Aggiornamento da HostScan a Secure Firewall Posture in Windows

Sommario

Introduzione

In questo documento viene descritta la procedura per eseguire l'aggiornamento da HostScan a Secure Firewall Posture (in precedenza HostScan) in Windows.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- Configurazione di Cisco Anyconnect e Hostscan

Componenti usati

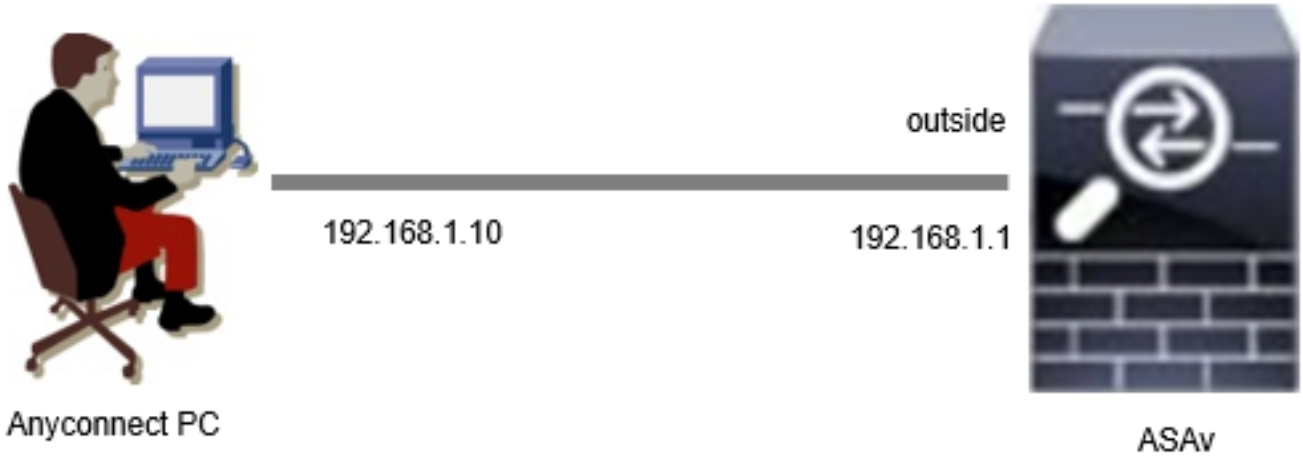
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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
- Postura protetta del firewall 5.1.2.42

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.



Esempio di rete

Configurazioni

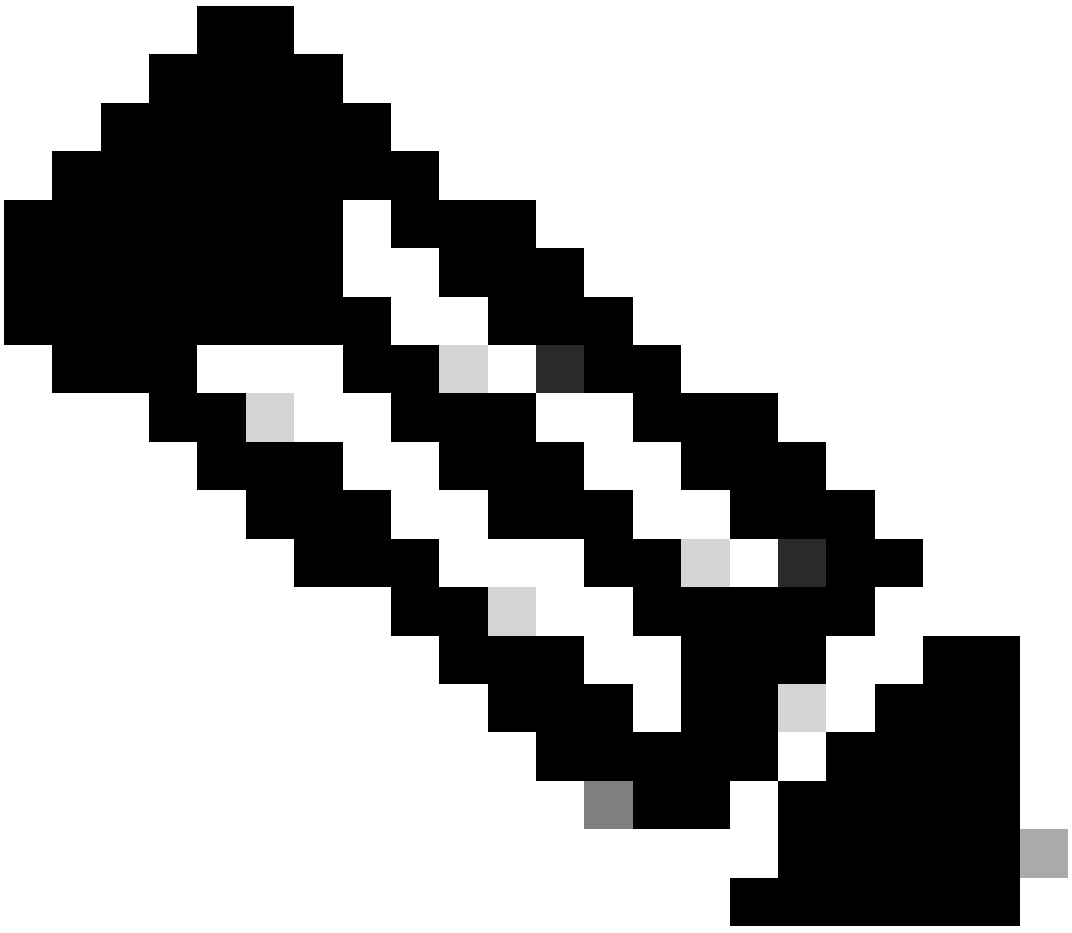
Questa è la configurazione minima nella CLI di ASA.

```
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
```

Aggiornamento

Questo documento offre un esempio di come aggiornare AnyConnect HostScan versione 4.10.07073 alla versione 5.1.2.42 di Secure Firewall Posture, insieme all'aggiornamento di Cisco Secure Client (in precedenza Cisco AnyConnect Secure Mobility Client).



Nota: Cisco consiglia di eseguire la versione più recente di Secure Firewall Posture (la stessa della versione di Cisco Secure Client).

Metodo 1. Installazione sul lato ASA

Passaggio 1. Scarica file immagine

Scaricare i file immagine per Cisco Secure Client e Secure Firewall Posture dal download del software.

- Cisco Secure Client : cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
- Postura protetta del firewall : secure-firewall-posture-5.1.2.42-k9.pkg

Passaggio 2. Trasferisci file immagine in ASA Flash

In questo esempio, usare ASA CLI per trasferire i file immagine da un server HTTP alla memoria 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
```

Passaggio 3. Specificare il file di immagine dalla CLI di ASA

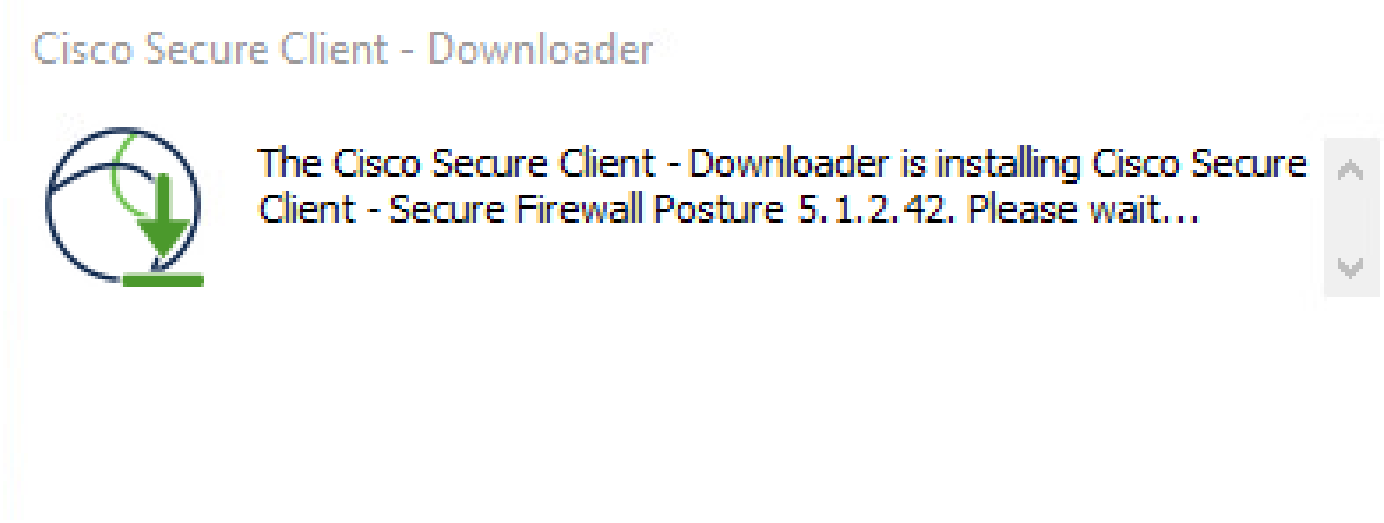
Specificare i nuovi file di immagine utilizzati per la connessione Cisco Secure Client sulla CLI ASA.

```
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
```

Passaggio 4. Aggiorna automaticamente

Sia Cisco Secure Client che Secure Firewall Posture possono essere aggiornati automaticamente alla successiva connessione del client.

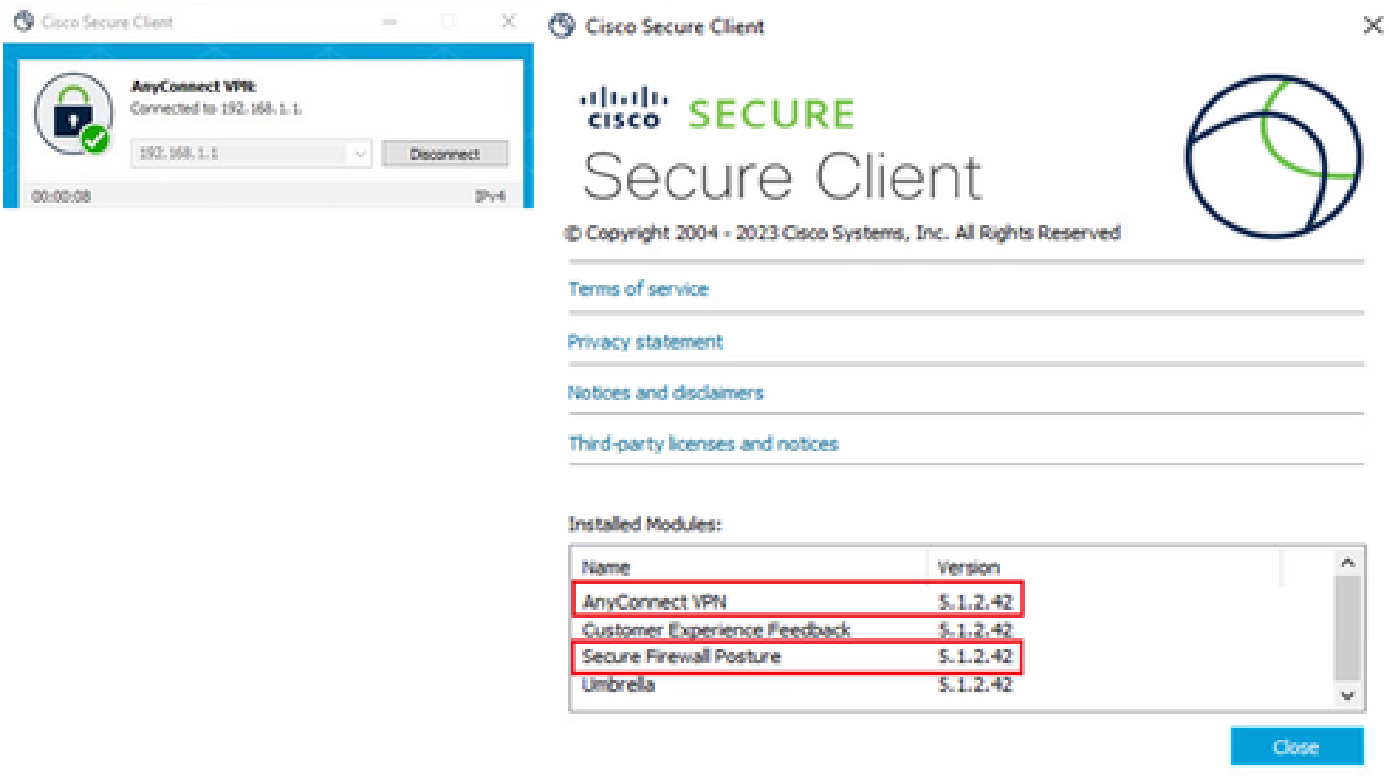
Il modulo Secure Firewall Posture viene aggiornato automaticamente come mostrato nell'immagine.



Aggiorna automaticamente

Passaggio 5. Conferma nuova versione

Confermare che Cisco Secure Client e Secure Firewall Posture siano stati aggiornati correttamente come mostrato nell'immagine.



Nuova versione

Metodo 2. Installazione sul lato client

Passaggio 1. Scarica programma di installazione

Scaricare il programma di installazione da Software Download.

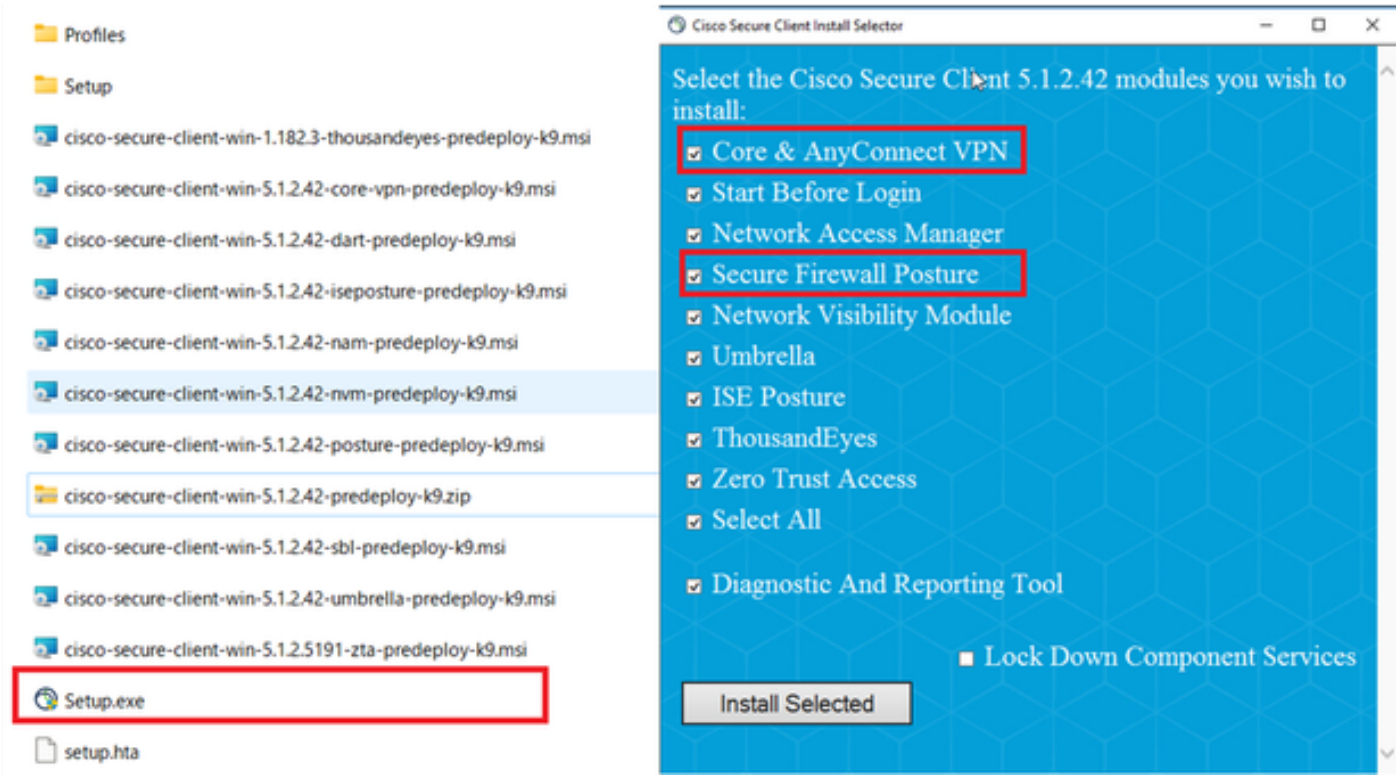
- cisco-secure-client-win-5.1.2.42-predeploy-k9.zip

Passaggio 2. Trasferisci programma di installazione a dispositivo di destinazione

Trasferire il programma di installazione scaricato sul dispositivo di destinazione utilizzando metodi quali FTP (File Transfer Protocol), un'unità USB o altri metodi.

Passaggio 3. Esegui programma di installazione

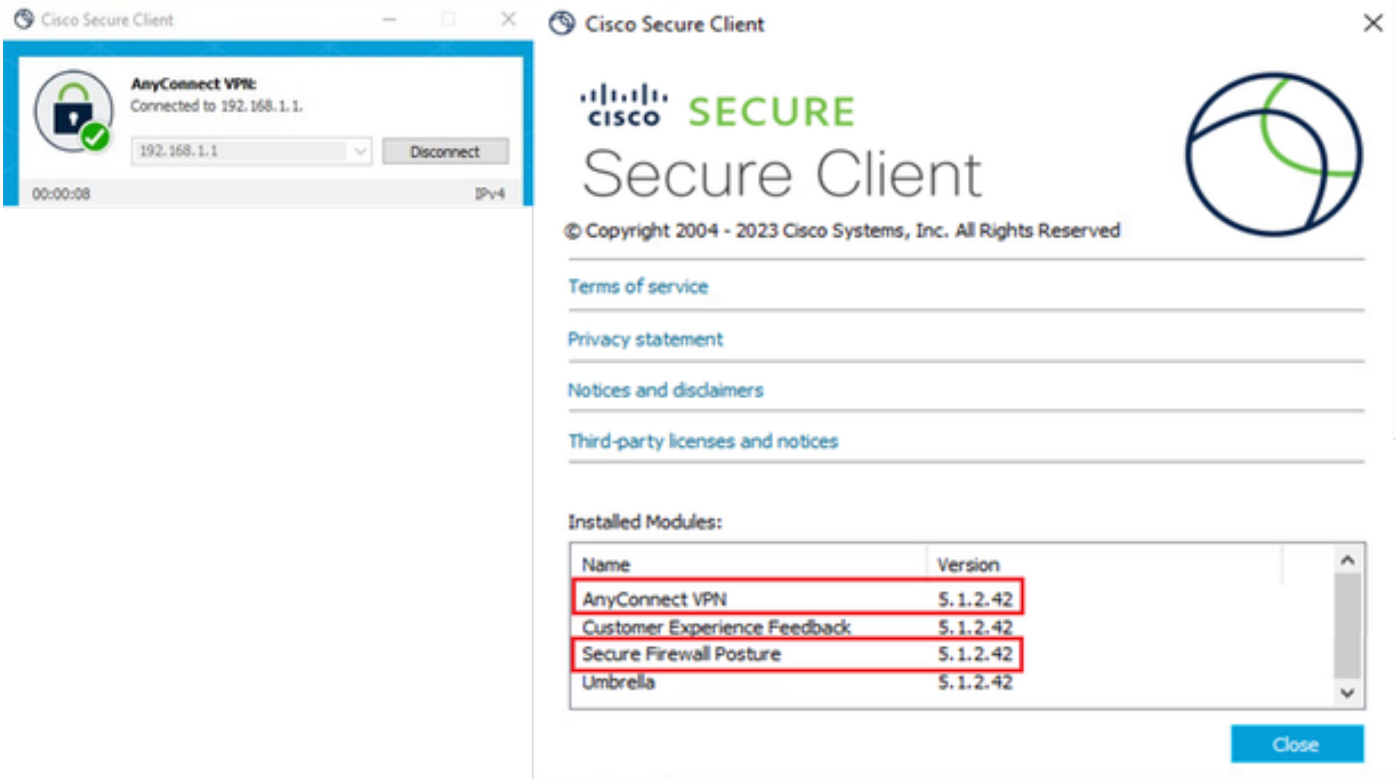
Nel dispositivo di destinazione estrarre i file compressi ed eseguire Setup.exe.



Esegui programma di installazione

Passaggio 4. Conferma nuova versione

Confermare che Cisco Secure Client e Secure Firewall Posture siano stati aggiornati correttamente come mostrato nell'immagine.

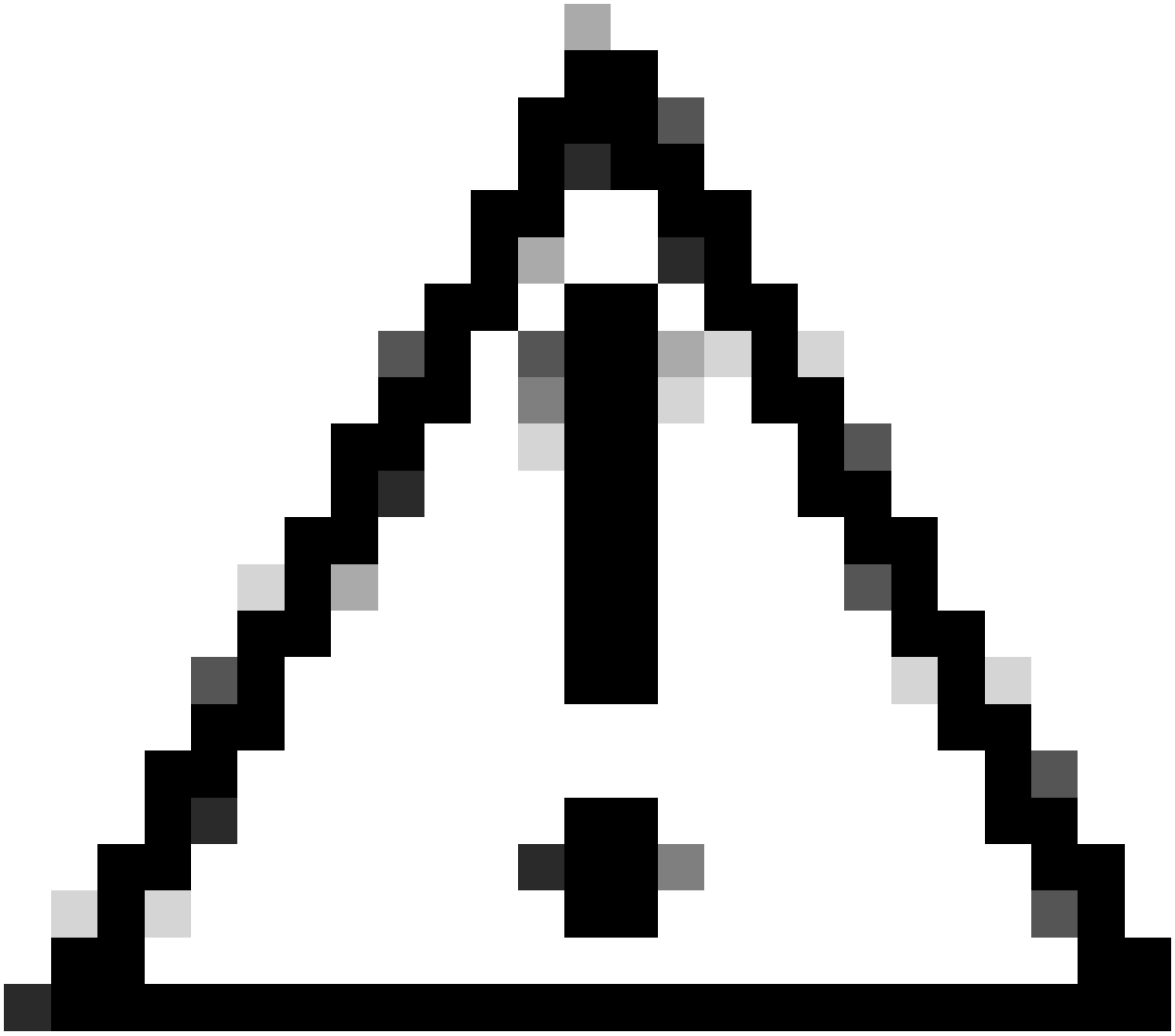


Nuova versione

Domande frequenti (FAQ)

D: Se la versione di Secure Firewall Posture (in precedenza HostScan) specificata sul lato ASA è precedente alla versione installata sul terminale, funziona ancora correttamente?

R: Sì. Questo è un esempio di verifica operativa dopo l'aggiornamento di HostScan versione 4.10.07073 alla versione 5.1.2.42 di Secure Firewall Posture su un terminale specifico, con DAP (scenario3). Più DAP (Azione: Continua) corrispondenti) configurati in HostScan 4.10.07073.



Attenzione: il comportamento può dipendere dalla versione di Secure Firewall Posture/Cisco Secure Client, quindi accertarsi di controllare le note sulla versione più recenti per ciascuna versione.

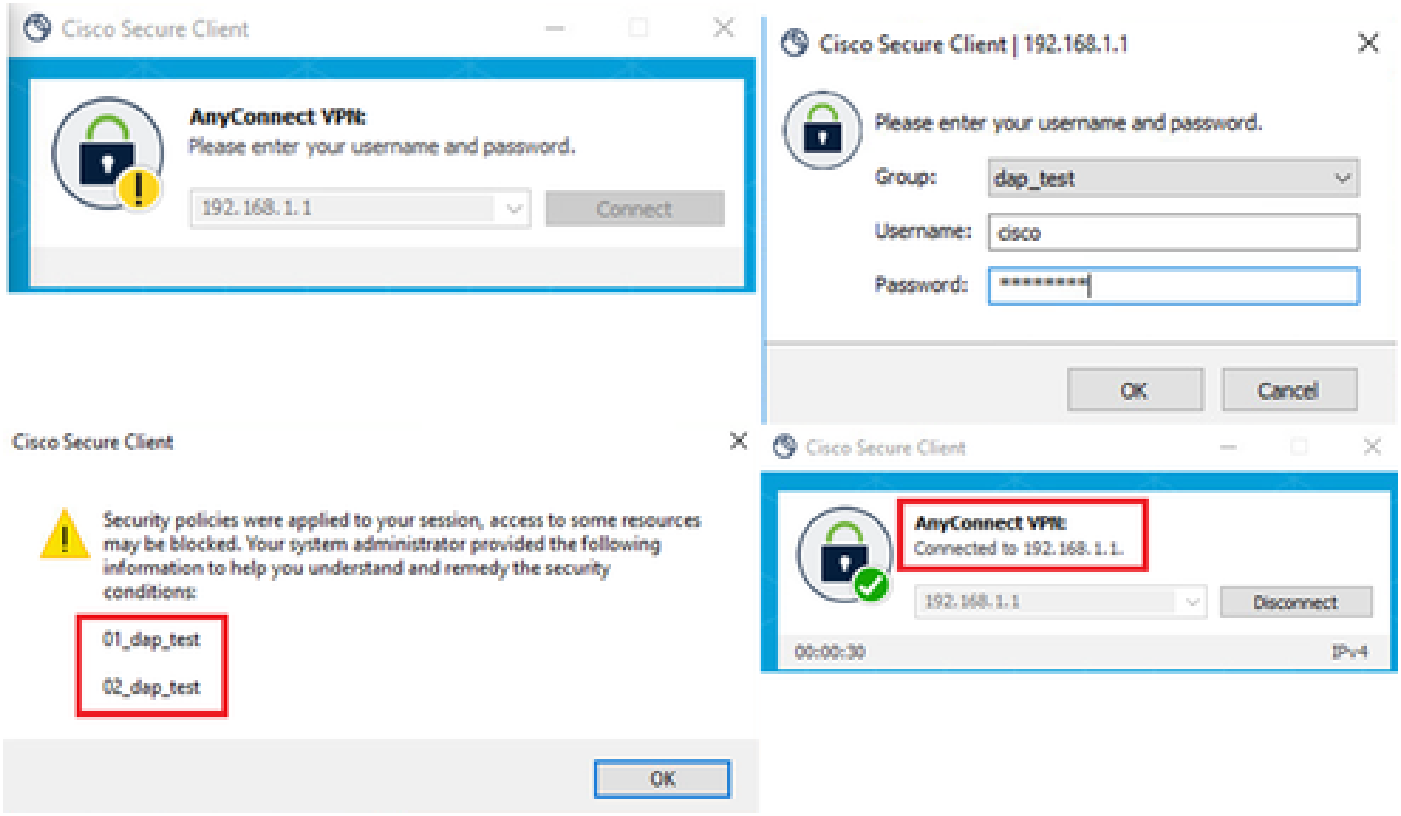
Versione immagine configurata sul lato ASA:

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

Versione immagine sul dispositivo di destinazione:

Versione immagine sul dispositivo

Esempio di connessione Cisco Secure Client:



Cisco Secure Client Connection

D: Cisco Secure Client 5.x funziona correttamente in combinazione con HostScan 4.x?

R: No. La combinazione di Cisco Secure Client 5.x e HostScan 4.x non è supportata.

D: Quando si esegue l'aggiornamento da HostScan 4.x a Secure Firewall Posture 5.x, è possibile eseguire l'aggiornamento solo su determinati dispositivi?

R: Sì. È possibile aggiornare dispositivi specifici utilizzando il metodo 2 indicato.

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).