GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

GUIDE DE MIGRATION

Version 2.7.1

Dernière mise à jour du document : 30 juin 2025

Référence : ses-fr-guide_de_migration-v2.7.1

Table des matières

Dans la documentation, Stormshield Endpoint Security Evolution est désigné sous la forme abrégée : SES Evolution.

1. Avant de commencer

Bienvenue dans le guide de migration de Stormshield Endpoint Security Evolution version 2.7.1.

Ce document contient toutes les informations nécessaires pour migrer votre environnement SES Evolution des versions 2.6.x aux versions 2.7.x.

Vous devez suivre pas à pas les procédures décrites dans ce guide pour disposer d'une solution SES Evolution fonctionnelle après migration.

2. Connaître les prérequis

Pour procéder à la migration vers SES Evolution 2.7.1, vous devez disposer au minimum des prérequis ci-dessous :

- SES Evolution 2.6.x doit être installé sur tous les composants backoffice : gestionnaires d'agents, backends et consoles d'administration.
- Les Runtimes suivants en version 8.0.x la plus récente doivent être installés sur les machines hébergeant les gestionnaires d'agents. Les liens ci-dessous vous permettent de télécharger la version 8.0.11 :
  - ASP.NET Core 8.0.x
  - Exécution de bureau .NET 8.0.x
- Si vous utilisez un firewall, sa configuration doit être mise à jour pour refléter les changements de ports de communication effectués en version 2.7.1. Pour plus d'informations, reportez-vous à la section Configurer le firewall.
- Vous devez avoir lu attentivement les Notes de version SES Evolution 2.7.1.

3. Configurer le firewall

SES Evolution 2.7.1 utilise désormais le port standard HTTPS (443) entre les agents et les gestionnaires d'agents afin de faciliter le déploiement. Vous devez préparer la nouvelle configuration de votre firewall avant d'installer SES Evolution 2.7.1.

3.1 Avertissement

Vous devez impérativement maintenir l'ancienne ET la nouvelle configuration du firewall pendant toute la phase de migration du backoffice.
Ne supprimez définitivement l'ancienne configuration firewall qu'une fois la migration terminée sur tous les composants backoffice : gestionnaires d'agents, backends et consoles d'administration.

3.2 Mettre à jour la configuration du firewall

La version 2.7.1 de SES Evolution apporte les changements suivants concernant les ports de communication :

- Le port 443 est désormais utilisé pour la communication des agents avec les gestionnaires d'agents,
- Le port 8443 est désormais utilisé par les backends pour communiquer avec les consoles d'administration et les gestionnaires d'agents.

Modifiez donc les règles de votre firewall en vous aidant du tableau ci-dessous. Ce dernier détaille les ports utilisés par les composants de SES Evolution et les différences entre les versions 2.6 et 2.7.1. Les nouveautés sont indiquées en gras.

Si vous disposez uniquement de Windows Defender Firewall, certains changements de ports sont appliqués automatiquement par SES Evolution. Pour plus d'informations, reportez-vous à la sectionCas de Windows Defender Firewall.

Composant	Sens	Port 2.6	Port 2.7 si backend et gestionnaire d'agents sont installés sur la même machine	Port 2.7 si backend et gestionnaire d'agents sont installés sur des machines différentes	Objectif
Backend	entrant	TCP 443	**TCP 8443**	**TCP 443**	Communication avec la console d'administration et le gestionnaire d'agents.
	entrant	TCP 10443	TCP 10443	TCP 10443	API publique.
	sortant	TCP 443	TCP 443	TCP 443	Accès au serveur public Stormshield de mise à jour des politiques
	sortant	TCP 1433 (SQL) TCP 1434 (SQL) UDP 1434 (SQL)	TCP 1433 (SQL) TCP 1434 (SQL) UDP 1434 (SQL)	TCP 1433 (SQL) TCP 1434 (SQL) UDP 1434 (SQL)	Communication avec la base de données SQL Server. Ce sont les ports par défaut, ils peuvent être modifiés lors de la création de l'instance.
Console d'administration	sortant	TCP 443	**TCP 8443**	**TCP 443**	Communication avec le backend.
Gestionnaire d'agents	sortant	TCP 443	**TCP 8443**	**TCP 443**	Communication avec le backend.
	sortant	TCP 1468 UDP 514 TCP 5614	TCP 1468 UDP 514 TCP 5614	TCP 1468 UDP 514 TCP 5614	Communication avec le serveur Syslog. Les ports utilisés dépendent de la configuration des groupes de gestionnaires d'agents dans la console d'administration.
	entrant	TCP 17000	TCP 17000	TCP 17000	Communication avec les agents dont la version **est inférieure à 2.7.1** en MSRPC.
	entrant	N/A	**TCP 443**	**TCP 443**	Communication avec les agents dont la version est **2.7.1 ou supérieure** en HTTPS.
Agent inférieur à 2.7.1	sortant	TCP 17000	TCP 17000	17000	Communication avec les gestionnaires d'agents.
Agent supérieur ou égal à 2.7.1	sortant	N/A	**TCP 443**	**TCP 443**	Communication avec les gestionnaires d'agents.

3.3 Cas de Windows Defender Firewall

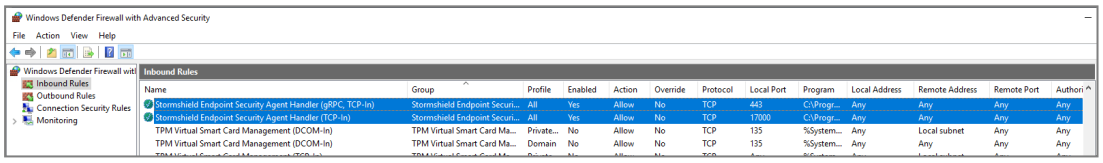
Lors de l'installation des composants backoffice, SES Evolution crée automatiquement des règles sur Windows Defender Firewall, que ce dernier soit actif ou non.

Les règles créées pour la version 2.7.1 sont les suivantes :

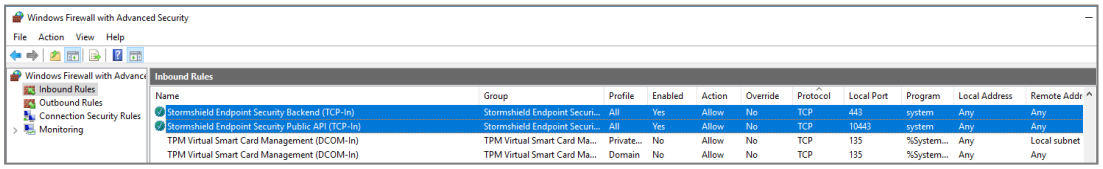
3.3.1 Si backend et gestionnaire d'agents sont installés sur des machines différentes

Règles entrantes

- Sur la machine hébergeant le gestionnaire d'agents :
  - *Stormshield Endpoint Security Evolution Agent Handler (TCP-In)* sur le port 17000 pour la communication avec les agents dont la version **est inférieure à 2.7.1** via EsServer en MSRPC.
  - *Stormshield Endpoint Security Evolution Agent Handler (TCP-In)* sur le port 443 pour la communication avec les agents dont la version est **2.7.1 ou supérieure** via EsServer en HTTPS.



- Sur la machine hébergeant le backend :
  - *Stormshield Endpoint Security Evolution Backend (TCP-In)* sur le port 443 pour la communication avec les consoles, et les gestionnaires d'agents en tant qu'utilisateur *system*.
  - *Stormshield Endpoint Security Evolution Public API (TCP-In)* sur le port 10443 pour la communication avec les SIEM / SOAR en tant qu'utilisateur *system*.



Règles sortantes

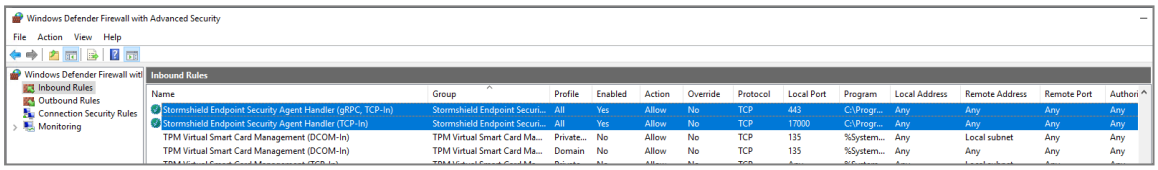
L'installation de SES Evolution ne crée aucune règle sortante sur Windows Defender Firewall.

Si vous filtrez les connexions sortantes, vous devez modifier vos règles manuellement afin que les consoles d'administration et les gestionnaires d'agents puissent se connecter aux backends sur le port TCP 8443.

3.3.2 Si backend et gestionnaire d'agents sont installés sur la même machine

Règles entrantes

- Sur la machine hébergeant le gestionnaire d'agents :
  - *Stormshield Endpoint Security Evolution Agent Handler (TCP-In)* sur le port 17000 pour la communication avec les agents dont la version **est inférieure à 2.7.1** via EsServer en MSRPC.
  - *Stormshield Endpoint Security Evolution Agent Handler (TCP-In)* sur le port 443 pour la communication avec les agents dont la version est **2.7.1 ou supérieure** via EsServer en HTTPS.
- Sur la machine hébergeant le backend :
  - *Stormshield Endpoint Security Evolution Backend (TCP-In)* sur le port 8443 pour la communication avec les consoles, et les gestionnaires d'agents en tant qu'utilisateur *system*.
  - *Stormshield Endpoint Security Evolution Public API (TCP-In)* sur le port 10443 pour la communication avec les SIEM / SOAR en tant qu'utilisateur *system*.



Règles sortantes

L'installation de SES Evolution ne crée aucune règle sortante sur Windows Defender Firewall.

Si vous filtrez les connexions sortantes, vous devez modifier vos règles manuellement afin que les consoles d'administration et les gestionnaires d'agents puissent se connecter aux backends sur le port TCP 8443.

4. Mettre à jour le backoffice SES Evolution en 2.7.1

1. Mettez à jour le backoffice SES Evolution en suivant la procédure décrite dans la section Mettre à jour SES Evolution du guide d'installation de SES Evolution.
2. Ouvrez la console d'administration. Elle se met à jour automatiquement en 2.7.1 lors de son démarrage.
   La nouvelle console 2.7.1 présente les caractéristiques suivantes :
   - Un bandeau jaune indique que les politiques de sécurité n'utilisent plus les dernières versions des jeux de règles Stormshield.
   - Une demande de déploiement est en attente dans le panneau **Sécurité > Déploiement**.
3. Cliquez sur le bouton **Déployer** pour mettre à jour l'environnement.
4. Dans le menu **Backoffice > Système** logs, vérifiez qu'il n'y ait aucune erreur liée à la migration.
5. Dans le menu **Environnement > Logs agents**, vérifiez qu'il n'y ait aucune erreur liée à la migration.
6. Mettez à jour les politiques de sécurité par défaut. Cette étape peut être effectuée immédiatement ou plus tard à votre convenance. Assurez-vous de :
   - Lire attentivement les Notes de version de la politique de sécurité par défaut *2506a* pour connaître les changements apportés aux politiques de sécurité Stormshield et aux jeux de règles.
   - Lire attentivement les Notes de version SES Evolution 2.7.1, en particulier la section Préconisations.
7. Cliquez sur le bouton **Déployer** pour mettre à jour les agents existants.
   Le bandeau jaune ne s'affiche plus.
8. Une fois la migration vers la version 2.7.1 effectuée pour le backoffice et tous les agents sans exception, fermez le port 17000 des gestionnaires d'agents et agents.

5. Mettre à jour les agents en 2.7.1

1. Mettez à jour les agents en suivant la procédure décrite dans la section Mettre à jour SES Evolution du guide d'installation de SES Evolution.
2. Redémarrez les machines lorsque la procédure le demande.
3. Une fois la migration vers la version 2.7.1 effectuée pour le backoffice et tous les agents sans exception, fermez le port 17000 des gestionnaires d'agents et agents.

6. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur SES Evolution sont disponibles sur le site web Documentation et dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu