Téléchargements, mises à jour ou mises à jour d'appareils de sécurité du contenu utilisant un hôte statique

Contenu

Introduction

Ce document décrit l'adresse IP et la héberge nécessaire pour configurer votre appliance de sécurité du contenu de Cisco pour l'usage avec un hôte statique pour des téléchargements, des mises à jour, et des mises à jour. Ces configurations doivent être utilisées pour le matériel ou l'appliance virtuelle de sécurité du courrier électronique de Cisco (ESA), l'appliance de sécurité Web (WSA), ou l'appliance de Gestion de la sécurité (SMA).

Téléchargements, mises à jour ou mises à jour d'appareils de sécurité du contenu utilisant un hôte statique

Cisco offre les hôtes statiques pour les clients qui ont des conditions requises strictes de Pare-feu ou de proxy. Il est important de noter que si vous configurez votre appliance pour utiliser les hôtes statiques pour des téléchargements et des mises à jour, les mêmes hôtes de charge statique pour des téléchargements et on doit permettre aussi bien des mises à jour dans le Pare-feu et le proxy sur le réseau.

Voici les noms d'hôte, les adresses IP, et les ports statiques qui sont impliqués dans le téléchargement, la mise à jour, et les processus de mise à niveau :

- downloads-static.ironport.com 208.90.58.105 (port 80)
- updates-static.ironport.com 208.90.58.25 (port 80)184.94.240.106 (port 80)

Entretenez la configuration de mise à jour par l'intermédiaire du

GUI

Terminez-vous ces étapes afin de changer le téléchargement, la mise à jour, ou la configuration de mise à jour sur AsyncOS du GUI :

1. Naviguez vers la page de configuration de configurations de mise à jour WSA : **Configurations d'administration système > de mise à jour et de mise à jour**ESA : **Services de sécurité > mises à jour de service**SMA : **Configurations d'administration système > de mise à jour**
2. Cliquez sur Edit les **configurations de mise à jour….**
3. Dans les *serveurs de mise à jour (images)* sectionnez, « les serveurs locaux choisis de mise à jour (emplacement des fichiers d'image de mise à jour) ».
4. Pour le *champ URL de base*, entrez dans http://downloads-static.ironport.com et pour le champ de *port*, positionnement pour le port **80**.
5. Quittez les champs *(facultatifs) d'authentification* vides.
6. (*) ESA seulement - Pour l'*hôte (les définitions d'antivirus de McAfee, les mises à jour d'engine PXE, les définitions d'antivirus de Sophos, les règles d'anti-Spam d'IronPort, les règles de filtres d'épidémie, les mises à jour DLP, les règles du fuseau horaire et le client d'inscription (utilisés pour chercher des Certificats pour le Filtrage URL)* mettent en place, entrent dans **updates-static.ironport.com**. (Le port 80 est facultatif.)
7. Laissez les *serveurs de mise à jour (liste)* sectionner et mettez en place tout réglé aux serveurs par défaut de mise à jour d'IronPort Cisco.
8. Assurez-vous que vous avez l'interface sélectionnée comme nécessaire pour la transmission externe, s'il y a lieu pour communiquer au-dessus d'une interface spécifique. La configuration par défaut sera placée à l'**automatique choisie**.
9. Vérifiez et mettez à jour les serveurs proxys configurés, s'il y a lieu.
10. Cliquez sur **Submit**.
11. Dans le coin supérieur droit, **modifications de validation de** clic.
12. En conclusion, cliquez sur en fonction les **modifications de validation** de nouveau afin de confirmer toutes les modifications de configuration.

Poursuivez à la section de vérification de ce document.

Configuration d'updateconfig par l'intermédiaire du CLI

Les mêmes modifications peuvent être appliquées par l'intermédiaire du CLI sur l'appliance. Terminez-vous ces étapes afin de changer le téléchargement, la mise à jour, ou la configuration de mise à jour sur AsyncOS du CLI :

1. Exécutez l'**updateconfig de** commande CLI.
2. Entrez dans l'**INSTALLATION de** commande.
3. La première section présentée pour configurer est « touche de fonction met à jour ». Utilisation « **2. L'utilisez pour posséder le serveur** » et pour entrer dans http://downloads-static.ironport.com:80/.
4. (*) ESA seulement - La deuxième section présentée pour configurer est « service (images) ». Utilisation « **2. L'utilisez pour posséder le serveur** » et pour entrer dans **updates-static.ironport.com**.
5. Toutes autres demandes de configuration peuvent rester réglé pour se transférer.

6. Assurez-vous que vous avez l'interface sélectionnée comme nécessaire pour la transmission externe, s'il y a lieu pour communiquer au-dessus d'une interface spécifique. La configuration par défaut sera placée à l'**automatique**.
7. Vérifiez et mettez à jour le serveur proxy configuré, s'il y a lieu.
8. Retour de hit à retourner à la demande principale CLI.
9. Exécutez la **VALIDATION de** commande CLI pour sauvegarder toutes les modifications de configuration.

Poursuivez à la section de vérification de ce document.

Vérification

Mises à jour

Pour la vérification des mises à jour sur l'appliance il est le meilleur de valider du CLI.

Du CLI :

1. Exécutez l'**updatenow**. (*) ESA seulement - vous pouvez exécuter la **force d'updatenow** pour avoir tous les services et mise à jour d'ensembles de règles.
2. Exécutez les **updater_logs de queue**.

Vous voudrez prêter la grande attention aux lignes suivantes « http://updates-static.ironport.com/.. » Ceci devrait signaler la transmission et le téléchargement avec le serveur statique d'updater.

Exemple, d'un ESA mettant à jour l'engine de courrier indésirable de Cisco (CAS) et des règles associées :

```
Wed Aug 2 09:22:05 2017 Info: case was signalled to start a new update
Wed Aug 2 09:22:05 2017 Info: case processing files from the server manifest
Wed Aug 2 09:22:05 2017 Info: case started downloading files
Wed Aug 2 09:22:05 2017 Info: case waiting on download lock
Wed Aug 2 09:22:05 2017 Info: case acquired download lock
Wed Aug 2 09:22:05 2017 Info: case beginning download of remote file "http://updates-
static.ironport.com/case/2.0/case/default/1480513074538790"
Wed Aug 2 09:22:07 2017 Info: case released download lock
Wed Aug 2 09:22:07 2017 Info: case successfully downloaded file
"case/2.0/case/default/1480513074538790"
Wed Aug 2 09:22:07 2017 Info: case waiting on download lock
Wed Aug 2 09:22:07 2017 Info: case acquired download lock
Wed Aug 2 09:22:07 2017 Info: case beginning download of remote file "http://updates-
static.ironport.com/case/2.0/case_rules/default/1501673364679194"
Wed Aug 2 09:22:10 2017 Info: case released download lock
<<<SNIP FOR BREVITY>>>
```

Tant que le service communique, des téléchargements, et puis avec succès des mises à jour, vous êtes placé.

Une fois que la mise à jour de service est terminée, les updater_logs afficheront :

```
Wed Aug 2 09:22:50 2017 Info: case started applying files
Wed Aug 2 09:23:04 2017 Info: case cleaning up base dir [bindir]
Wed Aug 2 09:23:04 2017 Info: case verifying applied files
Wed Aug 2 09:23:04 2017 Info: case updating the client manifest
Wed Aug 2 09:23:04 2017 Info: case update completed
Wed Aug 2 09:23:04 2017 Info: case waiting for new updates
```

Mises à jour

Afin de vérifier que la transmission de mise à jour est réussie et se termine, naviguez vers la page de **mise à jour de système** et cliquez sur les **mises à jour disponibles**. Si la liste d'affichages disponibles de versions, alors votre installation est complète.

Du CLI, vous pouvez simplement exécuter la commande de **mise à jour**. Choisissez l'option de **téléchargement** de visualiser la mise à jour manifeste, s'il y a des mises à jour disponibles.

```
myesa.local> upgrade


Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
[]> download

Upgrades available.
1. AsyncOS 9.6.0 build 051 upgrade For Email, 2015-09-02 this release is for General Deployment
2. AsyncOS 9.7.0 build 125 upgrade For Email, 2015-10-15. This release is for General Deployment
3. AsyncOS 9.7.1 build 066 upgrade For Email, 2016-02-16. This release is for General
Deployment.
4. cisco-sa-20150625-ironport SSH Keys Vulnerability Fix
[4]>
```

Dépannage

Mises à jour

L'appliance envoie des alertes de notification quand les mises à jour échouent. Voici un exemple de la notification électronique le plus généralement reçue :

```
The updater has been unable to communicate with the update server for at least 1h.

Last message occurred 4 times between Tue Mar 1 18:02:01 2016 and Tue Mar 1 18:32:03 2016.

Version: 9.7.1-066
Serial Number: 888869DFCCCC-3##CV##
Timestamp: 01 Mar 2016 18:52:01 -0500
```

Vous voudrez tester la transmission de l'appliance au serveur spécifié d'updater. Dans ce cas, nous sommes concernés par downloads-static.ironport.com. Utilisant le telnet, l'appliance devrait avoir la transmission ouverte au-dessus du port 80 :

```
myesa.local> telnet downloads-static.ironport.com 80

Trying 208.90.58.105...
Connected to downloads-static.ironport.com.
Escape character is '^]'.
```

De même, les mêmes devraient être vus pour updates-static.ironport.com :

```
> telnet updates-static.ironport.com 80

Trying 208.90.58.25...
Connected to origin-updates.ironport.com.
Escape character is '^]'.
```

Si votre appliance a des plusieurs interfaces, vous pouvez souhaiter exécuter le **telnet du** CLI, et spécifiez l'interface, afin de valider que l'interface appropriée est sélectionnée :

```
> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (172.18.249.120/24: myesa.local)
[1]>

Enter the remote hostname or IP address.
[]> downloads-static.ironport.com

Enter the remote port.
[25]> 80

Trying 208.90.58.105...
Connected to downloads-static.ironport.com.
Escape character is '^]'.
```

Mises à jour

En essayant d'améliorer, vous pouvez voir la réponse suivante :

```
No available upgrades. If the image has already been downloaded it has been de-provisioned from
the upgrade server. Delete the downloaded image, if any and run upgrade.
```

Vous voudrez passer en revue la version d'AsyncOS qui s'exécute sur l'appliance et examiner également les notes de mise à jour de la version d'AsyncOS à la laquelle vous améliorez. Il est possible qu'il n'y ait pas un chemin de mise à niveau de la version que vous exécutez à la version vous essayez d'améliorer à.

Si vous améliorez à un correctif chaud (HP), à Early Deployment (ED), ou à la version d'AsyncOS du déploiement limité (LD), vous pouvez devoir ouvrir une valise de support afin de demander le ravitaillement approprié est terminé, pour que votre appliance voie le chemin de mise à niveau comme nécessaire.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Notes de mise à jour
- Appliance de sécurité Web de Cisco - Notes de mise à jour
- Appliance de Gestion de sécurité Cisco - Notes de mise à jour
- Support et documentation techniques - Cisco Systems