Upgrade von HostScan auf Secure Firewall Posture unter Windows

Inhalt

Einleitung

In diesem Dokument wird das Upgrade von HostScan auf Secure Firewall Posture (ehemals HostScan) unter Windows beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- Konfiguration von Cisco AnyConnect und HostScan

Verwendete Komponenten

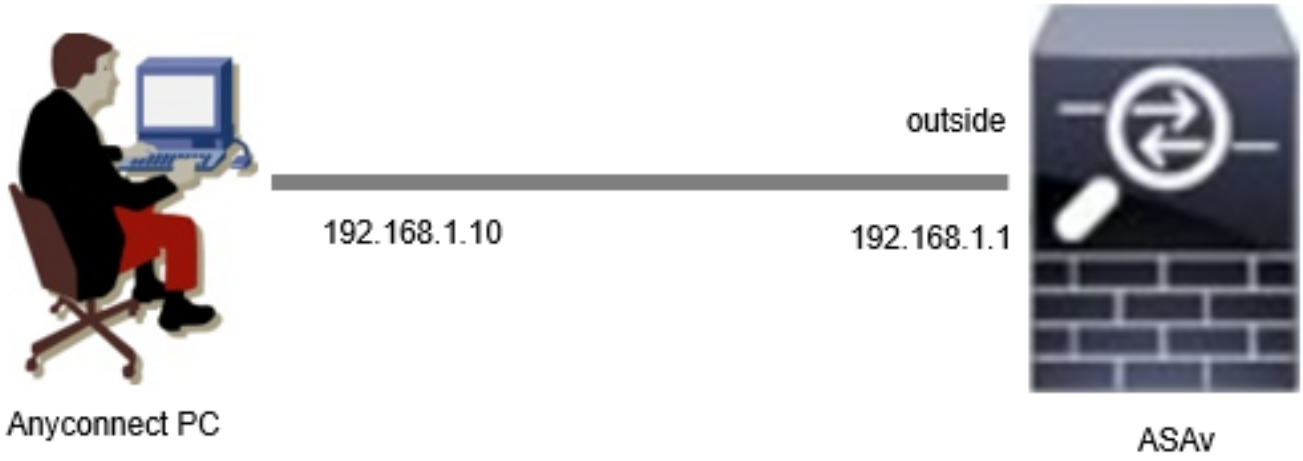
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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
- Secure Firewall Status 5.1.2.42

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.



Netzwerkdiagramm

Konfigurationen

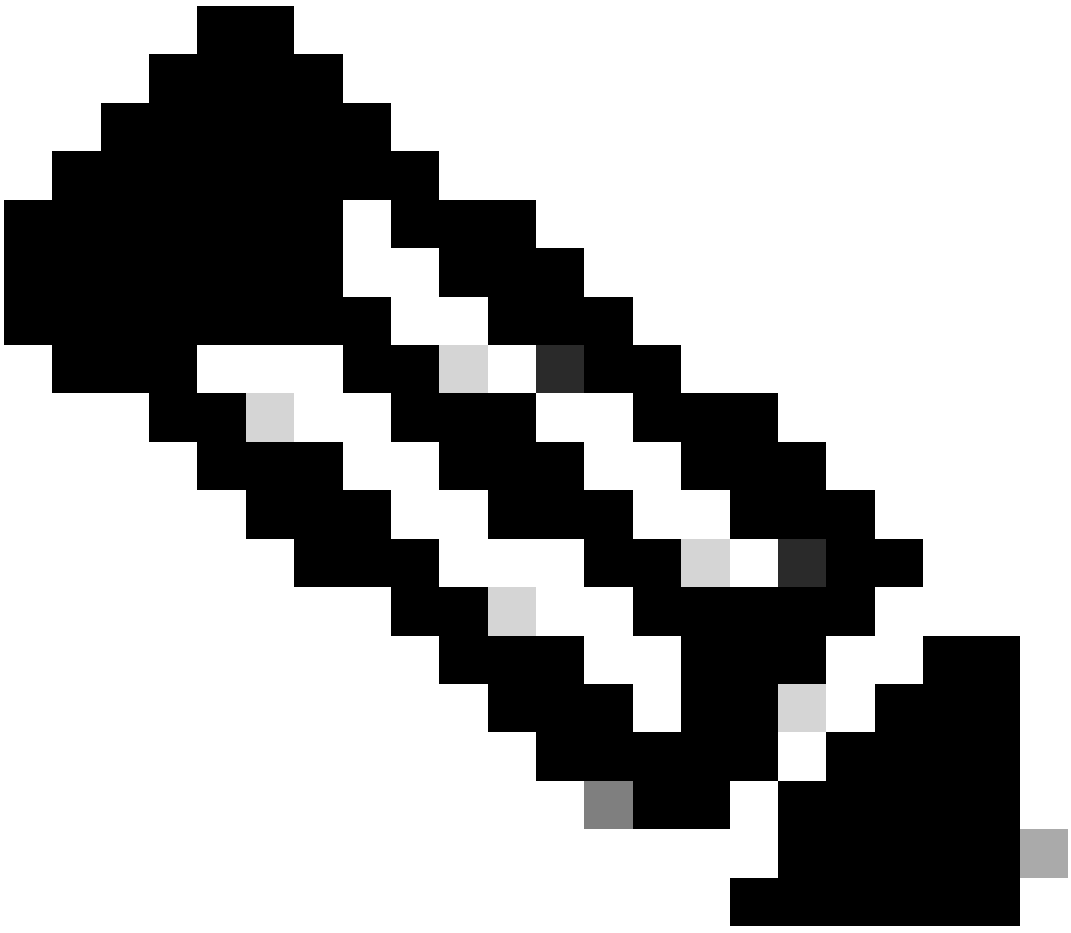
Dies ist die minimale Konfiguration in der ASA CLI.

```
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
```

Upgrade

Dieses Dokument enthält ein Beispiel für ein Upgrade von AnyConnect HostScan Version 4.10.07073 auf Secure Firewall Posture Version 5.1.2.42 in Verbindung mit dem Upgrade von Cisco Secure Client (früher Cisco AnyConnect Secure Mobility Client).



Hinweis: Cisco empfiehlt die Ausführung der neuesten Version von Secure Firewall Posture (entspricht der Version von Cisco Secure Client).

Methode 1: Bereitstellung auf ASA-Seite

Schritt 1: Bilddatei herunterladen

Laden Sie die Image-Dateien für Cisco Secure Client und Secure Firewall Posture vom Software-Download herunter.

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

Schritt 2: Übertragung der Image-Datei auf ASA Flash

Verwenden Sie in diesem Beispiel die ASA CLI, um die Image-Dateien von einem HTTP-Server auf ASA Flash zu übertragen.

```
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
```

Schritt 3: Angeben der Image-Datei von ASA CLI

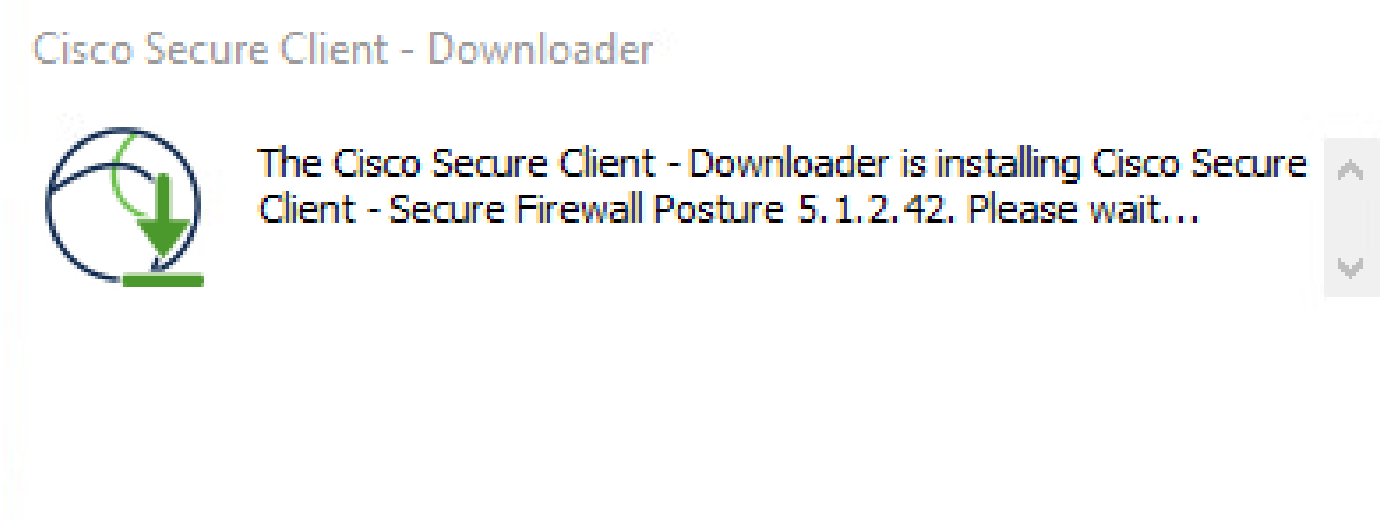
Geben Sie die neuen Image-Dateien an, die für die Verbindung mit dem Cisco Secure Client auf der ASA CLI verwendet werden.

```
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
```

Schritt 4: Automatische Aktualisierung

Sowohl der Cisco Secure Client als auch der Secure Firewall Posture können bei der nächsten Verbindungsherstellung automatisch aktualisiert werden.

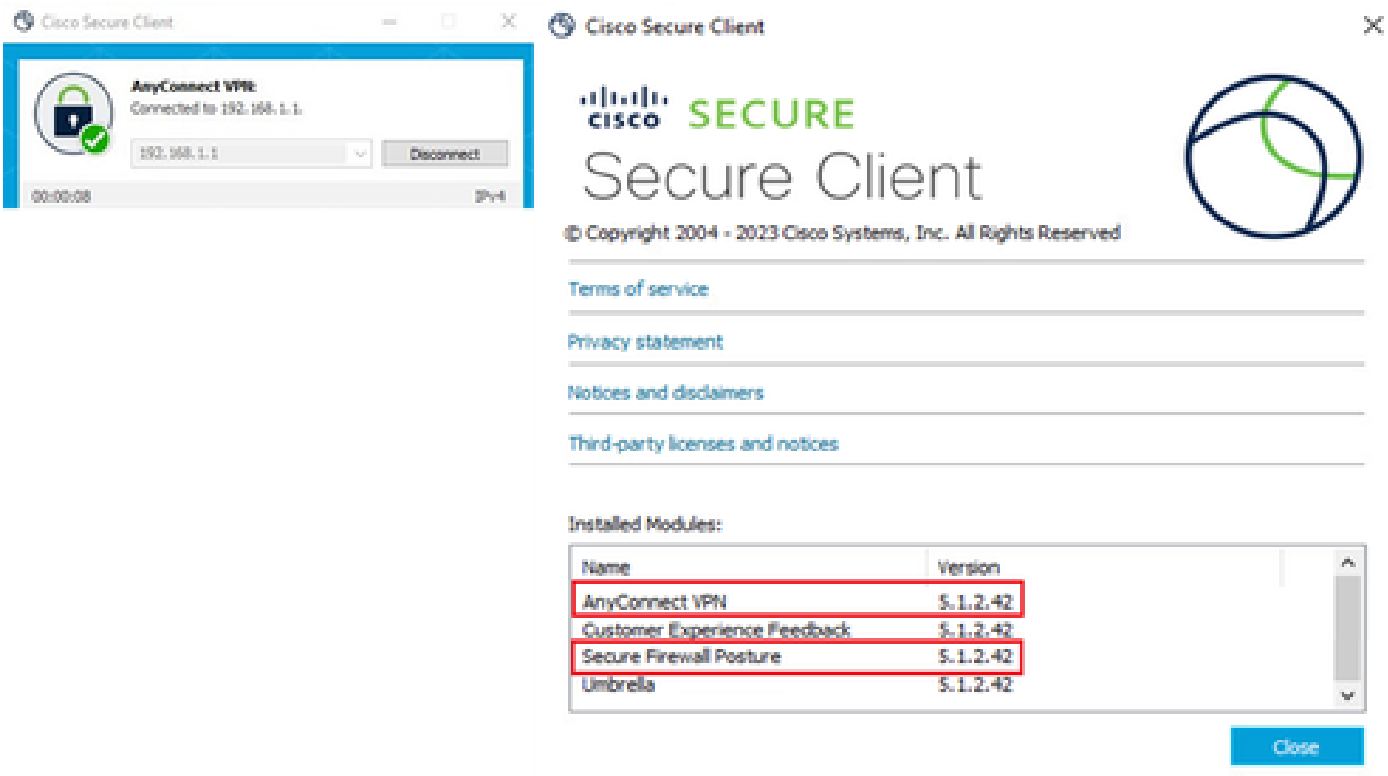
Das Secure Firewall Posture-Modul wird automatisch aktualisiert, wie im Image gezeigt.



Automatische Aktualisierung

Schritt 5: Neue Version bestätigen

Vergewissern Sie sich, dass das Upgrade von Cisco Secure Client und Secure Firewall Posture erfolgreich durchgeführt wurde, wie im Image gezeigt.



Neue Version

Methode 2. Client-seitig installieren

Schritt 1: Installationsprogramm herunterladen

Laden Sie das Installationsprogramm von Software Download herunter.

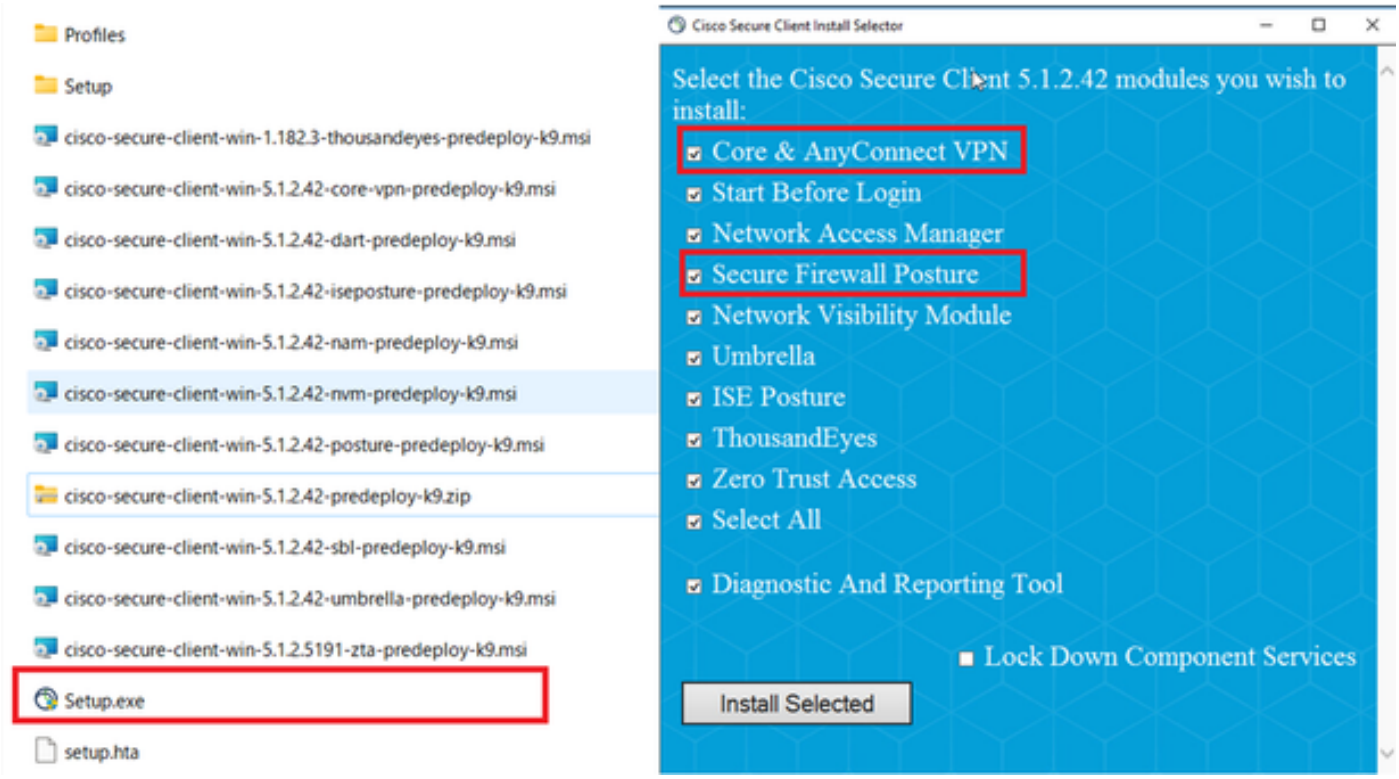
- cisco-secure-client-win-5.1.2.42-predeploy-k9.zip

Schritt 2: Installer auf Zielgerät übertragen

Übertragen Sie das heruntergeladene Installationsprogramm mithilfe von Methoden wie FTP (File Transfer Protocol), einem USB-Laufwerk oder anderen Methoden auf das Zielgerät.

Schritt 3: Installationsprogramm ausführen

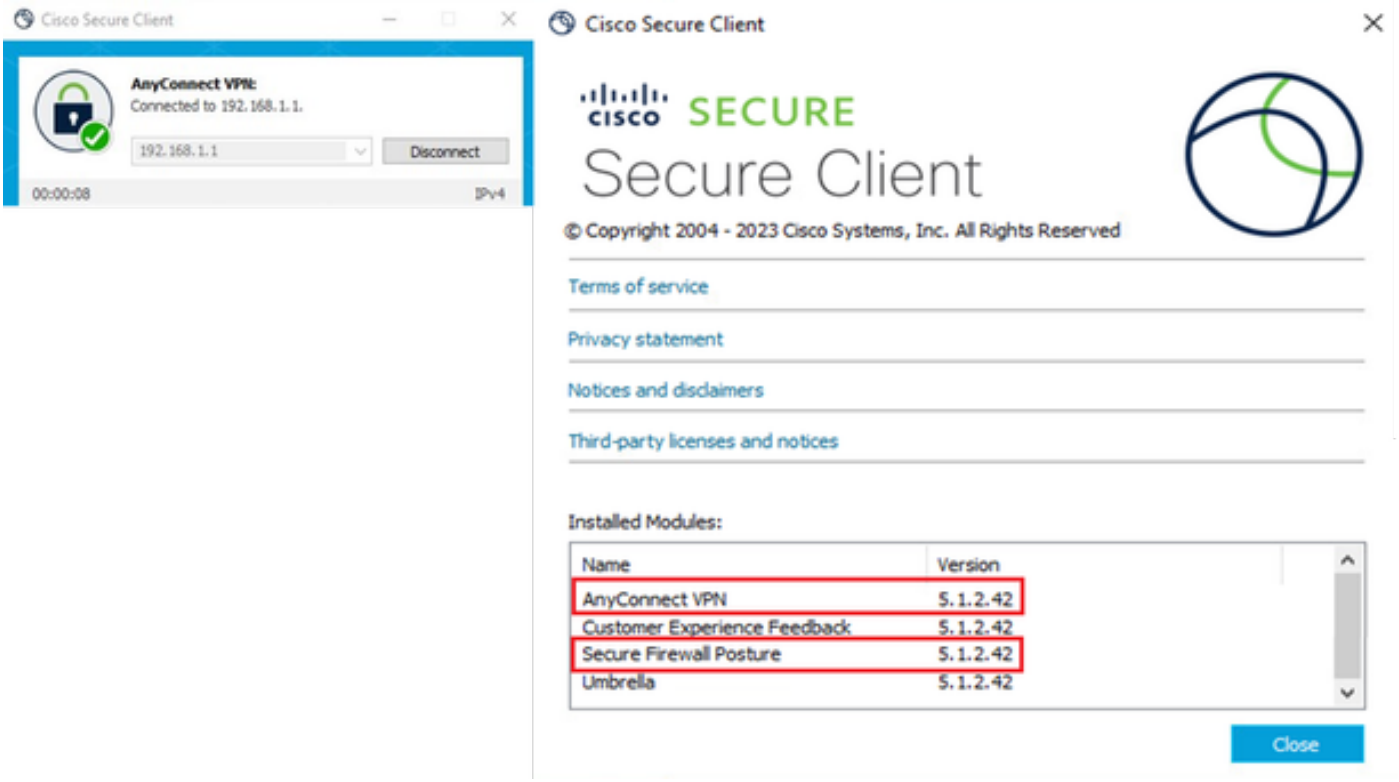
Extrahieren Sie die komprimierten Dateien auf dem Zielgerät, und führen Sie Setup.exe aus.



Installationsprogramm ausführen

Schritt 4: Neue Version bestätigen

Vergewissern Sie sich, dass das Upgrade von Cisco Secure Client und Secure Firewall Posture erfolgreich durchgeführt wurde, wie im Image gezeigt.

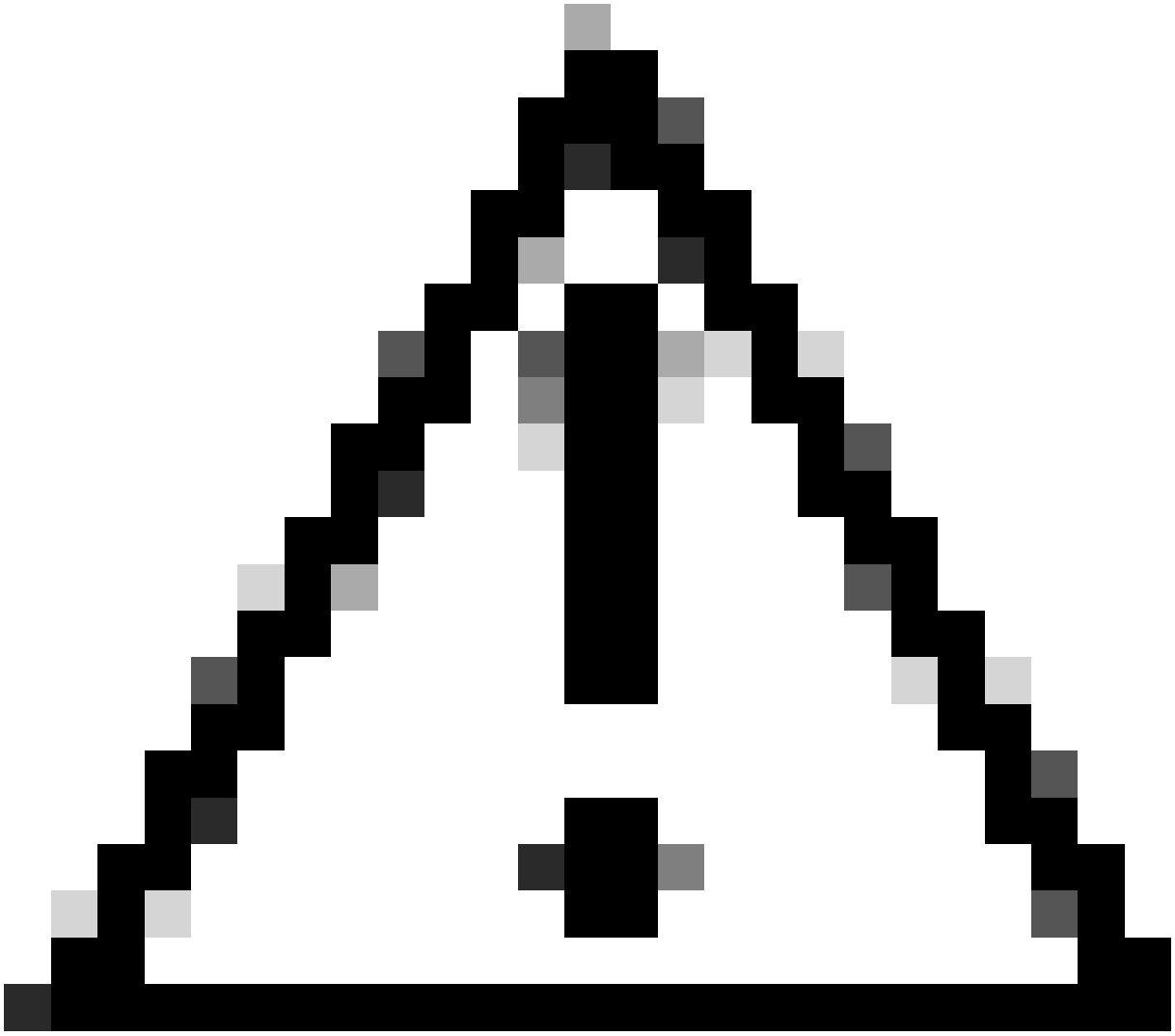


Neue Version

Häufig gestellte Fragen

F: Funktioniert die auf der ASA-Seite angegebene Version von Secure Firewall Posture (ehemals HostScan) noch immer korrekt, wenn sie älter ist als die auf dem Terminal installierte Version?

A: Ja. Dies ist ein Beispiel für eine Betriebsverifizierung nach dem Upgrade von HostScan Version 4.10.07073 auf Secure Firewall Posture Version 5.1.2.42 auf einem bestimmten Terminal mit DAP (Scenario3. Mehrere DAPs (Aktion: Fortfahren) werden zugeordnet), die in HostScan 4.10.07073 konfiguriert sind.



Vorsicht: Das Verhalten kann von der Version von Secure Firewall Posture/Cisco Secure Client abhängen. Lesen Sie daher für jede Version die neuesten Versionshinweise.

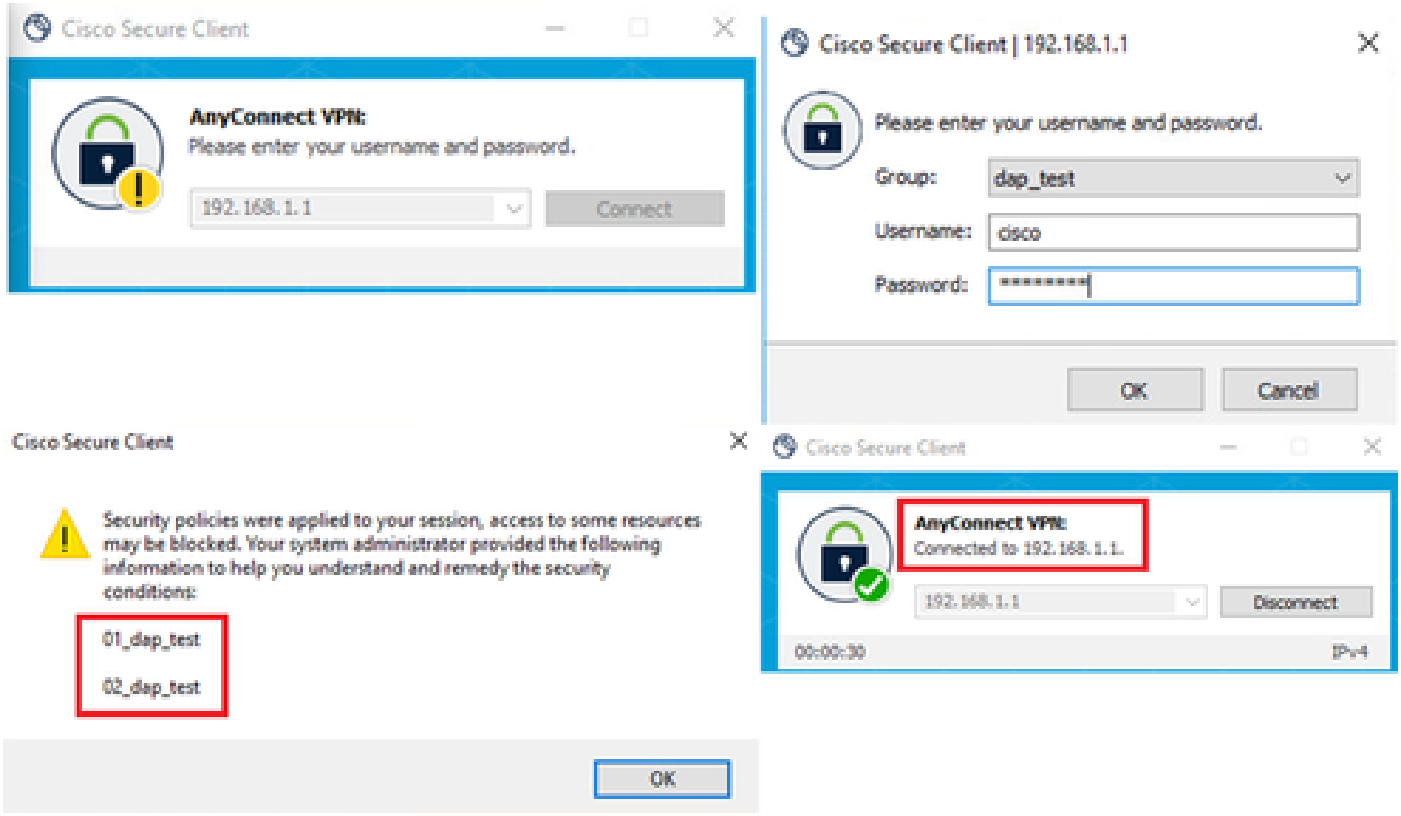
Auf ASA-Seite konfigurierte Image-Version:

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

Image-Version auf Zielgerät:

Bildversion auf Gerät

Beispiel für eine Cisco Secure Client-Verbindung:



Cisco Secure Client-Verbindung

F: Funktioniert Cisco Secure Client 5.x ordnungsgemäß in Kombination mit HostScan 4.x?

A : Nein. Die Kombination aus Cisco Secure Client 5.x und HostScan 4.x wird nicht unterstützt.

F: Ist es bei einem Upgrade von HostScan 4.x auf Secure Firewall Posture 5.x möglich, nur auf bestimmten Geräten ein Upgrade durchzuführen?

A: Ja. Sie können bestimmte Geräte mithilfe der genannten Methode 2 aktualisieren.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.