Contenu

Introduction

Ce document décrit comment améliorer ou mettre à jour votre appliance de sécurité du contenu de Cisco avec l'utilisation d'un serveur statique.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité du courrier électronique de Cisco (ESA)
- Appliance de sécurité Web de Cisco (WSA)
- Appliance de Gestion de sécurité Cisco (SMA)
- AsyncOS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Toutes les versions d'AsyncOS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Améliorez ou mettez à jour l'appliance

Cisco offre les serveurs statiques pour les sites qui ont des conditions requises strictes de Pare-feu. Il est important de noter que si vous configurez les configurations de mise à jour et de mise à jour sur votre appliance avec l'utilisation cette méthode statique, toutes les informations est aussi

bien nécessaire dans les Pare-feu.

Voici les adresses Internet, les adresses IP, et les ports qui sont impliqués dans le processus de mise à jour et de mise à jour :

- **downloads-static.ironport.com** : 208.90.58.105 sur le port 80
- **update-manifests.ironport.com** : 208.90.58.5 sur le port 443
- **updates-static.ironport.com** : 208.90.58.25 sur le port 80

Terminez-vous ces étapes afin de changer les configurations de mise à jour et de mise à jour sur l'AsyncOS :

1. Naviguez vers l'onglet de **mises à jour de service de la** page de Services de sécurité.
2. Cliquez sur Edit les **configurations de mise à jour….**
3. **Les serveurs locaux** choisis de **mise à jour des** serveurs de mise à jour (images) mettent en place.
4. Entrez dans **http://downloads-static.ironport.com** dans le domaine URL de base (tous les services excepté des définitions d'antivirus de McAfee et des mises à jour d'IronPort AsyncOS) et placez le port à **80**. Laissez le champ vide de configurations d'authentification.
5. Entrez dans **updates-static.ironport.com** dans le domaine d'hôte (définitions d'antivirus de McAfee, mises à jour d'engine PXE, mises à jour d'IronPort AsyncOS).
6. Assurez-vous que le gisement de serveurs de mise à jour (liste) est placé aux **serveurs de mise à jour d'IronPort**.
7. Mettez à jour les configurations de **serveurs proxys** s'il y a lieu.
8. Cliquez sur **Submit**.
9. **Modifications de validation de** clic.
10. **Modifications de validation de** clic de nouveau afin de confirmer.

Vérifiez les mises à jour et les mises à jour

Afin de vérifier que les mises à jour sont complètes, naviguent vers la page de **mise à jour de système** et cliquent sur des **mises à jour disponibles**. Si la liste d'affichages disponibles de versions, alors votre installation est complète.

Afin de vérifier que les mises à jour fonctionnent correctement, sélectionnent la commande de **queue** dans le CLI et visualisent les updater_logs pour des erreurs.

- Pour des mises à jour de Sophos, surveillez les updater_logs pour des **sophos**, ou surveillez le log d'antivirus :
- Pour des mises à jour de McAfee, surveillez les updater_logs pour le **mcafee**,
- Pour les mises à jour de CAS qui sont utilisées par IPAS et VOF, surveillez les updater_logs pour le **cas :**

L'appliance enverra des alertes de notification quand les mises à jour échouent. Voici un exemple du le plus généralement reçu :