Secure Client (services client sécurisés) Analyse de l'hôte

Le module de posture AnyConnect Secure Client (services client sécurisés) permet d'identifier le système d'exploitation, l'anti-programme malveillant et le logiciel de pare-feu installés sur l'hôte. L'application HostScan recueille ces informations. L'évaluation de la posture nécessite l'installation de HostScan sur l'hôte.

Préalables pour la posture HostScan/Secure Firewall

L'Secure Client (services client sécurisés) avec le module Secure Firewall Posture/HostScan nécessite au minimum les composants ASA suivants :

- ASA 8.4
- ASDM 6.4

Vous devez installer Secure Firewall Posture/HostScan pour utiliser la fonction d'authentification SCEP.

Reportez-vous à Plateformes VPN prises en charge, série Cisco ASA pour connaître les systèmes d'exploitation pris en charge pour l'installation de Secure Firewall Posture/HostScan.

Licences pour HostScan

Voici les exigences de licence Secure Client (services client sécurisés) pour HostScan :

- AnyConnect Apex

- AnyConnect VPN seulement

Progiciel HostScan

Vous pouvez charger le package HostScan sur l'ASA en tant que package autonome : **hostscan-version.pkg**. Ce fichier contient le logiciel HostScan ainsi que la bibliothèque et les tableaux d'assistance de HostScan.

Installer ou mettre à niveau HostScan/Secure Firewall Posture

Utilisez cette procédure pour installer ou mettre à niveau le progiciel HostScan ou Secure Firewall Posture et l'activer à l'aide de l'interface de ligne de commande de l'ASA.

Avant de commencer

Remarque Si vous tentez d'effectuer une mise à niveau vers HostScan version 4.6.x ou ultérieure à partir d'une version 4.3.x ou d'une version antérieure, vous recevrez un message d'erreur en raison du fait que toutes les politiques DAP existantes d'AV/AS/FW et les scripts LUA que vous avez établis précédemment sont incompatibles avec HostScan 4.6.x ou version ultérieure.

Il existe une procédure de migration unique qui doit être effectuée pour adapter votre configuration. Cette procédure implique de quitter cette boîte de dialogue afin de migrer votre configuration pour qu'elle soit compatible avec HostScan 4.4.x avant d'enregistrer cette configuration. Abandonnez cette procédure et consultez le Secure Client (services client sécurisés) guide de migration HostScan de la version 4.3.x à la version 4.6.x pour obtenir des instructions détaillées. En résumé, la migration implique la navigation vers la page de politique DAP d'ASDM pour passer en revue et supprimer manuellement les attributs incompatibles d'AV/AS/FW, puis de passer en revue et de réécrire les scripts LUA.

- Au niveau de l'interface de ligne de commande de l'ASA, entrez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : hostname(config)#
- Chargez le fichier secure-firewall-posture-*version*-k9.pkg sur l'ASA. Si vous utilisez la version HostScan 4.x, vous devez charger le fichier hostscan_*version*-k9.pkg.

Procédure

Étape 1 Entrez en mode de configuration webvpn.

Exemple :

```
hostname(config)# webvpn
```

Étape 2 Ouvrez ASDM et choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Posture (for Secure Firewall) (Posture [pour Secure Firewall]) > Posture Image (Image Posture)**. Si vous utilisez la version HostScan 4.x, le chemin d'accès sera **Configuration > Remote Access VPN (VPN d'accès à distance) > Secure Desktop Manager (Gestionnaire Secure Desktop) > HostScan Image (Image HostScan)**.

Étape 3 Précisez le chemin d'accès au paquet que vous souhaitez désigner comme image HostScan/Secure Firewall Posture. Vous pouvez préciser un progiciel autonome ou le progiciel Secure Client (services client sécurisés).

hostscan image *path*

Exemple :

Si vous utilisez la version HostScan 4.x,

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081.pkg
```

Si vous utilisez la version Secure Firewall Posture 5.x,

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture5.0.00556.pkg
```

Étape 4 Activez l'image HostScan/Secure Firewall Posture que vous avez désignée à l'étape précédente.

Exemple :

```
ASAName(webvpn)#hostscan enable
```

Étape 5 Enregistrez la configuration en cours d'exécution dans la mémoire flash. Après avoir enregistré avec succès la nouvelle configuration dans la mémoire flash, vous recevez le message [OK].

Exemple :

```
hostname(webvpn)# write memory
```

Étape 6

Activer ou désactiver HostScan

Ces commandes activent ou désactivent une image HostScan installée à l'aide de l'interface de ligne de commande de l'ASA.

Avant de commencer

Au niveau de l'interface de ligne de commande de l'ASA, entrez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : hostname(config)#

Procédure

Étape 1 Entrez en mode de configuration webvpn.

Exemple :

webvpn

Étape 2 Activez l'image autonome HostScan si elle n'a pas été désinstallée de l'ASA.

hostscan enable

Étape 3 Désactivez HostScan pour tous les progiciels HostScan installés.

Remarque
Avant de désinstaller l'image HostScan activée, vous devez d'abord désactiver HostScan à l'aide de cette commande.

no hostscan enable

Afficher la version de HostScan/Secure Firewall Posture activée sur l'ASA

Utilisez cette procédure pour déterminer la version de HostScan/Secure Firewall Posture activée à l'aide de l'interface de ligne de commande de l'ASA.

Avant de commencer

Connectez-vous à l'ASA et passez en mode d'exécution privilégié. En mode d'exécution privilégié, l'ASA affiche cette invite : hostname#

Procédure

Affichez la version de HostScan/Secure Firewall Posture activée sur l'ASA.

show webvpn hostscan

Désinstaller HostScan/Secure Firewall Posture

La désinstallation du package HostScan/Secure Firewall Posture le retire de l'affichage dans l'interface ASDM et empêche l'ASA de le déployer, même lorsqu'il est activé. La désinstallation de HostScan/Secure Firewall Posture ne supprime pas le paquet de la mémoire flash.

Avant de commencer

Connectez-vous à l'ASA et passez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : hostname(config)#

Procédure

Étape 1 Entrez en mode de configuration webvpn.

webvpn

Étape 2 Désactivez l'image HostScan/Secure Firewall Posture que vous souhaitez désinstaller.

no hostscanenable

Étape 3 Précisez le chemin d'accès à l'image HostScan/Secure Firewall Posture que vous souhaitez désinstaller. Un progiciel autonome peut avoir été désigné comme progiciel HostScan/Secure Firewall Posture.

no hostscan image *path*

Exemple :

Si vous utilisez la version HostScan 4.x,

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081-k9.pkg
```

Si vous utilisez la version 5.x de Secure Firewall Posture,

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture-5.0.00556-k9.pkg
```

Étape 4 Enregistrez la configuration en cours dans la mémoire flash. Après l'enregistrement réussi de la nouvelle configuration dans la mémoire flash, le message [OK] s'affiche.

write memory

Attribuer des modules de fonctionnalité Secure Client (services client sécurisés) aux stratégies de groupe

Cette procédure associe les modules de fonctionnalité Secure Client (services client sécurisés) à une stratégie de groupe. Lorsque les utilisateurs VPN se connectent à l'ASA, l'ASA télécharge et installe ces modules de fonctionnalité Secure Client (services client sécurisés) sur leur ordinateur terminal.

Avant de commencer

Au niveau de l'interface de ligne de commande de l'ASA, entrez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : hostname(config)#

Procédure

Étape 1 Ajoute une stratégie de groupe interne pour Network Client Access (Accès client réseau)

group-policy *name* **internal**

Exemple :

```
hostname(config)# group-policy PostureModuleGroup internal
```

Étape 2 Modifiez la nouvelle stratégie de groupe. Après avoir saisi la commande, vous recevez une invite pour le mode de configuration de la stratégie de groupe, hostname(config-group-policy)#.

group-policy *name* **attributes**

Exemple :

```
hostname(config)# group-policy PostureModuleGroup attributes
```

Étape 3 Entrez le mode de configuration webvpn de stratégie de groupe. Après avoir saisi la commande, l'ASA renvoie cette invite : hostname(config-group-webvpn)#

webvpn

Étape 4 Configurez la stratégie de groupe pour télécharger les modules de fonctionnalité Secure Client (services client sécurisés) pour tous les utilisateurs du groupe.

AnyConnect modules value *Secure Firewall Module Name*

La valeur de la commande AnyConnect modules peut contenir une ou plusieurs des valeurs suivantes : Lorsque vous spécifiez plusieurs modules, séparez les valeurs par une virgule :

valeur	Secure Firewall Module/Feature Name
dart	Secure Client DART (Diagnostics and Reporting Tool)
vpngina	Secure Client SBL (Start Before Logon)
posture	Secure Firewall Posture/HostScan
nam	Secure Client Network Access Manager
none	Utilisé seul, supprime tous les modules AnyConnect de la stratégie de groupe.
profileMgmt	Secure Client Management Tunnel VPN

Exemple :

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

Pour supprimer l'un des modules, envoyez de nouveau la commande en précisant uniquement les valeurs du module que vous souhaitez conserver. Par exemple, cette commande supprime le module websecurity :

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

Étape 5 Enregistrez la configuration en cours d'exécution dans la mémoire flash.

Après avoir enregistré avec succès la nouvelle configuration dans la mémoire flash, vous recevez le message [OK], puis l'ASA vous renvoie à l'invite hostname(config-group-webvpn)#.

write memory

Documentation associée à HostScan/Secure Firewall Posture

Une fois que HostScan/Secure Firewall Posture a collecté les informations de posture sur l'ordinateur terminal, vous devrez comprendre des sujets tels que la configuration des politiques d'accès dynamique et l'utilisation d'expressions LUA pour exploiter ces informations.

Ces sujets sont traités en détail dans les documents suivants : Guides de configuration de Cisco Adaptive Security Device Manager. Consultez également le *guide d'administration de Cisco Secure Client (y compris*

AnyConnect) de Cisco pour obtenir plus d'informations sur le fonctionnement de HostScan/Secure Firewall Posture avec Secure Client (services client sécurisés).

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.