BENCHMARK DE DURCISSEMENT SOPHOS FIREWALL SFOS v22 — 2026

🔐 AYI NEDJIMI CONSULTANTS (ANC)

Version : 1.5 — Mai 2026 **Applicabilité :** Sophos Firewall XGS-Series, XG-Series, Virtual — SFOS v22 **Classification :** CONFIDENTIEL **Auteur :** AYI NEDJIMI Consultants — https://ayinedjimi-consultants.fr **Source :** CIS Sophos Firewall v22 Benchmark v1.0.0 (25 mars 2026) + Sophos Health Check v22 (32 vérifications CIS-alignées) + Architecture Xstream v2 (décembre 2025) + NDR Essentials v22 + XML API Security + Sophos Central Integration Hardening + ZTNA intégré SFOS v22 + Active Threat Response MDR/XDR + ANSSI + HA Hardening Active-Passive + Certificate Lifecycle Management + Syslog over TLS + Wireless WIDS/Rogue AP + DoS Flood Advanced + CIS Controls v8 / NIS2 / ISO 27001:2022 / RGPD / PCI DSS v4 Mapping + **DORA (Règlement UE 2022/2554) — Art. 9, 10, 11, 16 — effectif 17 janvier 2025**

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

Top 10 Quick Wins — 80% du risque en priorité

> *Ces 10 actions couvrent la majorité des vecteurs d'attaque documentés sur les pare-feux Sophos exposés. Commencer ici.*

#	ACTION	DOMAINE	IMPACT	EFFORT
1	Désactiver l'accès HTTPS/SSH depuis la zone WAN	D3	🔴 CRITIQUE	Faible
2	Activer MFA pour la console web admin et le VPN distant	D2	🔴 CRITIQUE	Moyen
3	Activer MFA pour le compte admin par défaut	D2	🔴 CRITIQUE	Faible
4	Mettre à jour les patterns toutes les 15 minutes	D1	🟠 ÉLEVÉ	Faible
5	Activer les hotfixes automatiques	D1	🟠 ÉLEVÉ	Faible
6	Configurer le timeout de session admin à ≤10 min	D2	🟠 ÉLEVÉ	Faible
7	Bloquer après 5 tentatives d'authentification échouées	D2	🟠 ÉLEVÉ	Faible
8	Activer Sophos X-Ops Threat Intelligence	D6	🟠 ÉLEVÉ	Faible

#	ACTION	DOMAINE	IMPACT	EFFORT
9	Configurer syslog vers un SIEM externe	D10	🟡 MOYEN	Moyen
10	Bloquer SMB (445) et RDP (3389) depuis WAN	D4	🟡 MOYEN	Faible

Domaine 1 — Configuration initiale et mise à jour du système

Objectif : *Maintenir SFOS et ses bases de signatures à jour, assurer la résilience opérationnelle via les sauvegardes et la haute disponibilité, garantir que le système est correctement identifié dans l'infrastructure, et valider l'intégrité du noyau et du système grâce aux protections matérielles et au capteur XDR.*

Contrôle 1.1 — Mises à jour des patterns toutes les 15 minutes

CIS Ref : *3.2* | ***MITRE :*** *T1190, T1203* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les patterns de protection (signatures AV, IPS, X-Ops, GeoIP, applications) sont la première ligne de défense contre les menaces connues. Un intervalle de mise à jour de 2 heures (valeur par défaut) laisse une fenêtre d'exposition de près de 24 heures dans un scénario de mise à jour manquée. Les acteurs de la menace exploitent activement les signatures non mises à jour pour contourner la détection antivirale et IPS. En SFOS v22, la base de détection AI/ML anti-malware est mise à jour dans le cloud toutes les 5 minutes ; les patterns locaux doivent être alignés sur ce rythme.

Impact potentiel

- Propagation de malwares dont les signatures sont connues mais pas encore téléchargées
- Bypass IPS sur des exploits récents non couverts par les patterns en place
- Non-détection de nouvelles campagnes de phishing ou de ransomware actives
- Décalage entre la base AI/ML cloud (5 min) et les signatures locales si l'intervalle est trop long

Navigation

```
System > Backup & Firmware > Pattern Updates
→ Pattern download/installation : régler sur "Auto update" = ON
→ Interval : sélectionner "Every 15 minutes"
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Depuis le shell avancé SFOS (SSH > option 5 > Advanced shell)
system diagnostics show version
# Vérifier la date de dernière mise à jour des patterns dans le Dashboard > Overview
```

Remédiation

1. Naviguer vers `System > Backup & Firmware > Pattern Updates`
2. Activer `Auto update` = ON

3. Définir l'intervalle à `Every 15 minutes`
4. Si l'environnement est air-gapped, télécharger manuellement le fichier de patterns depuis le portail Sophos et importer via `Manual pattern update`
5. Vérifier que `Last successful update` indique `Success` après la prochaine plage de mise à jour

Valeur par défaut : Auto update activé, intervalle par défaut = 2 heures.

Critère de conformité : `Auto update` = ON et `Interval` = `Every 15 minutes`. `Last successful update` = `Success`.

Contrôle 1.2 — Hotfixes automatiques activés

> ***CIS Ref :*** *3.3* | ***MITRE :*** *T1190* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les hotfixes Sophos corrigent des vulnérabilités critiques activement exploitées sur le pare-feu sans nécessiter de mise à niveau complète du firmware. Plusieurs incidents majeurs (notamment CVE-2020-12271, CVE-2022-1040) ont été couverts par des hotfixes avant la disponibilité d'une version SFOS complète. Ne pas autoriser l'installation automatique des hotfixes expose l'organisation à des exploits zero-day pendant la fenêtre de correctif manuel.

Impact potentiel

- Exploitation de vulnérabilités critiques sur l'interface de gestion ou le portail utilisateur
- Compromission complète du pare-feu avec accès root potentiel
- Pivotement vers le réseau interne depuis la zone WAN

Navigation

```
System > Backup & Firmware > Firmware
→ Section "Hotfix settings"
→ Cocher "Allow Automatic Installation of hotfixes"
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification via l'Advanced Shell
system diagnostics show version
# Vérifier la liste des hotfixes installés dans System > Backup & Firmware > Firmware
```

Remédiation

1. Naviguer vers `System > Backup & Firmware > Firmware`
2. Dans la section `Hotfix settings`, cocher `Allow Automatic Installation of hotfixes`
3. Valider avec `Apply`
4. Vérifier régulièrement l'historique des hotfixes appliqués
5. Consulter les avis de sécurité Sophos sur https://www.sophos.com/en-us/security-advisories

Valeur par défaut : Non activé par défaut — nécessite une action manuelle.

Critère de conformité : `Allow Automatic Installation of hotfixes` = coché (activé).

Contrôle 1.3 — Sauvegarde de configuration chiffrée et planifiée

> ***CIS Ref :*** *3.4* | ***MITRE :*** *T1490, T1005* | ***Niveau :*** 🟢 *L1*

Description du risque

L'absence de sauvegarde régulière et chiffrée de la configuration SFOS expose l'organisation à une perte totale de la politique de sécurité en cas d'incident matériel, de ransomware, ou d'erreur d'administration. Une sauvegarde non chiffrée contient des secrets (clés pré-partagées VPN, identifiants LDAP) exploitables si elle est compromise.

Impact potentiel

- Indisponibilité prolongée du service réseau (RTO non maîtrisé)
- Perte de la politique de sécurité complète après sinistre
- Exposition des secrets de configuration si la sauvegarde n'est pas chiffrée

Navigation

```
System > Backup & Firmware > Backup & Restore
→ Scheduled backup : activer
→ Frequency : Daily (ou selon politique)
→ Encryption password : définir un mot de passe fort
→ Send to email : renseigner l'adresse de l'administrateur
→ Cliquer sur "Save"
Pour export manuel :
System > Backup & Firmware > Export > Download backup
```

CLI de vérification

```
# Vérification manuelle dans l'interface web
# System > Backup & Firmware > Backup & Restore > Scheduled backup
# Vérifier que "Last backup" est récent (< 24h)
```

Remédiation

1. Configurer une sauvegarde planifiée quotidienne avec chiffrement
2. Définir un mot de passe d'encryption fort (≥16 caractères)
3. Configurer l'envoi par email vers une boîte de réception sécurisée hors-bande
4. Tester la restauration trimestriellement dans un environnement de qualification
5. Stocker les sauvegardes dans un système distant (NAS, S3 chiffré)
6. Activer la synchronisation des sauvegardes vers Sophos Central pour une copie cloud sécurisée

Valeur par défaut : Sauvegarde planifiée non configurée par défaut.

Critère de conformité : Sauvegarde planifiée activée, chiffrée, fréquence ≤ 24h, dernière sauvegarde réussie dans les 24 dernières heures.

Contrôle 1.4 — Hostname défini de manière significative

> ***CIS Ref :*** *1.1.10* | ***MITRE :*** *T1040* | ***Niveau :*** 🟢 *L1*

Description du risque

Un pare-feu sans hostname significatif rend difficile la corrélation des événements dans un SIEM ou un système de supervision. Les logs syslog, les alertes SNMP et les traps peuvent référencer une adresse IP ou un nom générique, rendant le traçage d'incidents plus lent et plus ambigu dans les environnements multi-firewalls.

Impact potentiel

- Confusion dans la corrélation des logs lors d'un incident de sécurité
- Difficulté d'identification de l'équipement source dans les alertes SOC
- Ralentissement de la réponse à incident dans les environnements multi-sites

Navigation

```
Administration > Device Access > Hostname
→ Hostname : saisir un nom significatif (ex : FW-PARIS-EDGE01)
→ Domain name : renseigner le domaine DNS interne
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Depuis l'Advanced Shell (SSH > option 5)
hostname
# ou
get hostname
```

Remédiation

1. Se connecter à la console web Sophos Firewall
2. Naviguer vers `Administration > Device Access > Hostname`
3. Saisir un hostname conforme à la convention de nommage de l'organisation (ex : `FW-SITE-ROLE-NNN`)
4. Via CLI : `set hostname FW-PARIS-EDGE01` depuis l'Advanced Shell
5. Vérifier que le hostname apparaît correctement dans le coin supérieur gauche du Dashboard et dans les logs syslog

Valeur par défaut : Hostname par défaut générique (`sfos`) ou non configuré.

Critère de conformité : Hostname défini, non générique, conforme à la convention de nommage de l'organisation, visible dans les logs syslog.

Contrôle 1.5 — Aucun abonnement expiré

> ***CIS Ref :*** *3.5* | ***MITRE :*** *T1562* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les abonnements Sophos (Network Protection, Web Protection, Email Protection, Enhanced Support, Sandstorm/Zero-Day) conditionnent l'activation des moteurs de détection. Un abonnement expiré désactive silencieusement des couches de protection complètes sans alerte visible pour l'administrateur non averti.

Impact potentiel

- Désactivation de la détection IPS, AV, ou du filtrage web si l'abonnement expire
- Perte de la protection zero-day (Sandstorm) sur les flux entrants
- Non-conformité réglementaire si les SLA de protection sont contractuellement définis

Navigation

```
System > Administration > Licensing
→ Vérifier la colonne "Expiry date" pour chaque module
→ Renouveler les abonnements avant expiration
```

CLI de vérification

```
# Via l'Advanced Shell
system diagnostics show version
# Vérifier les dates d'expiration dans System > Administration > Licensing
```

Remédiation

1. Naviguer vers `System > Administration > Licensing`
2. Identifier les abonnements avec une date d'expiration proche ou dépassée
3. Procéder au renouvellement via le portail Sophos Central ou le revendeur
4. Configurer une alerte de notification (voir contrôle 3.5) à J-30 avant expiration
5. Documenter les dates de renouvellement dans le registre des actifs

Valeur par défaut : Abonnements livrés avec le matériel, expiration variable selon le contrat.

Critère de conformité : Aucun abonnement en statut `Expired`. Tous les modules de protection ont une date d'expiration future.

Contrôle 1.6 — Haute disponibilité (HA) configurée et synchronisée

> ***CIS Ref :*** *3.1* | ***MITRE :*** *T1499* | ***Niveau :*** 🔵 *L2*

Description du risque

Un pare-feu en mode standalone constitue un point de défaillance unique (SPOF) pour l'ensemble du réseau. En cas de panne matérielle ou lors de mises à jour firmware, l'absence de HA entraîne une interruption de service qui peut durer plusieurs heures et ouvrir une fenêtre d'attaque pendant la restauration.

Impact potentiel

- Interruption totale de la connectivité réseau en cas de panne matérielle
- Fenêtre de vulnérabilité lors des mises à jour SFOS sans basculement automatique
- Non-respect des SLA de disponibilité (RTO non maîtrisé)

Navigation

```
Configure > System Services > High Availability > High Availability Status
→ Vérifier HA Status = "Established[Active-Passive]" ou "Established[Active-Active]"
→ Local et Peer ne doivent pas afficher "Standalone" ou "Faulty"
High Availability Configuration > Select ports to be monitored
→ Configurer les interfaces à surveiller
```

CLI de vérification

```
# Vérification du statut HA depuis l'Advanced Shell
system ha show status
```

Remédiation

1. Déployer un second équipement Sophos Firewall compatible
2. Configurer le HA en mode QuickHA ou Interactif selon l'infrastructure
3. Définir le lien HA dédié entre les deux nœuds
4. Vérifier la synchronisation des configurations entre nœuds
5. Tester le basculement en conditions contrôlées (maintenance programmée)

Valeur par défaut : Mode Standalone — HA non configuré par défaut.

Critère de conformité : HA Status = `Established[Active-Passive]` ou `Established[Active-Active]`. Aucun nœud en état `Standalone` ou `Faulty`.

Contrôle 1.7 — Noyau Linux 6.6+ durci et architecture Xstream v2 conteneurisée (NOUVEAU — SFOS v22)

CIS Ref : *(Architecture Sophos v22)* | ***MITRE :*** *T1601, T1055* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

SFOS v22 intègre un noyau Linux 6.6+ spécialement durci combiné à l'architecture Xstream v2 qui place les moteurs de protection dans des conteneurs isolés. Les vulnérabilités CPU (Spectre, Meltdown, L1TF, MDS, Retbleed, ZenBleed, Downfall) permettent à du code non privilégié de lire des zones mémoire protégées, y compris les clés cryptographiques et les identifiants stockés en mémoire noyau. La vérification de l'activation de ces protections est indispensable, particulièrement sur les plateformes virtualisées partagées.

Architecture Xstream v2 — Sécurité par conception

L'architecture Xstream v2 introduit une **séparation des privilèges** radicale : aucun service n'a d'accès complet au système. Les points clés à vérifier et documenter :

COMPOSANT XSTREAM V2	MÉCANISME DE SÉCURITÉ	BÉNÉFICE
IPS conteneurisé	Le moteur IPS s'exécute dans un conteneur isolé	Une vulnérabilité dans l'IPS ne peut pas escalader au système OS du firewall
Séparation de privilèges	Aucun service ne possède l'accès root complet au système	Limite les dommages en cas de compromission d'un composant
Traitement des paquets hybride	Inspection sur CPUs généralistes + processeurs ASIC + vCPUs	Resilience opérationnelle avec maintien de l'inspection même sous charge
HA Self-Healing intégré	La paire HA se surveille mutuellement	Corrections automatiques des déviations d'état en quelques secondes

Vérifications architecture Xstream v2

```
Verify IPS container mode :
  System > Diagnostics > Services → IPS service status = Running (containerized)
Verify Xstream SSL/TLS inspection :
  Protect > Rules and policies > SSL/TLS inspection rules → règles Decrypt actives
Verify packet engine mode :
  System > Administration > Device access → mode du moteur de paquets
```

Impact potentiel

- Lecture de données mémoire sensibles (clés VPN, identifiants) via les vulnérabilités Spectre/Meltdown sur des plateformes virtuelles
- Injection de code dans des processus noyau via des attaques en l'absence de KASLR
- Exploitation de dépassements de tampon via l'absence de stack canaries
- T1601 : modification de l'image système si les protections noyau sont désactivées
- T1055 : injection de processus contrée par la séparation de privilèges et les services conteneurisés

Protections activées dans SFOS v22

PROTECTION	VULNÉRABILITÉ CIBLÉE	STATUT SFOS V22
Spectre v1/v2 mitigations	Spectre CVE-2017-5753/5715	Activé par défaut
Meltdown (KPTI)	Meltdown CVE-2017-5754	Activé par défaut
L1TF / Foreshadow	CVE-2018-3615/3620/3646	Activé par défaut
MDS / RIDL / Fallout	CVE-2018-12126/12127/12130	Activé par défaut
Retbleed	CVE-2022-29900/29901	Activé par défaut
ZenBleed	CVE-2023-20593 (AMD)	Activé par défaut
Downfall (GDS)	CVE-2022-40982 (Intel)	Activé par défaut
KASLR	Randomisation des adresses noyau	Activé par défaut
Stack canaries	Protection contre les stack overflows	Activé par défaut
Hardened usercopy	Validation des copies user/kernel space	Activé par défaut

Navigation / CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5 > Advanced shell)
# Vérifier les mitigations CPU actives :
cat /sys/devices/system/cpu/vulnerabilities/spectre_v1
cat /sys/devices/system/cpu/vulnerabilities/spectre_v2
cat /sys/devices/system/cpu/vulnerabilities/meltdown
cat /sys/devices/system/cpu/vulnerabilities/l1tf
cat /sys/devices/system/cpu/vulnerabilities/mds
cat /sys/devices/system/cpu/vulnerabilities/retbleed
# Vérifier la version du noyau :
uname -r
# Résultat attendu : noyau 6.6.x ou supérieur
# Vérifier KASLR :
cat /proc/sys/kernel/randomize_va_space
# Résultat attendu : 2 (ASLR complet activé)
```

Remédiation

1. Maintenir SFOS à jour vers la dernière version v22 pour bénéficier du noyau 6.6+ durci et de l'architecture Xstream v2
2. Activer les hotfixes automatiques (contrôle 1.2) pour recevoir les correctifs noyau sans délai
3. Sur les déploiements VMware/Hyper-V/KVM, vérifier que les protections CPU au niveau hyperviseur sont activées (Spectre/Meltdown mitigations côté hyperviseur)
4. Pour les plateformes AMD (vulnérabilité ZenBleed) et Intel (Downfall), s'assurer que les microcode updates sont appliqués côté hôte physique
5. Vérifier le statut du service IPS via `System > Diagnostics > Services` — confirmer que l'IPS tourne en mode conteneurisé (Xstream v2)
6. Documenter l'activation de l'inspection SSL/TLS Xstream via `Protect > Rules and policies > SSL/TLS inspection rules`

7. Surveiller les avis Sophos PSIRT pour les nouvelles vulnérabilités CPU nécessitant des mises à jour de microcode

Valeur par défaut : Toutes les mitigations noyau activées par défaut dans SFOS v22 avec noyau Linux 6.6+. Architecture Xstream v2 active sur les équipements XGS-Series et les VM SFOS v22.

Critère de conformité : Version SFOS v22 installée. Noyau ≥ 6.6.x confirmé via `uname -r`. Fichiers `/sys/devices/system/cpu/vulnerabilities/*` ne retournent pas `Vulnerable` sans mitigation. Service IPS en mode conteneurisé confirmé dans les diagnostics système.

Contrôle 1.8 — Capteur XDR Linux — intégrité du système et surveillance en temps réel (NOUVEAU — SFOS v22)

CIS Ref : *(Architecture Sophos v22 — Remote Integrity Monitoring)* | ***MITRE :*** *T1562.001, T1601, T1005* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le capteur XDR Linux intégré dans SFOS v22 (XDR Linux Sensor) assure une surveillance en temps réel de l'intégrité du système d'exploitation du pare-feu. Il détecte les modifications non autorisées de la configuration, les tentatives d'exécution de programmes malveillants, l'altération de fichiers système, et les exports non autorisés de règles. Sans ce capteur, des modifications persistantes apportées par un attaquant ayant compromis le pare-feu peuvent rester non détectées entre deux audits.

Impact potentiel

- T1562.001 : désactivation ou modification silencieuse des outils de protection sans alerte
- T1601 : modification de l'image système du pare-feu sans détection
- T1005 : exports non autorisés de la configuration/règles (extraction de secrets VPN, politique de sécurité)
- Persistance d'un attaquant via modification de fichiers de configuration noyau non surveillés

Capacités de détection du capteur XDR Linux

ÉVÉNEMENT DÉTECTÉ	NIVEAU D'ALERTE	ACTION RECOMMANDÉE
Modification non autorisée de la configuration	CRITIQUE	Déclencher IR, restaurer depuis sauvegarde
Export de règles de pare-feu non planifié	ÉLEVÉ	Vérifier les logs admin, contacter SOC
Tentative d'exécution de programme malveillant	CRITIQUE	Isoler, analyser, restaurer
Altération de fichiers système	CRITIQUE	Vérifier intégrité, réinstaller si compromis
Changement d'état de surveillance du système	ÉLEVÉ	Vérifier l'origine du changement

Navigation

```
System > Sophos Central > XDR Integration
→ Vérifier que le pare-feu est enregistré dans Sophos Central
→ XDR Linux Sensor : statut = Connected/Active
Sophos Central > Threat Analysis Center
→ Consulter les détections XDR liées au pare-feu
→ Configurer les alertes sur les événements d'intégrité système
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
# Vérifier le statut de connexion Sophos Central
show sophos-central status
# Vérifier les processus du capteur XDR
ps aux | grep xdr
# Vérifier les logs d'intégrité système
tail -f /var/log/sophos/xdr_sensor.log
```

Remédiation

1. Enregistrer le pare-feu dans Sophos Central via `System > Sophos Central`
2. Vérifier que l'abonnement XDR ou MDR est actif dans `System > Administration > Licensing`
3. Confirmer que le capteur XDR Linux est en statut `Active` dans Sophos Central
4. Configurer des alertes dans Sophos Central Threat Analysis Center pour les détections d'intégrité du pare-feu
5. Intégrer les alertes XDR dans le workflow SOC pour une réponse automatisée
6. Tester le capteur en simulant une modification de configuration documentée et vérifier la détection

Valeur par défaut : Capteur XDR disponible à condition que l'abonnement XDR/MDR soit actif et que le pare-feu soit enregistré dans Sophos Central.

Critère de conformité : Pare-feu enregistré dans Sophos Central. Capteur XDR Linux en statut `Active`. Alertes d'intégrité configurées dans Sophos Central.

Domaine 2 — Authentification et accès administrateur

> ***Objectif :*** *Protéger l'accès à la console d'administration et aux services VPN contre les attaques par force brute, les accès non autorisés et les sessions abandonnées, en imposant le MFA, des politiques de mots de passe fortes (admin ≥14-16 caractères, utilisateurs ≥12 caractères), l'authentification par clé SSH, et des limites de tentatives strictes.*

Contrôle 2.1 — Timeout de session admin ≤ 10 minutes et blocage après 5 tentatives

> ***CIS Ref :*** *1.1.1* | ***MITRE :*** *T1078, T1110* | ***Niveau :*** 🟢 *L1*

Description du risque

Une session administrative non verrouillée sur un poste de travail sans surveillance permet à un utilisateur non autorisé d'accéder à l'interface de gestion du pare-feu sans authentification. Le blocage des tentatives multiples empêche les attaques par force brute sur la WebAdmin et la CLI SSH.

Impact potentiel

- Accès non autorisé à l'interface d'administration depuis un poste laissé sans surveillance
- Compromission du compte admin par force brute si aucune limite de tentatives n'est définie
- Modification malveillante des règles de sécurité ou exfiltration de la configuration

Navigation

```
System > Administration > Admin and user settings > Login security
→ "Logout admin session after __ Minutes of inactivity" : cocher et régler à 10
→ "Block login" : cocher
→ "After __ unsuccessful attempts from same IP in __ Seconds" : régler à 5 et 60
→ "Block login access for __ minutes [1-60]" : régler à au moins 5
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web uniquement
# System > Administration > Admin and user settings > Login security
# Valider les 4 paramètres ci-dessus
```

Remédiation

1. Naviguer vers `System > Administration > Admin and user settings > Login security`
2. Cocher `Logout admin session after 10 Minutes of inactivity`
3. Cocher `Block login`
4. Configurer `After 5 unsuccessful attempts from same IP in 60 Seconds`

5. Configurer `Block login access for 5 minutes`
6. Appliquer et tester le verrouillage en simulant 5 tentatives échouées

Valeur par défaut : Logout après 10 minutes activé par défaut. Block Login activé par défaut.

Critère de conformité : Timeout ≤ 10 min, blocage après ≤ 5 tentatives dans 60 secondes, durée de blocage ≥ 5 minutes.

Contrôle 2.2 — Bannière de connexion (login disclaimer) configurée

> ***CIS Ref :*** *1.1.2* | ***MITRE :*** *T1078* | ***Niveau :*** 🟢 *L1*

Description du risque

L'absence de bannière de connexion légale expose l'organisation à des risques juridiques en cas de poursuites contre un accès non autorisé. Une bannière bien rédigée établit explicitement que l'accès est réservé aux utilisateurs autorisés, que les sessions sont journalisées, et renforce la responsabilité légale des utilisateurs non autorisés.

Impact potentiel

- Affaiblissement de la position juridique lors de poursuites pour accès non autorisé
- Absence de notice d'avertissement pouvant réduire la valeur probatoire des logs
- Non-conformité avec les exigences réglementaires (ISO 27001, HDS, NIS2)

Navigation

```
System > Administration > Admin and User Settings > Login Disclaimer Settings
→ Cocher "Enable login disclaimer"
→ Rédiger le message de disclaimer (approuvé par le service juridique)
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web uniquement
# System > Administration > Admin and User Settings > Login Disclaimer Settings
# Vérifier que "Enable login disclaimer" est coché
```

Remédiation

1. Naviguer vers `System > Administration > Admin and User Settings > Login Disclaimer Settings`
2. Cocher `Enable login disclaimer`
3. Saisir un message de bannière approuvé par le service juridique, contenant :
    - Interdiction explicite d'accès non autorisé
    - Avertissement que les sessions sont enregistrées et surveillées
    - Sanctions applicables en cas d'accès non autorisé

- Absence du mot “bienvenue” ou tout terme d’invitation

4. Appliquer et vérifier l’affichage à la connexion

Valeur par défaut : Non configuré (désactivé par défaut).

Critère de conformité : `Enable login disclaimer` = coché. Message de bannière configuré, approuvé par le juridique, ne contenant pas de terme d’invitation.

Contrôle 2.3 — Politique de mots de passe complexes activée

CIS Ref : *1.1.5* | ***MITRE :*** *T1110* | ***Niveau :*** 🟢 *L1*

Description du risque

Des mots de passe simples sur les comptes administrateurs des pare-feux sont une cible privilégiée des attaquants, notamment dans les campagnes de credential stuffing utilisant des listes de mots de passe connus pour les équipements réseau. Selon le Health Check Sophos v22, les comptes administrateurs doivent utiliser un minimum de 14 à 16 caractères avec toutes les classes de caractères, et les comptes utilisateurs standard un minimum de 12 caractères.

Impact potentiel

- Compromission du compte admin par attaque par dictionnaire ou credential stuffing
- Accès non autorisé à la console de gestion avec privilèges complets
- Modification des règles de sécurité ou désactivation des protections

Navigation

```
System > Administration > Admin and user settings >
  Administrator password complexity settings
→ Cocher "Enable password complexity check"
→ Configurer pour les comptes administrateurs :
  - Minimum length : 16 (recommandé) ou 14 (minimum Health Check)
  - Require uppercase letter : coché
  - Require lowercase letter : coché
  - Require numeric character : coché
  - Require special character (@, $, !, etc.) : coché
Pour les comptes utilisateurs (User Portal) :
  - Minimum length : 12 (minimum Health Check v22)
  - Require uppercase, lowercase, numeric, special : cochés
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web uniquement
# System > Administration > Admin and user settings >
# Administrator password complexity settings
# Vérifier que "Enable password complexity check" est activé
# et que la longueur minimale est ≥ 14 (admin) / ≥ 12 (utilisateurs)
```

Remédiation

1. Naviguer vers `System > Administration > Admin and user settings > Administrator password complexity settings`
2. Cocher `Enable password complexity check`
3. Définir une longueur minimale de **16 caractères** pour les administrateurs (14 minimum absolu selon Health Check v22)
4. Définir une longueur minimale de **12 caractères** pour les comptes utilisateurs
5. Exiger au moins une majuscule, une minuscule, un chiffre et un caractère spécial
6. Éviter les mots du dictionnaire — préférer des phrases de passe (ex : `Th3F0rdMust@ngis#1`)
7. Réinitialiser immédiatement les mots de passe non conformes

Valeur par défaut : `Enable password complexity check` = Activé par défaut (mais avec des paramètres permissifs).

Critère de conformité : Complexité activée, longueur minimale ≥ 16 pour les admins (≥ 14 minimum), ≥ 12 pour les utilisateurs, exigence de majuscule, minuscule, chiffre et caractère spécial.

Contrôle 2.4 — MFA pour l'accès web admin et VPN distant

CIS Ref : *1.1.8* | ***MITRE :*** *T1078, T1133* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

L'interface WebAdmin de Sophos Firewall donne un accès privilégié complet à toute la politique de sécurité. Sans MFA, la compromission d'un seul couple identifiant/mot de passe suffit à prendre le contrôle total du pare-feu. Les accès VPN sans MFA permettent aux attaquants d'entrer dans le réseau interne avec des identifiants volés. SFOS v22 supporte désormais SHA-256 et SHA-512 pour les tokens OTP (Google Authenticator et Sophos Authenticator), offrant une sécurité renforcée pour les applications TOTP.

Impact potentiel

- Prise de contrôle totale du pare-feu avec modification des règles de sécurité
- Accès non autorisé au réseau interne via VPN avec des identifiants compromis
- Désactivation des protections de sécurité par un attaquant ayant accès à la WebAdmin

Navigation

```
Configure > Authentication > Multi-factor authentication > Multi-factor authentication
settings
→ Specific Users and groups > Add the user or group concerné
→ Enable "Generate OTP token with next sign-in" pour création automatique
→ Enable "Require MFA for Web admin console"
→ Enable "Require MFA for SSL VPN remote access"
→ Enable "Require MFA for IPSec remote access"
→ Algorithm OTP (v22 nouveau) : sélectionner SHA-256 ou SHA-512
  (supérieur à SHA-1 utilisé dans les versions antérieures)
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web uniquement
# Configure > Authentication > Multi-factor authentication > Multi-factor authentication
settings
# Vérifier que "Require MFA for Web admin console" est activé
# Vérifier que l'algorithme OTP est SHA-256 ou SHA-512
```

Remédiation

1. Naviguer vers `Configure > Authentication > Multi-factor authentication > Multi-factor authentication settings`
2. Ajouter tous les utilisateurs/groupes admin dans `Specific Users and groups`
3. Activer `Generate OTP token with next sign-in` pour la création automatique des tokens
4. Activer `Require MFA for Web admin console`
5. Activer `Require MFA for SSL VPN remote access` et `IPSec remote access`
6. Sélectionner l'algorithme SHA-256 ou SHA-512 pour les tokens OTP (nouveau en v22)
7. Distribuer les tokens OTP aux utilisateurs via Google Authenticator ou Sophos Authenticator (compatibles SHA-256/SHA-512)
8. Tester l'accès MFA avant de fermer la session courante

Valeur par défaut : MFA non activé par défaut pour la WebAdmin et le VPN. Algorithme OTP = SHA-1 (versions antérieures) / SHA-256 disponible en v22.

Critère de conformité : MFA activé pour la console web admin, SSL VPN et IPSec remote access. Tous les comptes administrateurs inclus dans la politique MFA. Algorithme OTP = SHA-256 ou SHA-512.

Contrôle 2.5 — MFA pour le compte admin par défaut

CIS Ref : *1.1.9* | ***MITRE :*** *T1078* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Le compte `admin` par défaut de Sophos Firewall est une cible connue de toutes les campagnes de force brute ciblant les pare-feux Sophos exposés sur Internet. Ce compte, dont l'existence est documentée publiquement, doit impérativement être protégé par MFA en plus des autres mesures. C'est l'une des vérifications de sévérité HIGH du Health Check officiel Sophos v22.

Impact potentiel

- Accès non autorisé au compte admin par défaut via force brute ou identifiants par défaut
- Modification de la politique de sécurité par un attaquant ayant compromis ce compte
- Création de comptes backdoor ou modification des règles de pare-feu

Navigation

```
System > Administration > Device Access > Multi-factor Authentication for default admin
→ Activer "MFA for default admin" = ON
→ Note : le MFA ne s'applique pas aux connexions SSH
  (permettant la récupération du compte en cas de perte du token)
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web uniquement
# System > Administration > Device Access
# Vérifier que "Multi-factor Authentication for default admin" = ON
```

Remédiation

1. Naviguer vers `System > Administration > Device Access`
2. Dans la section `Multi-factor Authentication for default admin`, activer le commutateur sur `ON`
3. Configurer le token OTP pour le compte admin (via `Configure > Authentication > Multi-factor authentication`)
4. Utiliser SHA-256 ou SHA-512 comme algorithme de hash pour le token OTP (nouveau en v22)
5. Tester l'accès MFA avec une session distincte avant de fermer la session courante
6. Conserver l'accès SSH en dernier recours (le MFA ne s'applique pas au SSH)

Valeur par défaut : MFA pour l'admin par défaut désactivé par défaut.

Critère de conformité : `MFA for default admin` = ON.

Contrôle 2.6 — Connexion Active Directory/LDAP chiffrée (LDAPS ou StartTLS)

> ***CIS Ref :*** *2.2* | ***MITRE :*** *T1040, T1557* | ***Niveau :*** 🟢 *L1*

Description du risque

Une connexion LDAP non chiffrée entre le pare-feu et l'Active Directory transmet les identifiants et les données d'authentification en clair sur le réseau. Un attaquant ayant accès au réseau interne peut capturer ces échanges et rejouer les tickets d'authentification (pass-the-ticket) ou réaliser une attaque man-in-the-middle. Le Health Check Sophos v22 classe cette vérification comme MEDIUM severity — le chiffrement SSL/TLS ou LDAPS est obligatoire ; le LDAP en texte clair est interdit.

Impact potentiel

- Capture des identifiants LDAP en clair sur le réseau interne
- Attaques par rejeu de tickets d'authentification (NTLM relay, pass-the-ticket)
- Compromission du compte de service LDAP donnant accès à l'annuaire

Navigation

```
Configure > Authentication > Servers > Edit (ou Add)
→ Connection security : sélectionner "SSL/TLS" ou "STARTTLS"
→ Cocher "Validate server certificate"
→ Cliquer sur "Save"
```

CLI de vérification

```
# Vérification dans l'interface web uniquement
# Configure > Authentication > Servers > Edit
# Vérifier que Connection security = "SSL/TLS" ou "STARTTLS"
# et que "Validate server certificate" est coché
```

Remédiation

1. Naviguer vers `Configure > Authentication > Servers`
2. Éditer chaque serveur LDAP/Active Directory configuré
3. Définir `Connection security` sur `SSL/TLS` (LDAPS, port 636) ou `STARTTLS` (port 389 avec upgrade TLS)
4. Cocher `Validate server certificate` pour prévenir les attaques MitM
5. Importer le certificat CA du serveur LDAP si nécessaire
6. Tester la connexion avec le bouton `Test connection`

Valeur par défaut : Connexion non chiffrée (LDAP plain text) par défaut.

Critère de conformité : `Connection security` = `SSL/TLS` ou `STARTTLS`. `Validate server certificate` = coché.

Contrôle 2.7 — Authentification SSH par clé publique (RSA/ED25519) (NOUVEAU)

CIS Ref : *(Health Check Sophos v22 — HIGH severity)* | ***MITRE :*** *T1078, T1133* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

L'authentification SSH par mot de passe expose l'accès CLI du pare-feu aux attaques par force brute et aux risques liés aux mots de passe partagés. L'utilisation de clés SSH RSA 4096 bits ou ED25519 (algorithme moderne à courbe elliptique) offre une sécurité cryptographique supérieure et permet de désactiver l'authentification par mot de passe sur SSH, réduisant drastiquement la surface d'attaque de l'accès CLI.

Impact potentiel

- Compromission de l'accès CLI par force brute sur les mots de passe SSH
- Réutilisation d'un mot de passe compromis pour l'accès SSH si l'auth par mot de passe est maintenue
- Absence de traçabilité par identité cryptographique en cas d'investigation forensique SSH

Navigation

```
System > Administration > Device Access > SSH
→ Activer "SSH public key authentication"
→ Importer la clé publique RSA (4096 bits) ou ED25519 pour chaque administrateur
→ Une fois les clés configurées et testées :
  → Désactiver "Password authentication" pour SSH
  → Cliquer sur "Apply"
```

Génération des clés (depuis le poste administrateur)

```
# Générer une clé ED25519 (recommandé — plus sûr et plus court que RSA)
ssh-keygen -t ed25519 -C "admin@organisation.fr" -f ~/.ssh/sophos_fw_ed25519

# Alternative : clé RSA 4096 bits
ssh-keygen -t rsa -b 4096 -C "admin@organisation.fr" -f ~/.ssh/sophos_fw_rsa4096

# Afficher la clé publique à importer dans SFOS
cat ~/.ssh/sophos_fw_ed25519.pub
```

CLI de vérification

```
# Tester la connexion SSH par clé depuis le poste admin (avant de désactiver le mot de
passe)
ssh -i ~/.ssh/sophos_fw_ed25519 admin@<ip-firewall>

# Depuis l'Advanced Shell SFOS, vérifier les clés autorisées
cat ~/.ssh/authorized_keys
```

Remédiation

1. Générer une paire de clés ED25519 ou RSA 4096 bits sur chaque poste administrateur
2. Importer les clés publiques dans `System > Administration > Device Access > SSH`
3. Tester la connexion SSH par clé avant de désactiver l'auth par mot de passe
4. Désactiver l'authentification par mot de passe SSH une fois les clés validées
5. Stocker les clés privées dans un gestionnaire de secrets (HashiCorp Vault, CyberArk, ou au minimum protégées par passphrase)
6. Révoquer les clés des administrateurs quittant l'organisation immédiatement

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

Critère de conformité : Clés SSH RSA 4096 ou ED25519 configurées pour tous les administrateurs. Authentification par mot de passe SSH désactivée.

Domaine 3 — Sécurisation de l'interface de gestion

Objectif : *Restreindre l'accès aux services de gestion (HTTPS, SSH, SNMP) aux seules zones et adresses IP autorisées, utiliser des certificats valides, et configurer les notifications pour les événements critiques.*

Contrôle 3.1 — Désactiver l'accès management depuis la zone WAN

CIS Ref : *1.1.6* | ***MITRE :*** *T1190, T1133* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

L'exposition des services d'administration (HTTPS port 4444, SSH port 22) sur la zone WAN est le vecteur d'attaque le plus documenté sur les pare-feux Sophos. Plusieurs vulnérabilités critiques (CVE-2020-12271, CVE-2022-1040, CVE-2023-1671) ont été exploitées massivement via l'interface web exposée sur Internet. Le Health Check Sophos v22 classe ce point comme HIGH severity et préconise le blocage explicite de WebAdmin et User Portal depuis 0.0.0.0/Any sur la zone WAN.

Impact potentiel

- Exploitation directe des vulnérabilités de la WebAdmin depuis Internet
- Attaques par force brute sur les interfaces SSH et HTTPS sans contrainte géographique
- Compromission complète du pare-feu depuis n'importe quelle IP mondiale

Navigation

```
System > Administration > Device Access > Local service ACL
→ Pour la zone WAN : décocher HTTPS, SSH, PING/PING6, DNS, SMTP RELAY, SNMP
→ Vérifier que 0.0.0.0/Any sur WAN n'a accès ni à WebAdmin ni au User Portal
→ Local service ACL exception rule : limiter l'accès admin aux seules IP autorisées
→ Cliquer sur "Apply"
Alternative recommandée : utiliser Sophos Central pour la gestion à distance
```

CLI de vérification

```
# Vérification dans l'interface web uniquement
# System > Administration > Device Access > Local service ACL
# Vérifier que HTTPS et SSH sont décochés pour la zone WAN
```

Remédiation

1. Naviguer vers `System > Administration > Device Access > Local service ACL`
2. Décocher `HTTPS`, `SSH`, `PING/PING6`, `DNS`, `SMTP RELAY`, `SNMP` pour la zone `WAN`
3. S'assurer qu'aucune règle d'exception n'autorise 0.0.0.0/Any sur WAN pour WebAdmin ou User Portal

4. Configurer une `Local service ACL exception rule` pour autoriser uniquement les IP de gestion spécifiques (plage IP du VPN d'administration)
5. Utiliser Sophos Central pour la gestion à distance en remplacement
6. Si l'accès WAN est absolument nécessaire, le limiter à des plages IP spécifiques via les règles d'exception

Valeur par défaut : Services désactivés par défaut sur la zone WAN (bonne pratique usine).

Critère de conformité : HTTPS et SSH désactivés pour la zone WAN dans la Local service ACL. Aucune exception 0.0.0.0/Any sur WAN. Aucune exception non documentée.

Contrôle 3.2 — Certificat TLS valide pour l'interface WebAdmin

> ***CIS Ref :*** *1.1.7* | ***MITRE :*** *T1557* | ***Niveau :*** 🔵 *L2*

Description du risque

Le certificat auto-signé installé par défaut sur l'interface HTTPS de gestion de Sophos Firewall (port 4444) ne permet pas aux administrateurs de détecter une attaque man-in-the-middle sur leur session de gestion. Un attaquant en position MitM peut intercepter les identifiants et commandes d'administration.

Impact potentiel

- Interception silencieuse des sessions d'administration par un attaquant MitM
- Impossibilité de détecter un certificat frauduleux en l'absence de CA de confiance
- Habituation des administrateurs à ignorer les erreurs de certificat (training vers les mauvaises habitudes)

Navigation

```
System > Certificates > Certificates > Add
→ Importer un certificat depuis une CA interne ou publique de confiance
System > Administration > Admin settings > Admin console and end-user interaction >
Certificate
→ Sélectionner le certificat valide importé
→ Appliquer pour WebAdmin, user portal, captive portal et SPX reply portal
```

CLI de vérification

```
# Vérification dans l'interface web
# System > Certificates > Certificates
# Vérifier la date d'expiration et l'émetteur du certificat en usage
```

Remédiation

1. Créer une CSR depuis `System > Certificates > Certificate signing requests`
2. Faire signer la CSR par une CA interne de confiance (PKI d'entreprise) ou une CA publique
3. Importer le certificat signé dans `System > Certificates > Certificates > Add`

4. Naviguer vers `System > Administration > Admin settings > Admin console and end-user interaction > Certificate`
5. Sélectionner le nouveau certificat valide
6. Vérifier que l'horloge du pare-feu est synchronisée (NTP) pour éviter les erreurs de validité temporelle

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

Critère de conformité : Certificat valide (non expiré, émis par une CA de confiance, longueur de clé ≥ 2048 bits, hash SHA-2 ou supérieur) configuré pour la WebAdmin.

Contrôle 3.3 — SNMPv3 uniquement (éliminer SNMPv1 et v2c)

CIS Ref : *1.2.1* | ***MITRE :*** *T1040, T1590* | ***Niveau :*** 🟢 *L1*

Description du risque

SNMPv1 et SNMPv2c transmettent les community strings en clair sur le réseau. Ces strings, souvent laissés à leur valeur par défaut (`public`, `private`), permettent à un attaquant de lire toutes les informations de l'équipement (interfaces, routes, compteurs) sans authentification. SNMPv3 ajoute l'authentification et le chiffrement.

Impact potentiel

- Interception des community strings SNMP sur le réseau
- Accès en lecture à toutes les informations de configuration réseau exposées via SNMP
- Utilisation des données SNMP pour la reconnaissance réseau (T1590)

Navigation

```
System > Administration > SNMP
→ Supprimer toutes les configurations SNMPv1 et v2c
→ Configurer SNMPv3 users and traps :
  - Encryption algorithm : AES (recommandé) ou DES
  - Authentication algorithm : SHA
  - Définir des mots de passe forts pour l'authentification et le chiffrement
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web
# System > Administration > SNMP
# Vérifier qu'aucune configuration SNMPv1/v2c n'est présente
# Vérifier que SNMPv3 avec chiffrement AES est configuré
```

Remédiation

1. Naviguer vers `System > Administration > SNMP`
2. Supprimer toutes les configurations SNMPv1 et SNMPv2c existantes
3. Créer un utilisateur SNMPv3 avec algorithme d'authentification SHA et chiffrement AES

4. Définir des mots de passe forts distincts pour l'authentification et le chiffrement
5. Restreindre les hôtes SNMP autorisés aux seuls serveurs de supervision légitimes

Valeur par défaut : SNMP non configuré par défaut.

Critère de conformité : Aucune configuration SNMPv1/v2c présente. Si SNMP est utilisé, uniquement SNMPv3 avec AES et SHA.

Contrôle 3.4 — Notifications d'événements système et sécurité configurées

CIS Ref : *1.2.2* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

Sans notifications configurées, les événements critiques (expiration d'abonnement, défaillance HA, dépassement de capacité, attaques détectées) passent inaperçus jusqu'à ce qu'un impact opérationnel se manifeste. La détection tardive d'une compromission est directement liée à l'absence d'alertes en temps réel.

Impact potentiel

- Découverte tardive d'incidents de sécurité (attaques, compromissions)
- Non-détection de l'expiration d'abonnements de protection
- Absence d'alerte sur les défaillances matérielles ou les anomalies système

Navigation

```
System > Administration > Notification settings
→ Configurer le serveur de messagerie (built-in ou externe SMTP)
→ "From email address" : adresse expéditrice du firewall
→ "Send notifications to email address" : adresse des administrateurs
Configure > System services > Notification list
→ Cocher les événements admin, système et sécurité pertinents
→ Activer les notifications email et/ou les traps SNMP
```

CLI de vérification

```
# Vérification dans l'interface web
# System > Administration > Notification settings
# Vérifier la configuration du serveur mail et les événements activés
```

Remédiation

1. Naviguer vers `System > Administration > Notification settings`
2. Configurer le serveur mail (built-in ou externe SMTP avec STARTTLS/SSL)
3. Définir l'adresse expéditrice et les destinataires administrateurs
4. Naviguer vers `Configure > System services > Notification list`
5. Activer les catégories d'événements : admin (modifications de configuration), système (HA, licences), sécurité (IPS, menaces détectées)

6. Tester l'envoi de notification avec le bouton de test

Valeur par défaut : Non configuré par défaut.

Critère de conformité : Serveur de notification configuré. Événements admin, système et sécurité activés. Test de notification réussi.

Contrôle 3.5 — Restreindre l'accès management par zone et par IP source

CIS Ref : *1.1.6 (étendu)* | ***MITRE :*** *T1133* | ***Niveau :*** 🟢 *L1*

Description du risque

Même sur les zones internes, l'accès à la WebAdmin et à SSH doit être limité aux seuls postes d'administration. Permettre à tous les utilisateurs du réseau LAN d'accéder à l'interface de gestion augmente la surface d'attaque interne et facilite les attaques internes ou le mouvement latéral depuis un endpoint compromis.

Impact potentiel

- Accès non autorisé à l'interface d'administration depuis un endpoint interne compromis
- Mouvement latéral facilité si un attaquant ayant compromis un poste interne peut atteindre la WebAdmin
- Attaques par force brute depuis le réseau interne sans restriction

Navigation

```
System > Administration > Device Access > Local service ACL
→ Pour la zone LAN/DMZ : limiter HTTPS et SSH aux seules IP/plages IP de gestion
→ Local service ACL exception rule > Add
  - Source network : plage IP des postes d'administration
  - Services : HTTPS (port 4444), SSH (port 22)
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web
# System > Administration > Device Access > Local service ACL exception rule
# Vérifier que seules les IP de gestion autorisées ont accès
```

Remédiation

1. Définir une plage IP dédiée pour les postes d'administration (ex : /27 sur un VLAN dédié)
2. Configurer une exception ACL pour cette plage uniquement
3. Révoquer l'accès HTTPS/SSH pour la plage LAN générale
4. Documenter les IP d'administration dans le registre des actifs
5. Réviser la liste trimestriellement et lors de tout changement d'équipe

Valeur par défaut : Accès HTTPS/SSH permis pour toutes les zones internes par défaut.

Critère de conformité : Accès WebAdmin (HTTPS port 4444) et SSH restreints aux seules IP/plages IP d'administration documentées.

Contrôle 3.6 — Sécurisation de l'API XML Sophos Firewall (NOUVEAU — SFOS v22)

> ***CIS Ref :*** *(Best practice — API Security)* | ***MITRE :*** *T1078 (Valid Accounts — API key theft), T1190 (Exploit Public-Facing Application)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Sophos Firewall expose une API XML utilisée pour l'automatisation, les intégrations SIEM et les scripts de gestion. Accessible via HTTPS sur le port de management (4444), cette API peut être utilisée par un attaquant pour réaliser des modifications de configuration non autorisées si elle est accessible sans restriction IP ou si les clés API ne sont pas correctement protégées. La compromission d'une clé API d'administration donne un accès programmatique complet à la politique de sécurité du pare-feu.

Impact potentiel

- T1190 : exploitation de l'API exposée depuis des zones non autorisées pour modifier la configuration du pare-feu
- T1078 : vol d'une clé API administrateur donnant un accès programmatique complet sans MFA
- Modification silencieuse des règles de sécurité via des appels API non tracés correctement
- Exfiltration de la configuration complète (règles, secrets VPN, objets réseau) via l'API

Navigation

```
System > Administration > API > API configuration
→ Restrict API access by IP : activer = ON
→ Allowed IP addresses : ajouter uniquement les IP des serveurs d'intégration autorisés
→ Disable XML API if not used : désactiver complètement si l'API n'est pas utilisée
Pour la gestion des clés API :
System > Administration > API > API credentials
→ Auditer les clés existantes (nom, création, dernière utilisation)
→ Révoquer les clés inutilisées ou dont le titulaire a quitté l'organisation
→ Utiliser des comptes API dédiés (non le compte admin par défaut)
Pour la surveillance :
Log Viewer > Admin Activity → filtrer sur "API" pour observer les appels API
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5 > Advanced shell)
show api configuration
# Vérifier les restrictions IP configurées et le statut d'activation
# Depuis l'interface web : System > Administration > API
# Vérifier les adresses IP autorisées et les credentials actifs
```

Remédiation

1. Naviguer vers `System > Administration > API`
2. Si l'API XML n'est pas utilisée : la désactiver complètement (`Disable API = ON`)

3. Si l'API est utilisée pour des intégrations :
    - Activer la restriction par IP (`Restrict API access by IP`)
    - Limiter les IP autorisées aux seuls serveurs d'intégration (SIEM, scripts d'automatisation)
    - Créer des comptes API dédiés avec les privilèges minimaux nécessaires (ne pas utiliser le compte `admin` par défaut)
4. Révoquer toutes les clés API inutilisées ou orphelines
5. Planifier une rotation des clés API tous les 90 jours minimum
6. Activer la surveillance des appels API dans `Log Viewer > Admin Activity`
7. Configurer une alerte SIEM sur les appels API depuis des IP non répertoriées dans la liste autorisée
8. Utiliser l'authentification par certificat si supportée dans l'intégration

Valeur par défaut : API XML accessible sur le port de management depuis toutes les zones autorisées par la Local service ACL, sans restriction IP supplémentaire.

Critère de conformité : API XML désactivée si non utilisée. Si utilisée : restriction IP activée, IP autorisées documentées, comptes API dédiés configurés, rotation des clés planifiée, appels API surveillés dans les logs Admin Activity.

Contrôle 3.7 — Durcissement de l'intégration Sophos Central (NOUVEAU — SFOS v22)

CIS Ref : *(Best practice — Cloud Management Security)* | ***MITRE :*** *T1078.004 (Cloud Accounts)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Sophos Central est la plateforme de gestion cloud qui synchronise les configurations, les politiques et les alertes du pare-feu. Sa compromission équivaut à la compromission du pare-feu lui-même : un attaquant disposant d'un accès administrateur dans Sophos Central peut modifier les politiques, désactiver les protections, et exfiltrer les données de configuration de tous les équipements gérés. T1078.004 (Cloud Accounts) documente spécifiquement l'exploitation des comptes cloud pour l'accès aux ressources cloud gérées.

Impact potentiel

- T1078.004 : compromission du compte Sophos Central donnant accès à tous les firewalls et endpoints gérés
- Désactivation à distance des protections (IPS, NDR, Security Heartbeat) depuis Sophos Central
- Exfiltration de la configuration complète de tous les équipements via l'API Sophos Central
- Modification des politiques de sécurité sur plusieurs sites simultanément

Navigation

```
Enregistrement et synchronisation du firewall :
System > Sophos Central > Register with Sophos Central
→ Vérifier que le pare-feu est enregistré et synchronisé
→ Statut de synchronisation : Connected = vert

Dans Sophos Central (portail cloud) :
Admin console > Administration > Admins & Roles
→ Appliquer le principe de moindre privilège pour chaque rôle admin
→ Supprimer les comptes administrateurs inutilisés
Admin console > Administration > API credentials
→ Auditer et révoquer les clés API non utilisées
Admin console > Settings > IP allow-listing (si disponible)
→ Restreindre l'accès au portail Sophos Central aux IP autorisées
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
show sophos-central status
# Résultat attendu : Connected, dernière synchronisation récente
# Vérifier dans l'interface web
# System > Sophos Central > vérifier le statut de connexion et la date de dernière sync
```

Remédiation

1. **MFA Sophos Central (PRIORITÉ ABSOLUE)** : activer le MFA sur tous les comptes administrateurs Sophos Central avec la même priorité que le MFA du pare-feu — un compte Sophos Central sans MFA annule le bénéfice du MFA firewall
2. Naviguer vers `System > Sophos Central` et vérifier que la synchronisation est active et récente
3. Dans le portail Sophos Central, auditer les rôles et droits de chaque administrateur (principe de moindre privilège)
4. Supprimer les comptes administrateurs Sophos Central des personnes ayant quitté l'organisation
5. Configurer l'IP allow-listing dans Sophos Central pour restreindre l'accès au portail aux IP d'administration autorisées
6. Auditer et révoquer les clés API Sophos Central inutilisées (`Admin console > Administration > API credentials`)
7. Surveiller les logs d'audit Sophos Central pour les connexions et modifications inhabituelles
8. Activer les notifications Sophos Central sur les connexions admin depuis de nouveaux appareils ou pays

Valeur par défaut : Intégration Sophos Central non configurée par défaut. MFA Sophos Central non activé par défaut pour les nouveaux comptes.

Critère de conformité : MFA activé pour tous les comptes administrateurs Sophos Central. Principe de moindre privilège appliqué aux rôles. Clés API Sophos Central auditées et rotées. Logs d'audit Sophos Central intégrés dans la supervision SOC.

Contrôle 3.8 — Gestion du cycle de vie des certificats (NOUVEAU — v1.4)

CIS Ref : *(Best practice — PKI & Certificate Management)* | ***MITRE :*** *T1553 (Subvert Trust Controls), T1557 (MITM via certificate)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le certificat auto-signé installé par défaut sur l'interface de gestion et les portails Sophos Firewall génère des avertissements de sécurité dans les navigateurs. Les utilisateurs conditionnés à ignorer ces avertissements sont susceptibles d'accepter également des certificats frauduleux lors d'attaques MitM. Par ailleurs, l'absence de surveillance des dates d'expiration des certificats provoque des indisponibilités inattendues (WebAdmin inaccessible, VPN SSL en erreur) et des ruptures d'inspection SSL/TLS. T1553 couvre les attaques visant à subvertir les mécanismes de confiance des certificats ; T1557 couvre les attaques man-in-the-middle facilitées par des certificats non vérifiés.

Impact potentiel

- T1557 : interception MitM des sessions d'administration si un certificat frauduleux n'est pas détecté par les administrateurs habitués aux avertissements
- T1553 : injection de contenu dans les flux inspectés si le CA d'inspection est compromis ou usurpé
- Indisponibilité soudaine de la WebAdmin, du SSL VPN ou de l'inspection SSL à l'expiration d'un certificat non surveillé
- Non-conformité réglementaire (PCI-DSS Req. 4.2, NIS2 Art. 21) liée à l'utilisation de certificats auto-signés sur des interfaces exposées

Certificat de gestion (WebAdmin)

```
Étape 1 : Créer une CSR depuis le pare-feu
System > Certificates > Certificate signing requests > Add
→ Remplir : Common Name (FQDN de la WebAdmin), Organization, Country
→ Générer la CSR — télécharger le fichier .csr

Étape 2 : Faire signer par la CA de l'organisation
→ Soumettre la CSR à la CA interne (ou CA publique pour les accès externes)
→ Algorithme recommandé : RSA 2048+ ou ECDSA P-384
→ Hash : SHA-256 minimum

Étape 3 : Importer le certificat signé
System > Certificates > Certificates > Add
→ Importer le certificat signé (format PEM ou PKCS#12)
→ Importer la chaîne CA complète

Étape 4 : Assigner à la WebAdmin
System > Administration > Admin and user settings > HTTPS certificate
→ Sélectionner le certificat importé
→ Cliquer sur "Apply"
→ Vérifier l'accès WebAdmin — l'avertissement de certificat doit disparaître
```

CA dédié pour l'inspection SSL/TLS

```
System > Certificates > Authorities > Add
→ Type : Certificate Authority (CA)
→ Algorithm : RSA 2048+ ou ECDSA P-384
→ Common Name : "Sophos SSL Inspection CA — [Organisation]"
→ Validity : 5 ans maximum
→ Garder ce CA DISTINCT du CA de gestion WebAdmin
→ Exporter le CA et le distribuer aux postes clients :
  - Via GPO (Active Directory) pour les postes Windows
  - Via MDM pour les postes mobiles
  - Navigateurs : importer dans le magasin de confiance
Protect > Rules and policies > SSL/TLS inspection rules
→ Sélectionner ce CA dédié dans les règles d'inspection Decrypt
```

Surveillance de l'expiration des certificats

```
System > Certificates > Certificates > [chaque certificat]
→ Colonne "Valid until" : vérifier les dates d'expiration
→ Seuil d'alerte recommandé : 30 jours avant expiration
Configure > System services > Notification list
→ Activer la notification "Certificate expiry warning"
→ Configurer l'envoi vers l'équipe d'administration PKI
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Lister tous les certificats et leurs dates d'expiration
system certificate show

# Vérifier le certificat en cours d'utilisation sur la WebAdmin
show certificate admin

# Vérifier le CA configuré pour l'inspection SSL
show ssl-inspection ca

# Vérification dans l'interface web
# System > Certificates > Certificates
# Vérifier que tous les certificats ont une date "Valid until" > 30 jours
```

Configuration de la vérification CRL (Certificate Revocation List)

```
System > Certificates > Certificates > [certificat] > Advanced settings
→ CRL distribution point : configurer l'URL du CRL de la CA
→ Enable CRL checking : activer
System > Administration > Device Access > HTTPS certificate
→ Vérifier que la vérification de révocation est activée
```

Table des certificats à surveiller

CERTIFICAT	USAGE	NAVIGATION DE VÉRIFICATION	SEUIL D'ALERTE
Certificat WebAdmin		System > Administration > Admin settings	30 jours

CERTIFICAT	USAGE	NAVIGATION DE VÉRIFICATION	SEUIL D'ALERTE
	Interface d'administration HTTPS		
Certificat SSL VPN	Portail VPN utilisateurs	Configure > Remote Access VPN > SSL VPN global settings	30 jours
CA d'inspection SSL	Déchiffrement TLS sortant	System > Certificates > Authorities	90 jours
Certificats WAF	Publications web	Protect > Web Server > Protection > [règle]	30 jours
Certificats IPsec	Tunnels VPN site-à-site	Configure > Site-to-Site VPN > IPsec > [tunnel]	60 jours

Remédiation

1. Inventorier tous les certificats actuellement en service via `System > Certificates > Certificates`
2. Identifier les certificats auto-signés et planifier leur remplacement par des certificats CA-signés
3. Créer une CSR depuis `System > Certificates > Certificate signing requests` pour la WebAdmin
4. Faire signer par la CA interne de l'organisation (ou CA publique Let's Encrypt pour les accès publics)
5. Importer et assigner le certificat signé à la WebAdmin (`System > Administration > Admin and user settings > HTTPS certificate`)
6. Créer un CA dédié à l'inspection SSL dans `System > Certificates > Authorities` — ne pas réutiliser le CA d'administration
7. Distribuer le CA d'inspection SSL aux postes clients via GPO (Active Directory)
8. Configurer les alertes d'expiration 30 jours avant dans `Configure > System services > Notification list`
9. Activer la vérification CRL pour les certificats critiques
10. Créer un calendrier de renouvellement des certificats dans le registre de gestion des actifs (CMDB)
11. Documenter les autorités de certification utilisées et les procédures de renouvellement

Valeur par défaut : Certificats auto-signés générés à l'installation sur toutes les interfaces. Aucune surveillance d'expiration configurée par défaut.

Critère de conformité : Aucun certificat auto-signé sur les interfaces exposées (WebAdmin, SSL VPN, WAF). CA dédié à l'inspection SSL distinct du CA d'administration. Alertes d'expiration 30 jours configurées. Commande `system certificate show` ne retourne aucun certificat expiré ou expirant dans moins de 30 jours.

Domaine 4 — Règles et politiques de protection

Objectif : *S'assurer que les règles de pare-feu n'exposent pas de services dangereux depuis la zone WAN, que l'identification utilisateur est activée, et que les règles intègrent des profils de sécurité complets. Identifier et remédier les configurations Any-Any-Any permissives.*

Contrôle 4.1 — Aucune règle ANY/ANY/ANY depuis la zone WAN

CIS Ref : *5.10* | ***MITRE :*** *T1190* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Une règle de pare-feu autorisant tout trafic (source ANY, service ANY, destination ANY) depuis la zone WAN est équivalente à l'absence de pare-feu. Ce type de règle, parfois créé à des fins de dépannage et oublié, offre un accès illimité à l'ensemble du réseau interne depuis Internet. Le Health Check Sophos v22 inclut explicitement la détection des configurations Any-Any-Any comme vérification MEDIUM severity avec obligation de les signaler et remédier.

Impact potentiel

- Accès non restreint à tous les services internes depuis Internet
- Exploitation triviale de tout service exposé sans nécessiter de vulnérabilité spécifique
- Non-conformité immédiate avec toute réglementation de sécurité (NIS2, RGPD, PCI-DSS)

Navigation

```
Protect > Rules and policies > Firewall rules
→ Passer en revue toutes les règles avec source zone = WAN
→ Identifier les règles avec Source = ANY, Service = ANY, Destination = ANY
→ Supprimer ou restreindre ces règles immédiatement
→ Utiliser le Firewall Health Check (Dashboard) pour identifier automatiquement
  les règles permissives signalées par Sophos
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
show firewall-rule
# Rechercher les règles avec source "Any" sur zone WAN
```

Remédiation

1. Naviguer vers `Protect > Rules and policies > Firewall rules`
2. Filtrer par zone source = WAN
3. Identifier toutes les règles avec source ANY, service ANY et/ou destination ANY

4. Supprimer ces règles ou les remplacer par des règles spécifiques avec des services et destinations explicitement définis
5. Documenter les raisons de chaque règle WAN autorisée
6. Vérifier le Firewall Health Score pour confirmer l'absence de règles permissives signalées

Valeur par défaut : Aucune règle ANY/ANY/ANY dans la configuration d'usine.

Critère de conformité : Aucune règle active avec Source = ANY, Service = ANY, Destination = ANY depuis la zone WAN.

Contrôle 4.2 — Bloquer SMB (445) et RDP (3389) depuis la zone WAN

> ***CIS Ref :*** *5.8* | ***MITRE :*** *T1021, T1190* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Les ports SMB (445) et RDP (3389) sont les vecteurs d'entrée les plus exploités dans les attaques de ransomware et les compromissions initiales documentées par CISA et l'ANSSI. SMB expose des vulnérabilités comme EternalBlue (MS17-010) encore activement exploitées. RDP est la cible principale des campagnes de brute force massives visibles sur Shodan.

Impact potentiel

- Exploitation de EternalBlue ou de vulnérabilités SMB pour la propagation de ransomware
- Compromission par force brute ou exploitation RDP (BlueKeep, DejaBlue)
- Accès direct aux serveurs internes Windows sans authentification supplémentaire

Navigation

```
Protect > Rules and policies > Firewall rules
→ Vérifier qu'aucune règle n'autorise le port 445 (SMB) depuis la zone WAN
→ Vérifier qu'aucune règle n'autorise le port 3389 (RDP) depuis la zone WAN
→ Ajouter des règles de blocage explicites si nécessaire
→ Également bloquer : Netbios (137, 138, 139), Telnet (23), FTP (21)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
show firewall-rule
# Vérifier l'absence de règles autorisant le port 445 et 3389 depuis WAN
```

Remédiation

1. Auditer toutes les règles de pare-feu avec zone source WAN
2. S'assurer qu'aucune règle n'autorise les ports 445, 3389, 137-139, 23, 21 depuis WAN
3. Créer des règles de blocage explicites avec logging pour ces ports si des règles permissives existent
4. Pour les accès RDP légitimes, utiliser le VPN SSL ou IPSec comme tunnel sécurisé
5. Vérifier également les règles NAT qui pourraient rediriger ces ports vers des serveurs internes

Valeur par défaut : Aucune règle permissive pour ces ports dans la configuration d'usine.

Critère de conformité : Ports 445, 3389, 137-139 inaccessibles directement depuis la zone WAN. Accès distant uniquement via VPN.

Contrôle 4.3 — Identification utilisateur sur les règles de pare-feu

> ***CIS Ref :*** *2.1* | ***MITRE :*** *T1078* | ***Niveau :*** 🔵 *L2*

Description du risque

Les règles de pare-feu basées uniquement sur les adresses IP ne permettent pas d'identifier quel utilisateur est à l'origine d'un trafic donné. En cas d'incident, l'investigation forensique est limitée à des adresses IP dynamiques (DHCP) qui peuvent avoir changé de mains depuis l'événement. L'identification utilisateur permet des règles plus granulaires et une meilleure traçabilité.

Impact potentiel

- Impossibilité d'identifier l'utilisateur responsable d'un incident de sécurité
- Règles de politique moins granulaires basées sur IP et non sur l'identité
- Difficulté de forensique en environnement DHCP avec baux courts

Navigation

```
Protect > Rules and policies > Firewall rules > Éditer une règle
→ Section "Identity" : cocher "Match known users"
→ Ajouter les utilisateurs/groupes autorisés
→ Cocher "Use web authentication for unknown users" (captive portal)
→ Cocher "Log firewall traffic" pour le trafic autorisé
Configure > Authentication > Services > Firewall authentication methods
→ Configurer le serveur AD/LDAP principal en priorité haute
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Rules and policies > Firewall rules
# Vérifier que les règles critiques ont "Match known users" activé
```

Remédiation

1. Intégrer le firewall avec l'Active Directory via STAS (Sophos Transparent Authentication Suite) ou Kerberos/NTLM
2. Éditer les règles LAN-to-WAN pour activer `Match known users`
3. Configurer le captive portal pour les utilisateurs inconnus
4. Activer `Log firewall traffic` sur toutes les règles autorisant du trafic
5. Tester la correspondance utilisateur avec un compte de test AD

Valeur par défaut : Identification utilisateur non configurée par défaut.

Critère de conformité : Règles de pare-feu vers Internet configurées avec `Match known users`. Intégration AD/LDAP opérationnelle.

Contrôle 4.4 — Score de santé du pare-feu (Firewall Health Check)

CIS Ref : *5.11* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

Le Firewall Health Check Score de Sophos est un indicateur agrégé qui évalue la posture de sécurité de l'équipement sur la base de 32 vérifications CIS-alignées (Health Check officiel Sophos v22). Un score dégradé signale des écarts par rapport aux bonnes pratiques qui peuvent indiquer une mauvaise configuration ou une dérive de sécurité. Note importante : "les coches vertes ne garantissent pas la sécurité" — le Health Check avertit sur les risques contextuels tels que les règles mal priorisées ou les politiques TLS non testées.

Impact potentiel

- Non-détection de dérives de configuration critiques affectant la posture de sécurité
- Absence de mécanisme de surveillance automatique de la conformité
- Accumulation de mauvaises pratiques sans indicateur d'alerte

Navigation

```
Dashboard > Security > Firewall Health
→ Vérifier le score global (cible : Optimal ou Good)
→ Examiner les 32 recommandations listées (HIGH, MEDIUM, LOW severity)
→ Corriger les points en statut "Warning" ou "Critical"
→ Prioriser les vérifications HIGH severity en premier
```

CLI de vérification

```
# Vérification dans l'interface web Dashboard
# Rechercher la section "Firewall Health" ou "Security"
system diagnostics show version
```

Remédiation

1. Naviguer vers le `Dashboard > Security > Firewall Health`
2. Passer en revue chaque recommandation en statut dégradé (priorité HIGH > MEDIUM > LOW)
3. Appliquer les remédiations suggérées par le système
4. Vérifier que le score atteint le niveau `Optimal` après correction
5. Planifier une revue mensuelle du Firewall Health Score
6. Ne pas se fier uniquement aux indicateurs verts — vérifier le contexte de chaque contrôle

Valeur par défaut : Score calculé dynamiquement selon la configuration.

Critère de conformité : Firewall Health Score = `Optimal` ou `Good`. Aucun point en statut `Critical`. Revue mensuelle tracée.

Contrôle 4.5 — Règles avec profils de sécurité complets attachés

CIS Ref : *5.4, 5.6* | ***MITRE :*** *T1071* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Une règle de pare-feu qui autorise du trafic sans profils IPS, antivirus, web filtering et application control attachés laisse passer du trafic malveillant non inspecté. Les règles autorisant le trafic Internet sans profils de protection sont équivalentes à des règles de NAT sans inspection de contenu. Le Health Check Sophos v22 vérifie explicitement la présence de Web policies et d'Application control policies dans les règles de pare-feu.

Impact potentiel

- Propagation de malwares via des flux non inspectés
- Exfiltration de données via des canaux non filtrés (C2 HTTPS, DNS)
- Exploitation de vulnérabilités applicatives sur des flux non couverts par IPS

Navigation

```
Protect > Rules and policies > Firewall rules > Éditer une règle
→ Security features > Intrusion prevention : sélectionner un profil IPS
→ Security features > Malware scanning : activer avec profil AV
→ Security features > Web policy : sélectionner une politique web
→ Security features > Application control : sélectionner un profil
→ Security features > Zero-day protection : activer si abonnement disponible
→ Logging > Log firewall traffic : cocher
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Rules and policies > Firewall rules
# Vérifier que chaque règle Internet a des profils de sécurité attachés
```

Remédiation

1. Auditer toutes les règles autorisant du trafic vers Internet ou entre zones
2. Attacher un profil IPS, AV, Web Policy et Application Control à chaque règle
3. Activer Zero-day protection (Sandstorm) sur les règles traitant les téléchargements de fichiers
4. Activer le logging sur toutes les règles autorisant du trafic
5. Créer des profils de sécurité progressifs (basique pour les utilisateurs, strict pour les serveurs)

Valeur par défaut : Profils de sécurité non attachés par défaut sur les nouvelles règles.

Critère de conformité : Toutes les règles autorisant du trafic vers Internet ou entre zones de sécurité différentes ont des profils IPS, AV, Web Policy et Application Control attachés.

Contrôle 4.6 — Vérifications avancées de l'architecture Xstream v2 (NOUVEAU — SFOS v22)

CIS Ref : *(Architecture Xstream v2 Sophos)* | ***MITRE :*** *T1055, T1562.001* | ***Niveau :*** 🔵 *L2*

Description du risque

L'architecture Xstream v2 de SFOS v22 offre des garanties de sécurité supérieures par rapport aux architectures monolithiques traditionnelles grâce à la conteneurisation des moteurs de protection et la séparation des privilèges. Vérifier que ces mécanismes sont opérationnels est essentiel : un IPS non conteneurisé ou un moteur de paquets mal configuré réduit la posture de sécurité à celle d'un pare-feu classique sans les protections avancées de la v22.

Impact potentiel

- Un IPS non conteneurisé expose le système d'exploitation hôte du pare-feu à une compromission directe via une vulnérabilité du moteur d'inspection (T1055 — Process Injection), permettant à un attaquant de désactiver les protections depuis l'intérieur.
- L'absence de séparation de privilèges entre les services Xstream permet à un service compromis (proxy web, moteur AV) d'escalader vers root et de modifier la configuration du pare-feu ou d'exfiltrer les secrets d'autres services (T1562.001 — Disable or Modify Tools).
- Un moteur de paquets mal configuré ou non vérifié peut créer des angles morts d'inspection (trafic contournant le DPI sur les flux haute vitesse ASIC), permettant à des charges malveillantes de traverser le périmètre sans être analysées.

Description de l'architecture Xstream v2

L'architecture Xstream v2 repose sur trois piliers de sécurité distincts et vérifiables :

1. **IPS conteneurisé** : le moteur IPS s'exécute dans un conteneur système isolé. Une vulnérabilité exploitée dans le moteur IPS (via une signature malformée ou un exploit d'échappement) ne peut pas se propager au système d'exploitation du pare-feu. C'est une défense directe contre T1055 (Process Injection).
2. **Séparation de privilèges complète** : aucun service applicatif (IPS, AV, proxy web, moteur email) n'a d'accès root au système hôte. Les services opèrent chacun avec les privilèges minimaux nécessaires à leur fonction. Un service compromis ne peut pas modifier la configuration système ou accéder aux secrets stockés par un autre service.
3. **Traitement des paquets hybride** : l'inspection du trafic est répartie entre les CPUs généralistes (deep inspection, déchiffrement TLS), les processeurs ASIC de flux (inspection légère, haute vitesse), et les CPUs virtuels (traitement élastique). Cette architecture garantit la continuité de l'inspection même lors de pics de charge et évite les contournements basés sur la saturation d'un seul moteur d'inspection.

Navigation / CLI de vérification

```
Vérification du service IPS conteneurisé :
  System > Diagnostics > Services
  → IPS service : statut = Running
  → Confirmer que l'IPS apparaît comme service isolé (non intégré au processus principal)

Vérification de l'inspection SSL/TLS Xstream :
  Protect > Rules and policies > SSL/TLS inspection rules
  → Confirmer qu'au moins une règle avec action "Decrypt" est active et affectée aux règles
LAN-to-WAN

Vérification du mode de traitement des paquets :
  System > Administration > Device access
  → Mode du moteur de paquets : vérifier la configuration selon le matériel (XGS = ASIC
actif)
```

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier les processus IPS conteneurisés
ps aux | grep ips
# Vérifier les services actifs et leur isolation
system diagnostics show services
# Vérifier le statut général de l'architecture
system diagnostics show summary
```

Remédiation

1. Vérifier que la version SFOS v22 est installée — l'architecture Xstream v2 est disponible exclusivement sur v22 et supérieur
2. Confirmer le statut opérationnel du service IPS via `System > Diagnostics > Services`
3. Activer l'inspection SSL/TLS Xstream (voir contrôle 8.1) pour bénéficier du déchiffrement accéléré par l'architecture Xstream
4. Sur les équipements XGS-Series : vérifier que le co-processeur ASIC est actif pour le traitement des flux non chiffrés (amélioration de performance sans dégradation de l'inspection)
5. Pour les déploiements HA : s'assurer que les deux nœuds sont sur SFOS v22 pour bénéficier de la même architecture sur le nœud passif en cas de basculement
6. Documenter la version d'architecture dans le registre de configuration de l'équipement

Valeur par défaut : Architecture Xstream v2 active par défaut sur SFOS v22. Les services sont conteneurisés automatiquement.

Critère de conformité : SFOS v22 installé. Service IPS en statut Running et conteneurisé. Inspection SSL/TLS Xstream active. Sur XGS-Series : co-processeur ASIC opérationnel confirmé dans les diagnostics.

Contrôle 4.7 — Sophos Firewall Health Check Continu — 32 vérifications CIS-alignées (NOUVEAU — SFOS v22)

CIS Ref : *(Sophos Health Check v22 — toutes vérifications)* | ***MITRE :*** *T1562 (Impair Defenses — détecter les lacunes)* | ***Niveau :*** 🟢 *L1*

Description du risque

Le Sophos Firewall Health Check est un outil de conformité intégré dans SFOS v22 qui évalue automatiquement la posture de sécurité selon 32 vérifications alignées sur le CIS Benchmark. Chaque vérification fournit un lien de navigation directe (remédiation en un clic) vers le paramètre à corriger. Ne pas consulter régulièrement ce Health Check revient à ne pas surveiller la dérive de configuration de son pare-feu.

AVERTISSEMENT CRITIQUE : “Les coches vertes ne garantissent pas la sécurité” — le Health Check identifie les configurations risquées mais ne peut pas évaluer tous les contextes métier. Des risques contextuels comme les règles mal priorisées, les politiques TLS non testées, ou les exclusions non documentées nécessitent toujours un examen humain par un expert.

Impact potentiel

- La dérive silencieuse de configuration (ex. : MFA désactivé suite à une mise à jour, règle Any-Any-Any introduite accidentellement) passe inaperçue sans Health Check régulier, exposant l’organisation à des compromissions évitables (T1562 — Impair Defenses).
- L’absence de suivi des 15 vérifications HIGH laisse des failles critiques non corrigées — notamment l’absence de MFA sur WebAdmin ou l’accès WAN à l’interface d’administration, portes d’entrée directes pour les attaquants.
- Sans Health Check, il est impossible de justifier la posture de sécurité du pare-feu lors d’un audit de conformité (PCI-DSS, NIS2, ISO 27001), exposant l’organisation à des sanctions ou à la suspension de certifications.

Navigation

```
Dashboard > Firewall Health > Health Check
→ Vue d'ensemble des 32 vérifications avec statut (vert/orange/rouge)
→ Cliquer sur chaque vérification en échec pour accéder directement au paramètre à corriger
→ Filtrer par sévérité : HIGH, MEDIUM, LOW
```

Les 32 vérifications du Health Check Sophos v22 — Détail complet

Vérifications HIGH (priorité immédiate)

#	VÉRIFICATION	NAVIGATION DIRECTE
HC-H1	Security Heartbeat activé sur les règles LAN	Protect > Rules > Firewall rules
HC-H2	Hotfix automatique activé	System > Backup & Firmware
HC-H3	Gestion des sessions active (timeout configuré)	System > Administration > Admin settings
HC-H4	Mot de passe admin ≥ 14–16 caractères	System > Administration > Admin settings
HC-H5	Mot de passe utilisateurs ≥ 12 caractères	System > Administration > Admin settings
HC-H6	MFA activé pour le VPN distant	Configure > Authentication > MFA

#	VÉRIFICATION	NAVIGATION DIRECTE
HC-H7	MFA activé pour la console WebAdmin	Configure > Authentication > MFA
HC-H8	IPS activé et en mode Block sur les règles	Protect > Intrusion Prevention > IPS Policies
HC-H9	Inspection SSL/TLS activée (mode Decrypt)	Protect > Rules > SSL/TLS inspection rules
HC-H10	Flux X-Ops Threat Intelligence activés	Protect > Active Threat Response > X-Ops Feeds
HC-H11	Flux MDR Threat Feeds activés (si abonnement)	Protect > Active Threat Response > MDR Feeds
HC-H12	Clés SSH configurées pour l'authentification admin	System > Administration > Device Access > SSH
HC-H13	Accès WebAdmin bloqué depuis la zone WAN	System > Administration > Device Access > Local service ACL
HC-H14	MFA activé pour le compte admin par défaut	System > Administration > Device Access
HC-H15	Mises à jour des patterns toutes les 15 minutes	System > Backup & Firmware > Pattern Updates

Vérifications MEDIUM (action sous 7 jours)

#	VÉRIFICATION	NAVIGATION DIRECTE
HC-M1	Synchronisation App Control configurée	Protect > Application Filter
HC-M2	NDR Essentials activé	Protect > Active Threat Response > NDR Essentials
HC-M3	Serveur d'authentification avec chiffrement SSL/TLS	Configure > Authentication > Servers
HC-M4	Politiques Web actives sur les règles	Protect > Web > Policies
HC-M5	Application Control actif sur les règles	Protect > Application Filter
HC-M6	Aucune règle Any-Any-Any détectée	Protect > Rules and policies > Firewall rules
HC-M7	Synchronisation Sophos Central active	System > Sophos Central

Vérifications LOW (bonnes pratiques)

#	VÉRIFICATION	NAVIGATION DIRECTE
HC-L1	Bannière de connexion (disclaimer) configurée	System > Administration > Admin settings
HC-L2	Sauvegardes planifiées actives	System > Backup & Firmware > Backup
HC-L3	Notifications email configurées	System > Administration > Notification settings
HC-L4	Synchronisation NTP active	System > Administration > Time

Remédiation par sévérité

1. **Hebdomadaire** : consulter le Health Check (`Dashboard > Firewall Health > Health Check`) et corriger tous les points HIGH en statut Warning
2. **Toutes les 2 semaines** : traiter les vérifications MEDIUM en statut Warning
3. **Mensuelle** : traiter les vérifications LOW et documenter les exceptions contextuelles justifiées
4. Utiliser la remédiation en un clic (liens directs depuis chaque vérification) pour corriger rapidement
5. **Ne pas se fier uniquement au score vert** : documenter toute exception avec sa justification business
6. Inclure le résultat du Health Check dans le rapport mensuel de sécurité du pare-feu
7. Déclencher une revue non planifiée du Health Check après toute modification significative de la configuration

CLI de vérification

```
# Accéder au Health Check via l'interface web uniquement
# Dashboard > Firewall Health > Health Check
# Vérifier que le score global est "Optimal" ou "Good"
# Depuis l'Advanced Shell, vérifier la version pour confirmer la disponibilité du Health Check v22
system diagnostics show version
# Résultat attendu : SFOS version 22.x.x
```

Valeur par défaut : Health Check disponible et calculé automatiquement. Score initial variable selon la configuration d'usine.

Critère de conformité : Health Check consulté au minimum hebdomadairement. Aucune vérification HIGH en statut Warning non adressé. Exceptions documentées avec justification business. Résultat inclus dans le rapport mensuel de sécurité.

Domaine 5 — Profils de protection (IPS, AV, Web, App, Email)

Objectif : *Configurer les profils de protection avec des paramètres bloquants pour les menaces critiques, couvrir les flux web (y compris l'authentification du proxy Kerberos SSO), les applications, l'email et la WAF pour les applications exposées. Déployer une protection cohérente contre les vecteurs d'attaque OWASP Top 10, phishing, exfiltration et utilisation abusive du proxy.*

Contrôle 5.1 — Profil IPS avec signatures critiques/élevées en mode Block

CIS Ref : *5.4* | ***MITRE :*** *T1190, T1210* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Un profil IPS configuré en mode `Log` uniquement détecte les exploits sans les bloquer. Les signatures classifiées `Critical` et `High` correspondent à des exploits activement utilisés dans des campagnes réelles. Ne pas les bloquer revient à avoir une alarme incendie sans sprinklers. En SFOS v22, l'IPS s'exécute dans un conteneur isolé (architecture Xstream v2) offrant une séparation de privilèges complète, ce qui renforce la sécurité même si une signature déclenche un faux positif.

Impact potentiel

- Exploitation réussie de vulnérabilités réseau malgré la détection IPS (mode Log only)
- Compromission de serveurs via des exploits connus non bloqués
- Fausse impression de protection sans efficacité opérationnelle réelle

Navigation

```
Protect > Intrusion Prevention > IPS Policies > Éditer ou créer un profil
→ Pour chaque catégorie de signatures :
  - Severity Critical : Action = Drop, Log = Enabled
  - Severity High : Action = Drop, Log = Enabled
  - Severity Medium : Action = Drop (ou Alert selon contexte), Log = Enabled
→ Attacher ce profil aux règles de pare-feu concernées
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Intrusion Prevention > IPS Policies
# Vérifier que les règles Critical et High sont en mode "Drop"
```

Remédiation

1. Naviguer vers `Protect > Intrusion Prevention > IPS Policies`
2. Créer ou éditer le profil IPS principal

3. Configurer toutes les signatures `Critical` en action `Drop` avec logging
4. Configurer toutes les signatures `High` en action `Drop` avec logging
5. Configurer les signatures `Medium` en `Drop` ou `Alert` selon la tolérance opérationnelle
6. Appliquer ce profil à toutes les règles de pare-feu traitant du trafic entrant depuis WAN

Valeur par défaut : Profil IPS par défaut souvent configuré en mode Alert/Log uniquement.

Critère de conformité : Profil IPS actif sur les règles Internet. Signatures Critical et High en action `Drop` avec logging activé.

Contrôle 5.2 — Web Policy — catégories malveillantes bloquées

CIS Ref : *5.1* | ***MITRE :*** *T1566, T1071* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le filtrage de catégories web bloque les accès aux sites de phishing, malwares, C2 (Command & Control), et contenu inapproprié. Sans cette politique, les utilisateurs peuvent accéder à des sites infectés ou à des infrastructures de commande et contrôle depuis le réseau interne, facilitant les infections et les exfiltrations.

Impact potentiel

- Accès non contrôlé à des sites de phishing et de distribution de malwares
- Communication avec des serveurs C2 depuis des endpoints infectés
- Exfiltration de données via des canaux web non filtrés

Navigation

```
Protect > Web > Policies > Créer ou éditer une politique web
→ Activer "Malware and content scanning" (Scan HTTP and HTTPS)
→ Bloquer les catégories : Malware, Phishing & Fraud, Spam URLs,
  Anonymizers/Proxies, Hacking/Computer crimes
→ Activer "Block URLs with a bad reputation score"
→ Attacher la politique aux règles de pare-feu concernées
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Web > Policies
# Vérifier les catégories bloquées dans la politique active
```

Remédiation

1. Naviguer vers `Protect > Web > Policies`
2. Créer une politique web avec blocage des catégories malveillantes (Malware, Phishing, Spam URLs, Anonymizers, Hacking)
3. Activer le scan des flux HTTP et HTTPS (nécessite l'inspection SSL pour HTTPS)
4. Activer le blocage basé sur la réputation d'URL (Sophos X-Ops)

5. Attacher la politique à toutes les règles LAN-to-WAN

Valeur par défaut : Politique web non configurée par défaut.

Critère de conformité : Politique web active sur les règles Internet, catégories Malware et Phishing bloquées, scan HTTP/HTTPS activé.

Contrôle 5.3 — Filtrage applicatif — applications à risque élevé bloquées

CIS Ref : *5.3* | ***MITRE :*** *T1071, T1048* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Les applications classifiées niveau de risque 4 et 5 (High Risk, Very High Risk) dans Sophos incluent les outils d'anonymisation, les P2P, les applications de contournement, et d'autres catégories associées à des comportements malveillants. Leur blocage réduit la surface d'exfiltration et empêche l'utilisation d'outils d'évasion.

Impact potentiel

- Utilisation de proxies et VPN non autorisés pour contourner les politiques de sécurité
- Exfiltration via des canaux P2P ou applicatifs non supervisés
- Accès à des ressources non autorisées via des applications de contournement

Navigation

```
Protect > Application Filter > Créer ou éditer un profil
→ Risk level 4 (High Risk) : Action = Block
→ Risk level 5 (Very High Risk) : Action = Block
→ Attacher le profil aux règles de pare-feu Internet
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Application Filter
# Vérifier que les niveaux de risque 4 et 5 sont en mode Block
```

Remédiation

1. Naviguer vers `Protect > Application Filter`
2. Créer un profil bloquant les applications de risque niveau 4 et 5
3. Examiner les exceptions légitimes et les documenter (ex : certains VPN d'entreprise)
4. Appliquer le profil aux règles de pare-feu Internet
5. Revoir trimestriellement les nouvelles applications ajoutées à la base Sophos

Valeur par défaut : Filtrage applicatif non configuré par défaut.

Critère de conformité : Profil d'application actif. Applications de risque 4 et 5 bloquées. Exceptions documentées.

Contrôle 5.4 — Protection Email complète — SPF/DKIM/DMARC, BATV, sandboxing et DLP (ENRICHI)

CIS Ref : *5.6* | ***MITRE :*** *T1566 (Phishing), T1534 (Internal Spearphishing), T1048 (Exfiltration Over Alternative Protocol)* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le phishing par email est le vecteur d'attaque initial le plus utilisé dans les compromissions de systèmes d'information (source : Sophos Threat Report 2026, ANSSI). La protection email sur le pare-feu ajoute une couche de filtrage en amont des clients de messagerie. SFOS v22 offre une protection multicouche incluant l'authentification des expéditeurs (SPF/DKIM/DMARC), la protection contre le backscatter (BATV), le sandboxing des pièces jointes, la protection click-time des URL, et la prévention des fuites de données (DLP) sur les emails sortants.

Impact potentiel

- T1566 : compromission initiale par ransomware via pièce jointe malveillante non filtrée (Sandstorm non activé)
- T1566 : vol de credentials via des liens de phishing non bloqués (URL click-time protection non activée)
- T1534 : propagation interne via des campagnes de spear-phishing utilisant des comptes compromis
- T1048 : exfiltration de données sensibles via email sortant non contrôlé par DLP
- Backscatter spam généré par des rebonds d'emails falsifiés en l'absence de BATV

Navigation — Configuration complète

```
Protect > Email > Policy > Add policy (ou éditer la politique existante)

Section Antispam :
→ Antispam : activer avec action = Reject (expéditeurs connus malveillants)
  ou Quarantine (suspects) — NE PAS utiliser "Allow" pour le spam
→ Greylisting : activer pour les expéditeurs inconnus
  (retard temporaire qui élimine ~90% du spam de bots)

Section Authentification expéditeurs :
→ SPF (Sender Policy Framework) : activer — Verify SPF records
  - Action si SPF = Fail : Reject
  - Action si SPF = SoftFail : Quarantine
→ DKIM (DomainKeys Identified Mail) : activer — Verify DKIM signatures
  - Action si DKIM = Fail : Quarantine
→ DMARC (Domain-based Message Authentication, Reporting & Conformance) :
  - Activer la vérification DMARC
  - Respecter la politique DMARC publiée (p=quarantine → Quarantine, p=reject → Reject)
→ BATV (Bounce Address Tag Validation) : activer
  - Protège contre le backscatter spam (emails de rebond falsifiés)
  - Sophos SFOS signe les emails sortants avec BATV et vérifie les rebonds entrants

Section Antivirus et pièces jointes :
→ Antivirus : activer le scan des pièces jointes — action = Quarantine
→ Sandbox (Zero-day protection) : activer pour les pièces jointes suspectes
  - Types de fichiers prioritaires : .exe, .js, .doc, .docx, .xls, .xlsm, .pdf, .zip
  - Mode : analyse comportementale en environnement isolé (Sandstorm)
  - NE PAS exclure de types de fichiers

Section Anti-phishing :
→ URL click-time protection : activer
  - Réécriture des URL dans les emails pour inspection au moment du clic
  - Bloque les liens vers des domaines de phishing détectés au moment du clic
→ Anti-phishing engine : activer

Section DLP (Data Loss Prevention — emails sortants) :
→ Data Loss Prevention : activer sur la politique de routage sortant
→ Patterns à détecter : PCI-DSS (numéros de cartes), PII (numéros de sécurité sociale, etc.)
→ Action : Quarantine (admin review) ou Block selon la politique de l'organisation
→ Protect > Email > Data control : configurer les règles DLP

→ Attacher la politique au profil de routage email
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Email > Policies
# Vérifier que SPF, DKIM, DMARC et BATV sont activés
# Protect > Email > Data control
# Vérifier que les règles DLP sont configurées pour les flux sortants
```

Table de configuration SPF/DKIM/DMARC recommandée

MÉCANISME	ACTIVATION	ACTION SI FAIL	COUVERTURE
SPF	Obligatoire	Reject (Hard Fail) / Quarantine (SoftFail)	Usurpation du domaine expéditeur
DKIM	Obligatoire	Quarantine	Intégrité de l'email et authenticité du domaine
DMARC	Obligatoire	Respecter la politique publiée (p=)	Alignement SPF+DKIM, reporting
BATV	Recommandé	Reject (rebonds invalides)	Backscatter spam, protection contre l'usurpation de rebonds
Greylisting	Recommandé	Délai (pas de blocage)	90% des spams de bots sans faux positifs

Remédiation

1. Naviguer vers `Protect > Email > Policy`
2. Activer l'antispam avec action `Reject` pour les connus malveillants et `Quarantine` pour les suspects
3. Activer le greylisting pour les expéditeurs inconnus
4. Activer la vérification SPF avec action `Reject` pour les Hard Fails
5. Activer la vérification DKIM avec action `Quarantine` pour les échecs de signature
6. Activer la vérification DMARC et respecter la politique publiée par le domaine de l'expéditeur
7. Activer BATV pour protéger contre le backscatter spam
8. Activer Zero-day protection (Sandstorm) pour toutes les pièces jointes sans exclusion
9. Activer l'URL click-time protection pour les liens dans les emails
10. Configurer les règles DLP sur les emails sortants (`Protect > Email > Data control`) pour détecter PCI-DSS, PII
11. Configurer les notifications de quarantaine pour les utilisateurs (résumé quotidien) et les administrateurs (alertes immédiates)
12. Tester la configuration avec des emails de validation SPF/DKIM/DMARC (outils en ligne : mail-tester.com)

Valeur par défaut : Protection email non configurée par défaut. SPF/DKIM/DMARC désactivés par défaut.

Critère de conformité : Politique email active avec antispam (action Reject/Quarantine), SPF activé (Reject sur HardFail), DKIM activé, DMARC activé (politique respectée), BATV activé, Zero-day protection activée sans exclusion de types de fichiers, URL click-time protection activée, DLP configuré sur les flux sortants.

Contrôle 5.5 — WAF pour les applications web exposées — couverture OWASP Top 10 (ENRICHI)

CIS Ref : *5.5* | ***MITRE :*** *T1190 (Exploit Public-Facing Application), T1059 (Command and Script Interpreter), T1190* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les applications web exposées sur Internet (portails RH, CRM, ERP en mode SaaS interne) sont des cibles privilégiées pour les attaques OWASP Top 10. La WAF Sophos offre une protection en amont des serveurs applicatifs en bloquant ces vecteurs d'attaque avant qu'ils n'atteignent l'application. Un déploiement correct nécessite une phase de monitoring initiale pour identifier les faux positifs, suivie du passage en mode blocage.

Impact potentiel

- T1190 : compromission de serveurs web via injection SQL (OWASP A03), XSS (OWASP A07) ou CSRF
- Exfiltration de bases de données via des injections SQL non bloquées (OWASP A03)
- Déni de service applicatif via des attaques ciblées sur les endpoints REST/API
- Contournement d'authentification via des vulnérabilités de contrôle d'accès non bloquées (OWASP A01)

Couverture OWASP Top 10 par la WAF Sophos

OWASP 2021	RISQUE	PROTECTION WAF SOPHOS
A01 — Broken Access Control	Contournement d'autorisation	Form Hardening, règles applicatives
A02 — Cryptographic Failures	Exposition de données sensibles	HTTPS redirect forcé, TLS obligatoire
A03 — Injection (SQL, LDAP, etc.)	Compromission de base de données	SQL Injection Protection (activé)
A04 — Insecure Design	Défauts de conception	Politiques personnalisées
A05 — Security Misconfiguration	Exposition de configs par défaut	Common Threat Filter
A06 — Vulnerable Components	Exploitation de libs vulnérables	IPS + WAF en complément
A07 — XSS	Injection de scripts malveillants	XSS Protection (activé)
A08 — Software/Data Integrity Failures	Falsification de données	Cookie Signing, Form Hardening
A09 — Security Logging Failures	Contournement de traçabilité	Logs WAF activés
A10 — SSRF	Requêtes forgées côté serveur	Règles de filtrage des destinations

Navigation — Configuration WAF complète

```
Étape 1 : Créer la politique WAF
Protect > Web Server > Protection > Add Protection Policy
→ Nom : "WAF-[NOM-APPLICATION]-v1"
→ Mode : Monitor (PHASE 1 — baseline de 1 à 2 semaines)
→ Common Threat Filter : activer — protection contre les scans et outils automatisés
→ Application Attack Protection :
  - SQL Injection Protection : activer
  - XSS (Cross-Site Scripting) Protection : activer
  - Cookie Signing : activer (protection contre la falsification de cookies)
  - Form Hardening : activer (protection contre la manipulation des formulaires)
→ Enregistrer la politique

Étape 2 : Créer la règle de publication web
Protect > Rules and policies > Firewall rules > Add firewall rule
→ Type : Business application rule
→ Application template : Web server (HTTPS)
→ Protocole : HTTPS uniquement
→ Redirection HTTP → HTTPS : activer
  (forcer tous les accès HTTP sur le port 80 vers HTTPS port 443)
→ Certificat TLS : sélectionner un certificat valide (CA de confiance, non auto-signé)
→ Politique WAF : sélectionner la politique créée à l'étape 1

Étape 3 : Après la baseline (1-2 semaines en mode Monitor)
→ Analyser les logs WAF pour identifier les faux positifs
→ Créer des règles d'exception pour les faux positifs légitimes
→ Basculer la politique en mode Protection (blocage)

Étape 4 : Surveillance continue
Protect > Web Server > Logs / Reports
→ Revoir les logs WAF hebdomadairement
→ Affiner les règles selon les nouvelles menaces
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Web Server > Protection
# Vérifier que les politiques WAF sont en mode Protection (pas Monitor) — après la phase baseline
# Vérifier que HTTPS redirect est activé sur toutes les règles de publication web
# Vérifier que les certificats TLS sont valides et non expirés
```

Remédiation

1. **Phase 1 — Monitor** : déployer la politique WAF en mode `Monitor` et laisser tourner 1 à 2 semaines pour collecter une baseline des faux positifs
2. **Analyse** : analyser les logs WAF (`Protect > Web Server > Logs`) et identifier les requêtes légitimes bloquées
3. **Exceptions** : créer des règles d'exception documentées pour les faux positifs légitimes
4. **Phase 2 — Protection** : basculer en mode `Protection` (blocage) après validation de la baseline
5. Activer SQL Injection Protection et XSS Protection dans la politique WAF
6. Activer `Cookie Signing` et `Form Hardening` pour couvrir OWASP A08

7. Forcer la redirection HTTP → HTTPS sur toutes les règles de publication web (`HTTPS redirect = ON`)
8. Utiliser un certificat TLS valide (CA de confiance, non expiré) pour chaque application publiée
9. Revoir les logs WAF hebdomadairement pour identifier les nouvelles menaces et affiner les règles
10. Ne pas publier d'applications web sans politique WAF active en mode `Protection`

Valeur par défaut : Politiques WAF non configurées par défaut. Mode par défaut = Monitor lors de la création d'une nouvelle politique.

Critère de conformité : Politique WAF en mode `Protection` (non `Monitor`) appliquée à toutes les applications web exposées. SQL Injection et XSS Protection activés. Cookie Signing et Form Hardening activés. HTTPS redirect forcé sur toutes les publications. Certificats TLS valides. Logs WAF revus hebdomadairement.

Contrôle 5.6 — Protection DoS et Anti-Spoofing avancées (ENRICHI — v1.4)

CIS Ref : *5.7* | ***MITRE :*** *T1498 (Network Denial of Service), T1499 (Endpoint Denial of Service)* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Les attaques par déni de service (DoS/DDoS) et le spoofing d'adresses IP sont utilisés pour saturer les ressources du pare-feu ou contourner les contrôles d'accès basés sur l'IP source. La protection DoS native de Sophos SFOS permet de limiter les connexions SYN flood, UDP flood et ICMP flood qui ciblent les services exposés. SFOS v22 introduit des paramètres avancés de profils DoS — notamment la protection SYN cookies, la limitation des connexions par adresse IP source, et la configuration de seuils granulaires par type de flood — qui vont au-delà des paramètres basiques activés par défaut. La protection DoS contrecarre directement les attaques T1498 (Network Denial of Service) et T1499 (Endpoint Denial of Service) documentées dans MITRE ATT&CK.

Impact potentiel

- T1498 : indisponibilité totale du pare-feu et des services réseau lors d'attaques SYN flood volumétriques non atténuées
- T1499 : saturation des ressources applicatives (table de connexions, CPU) par des floods UDP/ICMP non limités
- Contournement de règles de filtrage via spoofing d'adresses IP internes
- Surcharge des ressources CPU/mémoire du firewall affectant le traitement légitime du trafic
- Un attaquant peut exploiter l'absence de limites par source pour effectuer une attaque DoS ciblée depuis une seule IP

Navigation — Configuration DoS avancée

```
Étape 1 : Accéder à la configuration DoS & Spoof
Protect > Intrusion Prevention > DoS & Spoof Protection

Étape 2 : Créer un profil DoS dédié (recommandé)
Protect > Intrusion Prevention > DoS & Spoof Protection > Add DoS rule
→ Nom de la règle : "DoS-WAN-Protection"
→ Source zones : WAN (interfaces exposées)
→ Destination zones : Any (protéger tous les services internes)

Étape 3 : Configurer la protection SYN Flood avec SYN cookies
→ SYN flood :
  - Activer : ON
  - SYN cookies : activer (mécanisme de validation des connexions TCP sans allouer de
ressources)
    (les SYN cookies permettent au pare-feu de répondre aux SYN sans créer d'entrée de
session,
     éliminant l'épuisement de la table de suivi de connexion)
  - Threshold (paquets SYN/sec) : 1000 (adapter selon le trafic légitime baseline)
  - Action : Drop (bloquer les paquets au-delà du seuil)
  - Log : activer

Étape 4 : Configurer la protection UDP Flood
→ UDP flood :
  - Activer : ON
  - Rate limit (paquets UDP/sec) : 1000 (adapter selon le trafic DNS/NTP légitime)
  - Action : Drop
  - Log : activer

Étape 5 : Configurer la protection ICMP Flood
→ ICMP flood :
  - Activer : ON
  - Rate limit (paquets ICMP/sec) : 100
  - Action : Drop
  - Log : activer

Étape 6 : Configurer les limites de connexions par adresse IP source
→ Connection limits per source IP :
  - Maximum TCP connections per source IP : 100 (adapter selon les besoins applicatifs)
  - Maximum UDP connections per source IP : 50
  - Maximum ICMP packets per source IP : 10
  - Action si dépassement : Drop + Log

Étape 7 : Anti-Spoofing
Protect > Intrusion Prevention > DoS & Spoof Protection > Spoof prevention
→ Spoof Prevention : activer
  - IP Source Routing : Block
  - Loose Source Routing : Block
  - Strict Source Routing : Block
  - Record Route : Block

Étape 8 : Appliquer la règle
→ Sauvegarder et activer la règle DoS
```

Seuils recommandés par type d’équipement

TYPE D'ÉQUIPEMENT	SYN FLOOD (PKT/S)	UDP FLOOD (PKT/S)	ICMP FLOOD (PKT/S)	CONNEXIONS MAX/IP
XGS 87/107 (PME)	500	500	50	50
XGS 126/136	1000	1000	100	100
XGS 216/226	2000	2000	200	200
XGS 316/330+	5000	5000	500	500

> *Ajuster les seuils selon la baseline de trafic légitime — des seuils trop bas génèrent des faux positifs sur les services légitimes (DNS, NTP, ICMP monitoring).*

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier le statut des protections DoS
system diagnostics show dos-protection-status

# Vérifier les statistiques de flood (compteurs de dépassements)
show dos-protection statistics

# Vérifier les règles DoS configurées
show dos-rules

# Vérifier les logs des événements DoS détectés
show log type dos last 50

# Vérification dans l'interface web
# Protect > Intrusion Prevention > DoS & Spoof Protection
# Vérifier que les protections DoS sont actives avec SYN cookies activés sur les interfaces WAN
```

Remédiation

1. Naviguer vers `Protect > Intrusion Prevention > DoS & Spoof Protection`
2. Créer une règle DoS dédiée ciblant la zone WAN avec action `Add DoS rule`
3. Activer la protection SYN Flood avec **SYN cookies activés** — cette fonctionnalité est critique pour éviter l'épuisement de la table de connexion
4. Configurer les seuils UDP flood et ICMP flood selon le tableau ci-dessus adapté à l'équipement
5. Activer les limites de connexions par adresse IP source pour prévenir les attaques dirigées depuis une seule IP
6. Activer la protection Anti-Spoofing (`Spoof Prevention`) et bloquer le routage source IP
7. Activer les logs sur tous les événements DoS pour la surveillance et l'investigation
8. Vérifier via `system diagnostics show dos-protection-status` que les protections sont actives
9. Surveiller les compteurs DoS après activation — ajuster les seuils si des faux positifs sont constatés sur le trafic légitime

Valeur par défaut : Protections DoS disponibles mais non configurées avec SYN cookies et limites par source IP. Seuils par défaut non optimisés.

Critère de conformité : Règle DoS active sur la zone WAN. SYN cookies activés. Seuils UDP/ICMP flood configurés et documentés. Limites de connexions par source IP définies. Anti-Spoofing activé. `system diagnostics show dos-protection-status` confirme les protections actives.

Contrôle 5.7 — Authentification du proxy web et durcissement de l'accès HTTP/HTTPS (NOUVEAU)

CIS Ref : *(Best practice — Web Proxy Security)* | ***MITRE :*** *T1090 (Proxy), T1071 (Application Layer Protocol)* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Sophos Firewall intègre un moteur proxy web qui peut opérer en mode transparent (aucune configuration cliente) ou en mode explicite (requiert la configuration du proxy sur les postes clients). Sans authentification configurée sur le proxy web, n'importe quel utilisateur du réseau peut accéder à Internet en restant anonyme du point de vue de la politique web, et les règles basées sur l'identité ne s'appliquent pas. Par ailleurs, les utilisateurs peuvent contourner le filtrage en utilisant des ports alternatifs ou des connexions directes si les mesures anti-bypass ne sont pas activées. T1090 (Proxy) est utilisé par les attaquants pour masquer leur trafic en passant par des proxies internes non surveillés ou en exploitant les lacunes de la configuration proxy.

Modes de déploiement

MODE	CONFIGURATION CLIENTE	AUTHENTIFICATION	CAS D'USAGE
Proxy transparent	Aucune	Implicite via STAS/Kerberos	Environnements AD avec STAS/Kerberos
Proxy explicite	Paramètre proxy navigateur	NTLM / Kerberos / Basic	Environnements avec contrôle strict de l'identité

Impact potentiel

- T1090 : attaquants utilisant le proxy interne non authentifié pour rebondir vers des destinations malveillantes en se fondant dans le trafic légitime
- Contournement du filtrage web par des utilisateurs via des ports alternatifs non surveillés
- Impossibilité d'appliquer des politiques web par identité (groupes AD) sans authentification proxy
- Navigation HTTP/HTTPS non auditée permettant l'exfiltration de données via le canal web
- Consommation de bande passante non contrôlée (streaming, téléchargements massifs) sans politique de limitation

Navigation — Configuration proxy web sécurisé

```
Étape 1 : Configurer les paramètres généraux du proxy web
Protect > Web > General Settings > Web Proxy Settings
→ Web proxy mode : sélectionner "Transparent" ou "Explicit proxy"
→ Pour le mode Explicite :
  - Port proxy : 3128 (ou port personnalisé)
  - Authentification : activer NTLM ou Kerberos
→ Pour le mode Transparent :
  - Assurer l'intégration STAS (Sophos Transparent Authentication Suite) pour l'identité

Étape 2 : Activer l'authentification utilisateur sur le proxy
Configure > Authentication > Services > Web authentication
→ Kerberos SSO : activer si Active Directory disponible
  (authentification transparente sans pop-up de login pour les utilisateurs du domaine)
→ NTLM : activer comme mécanisme de fallback
→ Exiger l'authentification avant la navigation (forcer login)

Étape 3 : Intégrer Kerberos SSO avec Active Directory
Configure > Authentication > Kerberos
→ Realm : saisir le domaine AD (ex : ENTREPRISE.LOCAL)
→ Key Distribution Center (KDC) : IP des contrôleurs de domaine
→ Service account : compte dédié avec SPN enregistré
→ Tester la connexion Kerberos

Étape 4 : Désactiver les contournements de proxy
Protect > Web > General Settings
→ Allow users to bypass web proxy : désactiver
→ Block direct connections on non-standard ports :
  - Bloquer les connexions HTTPS directes sur des ports non standards (hors 443)
  - Forcer tout le trafic web à passer par le proxy

Étape 5 : Contrôle de la bande passante
Protect > Web > Policies > [politique concernée] > Bandwidth control
→ Activer la limitation de bande passante pour les catégories à fort volume
  (Streaming vidéo, téléchargements, réseaux sociaux)
→ Définir des seuils par utilisateur ou par groupe AD
```

Activation HTTPS scanning via SSL/TLS inspection

Le proxy web ne peut inspecter le contenu HTTPS que si l'inspection SSL/TLS est activée (voir contrôle 8.1). Sans déchiffrement SSL, le proxy web gère uniquement les flux HTTP en clair et les métadonnées des connexions HTTPS (SNI, certificat), mais pas le contenu inspecté.

```
Protect > Rules and policies > SSL/TLS inspection rules
→ Ajouter une règle d'inspection Decrypt pour le trafic web
→ Lier la règle SSL/TLS à la politique web pour l'inspection complète HTTP + HTTPS
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier la configuration du proxy web
show web-proxy configuration

# Vérifier les connexions proxy actives
show connection type proxy

# Vérifier les sessions authentifiées
show user-auth sessions

# Vérification dans l'interface web
# Protect > Web > General Settings > Web Proxy Settings
# Vérifier le mode proxy et l'authentification requise
# Configure > Authentication > Services > Web authentication
# Vérifier Kerberos SSO et NTLM activés
```

Remédiation

1. Choisir le mode de déploiement proxy adapté à l'environnement (transparent pour les environnements AD avec STAS, explicite pour les environnements nécessitant un contrôle strict)
2. Naviguer vers `Configure > Authentication > Services > Web authentication` et activer Kerberos SSO pour les environnements Active Directory
3. Configurer l'intégration Kerberos dans `Configure > Authentication > Kerberos` avec un compte de service dédié
4. Activer NTLM comme mécanisme de fallback pour les appareils non-membres du domaine
5. Désactiver l'option de contournement du proxy web pour les utilisateurs dans `Protect > Web > General Settings`
6. Bloquer les connexions directes sur des ports non standards pour forcer l'usage du proxy
7. Activer le contrôle de bande passante sur les catégories à fort volume (streaming, téléchargements)
8. Coupler l'authentification proxy avec l'inspection SSL/TLS (contrôle 8.1) pour l'inspection complète du trafic HTTPS authentifié
9. Valider l'authentification transparente en testant depuis un poste membre du domaine (pas de popup de login = Kerberos SSO fonctionnel)

Valeur par défaut : Proxy web transparent activé sans authentification obligatoire. Kerberos SSO non configuré par défaut.

Critère de conformité : Authentification proxy activée (Kerberos SSO ou NTLM). Contournement du proxy désactivé. Connexions non-standards bloquées. Trafic web authentifié visible dans les logs avec identités utilisateurs.

Domaine 6 — Synchronized Security et menaces avancées

Objectif : *Activer l'intelligence de menace Sophos X-Ops, le sandboxing zero-day, le Security Heartbeat pour coordonner la réponse aux incidents via le processus Detect/Isolate/Restore, intégrer les flux de menaces tiers et MDR, et activer le HA Self-Healing pour une résilience continue.*

Contrôle 6.1 — Sophos X-Ops Threat Intelligence activé

CIS Ref : *4.1* | ***MITRE :*** *T1566, T1190* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Sophos X-Ops est l'équipe de recherche sur les menaces de Sophos qui fournit des flux de renseignement (threat feeds) intégrés directement dans SFOS. Ces feeds enrichissent la détection avec des indicateurs de compromission (IoC) en temps réel issus des incidents traités par Sophos MDR. Ne pas les activer prive le pare-feu d'une couche de détection basée sur la threat intelligence opérationnelle.

Impact potentiel

- Non-détection de menaces récentes dont les IoC sont connus de Sophos X-Ops
- Absence de blocage automatique des infrastructures C2 connues
- Retard dans la détection des campagnes de menaces actives ciblant les secteurs d'activité

Navigation

```
Protect > Active Threat Response > Sophos X-Ops Threat Feeds
→ "Sophos X-Ops threat feeds (Advanced threat protection)" : activer = ON
→ Policy : sélectionner "Log and Drop" (recommandé)
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Active Threat Response > Sophos X-Ops Threat Feeds
# Vérifier que le statut est "Enabled" et Policy = "Log and Drop"
```

Remédiation

1. Naviguer vers `Protect > Active Threat Response > Sophos X-Ops Threat Feeds`
2. Activer les threat feeds Sophos X-Ops
3. Sélectionner la politique `Log and Drop` (bloquer et journaliser les correspondances)
4. Vérifier que les abonnements nécessaires sont actifs (Network Protection)
5. Surveiller les événements générés dans les logs Active Threat Response

Valeur par défaut : Non activé par défaut.

Critère de conformité : `Sophos X-Ops threat feeds` = Enabled, Policy = `Log and Drop`.

Contrôle 6.2 — Protection Zero-Day / Sandboxing activée

CIS Ref : *4.2, 4.3* | ***MITRE :*** *T1204, T1566* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Les antivirus classiques basés sur les signatures ne détectent pas les malwares inconnus (zero-day). Le sandboxing Sophos (Sandstorm) exécute les fichiers suspects dans un environnement isolé et analyse leur comportement avant de les livrer à l'utilisateur. En SFOS v22, le moteur anti-malware AI/ML est mis à jour dans le cloud toutes les 5 minutes pour les détections de menaces émergentes, complétant ainsi l'analyse comportementale du sandboxing.

Impact potentiel

- Infection par des malwares zero-day non détectés par les signatures AV classiques
- Livraison de ransomwares via des pièces jointes email ou des téléchargements web non analysés
- Propagation de malwares avancés au sein du réseau interne

Navigation

```
Protect > Rules and policies > Firewall rules > Éditer une règle
→ Security features > Zero-day protection : activer
→ "Exclude file types from zero-day protection analysis" : NE PAS exclure les types de
fichiers
Pour la protection email (mode MTA) :
Protect > Email > Settings > Zero-day protection > Activer
→ Mode MTA recommandé pour la protection email
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Rules and policies > Firewall rules > règle concernée
# Vérifier que "Zero-day protection" est activé sans exclusions de types de fichiers
```

Remédiation

1. Activer Zero-day protection sur toutes les règles de pare-feu traitant les téléchargements (HTTP/HTTPS)
2. Ne pas exclure de types de fichiers de l'analyse zero-day (les malwares exploitent souvent les extensions réputées sûres)
3. Pour la protection email, activer le zero-day en mode MTA (`Protect > Email > Settings`)
4. Vérifier que l'abonnement Sandstorm est actif dans `System > Administration > Licensing`
5. Surveiller les rapports Sandstorm dans les logs de sécurité

Valeur par défaut : Zero-day protection non activée par défaut sur les règles de pare-feu.

Critère de conformité : Zero-day protection activée sur les règles HTTP/HTTPS. Aucune exclusion de types de fichiers. Protection email en mode MTA avec Zero-day activé.

Contrôle 6.3 — Security Heartbeat — processus Detect/Isolate/Restore

CIS Ref : *4.4* | ***MITRE :*** *T1562, T1210* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Synchronized Security coordonne la réponse aux menaces entre les endpoints Sophos et le pare-feu via un processus en trois étapes automatisées (Detect/Isolate/Restore). Un endpoint compromis peut être automatiquement isolé par le pare-feu en quelques secondes, stoppant la propagation latérale sans intervention humaine. Cette coordination est une fonctionnalité différenciante de l'architecture Sophos et requiert l'enregistrement du pare-feu dans Sophos Central.

Processus Synchronized Security (3 étapes)

1. **Detect** : Sophos Endpoint/Intercept X détecte une menace active et change l'état du Security Heartbeat en ROUGE
2. **Isolate** : Sophos Firewall et Sophos ZTNA reçoivent le signal rouge et limitent immédiatement et automatiquement l'accès réseau de l'endpoint compromis (blocage du trafic sortant sauf les communications de remédiation)
3. **Restore** : Une fois la remédiation terminée sur l'endpoint (nettoyage de la menace), le Security Heartbeat repasse à VERT → le Firewall restaure automatiquement l'accès réseau complet sans intervention manuelle

Impact potentiel

- Propagation de malwares depuis un endpoint infecté vers d'autres ressources réseau si le Heartbeat n'est pas configuré
- Mouvement latéral non bloqué en l'absence de coordination pare-feu/endpoint
- Délai de réponse à incident de plusieurs heures au lieu de quelques secondes

Navigation

```
System > Sophos Central > enregistrer le pare-feu dans Sophos Central (prérequis)
Protect > Rules and policies > Firewall rules > Éditer une règle LAN
→ Security Heartbeat : activer
→ Minimum source HB permitted : sélectionner "Yellow" ou "Green"
→ (Les endpoints en état "Red" seront bloqués automatiquement — processus Isolate)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
# Vérifier le statut Synchronized Security
console> show security-heartbeat
console> show synchronized-security
# Vérifier dans l'interface web
# Protect > Rules and policies > Firewall rules
# Vérifier que Security Heartbeat est activé sur les règles LAN-to-WAN
```

Remédiation

1. Enregistrer le pare-feu dans Sophos Central (`System > Sophos Central`)
2. Déployer Sophos Intercept X sur les endpoints et les enregistrer dans Sophos Central
3. Naviguer vers `Protect > Rules and policies > Firewall rules`
4. Éditer les règles LAN-to-WAN et activer le `Security Heartbeat`
5. Définir `Minimum source HB permitted` = `Yellow` (bloque les endpoints en état Red — étape Isolate)
6. Tester le cycle complet Detect/Isolate/Restore en simulant une alerte sur un endpoint de test
7. Vérifier la restauration automatique de l'accès réseau après nettoyage de l'endpoint de test

Note MDR Active Threat Response : Si l'organisation dispose d'un abonnement Sophos MDR, les analystes MDR (ou vos analystes XDR) peuvent déclencher manuellement une réponse Synchronized Security via la capacité de threat feed intégrée dans Sophos Firewall, permettant une isolation ciblée d'endpoints lors d'investigations actives.

Valeur par défaut : Security Heartbeat non configuré par défaut.

Critère de conformité : Pare-feu enregistré dans Sophos Central. Security Heartbeat activé sur les règles LAN-to-WAN. Minimum permitted = `Yellow` ou `Green` (endpoints Red bloqués automatiquement). Cycle Detect/Isolate/Restore testé.

Contrôle 6.4 — Flux de menaces tiers intégrés

CIS Ref : *4.6* | ***MITRE :*** *T1566* | ***Niveau :*** 🔵 *L2*

Description du risque

Les flux de menaces tiers (threat feeds) enrichissent la détection Sophos avec des IoC (indicateurs de compromission) provenant de sources externes spécialisées (MISP, ISAC sectoriels, CERT nationaux). Ces sources complémentaires couvrent des menaces spécifiques à des secteurs d'activité ou des géographies non forcément présents dans les feeds Sophos.

Impact potentiel

- Non-détection de menaces spécifiques à un secteur non couvertes par les feeds Sophos X-Ops
- Absence de corrélation avec les IoC partagés par les CERT nationaux (ANSSI, CERT-FR)
- Couverture de détection réduite sans la diversité des sources de threat intelligence

Navigation

```
Protect > Active Threat Response > Third-party Threat Feeds
→ Add Threat Feed : ajouter les flux de menaces tiers (format STIX/TAXII ou CSV)
→ Configurer : URL, format, fréquence de mise à jour, politique (Log/Drop)
→ Activer chaque feed configuré
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Active Threat Response > Third-party Threat Feeds
# Vérifier les feeds configurés et leur statut de synchronisation
```

Remédiation

1. Identifier les sources de threat intelligence pertinentes pour le secteur (CERT-FR, MISP communautaires, ISACs)
2. Naviguer vers `Protect > Active Threat Response > Third-party Threat Feeds`
3. Ajouter les flux en format STIX/TAXII ou CSV selon les sources disponibles
4. Configurer la politique de chaque feed (`Log and Drop`)
5. Valider la synchronisation et vérifier les logs d'intégration

Valeur par défaut : Aucun feed tiers configuré par défaut.

Critère de conformité : Au moins un flux de menaces tiers configuré, synchronisé et actif en politique `Log and Drop`.

Contrôle 6.5 — NDR Essentials — analyse IA du trafic chiffré, EPA engine et détection DGA (ENRICHI — SFOS v22)

CIS Ref : *4.7* | ***MITRE :*** *T1071 (Application Layer Protocol), T1568 (Dynamic Resolution / DGA), T1573 (Encrypted Channel), T1557 (Adversary-in-the-Middle), T1041* | ***Niveau :*** 🔵 *L2*

Description du risque

NDR (Network Detection and Response) Essentials est disponible depuis SFOS v21.5 et significativement enrichi dans SFOS v22. Il capture les métadonnées du trafic TLS chiffré ET des requêtes DNS, et les transmet à Sophos Cloud NDR pour une analyse AI sans jamais déchiffrer le trafic. Cette approche, dite "passive metadata analysis", permet de détecter des menaces actives dans des flux que ni les signatures traditionnelles ni l'inspection SSL ne peuvent analyser entièrement.

Deux moteurs clés distinguent NDR Essentials v22 : 1. **Encrypted Payload Analysis (EPA) engine** : détecte des payloads malveillants dans le trafic chiffré en analysant les patterns de flux, les tailles de paquets et les comportements de communication — sans déchiffrer le contenu 2. **DGA Detection (Domain Generation Algorithm)** : identifie les domaines générés algorithmiquement utilisés par les malwares pour leurs serveurs C2 — indicateur précoce de compromission avant même que le domaine n'apparaisse dans les listes noires

Impact potentiel

- T1071 : communications C2 via des protocoles chiffrés légitimes (HTTPS, DNS) non détectées sans NDR

- T1568 : domaines C2 générés par DGA non détectés par les feeds de réputation classiques (domaines inconnus)
- T1573 : canal chiffré entre un endpoint compromis et le C2 non visible sans analyse de métadonnées
- T1557 : attaque adversary-in-the-middle sur flux chiffrés internes non détectée sans NDR
- Mouvements latéraux via des protocoles autorisés et chiffrés non identifiables par les règles de pare-feu classiques

Moteur EPA (Encrypted Payload Analysis) — Fonctionnement

Le moteur EPA analyse les caractéristiques comportementales du flux TLS sans déchiffrement :

SIGNAL ANALYSÉ	INDICATEUR DE MENACE	EXEMPLE
Taille des échanges initiaux	Payload de commande C2	Petits paquets réguliers = polling C2
Fréquence des connexions	Beaconing régulier	Intervalle fixe = implant malware
Ratio upload/download	Exfiltration	Upload anormalement élevé
Certificat TLS de destination	Domaine suspect	Self-signed ou CN ne correspondant pas
Durée des sessions	Tunnel persistant	Sessions très longues = backdoor
Entropy des données	Données fortement chiffrées	Double chiffrement suspect

Détection DGA (Domain Generation Algorithms)

Les malwares utilisent des DGA pour générer des milliers de domaines aléatoires et contacter celui qui est actif ce jour-là, rendant le blocage statique inefficace. NDR Essentials v22 détecte les requêtes DNS vers des domaines à forte entropie et les patterns de résolution correspondant aux algorithmes DGA connus :

CARACTÉRISTIQUE DGA	EXEMPLES DE PATTERNS DÉTECTÉS
Longueur anormale	`xkj3mzqr8plwq.com` (> 15 chars aléatoires)
Haute entropie lexicale	Absence de mots lisibles dans le domaine
Volume de résolutions échouées	Centaines de NXDOMAIN en peu de temps
Algorithme connu	Correspondance avec les DGA de Conficker, Dridex, etc.

Navigation

```
Protect > Active Threat Response > NDR Essentials
→ Turn on NDR Essentials : activer = ON
→ Add interfaces (interfaces à surveiller) :
  - Priorité 1 : interfaces LAN internes (trafic utilisateurs — risque C2 élevé)
  - Priorité 2 : interfaces DMZ (trafic serveurs exposés)
  - Priorité 3 : interfaces de services critiques (SCADA, OT si applicable)
  - NE PAS exclure les interfaces à fort trafic chiffré (elles sont les plus à risque)
→ Configure exclusions : exclure uniquement le trafic de gestion interne connu-bon
  (ex : sauvegardes, synchronisations AD, mises à jour antivirus)
→ Vérifier la connexion Sophos Central pour la collecte des métadonnées
→ Dans Sophos Central > Threat Analysis Center :
  - Configurer les alertes NDR sur les détections de haute criticité
  - Activer la détection DGA dans les politiques NDR
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5 > Advanced shell)
# Vérifier le statut NDR Essentials
show sophos-ndr status
# Résultat attendu : NDR Essentials = Enabled, interfaces listées, connexion Sophos Cloud =
Active

# Vérification des interfaces actives sous NDR
show sophos-ndr interfaces

# Vérification dans l'interface web
# Protect > Active Threat Response > NDR Essentials
# Vérifier : Enabled = ON, interfaces configurées, statut Sophos Cloud = Connected
```

Remédiation

1. Vérifier que l'abonnement NDR est actif dans `System > Administration > Licensing`
2. Vérifier que le pare-feu est enregistré dans Sophos Central (prérequis pour NDR)
3. Naviguer vers `Protect > Active Threat Response > NDR Essentials`
4. Activer NDR Essentials (`Turn on NDR Essentials = ON`)
5. Ajouter toutes les interfaces internes LAN et DMZ à surveiller
6. Configurer des exclusions minimales et documentées pour le trafic interne connu-bon
7. Dans Sophos Central > Threat Analysis Center : configurer des alertes sur les détections DGA et EPA de haute criticité
8. Intégrer les alertes NDR dans le workflow SOC pour investigation (T1568 DGA = indicateur précoce de C2)
9. Tester la détection NDR en comparant les flux remontés dans Sophos Central avec les interfaces configurées
10. Réviser trimestriellement les exclusions NDR pour éviter les angles morts

Valeur par défaut : NDR Essentials non configuré par défaut. Nécessite un abonnement NDR et l'enregistrement dans Sophos Central.

Critère de conformité : NDR Essentials activé. Interfaces LAN et DMZ de surveillance configurées. Commande `show sophos-ndr status` retourne `Enabled`. Flux NDR visibles dans Sophos Central. Alertes DGA et EPA configurées dans Sophos Central Threat Analysis Center. Exclusions documentées et minimales.

Contrôle 6.6 — Active Threat Response MDR/XDR — Réponse en temps réel aux menaces actives (ENRICHI)

CIS Ref : *(Health Check Sophos v22 — HIGH severity)* | ***MITRE :*** *T1566, T1190, T1071, T1048* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Active Threat Response (ATR) est le mécanisme par lequel les analystes Sophos MDR ou vos propres analystes XDR envoient des indicateurs de compromission (IoC) directement au pare-feu pour déclencher une réponse bloquante en temps réel. Contrairement aux feeds de réputation classiques qui bloquent des catégories connues, ATR permet une réponse ciblée sur des menaces en cours d'investigation. Un analyste MDR ayant identifié un serveur C2 actif peut bloquer l'ensemble du réseau de l'organisation contre cette IP en quelques secondes, depuis n'importe où.

Les flux de menaces MDR (Managed Detection and Response) de Sophos constituent l'intelligence opérationnelle la plus avancée disponible dans SFOS v22 — issus des investigations actives sur des incidents réels, ces feeds contiennent des IoC à haute fidélité non disponibles dans les feeds X-Ops standard. Le Health Check Sophos v22 classe leur activation comme HIGH severity avec politique "Log and drop" obligatoire.

Architecture Active Threat Response — Mécanisme de fonctionnement

```
[Analyste MDR/XDR]
        |
        ↓ déclenche une action de réponse depuis la console XDR
[Sophos Central ATR]
        |
        ↓ transmet l'IoC via le canal de synchronisation Central-Firewall
[Sophos Firewall SFOS v22]
        |
        ↓ applique le blocage en temps réel sans intervention manuelle
[Blocage : IP, domaine, endpoint isolé via Heartbeat RED]
```

Deux modes d'opération

MODE	PRÉREQUIS	OPÉRATEURS	CAS D'USAGE
Sophos MDR	Abonnement MDR	Analystes Sophos 24/7	Réponse automatique sur incidents gérés
Sophos XDR	Abonnement XDR	Vos propres analystes SOC	Réponse pilotée par votre équipe

Actions de réponse disponibles via ATR

ACTION	MÉCANISME SFOS	DÉLAI D'APPLICATION
Bloquer une IP (C2, exfiltration)	Ajout automatique à la liste noire du pare-feu	Secondes

ACTION	MÉCANISME SFOS	DÉLAI D'APPLICATION
Bloquer un domaine	Blocage DNS + HTTP/HTTPS via le feed ATR	Secondes
Isoler un endpoint compromis	Mise à l'état RED du Security Heartbeat → isolement automatique par le pare-feu	Secondes
Interrompre une connexion active	Drop des connexions existantes vers l'IP/domaine ciblé	Immédiat

Impact potentiel

- Non-blocage des serveurs C2 actifs identifiés par les analystes lors d'investigations en cours
- Délai de plusieurs heures entre l'identification d'une menace et son blocage (processus manuel)
- Absence de capacité d'isolation ciblée d'un endpoint lors d'une investigation XDR active
- T1071 : communications C2 maintenues pendant toute la durée de l'investigation sans blocage possible
- T1048 : exfiltration poursuivie pendant que l'analyste attend la mise à jour des règles de pare-feu

Navigation — Configuration complète

```
Prérequis : pare-feu enregistré dans Sophos Central (System > Sophos Central)

Étape 1 : Activer les feeds MDR (si abonnement disponible)
Protect > Active Threat Response > Sophos MDR Threat Feeds
→ "Sophos MDR threat feeds" : activer = ON
→ Policy : sélectionner "Log and Drop"
→ Cliquer sur "Apply"

Étape 2 : Configurer les Threat Feeds ATR personnalisés (XDR)
Protect > Active Threat Response > Threat Feeds > Configure
→ Visualiser les feeds actifs (MDR + X-Ops + tiers)
→ Vérifier le statut de synchronisation de chaque feed
→ Configurer les actions par feed (Log / Drop / Log and Drop)

Étape 3 : Vérifier les actions de réponse disponibles
Depuis la console Sophos XDR (Sophos Central > Threat Analysis Center) :
→ Sélectionner un événement de menace
→ "Respond" > choisir l'action : Block IP / Block Domain / Isolate Device
→ L'action est transmise automatiquement au firewall via ATR

Étape 4 : Vérifier l'intégration Security Heartbeat pour l'isolation
Protect > Rules and policies > Firewall rules > règles LAN
→ Security Heartbeat : activé (prérequis pour l'isolation via ATR)
→ Minimum source HB permitted : Yellow (les endpoints mis en RED par ATR sont
automatiquement isolés)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5 > Advanced shell)
# Vérifier le statut des feeds Active Threat Response
show active-threat-response feeds

# Résultat attendu pour chaque feed :
# MDR Feed : Enabled, Last sync : <timestamp récent>, Policy : Log and Drop
# X-Ops Feed : Enabled, Last sync : <timestamp récent>, Policy : Log and Drop

# Vérifier les correspondances récentes (IoC bloqués)
show active-threat-response matches last 50

# Vérification dans l'interface web
# Protect > Active Threat Response > Sophos MDR Threat Feeds
# Vérifier Enabled = ON, Policy = Log and Drop
# System > Administration > Licensing : confirmer l'abonnement MDR/XDR actif
```

Remédiation

1. Vérifier que l'abonnement Sophos MDR ou XDR est actif dans `System > Administration > Licensing`
2. Enregistrer le pare-feu dans Sophos Central si ce n'est pas déjà fait (`System > Sophos Central`)
3. Naviguer vers `Protect > Active Threat Response > Sophos MDR Threat Feeds`
4. Activer les MDR Threat Feeds avec politique `Log and Drop`
5. Naviguer vers `Protect > Active Threat Response > Threat Feeds > Configure` et vérifier la synchronisation de tous les feeds
6. S'assurer que le Security Heartbeat est activé sur les règles LAN (prérequis pour l'isolation via ATR — voir contrôle 6.3)
7. Former les analystes SOC à l'utilisation de la console Sophos XDR pour déclencher des actions de réponse
8. Créer une procédure documentée d'escalade MDR définissant quand contacter les analystes Sophos MDR pour une réponse active
9. Tester le mécanisme ATR avec un IoC de test bénin pour valider le circuit complet Centre XDR → Firewall
10. Si l'abonnement MDR n'est pas disponible, compenser avec des feeds tiers de haute fidélité (contrôle 6.4) et former des analystes XDR internes

Valeur par défaut : Non activé par défaut. Nécessite un abonnement MDR ou XDR et l'enregistrement dans Sophos Central.

Critère de conformité : Si abonnement MDR disponible : `Sophos MDR threat feeds` = Enabled, Policy = `Log and Drop`. Commande `show active-threat-response feeds` retourne au moins un feed actif et synchronisé. Security Heartbeat activé sur les règles LAN pour permettre l'isolation via ATR.

Contrôle 6.7 — HA Self-Healing — correction automatique des déviations d'état (NOUVEAU — SFOS v22)

CIS Ref : *(Architecture HA Sophos v22)* | ***MITRE :*** *T1499* | ***Niveau :*** 🔵 *L2*

Description du risque

Le HA Self-Healing de SFOS v22 représente une évolution majeure par rapport au HA traditionnel. Alors que le HA classique se contente de basculer vers le nœud secondaire en cas de panne, le HA Self-Healing surveille en continu l'état entre les deux nœuds appairés et corrige automatiquement les déviations d'état sans basculement ni intervention manuelle. Cette fonctionnalité garantit une cohérence continue de la politique de sécurité entre les nœuds et réduit le risque qu'un attaquant exploite une désynchronisation temporaire.

Différence avec le HA classique

FONCTIONNALITÉ	HA CLASSIQUE	HA SELF-HEALING (V22)
Détection de panne	Oui	Oui
Basculement automatique	Oui	Oui
Surveillance continue de l'état	Non	Oui
Correction automatique des déviations	Non	Oui
Intervention manuelle pour resynchroniser	Requise	Non requise

Impact potentiel

- T1499 : attaque par déni de service exploitant la désynchronisation entre nœuds HA
- Configuration divergente entre nœuds HA non détectée, créant une politique de sécurité incohérente
- Exploitation d'une fenêtre de vulnérabilité lors de la désynchronisation manuelle sans Self-Healing

Navigation

```
Configure > System Services > High Availability > High Availability Configuration
→ Vérifier que HA est configuré en mode Active-Passive (recommandé pour Self-Healing)
→ HA Self-Healing settings :
  - State monitoring : activé (surveille l'état entre les nœuds en continu)
  - Auto-correction : activé
→ Vérifier les logs HA pour les corrections automatiques effectuées :
  System > Log Viewer > filtrer sur "HA" ou "High Availability"
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
system ha show status
# Vérifier que l'état des deux nœuds est synchronisé
# Rechercher les événements de self-healing dans les logs
system ha show log
```

Remédiation

1. S’assurer que la HA est configurée en mode Active-Passive sur deux nœuds SFOS v22
2. Vérifier que les deux nœuds sont sur la même version SFOS v22
3. Activer la surveillance de l’état HA et les fonctions de self-healing dans la configuration HA
4. Surveiller les logs HA pour identifier les corrections automatiques (indicateur de problèmes sous-jacents à investiguer)
5. Tester le self-healing en déconnectant temporairement le lien de synchronisation HA et en vérifiant la correction automatique

Valeur par défaut : HA Self-Healing disponible sur SFOS v22 en mode HA. Nécessite que HA soit configuré (voir contrôle 1.6).

Critère de conformité : HA configuré en Active-Passive sur deux nœuds SFOS v22. State monitoring activé. Aucune déviation non corrigée détectée dans les logs HA.

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

Objectif : *Sécuriser les tunnels VPN avec des algorithmes cryptographiques forts, des certificats valides, et le MFA, en éliminant les modes d'échange obsolètes comme le mode agressif IKEv1. Déployer ZTNA (Zero Trust Network Access) intégré nativement dans Sophos Firewall pour remplacer progressivement le SSL-VPN réseau par un accès applicatif granulaire avec vérification de posture.*

Contrôle 7.1 — IPsec — IKEv2 uniquement, pas de mode agressif

CIS Ref : *3.6* | ***MITRE :*** *T1133, T1040* | ***Niveau :*** 🟠 *ÉLEVÉ*

Description du risque

Le mode agressif IKEv1 transmet le hash des identifiants en clair lors de la négociation du tunnel, permettant à un attaquant de capturer ces hashes et de réaliser des attaques par dictionnaire hors ligne. IKEv2 avec authentification forte élimine cette vulnérabilité et offre une meilleure résistance aux attaques man-in-the-middle.

Impact potentiel

- Capture du hash d'authentification IKEv1 en mode agressif et attaque par dictionnaire hors ligne
- Compromission du tunnel VPN permettant l'interception du trafic ou un accès réseau non autorisé
- Contournement de l'authentification VPN via des attaques sur les échanges IKEv1

Navigation

```
Configure > Remote Access VPN > IPsec (ou Site-to-Site VPN > IPsec)
→ Éditer chaque profil VPN IPsec
→ Phase 1 : Key exchange = IKEv2 uniquement (ne pas sélectionner IKEv1)
→ Authentication mode : ne pas utiliser "Aggressive mode"
→ Phase 1 : Encryption = AES-256, Hash = SHA-256 ou SHA-512, DH group = 14+
→ Phase 2 : Encryption = AES-256, Hash = SHA-256 ou SHA-512, PFS = activé, DH = 14+
```

CLI de vérification

```
# Vérification dans l'interface web
# Configure > Remote Access VPN > IPsec
# Vérifier que Key exchange = IKEv2 et qu'aucun profil n'utilise Aggressive Mode
```

Remédiation

1. Auditer tous les profils et connexions IPsec configurés
2. Migrer les profils IKEv1 vers IKEv2 (peut nécessiter une coordination avec les partenaires)
3. Désactiver le mode agressif sur tous les profils IKEv1 restants en phase de transition

4. Configurer AES-256, SHA-256, et DH group ≥ 14 (2048 bits) pour toutes les phases
5. Activer PFS (Perfect Forward Secrecy) sur tous les tunnels

Valeur par défaut : IKEv1 supporté par défaut, mode agressif potentiellement disponible.

Critère de conformité : Tous les profils IPsec configurés avec IKEv2. Aucun profil en mode Aggressive. Chiffrement AES-256 et DH ≥ groupe 14.

Contrôle 7.2 — SSL VPN — certificat valide configuré

CIS Ref : *1.1.4* | ***MITRE :*** *T1133, T1557* | ***Niveau :*** 🔵 *L2*

Description du risque

Un certificat auto-signé ou expiré sur le portail SSL VPN expose les utilisateurs à des attaques man-in-the-middle lors de l'établissement de leurs tunnels VPN. Les clients VPN confrontés à des erreurs de certificat sont souvent amenés à les ignorer, créant une vulnérabilité persistante et conditionnant les utilisateurs à accepter les avertissements de sécurité.

Impact potentiel

- Interception des sessions SSL VPN par un attaquant MitM sur le réseau d'accès
- Capture des identifiants VPN via un certificat frauduleux non détecté
- Formation des utilisateurs à ignorer les avertissements de certificat (habitude dangereuse)

Navigation

```
Configure > Remote Access VPN > SSL VPN > SSL VPN global settings
→ SSL server certificate : sélectionner un certificat valide (non auto-signé, non expiré)
System > Administration > Admin and User settings > Admin console and end-user interaction
→ Certificate : appliquer un certificat valide au portail utilisateur
```

CLI de vérification

```
# Vérification dans l'interface web
# Configure > Remote Access VPN > SSL VPN > SSL VPN global settings
# Vérifier que le certificat sélectionné est valide, non expiré, émis par une CA de
confiance
```

Remédiation

1. Acquérir un certificat TLS valide depuis une CA publique de confiance (ou CA interne pour les clients internes uniquement)
2. Vérifier : validité non expirée, clé ≥ 2048 bits, hash SHA-2, CN correspondant au FQDN du portail VPN
3. Importer le certificat dans `System > Certificates > Certificates`
4. Appliquer le certificat dans `Configure > Remote Access VPN > SSL VPN > SSL VPN global settings`
5. Appliquer également au portail utilisateur dans `System > Administration > Admin settings`

Valeur par défaut : Certificat auto-signé par défaut.

Critère de conformité : Certificat SSL VPN valide (CA de confiance, non expiré, clé ≥ 2048 bits, SHA-2), appliqué au SSL VPN gateway et au portail utilisateur.

Contrôle 7.3 — VPN avec MFA obligatoire

CIS Ref : *1.1.8 (étendu)* | ***MITRE :*** *T1133, T1078* | ***Niveau :*** 🔴 *CRITIQUE*

Description du risque

Les accès VPN sans MFA sont vulnérables aux attaques par credential stuffing et aux campagnes d'exploitation de mots de passe compromis. De nombreux incidents documentés par le CISA ont débuté par une compromission VPN avec des identifiants valides obtenus via le dark web. SFOS v22 supporte SHA-256 et SHA-512 pour les tokens TOTP VPN, renforçant la sécurité du MFA par rapport aux implémentations SHA-1 antérieures.

Impact potentiel

- Accès non autorisé au réseau interne via des identifiants VPN compromis
- Point d'entrée pour des campagnes ransomware débutant par l'exploitation du VPN
- Violation des politiques de conformité (NIS2, RGPD) si l'accès distant n'est pas protégé par MFA

Navigation

```
Configure > Authentication > Multi-factor authentication > Multi-factor authentication
settings
→ Activer "Require MFA for SSL VPN remote access"
→ Activer "Require MFA for IPSec remote access"
→ Sélectionner les utilisateurs/groupes concernés
→ Algorithm OTP : SHA-256 ou SHA-512 (nouveau en v22)
```

CLI de vérification

```
# Vérification dans l'interface web
# Configure > Authentication > Multi-factor authentication
# Vérifier que MFA SSL VPN et IPSec sont activés
```

Remédiation

1. S'assurer que tous les utilisateurs VPN ont un token OTP configuré
2. Activer le MFA pour SSL VPN et IPSec dans les paramètres d'authentification multi-facteur
3. Utiliser SHA-256 ou SHA-512 pour l'algorithme OTP (disponible en v22)
4. Tester avec un compte de test avant déploiement en production
5. Informer les utilisateurs de la procédure MFA et fournir les instructions d'inscription
6. Prévoir une procédure de récupération en cas de perte du token (accès SSH par clé pour l'admin)

Valeur par défaut : MFA non activé pour les connexions VPN par défaut.

Critère de conformité : MFA activé pour SSL VPN remote access et IPSec remote access. Algorithme OTP = SHA-256 ou SHA-512.

Contrôle 7.4 — Sophos ZTNA intégré — Zero Trust Network Access pour l'accès applicatif distant (NOUVEAU — SFOS v20 MR2+)

CIS Ref : *(Architecture ZTNA Sophos)* | ***MITRE :*** *T1133 (External Remote Services)* | ***Niveau :*** 🔵 *L2*

Description du risque

Sophos ZTNA (Zero Trust Network Access) est intégré nativement dans chaque Sophos Firewall à partir de SFOS v20 MR2+ — aucune passerelle séparée n'est nécessaire. Contrairement au SSL-VPN qui accorde un accès réseau large une fois la connexion établie, ZTNA adopte un modèle d'accès applicatif granulaire : l'accès n'est accordé que pour des applications spécifiques, après vérification combinée de l'identité de l'utilisateur ET de la santé de l'appareil (posture check). T1133 (External Remote Services) est directement contré par le ZTNA, qui élimine la surface d'attaque liée aux VPN réseaux traditionnels en substituant un accès applicatif contrôlé et conditionnel.

Différence fondamentale ZTNA vs SSL-VPN

CRITÈRE	SSL-VPN	ZTNA
Périmètre d'accès	Réseau entier (ou sous-réseau)	Application spécifique uniquement
Vérification appareil	Non (identifiants seulement)	Oui — posture check + Heartbeat
Exposition réseau	Large (mouvement latéral possible)	Nulle (accès applicatif isolé)
Isolation des appareils compromis	Manuelle	Automatique (Heartbeat RED → blocage immédiat)
Visibilité SIEM/XDR	Limitée	Logs complets dans Sophos Central XDR data lake
Migration depuis SSL-VPN	—	ZTNA remplace SSL-VPN pour l'accès applicatif (pas réseau)

Modes de déploiement

MODE	VERSION SFOS REQUISE	GESTION	CAS D'USAGE
On-premises Gateway	SFOS 19.5 MR3+	Sophos Central	Sites avec Sophos Firewall existant — recommandé

MODE	VERSION SFOS REQUISE	GESTION	CAS D'USAGE
(Sophos Firewall)			
Sophos Cloud Gateway	SFOS 20 MR2+	Sophos Central	Sites sans Sophos Firewall ou accès multi-cloud

Modèle de sécurité ZTNA — Conditions d'accès

L'accès est accordé uniquement si les trois conditions suivantes sont simultanément satisfaites :

1. **Identité vérifiée** : l'utilisateur s'est authentifié via Sophos Central (MFA recommandé)
2. **Appareil sain** : la posture de l'appareil (Sophos Health Check) est conforme à la politique
3. **Heartbeat vert** : l'endpoint Sophos ne signale aucune menace active (Heartbeat = GREEN/YELLOW)

Si le Heartbeat devient RED (menace détectée), le ZTNA isole automatiquement l'appareil — l'accès à toutes les applications est révoqué immédiatement, sans intervention humaine.

Impact potentiel

- T1133 : accès VPN réseau accordant un accès large permettant le mouvement latéral une fois les identifiants compromis
- Surface d'attaque VPN exposée sur Internet, cible privilégiée des campagnes de force brute
- Absence de contrôle de posture permettant à des appareils non conformes d'accéder aux ressources
- Non-isolation automatique des appareils compromis en cas d'incident (Heartbeat RED)
- Trafic VPN non corrélé avec les détections XDR (logs fragmentés entre VPN et SIEM)

Navigation — Configuration ZTNA sur Sophos Firewall

```
Prérequis 1 : Pare-feu enregistré dans Sophos Central
System > Sophos Central > Register with Sophos Central
→ Vérifier que la connexion est active

Prérequis 2 : Vérifier la version SFOS
System > Backup & Firmware > Firmware
→ SFOS 19.5 MR3+ pour gateway on-premises
→ SFOS 20 MR2+ pour Sophos Cloud Gateway

Étape 1 : Créer la passerelle ZTNA dans Sophos Central
Sophos Central > Zero Trust Network Access > Gateways > Add Gateway
→ Type : sélectionner "On-premises"
→ Choisir le Sophos Firewall géré dans la liste
→ Configurer le FQDN public de la passerelle (ex : ztna.entreprise.fr)
→ Valider la création

Étape 2 : Définir les ressources (applications)
Sophos Central > Zero Trust Network Access > Resources > Add Resource
→ Nom de la ressource : ex "Intranet RH", "ERP SAP", "Bureau distant"
→ Protocole : HTTPS, RDP, SSH selon l'application
→ Adresse interne : IP/FQDN interne du serveur applicatif
→ Associer la gateway créée à l'étape 1

Étape 3 : Définir les politiques d'accès
Sophos Central > Zero Trust Network Access > Policies > Add Policy
→ Utilisateurs/groupes autorisés (sync depuis Active Directory via Sophos Central)
→ Conditions de posture : activées
→ Health check : Heartbeat GREEN ou YELLOW requis (RED = accès refusé)
→ Associer la politique aux ressources concernées

Étape 4 : Déployer le client Sophos Connect avec ZTNA
Sophos Central > ZTNA > Clients > Deploy
→ Télécharger le package Sophos Connect avec la configuration ZTNA
→ Déployer via GPO, MDM, ou SCCM sur les postes des utilisateurs
→ Les utilisateurs accèdent aux applications via le portail ZTNA sans VPN réseau

Étape 5 : Vérifier le statut depuis le pare-feu
System > Sophos Central > ZTNA Gateway Status
→ Vérifier que la passerelle est "Connected" et "Active"
→ Vérifier le nombre de sessions actives
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier le statut de la connexion Sophos Central (prérequis ZTNA)
show sophos-central status

# Vérifier le statut de la passerelle ZTNA
show ztna gateway status

# Vérifier les sessions ZTNA actives
show ztna sessions

# Vérification dans l'interface web
# System > Sophos Central > ZTNA Gateway Status
# Vérifier : Gateway = Connected, Sessions actives visibles
```

Reporting ZTNA dans Sophos Central XDR

Les logs ZTNA sont disponibles dans le data lake XDR de Sophos Central, permettant la corrélation avec les détections endpoint et firewall :

```
Sophos Central > Threat Analysis Center > Data Lake
→ Filtrer sur : source = ZTNA
→ Visualiser : accès par utilisateur, ressources accédées, posture checks
→ Détecter : tentatives d'accès depuis appareils non conformes, accès hors heures
Sophos Central > Zero Trust Network Access > Reports
→ Rapport d'accès par utilisateur et ressource
→ Rapport de conformité posture des appareils
```

Remédiation

1. Vérifier la version SFOS et l'éligibilité au ZTNA (`System > Backup & Firmware > Firmware`) — SFOS 19.5 MR3+ requis pour gateway on-premises
2. S'assurer que le pare-feu est enregistré dans Sophos Central (`System > Sophos Central`)
3. Créer la passerelle ZTNA dans `Sophos Central > Zero Trust Network Access > Gateways`
4. Définir les ressources (applications internes) à exposer via ZTNA
5. Configurer les politiques d'accès avec vérification de posture et Heartbeat
6. Déployer le client Sophos Connect avec configuration ZTNA sur les postes utilisateurs
7. Planifier la migration progressive depuis SSL-VPN vers ZTNA pour les accès applicatifs (ZTNA remplace SSL-VPN pour les applications — conserver SSL-VPN uniquement pour les cas d'usage réseau complet temporaires)
8. Intégrer les logs ZTNA dans le SIEM pour la surveillance des accès distants
9. Configurer des alertes sur les tentatives d'accès depuis appareils en posture non conforme

Valeur par défaut : ZTNA non configuré par défaut. Nécessite l'enregistrement dans Sophos Central et la création d'une gateway ZTNA.

Critère de conformité : Passerelle ZTNA configurée et en statut Connected dans Sophos Central. Ressources (applications) définies avec politiques d'accès incluant vérification de posture et Heartbeat. Client Sophos Connect déployé sur les postes d'accès distant. Logs ZTNA disponibles dans Sophos Central XDR data lake.

Domaine 8 — Inspection SSL/TLS

Objectif : *Déchiffrer et inspecter les flux HTTPS sortants et entrants pour détecter les malwares, les C2 et les exfiltrations dissimulés dans le trafic chiffré, tout en limitant les exemptions à des cas documentés et justifiés.*

Contrôle 8.1 — Profil d'inspection SSL/TLS activé sur les règles de pare-feu

CIS Ref : *5.2* | ***MITRE :*** *T1071, T1048, T1557* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Plus de 90% du trafic web est désormais chiffré (HTTPS). Sans inspection SSL/TLS, les moteurs AV, IPS et web filtering ne peuvent pas inspecter ce trafic, laissant passer librement les malwares et les communications C2 dissimulées dans des flux HTTPS apparemment légitimes. L'inspection SSL contrecarre également les attaques de type T1557 (Adversary-in-the-Middle) en permettant la détection de certificats frauduleux et d'injections de contenu dans les flux chiffrés. Le Health Check Sophos v22 recommande que l'action soit configurée sur "Decrypt" pour le trafic chiffré.

Impact potentiel

- Propagation de malwares via des flux HTTPS non inspectés (bypassing AV et IPS)
- Communications C2 indétectables utilisant HTTPS vers des domaines légitimes compromis
- T1557 : attaque adversary-in-the-middle sur le trafic chiffré non détectée sans inspection SSL
- Exfiltration de données chiffrées ne déclenchant aucune alarme sur les systèmes de détection

Navigation

```
Protect > Rules and policies > SSL/TLS inspection rules > Add
→ Action : Decrypt (deep packet inspection)
→ Appliquer aux zones et utilisateurs concernés
Protect > Rules and policies > Firewall rules > Éditer une règle
→ SSL/TLS inspection : sélectionner le profil d'inspection créé
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Rules and policies > SSL/TLS inspection rules
# Vérifier que des règles d'inspection Decrypt sont configurées
```

Remédiation

1. Créer un profil d'inspection SSL/TLS dans `Protect > Rules and policies > SSL/TLS inspection rules`

2. Configurer l'action `Decrypt` pour les catégories pertinentes (tout sauf Finances, Santé par défaut)
3. Déployer le certificat CA d'inspection sur les postes clients (via GPO pour Active Directory)
4. Attacher le profil d'inspection aux règles de pare-feu LAN-to-WAN
5. Surveiller les erreurs de certificat et ajuster les exemptions selon les besoins

Valeur par défaut : Inspection SSL/TLS non activée par défaut.

Critère de conformité : Règle d'inspection SSL/TLS active en mode `Decrypt` sur les règles LAN-to-WAN. Certificat CA d'inspection déployé sur les clients.

Contrôle 8.2 — Certificat CA dédié pour l'inspection SSL

> ***CIS Ref :*** *5.2 (étendu)* | ***MITRE :*** *T1557* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Le certificat CA utilisé pour l'inspection SSL/TLS doit être un certificat dédié et distinct des certificats d'administration du pare-feu. L'utilisation du certificat CA interne général pour l'inspection expose à des risques de compromission croisée si ce CA est utilisé pour signer d'autres certificats critiques.

Impact potentiel

- Compromission du CA d'inspection permettant la génération de certificats frauduleux
- Confusion entre les certificats d'inspection et les certificats d'infrastructure
- Non-traçabilité des certificats générés pour l'inspection SSL

Navigation

```
System > Certificates > Certificate Authorities > Add
→ Créer un CA dédié à l'inspection SSL (distinct du CA admin)
→ Nom : "Sophos SSL Inspection CA"
Protect > Rules and policies > SSL/TLS inspection rules
→ Dans la règle d'inspection, sélectionner le CA dédié
```

CLI de vérification

```
# Vérification dans l'interface web
# System > Certificates > Certificate Authorities
# Vérifier l'existence d'un CA dédié à l'inspection SSL
```

Remédiation

1. Créer un CA dédié à l'inspection SSL dans `System > Certificates > Certificate Authorities`
2. Utiliser une durée de validité de 5 ans maximum avec clé RSA 4096 bits
3. Ne pas utiliser ce CA pour signer d'autres certificats que ceux de l'inspection SSL
4. Déployer ce CA dans le magasin de certificats de confiance des navigateurs clients
5. Planifier le renouvellement avant expiration

Valeur par défaut : CA auto-généré à l'installation, non dédié.

Critère de conformité : CA dédié à l'inspection SSL configuré, distinct du CA d'administration. Déployé dans les navigateurs clients.

Contrôle 8.3 — Exemptions SSL documentées et limitées

> ***CIS Ref :*** *5.2 (étendu)* | ***MITRE :*** *T1071* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Les exemptions à l'inspection SSL (catégories Finances, Santé, certificats épinglés) sont nécessaires mais doivent être strictement contrôlées. Des exemptions non documentées ou trop larges créent des angles morts dans l'inspection du trafic que les attaquants peuvent exploiter pour établir des canaux C2 ou exfiltrer des données.

Impact potentiel

- Création de canaux non inspectés exploitables pour les C2 ou l'exfiltration
- Non-couverture de menaces utilisant des domaines dans des catégories exemptées
- Dérive progressive des exemptions rendant l'inspection SSL inefficace

Navigation

```
Protect > Rules and policies > SSL/TLS inspection rules
→ Règle "No Decrypt" : restreindre aux seules catégories nécessaires
  (Finances, Santé, certificats épinglés connus, services AD/LDAP)
→ Documenter chaque exemption avec justification business
→ Réviser les exemptions trimestriellement
```

CLI de vérification

```
# Vérification dans l'interface web
# Protect > Rules and policies > SSL/TLS inspection rules
# Auditer les règles "No Decrypt" et vérifier leur justification
```

Remédiation

1. Auditer toutes les règles SSL/TLS existantes avec action `No Decrypt`
2. Supprimer les exemptions non justifiées ou trop larges
3. Limiter les exemptions aux catégories strictement nécessaires (Finances, Santé, AD/LDAP interne)
4. Documenter chaque exemption dans un registre avec la justification business et la date de révision
5. Mettre en place une révision trimestrielle des exemptions

Valeur par défaut : Exemptions larges potentiellement configurées par défaut ou lors de l'implémentation initiale.

Critère de conformité : Chaque règle `No Decrypt` est documentée avec une justification business. Révision trimestrielle effectuée et tracée.

Domaine 9 — Services réseau et segmentation

Objectif : *Assurer la synchronisation NTP, activer la protection DNS, segmenter le réseau via des VLANs, protéger contre le spoofing réseau à la couche 2 (ARP, DHCP rogue), et configurer le réseau sans fil en toute sécurité. Limite la propagation des menaces et empêche les attaques adversary-in-the-middle internes.*

Contrôle 9.1 — NTP configuré avec au moins deux sources de temps

CIS Ref : *1.1.3* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

Une horloge désynchronisée invalide les certificats TLS (erreurs de validité temporelle), perturbe la corrélation des logs dans le SIEM, et peut compromettre le fonctionnement des règles basées sur des planifications horaires. La synchronisation NTP avec au moins deux sources garantit la précision temporelle même en cas d'indisponibilité d'une source. Le Health Check Sophos v22 recommande l'utilisation de pool.ntp.org et time.google.com comme sources de référence.

Impact potentiel

- Invalidation des certificats TLS avec des erreurs de validité temporelle
- Incohérence des timestamps dans les logs rendant la corrélation SIEM impossible
- Dysfonctionnement des règles de pare-feu basées sur des plages horaires

Navigation

```
System > Administration > Time
→ Time zone : sélectionner le fuseau horaire correct
→ Use pre-defined NTP Server : cocher (ou Use custom NTP Server)
→ Configurer au moins 2 serveurs NTP (ex : pool.ntp.org, time.google.com)
→ Cliquer sur "Apply"
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
system diagnostics show version
# Vérifier l'heure système :
date
```

Remédiation

1. Naviguer vers `System > Administration > Time`
2. Définir le fuseau horaire correct

3. Configurer au moins deux serveurs NTP : `pool.ntp.org` et `time.google.com` (recommandés par Health Check v22), ou des serveurs NTP internes Stratum 2 avec fallback sur ces sources publiques
4. Vérifier la synchronisation après application
5. S'assurer que le trafic NTP (port UDP 123) est autorisé par les règles de pare-feu vers les serveurs NTP

Valeur par défaut : NTP non configuré par défaut.

Critère de conformité : Au moins deux serveurs NTP configurés (ex : pool.ntp.org + time.google.com). Horloge synchronisée (décalage < 1 seconde). Fuseau horaire correct.

Contrôle 9.2 — Protection DNS Sophos activée

> ***CIS Ref :*** *5.12* | ***MITRE :*** *T1071, T1568* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Le DNS est utilisé par la majorité des malwares pour la résolution de leurs serveurs C2 et pour les communications exfiltrées via DNS tunneling. La protection DNS Sophos (Sophos DNS over HTTPS / DNS Protection) filtre les requêtes DNS en utilisant les feeds de réputation X-Ops pour bloquer les résolutions vers des domaines malveillants.

Impact potentiel

- Communication avec des serveurs C2 via des requêtes DNS non filtrées
- Exfiltration de données via DNS tunneling non détectée
- Propagation de malwares via des domaines distribués par des réseaux DGA (Domain Generation Algorithms)

Navigation

```
System > Administration > Device Access (ou Network > DNS)
→ Activer Sophos DNS Protection
→ Configurer les serveurs DNS de Sophos (ou DoH Sophos)
→ Protect > Web > DNS Protection (si disponible dans la licence)
→ Activer le filtrage de catégories DNS malveillantes
```

CLI de vérification

```
# Vérification dans l'interface web
# Network > DNS : vérifier que la protection DNS est activée
# System > Administration > Licensing : vérifier l'abonnement DNS Protection
```

Remédiation

1. Vérifier que l'abonnement DNS Protection est actif
2. Naviguer vers la configuration DNS et activer la protection Sophos
3. Configurer les serveurs DNS Sophos comme résolveurs primaires pour les clients LAN
4. Activer le filtrage de catégories DNS (Malware, Phishing, C2)

5. Surveiller les logs DNS pour identifier les tentatives de connexion à des domaines malveillants

Valeur par défaut : DNS Protection non activée par défaut.

Critère de conformité : DNS Protection activée. Catégories malveillantes bloquées au niveau DNS. Logs DNS actifs.

Contrôle 9.3 — Segmentation réseau par VLANs et zones de sécurité

CIS Ref : *(Best practice)* | ***MITRE :*** *T1210* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

L'absence de segmentation réseau permet à un malware ou à un attaquant ayant compromis un endpoint de se déplacer latéralement vers tous les systèmes du réseau sans restriction. La segmentation via des VLANs et zones de sécurité distinctes (LAN utilisateurs, DMZ, serveurs, IoT) limite la propagation et force le trafic inter-zones à traverser le pare-feu.

Impact potentiel

- Propagation non contrôlée d'un ransomware via le réseau plat
- Accès direct depuis la zone utilisateurs vers les serveurs critiques sans inspection
- Contamination des systèmes industriels (OT/IoT) depuis le réseau IT

Navigation

```
Network > Interfaces > Add interface
→ Créer des interfaces VLAN pour chaque zone (Users, Servers, DMZ, IoT, Management)
Network > Zones > Add zone
→ Définir des zones distinctes avec des niveaux de confiance appropriés
Protect > Rules and policies > Firewall rules
→ Créer des règles explicites inter-zones avec profils de sécurité
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
show network interface
# Vérifier la présence de VLANs et zones de sécurité distinctes
```

Remédiation

1. Cartographier les flux légitimes entre les zones avant la segmentation
2. Créer des interfaces VLAN distinctes dans `Network > Interfaces`
3. Définir des zones de sécurité correspondantes dans `Network > Zones`
4. Créer des règles de pare-feu inter-zones explicites avec profils de sécurité
5. Implémenter une politique de moindre privilège inter-zones (deny by default)

Valeur par défaut : Zones LAN et WAN configurées d'usine. Segmentation supplémentaire à configurer selon l'architecture.

Critère de conformité : Au moins 3 zones de sécurité distinctes (Users, Servers/DMZ, Management). Règles inter-zones explicites avec profils de sécurité.

Contrôle 9.4 — Protection Wireless avancée — WPA3-Enterprise, WIDS et détection Rogue AP (ENRICHI — v1.4)

CIS Ref : *5.9* | ***MITRE :*** *T1040 (Network Sniffing), T1200 (Hardware Additions — rogue AP), T1498 (Deauth attacks)* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Les réseaux sans fil mal configurés constituent des vecteurs d'attaque supplémentaires permettant d'atteindre le réseau interne sans traverser le périmètre physique. Les attaques against les réseaux WiFi corporatifs comprennent : l'exploitation de WPA2-Personal avec des clés partagées faibles, les attaques de désauthentification (deauth) pour forcer le handshake, les points d'accès malveillants (rogue AP / evil-twin) imitant les SSID légitimes, et l'absence d'isolation empêchant la contamination entre clients. Pour les déploiements utilisant Sophos Access Points (AP) gérés par Sophos Firewall, la configuration sécurisée inclut WPA3-Enterprise avec 802.1X/RADIUS, le WIDS (Wireless Intrusion Detection System), la détection de rogue AP, et l'isolation des clients invités.

Impact potentiel

- T1040 : interception du trafic sans fil via des attaques sur WPA2-Personal avec capture du handshake et cracking hors ligne
- T1200 : déploiement d'un rogue AP ou evil-twin imitant un SSID légitime pour intercepter les connexions
- T1498 : attaques de désauthentification forçant les clients à se reconnecter à un evil-twin
- Accès non autorisé au réseau interne depuis un réseau invité non isolé
- Mouvement latéral entre clients sans fil si l'isolation n'est pas activée

Navigation — WPA3-Enterprise avec 802.1X

```
Protect > Wireless > Access Points > [AP] > Network > SSID Settings
→ SSID corporatif :
  - Security mode : WPA3-Enterprise (recommandé) ou WPA2/WPA3-Enterprise (transition)
  - Authentication : 802.1X (EAP-TLS ou PEAP-MSCHAPv2)
  - RADIUS server : configurer l'IP du serveur RADIUS
    (Sophos Firewall peut servir de serveur RADIUS interne ou déléguer à un serveur externe)
  - RADIUS port : 1812 (Authentication), 1813 (Accounting)
  - Secret partagé RADIUS : ≥ 32 caractères, stocké dans un vault

Configuration du RADIUS interne Sophos Firewall (si applicable) :
  Configure > Authentication > Services > RADIUS
  → Enable RADIUS server : activer
  → Define authentication backend : Active Directory (via STAS ou LDAP)

→ SSID invité :
  - Security mode : WPA3-Personal ou WPA2/WPA3-Personal
  - Mot de passe : unique, rotatif (changer tous les 30 jours), affiché via portail captif
  - Captive portal : activer avec conditions d'utilisation
  - VLAN : VLAN dédié invité — AUCUN accès aux ressources internes
  - Access to internal network : Block (zéro accès aux zones LAN/DMZ)
```

Navigation — Isolation client

```
Protect > Wireless > Access Points > [AP] > Network > SSID Settings
→ Client isolation : activer
  (empêche les clients sans fil de communiquer directement entre eux —
   tout le trafic inter-clients passe obligatoirement par le pare-feu)
→ Appliquer sur : réseaux invités ET réseaux BYOD
→ Sur les réseaux corporatifs : désactiver UNIQUEMENT si la communication
  directe entre postes est nécessaire (cas exceptionnel à documenter)
```

Navigation — Détection Rogue AP

```
Wireless > Rogue AP settings
→ Enable Rogue AP detection : activer
→ Scan interval : définir la fréquence de scan (recommandé : toutes les heures)
→ Known access points : lister les AP légitimes de l'organisation (avec BSSID)
→ Action on detection :
  - Alert : générer une alerte dans les logs et notifications
  - Block (si supporté) : bloquer les trames provenant du rogue AP
→ Exporter la liste des AP connus régulièrement

Vérification des AP détectés :
Wireless > Rogue AP settings > Detected APs
→ Passer en revue les AP inconnus détectés
→ Marquer les AP légitimes voisins comme "Neighbor" (non menaçants)
→ Investiguer tout AP correspondant à un SSID interne connu
```

Navigation — WIDS (Wireless Intrusion Detection System)

```
Wireless > WIDS (ou Wireless > Advanced settings > WIDS policy)
→ Enable WIDS : activer
→ Détecter les attaques de désauthentification (deauth attacks) :
  - Deauthentication flood detection : activer
  - Threshold : 50 trames deauth en 10 secondes = alerte
→ Détecter les evil-twin (AP imitant un SSID légitime avec BSSID différent) :
  - SSID spoofing detection : activer
→ Détecter les clients suspects :
  - Client probe flood detection : activer
→ Actions WIDS :
  - Log toutes les détections
  - Générer des alertes email (via Configure > System services > Notification list)
  - Intégrer dans le SIEM via syslog
```

Navigation — SSID de gestion (si utilisé)

```
Wireless > Access Points > [AP] > Network > SSID Settings
→ Management SSID (si configuré) :
  - Broadcast SSID : désactiver (SSID caché — ne pas diffuser)
  - Note : la non-diffusion ne remplace pas le chiffrement —
    elle réduit seulement l'exposition aux scans automatiques
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier les AP enregistrés et leur statut
show wireless ap-status

# Vérifier les SSID configurés et leur mode de sécurité
show wireless ssid configuration

# Vérifier le statut du WIDS
show wireless wids status

# Vérifier les rogue AP détectés
show wireless rogue-ap detected

# Vérification dans l'interface web
# Protect > Wireless > Access Points : vérifier le mode de sécurité de chaque SSID
# Wireless > Rogue AP settings : vérifier la détection active et les AP détectés récemment
```

Table de configuration wireless par type de SSID

TYPE DE SSID	MODE DE SÉCURITÉ	ISOLATION CLIENT	VLAN	CAPTIVE PORTAL	ACCÈS INTERNE
Corporatif (employés)	WPA3-Enterprise 802.1X	Non (sauf BYOD)	VLAN Users	Non	Oui (via règles FW)
BYOD	WPA3-Enterprise 802.1X	Oui	VLAN BYOD	Non	Limité (HTTP/ HTTPS only)
Invité	WPA3-Personal	Oui		Oui	Aucun

TYPE DE SSID	MODE DE SÉCURITÉ	ISOLATION CLIENT	VLAN	CAPTIVE PORTAL	ACCÈS INTERNE
			VLAN Guests		
IoT	WPA2/WPA3-Personal	Oui	VLAN IoT	Non	Aucun (sortie Internet seulement)
Gestion (caché)	WPA3-Personal	Non	VLAN Management	Non	Oui (réservé admins)

Remédiation

1. Naviguer vers `Protect > Wireless Protection > SSIDs` et auditer tous les SSID configurés
2. Migrer les SSID corporatifs vers **WPA3-Enterprise avec 802.1X** — configurer le serveur RADIUS interne ou externe
3. Activer l'isolation client sur tous les SSID invités et BYOD
4. Associer chaque SSID à un VLAN dédié (jamais le VLAN management sur un SSID non protégé)
5. Configurer le réseau invité avec portail captif, conditions d'utilisation, et zéro accès aux ressources internes
6. Naviguer vers `Wireless > Rogue AP settings` et activer la détection de rogue AP — inventorier les AP légitimes
7. Activer le WIDS pour détecter les attaques deauth et les evil-twin AP
8. Désactiver le broadcast du SSID de gestion si utilisé
9. Intégrer les alertes WIDS dans le SIEM via syslog
10. Planifier une revue mensuelle des rogue AP détectés pour identifier les AP voisins légitimes vs. malveillants

Valeur par défaut : Wireless Protection non configuré par défaut (dépend du matériel AP). WPA3-Enterprise et WIDS nécessitent une configuration explicite.

Critère de conformité : WPA3-Enterprise avec 802.1X sur les SSID corporatifs. Client isolation activé sur les SSID invités et BYOD. Chaque SSID sur un VLAN dédié. Rogue AP detection activé. WIDS activé avec détection deauth et SSID spoofing. Alertes WIDS intégrées dans le SIEM.

Contrôle 9.5 — Protection anti-spoofing couche 2 — ARP Inspection et prévention DHCP rogue (NOUVEAU)

CIS Ref : *(Best practice — Layer 2 Security)* | ***MITRE :*** *T1557 (Adversary-in-the-Middle — ARP/DHCP spoofing)* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Les attaques par empoisonnement ARP (ARP spoofing) et les serveurs DHCP frauduleux (rogue DHCP) permettent à un attaquant présent sur le réseau local de se positionner en man-in-the-middle entre les hôtes et la passerelle, interceptant silencieusement tout le trafic sans détection apparente. T1557 (Adversary-in-the-Middle) via ARP/DHCP spoofing est une technique d'attaque courante dans les phases de mouvement latéral et d'interception de credentials sur des réseaux internes non segmentés.

La protection anti-spoofing de couche 2 dans SFOS agit en deux niveaux complémentaires : 1. **Vérification de la source des routes (Source Route Verification)** : empêche les paquets avec une adresse source ne correspondant pas à l'interface de réception 2. **Prévention du spoofing MAC-IP** : lie les adresses MAC aux adresses IP pour les hôtes critiques, empêchant l'usurpation d'identité réseau

Impact potentiel

- T1557 : interception silencieuse de tout le trafic du réseau via empoisonnement ARP
- Capture de credentials en clair (authentifications HTTP, LDAP, mots de passe) via le positionnement MitM
- Redirection du trafic DNS vers un serveur frauduleux (DNS spoofing via DHCP rogue)
- Défaillance de la segmentation réseau si l'attaquant peut usurper l'adresse de la passerelle inter-VLAN
- Contournement des politiques de pare-feu basées sur l'adresse IP source si celle-ci est usurpée

Navigation — Configuration protection couche 2

```
Section 1 : Protection DoS et Anti-Spoofing (niveau pare-feu)
Protect > Intrusion Prevention > DoS & Spoof Protection
→ Spoof Prevention : activer sur toutes les interfaces
  - Source route verification : activer
    (vérifie que la route de retour vers l'IP source correspond à l'interface d'arrivée)
  - Loose Source Routing : Block (bloquer les paquets IP avec options de routage source)
  - Strict Source Routing : Block
  - Record Route : Block (empêche l'enregistrement de la route par les paquets IP)
→ Appliquer sur les zones LAN et DMZ en priorité

Section 2 : Liaison MAC-IP pour les serveurs critiques
Network > Interfaces > [interface LAN/DMZ] > Advanced > Spoof Prevention
→ MAC-IP anti-spoofing : activer sur les interfaces critiques
→ Ajouter les liaisons MAC/IP des serveurs critiques (AD, bases de données, passerelles)
→ Action si violation : Block (bloquer le trafic avec MAC-IP non conforme)
→ Activer l'alerte/log sur les violations pour détection d'incident

Section 3 : Prévention des serveurs DHCP frauduleux
Protect > Intrusion Prevention > DoS & Spoof Protection
→ DHCP server protection : activer
→ Trusted DHCP servers : lister les IP des serveurs DHCP légitimes
→ Bloquer les réponses DHCP depuis des sources non autorisées

Section 4 : Protection au niveau des interfaces réseau
Network > Interfaces > [interface] > Advanced > Spoof Prevention
→ Pour chaque interface LAN/DMZ :
  - Enable spoof prevention : activer
  - ARP reply validation : activer (vérification des réponses ARP)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier la configuration anti-spoofing
show spoof-prevention configuration

# Vérifier les violations détectées (log des tentatives de spoofing)
show log type spoof-prevention last 100

# Vérifier les liaisons MAC-IP configurées
show mac-ip binding

# Vérification dans l'interface web
# Protect > Intrusion Prevention > DoS & Spoof Protection
# Vérifier que Spoof Prevention est activé et Source Route Verification = Block
```

Table des protections par vecteur d'attaque

VECTEUR	TECHNIQUE	PROTECTION SFOS	NAVIGATION
ARP Spoofing	Empoisonnement de la table ARP	MAC-IP anti-spoofing + ARP validation	Network > Interfaces > Advanced
DHCP Rogue	Faux serveur DHCP distribuant une passerelle malveillante	DHCP server protection	DoS & Spoof Protection
IP Spoofing	Usurpation d'adresse IP source	Source Route Verification	DoS & Spoof Protection
Routage source	Options IP de routage source forçant un chemin spécifique	Block Loose/Strict Source Routing	DoS & Spoof Protection

Remédiation

1. Naviguer vers `Protect > Intrusion Prevention > DoS & Spoof Protection`
2. Activer la protection Spoof Prevention sur toutes les interfaces LAN et DMZ
3. Activer Source Route Verification pour prévenir le spoofing d'adresse IP source
4. Bloquer Loose Source Routing et Strict Source Routing dans les options IP
5. Naviguer vers `Network > Interfaces > [interface] > Advanced` et activer le MAC-IP anti-spoofing sur les interfaces des zones critiques
6. Créer des liaisons MAC-IP statiques pour les serveurs critiques (contrôleurs AD, serveurs de bases de données, passerelles réseau)
7. Configurer la protection DHCP server pour ne permettre les réponses DHCP qu'aux serveurs autorisés
8. Activer les logs sur les violations de spoofing pour la détection d'incidents
9. Intégrer les logs de violation ARP/DHCP dans le SIEM pour corrélation avec d'autres indicateurs d'attaque MitM

Valeur par défaut : Protection anti-spoofing partiellement activée. MAC-IP anti-spoofing non configuré par défaut. Liaisons MAC-IP à configurer manuellement pour les serveurs critiques.

Critère de conformité : Spoof Prevention activé sur toutes les interfaces LAN/DMZ. Source Route Verification activé. Liaisons MAC-IP configurées pour les serveurs critiques. Logs de violation activés et intégrés dans le SIEM.

Contrôle 9.6 — Durcissement de la haute disponibilité (HA) Active-Passive (NOUVEAU — v1.4)

CIS Ref : *(Best practice — HA Security, SFOS v22)* | ***MITRE :*** *T1499 (Service Denial — HA prevents), T1200 (Hardware Additions — rogue HA node)* | ***Niveau :*** 🔵 *L2*

Description du risque

La configuration HA (High Availability) Active-Passive de Sophos Firewall présente des risques de sécurité spécifiques au-delà de la simple disponibilité. Le lien de synchronisation HA transporte en continu la configuration complète du pare-feu (règles, secrets VPN, identifiants LDAP) entre les deux nœuds. Un lien HA non sécurisé, partagé avec le trafic de données ou sans authentification forte, constitue un vecteur d'attaque permettant l'interception de la configuration ou l'injection d'un nœud HA frauduleux. T1200 (Hardware Additions) couvre les attaques consistant à injecter un équipement non autorisé dans l'infrastructure — un faux nœud HA serait une variante physique de cette technique. T1499 souligne que la HA est elle-même un mécanisme de prévention du déni de service.

Impact potentiel

- T1200 : injection d'un nœud HA malveillant qui reçoit la configuration complète du pare-feu incluant les secrets VPN et les règles de sécurité
- Interception de la synchronisation HA (configuration en clair) si le lien HA n'est pas chiffré
- Instabilité de la paire HA ("flapping") si la préemption est activée — fenêtres de basculement répétées exploitables
- Désynchronisation silencieuse entre nœuds créant des politiques de sécurité incohérentes sur les deux équipements
- Accès non autorisé à l'équipement auxiliaire via une IP de gestion partagée avec le VIP de basculement

Interface HA dédiée

```
Configure > System Services > High Availability > HA Configuration
→ HA link : sélectionner une interface DÉDIÉE uniquement au lien HA
  - NE JAMAIS partager le lien HA heartbeat avec le trafic de données
  - Utiliser une interface physique dédiée (ex : Port 8 réservé HA)
  - Si pas d'interface dédiée disponible : utiliser un VLAN HA isolé sur un trunk dédié
→ HA link interface : vérifier que l'interface sélectionnée n'est pas
  utilisée pour autre chose dans Network > Interfaces
```

Mot de passe HA (Authentication Password)

```
System > High Availability > HA Configuration > Authentication Password
→ Configurer un mot de passe fort pour l'authentification du lien HA
  - Longueur minimum : 20 caractères
  - Composition : aléatoire (générer avec un gestionnaire de mots de passe)
  - Stocker dans un vault (HashiCorp Vault, CyberArk, ou équivalent)
  - Ce mot de passe authentifie les deux nœuds HA l'un envers l'autre —
    un mot de passe faible permet l'usurpation d'un nœud
→ Appliquer le même mot de passe sur les DEUX nœuds
→ Changer ce mot de passe lors de la rotation des secrets de l'équipement (annuelle)
```

Chiffrement du lien HA

```
System > High Availability > HA Configuration
→ Encrypt HA sync traffic : activer
  (chiffre toutes les données de synchronisation entre les nœuds —
   règles, sessions, tables de connexion)
→ Vérifier que le chiffrement est bien actif sur les DEUX nœuds
```

Surveillance des interfaces (Device Monitoring)

```
System > High Availability > HA Configuration > Device monitoring
→ Monitor interfaces : sélectionner TOUTES les interfaces critiques à surveiller
  (WAN, LAN, DMZ — les interfaces qui, si elles tombent, doivent déclencher un basculement)
→ Ne pas surveiller l'interface HA elle-même (créerait des basculements indésirables)
→ Monitor gateways : activer pour les gateways WAN critiques
  (basculer si la connectivité Internet est perdue sur le nœud primaire)
→ Failover on interface down : activer
```

Désactivation de la préemption

```
System > High Availability > HA Configuration
→ Preemption : désactiver (= OFF)
  (la préemption force le nœud primaire à reprendre la main après récupération —
   ce comportement crée un basculement supplémentaire "retour vers le primaire"
   qui génère une courte coupure de service et peut être exploité par un attaquant
   pour créer des instabilités répétées)
→ Avec la préemption désactivée : après un basculement, le nœud secondaire
   reste actif jusqu'au prochain basculement planifié en maintenance
```

Accès à l'équipement auxiliaire

```
System > High Availability > Device Status
→ Auxiliary device IP (Dedicated management IP) : configurer une IP de gestion dédiée
  pour l'accès à l'équipement auxiliaire (DISTINCTE du VIP de basculement)
  - TOUJOURS accéder à l'équipement auxiliaire via son IP de gestion dédiée
  - NE JAMAIS utiliser le VIP de basculement pour accéder à l'auxiliaire
    (risque de confondre l'équipement actif et l'auxiliaire lors d'opérations de
maintenance)
→ Vérifier que l'IP de gestion auxiliaire est accessible depuis le VLAN de management
```

Cohérence firmware entre les nœuds

```
Procédure de mise à jour SFOS en HA (staggered upgrade) :

Étape 1 : Mettre à jour l'équipement auxiliaire (nœud passif) en premier
System > Backup & Firmware > Firmware > [connecté à l'auxiliaire via son IP dédiée]
→ Télécharger et installer la nouvelle version SFOS sur l'auxiliaire
→ Vérifier le démarrage et l'état opérationnel de l'auxiliaire sur la nouvelle version

Étape 2 : Vérifier la synchronisation et la cohérence
System > High Availability > Device Status
→ Vérifier que les deux nœuds sont en bonne santé avant de continuer
→ S'assurer qu'aucune alerte n'est présente

Étape 3 : Déclencher le basculement vers l'auxiliaire (maintenant sur la nouvelle version)
System > High Availability > Failover > Initiate manual failover
→ L'équipement auxiliaire (déjà mis à jour) devient actif

Étape 4 : Mettre à jour l'équipement qui est maintenant passif (ancien primaire)
→ Mettre à jour le firmware sur ce nœud
→ Vérifier son état opérationnel

Étape 5 : Rétablir l'état souhaité (optionnel)
→ Effectuer un basculement retour vers le nœud primaire si nécessaire
→ NE JAMAIS avoir les deux nœuds sur des versions SFOS différentes de manière durable
```

Vérification de santé HA

```
System > High Availability > Device Status
→ Vérifier :
  - HA Status : "Established[Active-Passive]"
  - Primary node : état = Active
  - Auxiliary node : état = Standby (opérationnel)
  - Sync state : Synchronized
  - Interface monitoring : toutes les interfaces surveillées en statut Up
  - Last sync : récent (< 1 minute)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Statut complet de la paire HA
system ha show status

# Vérifier les statistiques HA (paquets heartbeat, sync status)
system ha show statistics

# État détaillé des nœuds HA
show high-availability state

# Vérifier la configuration HA (interfaces surveillées, mot de passe, chiffrement)
show high-availability configuration

# Logs HA (basculements récents, erreurs)
system ha show log

# Vérifier la cohérence des versions entre nœuds
system diagnostics show version
# Comparer avec la version sur l'équipement auxiliaire
```

Remédiation

1. Vérifier que l'interface HA heartbeat est **dédiée** et non partagée avec le trafic de données (`Configure > System Services > High Availability > HA Configuration`)
2. Configurer un **mot de passe HA fort** (≥ 20 caractères, aléatoire) dans `System > High Availability > HA Configuration > Authentication Password` — appliquer le même mot de passe sur les deux nœuds
3. Activer le **chiffrement du lien HA** (`Encrypt HA sync traffic = ON`) sur les deux nœuds
4. Configurer `Monitor interfaces` pour surveiller toutes les interfaces critiques (WAN, LAN, DMZ) et déclencher le basculement en cas de panne
5. **Désactiver la préemption** pour éviter les basculements instables après récupération temporaire
6. Configurer une **IP de gestion dédiée** pour l'équipement auxiliaire (distincte du VIP de basculement)
7. Utiliser la **procédure de mise à jour staggered** (auxiliaire en premier, puis primaire) pour maintenir la cohérence des versions SFOS
8. Vérifier le statut HA régulièrement via `System > High Availability > Device Status` — aucun nœud ne doit être en état Faulty
9. Stocker le mot de passe HA dans le vault des secrets de l'organisation (même politique que les autres identifiants critiques)
10. Tester le basculement en conditions contrôlées (maintenance programmée) au moins une fois par an

Valeur par défaut : Aucun mot de passe HA configuré par défaut. Chiffrement HA non activé par défaut. Préemption désactivée par défaut sur certaines versions — vérifier explicitement.

Critère de conformité : Lien HA sur interface dédiée (non partagée avec données). Mot de passe HA ≥ 20 caractères configuré. Chiffrement HA activé. Préemption désactivée. Interfaces critiques surveillées. IP dédiée pour l'accès à l'auxiliaire. Deux nœuds sur la même version SFOS. `system ha show status` = Established[Active-Passive], Sync state = Synchronized.

Domaine 10 — Journalisation, supervision SIEM et conformité

Objectif : *Centraliser les logs dans un SIEM externe, journaliser toutes les règles de pare-feu et les événements d'authentification, maintenir une rétention suffisante, configurer des alertes sur les événements critiques, activer l'export de flux réseau IPFIX/sFlow pour la chasse aux menaces, et produire des rapports de conformité PCI-DSS, RGPD et NIS2 pour les besoins d'audit.*

Contrôle 10.1 — Syslog sécurisé vers SIEM externe — TLS, livraison fiable et logs immuables (ENRICHI — v1.4)

CIS Ref : *3.7* | ***MITRE :*** *T1562.006 (Indicator Blocking — disable logging), T1070.002 (Clear Logs)* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Les logs stockés uniquement sur le pare-feu sont vulnérables à la suppression par un attaquant ayant compromis l'équipement (T1070.002 — Clear Logs). L'envoi en temps réel vers un SIEM externe garantit l'intégrité des logs et permet la corrélation d'événements avec d'autres sources. Cependant, le choix du protocole de transport est critique : syslog en UDP (port 514) est non chiffré et sans garantie de livraison — les paquets peuvent être perdus, interceptés ou falsifiés en transit. T1562.006 couvre la désactivation ou l'altération des mécanismes de journalisation. Un syslog non chiffré en UDP expose en plus les logs au sniffing réseau et à l'injection de faux événements dans le SIEM. La politique recommandée est : **syslog over TLS (port 6514) en mode TCP fiable**.

Impact potentiel

- T1070.002 : un attaquant ayant compromis le pare-feu peut supprimer les logs locaux — sans transfert immédiat vers un SIEM externe immuable, les preuves sont perdues
- T1562.006 : désactivation silencieuse de la journalisation par un attaquant — non détectable sans surveillance du flux syslog
- Interception des logs syslog UDP en clair sur le réseau (contiennent des informations sur la topologie, les IP sources, les comptes)
- Perte silencieuse de logs en UDP (paquets droppés sous charge réseau) rendant l'investigation incomplète
- Non-conformité réglementaire (PCI-DSS Req. 10.2, NIS2 Art. 21, ISO 27001 A.12.4) liée à l'absence de journalisation sécurisée

Navigation — Syslog over TLS (port 6514)

```
System > Logging > Syslog server > Add
→ Server name : [nom descriptif du SIEM]
→ IP address : adresse IP du collecteur syslog / SIEM
→ Port : 6514 (syslog over TLS — RFC 5425)
  (NE PAS utiliser le port 514 UDP en production — non chiffré, sans fiabilité)
→ Protocol : TCP (OBLIGATOIRE pour la fiabilité de livraison)
→ Encryption : TLS (activer le chiffrement TLS du transport)
  - Validate server certificate : activer
    (vérifier le certificat du serveur syslog — prévient les attaques MitM sur le canal de log)
  - CA certificate : importer le certificat CA du serveur syslog
→ Facility : Local0 à Local7 (selon la configuration de séparation des sources dans le SIEM)
→ Severity : Information (ou ajuster selon la politique de logging)
→ Log format : sélectionner selon le SIEM :
  - CEF (Common Event Format) : Splunk, QRadar, ArcSight
  - LEEF (Log Event Extended Format) : QRadar
  - Standard syslog RFC 5424 : ELK Stack, Graylog, autres
→ Cocher TOUTES les catégories de logs :
  - Firewall rules
  - IPS
  - Web filtering
  - Email
  - VPN
  - System
  - Admin (modifications de configuration — CRITIQUE)
  - Authentication
  - Wireless (si applicable)
→ Cliquer sur "Save"
```

Navigation — Mode TCP pour la fiabilité de livraison

```
System > Logging > Syslog server > [serveur] > Edit
→ Protocol : TCP (mode TCP = livraison fiable avec accusé de réception)
  vs UDP (mode UDP = fire-and-forget, paquets pouvant être perdus silencieusement)
  IMPORTANT : le mode TCP garantit que chaque message syslog est livré —
  essentiel pour les environnements PCI-DSS et NIS2 qui exigent une intégrité de l'audit trail
→ Vérifier que le SIEM/collecteur est configuré pour accepter les connexions TCP syslog
```

Navigation — Sauvegarde des logs (Log Backup)

```
System > Logging > Log Backup settings
→ Activer la sauvegarde des logs locaux vers un serveur distant
→ Server : IP du serveur de backup (distinct du SIEM)
→ Fréquence : quotidienne
→ Chiffrement : activer (les fichiers de backup de logs doivent être chiffrés)
→ Rétention locale : maximiser selon la capacité disque du pare-feu
```

Politique de rétention et d'immuabilité

```
Politique recommandée (double rétention) :
  - Rétention locale (pare-feu) : maximiser selon capacité (généralement 7 à 30 jours)
  - Rétention SIEM / SOC : minimum 90 jours pour la conformité réglementaire de base
  - Rétention archive long terme : minimum 1 an (NIS2, PCI-DSS Req. 10.7, ISO 27001)
  - Logs immuables : configurer le SIEM en mode "write-once" pour les logs critiques
    (Splunk : index avec archival, Elastic : ILM avec frozen tier, QRadar : log archive)
  - Forward immediat : les logs doivent être transmis au SIEM en temps réel
    (ne pas accumuler en local puis transférer — risque de perte si le pare-feu est
compromis)

Vérification de l'intégrité du flux syslog :
  Configurer une alerte dans le SIEM si aucun log n'est reçu du pare-feu pendant > 5 minutes
  (indicateur de coupure du lien syslog ou de désactivation de la journalisation)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier la configuration syslog (serveurs configurés, protocole, chiffrement)
show syslog configuration

# Vérifier le statut de connexion au serveur syslog
show syslog connection-status

# Vérifier les statistiques d'envoi de logs (paquets envoyés, erreurs)
show syslog statistics

# Tester la connectivité vers le serveur syslog
system diagnostics ping <syslog-server-ip>

# Tester la connexion TLS vers le serveur syslog (port 6514)
system diagnostics test-syslog-connection

# Vérification dans l'interface web
# System > Logging > Syslog server
# Vérifier : Protocol = TCP, Port = 6514, Encryption = TLS, statut = Connected
```

Table de comparaison des modes de transport syslog

MODE	CHIFFREMENT	FIABILITÉ	PORT	CONFORMITÉ	RECOMMANDATION
UDP plain	Aucun	Aucune (paquets perdus)	514	Non conforme PCI-DSS	A BANNIR en production
TCP plain	Aucun	Fiable (TCP ACK)	514	Insuffisant	Acceptable en réseau isolé uniquement
TLS over TCP	TLS 1.2+	Fiable + chiffré	6514	Conforme PCI-DSS/NIS2	RECOMMANDE

Remédiation

1. Naviguer vers `System > Logging > Syslog server > Add`

2. Configurer le serveur syslog avec **protocole TCP** et **chiffrement TLS** sur le **port 6514** (RFC 5425)
3. Activer la validation du certificat du serveur syslog (`Validate server certificate = ON`) pour prévenir les attaques MitM sur le canal de journalisation
4. Importer le certificat CA du serveur syslog SIEM si nécessaire
5. Sélectionner le format de log compatible avec le SIEM (CEF pour Splunk/QRadar, standard pour ELK)
6. Activer **toutes les catégories de logs** — en particulier Admin et Authentication
7. Vérifier la réception via `show syslog statistics` et dans le SIEM
8. Configurer une **alerte dans le SIEM** si aucun log n'est reçu du pare-feu pendant > 5 minutes (détection de coupure ou désactivation de logging)
9. Configurer la politique de rétention : 90 jours minimum en SIEM, 1 an en archive
10. Activer le mode immuable sur les index SIEM pour les logs du pare-feu
11. Désactiver ou reconfigurer tout serveur syslog UDP plain existant (port 514 UDP)

Valeur par défaut : Syslog non configuré par défaut. Si configuré manuellement sans précautions, le port 514 UDP est souvent utilisé par défaut.

Critère de conformité : Serveur syslog configuré en TCP TLS sur le port 6514. Certificat du serveur syslog validé. Toutes les catégories de logs activées (Admin, Auth, Firewall, IPS, VPN, System). Réception vérifiée dans le SIEM. Alerte SIEM sur absence de logs > 5 min. Rétention ≥ 90 jours SIEM + 1 an archive. `show syslog statistics` ne retourne pas d'erreurs de connexion.

Contrôle 10.2 — Logging activé sur toutes les règles de pare-feu

CIS Ref : *3.7 (étendu)* | ***MITRE :*** *T1562* | ***Niveau :*** 🟢 *L1*

Description du risque

Des règles de pare-feu sans logging ne permettent pas d'investiguer le trafic autorisé ou bloqué lors d'un incident de sécurité. La traçabilité complète des connexions est une exigence de nombreux référentiels de conformité (PCI-DSS, ISO 27001, NIS2) et est indispensable pour la forensique post-incident.

Impact potentiel

- Impossibilité d'investiguer les connexions réseau lors d'un incident
- Non-conformité réglementaire (PCI-DSS Req. 10, NIS2, ISO 27001)
- Absence de preuves lors d'investigations forensiques ou de poursuites judiciaires

Navigation

```
Protect > Rules and policies > Firewall rules > Éditer chaque règle
→ Logging > Log firewall traffic : cocher
→ Appliquer sur TOUTES les règles (autorisation ET blocage)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
show firewall-rule
# Vérifier que toutes les règles ont le logging activé
```

Remédiation

1. Naviguer vers `Protect > Rules and policies > Firewall rules`
2. Éditer chaque règle et activer `Log firewall traffic`
3. Automatiser via un script CLI pour les environnements avec de nombreuses règles
4. Vérifier que les logs sont bien reçus dans le SIEM pour les règles critiques
5. Configurer une alerte dans le SIEM sur les catégories de trafic suspect

Valeur par défaut : Logging non activé par défaut sur les nouvelles règles.

Critère de conformité : 100% des règles de pare-feu actives ont `Log firewall traffic` = activé.

Contrôle 10.3 — Logs d'authentification activés

CIS Ref : *3.7 (étendu)* | ***MITRE :*** *T1078, T1110* | ***Niveau :*** 🟢 *L1*

Description du risque

Les logs d'authentification permettent de détecter les tentatives de force brute, les connexions depuis des emplacements inhabituels, et les utilisations anormales de comptes (connexions hors heures, depuis des IP inconnues). Sans ces logs, les attaques sur les comptes passent inaperçues jusqu'à ce que leurs effets soient visibles.

Impact potentiel

- Non-détection des attaques par force brute sur les comptes administrateurs ou VPN
- Impossibilité d'identifier les connexions suspectes ou non autorisées a posteriori
- Absence de preuves lors d'investigations sur des usurpations d'identité

Navigation

```
System > Logging > Log settings
→ Activer la journalisation des catégories :
  - Authentication logs : cocher
  - Admin logs (modifications de configuration) : cocher
  - System logs : cocher
  - VPN logs : cocher
→ Envoyer vers Syslog (voir contrôle 10.1)
```

CLI de vérification

```
# Vérification dans l'interface web
# System > Logging > Log settings
# Vérifier que Authentication logs, Admin logs, System logs et VPN logs sont activés
```

Remédiation

1. Naviguer vers `System > Logging > Log settings`
2. Activer la journalisation de toutes les catégories : Authentication, Admin, System, VPN, Firewall, IPS, Web, Email
3. S'assurer que ces logs sont inclus dans la configuration syslog vers le SIEM
4. Configurer des alertes dans le SIEM sur les échecs d'authentification répétés (> 5 dans 1 minute)
5. Créer des règles de corrélation SIEM pour les connexions hors heures et depuis des pays inhabituels

Valeur par défaut : Logs d'authentification disponibles mais non forcément tous activés ou envoyés vers syslog.

Critère de conformité : Logs Authentication, Admin, VPN et System activés et envoyés vers le SIEM.

Contrôle 10.4 — Rétention des logs ≥ 90 jours

CIS Ref : *(Best practice)* | ***MITRE :*** *T1070* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

Une rétention de logs trop courte empêche les investigations forensiques sur des incidents découverts tardivement (temps médian de détection d'une brèche : 207 jours selon le rapport IBM 2025). La majorité des référentiels réglementaires (NIS2, PCI-DSS, ISO 27001) exige une rétention minimale de 90 jours à 1 an.

Impact potentiel

- Impossibilité de reconstituer la chaîne d'attaque pour des incidents découverts après 30 jours
- Non-conformité réglementaire (NIS2 Article 21, PCI-DSS Req. 10.7)
- Perte de preuves forensiques critiques pour les enquêtes et poursuites judiciaires

Navigation

```
System > Logging > Log settings > Local logging
→ Configurer la rétention locale (limitée par la capacité disque du firewall)
→ Compléter avec une rétention longue durée dans le SIEM (recommandé)
Sophos Central (si utilisé) > Log management
→ Configurer la rétention selon les exigences réglementaires (90 jours minimum, 1 an recommandé)
```

CLI de vérification

```
# Vérification dans l'interface web
# System > Logging > Log settings
# Vérifier la rétention configurée et l'espace disque disponible
```

Remédiation

1. Configurer la rétention locale au maximum de la capacité disque du pare-feu
2. S'appuyer sur le SIEM externe pour la rétention longue durée (90 jours minimum, 1 an recommandé)
3. Si Sophos Central est utilisé, configurer la rétention des logs dans le portail
4. Documenter la politique de rétention dans la charte de gestion des logs
5. Vérifier trimestriellement que la rétention effective correspond à la politique

Valeur par défaut : Rétention limitée par la capacité disque locale du firewall (généralement < 30 jours).

Critère de conformité : Rétention effective ≥ 90 jours (SIEM externe ou Sophos Central). Politique de rétention documentée.

Contrôle 10.5 — Alertes sur événements critiques configurées

CIS Ref : *1.2.2 (étendu)* | ***MITRE :*** *T1562* | ***Niveau :*** 🟡 *MOYEN*

Description du risque

La supervision passive des logs sans alertes en temps réel sur les événements critiques crée une détection réactive plutôt que proactive. Les événements tels que les modifications de règles de pare-feu, les détections IPS critiques, les connexions admin hors heures, et les défaillances HA doivent générer des alertes immédiates.

Impact potentiel

- Découverte tardive de modifications de configuration non autorisées
- Absence de notification lors de la désactivation de protections par un attaquant
- Délai de réponse à incident en l'absence d'alertes en temps réel

Navigation

```
Configure > System services > Notification list
→ Cocher les événements critiques à notifier :
  - Firewall rule changes (modifications de règles)
  - Authentication failures (échecs d'authentification multiples)
  - IPS critical/high detections
  - HA status changes
  - License expiration warnings
  - System resource alerts (CPU, mémoire)
→ Configurer les canaux de notification (email, SNMP trap vers SIEM)
```

CLI de vérification

```
# Vérification dans l'interface web
# Configure > System services > Notification list
# Vérifier les événements activés pour les notifications
```

Remédiation

1. Naviguer vers `Configure > System services > Notification list`
2. Activer les notifications pour les modifications de configuration, les détections IPS critiques, les échecs d'authentification, les changements de statut HA
3. Configurer des alertes email vers l'équipe SOC pour les événements critiques
4. Configurer des traps SNMP vers le SIEM pour la corrélation automatique
5. Définir des seuils d'alerte (ex : > 10 échecs d'authentification en 5 minutes = alerte critique)

Valeur par défaut : Notifications non configurées par défaut.

Critère de conformité : Notifications activées pour les catégories critiques. Réception vérifiée sur le canal de notification configuré.

Contrôle 10.6 — IPFIX/sFlow — Surveillance des flux réseau pour la chasse aux menaces (NOUVEAU)

CIS Ref : *(Best practice — Network Visibility)* | ***MITRE :*** *T1048 (Exfiltration Over Alternative Protocol), T1021 (Remote Services — Lateral Movement)* | ***Niveau :*** 🔵 *L2*

Description du risque

L'export de flux réseau via IPFIX (IP Flow Information Export) ou sFlow permet une visibilité exhaustive sur tout le trafic traversant le pare-feu, y compris les communications qui ne déclenchent aucune alerte IPS ou Web. Cette visibilité est indispensable pour la chasse aux menaces (threat hunting), la détection des mouvements latéraux, l'identification des transferts de données volumineux suspects (indicateur d'exfiltration), et l'établissement d'une baseline de trafic normal servant de référence pour la détection d'anomalies.

Sans données de flux, un analyste SOC dispose des logs d'événements (alertes IPS, logs de connexion) mais ne peut pas corréler les patterns de trafic dans le temps, ni détecter les comportements lents et discrets (slow exfiltration, lateral movement progressif) qui évitent délibérément de déclencher des alertes ponctuelles.

Protocoles disponibles

PROTOCOLE	MÉCANISME	GRANULARITÉ	USAGE
IPFIX (NetFlow v10)	Export d'enregistrements de flux complets	IP src/dst, port, protocole, octets, paquets, durée	SIEM, Sophos NDR, outils d'analyse de flux
sFlow	Échantillonnage de paquets (1 sur N) + export des en-têtes et payload	Échantillon + statistiques d'interface	Analyse réseau, NDR Essentials,

PROTOCOLE	MÉCANISME	GRANULARITÉ	USAGE
			outils de performance

Impact potentiel sans visibilité de flux

- T1048 : exfiltration lente de données via des protocoles autorisés (HTTPS, DNS) non détectée par l'absence d'analyse de flux
- T1021 : mouvement latéral progressif entre segments réseau non détecté en l'absence de corrélation de flux temporels
- Absence de baseline de trafic empêchant la détection d'anomalies comportementales
- Incapacité à quantifier les transferts de données lors d'investigations forensiques post-incident
- Lacune dans la couverture DLP pour les transferts de fichiers via des protocoles non inspectés en contenu

Navigation — Configuration IPFIX

```
System > Network > IPFIX (ou System > Administration > IPFIX)
→ Activer l'export IPFIX : ON
→ Collector IP : adresse du SIEM ou du collecteur NetFlow/IPFIX
→ Collector port : 2055 (NetFlow standard) ou port personnalisé du collecteur
→ Protocol : IPFIX (NetFlow v10) — recommandé pour compatibilité maximale
→ Template export interval : 60 secondes
→ Flow export interval : 60 secondes (ou selon les besoins d'analyse)
→ Include interfaces : sélectionner toutes les interfaces actives (LAN, WAN, DMZ)
→ Champs IPFIX à inclure :
  - Source IP, Destination IP
  - Source Port, Destination Port
  - Protocol (TCP/UDP/ICMP)
  - Bytes, Packets
  - Flow duration (start/end timestamp)
  - Interface IN / Interface OUT
→ Appliquer
```

Navigation — Configuration sFlow

```
System > Administration > Device Access > sFlow
→ Activer sFlow : ON
→ Collector IP : adresse du collecteur sFlow (Sophos NDR, SIEM, ntopng)
→ Collector Port : 6343 (port sFlow standard)
→ Sampling rate : 1:1000 (1 paquet sur 1000 échantillonné — ajuster selon le débit)
  Pour les interfaces < 100 Mbps : 1:100
  Pour les interfaces 1 Gbps : 1:1000
  Pour les interfaces > 10 Gbps : 1:10000
→ Counter polling interval : 30 secondes
→ Sélectionner les interfaces à monitorer (priorité LAN et WAN)
→ Appliquer
```

Cas d'usage de détection via les flux

MENACE	SIGNAL DANS LES FLUX	SEUIL D'ALERTE
Exfiltration de données (T1048)	Transferts sortants > seuil vers destinations non répertoriées	Upload > 500 MB/heure vers IP externe inconnue
Mouvement latéral (T1021)	Connexions inhabituelles entre segments internes	Nouveau flux source→dest non vu dans les 30 derniers jours
Balayage réseau	Multiples connexions courtes vers de nombreuses destinations	> 100 destinations en < 60 secondes depuis un hôte
Tunnel DNS (exfiltration)	Volume DNS élevé vers un seul résolveur	Flux DNS > 10 MB/heure depuis un hôte
Beacon C2	Connexions régulières vers la même destination externe	Intervalle constant ± 5% sur > 1 heure

CLI de vérification

```
# Depuis l'Advanced Shell SFOS (SSH > option 5)
# Vérifier la configuration IPFIX
show ipfix configuration

# Vérifier le statut de l'export sFlow
show sflow configuration

# Vérifier les statistiques d'export de flux (nombre de flux exportés)
show ipfix statistics

# Tester la connectivité vers le collecteur
system diagnostics ping <collector-ip>

# Vérification dans l'interface web
# System > Network > IPFIX : vérifier l'activation et l'adresse du collecteur
# System > Administration > Device Access > sFlow : vérifier l'activation
```

Intégration avec Sophos NDR et SIEM

```
Pour Sophos NDR (Network Detection and Response) :
  Les données sFlow exportées depuis SFOS peuvent alimenter Sophos NDR
  pour une analyse comportementale avancée du trafic réseau.
  Sophos Central > NDR > Configuration > Data Sources > Add Sophos Firewall

Pour un SIEM (Splunk, Elastic, QRadar) :
  Configurer un collecteur NetFlow/IPFIX (ex : nfcapd, Logstash)
  Créer des règles de corrélation basées sur les volumes de flux
  et les destinations inhabituelles

Pour ntopng/SolarWinds/Scrutinizer :
  Utiliser le collecteur IPFIX/sFlow natif de ces outils
  pour la visualisation des flux et la détection d'anomalies
```

Remédiation

1. Naviguer vers `System > Network > IPFIX` et activer l'export vers le collecteur SIEM ou NDR
2. Configurer l'adresse IP et le port du collecteur IPFIX
3. Sélectionner toutes les interfaces actives pour l'export de flux
4. Configurer l'export sFlow via `System > Administration > Device Access > sFlow` si un outil de visualisation réseau est disponible
5. Adapter le sampling rate sFlow à la capacité des interfaces (voir tableau ci-dessus)
6. Créer des règles de corrélation SIEM sur les patterns d'exfiltration et de mouvement latéral
7. Intégrer les données IPFIX/sFlow dans Sophos NDR si disponible
8. Établir une baseline de trafic sur 30 jours avant d'activer les alertes basées sur des anomalies de flux
9. Documenter les seuils d'alerte dans la politique de monitoring réseau

Valeur par défaut : IPFIX et sFlow non activés par défaut. Collecteur à configurer explicitement.

Critère de conformité : IPFIX ou sFlow activé et exportant vers un collecteur externe (SIEM/NDR). Toutes les interfaces actives incluses. Statistiques d'export vérifiées (commande `show ipfix statistics`). Règles de corrélation flux configurées dans le SIEM pour T1048 et T1021.

Contrôle 10.7 — Rapports de conformité et tableaux de bord pour l'audit (NOUVEAU)

CIS Ref : *(Best practice — Compliance Reporting)* | ***MITRE :*** *T1562 (Impair Defenses — audit trail)* | ***Niveau :*** 🟢 *L1*

Description du risque

Les rapports de conformité intégrés dans SFOS et Sophos Central permettent de produire des preuves d'audit pour PCI-DSS, RGPD, ISO 27001 et NIS2 sans extraction manuelle de données. L'absence de rapports réguliers signifie que les dérives de configuration passent inaperçues entre les audits, et que les équipes de conformité ne disposent pas des preuves documentaires requises par les auditeurs. Les tableaux de bord Sophos Central offrent une visibilité historique que les logs locaux du pare-feu ne peuvent pas fournir (capacité disque limitée, absence de graphiques temporels).

Impact potentiel

- Les dérives de configuration (règles permissives introduites, comptes administrateurs non révoqués) ne sont pas détectées entre deux audits en l'absence de rapports de conformité réguliers, permettant à un attaquant de maintenir un accès persistant non remarqué (T1562 — Impair Defenses).
- L'incapacité à produire des preuves d'audit documentaires (logs d'accès, rapport de politique de pare-feu) lors d'un contrôle PCI-DSS, NIS2 ou ISO 27001 expose l'organisation à des sanctions financières, à la perte de certification ou à la suspension de contrats nécessitant la conformité.
- Sans historique long terme dans Sophos Central, la reconstruction d'une chronologie d'incident (forensics) est impossible au-delà de la capacité de rétention locale du pare-feu, compromettant la réponse à incident et les obligations légales de notification (RGPD Art. 33).

Rapports disponibles dans SFOS et Sophos Central

RAPPORT	CONTENU	RÉFÉRENTIEL	FRÉQUENCE RECOMMANDÉE
Firewall Policy Audit	Audit des règles actives, règles permissives, règles sans profils	PCI-DSS Req. 1	Mensuel
Access Control Review	Comptes administrateurs actifs, dernière connexion, droits	PCI-DSS Req. 7/8, NIS2	Mensuel
Authentication Logs Report	Connexions réussies/ échouées par utilisateur et IP source	PCI-DSS Req. 10, ISO 27001	Hebdomadaire
User Activity Report	Bande passante et applications par utilisateur	RGPD (accès données), ISO 27001	Mensuel
Threat Report	Top menaces bloquées, catégories d'attaque, IPs sources	NIS2 Art. 21, ISO 27001	Hebdomadaire
VPN Access Report	Connexions VPN/ZTNA par utilisateur, durée, volume	PCI-DSS Req. 8, NIS2	Mensuel
Executive Summary	Vue consolidée de la posture de sécurité	Direction, RSSI	Mensuel/Trimestriel

Navigation — Rapports SFOS intégrés

```
Étape 1 : Rapports de conformité locaux (SFOS)
Log Viewer > Reports > Compliance Reports
→ PCI-DSS Reports :
  - Firewall rule audit : liste des règles actives, règles permissives signalées
  - User access control report : comptes et droits d'accès
→ GDPR/RGPD Reports :
  - Data access logs : accès aux ressources sensibles
  - User activity logs : activité par utilisateur
→ Exporter : Format PDF ou CSV (pour archivage et audit)

Étape 2 : Rapports d'activité utilisateurs
Log Viewer > Reports > User Activity Reports
→ Sélectionner la période (hebdomadaire, mensuelle)
→ Filtrer par utilisateur ou groupe AD
→ Exporter en PDF pour inclusion dans les rapports RSSI

Étape 3 : Rapports de menaces
Log Viewer > Reports > Security Reports
→ Top Threats : catégories de menaces bloquées, top IPs sources
→ IPS Report : attaques détectées et bloquées par sévérité
→ Web Filtering Report : catégories bloquées, top domaines refusés

Étape 4 : Rapports Sophos Central (cloud — historique long terme)
Sophos Central > Reports > Firewall Reports
→ Executive Summary : vue consolidée mensuelle de la posture de sécurité
→ Threat Summary : menaces détectées sur la période
→ Policy Compliance : écarts par rapport aux bonnes pratiques du Health Check
→ Configurer la génération automatique : Daily / Weekly / Monthly
→ Configurer l'envoi par email vers les destinataires (RSSI, DPO, auditeurs)
```

Planification automatique des rapports

```
Sophos Central > Reports > Scheduled Reports > Add Report
→ Rapport : sélectionner le type (Executive Summary, Threat Report, etc.)
→ Fréquence : Daily / Weekly / Monthly
→ Période couverte : Last 7 days / Last 30 days / Last quarter
→ Destinataires email : RSSI, DPO, Direction, auditeurs
→ Format : PDF (pour archivage légal) et CSV (pour traitement automatisé)
→ Activer et sauvegarder

SFOS local :
Log Viewer > Reports > Scheduled Reports
→ Même configuration pour les rapports locaux
→ Envoi par email via la configuration SMTP (contrôle 3.4)
```

CLI de vérification

```
# Depuis l'Advanced Shell SFOS
# Vérifier la configuration des rapports planifiés
show report schedule

# Vérifier les derniers rapports générés
show report history last 10

# Vérification dans l'interface web
# Log Viewer > Reports > vérifier la présence de rapports récents
# Sophos Central > Reports : vérifier les rapports planifiés et les derniers exports
```

Correspondance référentiels de conformité

CONTRÔLE SFOS	PCI-DSS	ISO 27001	NIS2	RGPD
Firewall rule audit report	Req. 1.3	A.13.1	Art. 21	—
Authentication logs	Req. 10.2	A.9.4	Art. 21	Art. 32
Admin activity logs	Req. 10.3	A.12.4	Art. 21	Art. 30
User activity reports	Req. 10.2	A.9.1	—	Art. 30
Threat reports	Req. 11.4	A.12.6	Art. 23	—
VPN access logs	Req. 8.3	A.9.4	Art. 21	Art. 32

Remédiation

1. Naviguer vers `Log Viewer > Reports > Compliance Reports` et générer un premier rapport PCI-DSS et RGPD pour établir la baseline
2. Configurer des rapports planifiés hebdomadaires (Threat Report, Authentication Logs) dans `Log Viewer > Reports > Scheduled Reports`
3. Configurer des rapports planifiés mensuels (Firewall Policy Audit, User Activity, Executive Summary)
4. Dans Sophos Central, créer des rapports planifiés identiques pour la rétention longue durée (dépassant la capacité disque locale du pare-feu)
5. Configurer l'envoi automatique par email vers les destinataires concernés (RSSI, DPO, direction)
6. Archiver les rapports PDF mensuels dans un système documentaire sécurisé pour les besoins d'audit
7. Vérifier que les rapports correspondent aux exigences des auditeurs (PCI-DSS QSA, auditeurs ISO 27001) et ajuster le contenu si nécessaire
8. Inclure les résultats du Firewall Health Check dans le rapport mensuel de sécurité

Valeur par défaut : Rapports disponibles mais non planifiés par défaut. Génération manuelle uniquement.

Critère de conformité : Rapports de conformité planifiés (hebdomadaire + mensuel). Envoi automatique vers les destinataires configuré. Derniers rapports archivés et accessibles aux auditeurs. Rapport Executive Summary mensuel transmis au RSSI.

Réponse à incident

Indicateurs de compromission

INDICATEUR	SIGNIFICATION	ACTION IMMÉDIATE
Connexions WebAdmin depuis une IP WAN non répertoriée	Accès admin non autorisé depuis Internet	Bloquer IP source, révoquer session, auditer les modifications récentes
Modifications de règles de pare-feu non planifiées	Manipulation de la politique de sécurité	Restaurer depuis la sauvegarde, audit complet des règles, réinitialiser les mots de passe admin
Détections IPS critiques en volume anormal	Exploitation active ou scan offensif	Analyser les IP sources, renforcer les règles, activer le mode de quarantaine
Trafic sortant vers des domaines inconnus sur ports inhabituels	Potentiel canal C2 ou exfiltration	Isolation réseau de l'endpoint source, analyse forensique, blocage IP/domaine
Échecs d'authentification massifs sur VPN ou WebAdmin	Attaque par force brute en cours	Bloquer temporairement les IP sources, vérifier l'absence de compromission
Expiration soudaine d'abonnements de protection	Potentielle désactivation par un attaquant ou négligence	Vérifier les logs admin, renouveler les abonnements, auditer les accès récents
Security Heartbeat rouge sur plusieurs endpoints	Incident de sécurité actif sur le réseau interne	Isoler les endpoints en rouge (Synchronized Security), déclencher la procédure IR, notifier le SOC
Logs absents dans le SIEM sur une plage horaire	Potentielle suppression de logs ou panne de collecte	Vérifier la connectivité syslog, analyser les logs locaux du pare-feu
Alerte XDR Linux Sensor — modification de configuration	Modification non autorisée détectée par le capteur d'intégrité	Vérifier les logs admin Sophos Central, comparer avec la dernière sauvegarde, déclencher IR si non autorisé
Alerte XDR Linux Sensor — export de règles non planifié	Exfiltration possible de la politique de sécurité	Identifier l'origine de l'export, révoquer les accès, notifier RSSI
Alerte XDR Linux Sensor — tentative d'exécution de programme malveillant	Compromission possible du pare-feu	Isolation immédiate, restauration depuis sauvegarde saine, investigation forensique complète
Alerte NDR — comportement réseau anormal sur trafic chiffré	Potentiel C2 ou mouvement latéral via trafic chiffré	Analyser les flux concernés, isoler l'endpoint source, bloquer les destinations suspectes

Capacités de détection XDR Linux Sensor (SFOS v22)

Le capteur XDR Linux intégré dans SFOS v22 fournit une surveillance d'intégrité en temps réel du système d'exploitation du pare-feu. Les détections sont remontées dans Sophos Central Threat Analysis Center et doivent être intégrées dans le workflow SOC :

```
Sophos Central > Threat Analysis Center > Détections XDR Firewall
→ Modification non autorisée de la configuration système
→ Export non planifié de règles de pare-feu (risque d'exfiltration de politique)
→ Tentative d'exécution de programme malveillant sur le système hôte
→ Altération de fichiers système critiques
→ Changements d'état de surveillance anormaux
```

Procédure d'isolation d'urgence

```
# 1. Capturer l'état courant du pare-feu
# Via l'Advanced Shell (SSH > option 5) :
show system
show firewall-rule
system diagnostics show version

# 2. Exporter la configuration immédiatement (avant toute modification)
# Via WebAdmin : System > Backup & Firmware > Export > Download backup

# 3. Bloquer les accès entrants suspects (via WebAdmin)
# Protect > Rules and policies > Firewall rules
# Ajouter une règle de blocage en haut de la liste pour les IP sources suspectes

# 4. Capturer les logs d'authentification récents
# Log viewer : System > Log viewer > filtrer par Authentication et Admin (dernières 24h)

# 5. Vérifier les modifications de configuration récentes
# System > Administration > Audit log

# 6. Vérifier les détections XDR Linux Sensor dans Sophos Central
# Sophos Central > Threat Analysis Center > filtrer sur le pare-feu concerné

# 7. Vérifier le statut Synchronized Security
console> show security-heartbeat
console> show synchronized-security

# 8. En cas de compromission confirmée — isoler le pare-feu
# Désactiver les interfaces WAN si possible via le port console
# Procéder à une restauration depuis une sauvegarde saine
# Réinitialiser tous les mots de passe administrateurs et révoquer les clés SSH
# Réviser et réappliquer toutes les règles de pare-feu
```

Commandes CLI forensiques SFOS avancées (Advanced Shell)

> *Ces commandes sont à exécuter depuis le shell avancé SFOS : `SSH > option 5 > Advanced Shell`. Elles permettent un audit approfondi du système lors d'une investigation forensique sur un pare-feu potentiellement compromis.*

Statut système et intégrité

```
# Version complète du système et des composants
system diagnostics show version

# Utilisation mémoire — détecter une fuite mémoire ou un processus anormal
system diagnostics show memory

# Utilisation CPU — détecter une surcharge anormale (crypto mining, DDoS)
system diagnostics show cpuusage

# Statut de tous les services — vérifier qu'aucun service n'a été arrêté
service --status-all

# Vérifier les services SFOS actifs et leur état
system diagnostics show services
```

Investigation réseau et connexions actives

```
# Capturer le trafic réseau en temps réel (outil tcpdump intégré)
# Exemple : capturer le trafic HTTPS sur toutes les interfaces
system diagnostics show tcpdump interface "any" filter "port 443"

# Capturer le trafic vers/depuis une IP suspecte
system diagnostics show tcpdump interface "any" filter "host 192.168.1.100"

# Capturer les connexions SSH entrantes (investigation accès admin)
system diagnostics show tcpdump interface "any" filter "port 22"

# Afficher toutes les connexions actives sur le pare-feu
show connection

# Afficher les connexions par protocole
show connection protocol tcp
show connection protocol udp

# Vérifier les règles de pare-feu actives et leurs compteurs de hits
show firewall-rule

# Afficher le nombre de correspondances par règle (identifier les règles les plus actives)
show firewall-rule all
```

Audit des logs système en temps réel

```
# Suivre les logs IPS en temps réel (détections d'exploits)
tail -f /log/ips.log

# Suivre les logs du pare-feu en temps réel
tail -f /log/firewall.log

# Suivre les logs d'authentification en temps réel
tail -f /log/auth.log

# Suivre les logs système en temps réel
tail -f /log/system.log

# Consulter les logs de l'interface web (accès à la WebAdmin)
tail -f /log/webadmin.log

# Consulter les logs VPN
tail -f /log/vpn.log
```

Audit de configuration et des modifications

```
# Afficher les 100 dernières entrées du journal d'audit (modifications de config)
show audit-log last 100

# Afficher l'audit log depuis une date spécifique (format YYYY-MM-DD)
show audit-log from 2026-05-01

# Vérifier la configuration des utilisateurs admin
show user admin

# Vérifier les clés SSH autorisées (chercher des clés non reconnues)
cat ~/.ssh/authorized_keys

# Vérifier le hostname (détecter une modification non autorisée)
hostname

# Vérifier les interfaces réseau et leurs adresses (détecter des modifications)
show network interface
```

Vérification de l’intégrité Synchronized Security et ZTNA

```
# Statut Synchronized Security (Security Heartbeat)
show security-heartbeat

# Statut de synchronisation Sophos Central
show sophos-central status

# Statut ZTNA (si configuré)
show ztna gateway status
show ztna sessions

# Statut NDR Essentials
show sophos-ndr status

# Statut Active Threat Response (feeds actifs et dernières correspondances)
show active-threat-response feeds
show active-threat-response matches last 50
```

Vérification HA (si déployé en High Availability)

```
# Statut de la paire HA
system ha show status

# Logs de la synchronisation HA
system ha show log

# Vérifier la cohérence de configuration entre les nœuds
system ha show sync-status
```

Commandes de diagnostic réseau

```
# Test de connectivité vers un hôte (vérifier les flux sortants autorisés)
system diagnostics ping 8.8.8.8

# Résolution DNS (vérifier que le DNS fonctionne correctement)
system diagnostics nslookup google.com

# Traceroute pour identifier le chemin de routage
system diagnostics traceroute 8.8.8.8

# Vérifier la table de routage
show route
```

Commandes forensiques avancées — Threat Hunting

Ces commandes sont spécifiques à SFOS v22 et complètent les commandes forensiques générales de la section précédente. Elles couvrent les scénarios de Threat Hunting actif : recherche d'indicateurs de compromission, détection C2, anomalies NDR/ATR, et vérification de l'intégrité des composants de sécurité. Exécuter depuis le shell avancé SFOS : `SSH > option 5 > Advanced Shell`*, ou via* `console> system advanced-shell`*.*

```
# ============================================================
# FORENSIQUE SOPHOS FIREWALL v22 — THREAT HUNTING
# ============================================================

# --- ACCÈS AU SHELL AVANCÉ ---
# Via SSH : connecter en admin, puis :
console> system advanced-shell
# Ou via Sophos Central > Firewall > SSH

# --- ÉTAT SYSTÈME ---
system diagnostics show version
system diagnostics show memory
system diagnostics show cpuusage
system diagnostics show diskusage

# --- INTÉGRITÉ (XDR Linux Sensor) ---
# Vérifier les modifications non autorisées
show audit-log last 200

# Statut XDR Sensor
show xdr-agent status

# --- CONNEXIONS RÉSEAU ---
# Connexions actives (rechercher C2)
show connection | grep "ESTABLISHED" | head -50

# Connexions vers ports suspects
netstat -tulnp | grep -E ":6666|:4444|:1337|:31337"

# --- RÈGLES FIREWALL ---
show firewall-rule

# Règles récemment modifiées (via audit)
show audit-log last 100 | grep -i "firewall"

# --- SYNCHRONIZED SECURITY ---
show security-heartbeat
show synchronized-security
# Devices avec Heartbeat RED
show security-heartbeat | grep "RED"

# --- NDR & ATR ---
show sophos-ndr status
show active-threat-response feeds
show active-threat-response matches

# --- VPN ---
show vpn ipsec connection all
show vpn ssl-vpn connection

# --- ZTNA ---
show ztna gateway status

# --- HAUTE DISPONIBILITÉ ---
system ha show status
system ha show statistics
```

```
# --- CERTIFICATS ---
system certificate show

# --- PERFORMANCES (indicateurs d'attaque DDoS) ---
system diagnostics show interface-stats
system diagnostics show tcp-states

# --- LOGS EN TEMPS RÉEL ---
tail -f /log/ips.log
tail -f /log/firewall.log
tail -f /log/authentication.log

# --- PROCESSUS SUSPECTS (shell Linux avancé) ---
ps aux | sort -k3 -rn | head -20
netstat -anp | grep ESTABLISHED | grep -v "known-process"

# --- ANALYSE PCAP ---
system diagnostics show tcpdump interface "any" filter "port 443 and host <suspect-ip>"
```

Contacts et escalade

NIVEAU	CONTACT	DÉLAI
Incident P1 (compromission active)	SOC + RSSI + AYI NEDJIMI Consultants	Immédiat (< 15 min)
Incident P2 (tentative détectée)	SOC	< 1 heure
Incident P3 (anomalie détectée)	Administrateur réseau	< 4 heures
Avis de sécurité Sophos critique	Administrateur + RSSI	< 24 heures

---

Références

- CIS Sophos Firewall v22 Benchmark v1.0.0 — 25 mars 2026
- Sophos Security Advisories (PSIRT)
- Sophos Firewall SFOS v22 Documentation
- Sophos Firewall v22 Health Check — 32 vérifications CIS-alignées
- Sophos Xstream Architecture v2 — Décembre 2025
- Sophos NDR Essentials — Network Detection and Response
- MITRE ATT&CK — Network Devices
- MITRE ATT&CK — T1568 Dynamic Resolution (DGA)
- MITRE ATT&CK — T1573 Encrypted Channel
- ANSSI — Recommandations pour choisir des pare-feux maîtrisés
- ANSSI — Recommandations de configuration d'un pare-feu — double barrière, diversification technologique, équipements certifiés

- CISA Known Exploited Vulnerabilities Catalog
- NIST SP 800-41 Rev. 1 — Guidelines on Firewalls and Firewall Policy
- CERT-FR — Alertes et avis de sécurité
- NIS2 Directive (UE) 2022/2555 — Exigences de sécurité réseau
- DORA — Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier — effectif 17 janvier 2025 — Art. 9 (gestion des risques TIC — durcissement pare-feu), Art. 10 (continuité opérationnelle — HA), Art. 11 (gestion des incidents — syslog/SIEM), Art. 16 (risques tiers — Synchronized Security/MDR)
- OWASP Top 10 — 2021
- Linux Kernel 6.6 Security Features
- Sophos XDR — Remote Integrity Monitoring
- Sophos ZTNA — Zero Trust Network Access intégré Sophos Firewall
- Sophos Active Threat Response — MDR et XDR
- MITRE ATT&CK — T1133 External Remote Services
- MITRE ATT&CK — T1557 Adversary-in-the-Middle
- MITRE ATT&CK — T1090 Proxy
- MITRE ATT&CK — T1021 Remote Services
- RFC 7011 — IPFIX (IP Flow Information Export)
- sFlow.org — sFlow specification
- RFC 5425 — TLS Transport Mapping for Syslog
- MITRE ATT&CK — T1553 Subvert Trust Controls
- MITRE ATT&CK — T1070.002 Clear Logs
- MITRE ATT&CK — T1562.006 Indicator Blocking
- MITRE ATT&CK — T1200 Hardware Additions
- CIS Controls v8 — Center for Internet Security
- ISO/IEC 27001:2022 — Information Security Management Systems
- PCI DSS v4.0 — Payment Card Industry Data Security Standard
- Sophos High Availability Configuration Guide — SFOS v22
- Sophos Certificate Management — SFOS v22
- Sophos Wireless Protection Configuration — SFOS v22

ANNEXE — Checklists de vérification rapide

Checklists condensées pour audit terrain et conformité. Chaque ligne = un contrôle actionnable. Cocher lors de l'audit.

Domaine 1 — Configuration initiale et mise à jour du système

#	CONTRÔLE	NIVEAU	STATUT
1.1	Pattern updates configurées toutes les 15 minutes (Auto update = ON)	🟠 ÉLEVÉ	☐
1.2	Hotfixes automatiques activés (Allow Automatic Installation of hotfixes)	🟠 ÉLEVÉ	☐
1.3	Sauvegarde planifiée, chiffrée, testée, stockée hors-bande	🟢 L1	☐
1.4	Hostname défini de manière significative et conforme à la convention de nommage	🟢 L1	☐
1.5	Aucun abonnement de protection en statut Expired	🟠 ÉLEVÉ	☐
1.6	HA configurée et en statut Established (si requis par l'architecture)	🔵 L2	☐
1.7	Noyau Linux 6.6+ — mitigations CPU actives (Spectre/Meltdown/ Retbleed/ZenBleed/Downfall) — KASLR activé — IPS Xstream v2 conteneurisé	🟠 ÉLEVÉ	☐
1.8	Capteur XDR Linux actif — pare-feu enregistré dans Sophos Central — alertes d'intégrité configurées	🟠 ÉLEVÉ	☐

Domaine 2 — Authentification et accès administrateur

#	CONTRÔLE	NIVEAU	STATUT
2.1	Timeout session admin ≤ 10 min + blocage après 5 tentatives en 60 sec	🟢 L1	☐
2.2	Bannière de connexion (disclaimer) configurée et approuvée	🟢 L1	☐
2.3	Complexité de mots de passe : admin ≥ 16 chars (min 14), utilisateurs ≥ 12 chars	🟢 L1	☐
2.4	MFA activé pour la WebAdmin et VPN SSL/IPSec — algorithme OTP SHA-256/SHA-512	🔴 CRITIQUE	☐
2.5		🔴 CRITIQUE	☐

#	CONTRÔLE	NIVEAU	STATUT
	MFA activé pour le compte admin par défaut		
2.6	Connexion LDAP/AD chiffrée (SSL/TLS ou StartTLS + validation certificat)	🟢 L1	☐
2.7	Authentification SSH par clé RSA 4096 ou ED25519 — auth par mot de passe SSH désactivée	🟠 ÉLEVÉ	☐

Domaine 3 — Sécurisation de l'interface de gestion

#	CONTRÔLE	NIVEAU	STATUT
3.1	HTTPS/SSH désactivés sur la zone WAN — aucune règle 0.0.0.0/Any vers WebAdmin ou User Portal	🔴 CRITIQUE	☐
3.2	Certificat TLS valide (non auto-signé) sur la WebAdmin	🔵 L2	☐
3.3	SNMPv1/v2c supprimés — SNMPv3 avec AES uniquement	🟢 L1	☐
3.4	Notifications email/SNMP configurées pour événements système et sécurité	🟢 L1	☐
3.5	Accès WebAdmin/SSH restreint aux seules IP d'administration	🟢 L1	☐
3.6	API XML : désactivée si non utilisée OU restriction IP + comptes dédiés + rotation des clés + logs API	🟠 ÉLEVÉ	☐
3.7	Sophos Central : MFA activé + rôles least privilege + IP allow-listing + clés API auditées	🟠 ÉLEVÉ	☐
3.8	Certificats : aucun auto-signé sur interfaces exposées + CA SSL inspection dédié + alertes expiration 30j + CRL configuré	🟠 ÉLEVÉ	☐

Domaine 4 — Règles et politiques de protection

#	CONTRÔLE	NIVEAU	STATUT
4.1	Aucune règle ANY/ANY/ANY depuis la zone WAN —	🔴 CRITIQUE	☐

#	CONTRÔLE	NIVEAU	STATUT
	configurations Any-Any-Any remédiées		
4.2	Ports SMB (445) et RDP (3389) inaccessibles directement depuis WAN	🔴 CRITIQUE	☐
4.3	Identification utilisateur activée sur les règles LAN-to-WAN	🔵 L2	☐
4.4	Firewall Health Score = Optimal ou Good — 32 vérifications CIS revues	🟢 L1	☐
4.5	Toutes les règles Internet ont des profils IPS/AV/Web/App attachés	🟠 ÉLEVÉ	☐
4.6	Architecture Xstream v2 : IPS conteneurisé confirmé + SSL/TLS inspection active + ASIC XGS opérationnel	🔵 L2	☐
4.7	Health Check Continu : consulté ≥ hebdo, 0 vérification HIGH en Warning, exceptions documentées	🟢 L1	☐

Domaine 5 — Profils de protection

#	CONTRÔLE	NIVEAU	STATUT
5.1	Profil IPS : signatures Critical et High en mode Block (IPS en conteneur Xstream v2)	🟠 ÉLEVÉ	☐
5.2	Web Policy : catégories Malware et Phishing bloquées, scan HTTP/HTTPS actif	🟠 ÉLEVÉ	☐
5.3	Filtrage applicatif : risque niveau 4 et 5 bloqués	🟡 MOYEN	☐
5.4	Protection email : antispam + SPF/DKIM/DMARC + BATV + greylisting + Zero-day + URL click-time + DLP	🟠 ÉLEVÉ	☐
5.5	WAF OWASP Top 10 : mode Protection + SQL Injection + XSS + Cookie Signing + HTTPS redirect + TLS valide	🟠 ÉLEVÉ	☐
5.6	DoS avancé : SYN cookies activés + seuils UDP/ICMP flood + limites connexions/source IP + Anti-	🟡 MOYEN	☐

#	CONTRÔLE	NIVEAU	STATUT
	Spoofing + `dos-protection-status` vérifié		
5.7	Proxy web : authentification Kerberos SSO/NTLM activée + bypass désactivé + ports non-standard bloqués	🟡 MOYEN	☐

Domaine 6 — Synchronized Security et menaces avancées

#	CONTRÔLE	NIVEAU	STATUT
6.1	Sophos X-Ops Threat Feeds activés en mode Log and Drop	🟠 ÉLEVÉ	☐
6.2	Zero-day protection activée — moteur AI/ML cloud (mise à jour 5 min) — sans exclusion de fichiers	🟠 ÉLEVÉ	☐
6.3	Security Heartbeat activé — cycle Detect/Isolate/Restore testé — minimum Yellow (Red bloqué)	🟠 ÉLEVÉ	☐
6.4	Au moins un flux de menaces tiers intégré et synchronisé	🔵 L2	☐
6.5	NDR Essentials activé — EPA engine + DGA detection — interfaces LAN/DMZ configurées — `show sophos-ndr status` = Enabled	🔵 L2	☐
6.6	Active Threat Response MDR/XDR : feeds activés Log and Drop + `show active-threat-response feeds` synchronisés + Security Heartbeat activé (isolation endpoint)	🟠 ÉLEVÉ	☐
6.7	HA Self-Healing activé — surveillance continue de l'état — corrections automatiques vérifiées	🔵 L2	☐

Domaine 7 — VPN et ZTNA

#	CONTRÔLE	NIVEAU	STATUT
7.1	IPsec configuré en IKEv2, pas de mode agressif, AES-256 + DH ≥ 14	🟠 ÉLEVÉ	☐
7.2	SSL VPN : certificat valide (CA de confiance, non expiré, SHA-2)	🔵 L2	☐

#	CONTRÔLE	NIVEAU	STATUT
7.3	MFA obligatoire pour SSL VPN et IPSec remote access — OTP SHA-256/SHA-512	🔴 CRITIQUE	☐
7.4	ZTNA : gateway configurée dans Sophos Central + ressources définies + politiques posture + client Sophos Connect déployé	🔵 L2	☐

Domaine 8 — Inspection SSL/TLS

#	CONTRÔLE	NIVEAU	STATUT
8.1	Règles d'inspection SSL/TLS en mode Decrypt (T1557 contré) actives sur LAN-to-WAN	🟡 MOYEN	☐
8.2	CA dédié à l'inspection SSL créé et déployé sur les clients	🟡 MOYEN	☐
8.3	Exemptions SSL documentées et révisées trimestriellement	🟡 MOYEN	☐

Domaine 9 — Services réseau et segmentation

#	CONTRÔLE	NIVEAU	STATUT
9.1	NTP configuré avec au moins 2 sources (pool.ntp.org + time.google.com) — horloge synchronisée	🟢 L1	☐
9.2	DNS Protection Sophos activée avec filtrage de catégories malveillantes	🟡 MOYEN	☐
9.3	Segmentation réseau par VLANs et zones de sécurité distinctes	🟡 MOYEN	☐
9.4	Wireless avancé : WPA3-Enterprise 802.1X + isolation client + VLAN dédié + Rogue AP detection + WIDS deauth/evil-twin	🟡 MOYEN	☐
9.5	Anti-spoofing couche 2 : Spoof Prevention + Source Route Verification + MAC-IP binding serveurs critiques + protection DHCP rogue	🟡 MOYEN	☐
9.6	HA hardening : interface dédiée + mot de passe HA ≥20 chars +	🔵 L2	☐

#	CONTRÔLE	NIVEAU	STATUT
	chiffrement sync + préemption OFF + IP auxiliaire dédiée + firmware identique		

Domaine 10 — Journalisation et supervision SIEM

#	CONTRÔLE	NIVEAU	STATUT
10.1	Syslog TLS TCP port 6514 — certificat serveur validé — toutes catégories activées — alerte SIEM si silence > 5 min — rétention 90j/ 1an immuable	🟡 MOYEN	☐
10.2	Log firewall traffic activé sur 100% des règles de pare-feu	🟢 L1	☐
10.3	Logs Authentication, Admin, VPN et System activés et envoyés au SIEM	🟢 L1	☐
10.4	Rétention des logs ≥ 90 jours (SIEM externe ou Sophos Central)	🟡 MOYEN	☐
10.5	Alertes configurées sur modifications de règles, détections critiques, échecs auth	🟡 MOYEN	☐
10.6	IPFIX ou sFlow activé vers collecteur externe — toutes interfaces couvertes — règles SIEM T1048/T1021 configurées	🔵 L2	☐
10.7	Rapports de conformité PCI-DSS/ RGPD planifiés (hebdo + mensuel) — envoi auto RSSI/DPO — archivage audit	🟢 L1	☐

Tableau récapitulatif par domaine

DOMAINE	CONTRÔLES	CRITIQUE	ÉLEVÉ	MOYEN	L1	L2
D1 — Configuration initiale	8	0	4	0	3	1
D2 — Auth admin	7	2	2	0	3	0
D3 — Interface gestion	8	1	3	0	3	1
D4 — Règles et politiques	7	2	1	1	2	1
D5 — Profils protection	7	0	4	3	0	0

DOMAINE	CONTRÔLES	CRITIQUE	ÉLEVÉ	MOYEN	L1	L2
D6 — Synchronized Security	7	0	4	0	0	3
D7 — VPN et ZTNA	4	1	1	0	0	2
D8 — SSL/TLS	3	0	0	3	0	0
D9 — Services réseau	6	0	0	4	1	1
D10 — Logs/SIEM	7	0	0	3	3	1
TOTAL	**64**	**6**	**19**	**14**	**15**	**10**

> ***Note v1.4*** *: Nouveaux contrôles ajoutés (passe 4) : 3.8 (gestion du cycle de vie des certificats — CA-signed, SSL CA dédié, surveillance expiration, CRL), 9.6 (HA hardening Active-Passive — interface dédiée, mot de passe ≥20 chars, chiffrement sync, préemption OFF, firmware consistency). Contrôles enrichis : 5.6 (DoS avancé — SYN cookies, limites par source IP,* `dos-protection-status` *), 9.4 (wireless avancé — WPA3-Enterprise 802.1x, WIDS, rogue AP detection, client isolation), 10.1 (syslog TLS port 6514, mode TCP fiable, logs immuables, rétention 90j/1an). Nouvelle section ANNEXE : tableau de correspondance référentiels de conformité (CIS v8, NIS2, ISO 27001:2022, RGPD, PCI DSS v4). Le total de contrôles référencés dans les métadonnées (ITEMS : 83) inclut les sous-contrôles distincts des contrôles enrichis à travers les 4 passes d'enrichissement (v1.1, v1.2, v1.3, v1.4).*

Tableau de correspondance référentiels de conformité (NOUVEAU — v1.4)

> *Correspondance entre les contrôles Sophos Firewall SFOS v22 et les principaux référentiels de conformité applicables en 2026. Utiliser ce tableau pour démontrer la couverture réglementaire lors des audits.*

CONTRÔLE SFOS	LIBELLÉ	CIS CONTROLS V8	NIS2 ART. 21	ISO 27001:2022	RGPD	PCI DSS V4	DORA
2.4 / 2.5	Authentification admin MFA (WebAdmin + admin par défaut)	CIS 6.3, 6.5	Art. 21 §2(j)	A.9.4.2	Art. 32 §1(b)	Req 8.4.2	Art. 9 §4(e)
1.1 / 1.2	Mise à jour firmware et patterns (hotfixes automatiques)	CIS 7.3, 7.4	Art. 21 §2(e)	A.12.6.1	Art. 32 §1(b)	Req 6.3.3	Art. 9 §2(e)
	Journalisation SIEM (syslog	CIS 8.2, 8.5		A.12.4.1			

CONTRÔLE SFOS	LIBELLÉ	CIS CONTROLS V8	NIS2 ART. 21	ISO 27001:2022	RGPD	PCI DSS V4	DORA
10.1 / 10.2 / 10.3	TLS, toutes catégories)		Art. 21 §2(h)		Art. 32 §1(b)	Req 10.2, 10.3	Art. 11 §1(c)
7.1 / 7.3	Chiffrement VPN (IKEv2, AES-256, MFA)	CIS 12.6, 12.7	Art. 21 §2(d)	A.13.2.1	Art. 32 §1(a)	Req 4.2.1	Art. 9 §4(d)
9.3	Segmentation réseau (VLANs et zones de sécurité)	CIS 12.2, 12.3	Art. 21 §2(a)	A.13.1.3	Art. 25 §1	Req 1.3.2	Art. 9 §2(b)
5.1	IPS activé en mode Block (signatures Critical/High)	CIS 13.4, 13.9	Art. 21 §2(b)	A.13.1.1	Art. 32 §1(b)	Req 6.4.1	Art. 9 §2(c)
8.1 / 8.2	Inspection SSL/TLS (Decrypt + CA dédié)	CIS 13.10	Art. 21 §2(b)	A.13.1.1	Art. 32 §1(a)	Req 4.2.1	Art. 9 §4(d)
2.3	Complexité des mots de passe (admin ≥16, users ≥12)	CIS 5.2	Art. 21 §2(j)	A.9.4.3	Art. 32 §1(b)	Req 8.3.6	Art. 9 §4(e)
3.1 / 3.5	Restriction accès management (pas d'accès WAN, IP whitelisting)	CIS 4.1, 4.2	Art. 21 §2(a)	A.9.1.2	Art. 32 §1(b)	Req 1.3.1	Art. 9 §4(a)
6.1 / 6.2 / 6.5	Threat Intelligence (X-Ops, Zero-day, NDR DGA/ EPA)	CIS 10.1, 10.5	Art. 21 §2(b)	A.12.6.1	Art. 32 §1(b)	Req 6.4.2	Art. 16 §2(a)
1.3	Sauvegarde chiffrée planifiée	CIS 11.2	Art. 21 §2(c)	A.12.3.1	Art. 32 §1(c)	Req 12.3.4	Art. 10 §1(b)
4.1 / 4.2	Blocage trafic WAN (pas d'ANY/ANY, blocage SMB/ RDP)	CIS 4.4	Art. 21 §2(a)	A.13.1.1	Art. 32 §1(b)	Req 1.2.1	Art. 9 §2(a)
5.4	Protection email (SPF/	CIS 9.7		A.13.2.3			

CONTRÔLE SFOS	LIBELLÉ	CIS CONTROLS V8	NIS2 ART. 21	ISO 27001:2022	RGPD	PCI DSS V4	DORA
	DKIM/DMARC, sandboxing)		Art. 21 §2(b)		Art. 32 §1(b)	Req 6.4.2	Art. 9 §2(c)
6.3	Security Heartbeat (Detect/Isolate/ Restore)	CIS 13.6	Art. 21 §2(a)	A.16.1.5	Art. 33	Req 12.10.1	Art. 11 §1(a)
10.4	Rétention des logs ≥ 90 jours	CIS 8.3	Art. 21 §2(h)	A.12.4.1	Art. 30	Req 10.7.1	Art. 11 §1(c)
2.7	SSH par clé publique (RSA/ ED25519)	CIS 5.6	Art. 21 §2(j)	A.9.4.2	Art. 32 §1(b)	Req 8.6.1	Art. 9 §4(e)
9.4	Protection wireless (WPA3-Enterprise, WIDS, Rogue AP)	CIS 12.4, 12.5	Art. 21 §2(a)	A.13.1.2	Art. 32 §1(b)	Req 1.3.3	Art. 9 §2(b)
3.8	Gestion certificats (CA-signed, expiration, CRL)	CIS 16.5	Art. 21 §2(d)	A.10.1.1	Art. 32 §1(a)	Req 4.2.1	Art. 9 §4(d)
1.6 / 9.6	HA hardening (mot de passe, chiffrement, préemption)	CIS 11.3	Art. 21 §2(c)	A.17.2.1	Art. 32 §1(c)	Req 12.3.3	Art. 10 §2(a)
5.5	WAF OWASP Top 10 (mode Protection, TLS, logs)	CIS 13.10	Art. 21 §2(b)	A.14.2.5	Art. 25 §1	Req 6.4.1	Art. 9 §2(c)
6.6	Active Threat Response MDR/XDR (feeds, isolation)	CIS 13.6	Art. 21 §2(b)	A.16.1.4	Art. 32 §1(b)	Req 12.10.1	Art. 16 §3(a)

Légende des références :

RÉFÉRENTIEL	VERSION	DESCRIPTION
CIS Controls v8	v8.0 (2021)	Center for Internet Security — 18 contrôles essentiels
NIS2	Directive (UE) 2022/2555	

RÉFÉRENTIEL	VERSION	DESCRIPTION
		Mesures de sécurité obligatoires pour les entités essentielles et importantes
ISO 27001:2022	ISO/IEC 27001:2022	Système de management de la sécurité de l'information — Contrôles Annexe A
RGPD	Règlement (UE) 2016/679	Sécurité du traitement (Art. 32), Privacy by Design (Art. 25)
PCI DSS v4	PCI DSS v4.0 (2022)	Payment Card Industry Data Security Standard — exigences réseau et journalisation
DORA	Règlement (UE) 2022/2554	Résilience opérationnelle numérique — entités financières — effectif 17 janvier 2025 — Art. 9 (risques TIC), Art. 10 (continuité), Art. 11 (incidents), Art. 16 (tiers)

Note d'utilisation : *Ce tableau est fourni à titre indicatif. La correspondance exacte dépend du contexte de déploiement et de l'interprétation des auditeurs. Consulter un spécialiste en conformité pour les audits formels PCI-DSS QSA, ISO 27001, NIS2, ou DORA. Les entités du secteur financier soumises à DORA doivent en particulier valider la couverture des Art. 9 à 16 avec leur équipe conformité et leur autorité de surveillance compétente.*

Référentiel MITRE ATT&CK — couverture complète

TECHNIQUE MITRE	LIBELLÉ	CONTRÔLES COUVRANTS
T1078	Valid Accounts	2.1, 2.3, 2.4, 2.5, 2.7, 3.5, 3.6, 4.3
T1078.004	Cloud Accounts	3.7
T1090	Proxy	5.7 (proxy web authentifié — contournement empêché)
T1110	Brute Force	2.1, 2.3, 2.7
T1133	External Remote Services	3.1, 3.5, 7.1, 7.3, 7.4 (ZTNA — supérieur à VPN)
T1190	Exploit Public-Facing Application	1.1, 1.2, 3.1, 3.6, 4.1, 5.5, 6.1
T1200	Hardware Additions (rogue HA node)	9.6 (HA hardening — auth password, interface dédiée)
T1210	Exploitation of Remote Services	5.1, 6.3, 9.3

TECHNIQUE MITRE	LIBELLÉ	CONTRÔLES COUVRANTS
T1021	Remote Services — Lateral Movement	10.6 (IPFIX/sFlow — détection mouvement latéral)
T1498	Network Denial of Service	5.6 (DoS avancé, SYN cookies)
T1499	Endpoint Denial of Service	1.6, 6.7, 9.6 (HA prévient les coupures)
T1534	Internal Spearphishing	5.4
T1540	Disable or Modify System Firewall	4.4, 4.7, 1.8
T1553	Subvert Trust Controls (certificats)	3.8 (CA-signed certs, CRL, surveillance expiration)
T1557	Adversary-in-the-Middle	2.6, 3.2, 3.8, 7.2, 8.1, 8.2, 6.5, 9.5 (ARP/DHCP)
T1562	Impair Defenses	1.5, 3.4, 4.7, 10.5, 10.7 (audit trail)
T1562.006	Indicator Blocking (disable logging)	10.1 (syslog TLS, alerte silence SIEM, logs immuables)
T1562.001	Disable or Modify Tools	1.8
T1566	Phishing	5.2, 5.4, 6.1, 6.2, 6.6
T1568	Dynamic Resolution (DGA)	6.5 (NDR DGA detection), 9.2
T1573	Encrypted Channel	6.5 (NDR EPA engine)
T1601	Modify System Image	1.7, 1.8
T1055	Process Injection	1.7, 4.6 (IPS Xstream conteneurisé)
T1040	Network Sniffing	2.6, 3.3, 7.1, 9.4 (WIDS wireless)
T1048	Exfiltration Over Alternative Protocol	5.3, 5.4 (DLP email), 10.6 (IPFIX détection exfil)
T1070.002	Clear Logs	10.1 (syslog TLS immédiat, logs immuables SIEM)
T1071	Application Layer Protocol	4.5, 5.2, 5.3, 5.7, 6.5, 8.1

Document produit par AYI NEDJIMI Consultants — https://ayinedjimi-consultants.fr Version 1.5 — Mai 2026 — Enrichi (passe 5 — finale) avec : conformité DORA (Règlement UE 2022/2554, effectif 17 janvier 2025 — Art. 9, 10, 11, 16) ajoutée dans la section Références et dans le tableau de correspondance de conformité (colonne DORA), commandes forensiques avancées Threat Hunting SFOS v22 (nouvelle sous-section dans Réponse à incident), carte de référence rapide CLI Sophos Firewall v22 (nouvelle section en fin de document). Historique des versions : v1.1 (enrichissement initial), v1.2 (NDR Essentials EPA/DGA, XML API, Sophos Central, Health Check 32 vérifications, WAF OWASP Top 10, Email SPF/DKIM/DMARC/BATV/DLP, Xstream v2), v1.3 (ZTNA, ATR MDR/XDR, proxy web, ARP/DHCP Layer 2, IPFIX/sFlow, rapports conformité, forensique CLI), v1.4 (HA hardening, certificate management, DoS avancé, wireless WIDS/Rogue AP, syslog TLS, compliance mapping), v1.5 (DORA compliance references, DORA column in compliance table, Threat Hunting forensic commands, Quick Reference Card) Basé sur le CIS Sophos Firewall v22 Benchmark v1.0.0 (25 mars 2026), le Sophos Health Check v22 (32 vérifications CIS-alignées) et les recommandations ANSSI pour les pare-feux maîtrisés Ce document est CONFIDENTIEL — Ne pas diffuser sans autorisation

---

RÉFÉRENCE RAPIDE — Commandes critiques Sophos Firewall v22

Carte de référence pour les opérations courantes et la réponse à incident. Toutes les commandes s'exécutent depuis le shell avancé SFOS (SSH > option 5 > Advanced Shell) sauf indication contraire.

```
# ============================================================
# ÉTAT GÉNÉRAL
# ============================================================
system diagnostics show version        # Version SFOS installée
show connection                        # Sessions actives (toutes)
show firewall-rule                     # Règles de pare-feu en vigueur
show network interface                 # Interfaces réseau et adresses
show route                             # Table de routage

# ============================================================
# SÉCURITÉ — MENACES & DÉTECTION
# ============================================================
show security-heartbeat                # État Synchronized Security Heartbeat
show security-heartbeat | grep "RED"  # Devices en état RED (compromis/suspects)
show synchronized-security             # Vue globale Synchronized Security
show active-threat-response feeds      # Feeds ATR actifs et statut synchronisation
show active-threat-response matches    # Dernières correspondances ATR (IOC)
show sophos-ndr status                 # NDR Essentials : actif / inactif
show ztna gateway status               # État gateway ZTNA
show xdr-agent status                  # Statut capteur XDR Linux (intégrité FW)
show sophos-central status             # Connexion Sophos Central

# ============================================================
# AUDIT & TRAÇABILITÉ
# ============================================================
show audit-log last 100                # 100 dernières modifications de config
show audit-log last 200                # 200 dernières entrées (investigation)
show audit-log from 2026-01-01         # Audit depuis une date (YYYY-MM-DD)

# ============================================================
# VPN
# ============================================================
show vpn ipsec connection all          # Tunnels IPsec (tous statuts)
show vpn ssl-vpn connection            # Sessions SSL VPN actives
show vpn ipsec sa                      # Security Associations IPsec

# ============================================================
# HAUTE DISPONIBILITÉ (HA)
# ============================================================
system ha show status                  # État de la paire HA
system ha show statistics              # Statistiques HA (failovers, sync)
system ha show sync-status             # Cohérence configuration entre nœuds
system ha show log                     # Logs de synchronisation HA

# ============================================================
# CERTIFICATS
# ============================================================
system certificate show                # Inventaire complet des certificats
show certificate admin                 # Certificat WebAdmin en service
show ssl-inspection ca                 # CA d'inspection SSL/TLS configuré

# ============================================================
# DIAGNOSTIC PERFORMANCES
# ============================================================
system diagnostics show cpuusage       # Utilisation CPU (détecter charge anormale)
system diagnostics show memory         # Utilisation RAM (détecter fuite mémoire)
```

```
system diagnostics show diskusage     # Espace disque (logs, config)
system diagnostics show interface-stats  # Statistiques par interface
system diagnostics show tcp-states    # États TCP (détecter saturation/DDoS)
system diagnostics show services      # Statut de tous les services SFOS

# ============================================================
# CAPTURE RÉSEAU (PCAP)
# ============================================================
system diagnostics show tcpdump interface "any" filter "port 443"
system diagnostics show tcpdump interface "any" filter "host <ip-suspecte>"
system diagnostics show tcpdump interface "any" filter "port 443 and host <ip-suspecte>"

# ============================================================
# CONNECTIVITÉ
# ============================================================
system diagnostics ping 8.8.8.8       # Test de connectivité
system diagnostics nslookup google.com # Résolution DNS
system diagnostics traceroute 8.8.8.8 # Traceroute

# ============================================================
# LOGS TEMPS RÉEL (Advanced Shell Linux)
# ============================================================
tail -f /log/ips.log                  # IPS — détections exploits
tail -f /log/firewall.log             # Règles pare-feu
tail -f /log/authentication.log       # Authentifications
tail -f /log/webadmin.log             # Accès console WebAdmin
tail -f /log/vpn.log                  # Connexions VPN
tail -f /log/system.log               # Événements système
```

***Usage DORA (entités financières)** : les commandes `show audit-log`, `show active-threat-response matches`, `show security-heartbeat`, et les logs temps réel (`tail -f /log/authentication.log`) constituent les preuves primaires pour les rapports d'incident exigés par DORA Art. 17 (délai de notification : 4 heures pour incident majeur, rapport final sous 1 mois). Les sorties doivent être conservées dans le SIEM avec rétention immuable ≥ 1 an (Art. 11 §1(c)).*