Actualización de HostScan a estado de firewall seguro en Windows

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Diagrama de la red
<u>Configuraciones</u>
Actualizar
Método 1. Implementación en ASA
Paso 1. Descargar archivo de imagen
Paso 2. Transferir archivo de imagen a la memoria flash ASA
Paso 3. Especificar archivo de imagen desde ASA CLI
Paso 4. Actualizar automáticamente
Paso 5. Confirmar nueva versión
Método 2. Instalación en el lado del cliente
Paso 1. Descargar instalador
Paso 2. Transferir instalador al dispositivo de destino
Paso 3. Ejecutar instalador
Paso 4. Confirmar nueva versión
Preguntas frecuentes
Información Relacionada

Introducción

Este documento describe el procedimiento para actualizar de HostScan a Secure Firewall Posture (anteriormente HostScan) en Windows.

Prerequisites

Requirements

Cisco le recomienda que tenga conocimiento acerca de este tema:

Configuración de Cisco Anyconnect y Hostscan

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad virtual Cisco Adaptive Security Virtual Appliance 9.18 (4)
- Cisco Adaptive Security Device Manager 7.20 (1)
- Cisco AnyConnect Secure Mobility Client 4.10.07073
- AnyConnect HostScan 4.10.07073
- Cisco Secure Client 5.1.2.42
- Condición de firewall seguro 5.1.2.42

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red

Esta imagen muestra la topología utilizada para el ejemplo de este documento.



Diagrama de la red

Configuraciones

Esta es la configuración mínima en ASA CLI.

```
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

Actualizar

Este documento proporciona un ejemplo de cómo actualizar de AnyConnect HostScan versión 4.10.07073 a Secure Firewall Posture versión 5.1.2.42, junto con la actualización de Cisco Secure Client (anteriormente Cisco AnyConnect Secure Mobility Client).



Nota: Cisco recomienda ejecutar la versión más reciente de Secure Firewall Posture (que es la misma que la versión de Cisco Secure Client).

Método 1. Implementación en ASA

Paso 1. Descargar archivo de imagen

Descargue los archivos de imagen para Cisco Secure Client y Secure Firewall Posture desde Descarga de Software.

- Cisco Secure Client: cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
- Estado de firewall seguro: secure-firewall-posture-5.1.2.42-k9.pkg

Paso 2. Transferir archivo de imagen a la memoria flash ASA

En este ejemplo, utilice ASA CLI para transferir los archivos de imagen de un servidor HTTP a la memoria flash ASA.

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

Paso 3. Especificar archivo de imagen desde ASA CLI

Especifique los nuevos archivos de imagen utilizados para la conexión de Cisco Secure Client en ASA CLI.

```
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
```

Paso 4. Actualizar automáticamente

Tanto Cisco Secure Client como Secure Firewall Posture se pueden actualizar automáticamente la próxima vez que el cliente se conecte.

El módulo de estado de firewall seguro se actualiza automáticamente tal y como se muestra en la imagen.

Cisco Secure Client - Downloader



The Cisco Secure Client - Downloader is installing Cisco Secure Client - Secure Firewall Posture 5.1.2.42. Please wait...

Actualizar automáticamente

Paso 5. Confirmar nueva versión

Confirme que Cisco Secure Client y Secure Firewall Posture se han actualizado correctamente como se muestra en la imagen.



Nueva versión

Método 2. Instalación en el lado del cliente

Paso 1. Descargar instalador

Descargue el instalador desde Descarga de software.

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

Paso 2. Transferir instalador al dispositivo de destino

Transfiera el instalador descargado al dispositivo de destino mediante métodos como FTP (protocolo de transferencia de archivos), una unidad USB u otros métodos.

Paso 3. Ejecutar instalador

En el dispositivo de destino, extraiga los archivos comprimidos y ejecute Setup.exe.

Profiles	O Cisco Secure Client Install Selector
Setup	Select the Cisco Secure Client 5.1.2.42 modules you wish to install:
🔁 cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9.msi	S Core & AnyConnect VPN
😓 cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9.msi	🖬 Start Before Login
cisco-secure-client-win-5.1.2.42-dart-predeploy-k9.msi	Network Access Manager
cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9.msi	Secure Firewall Posture Network Visibility Module
cisco-secure-client-win-5.1.2.42-nam-predeploy-k9.msi	S Umbrella
cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9.msi	
cisco-secure-client-win-5.1.2.42-posture-predeploy-k9.msi	ThousandEyes
a cisco-secure-client-win-5.1.2.42-predeploy-k9.zip	Zero Trust Access
cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9.msi	Select All
cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9.msi	Diagnostic And Reporting Tool
cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9.msi	Lock Down Component Services
🕲 Setup.exe	Install Selected
setup.hta	

Ejecutar instalador

Paso 4. Confirmar nueva versión

Confirme que Cisco Secure Client y Secure Firewall Posture se han actualizado correctamente como se muestra en la imagen.

🕲 Cisco Secure Client - 🗆 🗙	(S) Cisco Secure Client	>
AnyConnect VPIE Connected to 192.168.1.1. 192.168.1.1 00:00:08	© Copyright 2004 - 2023 Cisco Systems, Inc. All Rights Reserved	\bigcirc
	Terms of service	
	Privacy statement	
	Notices and disclaimers	
	Third-party licenses and notices	
	Installed Modules:	^
	AnyConnect VPN 5.1.2.42	
	Customer Experience Feedback 5.1.2.42	
	Secure Firewall Posture 5.1.2.42	
	Umbrella 5.1.2.42	~
		Close

Nueva versión

Preguntas frecuentes

P: Si la versión de Secure Firewall Posture (anteriormente HostScan) especificada en el lado ASA es anterior a la versión instalada en el terminal, ¿sigue funcionando correctamente?

R.: Sí. Este es un ejemplo de verificación operativa después de actualizar HostScan versión 4.10.07073 a Secure Firewall Posture versión 5.1.2.42 en un terminal específico, con DAP (<u>Scenario3</u>). <u>Se hacen coincidir varios DAP (Acción : Continuar</u>) configurados en HostScan 4.10.07073.



Precaución: el comportamiento puede depender de la versión de Secure Firewall Posture/Cisco Secure Client, así que asegúrese de comprobar las últimas notas de la versión para cada versión.

Versión de la imagen configurada en el lado ASA:

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

Versión de la imagen en el dispositivo de destino:

O Cisco Secure Client

Secure Client



© Copyright 2004 - 2023 Cisco Systems, Inc. All Rights Reserved

Terms of service
Privacy statement
Notices and disclaimers
Third-party licenses and notices

Installed Modules:

Name	Version	
AnyConnect VPN	5.1.2.42	
Customer Experience Feedback	5.1.2.42	
Secure Firewall Posture	5.1.2.42	
Umbrella	5.1.2.42	

Close

Versión de la imagen en el dispositivo

Ejemplo de conexión de Cisco Secure Client:

S Cisco Secure Client − □	×	Sisco Secure Client 192.168.1.1	×
AnyConnect VPII: Please enter your username and password. 192.168.1.1 V Connect		Please enter your username and po Group: dap_test Username: cisco Password: *******	assword.
Cisco Secure Client Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions: 01_dap_test 03_dap_test 04_d	×	CK Cisco Secure Client AnyConnect VPR Connected to 192.168.1.1. 192.168.1.1 00:00:30	Cancel
OK			

Conexión de Cisco Secure Client

P: ¿Cisco Secure Client 5.x funciona correctamente en combinación con HostScan 4.x?

R: No. La combinación de Cisco Secure Client 5.x y HostScan 4.x no es compatible.

P: Al actualizar de HostScan 4.x a Secure Firewall Posture 5.x, ¿es posible actualizar solo en ciertos dispositivos?

R: Sí. Puede actualizar dispositivos específicos mediante el método 2 mencionado.

Información Relacionada

Soporte técnico y descargas de Cisco

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).