Configuration Anti-Ransomware ESET

Sécurité multicouche contre le chiffrement

Version du document :
1.1

Auteurs :
Michael van der Vaart, Directeur de la Technologie
Donny Maasland, Directeur de la recherche en cybersécurité

ENJOY SAFER TECHNOLOGY™

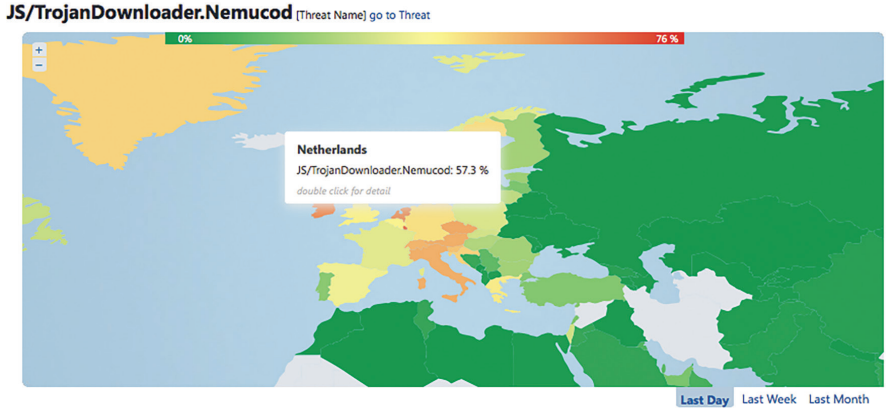
SOMMAIRE

OBJECTIF DE CE BRIEF TECHNIQUE

Dans ce brief technique, nous décrivons le paramétrage optimal pour nos solutions de sécurité ESET contre les formes actuelles de ransomwares et les scénarios d'infection les plus fréquents. Le but est de protéger au mieux nos clients contre une épidémie de ransomwares, où les données peuvent être chiffrées ou prises en otage en échange d'une demande de rançon.

POURQUOI CES PARAMÈTRES ADDITIONNELS ?

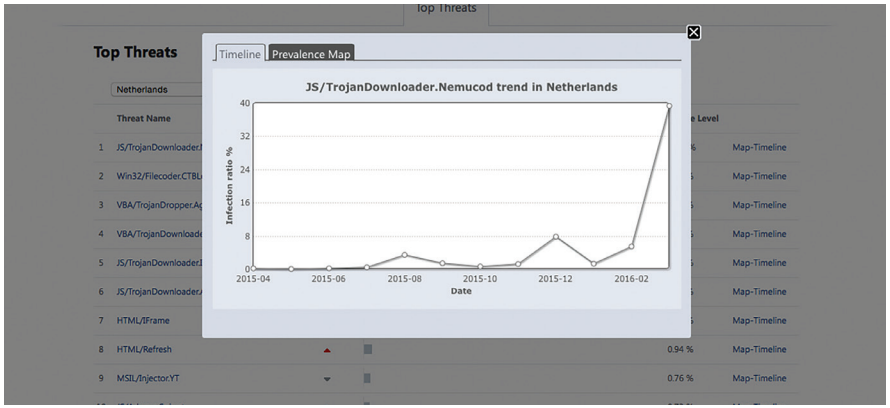
Près de 60% des malwares détectés en France peuvent aboutir à une infection par ransomware



Les attaques actuelles de ransomwares utilisent des techniques de contamination avancées, permettant au logiciel malveillant d'infecter votre appareil. Ils persuadent les utilisateurs d'exécuter ce qu'on appelle un dropper qui va ensuite télécharger le logiciel malveillant pour commencer le processus de chiffrement. En attachant le dropper à un email, les cybercriminels tentent d'empêcher la détection à l'entrée. Dans la plupart des cas, un email de phishing correctement constitué est utilisé avec un fichier ZIP en pièce jointe. Le fichier ZIP contient la plupart du temps un fichier JavaScript de type .JS.

JavaScript étant utilisé par de nombreux sites internet, il est impossible de le bloquer dans le navigateur. De plus, Windows exécute également JavaScript directement.

Dans le même temps, le code JavaScript dans le dropper est fortement obscurci voire effacé, et est continuellement modifié dans le but d'empêcher la détection. Cela nous donne l'opportunité d'influer sur l'exécution d'un code malveillant potentiel, en utilisant différents modules de sécurité à travers des processus standards.

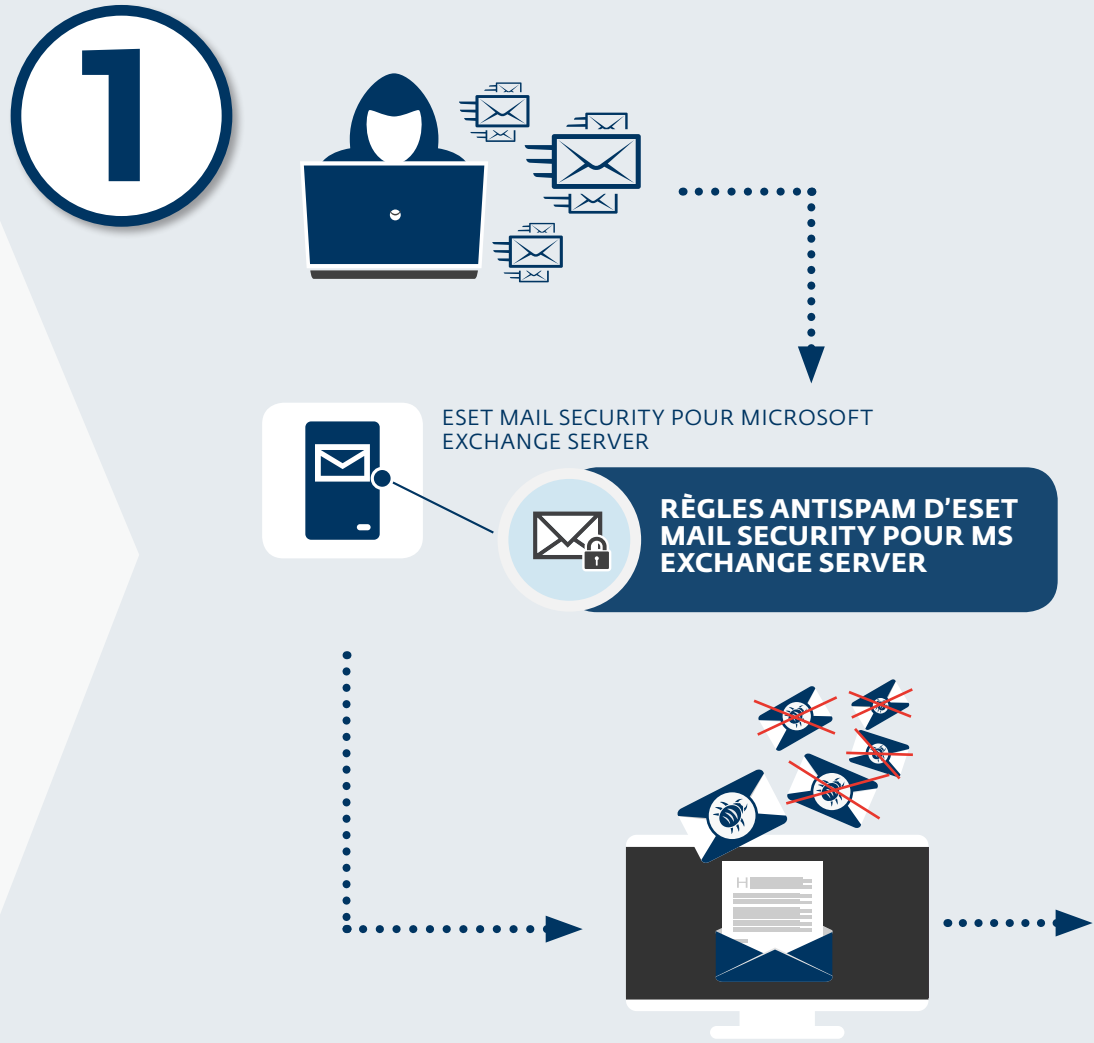


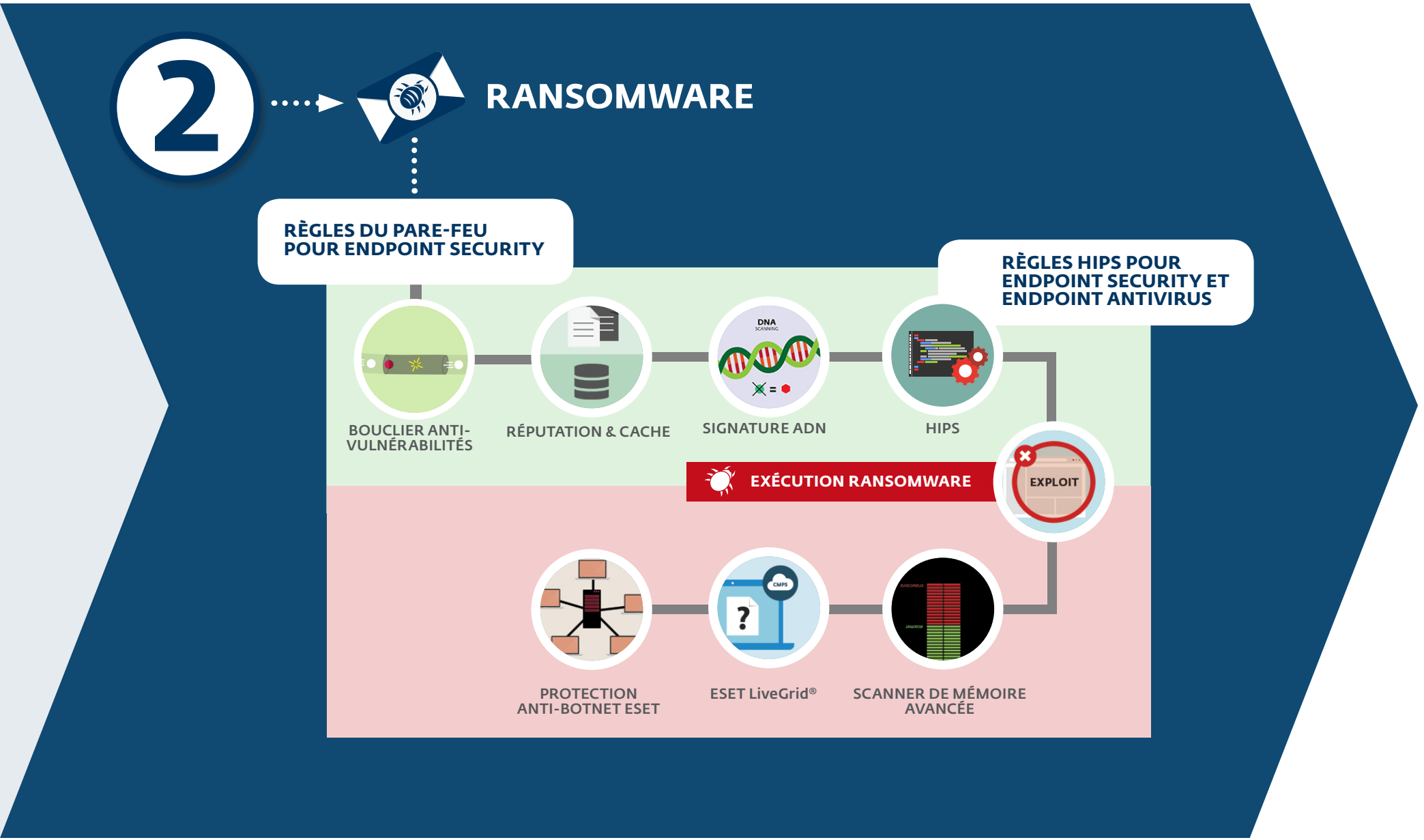
Clause de non responsabilité :
La configuration et les politiques Anti-Ransomware ESET sont établies de manière générale et peuvent varier selon les spécificités de chaque entreprise. Nous recommandons de tester les paramètres pour chaque implémentation avant de mettre en production.

CONFIGURATION ANTI-RANSOMWARE ESET POUR LES ENTREPRISES

En bloquant la méthode d'infection des ransomwares (utilisation d'un dropper Javascript), les paramètres supplémentaires de notre configuration Anti-Ransomware ESET empêchent les logiciels malveillants de lancer le téléchargement. Cette approche se révélant être très efficace, nous avons décidé d'expliquer ces paramètres supplémentaires en détail dans ce brief technique, et de les proposer en tant que stratégie de configuration que vous pourrez télécharger et mettre en œuvre en utilisant ESET Remote Administrator.

TÉLÉCHARGEZ LES PARAMÈTRES



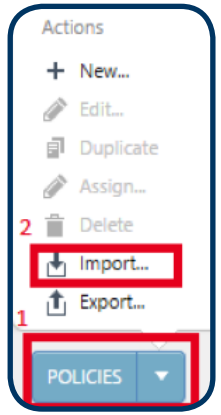

2
RANSOMWARE
RÈGLES DU PARE-FEU POUR ENDPOINT SECURITY
RÈGLES HIPS POUR ENDPOINT SECURITY ET ENDPOINT ANTIVIRUS
DNA
BOUCLIER ANTI-VULNÉRABILITÉS
RÉPUTATION & CACHE
SIGNATURE ADN
HIPS
EXÉCUTION RANSOMWARE
EXPLOIT
PROTECTION ANTI-BOTNET ESET
ESET LiveGrid®
SCANNER DE MÉMOIRE AVANCÉE

RÈGLES ANTISPAM D'ESET MAIL SECURITY POUR MS EXCHANGE

En utilisant les bonnes règles antispam, les emails entrants sont déjà filtrés sur le serveur de messagerie. Cela garantit que la pièce jointe qui contient le dropper malveillant ne sera pas délivrée dans la boîte mail de l'utilisateur, et que le ransomware ne pourra donc pas être exécuté

Comment importer et appliquer les stratégies ?*

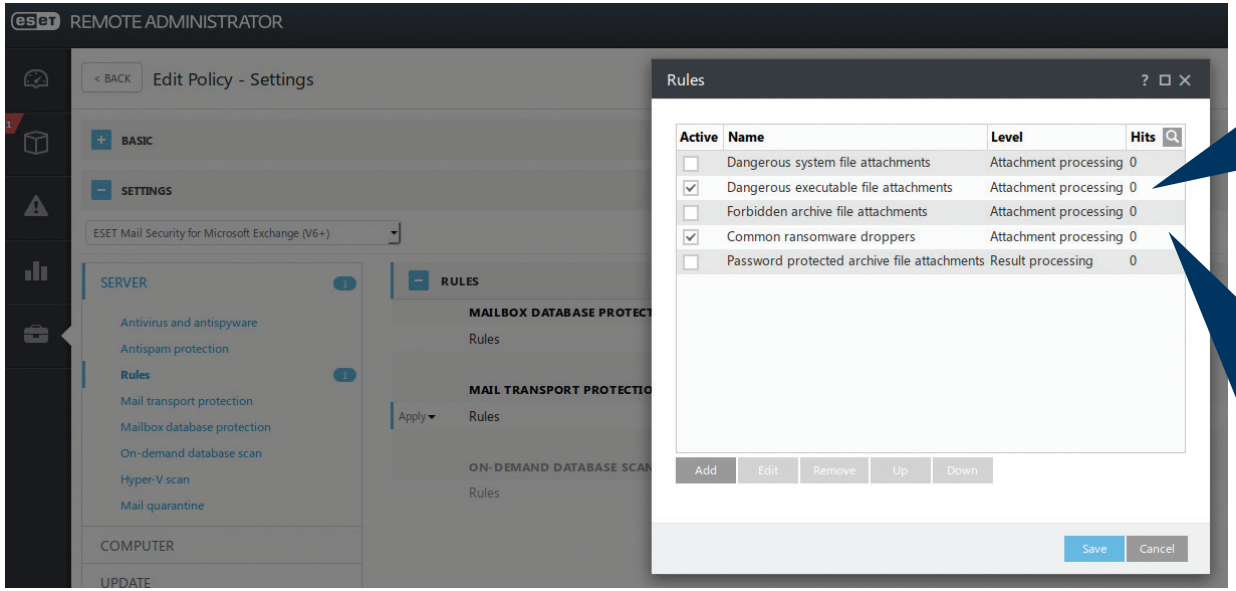
1. Connectez-vous à la console web ERA 6
2. Allez dans ADMIN > Stratégies
3. Choisissez « Stratégies » puis « Importer »
4. Importez les stratégies une par une
5. Attribuez les stratégies à un *groupe* ou un *client*

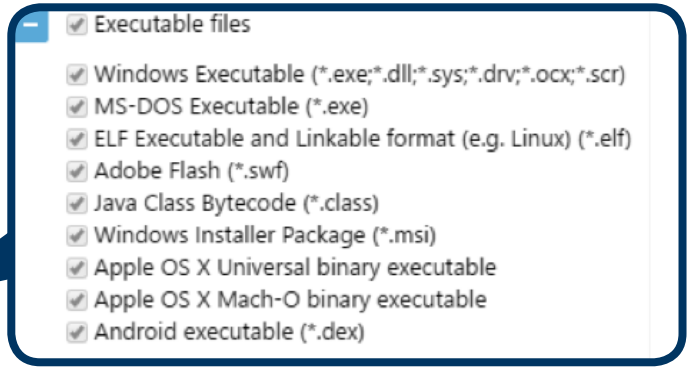


***La répétition n'est pas nécessaire avec les autres paramètres**

Important :

Mettez à niveau ESET Mail Security pour Microsoft Exchange Server à la dernière version disponible : 6.3 ou plus pour garantir le fonctionnement des règles de filtrage.





Règle « Common Ransomware droppers » qui bloque les extensions suivantes* :

*.js
*.hta
*.docm
*.xlsm
*.pptm
*.vbs
*.bat

*Dans ce cas, les fichiers Microsoft Office avec macros seront eux aussi bloqués (docm, xlsm et pptm). Lorsque de tels fichiers sont utilisés dans votre entreprise, cette règle doit être ajustée ou désactivée.

RÈGLES DE PARE-FEU POUR ENDPOINT SECURITY

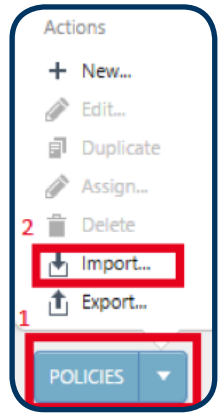
Si le dropper avec un code malveillant est exécuté, ESET Endpoint Security empêche toujours le téléchargement de logiciels malveillants grâce au pare-feu intégré.

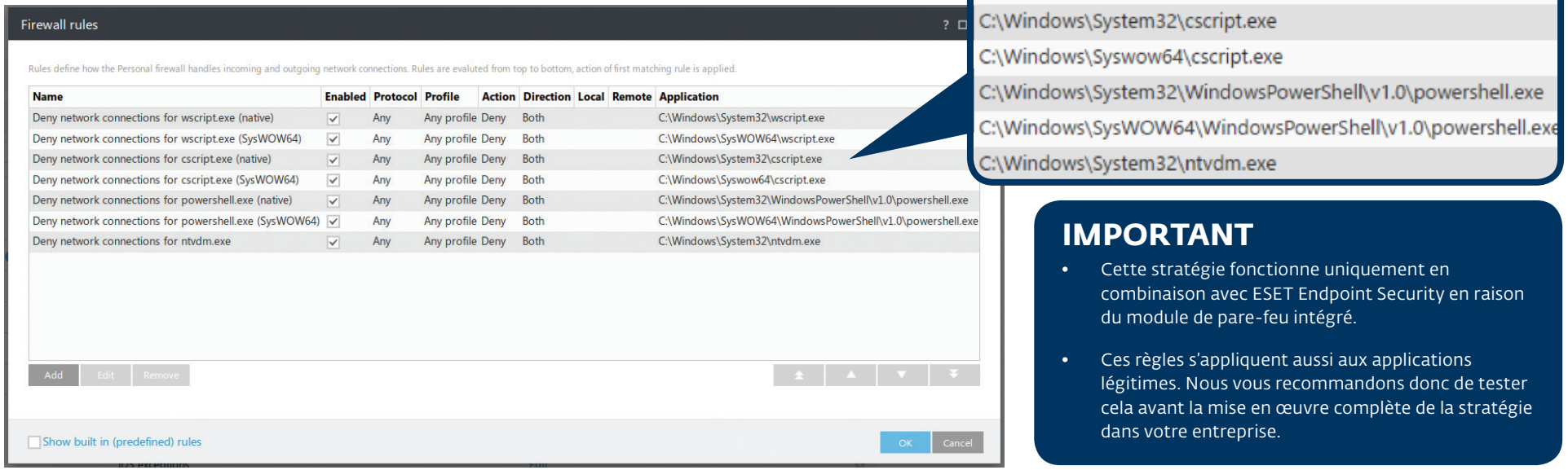
En appliquant ces règles de pare-feu, ESET Endpoint Security bloquera le téléchargement de charges utiles malveillantes et refusera tout autre accès à Internet scripté.

Comment importer et appliquer les stratégies

1. Connectez-vous à la console web ERA 6
2. Allez dans ADMIN > Stratégies
3. Choisissez « Stratégies » puis « Importer »
4. Importez les stratégies une par une
5. Attribuez les stratégies à un *groupe* ou un *client*

Veuillez noter que lorsque vous importez les règles de pare-feu, d'autres règles peuvent être écrasées.





IMPORTANT

- Cette stratégie fonctionne uniquement en combinaison avec ESET Endpoint Security en raison du module de pare-feu intégré.
- Ces règles s'appliquent aussi aux applications légitimes. Nous vous recommandons donc de tester cela avant la mise en œuvre complète de la stratégie dans votre entreprise.

RÈGLES HIPS POUR ENDPOINT SECURITY & ENDPOINT ANTIVIRUS

Le système de prévention d'intrusion basé sur l'hôte (HIPS) défend le système de l'intérieur, et est en mesure d'interrompre des actions non autorisées de processus avant qu'elles ne soient en cours d'exécution. En interdisant l'exécution standard de JavaScript et d'autres scripts, le ransomware ne peut pas exécuter le logiciel malveillant, et encore moins le télécharger.

Notre HIPS est disponible dans ESET File Security pour Windows Server, le rendant applicable aux serveurs. Veuillez noter que le HIPS ne distinguera pas les scripts légitimes qui seraient en production

Comment importer et appliquer les stratégies

1. Connectez-vous à la console web ERA 6
2. Allez dans ADMIN > Stratégies
3. Choisissez « Stratégies » puis « Importer »
4. Importez les stratégies une par une
5. Attribuez les stratégies à un *groupe* ou un *client*

IMPORTANT

- Ces règles bloquent des exécutables qui peuvent également être utilisés par des applications légitimes. Nous vous recommandons donc de tester cela avant la mise en œuvre complète de la stratégie dans votre entreprise.

Bloquez les processus enfants des exécutables dangereux

Application
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\Syswow64\cscript.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\ntvdm.exe

Bloquez les processus script lancés par l'explorateur

C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe

Bloquez les processus enfants dangereux de Office 201X

C:\Windows\System32\cmd.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe
C:\Windows\System32\ntvdm.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

CONFIGURATION ANTI-RANSOMWARE ESET : RÉSULTAT DU TEST

Avec une configuration Anti-Ransomware ESET complète du serveur de messagerie aux postes de travail, en passant même par les serveurs, les emails de ransomware avec des droppers en pièce jointe sont déjà filtrés avant même d'avoir été détectés en tant que code malveillant ou ransomware. En plus des terminaux où sont appliqués ces paramètres renforcés, nous avons effectué plusieurs tests où nous avons désactivé toutes les couches de détection de nos solutions de sécurité ESET, démontrant ainsi que ces types de ransomwares n'ont aucune chance de chiffrer le système et le réseau.

Pour conclure, la Configuration Anti-Ransomware ESET est un renforcement des solutions de sécurité ESET qui minimise le risque d'infection par ransomware et de chiffrement des données sensibles d'entreprise.