probing désactivé en haute sécurité, Include Networks = postes utilisateurs uniquement, Exclude Networks = DC/SIEM/DMZ/invités, Captive Portal restreint aux zones internes	🟠 ÉLEVÉ	☐

Domaine 6 — Threat Prevention et WildFire

#	CONTRÔLE	NIVEAU	STATUT
6.1	Profil Antivirus best-practice : reset-both sur FTP/HTTP/HTTP2/SMB/ SMTP dans WildFire Signature ET WildFire Inline ML, real-time lookup activé	🟠 ÉLEVÉ	☐
6.2	Profil Anti-Spyware best-practice : block-ip sur Critical, reset-both sur High/Medium, DNS Sinkholing actif sur 6 catégories de domaines, DNS	🟠 ÉLEVÉ	☐

#	CONTRÔLE	NIVEAU	STATUT
	uniquement vers serveurs sanctionnés		
6.3	Profil Vulnerability Protection best-practice : reset-both sur Critical/ High, single-packet PCAP, Inline Cloud Analysis = reset-both	🟠 ÉLEVÉ	☐
6.4	Profil WildFire best-practice : tous fichiers, direction both, Advanced WildFire temps réel, alertes configurées, exclusions documentées	🟠 ÉLEVÉ	☐
6.5	Profil URL Filtering best-practice : 7 catégories malveillantes + 8 haut-risque bloquées, Log Container Page Only = désactivé, Safe Search = activé, credential submission = block	🟢 L1	☐
6.6	Zone Protection Profile avec SYN Cookies, flood protection et reconnaissance protection sur zone untrust	🟠 ÉLEVÉ	☐
6.7	Kill Chain Étape 5 — Profil File Blocking : PE/DLL/HTA/LNK/ encrypted-zip/encrypted-rar bloqués dans les deux directions, exceptions Windows Update documentées	🟠 ÉLEVÉ	☐
6.8	Kill Chain Étape 6 — DNS Sinkholing pas-à-pas configuré : default-paloalto-dns source, PCAP activé, Log at Session Start, alerte SIEM P1 sur action = sinkhole	🟠 ÉLEVÉ	☐
6.9	Security Profile Groups “best-practice” et “default” créés, attachés à 100% des règles allow, vérification automatisée via BPA/ AIOps	🟠 ÉLEVÉ	☐
6.10	Profil Data Filtering (DLP) configuré avec patterns CB/SSN/IBAN et marqueurs internes personnalisés. Attaché au Security Profile Group best-practice. Alertes SIEM sur hits DLP. Procédure SOC documentée	🟠 ÉLEVÉ	☐

Domaine 7 — VPN et accès distant (GlobalProtect)

#	CONTRÔLE	NIVEAU	STATUT
7.1	IKEv2 uniquement, AES-256 minimum, SHA-256 minimum, PFS DH groupe ≥ 14	🟠 ÉLEVÉ	☐
7.2	GlobalProtect avec MFA obligatoire, profil HIP configuré avec AV + chiffrement disque	🟠 ÉLEVÉ	☐
7.3	Certificat TLS GlobalProtect signé par CA de confiance, validité > 30 jours	🟢 L1	☐
7.4	PAN-OS 11.1+ et environnements sensibles : PPK RFC 8784 activé en mode Mandatory, AES-256-GCM, PPK distribuée hors-bande	🔵 L2	☐

Domaine 8 — Décryptage SSL/TLS et gestion des certificats

#	CONTRÔLE	NIVEAU	STATUT
8.1	SSL Forward Proxy actif pour trafic Internet sortant, CA de décryptage distribuée	🟡 MOYEN	☐
8.2	SSL Inbound Inspection configurée pour serveurs DMZ exposés en HTTPS	🟡 MOYEN	☐
8.3	Exclusions de décryptage documentées, minimales, revue trimestrielle	🟢 L1	☐
8.4	Certificat de gestion HTTPS signé par CA interne (non auto-signé). CA SSL Inspection dédiée. OCSP/CRL configuré ≤ 24h. Alertes expiration ≥ 60 jours. SCEP si infrastructure disponible. Inventaire certif. documenté	🟢 L1	☐

Domaine 9 — Segmentation, NAT et Haute Disponibilité

#	CONTRÔLE	NIVEAU	STATUT
9.1	Minimum 3 zones distinctes (untrust/trust/DMZ), management isolé	🟢 L1	☐

#	CONTRÔLE	NIVEAU	STATUT
9.2	Règles NAT documentées, aucun any-source non justifié, revue trimestrielle	🟢 L1	☐
9.3	Intrazone-default avec logging. Zones sensibles : intrazone-default = deny	🔵 L2	☐
9.4	Zero Trust : < 5% de règles any sur flux inter-zones, zones granulaires par charge de travail (web/app/db/ users/mgmt/IoT), User-ID sur règles sensibles, flux DB→users = Deny, score BPA Zero Trust documenté	🔵 L2	☐
9.5	HA : chiffrement HA1 et HA2 activés, HA Group Password configuré, Pre-emption désactivé, Link/Path Monitoring configurés, interfaces HA dédiées, test de basculement < 90 jours, alertes SIEM sur transitions HA	🟠 ÉLEVÉ	☐

Domaine 10 — Journalisation et supervision SIEM

#	CONTRÔLE	NIVEAU	STATUT
10.1	Profil Syslog configuré, tous types de logs système (System, Config, User-ID, HIP, IP-Tag) transmis	🟢 L1	☐
10.2	Log Forwarding Profile attaché à 100% des règles de sécurité, Log at Session End actif	🟢 L1	☐
10.3	Si SNMP traps : SNMPv3 authPriv, traps sur événements Critical et High	🔵 L2	☐
10.4	Rétention logs ≥ 90 jours en ligne, archive ≥ 12 mois si PCI-DSS/NIS2	🟢 L1	☐
10.5	Log on High DP Load = Enabled	⚪ INFO	☐
10.6	Alertes SIEM CISA configurées : auth failures, changements comptes, connexions sortantes anormales	🟠 ÉLEVÉ	☐
10.7	Panorama sur VLAN dédié isolé, inaccessible depuis Internet. MFA sur 100% des comptes Panorama. RBAC par Device Group. HA	🔴 CRITIQUE	☐

#	CONTRÔLE	NIVEAU	STATUT
	Active/Passive. Deux Log Collectors redondants. Alertes SIEM sur commits Panorama hors maintenance		

Mapping de conformité — Référentiels

Ce tableau croise les contrôles Palo Alto NGFW avec les référentiels réglementaires et normatifs applicables : CIS Controls v8, NIS2 (Art. 21), ISO 27001:2022, PCI DSS v4, RGPD (Art. 32) et DORA (Art. 9, en vigueur depuis le 17 janvier 2025 pour les entités financières). Une coche (✓) indique que le contrôle contribue directement à la conformité du référentiel concerné.

CONTRÔLE PALO ALTO	CIS CONTROLS V8	NIS2 ART.21	ISO 27001:2022	PCI DSS V4	RGPD ART.32	DORA ART.9
Mise à jour PAN-OS (1.1)	CIS 7.3	✓	A.8.8	Req 6.3.3	✓	✓
IMA/Secure Boot (1.5)	CIS 4.1	✓	A.8.9	Req 2.2	✓	✓
Sauvegardes config (1.2)	CIS 11.2	✓	A.12.3.1	Req 12.3	✓	✓
Suppression admin défaut (2.5)	CIS 5.3	✓	A.9.2.3	Req 8.2.2	✓	✓
MFA administrateurs (2.1)	CIS 6.3	✓	A.9.4.2	Req 8.4.2	✓	✓
Politique mots de passe (2.2)	CIS 5.2	✓	A.9.4.3	Req 8.3.6	✓	✓
Idle timeout ≤10min (2.4)	CIS 4.3	✓	A.9.4.2	Req 8.2.8	✓	✓
RBAC et rôles admin (2.5/2.6)	CIS 6.8	✓	A.9.1.2	Req 7.2	✓	✓
Restriction IP management (3.1)	CIS 12.2	✓	A.8.15	Req 1.3.2	✓	✓
SNMPv3 uniquement (3.3)	CIS 12.3	✓	A.8.21	Req 2.2.1	✓	✓
Gestion API REST/XML (3.6)	CIS 4.1	✓	A.9.4.1	Req 8.6	✓	✓
CVE-2026-0300 mitigation (5.6)	CIS 7.3	✓	A.8.8	Req 6.3.3	✓	✓

CONTRÔLE PALO ALTO	CIS CONTROLS V8	NIS2 ART.21	ISO 27001:2022	PCI DSS V4	RGPD ART.32	DORA ART.9
App-ID (0 règle port-based) (5.1)	CIS 12.4	✓	A.8.23	Req 1.2.1	✓	✓
User-ID hardening (5.2/5.7)	CIS 6.1	✓	A.9.1.1	Req 8.2.1	✓	✓
Zone Protection / DoS (4.6/6.6)	CIS 13.4	✓	A.8.16	Req 6.4.2	✓	✓
Profil Anti-Virus (6.1)	CIS 10.1	✓	A.8.7	Req 5.2.1	✓	✓
Profil Anti-Spyware + DNS Sinkhole (6.2/6.8)	CIS 9.2	✓	A.8.16	Req 6.4.1	✓	✓
WildFire (tous fichiers) (6.4)	CIS 10.6	✓	A.8.7	Req 5.2.3	✓	✓
URL Filtering (6.5)	CIS 9.3	✓	A.8.23	Req 6.4.1	✓	✓
File Blocking profile (6.7)	CIS 10.2	✓	A.8.7	Req 5.2.1	✓	✓
DLP Data Filtering (6.10)	CIS 3.13	✓	A.8.12	Req 3.4.1	✓	✓
GlobalProtect VPN IKEv2 (7.1/7.2)	CIS 12.6	✓	A.8.24	Req 4.2.1	✓	✓
VPN Post-Quantique RFC 8784 (7.4)	CIS 12.6	✓	A.8.24	Req 4.2.1	✓	✓
SSL Forward Proxy (8.1)	CIS 13.10	✓	A.8.16	Req 4.2.1	✓	✓
Segmentation Zero Trust (9.4)	CIS 12.2	✓	A.8.22	Req 1.3.1	✓	✓
Syslog vers SIEM (10.1/10.2)	CIS 8.2	✓	A.8.15	Req 10.2	✓	✓
Panorama hardening (10.7)	CIS 4.6	✓	A.8.15	Req 10.3	✓	✓
HA hardening (9.5)	CIS 11.3	✓	A.17.2.1	Req 12.4	✓	✓
Gestion certificats PKI (8.4)	CIS 16.3	✓	A.8.24	Req 4.2.1	✓	✓

Note DORA : *Le règlement DORA (Digital Operational Resilience Act, Règlement UE 2022/2554) est applicable depuis le 17 janvier 2025 aux entités financières (banques, assurances, sociétés d'investissement, infrastructures de marché). L'Art. 9 couvre le cadre de gestion du risque TIC — le durcissement du firewall en est une exigence centrale. L'Art. 10 couvre la continuité (HA hardening) et l'Art. 11 les plans de réponse et rétablissement (section Réponse à incident ci-dessus).*

Note NIS2 : *La directive NIS2 (Directive UE 2022/2555, Art. 21) impose des mesures techniques et organisationnelles proportionnées au risque, notamment : gestion des incidents, continuité d'activité, sécurité de la chaîne d'approvisionnement, sécurité des réseaux et des systèmes d'information. Les contrôles de ce guide couvrent l'ensemble des exigences techniques Art. 21.*

Tableau récapitulatif par domaine

DOMAINE	CONTRÔLES	CRITIQUE	ÉLEVÉ	MOYEN	L1	L2	INFO
D1 — Firmware + IMA	5	2	0	0	3	0	0
D2 — Auth	6	2	0	0	3	1	0
D3 — Interface mgmt + API	6	2	3	0	1	0	0
D4 — Zones/Politiques	7	1	5	1	0	0	0
D5 — App-ID/User-ID + CVE-2026-0300	7	1	3	0	3	0	0
D6 — Threat/WildFire/Kill Chain/ DLP	10	0	9	0	1	0	0
D7 — VPN + Post-Quantum	4	0	2	0	1	1	0
D8 — SSL/TLS + Certificats PKI	4	0	0	2	2	0	0
D9 — Segmentation + Zero Trust + HA	5	0	1	0	2	2	0
D10 — Logs/SIEM/CISA + Panorama	7	1	1	0	3	1	1
TOTAL	**61**	**9**	**24**	**3**	**19**	**5**	**1**

> ***Version 4.1 — Mai 2026.*** *Le compte ITEMS = 84 dans les métadonnées inclut les contrôles numérotés (61 entrées dans les checklists annexe) plus les sous-contrôles et enrichissements significatifs des contrôles existants. Ajouts de cette cinquième version (4.1) : mapping de conformité multi-référentiels (CIS Controls v8 / NIS2 Art.21 / ISO 27001:2022 / PCI DSS v4 / RGPD Art.32 / DORA Art.9) pour 29 contrôles clés, ajout des références réglementaires DORA (Règlement UE 2022/2554, en vigueur 17 janvier 2025) et NIS2 (Directive UE 2022/2555), enrichissement de la section Réponse à incident avec des commandes forensiques avancées de threat hunting (CVE-2026-0300, IMA, WildFire, HA, API). Ajouts de la version 4.0 : durcissement HA (9.5 — chiffrement HA1/HA2, authentification group, pre-emption, tests basculement), gestion des certificats et PKI (8.4 — CA dédiée SSL Inspection, OCSP/CRL, SCEP renouvellement automatique, alertes expiration), durcissement API REST/XML PAN-OS (3.6 — clés API par application, rotation trimestrielle, restriction IP, désactivation si inutilisée), et enrichissement de D1 avec la vérification de signature IMA des mises à jour PAN-OS (hash SHA-256, anti-rollback). Ajouts de la version 3.0 : CVE-2026-0300 (5.6), User-ID hardening avancé (5.7), Data Filtering/DLP (6.10), Zero Trust architecture (9.4), Panorama hardening (10.7), et enrichissement de l'introduction D6 avec le déploiement phasé Threat Prevention.*

Document généré par AYI NEDJIMI CONSULTANTS — https://ayinedjimi-consultants.fr Basé sur : CIS Palo Alto Firewall 11 Benchmark v1.2.0 (10-03-2025) Sources additionnelles : CISA Hardening Guidance, Palo Alto PSIRT, Palo Alto Unit 42 Threat Brief CVE-2026-0300, CERT-EU Advisory CVE-2026-0300, Palo Alto Best Practices, RFC 8784/9242/9370, RFC 8894 (SCEP), MITRE ATT&CK v15, Palo Alto Kill Chain Controls, Palo Alto Best Practices for L4/L7 Evasions, Palo Alto Panorama Administrator's Guide, Palo Alto Zero Trust Architecture Guide, Palo Alto HA Administrator's Guide, Palo Alto Certificate Management Guide, Palo Alto XML/REST API Documentation, NIST SP 800-57 Applicable : PAN-OS 10.x, 11.x, 12.x — PA-Series, VM-Series Dernière mise à jour : Mai 2026 — Version 4.0