LOSTE TRADI-FRANCE

Sécurisation périmétrique via Fortinet NGFW

Procédure de monitoring FortiView

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

1. Objectif et périmètre

Ce document décrit la procédure de surveillance quotidienne et hebdomadaire du FortiGate via l'interface FortiView. Il est destiné à l'administrateur réseau en charge de la supervision de la sécurité périmétrique de Loste Tradi-France.

FortiView est le tableau de bord de supervision intégré à FortiOS. Il offre une vue en temps réel et historique des flux réseau, des menaces bloquées, des utilisateurs actifs et de la consommation de bande passante.

2. Accès à FortiView

2.1 Connexion à l'interface d'administration

1. Ouvrir un navigateur et accéder à l'adresse de gestion du FortiGate : https://<IP_MGMT_FORTIGATE>
2. S'authentifier avec les identifiants administrateur (compte nominatif recommandé, MFA activé)
3. Depuis le menu latéral gauche, cliquer sur « FortiView »
4. Sélectionner la vue souhaitée (voir section 3)

Accès alternatif via CLI : la commande diagnose debug flow permet une analyse en temps réel en mode console.

3. Vues FortiView principales

3.1 Vue « Threats »

Chemin : FortiView > Threats

- Affiche les menaces bloquées par IPS, Web Filter (catégorie malware), AV et Botnet C&C
- Colonnes clés : Source IP, Destination IP, Signature/Catégorie, Sévérité, Action, Timestamp
- Filtrer sur « Sévérité = Critique ou Haute » pour prioriser les investigations
- Double-clic sur une ligne pour afficher le détail complet du flux et le paquet capturé

3.2 Vue « Applications »

Chemin : FortiView > Applications

- Visualiser les applications identifiées et leur consommation de bande passante
- Identifier les applications bloquées (colonne Action = Blocked)
- Classer par « Bytes » pour détecter les transferts de données anormaux

3.3 Vue « Sources »

Chemin : FortiView > Sources

- Liste les sources de trafic internes les plus actives (par IP ou utilisateur si FSSO actif)
- Permet d'identifier un poste générant un trafic inhabituel (compromission, botnet interne)
- Filtrer par interface « LAN » pour n'afficher que le trafic interne

3.4 Vue « Destinations »

Chemin : FortiView > Destinations

- Visualiser les destinations externes les plus contactées
- Comparer avec les résolutions DNS pour détecter des requêtes vers des domaines suspects

3.5 Vue « Web Sites »

Chemin : FortiView > Web Sites

- Affiche les sites web accédés ou bloqués avec leur catégorie FortiGuard
- Colonne « Blocked » : cliquer sur le compteur pour lister les utilisateurs concernés

4. Procédure de monitoring quotidien

Durée estimée : 15 à 20 minutes — À réaliser chaque matin avant 9h00.

Étape	Action	Vue FortiView	Seuil d'alerte
1	Vérifier les menaces critiques bloquées depuis J-1	Threats	> 5 : escalader
2	Contrôler les événements IPS haute sévérité	Threats	> 20 : analyser
3	Identifier les sources internes anormalement actives	Sources	> 5 GB/jour
4	Vérifier l'absence de trafic C&C sortant	Threats / Destinations	Tout événement
5	Confirmer la mise à jour des signatures IPS (date last update)	System > FortiGuard	< 24 h
6	Consigner les incidents dans le registre des événements	—	—

5. Procédure de monitoring hebdomadaire

Durée estimée : 45 à 60 minutes — À réaliser chaque lundi matin.

- Générer et exporter le rapport FortiView hebdomadaire (FortiView > Reports > Security)
- Analyser l'évolution du top 10 des menaces IPS par rapport à la semaine précédente
- Vérifier les applications nouvellement détectées dans App Control > Review
- Contrôler les tentatives d'accès aux ressources bloquées par utilisateur (possible insider threat)
- Mettre à jour le Rapport d'Analyse des Menaces (DOC-FORT-01) avec les données de la semaine
- Planifier les éventuels ajustements de politiques de filtrage (DOC-FORT-02)

6. Procédure d'escalade

Situation	Niveau	Action
Trafic C&C sortant détecté	**CRITIQUE**	Isoler le poste source + alerter RSSI immédiatement
Exploit critique bloqué > 5 fois	**HAUTE**	Analyser l'IP source + renforcer la règle IPS
Pics de trafic inexpliqués (> 10 GB)	**HAUTE**	Identifier la source et ouvrir un ticket d'incident
Faux positif répété sur un flux métier	**MOYENNE**	Passer la signature en Monitor + documenter
Signature IPS non mise à jour > 48h	**MOYENNE**	Vérifier la licence FortiGuard + connectivité

7. Commandes CLI utiles

Commande FortiOS	Description
get system status	Version FortiOS et état des licences
diagnose sys top	Processus actifs et charge CPU/RAM
diagnose ip arp list	Table ARP (hôtes actifs sur LAN)
get ips status	Version et état des signatures IPS

diagnose autoupdate status	Statut de la dernière mise à jour FortiGuard
execute log display	Afficher les derniers logs système