LOSTE TRADI-FRANCE

Sécurisation périmétrique via Fortinet NGFW

Politiques de filtrageWeb Filter · Application Control · IPS

Rédacteur	Paul Barrault-Gautier
Entreprise	Loste Tradi-France
Date	Avril 2026
Version	1.0
Classification	Usage interne

1. Introduction

Ce document décrit les politiques de filtrage configurées sur le FortiGate de Loste Tradi-France. Il couvre les trois profils principaux appliqués aux flux réseau : Web Filter, Application Control et IPS (Intrusion Prevention System). Ces profils sont attachés aux règles de pare-feu (firewall policies) qui régissent les flux entre les différentes zones réseau.

1.1 Architecture de référence

Zone source	Zone destination	Profils appliqués
LAN (VLAN Users)	WAN (Internet)	Web Filter + App Control + IPS + AV
LAN (VLAN Production)	WAN (Internet)	IPS uniquement (flux métier)
WAN (Internet)	DMZ (serveurs exposés)	IPS + App Control
VPN SSL (Remote users)	LAN / ressources internes	IPS + Web Filter

2. Web Filter

Le Web Filter FortiGate s'appuie sur la base de données FortiGuard URL (plus de 2 milliards d'URL classifiées). La deep inspection SSL est activée pour analyser également les flux HTTPS.

2.1 Profil « WF-LAN-Users »

Catégorie FortiGuard	Action	Safe Search	Remarque
Malware / Phishing / Spam	**Block**	—	Priorité haute
Botnets / C&C	**Block**	—	FortiGuard Botnet DB
Contenu illicite / Adulte	**Block**	—	Politique RH
Peer-to-Peer / Torrents	**Block**	—	Bande passante
Jeux en ligne	**Block**	—	Politique interne
Réseaux sociaux (Facebook, etc.)	**Monitor**	—	Log uniquement
Moteurs de recherche	**Allow**	Activé	YouTube restrict: Modéré
Cloud professionnel (O365, etc.)	**Allow**	—	Whitelist explicite

2.2 Exceptions et overrides

- Les demandes d'accès exceptionnel transitent par un formulaire de dérogation soumis au responsable IT
- Un override authentifié (FortiGate Auth Challenge) peut être accordé pour 4 heures maximum
- La liste blanche statique est maintenue dans l'objet « URL-Whitelist-Corporate »

3. Application Control

L'Application Control FortiGate identifie les applications en analysant la signature des flux (L7), indépendamment du port utilisé. Cela permet de contrôler des applications qui contournent les filtres de port classiques.

3.1 Profil « AppCtrl-LAN »

Catégorie / Application	Risque	Action	Remarque
Proxy / Anonymizers	**Critique**	**Block**	Contournement VPN

BitTorrent, eMule	Haute	**Block**	P2P interdit
TeamViewer (non IT)	Haute	**Block**	Accès distant non maîtrisé
Zoom / Teams / Webex	Faible	**Allow**	Outils collaboratifs autorisés
Microsoft 365	Faible	**Allow**	Suite bureautique principale
Applications de jeu en ligne	Haute	**Block**	Usage non professionnel
Applications inconnues (default)	Variable	**Monitor**	Revue hebdomadaire des logs

4. IPS — Intrusion Prevention System

Le module IPS FortiGate analyse le contenu des paquets (DPI) pour détecter et bloquer les exploits réseau connus. Il s'appuie sur la base de signatures FortiGuard IPS, mise à jour automatiquement.

4.1 Profil IPS « IPS-Strict »

Groupe de signatures	Sévérité	Action	Remarque
Critique (Critical)	**Critique**	**Block + Reset**	Alerte SIEM
Haute (High)	Haute	**Block**	Log obligatoire
Moyenne (Medium)	Moyenne	**Monitor**	Revue hebdomadaire
Faible (Low)	Faible	**Monitor**	Log compressé 30 j
Informationnel	Info	Pass	Désactivé en prod.

4.2 Paramètres complémentaires

- Mise à jour des signatures : toutes les 24 h (schedulé à 02h00)
- Botnet C&C Detection : activé (incoming + outgoing)
- Protocol Anomaly Detection : activé pour HTTP, FTP, SMTP, DNS
- Rate-based IPS (DoS policy) : SYN flood > 500 pps → block 5 min

5. Procédure de maintenance des politiques

- Revue mensuelle : vérifier les faux positifs IPS et ajuster en Monitor si nécessaire
- Revue trimestrielle : analyser les catégories App Control bloquées et valider avec les métiers
- Mise à jour FortiOS : tester en environnement de lab avant déploiement en production
- Sauvegarde config : export de la configuration FortiGate avant toute modification