



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD MULTI-LAYER COLLABORATIVE SECURITY

ADAPTER LA POLITIQUE DE SÉCURITÉ SES D'UN POSTE SELON SA RÉPUTATION SNS

Produits concernés : SNS 3.x, SNS 4.x, SES 7.2 et versions supérieures

Date : 09 décembre 2019

Référence : mlcs-fr-adapter_politique_securite_SES_poste_reputation_SNS_note_technique



Table des matières

Avant de commencer	3
Comprendre l'interaction entre SES et le firewall SNS	3
Configurer le firewall SNS	4
Activer la gestion de réputation des machines internes	4
Configurer la règle de filtrage basée sur la réputation des machines	4
Visualiser la réputation des machines internes	5
Configurer la politique dans la console SES	5
Créer un script de génération de requêtes ICMP	5
Déployer le test sur les agents SES	6
Définir la politique de sécurité renforcée	6
Créer une ressource de script basée sur le script de génération de requêtes ICMP	6
Créer les scripts SES utilisant la ressource de script HostCheckResource	7
Principe	7
Définir ces scripts dans la console SES	8
Appliquer la politique de sécurité à des machines du domaine	10
Exemple de script Visual Basic	11



Avant de commencer

L'objectif de ce document est de présenter l'interaction de la gestion de réputation des machines sur un firewall Stormshield Network Security (SNS) avec le niveau de sécurité appliqué par Stormshield Endpoint Security (SES) à une machine infectée.

En effet, lorsque la gestion de réputation des machines internes est activée, et si la réputation d'une machine dépasse une valeur déterminée, il est possible d'augmenter localement le niveau de sécurité du poste à l'aide de SES.

L'exemple décrit dans cette Note Technique présente le cas d'un poste interne infecté. Stormshield Network Vulnerability Manager ayant détecté les vulnérabilités présentes sur cette machine, le score de réputation de celle-ci augmente donc naturellement. Le niveau de sécurité affecté au poste est alors automatiquement accru via SES afin d'éviter que l'infection ne s'étende au reste du réseau interne.

Comprendre l'interaction entre SES et le firewall SNS

Pour réaliser cette configuration, il est nécessaire de créer :

- une règle de filtrage basée sur la réputation des machines sources et le protocole ICMP. Cette règle interdit un *Ping* à destination d'une cible normalement joignable en permanence lorsque la réputation des machines sources excède un niveau déterminé.
- des scripts SES générant des requêtes ICMP vers la destination de la règle de filtrage. Lorsque une machine au score de réputation élevé n'est plus autorisée par le firewall à joindre cette destination, l'échec des *Ping* entraîne une modification du comportement de l'agent SES afin d'augmenter le niveau de sécurité du poste.

Consultez la suite de ce document pour les détails de la mise en place de chaque étape. Il s'agit d'un exemple, que vous pourrez adapter à d'autres situations du même type.



Configurer le firewall SNS

Activer la gestion de réputation des machines internes

1. Dans le module **Configuration** > **Protection applicative** > **Réputation des machines**, sur l'onglet *Configuration*, activez la gestion de réputation des machines. Il est possible d'adapter le poids respectif des différents critères intervenant dans le calcul du score de réputation de la machine (alarmes majeures et mineures, résultats d'analyse antivirus, résultats d'analyse sandboxing).

The screenshot shows the 'CONFIGURATION' tab for 'HOSTS MONITORED'. Under the 'General' section, there is a toggle switch set to 'ON'. Below this, a note states: 'Choose the value of points that increment a host's reputation score. This score will be leveled out over time.' The interface is divided into three risk categories, each with three sliders:

- Alarm risk:** Major [0-20] (orange slider at ~10), Minor [0-20] (yellow slider at ~5).
- Antivirus risk:** Infected [0-100] (red slider at ~90), Unknown [0-20] (yellow slider at ~5), Scan failed [0-20] (blue slider at ~5).
- Sandboxing risk:** Malicious [0-100] (orange slider at ~50), Suspicious [0-100] (yellow slider at ~10), Scan failed [0-20] (blue slider at ~5).

At the bottom, there is a 'Statistics' section and a button labeled 'Reset reputation scores for all hosts in the database'.

2. Dans l'onglet *Machines*, indiquez les réseaux, machines ou groupes de machines à superviser. L'objet **Network_internals** est sélectionné par défaut.

Configurer la règle de filtrage basée sur la réputation des machines

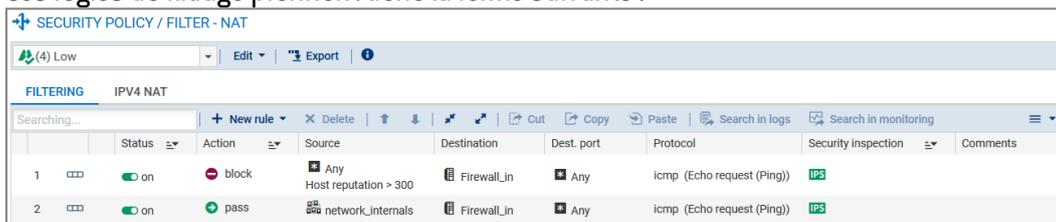
L'objectif de cette règle est de bloquer les requêtes ICMP des machines internes dont le score de réputation est supérieur à une valeur déterminée. De cette manière, le script générant ces requêtes et présent sur chacune des machines internes détectera l'absence de réponse et provoquera un changement de comportement de l'agent SES (sécurité accrue).

1. Dans le module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, sélectionnez votre politique de filtrage active dans le menu déroulant.
2. Positionnez-vous sur l'onglet *Filtrage*, cliquez sur **Nouvelle règle**, puis choisissez **Règle simple**.
3. Double cliquez sur le champ **État** afin d'activer la règle.
4. Double cliquez sur le champ **Source** afin d'éditer la règle de filtrage.



5. Dans l'onglet *Géolocalisation / réputation*, cochez la case **Activer le filtrage selon le score de réputation**.
6. Choisissez l'opérateur  (« Supérieur à ») et indiquez le score de réputation souhaité.
7. Sélectionnez la section **Destination** (menu gauche de la fenêtre d'édition de règle). Pour le champ **Machines destination**, sélectionnez (ou créez) la machine vers laquelle les requêtes ICMP seront dirigées. Cette machine doit être joignable en permanence. Il peut s'agir, comme dans cet exemple, de l'interface du firewall connectée aux réseaux internes (objet **Firewall_in**). Si cette interface nécessite d'être joignable en permanence (exemple : pour une solution de supervision réseau), il est conseillé de lui attribuer une seconde adresse IP dédiée à cette règle.
8. Sélectionnez la section **Port / Protocole**. Dans la partie **Protocoles**, remplissez les champs comme suit :
 - **Type de protocole** : Protocole IP,
 - **Protocole IP** : icmp,
 - **Message ICMP** : requête Echo (Ping).
9. Validez en cliquant sur **OK**.
10. En utilisant cette méthode, créez une règle, placée au dessous de celle-ci, et autorisant les requêtes ICMP pour toutes les autres machines.

Ces règles de filtrage prennent donc la forme suivante :



Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
on	block	Any Host reputation > 300	Firewall_in	Any	icmp (Echo request (Ping))	IPS	
on	pass	network_internals	Firewall_in	Any	icmp (Echo request (Ping))	IPS	

Visualiser la réputation des machines internes

Dans le module **Monitoring > Supervision > Machines**, la fenêtre supérieure présente les machines internes détectées par le firewall. La colonne **Réputation** permet de visualiser le score de chacune des machines supervisées.

Sélectionnez une machine pour afficher le détail de ses vulnérabilités ainsi que l'évolution de son score de réputation dans les onglets *Vulnérabilités* et *Historique des réputations* de la fenêtre inférieure.

Configurer la politique dans la console SES

Créer un script de génération de requêtes ICMP

1. Créez un script selon l'exemple présenté dans la section [Exemple de script Visual Basic](#).
2. Nommez ce script (*CheckHost.vbs* dans l'exemple) et déposez-le sur la machine hébergeant la console SES.



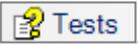
Déployer le test sur les agents SES

1. Dans le menu **Gestion des environnements**, cliquez sur **Politiques** puis sur le bouton  du panneau inférieur.
2. Sélectionnez le fichier que vous souhaitez transférer (*CheckHost.vbs* dans l'exemple).
3. Cliquez sur **Appliquer les changements à l'environnement** pour envoyer ce fichier vers le(s) serveur(s) SES afin qu'il soit récupéré par les agents lors de leur prochaine connexion à ce(s) serveur(s).

Définir la politique de sécurité renforcée

1. Dans le menu **Gestion des environnements**, cliquez sur **Politiques** puis sur l'icône  du panneau inférieur.
2. Sélectionnez le type **Sécurité**, nommez cette politique (*HostBadReputationPolicy* dans l'exemple) et validez.
3. Configurez les différents paramètres associés à cette politique renforcée. Cette configuration étant très dépendante de l'environnement d'utilisation des postes, aucun exemple n'est décrit dans ce document. Pour de plus amples renseignements sur la méthode de création d'une politique SES, veuillez consulter le *Guide d'Administration Stormshield Endpoint Security*.

Créer une ressource de script basée sur le script de génération de requêtes ICMP

1. Dans le menu **Gestion des environnements** > **Politiques**, faites un clic droit sur le dossier **Ressources de scripts** puis cliquez sur le bouton  de la fenêtre .
2. Nommez ce test (*HostCheckResource* dans l'exemple) et validez.

Adapter la condition "IF AND"

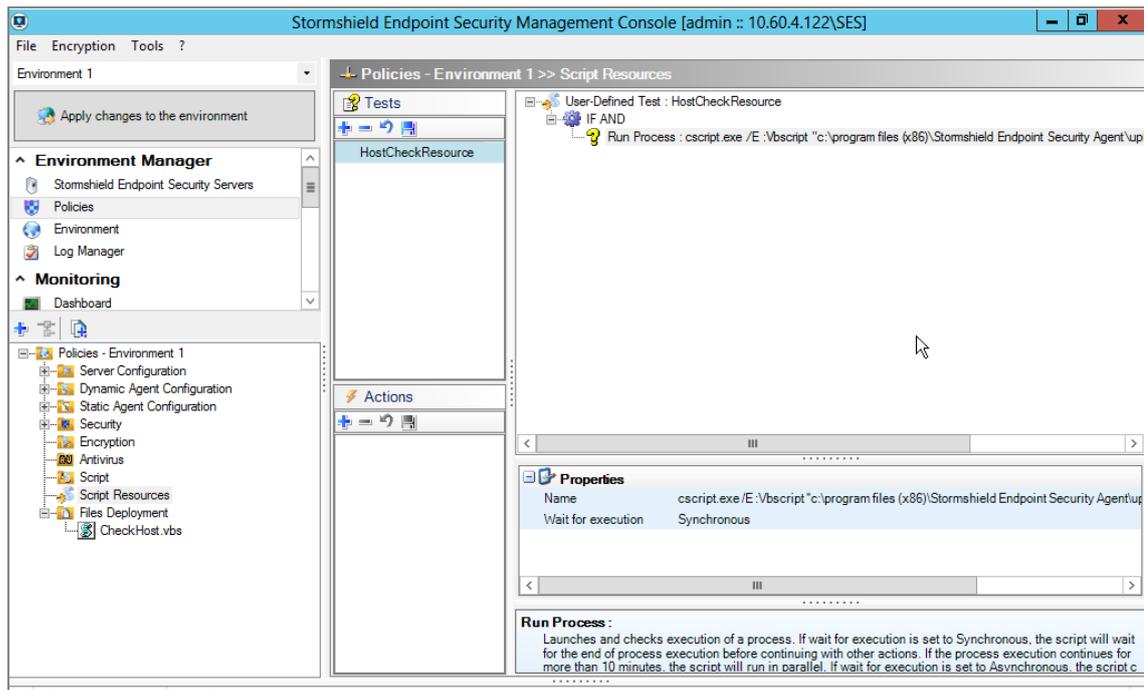
1. Faites un clic droit sur la condition IF AND et choisissez **Ajouter un test intégré** puis **Exécuter un programme**.
2. Dans les propriétés, cliquez sur le champ **Nom** et entrez la commande :

```
Cscript.exe /E:Vbscript "C:\Program Files (x86)\Stormshield Endpoint Security Agent\uploaded\CheckHost.vbs.srn"
```

NOTE

L'extension *.sm* est ajoutée par SES lors du [déploiement du script vers les agents SES](#).

3. Champ **Attente de l'exécution** : sélectionnez *Synchrone*. La valeur *Synchrone* signifie que l'agent SES attend la fin du script avant de laisser toute autre action se dérouler. La valeur *Asynchrone* indique au contraire que l'agent SES peut déclencher une autre action définie au préalable, sans attendre le retour du script.
4. Validez la création du test en cliquant sur l'icône  de la fenêtre .



Créer les scripts SES utilisant la ressource de script *HostCheckResource*

Principe

Deux scripts sont définis pour gérer la politique de sécurité appliquée au poste de travail selon le résultat du test de *Ping* :

Le script de base (*HostReputationOK* dans l'exemple) effectue un test de *Ping* par le biais de la ressource *HostCheckResource* :

- Tant que le poste parvient à joindre sa cible (réputation correcte), ce même script est relancé toutes les 20 secondes,
- Lorsque le poste ne parvient pas à joindre sa cible (réputation incorrecte) :
 1. Une politique de sécurité renforcée est appliquée au poste (*HostBadReputationPolicy* dans l'exemple),
 2. Un autre script (*HostBadReputation*) est exécuté toutes les 20 secondes.

Le script lancé en cas de mauvaise réputation (*HostBadReputation* dans l'exemple) effectue à son tour un test de *Ping* par le biais de la ressource *HostCheckResource* :

- Tant que le poste ne parvient pas à joindre sa cible (réputation incorrecte), ce même script est relancé toutes les 20 secondes,
- Lorsqu'il parvient de nouveau à joindre sa cible (remédiation effectuée - réputation correcte) :
 1. On réévalue la politique de sécurité appliquée au poste (pour permettre un éventuel retour à la politique standard),
 2. On revient à l'exécution du script *HostReputationOK*.



Définir ces scripts dans la console SES

Script *HostReputationOK*

1. Dans le menu **Gestion des environnements > Politiques**, faites un clic droit sur le dossier **Script**.
2. Cliquez sur le menu **Nouvelle politique...**
3. Sélectionnez le type **Script** et nommez cette politique (*HostReputationOK* dans l'exemple).

Adapter la condition "IF ..."

1. Faites un clic droit sur la condition "IF AND" et choisissez **Ajouter un test utilisateur**.
2. Sélectionnez le script *HostCheckResource*.

Adapter le résultat "Vrai"

1. Faites un clic droit sur la condition "IF AND" et choisissez **Ajouter une action intégrée > Exécution > Script**.
2. En déroulant la liste du champ **Nom** du panneau **Propriétés**, sélectionnez le script *HostReputationOK*.
3. Éditez le champ **Attente (secondes)** et indiquez *20*.

Adapter le résultat "Faux"

1. Faites un clic droit sur ce résultat et choisissez **Ajouter une action intégrée > Configuration > Appliquer une politique**.
2. En déroulant la liste du champ **Name** du panneau **Propriétés**, sélectionnez la politique de sécurité renforcée créée précédemment (*HostBadReputationPolicy*).
3. La dernière étape de configuration du résultat "Faux" ne peut être réalisée que lorsque le script *HostBadReputation* aura été créé.

Script *HostBadReputation*

1. Dans le menu **Gestion des environnements > Politiques**, faites un clic droit sur le dossier **Script**.
2. Cliquez sur le menu **Nouvelle politique...**
3. Sélectionnez le type **Script** et nommez cette politique (*HostBadReputation* dans l'exemple).

Adapter la condition "IF ..."

1. Cliquez sur la condition "IF AND".
2. Dans le panneau **Propriétés**, déroulez la liste du champ **Condition** et choisissez "IF NOT".
3. Dans le panneau **Politique**, faites un clic droit sur "IF NOT" et choisissez **Ajouter un test utilisateur**.
4. Sélectionnez le script *HostCheckResource*.

Adapter le résultat "Vrai"

1. Faites un clic droit sur la condition "IF AND" et choisissez **Ajouter une action intégrée > Exécution > Script**.
2. Dans le panneau **Propriétés**, déroulez la liste du champ **Nom** et sélectionnez le script *HostBadReputation*.
3. Éditez le champ **Attente (secondes)** et indiquez *20*.



Adapter le résultat "Faux"

1. Faites un clic droit sur ce résultat et choisissez **Ajouter une action intégrée** > **Configuration** > **Réévaluer les politiques**.
2. Faites un nouveau clic droit sur le résultat "Faux" et choisissez **Ajouter une action intégrée** > **Exécution** > **Script**.
3. Dans le panneau **Propriétés** : déroulez la liste du champ **Nom** et sélectionnez le script *HostReputationOK*. Éditez le champ **Attente (secondes)** et indiquez *20*.

Compléter le script CheckHostOK

Compléter le résultat "Faux"

1. Faites un clic droit sur le résultat "Faux" et choisissez **Ajouter une action intégrée** > **Exécution** > **Script**.
2. Dans le panneau **Propriétés** : éditez le champ **Nom** et sélectionnez le script *HostBadReputation*. Éditez le champ **Attente (secondes)** et indiquez *20*.

Les deux scripts prennent donc la forme suivante :

Environment 1

Apply changes to the environment

Environment Manager

- Stormshield Endpoint Security Servers
- Policies
- Environment
- Log Manager

Monitoring

- Dashboard

Policies - Environment 1

- Server Configuration
- Dynamic Agent Configuration
- Static Agent Configuration
- Security
- Encryption
- Antivirus
- Script
 - HostBadReputation
 - HostReputationOK

Policies - Environment 1 >> Script >> HostReputationOK

Check Out Export

Policy Links

- Script : HostReputationOK, Modified On : 29/03/2017 14:46:10
 - IF AND
 - User-Defined Test : HostCheckResource
 - Result True
 - Execution ~ Script : HostReputationOK:20
 - Result False
 - Configuration ~ Apply Policy : HostBadReputationPolicy
 - Execution ~ Script : HostBadReputation:20

Environment 1

Apply changes to the environment

Environment Manager

- Stormshield Endpoint Security Servers
- Policies
- Environment
- Log Manager

Monitoring

- Dashboard

Policies - Environment 1

- Server Configuration
- Dynamic Agent Configuration
- Static Agent Configuration
- Security
- Encryption
- Antivirus
- Script
 - HostBadReputation

Policies - Environment 1 >> Script >> HostBadReputation

Check Out Export

Policy Links

- Script : HostBadReputation, Modified On : 29/03/2017 14:46:10
 - IF NOT
 - User-Defined Test : HostCheckResource
 - Result True
 - Execution ~ Script : HostBadReputation:20
 - Result False
 - Configuration ~ Review policies
 - Execution ~ Script : HostReputationOK:20



Appliquer la politique de sécurité à des machines du domaine

1. Cliquez sur le menu **Environnement**. Dans l'arborescence de l'annuaire Microsoft Active Directory, sélectionnez les machines ou l'O.U. (Organizational Unit - Unité d'Organisation) contenant les machines sur lesquelles la politique doit être appliquée. Dans l'exemple, il s'agit de l'O.U. "SESComputers".
2. Dans le panneau **Scripts** (onglet **Politiques liées**), sélectionnez le script *HostReputationOK* (liste déroulante **Nom de la Politique**) et affectez lui la condition "*true*" :

Link order	Condition	Policy Name	Inherited from
1	{true}	DefaultDynamicAgentPolicy	Environment 1
1	{true}	DefaultStaticAgentPolicy	Environment 1
1	{true}	DefaultSecurityPolicy	Environment 1
1	{true}	HostReputationOK	

Le script *HostReputationOK* appelant *HostBadReputation* et *HostBadReputationPolicy*, ceux-ci sont implicitement liés et n'ont pas besoin d'être déclarés.

3. Cliquez sur **Appliquer les changements à l'environnement**. Cette action doit être effectuée à chaque modification de la politique de sécurité.
4. Les agents hébergés sur les machines appartenant à l'O.U. "SESComputers" peuvent alors récupérer automatiquement cette nouvelle politique auprès de leur serveur.



Exemple de script Visual Basic

Remplacez l'adresse IP colorée en rouge par l'adresse de la machine cible des requêtes ICMP :

```
Function Ping( myHostName )
    ' This function returns True if the specified host could be
    pinged.
    ' myHostName can be a computer name or IP address.
    ' The Win32_PingStatus class used in this function requires
    Windows XP or later.
    ' This function is based on the TestPing function in a sample
    script by Don Jones
    '
    http://www.scriptinganswers.com/vault/computer%20management/default.as
    p#activedirectoryquickworkstationinventorytxt
    ' Standard housekeeping
    Dim colPingResults, objPingResult, strQuery
    ' Define the WMI query
    strQuery = "SELECT * FROM Win32_PingStatus WHERE Address = '"
    & myHostName & "'"
    ' Run the WMI query
    Set colPingResults = GetObject
    ("winmgmts://./root/cimv2").ExecQuery( strQuery )
    ' Translate the query results to either True or False
    For Each objPingResult In colPingResults
    If Not IsObject( objPingResult ) Then
    Ping = False
    ElseIf objPingResult.StatusCode = 0 Then
    Ping = True
    Else
    Ping = False
    End If
    Next
    Set colPingResults = Nothing
    End Function
    If Ping("192.168.56.10") Then
    Wscript.echo "yes"
    Wscript.quit(1)
    Else
    Wscript.echo "no"
    wscript.quit(0)
    End If
```



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2019. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.