Upgrade van HostScan naar Secure Firewall Posture in Windows

Inhoud

Inleiding

Dit document beschrijft de procedure om van HostScan naar Secure Firewall Posture (voorheen HostScan) te upgraden op Windows.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met dit onderwerp:

- Configuratie van Cisco AnyConnect en Hostscan

Gebruikte componenten

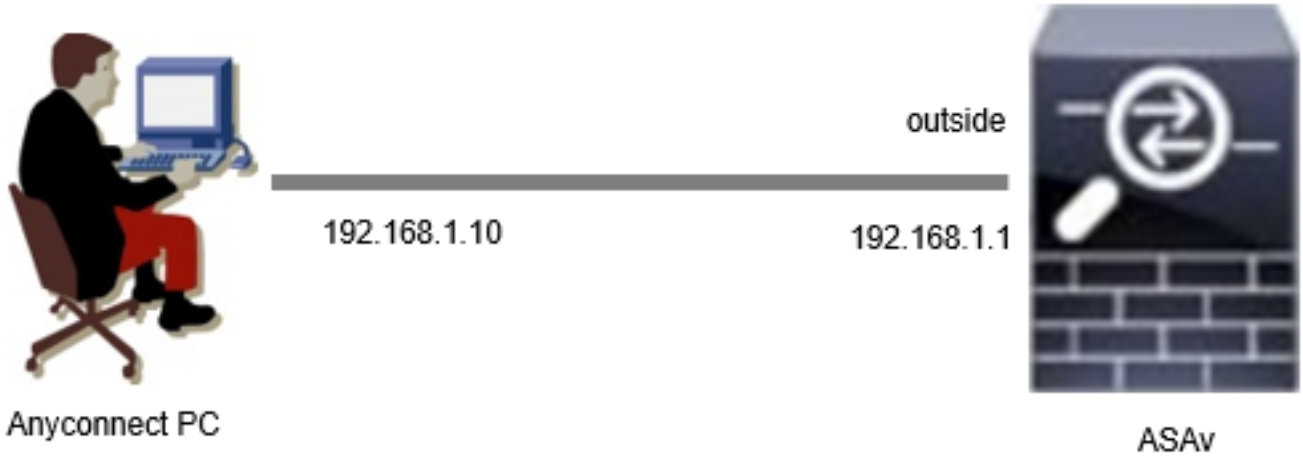
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco adaptieve security virtuele applicatie 9.18 (4)
- Cisco Adaptieve Security Device Manager 7.20 (1)
- Cisco AnyConnect Secure Mobility-client 4.10.07073
- AnyConnect HostScan 4.10.07073
- Cisco Secure-client 5.1.2.4
- Secure-firewallhouding 5.1.2.42

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdiagram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.



Netwerkdiagram

Configuraties

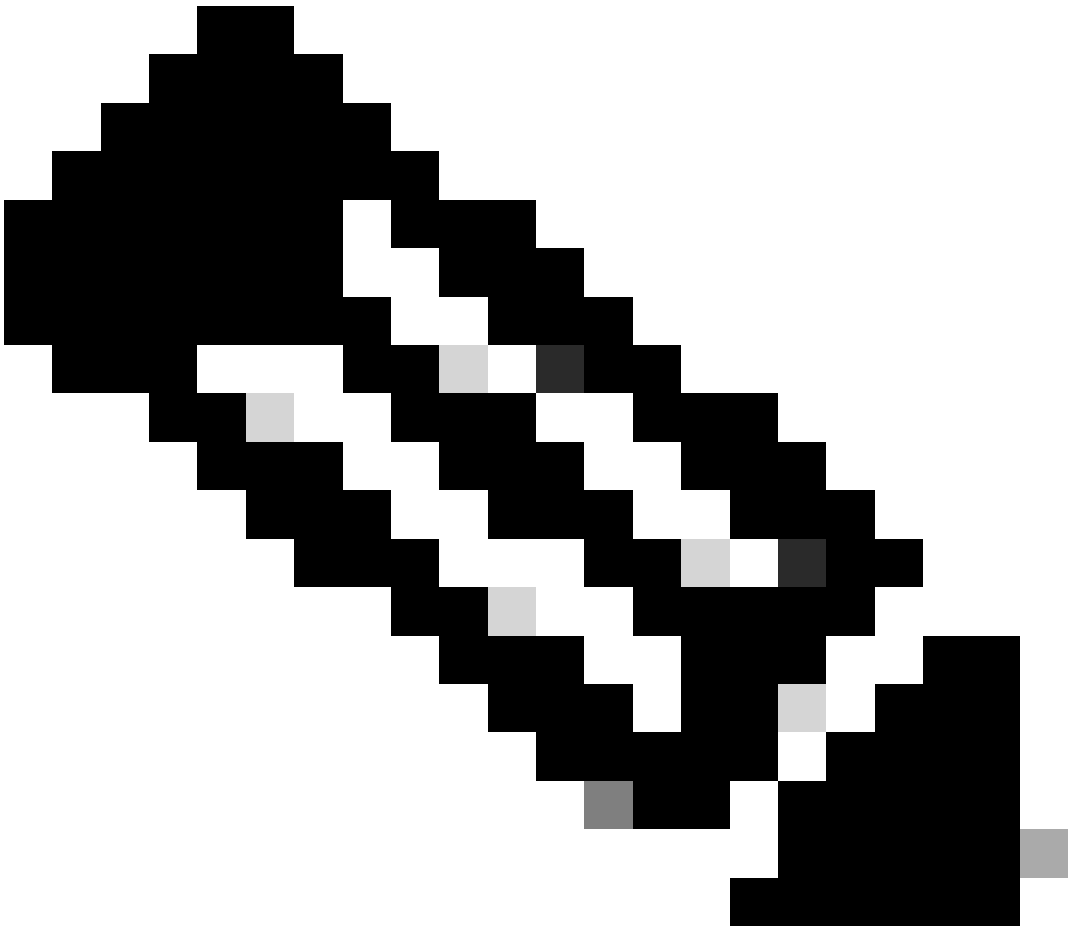
Dit is de minimale configuratie in ASA CLI.

```
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
```

Upgraden

Dit document bevat een voorbeeld van de manier waarop u kunt upgraden van AnyConnect HostScan, versie 4.10.07073 naar Secure Firewall Posture versie 5.1.2.42, in combinatie met de upgrade van Cisco Secure Client (voorheen Cisco AnyConnect Secure Mobility Client).



Opmerking: Cisco raadt u aan de meest recente versie van Secure Firewall Posture (dezelfde versie als de versie van Cisco Secure Client) uit te voeren.

Methode 1. Implementeren op ASA-kant

Stap 1. Afbeeldingsbestand downloaden

Download de beeldbestanden voor Cisco Secure Client en Secure Firewall Posture van de Software Download.

- Cisco Secure-client: cisco-secure-client-win-5.1.2.42-webimplementatie-k9.pkg
- Secure Firewall postuur: Secure-firewall-postuur-5.1.2.42-k9.pkg

Stap 2. Afbeeldingsbestand naar ASA Flash overzetten

In dit voorbeeld, gebruik ASA CLI om de beeldbestanden van een HTTP server naar ASA flitser over te brengen.

```
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
```

Stap 3. Afbeeldingsbestand van ASA CLI opgeven

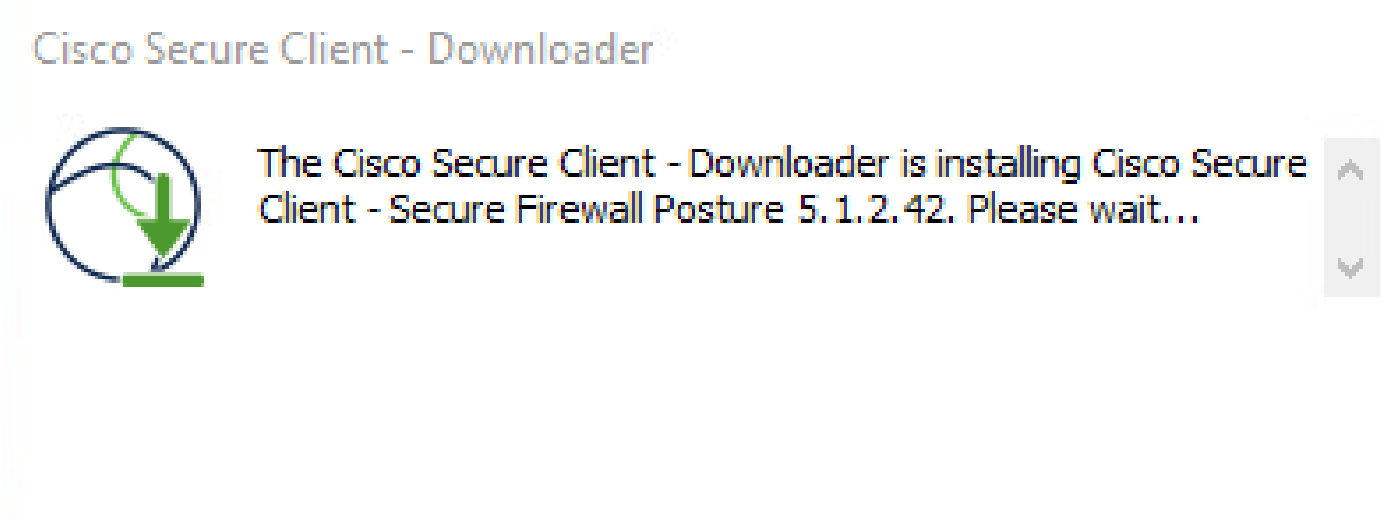
Specificeer de nieuwe beeldbestanden die worden gebruikt voor Cisco Secure Client-verbinding op ASA CLI.

```
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
```

Stap 4. Automatisch upgraden

Zowel Cisco Secure Client als Secure Firewall Posture kunnen automatisch worden bijgewerkt wanneer de client opnieuw verbinding maakt.

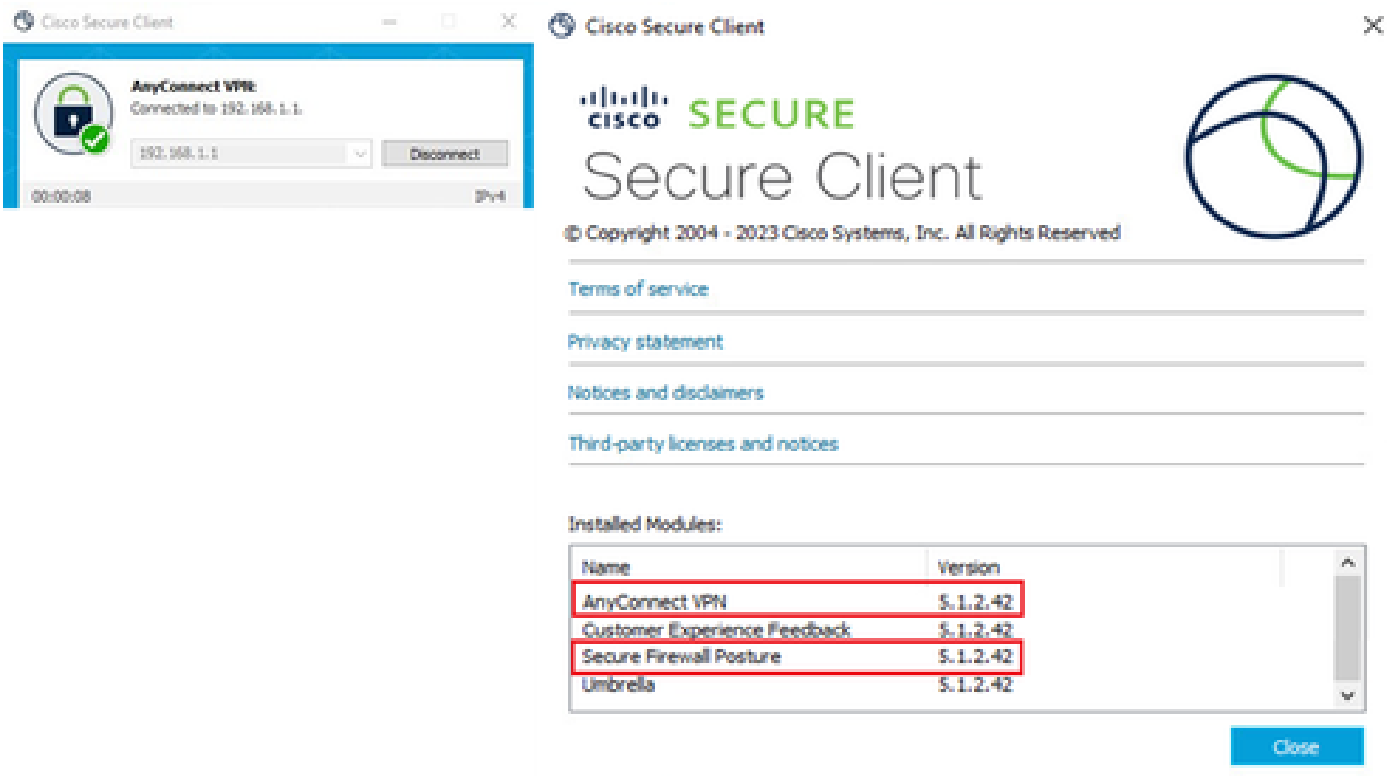
De Secure Firewall Posture-module wordt automatisch bijgewerkt zoals in de afbeelding wordt weergegeven.



Automatisch upgraden

Stap 5. Bevestig nieuwe versie

Bevestig dat de beveiligde client en de beveiligde firewall van Cisco met succes zijn bijgewerkt zoals in de afbeelding wordt getoond.



Nieuwe versie

Methode 2. Installeren op clientzijde

Stap 1. Downloadinstallatieprogramma

Download het installatieprogramma van Software Download.

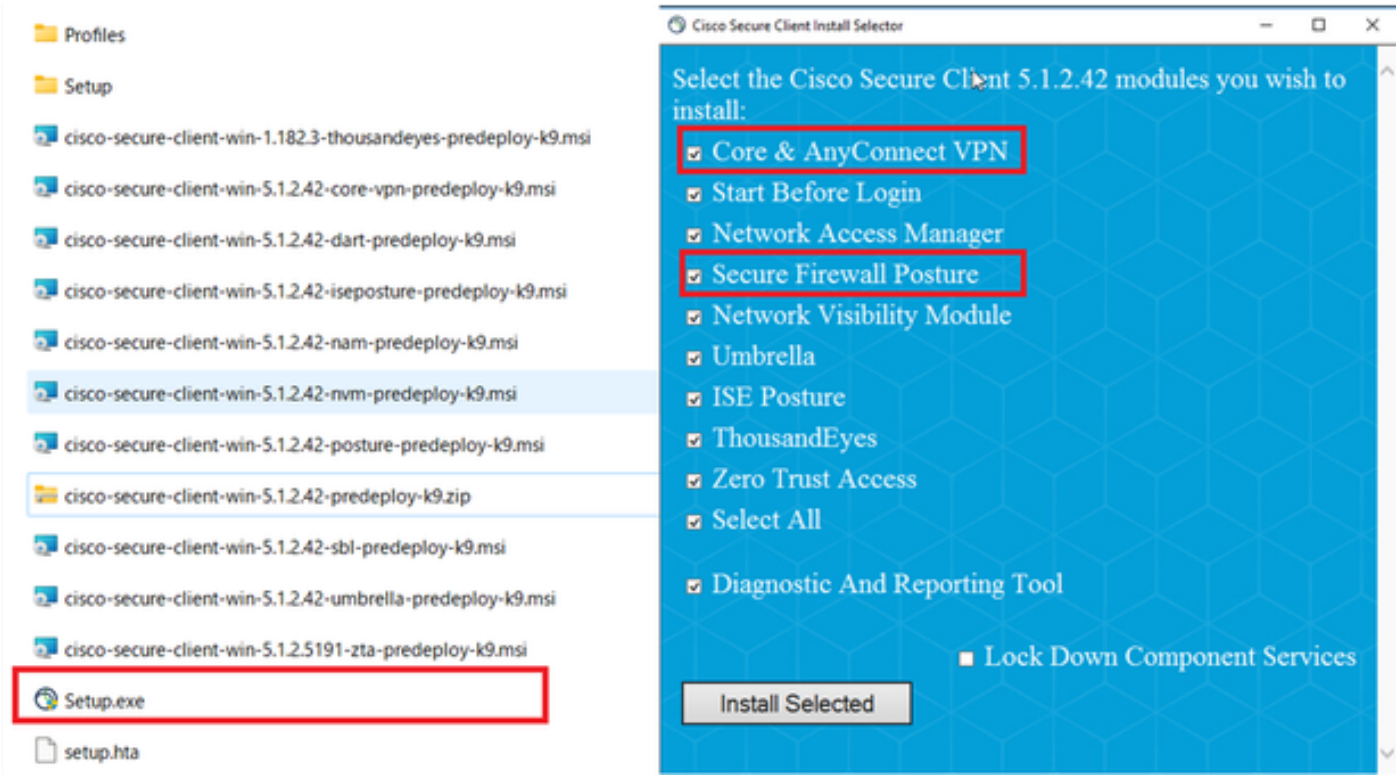
- cisco-secure-client-win-5.1.2.42-predeploy-k9.zip

Stap 2. Installateur naar doelapparaat overzetten

Breng het gedownloade installatieprogramma over naar het doelapparaat met behulp van methoden zoals FTP (File Transfer Protocol), een USB-station of andere methoden.

Stap 3. Installateur starten

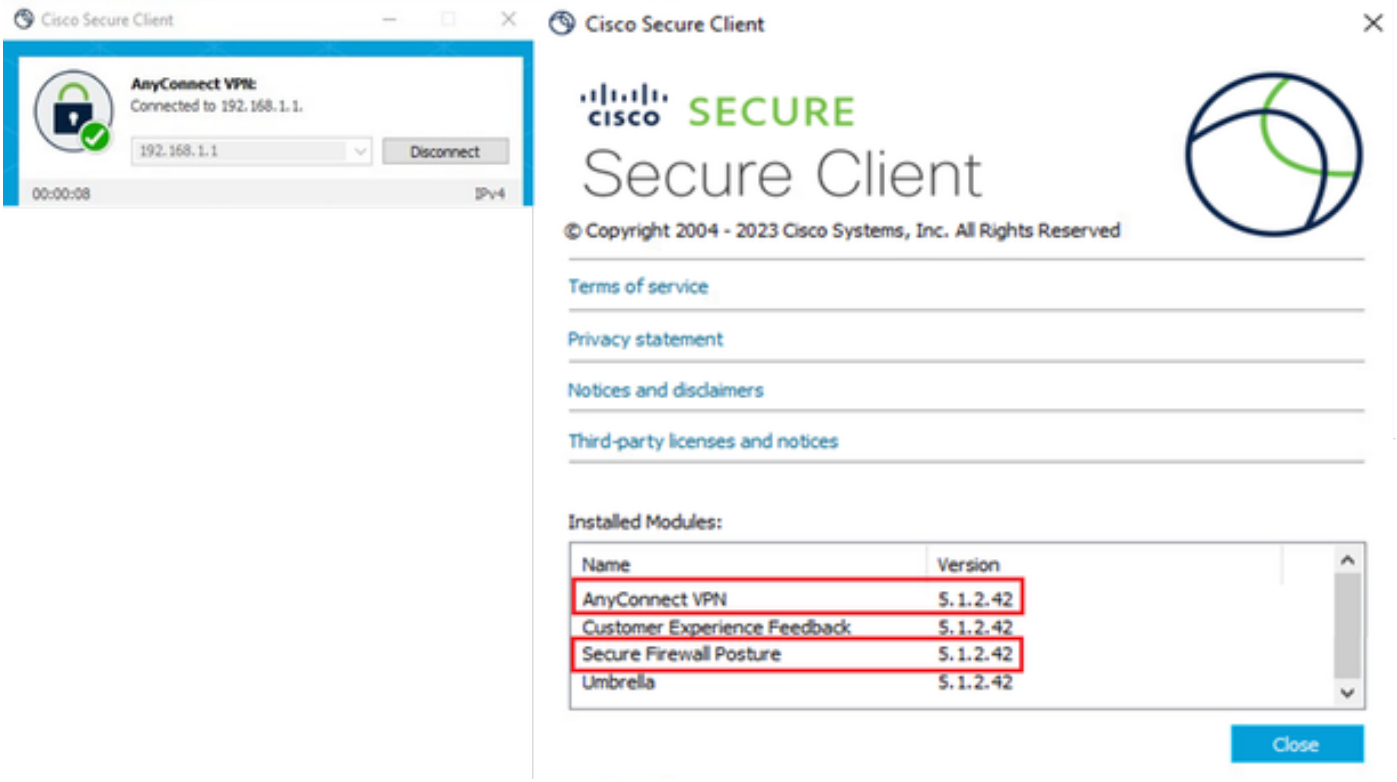
Haal op het doelapparaat de gecomprimeerde bestanden eruit en voer Setup.exe uit.



Installateur starten

Stap 4. Bevestig nieuwe versie

Bevestig dat de beveiligde client en de beveiligde firewall van Cisco met succes zijn bijgewerkt zoals in de afbeelding wordt getoond.

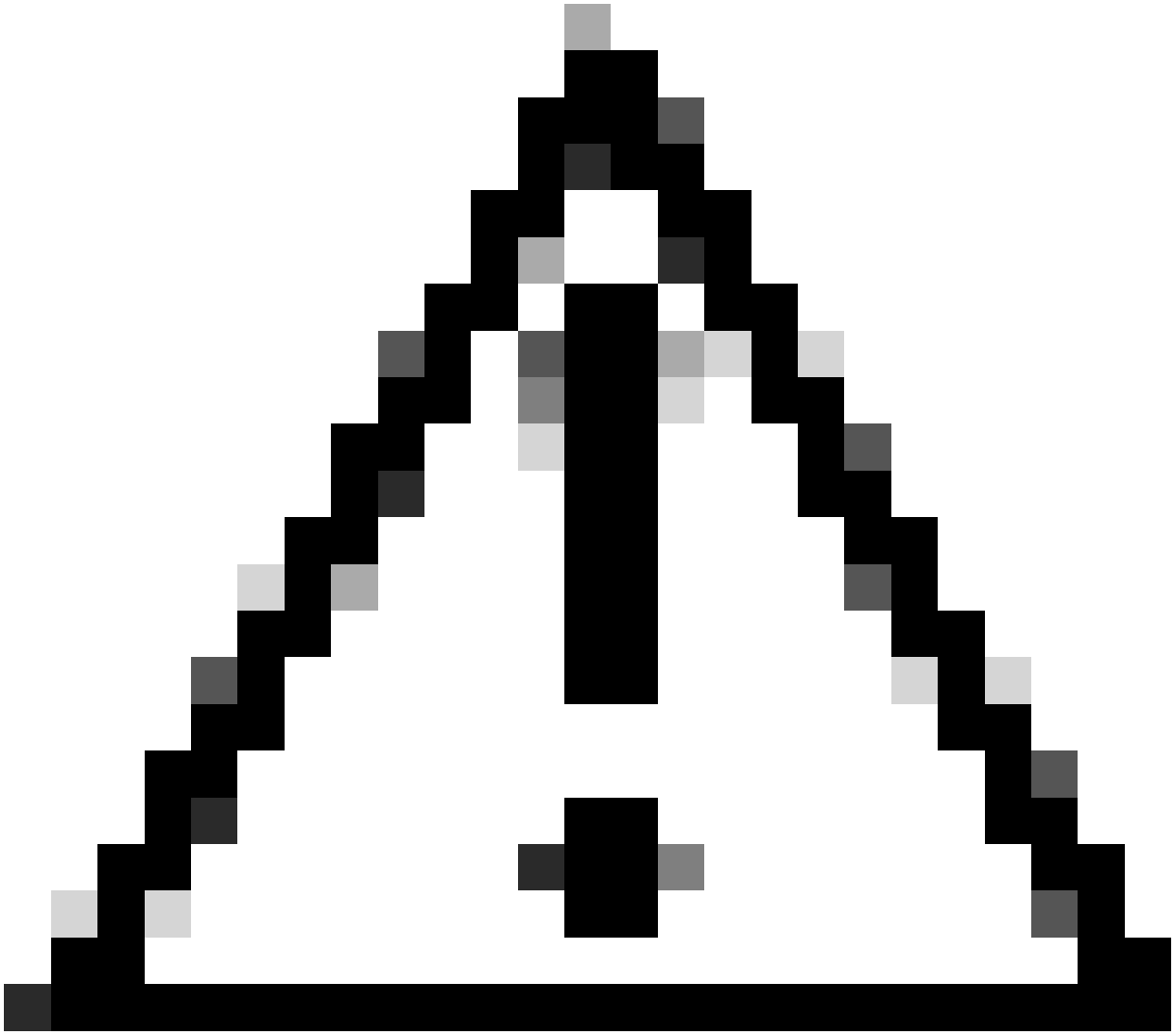


Nieuwe versie

Veelgestelde vragen (FAQ)

Q: Als de versie van Secure Firewall Posture (voorheen HostScan) die aan de ASA-kant is opgegeven ouder is dan de versie die op de terminal is geïnstalleerd, werkt deze dan nog steeds correct?

A: Ja. Dit is een voorbeeld van operationele verificatie na het upgraden van HostScan versie 4.10.07073 naar Secure Firewall Posture versie 5.1.2.42 op een specifieke terminal, met DAP (Scenario3). Meervoudige DAP's (Actie: Doorgaan) worden geconfigureerd in HostScan 4.10.07073.



Waarschuwing: het gedrag kan afhangen van de versie van Secure Firewall Posture/Cisco Secure Client, dus controleer of de nieuwste release opmerkingen voor elke versie beschikbaar zijn.

Afbeelding versie geconfigureerd op ASA zijde:

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

Beeldversie op doelapparaat :

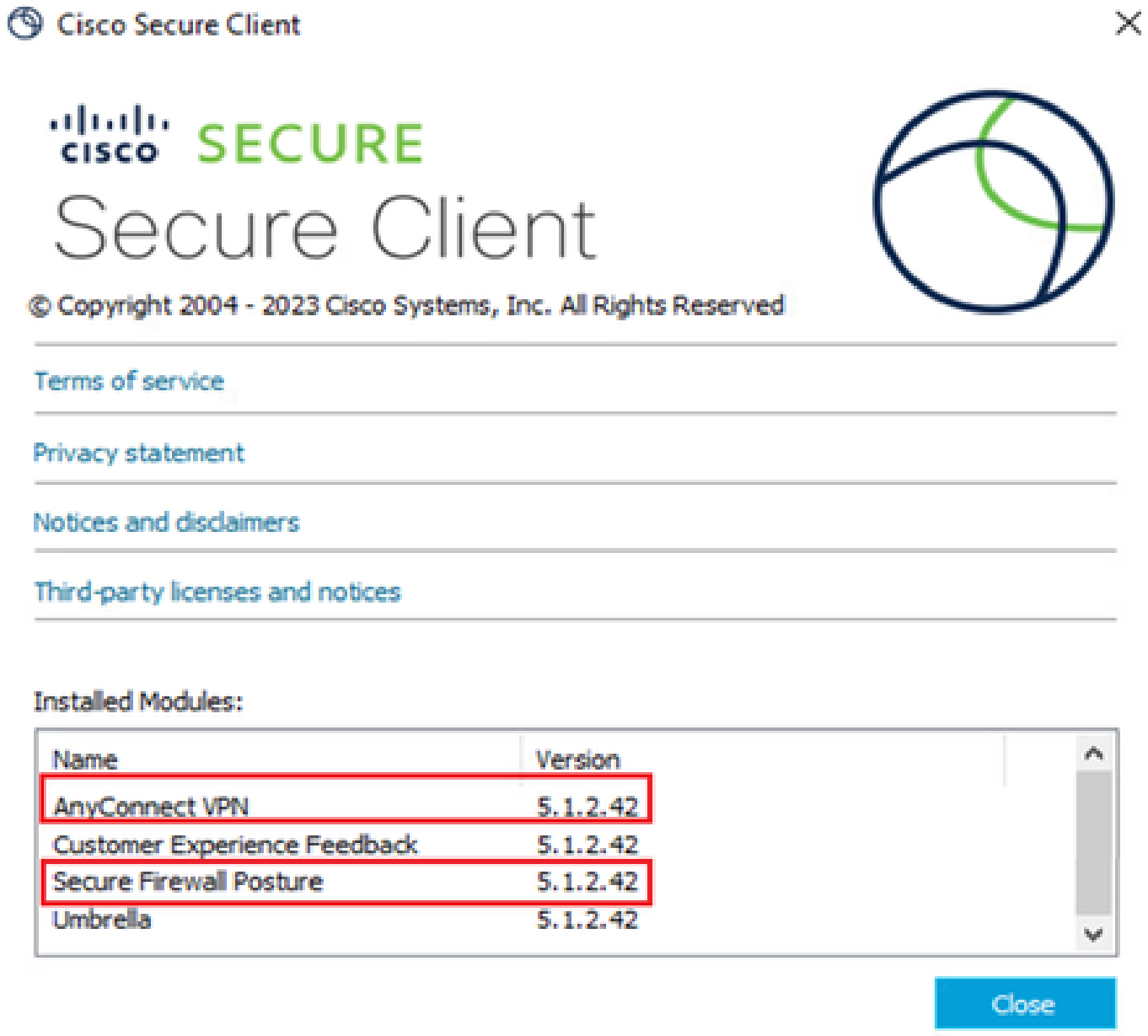
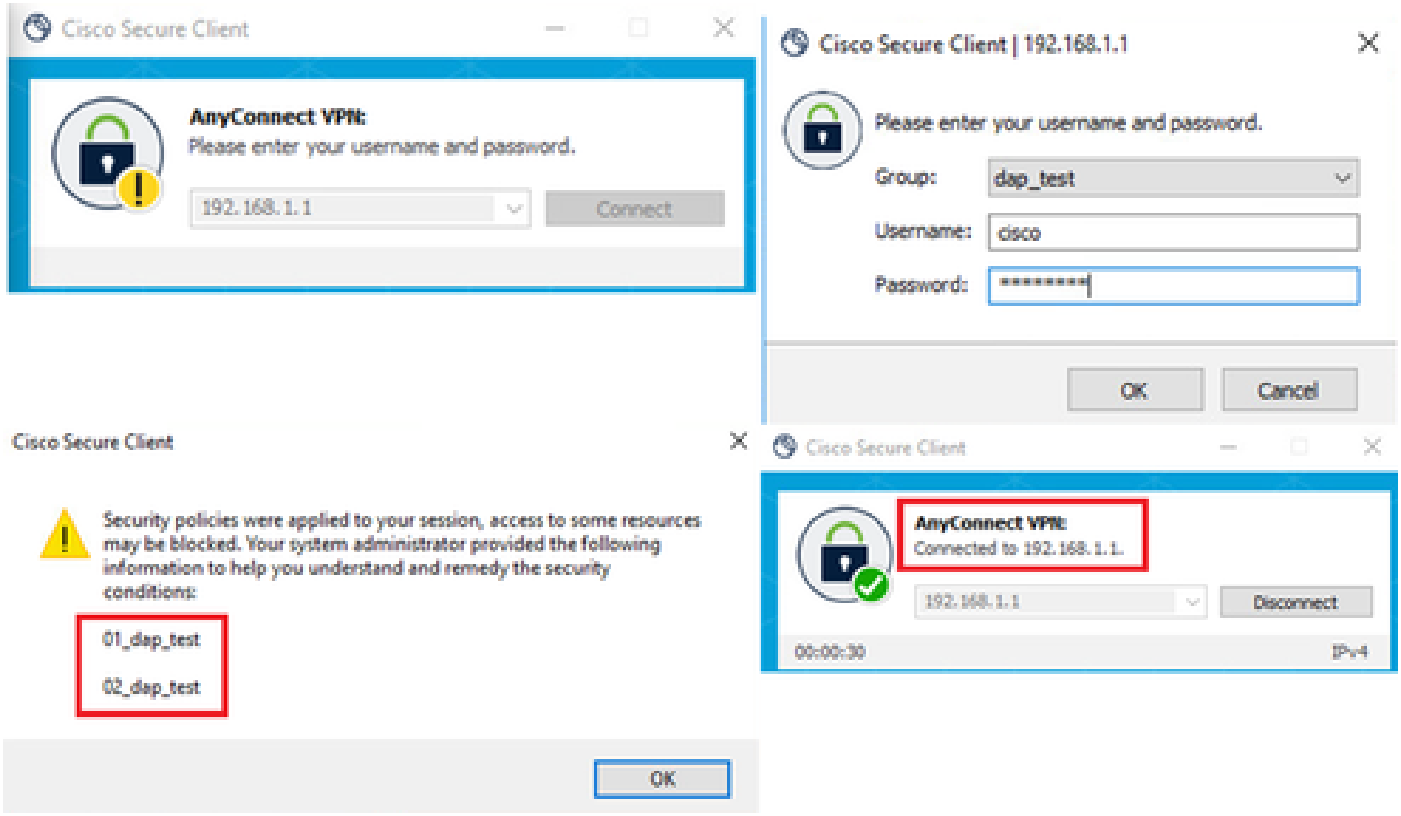


Image versie op apparaat

Voorbeeld van Cisco Secure Client-verbinding :



Cisco Secure-clientverbinding

V: Werkt Cisco Secure Client 5.x correct in combinatie met HostScan 4.x?

A: Nee. De combinatie van Cisco Secure Client 5.x en HostScan 4.x wordt niet ondersteund.

Q: Wanneer het bevorderen van van HostScan 4.x aan Secure Firewall Posture 5.x, is het mogelijk om slechts op bepaalde apparaten te bevorderen?

A : Ja. U kunt specifieke apparaten upgraden met de genoemde methode 2.

Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.