Mise à niveau de HostScan vers une position de pare-feu sécurisée sous Windows

Table des matières

Introduction

Ce document décrit la procédure de mise à niveau de HostScan vers Secure Firewall Posture (anciennement HostScan) sous Windows.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- Configuration de Cisco Anyconnect et Hostscan

Composants utilisés

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

- Appareil virtuel de sécurité adaptatif Cisco 9.18 (4)
- Cisco Adaptive Security Device Manager 7.20 (1)
- Client de mobilité sécurisée Cisco AnyConnect4.10.07073
- AnyConnect HostScan 4.10.07073
- Cisco Secure Client 5.1.2.42
- Posture du pare-feu sécurisé 5.1.2.42

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.

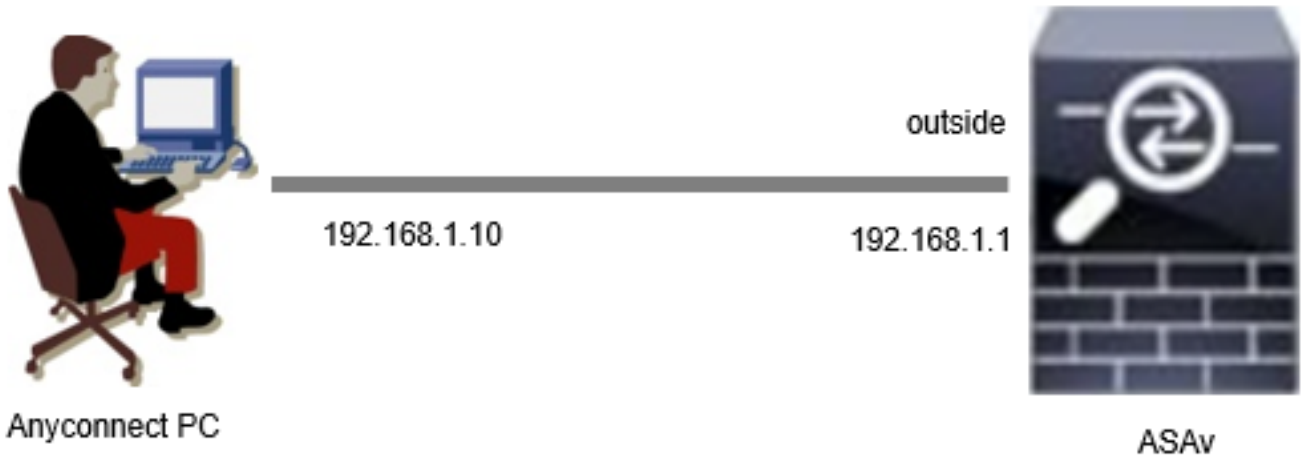


Diagramme du réseau

Configurations

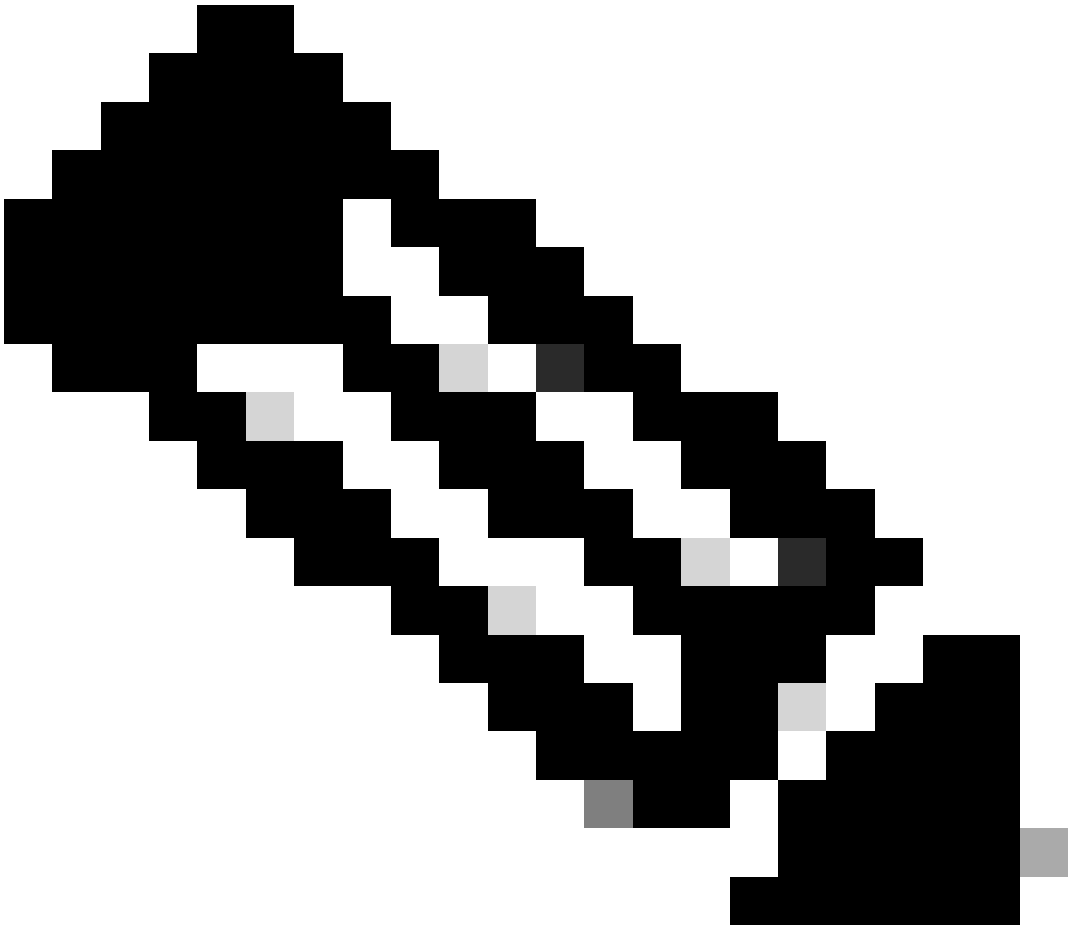
Il s'agit de la configuration minimale de l'interface CLI ASA.

```
tunnel-group dap_test_tg type remote-access
tunnel-group dap_test_tg general-attributes
default-group-policy dap_test_gp
tunnel-group dap_test_tg webvpn-attributes
group-alias dap_test enable

group-policy dap_test_gp internal
group-policy dap_test_gp attributes
vpn-tunnel-protocol ssl-client
address-pools value ac_pool
webvpn
anyconnect keep-installer installed
always-on-vpn profile-setting

ip local pool ac_pool 172.16.1.11-172.16.1.20 mask 255.255.255.0
```

```
webvpn
enable outside
hostscan image disk0:/hostscan_4.10.07073-k9.pkg
hostscan enable
anyconnect image disk0:/anyconnect-win-4.10.07073-webdeploy-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

Mise à niveau

Ce document fournit un exemple de mise à niveau d'AnyConnect HostScan version 4.10.07073 vers la version 5.1.2.42 de Secure Firewall Posture, en conjonction avec la mise à niveau de Cisco Secure Client (anciennement Cisco AnyConnect Secure Mobility Client).



> Remarque : Cisco recommande d'exécuter la version la plus récente de Secure Firewall Posture (identique à la version de Cisco Secure Client).

Méthode 1. Déploiement côté ASA

Étape 1. Télécharger le fichier image

Téléchargez les fichiers image pour Cisco Secure Client et Secure Firewall Posture à partir du téléchargement du logiciel.

- Cisco Secure Client : cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
- Secure Firewall Posture : secure-firewall-posture-5.1.2.42-k9.pkg

Étape 2. Transfert du fichier image vers ASA Flash

Dans cet exemple, utilisez l'interface de ligne de commande ASA pour transférer les fichiers image d'un serveur HTTP vers la mémoire flash ASA.

```
copy http://1.x.x.x/cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg flash:/
copy http://1.x.x.x/secure-firewall-posture-5.1.2.42-k9.pkg flash:/

ciscoasa# show flash: | in secure
139 117011512 Mar 26 2024 08:08:56 cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
140 92993311 Mar 26 2024 08:14:16 secure-firewall-posture-5.1.2.42-k9.pkg
```

Étape 3. Spécifier le fichier image de la CLI ASA

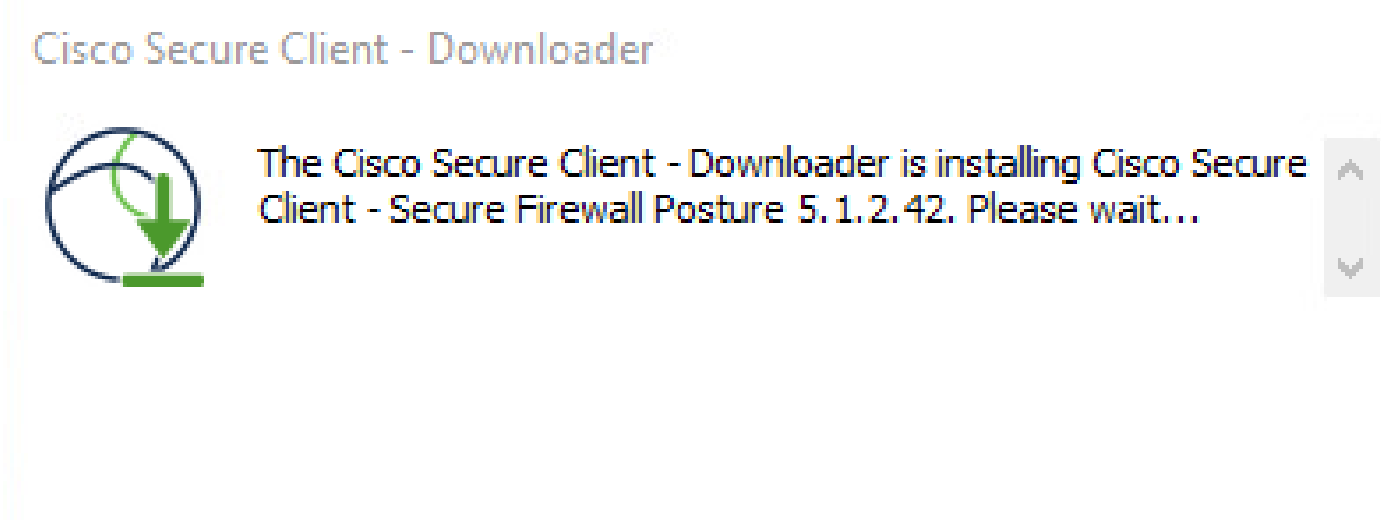
Spécifiez les nouveaux fichiers image utilisés pour la connexion Cisco Secure Client sur l'interface de ligne de commande ASA.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# hostscan image disk0:/secure-firewall-posture-5.1.2.42-k9.pkg
ciscoasa(config-webvpn)# anyconnect image disk0:/cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
```

Étape 4. Mise à niveau automatique

Cisco Secure Client et Secure Firewall Posture peuvent être mis à jour automatiquement lors de la prochaine connexion du client.

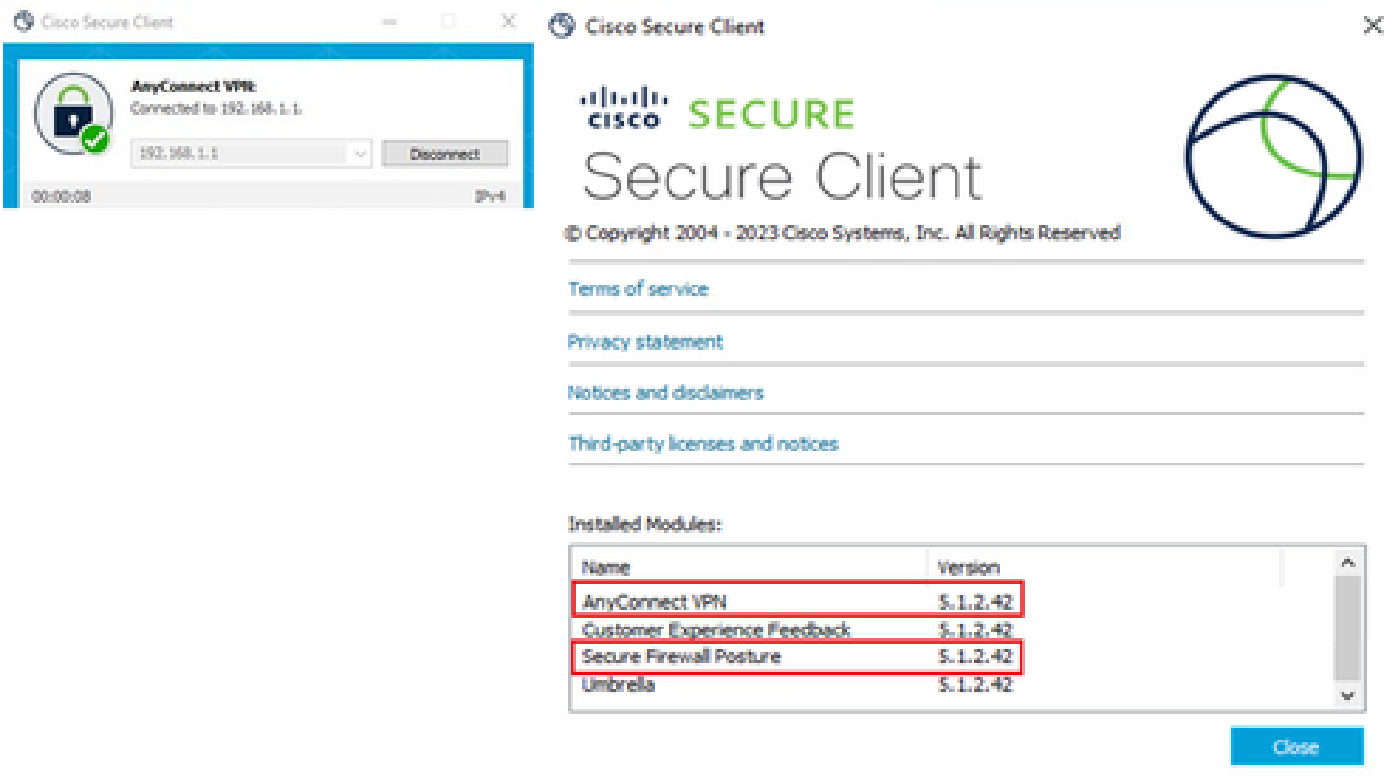
Le module Secure Firewall Posture est automatiquement mis à niveau comme indiqué dans l'image.



Mise à niveau automatique

Étape 5. Confirmer la nouvelle version

Vérifiez que Cisco Secure Client et Secure Firewall Posture ont bien été mis à niveau comme indiqué dans l'image.



Nouvelle version

Méthode 2. Installation côté client

Étape 1. Télécharger le programme

Téléchargez le programme d'installation à partir de Software Download.

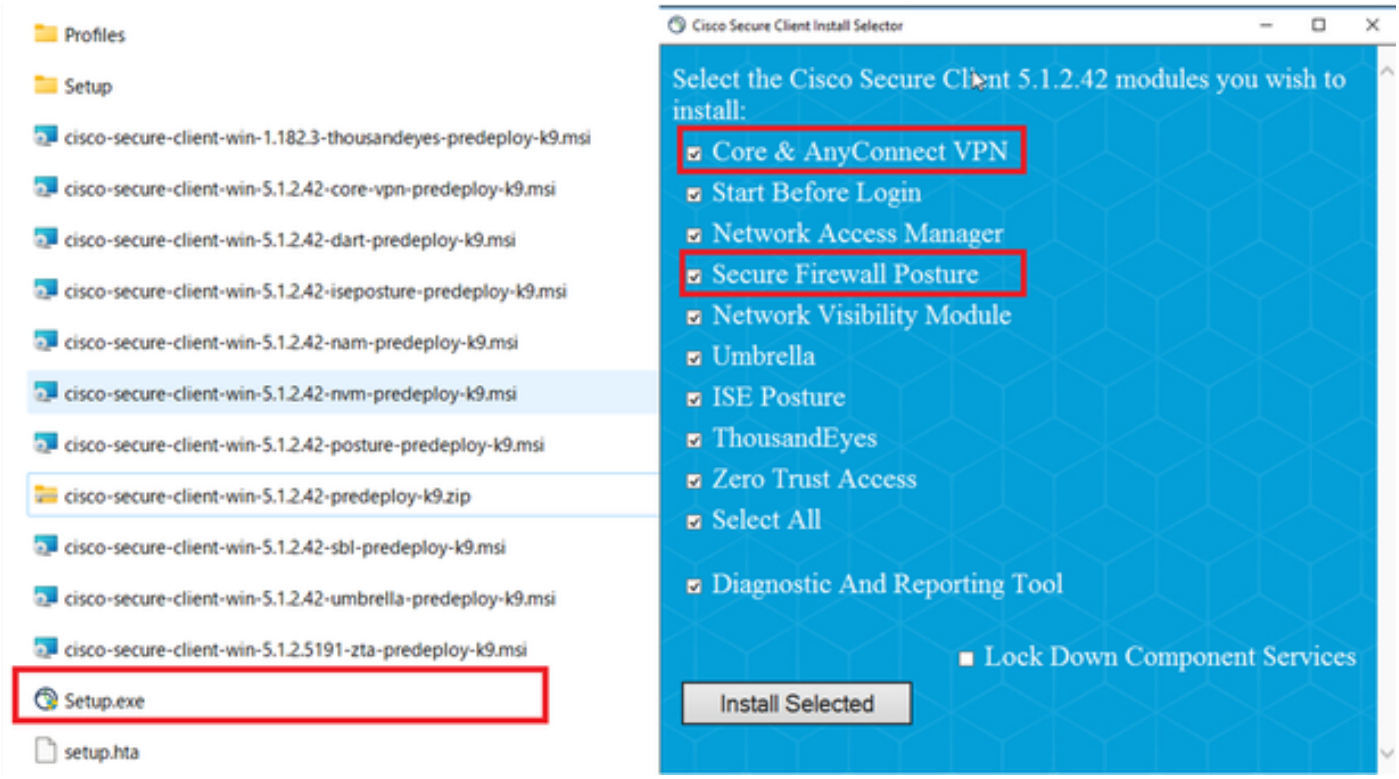
- cisco-secure-client-win-5.1.2.42-predeploy-k9.zip

Étape 2. Transférer le programme d'installation vers le périphérique cible

Transférez le programme d'installation téléchargé vers le périphérique cible à l'aide de méthodes telles que FTP (File Transfer Protocol), un lecteur USB ou d'autres méthodes.

Étape 3. Exécuter le programme

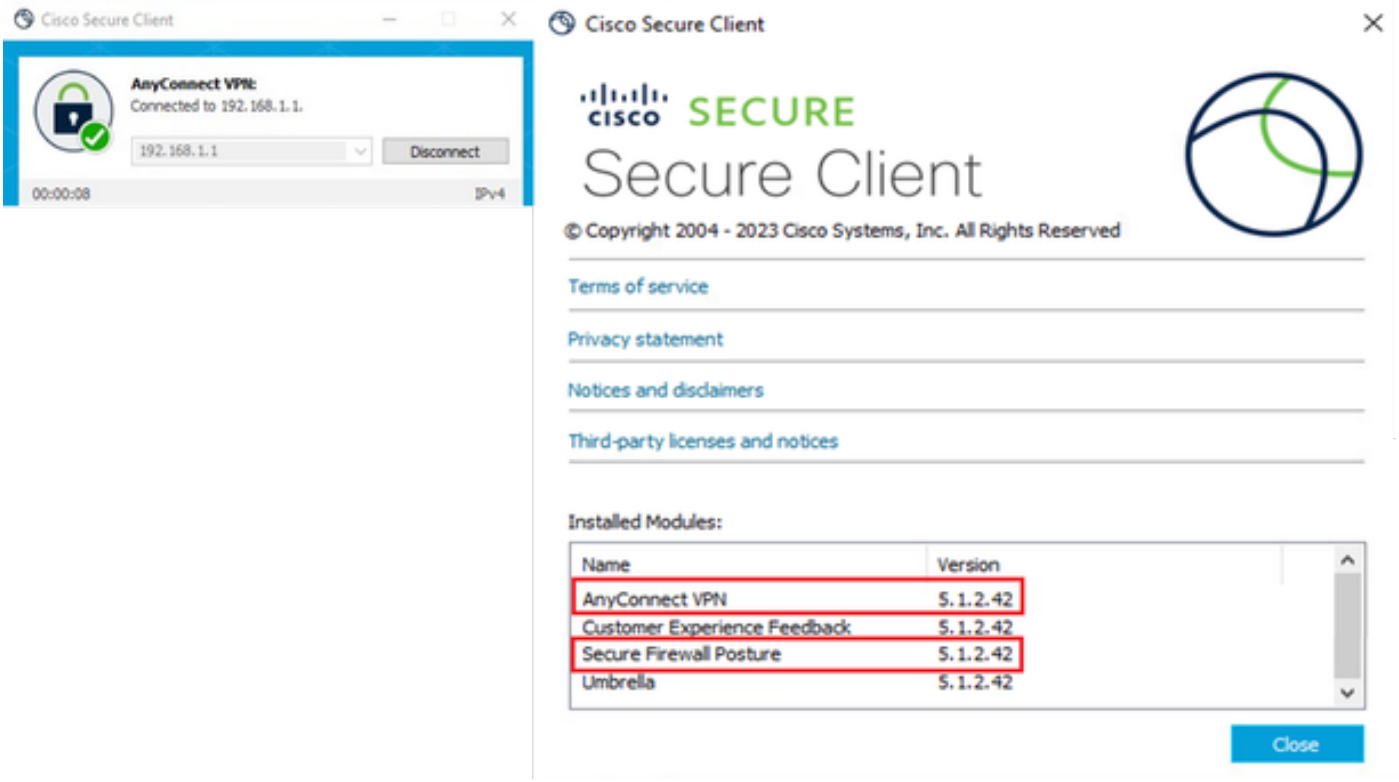
Sur le périphérique cible, extrayez les fichiers compressés et exécutez Setup.exe.



Exécuter le programme

Étape 4. Confirmer la nouvelle version

Vérifiez que Cisco Secure Client et Secure Firewall Posture ont bien été mis à niveau comme indiqué dans l'image.

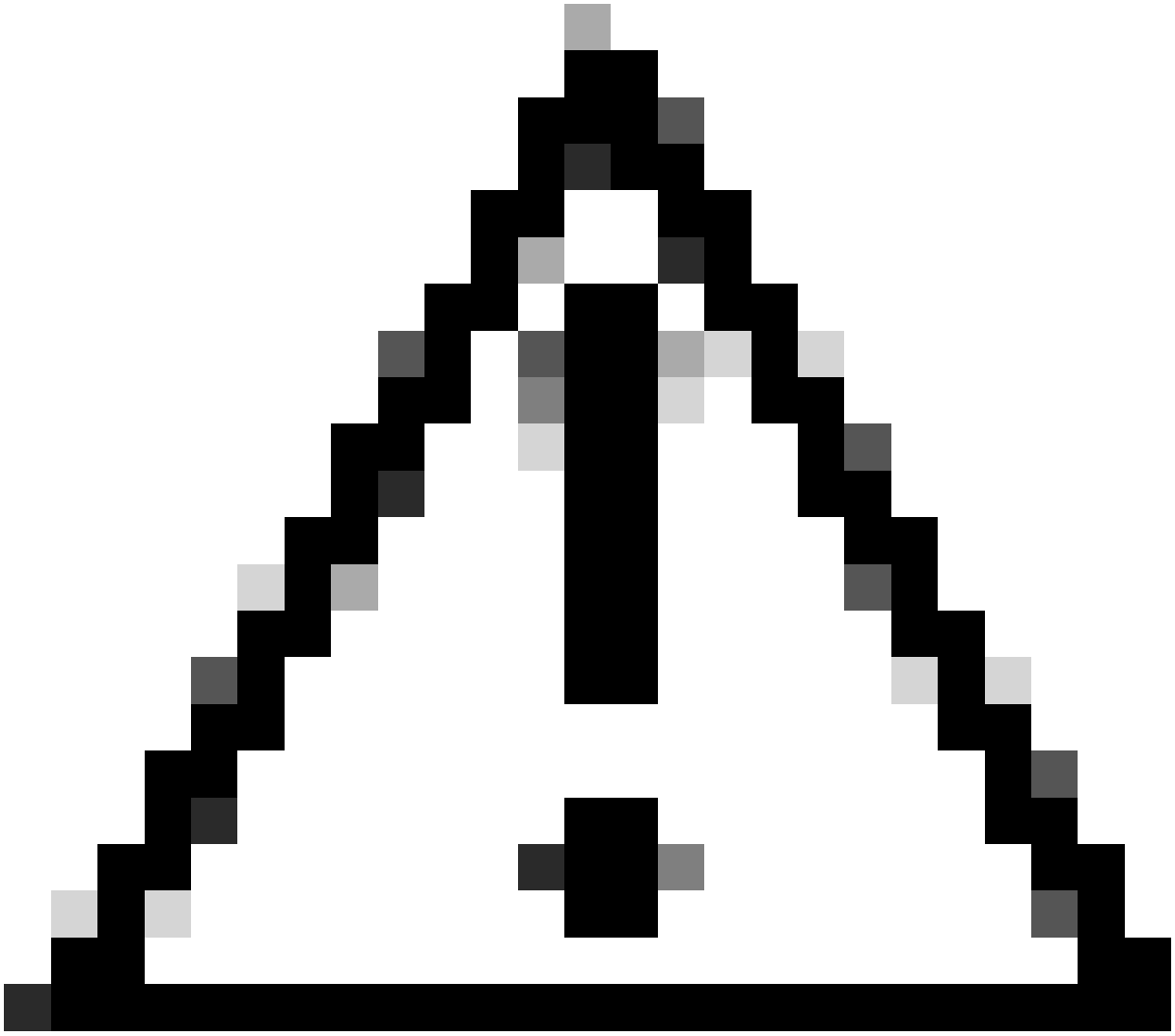


Nouvelle version

Foire aux questions (FAQ)

Q : Si la version de Secure Firewall Posture (anciennement HostScan) spécifiée côté ASA est plus ancienne que la version installée sur le terminal, fonctionne-t-elle toujours correctement ?

R : Oui. Ceci est un exemple de vérification opérationnelle après la mise à niveau de HostScan version 4.10.07073 vers la version 5.1.2.42 de Secure Firewall Posture sur un terminal spécifique, avec DAP (Scénario3). Plusieurs DAP (Action : Continue) sont configurés dans HostScan 4.10.07073.



Attention : le comportement peut dépendre de la version de Secure Firewall Posture/Cisco Secure Client. Veillez donc à consulter les dernières notes de version pour chaque version.

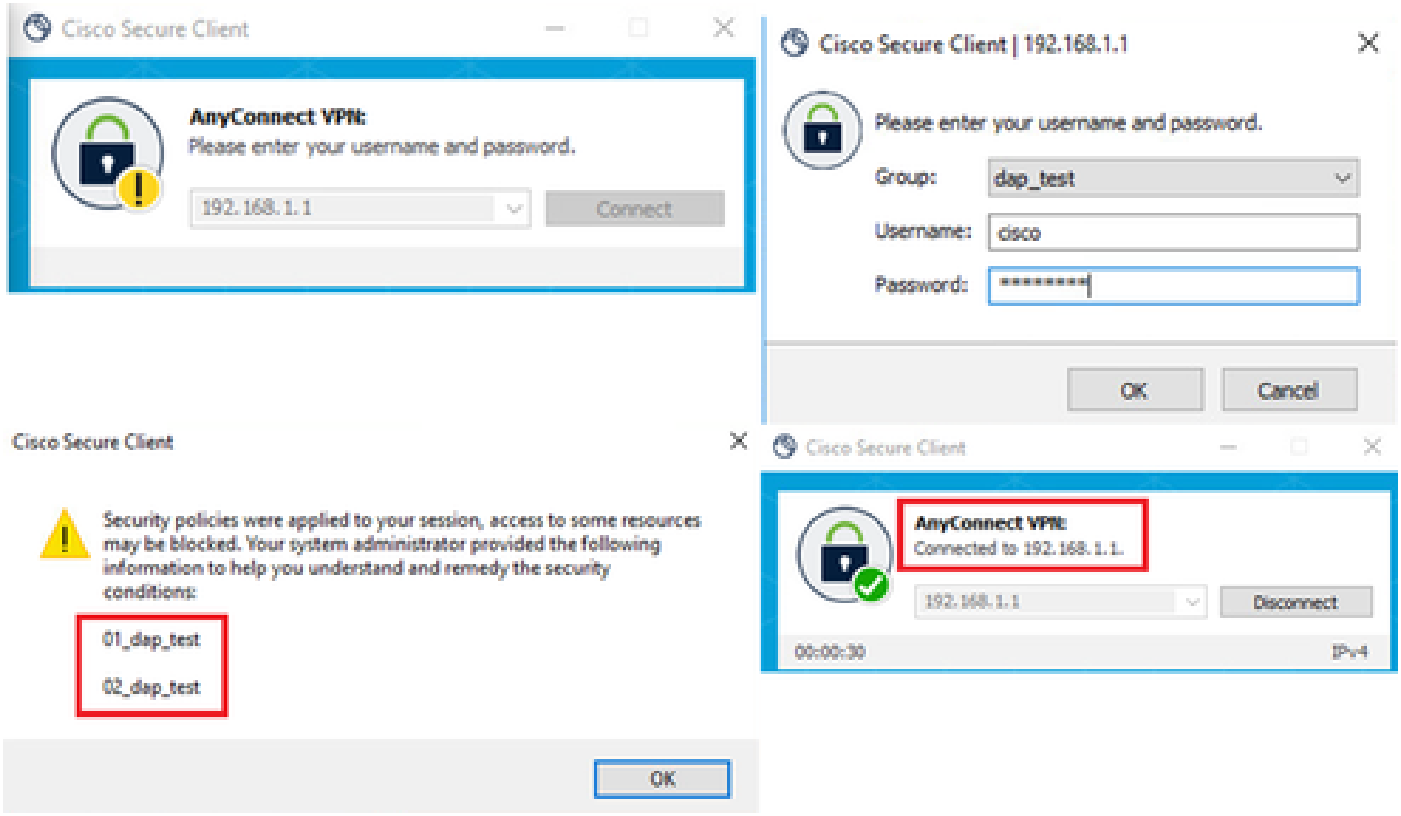
Version de l'image configurée côté ASA :

```
webvpn
hostscan image disk0:/hostscan_4.10.07073-k9.pkg
anyconnect image disk0:/anyconnect-win-4.10.07073-webdeploy-k9.pkg
```

Version de l’image sur l’équipement cible :

Version de l'image sur le périphérique

Exemple de connexion Cisco Secure Client :



Connexion client sécurisée Cisco

Q : Cisco Secure Client 5.x fonctionne-t-il correctement avec HostScan 4.x ?

R : Non. La combinaison de Cisco Secure Client 5.x et HostScan 4.x n'est pas prise en charge.

Q : Lors de la mise à niveau de HostScan 4.x vers Secure Firewall Posture 5.x, est-il possible de mettre à niveau uniquement sur certains périphériques ?

R : Oui. Vous pouvez mettre à niveau des périphériques spécifiques à l'aide de la méthode 2 mentionnée.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.