BTS SIO — OPTION SISR

Document Technique — Procédure d'exploitation

Paramétrage du pare-feu Sophos XG

SFOS v20 — Guide de configuration complet

Zones réseaux | Règles pare-feu | Filtrage web | VPN SSL & IPsec

Rédigé par : Rémi Carlier

Version : 1.0 | Date : Janvier 2025 | Statut : Valide

Applicable à : Sophos XG Series — SFOS 19.x / 20.x

Rédacteur	Vérificateur	Approbateur	Version
Rémi Carlier	F. Bonningues	Direction IT	1.0

Sommaire

1 Prérequis et connexion à l'interface web

Première connexion et configuration initiale

1.1 Prérequis matériels et logiciels

Avant de commencer le paramétrage, vérifier que les éléments suivants sont disponibles :

Élément	Détail	Obligatoire
Appliance Sophos XG	Modèle XGS 116/216/316 ou supérieur	Oui
Cable console ou Ethernet	Pour la connexion initiale au port LAN1	Oui
Navigateur web	Chrome, Firefox ou Edge (version récente)	Oui
Licence SFOS activée	Licence de base + modules (Network Protection, Web)	Oui
Adresse IP WAN	Fournie par le FAI (statique ou DHCP)	Oui
Plan d'adressage IP	Schema réseau avec les plages à utiliser	Recommande

1.2 Connexion à l'interface d'administration

L'interface web de gestion (WebAdmin) est accessible par défaut sur le port LAN1 du pare-feu. Suivre les étapes ci-dessous :

ATTENTION L'adresse IP par défaut de Sophos XG est 192.168.1.1 sur le port LAN. Configurer le poste d'administration avec une adresse dans le même sous-réseau (ex : 192.168.1.2/24) avant la première connexion.

1	Connecter le câble Ethernet du poste d'administration au port LAN1 de l'appareil. Configurer l'interface réseau du poste : IP 192.168.1.2 / Masque 255.255.255.0.
2	Ouvrir un navigateur et accéder a l'URL : https://192.168.1.1:4444
3	Accepter l'avertissement de certificat auto-signe (normal lors de la première connexion).
4	Saisir les identifiants par défaut : Utilisateur = admin / Mot de passe = admin
5	L'assistant de configuration initiale (Setup Wizard) se lance automatiquement. Suivre les étapes.
6	Changer immédiatement le mot de passe administrateur (16 caractères minimum, complexe).

IMPORTANT Ne jamais laisser le mot de passe par défaut en production. Définir une politique de mot de passe robuste dès la première connexion.

1.3 Tableau de bord et navigation

Une fois connecté, le tableau de bord (Dashboard) affiche l'état général du système. Les menus principaux sont :

Menu	Contenu	Accès rapide
Network	Interfaces, zones, routage, DNS, DHCP	Configuration réseau de base

Menu	Contenu	Accès rapide
Firewall	Règles de filtrage entrant/sortant	Politique de sécurité
VPN	Tunnels SSL et IPsec	Accès distant et site-a-site
Web	Filtrage URL, catégories, politiques	Protection navigation
System	Licences, mises à jour, sauvegardes	Administration système
Reports	Journaux, statistiques, alertes	Monitoring et audit

1.4 Mise à jour du firmware SFOS

Avant toute configuration, s'assurer que le firmware est à jour :

1	Aller dans System > Firmware.
2	Cliquer sur Check for Updates. Si une mise à jour est disponible, cliquer sur Download.
3	Une fois le téléchargement termine, cliquer sur Install.
4	Vérifier après redémarrage que la version SFOS affichée correspond bien à la dernière version stable.

2 Configuration des zones réseau

Définition des interfaces et des zones de sécurité

2.1 Concept des zones dans Sophos XG

Sophos XG organise le trafic réseau en zones de sécurité. Chaque interface physique ou virtuelle est assignée a une zone. Les règles de pare-feu contrôlent ensuite le trafic entre ces zones.

Zone	Type	Usage typique	Niveau de confiance
WAN	Externe	Connexion Internet / FAI	Non fiable
LAN	Interne	Réseau local entreprise	Fiable
DMZ	Semi-interne	Serveurs publics (web, mail)	Moyen
VPN	Virtuelle	Utilisateurs VPN distants	Contrôle
Wi-Fi	Interne	Réseau sans-fil	Limite

2.2 Configuration des interfaces physiques

Chemin : Network > Interfaces > Add Interface

NOTE Sophos XG nomme les interfaces Port1, Port2, etc. Renommer chaque interface avec un nom explicite (ex : WAN-FAI, LAN-Entreprise) facilite l'administration.

Interface WAN (Port1)

1	Aller dans Network > Interfaces. Cliquer sur Port1 pour l'éditer.
2	Renseigner les champs : - Name : WAN-FAI - Zone : WAN - IPv4 Configuration : Static (ou DHCP selon le FAI) - IP Adresse : Adresse fournie par le FAI - Subnet Mask : Masque fourni par le FAI - Gateway : Passerelle par défaut du FAI
3	Dans la section Advanced, activer MTU auto-detection.
4	Cliquer sur Save et vérifier l'état de l'interface (icone verte = lien actif).

Interface LAN (Port2)

1	Cliquer sur Port2. Renseigner : Name = LAN-Entreprise / Zone = LAN.
2	IPv4 : Static / IP Adresse : 192.168.10.1 / Subnet Mask : 255.255.255.0.
3	Activer le service DHCP sur cette interface (voir section DHCP ci-dessous).
4	Sauvegarder et vérifier la connectivité depuis le réseau local.

Interface DMZ (Port3) — optionnel

1	Cliquer sur Port3. Name = DMZ-Serveurs / Zone = DMZ.
2	IPv4 : Static / IP : 172.16.0.1 / Masque : 255.255.255.0.
3	Ne pas activer de DHCP sur la DMZ (adresses statiques obligatoires pour les serveurs).
4	Sauvegarder.

2.3 Configuration du serveur DHCP

Chemin : Network > DHCP > Add

1	Cliquer sur Add dans la section DHCP Servers.
2	Renseigner : - Name : DHCP-LAN - Interface : LAN-Entreprise - Lease Time : 86400 (24h) - Adresse Range : 192.168.10.100 - 192.168.10.200 - Subnet Mask : 255.255.255.0 - Gateway : 192.168.10.1 - DNS : 192.168.10.1 (ou DNS interne)
3	Ajouter des réservations DHCP pour les équipements critiques (imprimantes, serveurs).
4	Sauvegarder et tester depuis un poste client.

3 Règles de pare-feu

Création et gestion des politiques de filtrage

3.1 Principe de fonctionnement

Les règles de pare-feu Sophos XG sont évaluées de haut en bas. La première règle qui correspond au trafic est appliquée. Il est donc essentiel d'ordonner les règles du plus spécifique au plus général.

IMPORTANT Sophos XG applique par défaut une règle implicite 'Deny All' en fin de liste. Tout trafic non explicitement autorise est bloqué et journalise.

3.2 Règles fondamentales a créer

Chemin : Firewall > Add Firewall Rule > New Firewall Rule

#	Nom de la règle	Source	Destination	Service	Action
1	LAN-vers-Internet	LAN	WAN	Any	Accept
2	LAN-vers-DMZ	LAN	DMZ	HTTP, HTTPS, SMTP	Accept
3	DMZ-vers-Internet	DMZ	WAN	HTTP, HTTPS, DNS	Accept
4	DNAT-Web-Public	WAN	Serveur-Web (DMZ)	HTTP, HTTPS	DNAT
5	VPN-SSL-accès	VPN	LAN	Selon politique	Accept
6	Bloquer-tout	Any	Any	Any	Deny

3.3 Création d'une règle LAN vers Internet

1	Aller dans Firewall > Add Firewall Rule > New Firewall Rule.
2	Dans l'onglet General : - Rule Name : LAN-vers-Internet - Rule Position : Top - Action : Accept
3	Dans Source : - Source Zone : LAN - Source Network : Any (ou un groupe d'hôtes)
4	Dans Destination : - Destination Zone : WAN - Destination Network : Any
5	Dans Services : sélectionner Any ou créer un groupe de services (HTTP, HTTPS, DNS, NTP).
6	Dans Identity (optionnel) : activer User Authentication pour lier la règle a des utilisateurs ou groupes AD.
7	Dans Security Features : activer IPS Policy et Web Policy pour appliquer l'inspection.
8	Cocher Log Firewall Traffic pour activer la journalisation. Sauvegarder.

3.4 Création d'une règle NAT (DNAT) — publication de serveur

Pour rendre un serveur interne (ex : serveur web en DMZ) accessible depuis Internet :

1	Aller dans Firewall > Add Firewall Rule > New Firewall Rule.
2	General : Rule Name = DNAT-Web-Public / Action = DNAT.
3	Source : Zone = WAN / Network = Any.
4	Destination : Zone = WAN / Network = IP Publique du Sophos.
5	DNAT Settings : - Translated Destination : 172.16.0.10 (IP du serveur en DMZ) - Translated Service : laisser vide (même port)
6	Activer Reflexive Rule pour autoriser la réponse du serveur. Sauvegarder.

NOTE Apres création d'une règle DNAT, vérifier que le serveur cible est bien accessible depuis Internet via un test externe (navigateur ou outil en ligne).

4 Filtrage web et applications

Configuration du Web Protection et du contrôle applicatif

4.1 Activation du Web Protection

Le filtrage web de Sophos XG s'appuie sur le module Web Protection (licence requise). Il permet de filtrer les URL par catégories, de bloquer les malwares et de contrôler les applications.

ATTENTION Le filtrage web nécessite l'inspection HTTPS (SSL/TLS Inspection). Déployer au préalable le certificat CA Sophos sur tous les postes clients via GPO ou MDM.

4.2 Configuration de l'inspection HTTPS

1	Aller dans System > Certificates. Télécharger le certificat CA Sophos (bouton Download CA Certificate).
2	Déployer ce certificat sur tous les postes via GPO Active Directory (dans les Autorités de certification de confiance).
3	Aller dans Web > SSL/TLS Inspection Rules > Add Rule.
4	Configurer : - Action : Decrypt - Source Zone : LAN - Destination : Any - Exclure les sites de banque, sante et gouvernement (catégories sensibles)
5	Placer cette règle avant la règle 'Do Not Decrypt' générique. Sauvegarder.

4.3 Création d'une politique de filtrage web

Chemin : Web > Policies > Add Policy

1	Cliquer sur Add Policy. Nommer la politique : Politique-Standard-Entreprise.
2	Dans la section Catégories, configurer les actions par catégorie : - Malware, Phishing, Spam : Block - Adult Content, Gambling : Block - Streaming Video/Audio : Warn (avertissement utilisateur) - Social Networks : Monitor (journalise sans bloquer) - Professional/Business : Allow
3	Activer Malware and Content Scanning pour analyser les fichiers téléchargés.
4	Activer SafeSearch Enforcement pour Google, Bing et YouTube.
5	Définir les exceptions (URL whitelist) pour les sites métier spécifiques.
6	Sauvegarder la politique.

4.4 Application de la politique via les règles pare-feu

La politique de filtrage web est appliquée au niveau de la règle de pare-feu LAN-vers-Internet :

1	Editer la règle LAN-vers-Internet.
2	Dans Security Features > Web Policy : sélectionner Politique-Standard-Entreprise.
3	Activer également Application Control et sélectionner une App Policy (ex : bloquer P2P, Tor).
4	Sauvegarder la règle.

Catégorie	Action recommandée	Justification
Malware / Phishing	**Bloquer**	Sécurité obligatoire
Adult Content	**Bloquer**	Conformité RH
Streaming vidéo	**Avertir**	Bande passante
Réseaux sociaux	Monitorer	Journalisation
Applications métier	**Autoriser**	Productivité
P2P / Tor	**Bloquer**	Sécurité / conformité

5 VPN SSL — Accès distant

Configuration du VPN SSL pour les utilisateurs nomades

5.1 Principe du VPN SSL Sophos

Le VPN SSL de Sophos XG permet aux utilisateurs distants de se connecter au réseau de l'entreprise via un tunnel chiffre HTTPS. Deux modes sont disponibles : le mode Clientless (portail web) et le mode Full Tunnel (client Sophos Connect).

Mode	Description	Usage	Client requis
Clientless	Portail web avec accès aux applications internes	Accès léger depuis n'importe quel navigateur	Non
Full Tunnel	Tunnel IP complet, tout le trafic passe par le VPN	Postes distants gérés par l'entreprise	Sophos Connect

5.2 Configuration du VPN SSL (Full Tunnel)

Chemin : VPN > SSL VPN (Remote Access) > Add

1	Aller dans VPN > SSL VPN (Remote Access) > Add.
2	General Settings : - Name : VPN-SSL-Teleworkers - Policy Members : Groupe AD Teleworkers (ou utilisateurs locaux)
3	Tunnel Settings : - Protocol : TCP / Port : 443 - IP Pool : 10.100.0.0/24 (plage dédiée aux clients VPN) - DNS Server : 192.168.10.1
4	Accessible Networks : ajouter les réseaux accessibles depuis le VPN : - 192.168.10.0/24 (LAN Entreprise) - 172.16.0.0/24 (DMZ — si nécessaire)
5	Activer Split Tunneling si seul le trafic entreprise doit passer par le VPN (recommande pour économiser la bande passante).
6	Sauvegarder.

5.3 Déploiement du client Sophos Connect

1	Télécharger le client Sophos Connect depuis le portail MyAccount Sophos ou depuis VPN > SSL VPN > Download Client.
2	Installer le client sur le poste distant (Windows ou macOS).
3	Dans l'interface Sophos Connect, importer le fichier de configuration (.ovpn) téléchargé depuis le portail VPN Sophos (https://IP-WAN:443).
4	Se connecter avec les identifiants du compte utilisateur (AD ou local Sophos).
5	Vérifier la connectivité en pingant une ressource interne (ex : 192.168.10.1).

NOTE	Activer l'authentification multi-facteur (MFA) pour les connexions VPN SSL. Sophos XG supporte TOTP (Google Authenticator) et les SMS via le module OTP intégré.

5.4 Règle de pare-feu pour le VPN SSL

Apres configuration du VPN, créer la règle autorisant le trafic VPN vers le LAN :

1	Aller dans Firewall > Add Firewall Rule > New Firewall Rule.
2	Rule Name : VPN-SSL-vers-LAN / Action : Accept.
3	Source Zone : VPN / Source Network : 10.100.0.0/24 (pool VPN).
4	Destination Zone : LAN / Destination Network : 192.168.10.0/24.
5	Services : sélectionner les services autorises (RDP, SMB, HTTPS...). Eviter 'Any'.
6	Activer le logging. Sauvegarder.

6 VPN IPsec — Site a site

Configuration d'un tunnel IPsec entre deux sites

6.1 Prérequis

Le VPN IPsec site-a-site permet de connecter deux sites distants de manière transparente. Les deux extrémités du tunnel doivent disposer d'une IP publique fixe ou d'un FQDN dynamique.

Paramètre	Site A (Siege)	Site B (Agence)
IP Publique WAN	203.0.113.1	198.51.100.1
Réseau LAN	192.168.10.0/24	192.168.20.0/24
Identifiant IKE	siege@entreprise.fr	agence@entreprise.fr

6.2 Configuration du tunnel IPsec sur le Site A (Siege)

Chemin : VPN > IPsec Connections > Add

1	Aller dans VPN > IPsec Connections > Add.
2	General : - Name : IPsec-Siege-Agence - Connection Type : Site-to-Site - Gateway Type : Respond Only (ou Initiate) selon la topologie
3	Encryption : - IKE Version : IKEv2 (recommande) - Key Exchange : DH Group 14 (2048 bits) - Encryption : AES 256 / Hash : SHA-256 - SA Lifetime : 28800 secondes (8h)
4	Remote Gateway : - IP Adresse : 198.51.100.1 (IP WAN du Site B) - Local ID : siege@entreprise.fr - Remote ID : agence@entreprise.fr
5	Authentication : - Method : Preshared Key - Preshared Key : générer une clé aléatoire de 32+ caractères
6	Local Networks : 192.168.10.0/24 Remote Networks : 192.168.20.0/24
7	Activer Dead Peer Detection (DPD) : Action = Restart / Interval = 30s / Timeout = 120s.
8	Sauvegarder et activer le tunnel.

ATTENTION La Pre-Shared Key doit être identique sur les deux extrémités du tunnel. Utiliser un générateur de mots de passe aléatoires et ne jamais la transmettre en clair.

6.3 Règle de pare-feu pour le VPN IPsec

1	Creer une règle : VPN-IPsec-Siege-Agence / Action : Accept.
2	Source Zone : VPN / Source Network : 192.168.20.0/24 (LAN Agence).
3	Destination Zone : LAN / Destination Network : 192.168.10.0/24 (LAN Siege).
4	Services : sélectionner uniquement les services nécessaires (principe du moindre privilège).
5	Creer une règle inverse (LAN Siege vers LAN Agence) avec les mêmes critères inverses.
6	Tester le tunnel : aller dans VPN > IPsec Connections et vérifier l'état 'Connected'.

6.4 Vérification et troubleshooting

Problème	Cause possible	Solution
Tunnel ne monte pas	PSK incorrecte ou paramètres IKE différents	Vérifier PSK et paramètres Phase 1/2 sur les deux sites
Trafic bloque	Règle pare-feu manquante	Vérifier les règles source/destination VPN
Tunnel instable	Problème de DPD ou NAT-T	Activer NAT Traversal et ajuster les timers DPD
Latence élevée	Mauvais MTU	Fixer le MTU a 1400 sur les interfaces VPN

NOTE En cas de problème, utiliser le module Log Viewer de Sophos XG (Log Viewer > VPN) pour identifier la phase IKE qui échoue (Phase 1 = authentification, Phase 2 = chiffrement du trafic).

Annexes

A. Récapitulatif des paramètres de configuration

Paramètre	Valeur	Section
IP d'administration	https://192.168.10.1:4444	1.2
Compte admin	admin (à changer impérativement)	1.2
Interface LAN	Port2 — 192.168.10.1/24	2.2
Interface WAN	Port1 — IP FAI	2.2
Plage DHCP LAN	192.168.10.100 - 192.168.10.200	2.3
Pool VPN SSL	10.100.0.0/24	5.2
Port VPN SSL	TCP 443	5.2
IKE Version	IKEv2	6.2
Chiffrement IPsec	AES-256 / SHA-256 / DH Group 14	6.2

B. Checklist de validation finale

Avant mise en production, vérifier chaque point :

	Vérification	Statut
[ ]	Mot de passe admin change (16 car. min.)	A vérifier
[ ]	Firmware SFOS a jour	A vérifier
[ ]	Interfaces WAN/LAN/DMZ configurées et actives	A vérifier
[ ]	Règles pare-feu créées et testées	A vérifier
[ ]	Filtrage web actif et politique appliquée	A vérifier
[ ]	Certificat CA Sophos déployé sur les postes	A vérifier
[ ]	VPN SSL teste depuis un poste externe	A vérifier
[ ]	Tunnel IPsec monte et stable	A vérifier
[ ]	Sauvegarde de configuration effectuée	A vérifier
[ ]	Journalisation activée sur toutes les règles	A vérifier