Atualizar do HostScan para a postura de firewall seguro no Windows

Contents

Introdução

Este documento descreve o procedimento de atualização do HostScan para a Postura de Firewall Seguro (anteriormente, HostScan) no Windows.

Pré-requisitos

Requisitos

A Cisco recomenda ter conhecimento deste tópico:

- Configuração do Cisco Anyconnect e Hostscan

Componentes Utilizados

As informações neste documento são baseadas nestas versões de 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
- Secure Firewall Posture 5.1.2.42

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

Esta imagem mostra a topologia usada para o exemplo deste documento.

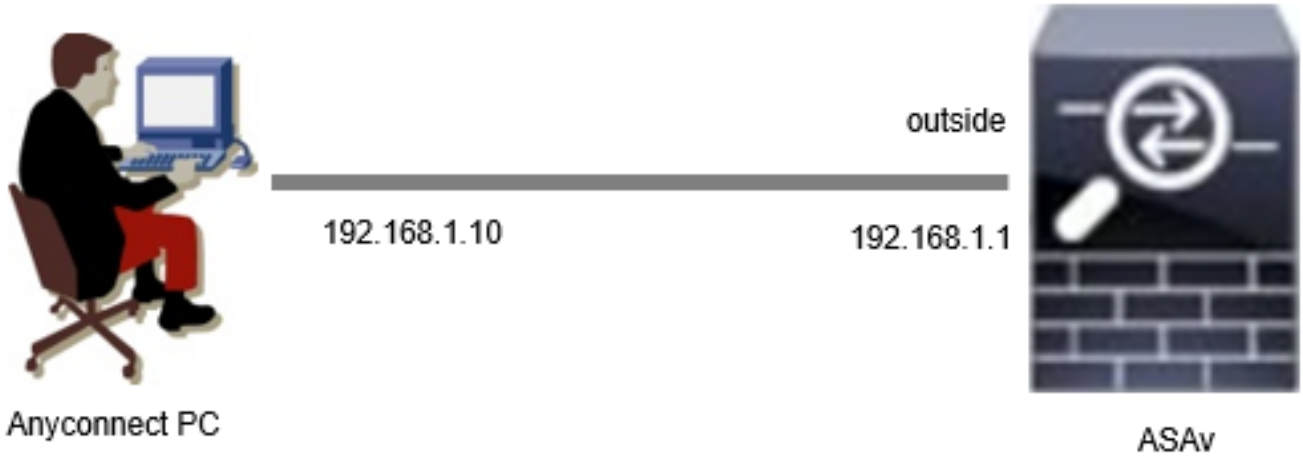


Diagrama de Rede

Configurações

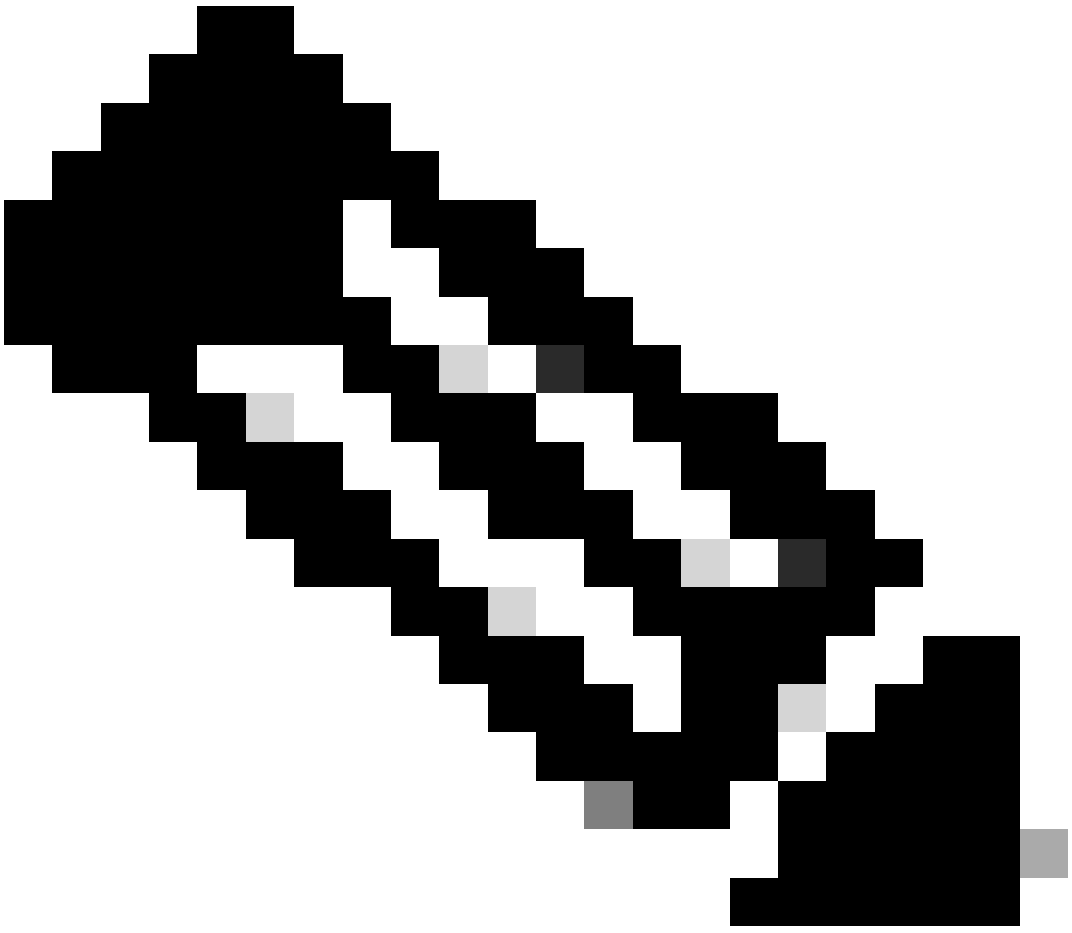
Essa é a configuração mínima no ASA CLI.

```
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
```

Atualização

Este documento fornece um exemplo de como atualizar o AnyConnect HostScan versão 4.10.07073 para o Secure Firewall Posture versão 5.1.2.42, em conjunto com a atualização do Cisco Secure Client (antigo Cisco AnyConnect Secure Mobility Client).



Observação: a Cisco recomenda que você execute a versão mais recente do Secure Firewall Posture (que é a mesma versão do Cisco Secure Client).

Método 1. Implantação no ASA

Etapa 1. Fazer download do arquivo de imagem

Faça o download dos arquivos de imagem do Cisco Secure Client e Secure Firewall Posture no Download de Software.

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

Etapa 2. Transferir arquivo de imagem para o ASA Flash

Neste exemplo, use a CLI do ASA para transferir os arquivos de imagem de um servidor HTTP para a flash do 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
```

Etapa 3. Especificar arquivo de imagem do ASA CLI

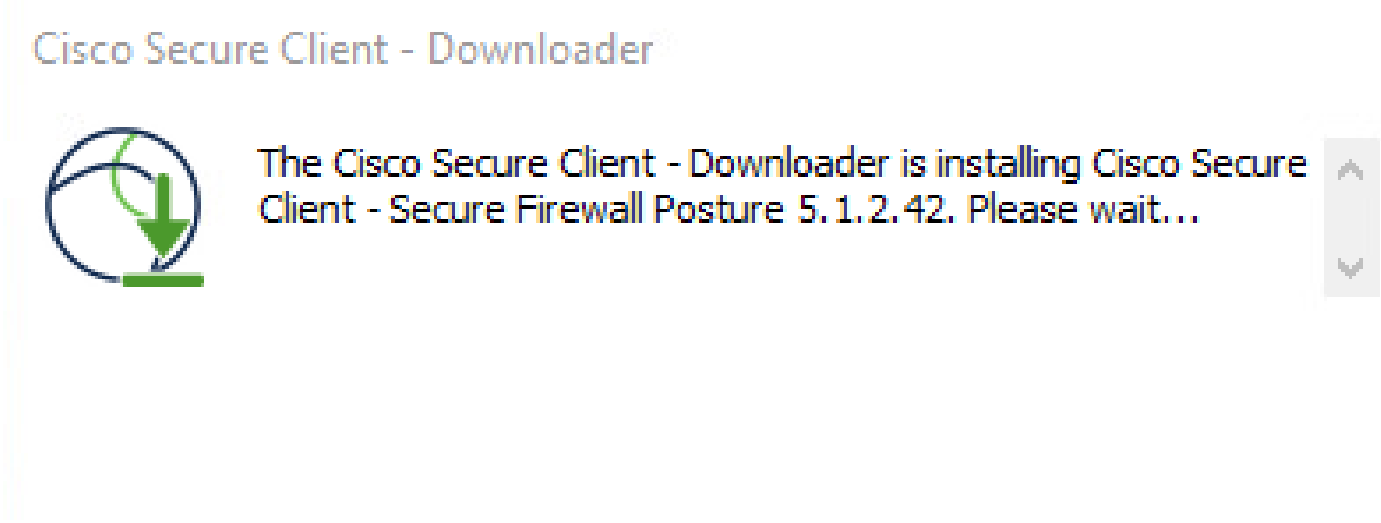
Especifique os novos arquivos de imagem usados para a conexão do Cisco Secure Client no ASA CLI.

```
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
```

Etapa 4. Atualizar automaticamente

Tanto o Cisco Secure Client quanto o Secure Firewall Posture podem ser atualizados automaticamente na próxima vez que o cliente se conectar.

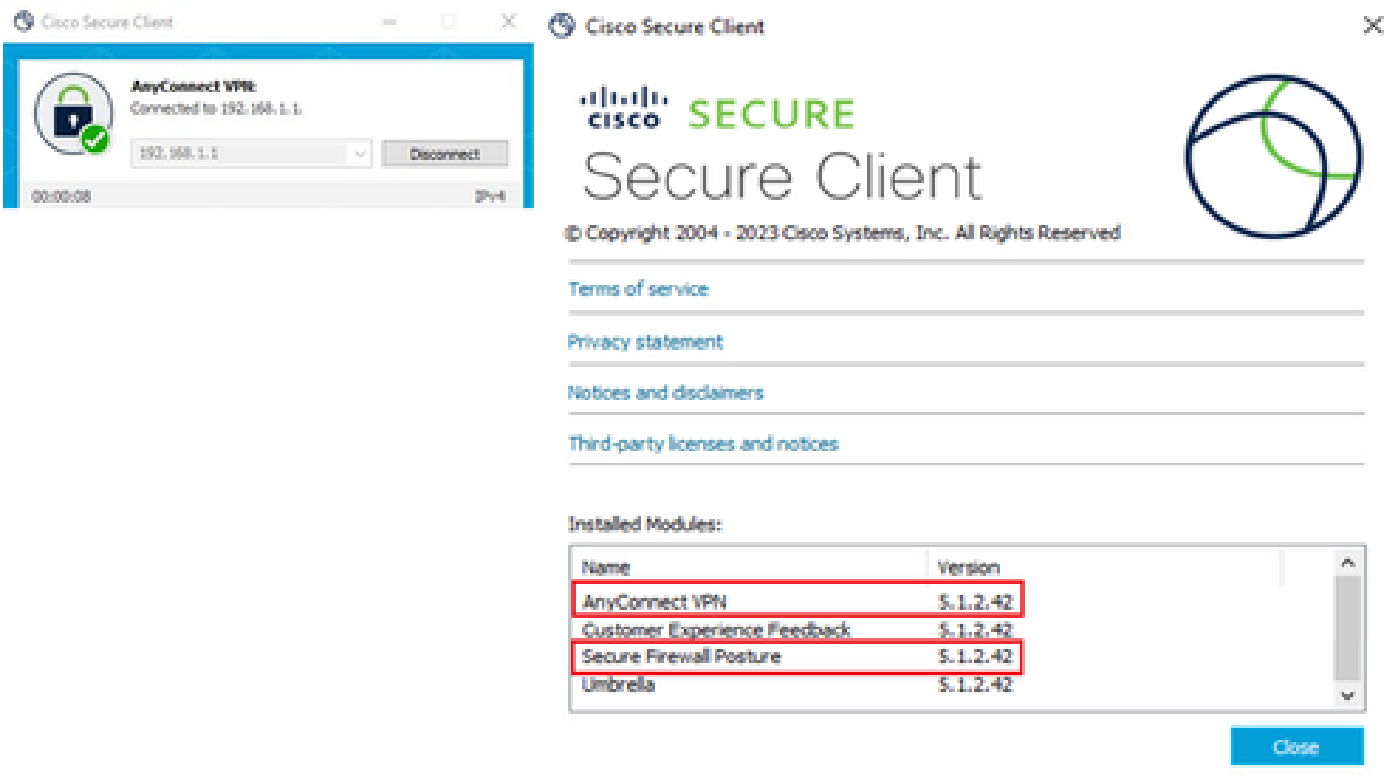
O módulo Secure Firewall Posture é atualizado automaticamente conforme mostrado na imagem.



Atualizar automaticamente

Etapa 5. Confirmar nova versão

Confirme se o Cisco Secure Client e o Secure Firewall Posture foram atualizados com êxito, conforme mostrado na imagem.



Nova versão

Método 2. Instalar no lado do cliente

Etapa 1. Baixar instalador

Faça o download do instalador em Download de software.

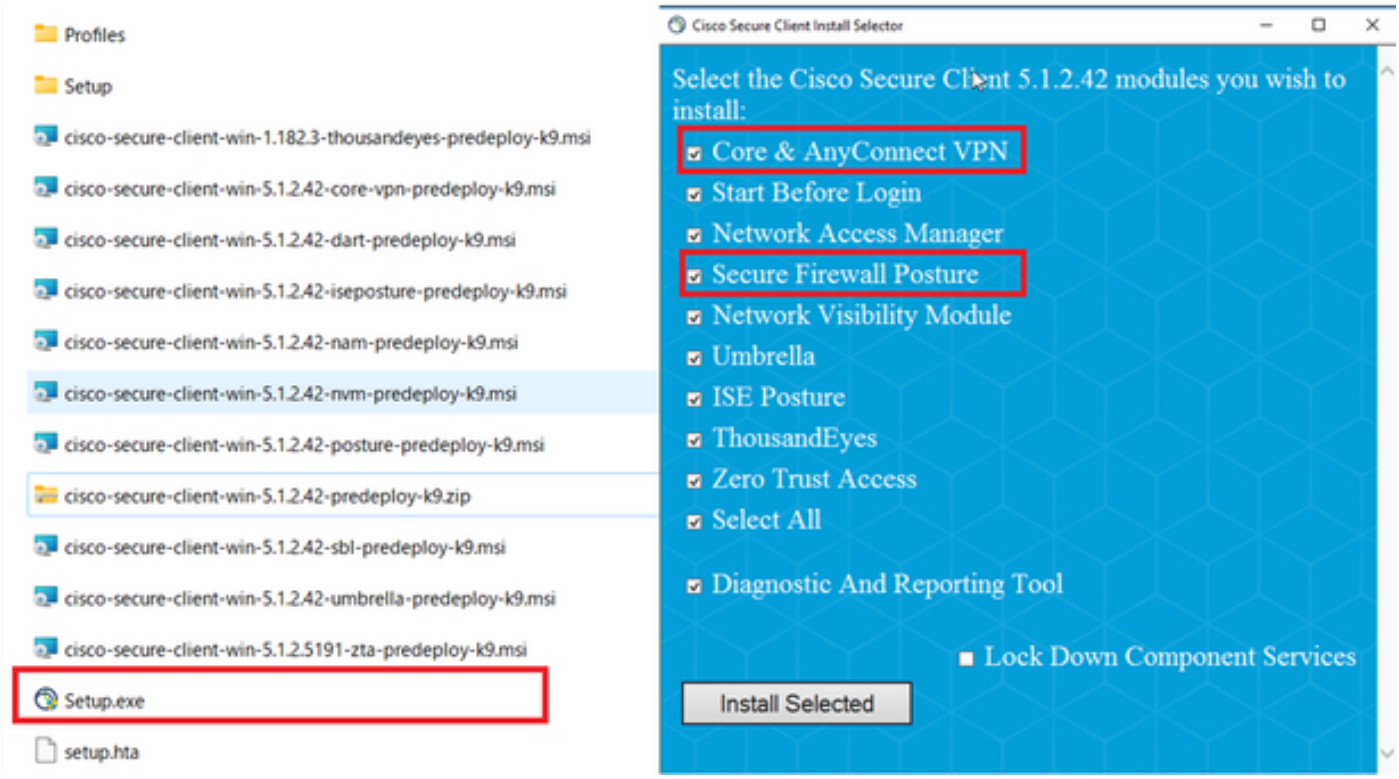
- cisco-secure-client-win-5.1.2.42-predeploy-k9.zip

Etapa 2. Transferir instalador para dispositivo de destino

Transfira o instalador baixado para o dispositivo de destino usando métodos como FTP (File Transfer Protocol), uma unidade USB ou outros métodos.

Etapa 3. Executar instalador

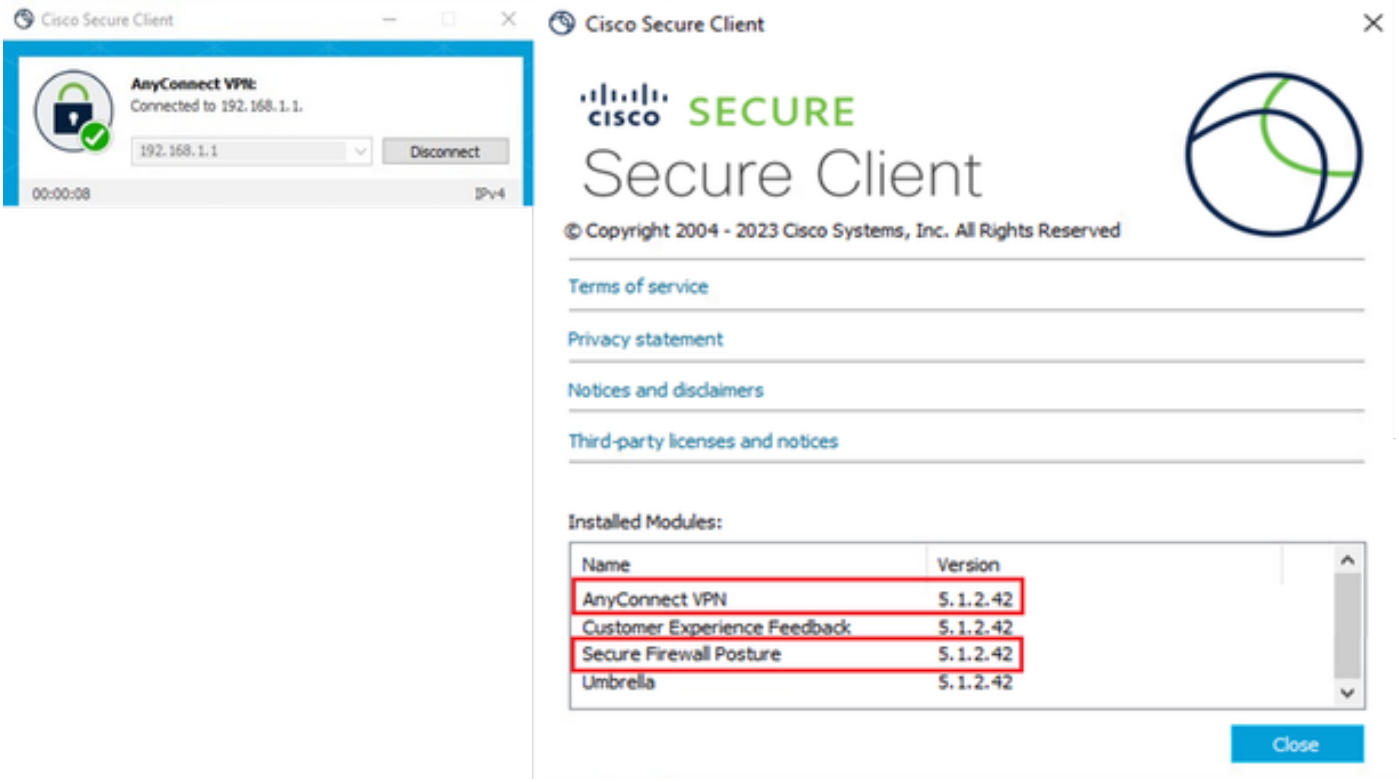
No dispositivo de destino, extraia os arquivos compactados e execute o Setup.exe.



Executar instalador

Etapa 4. Confirmar nova versão

Confirme se o Cisco Secure Client e o Secure Firewall Posture foram atualizados com êxito, conforme mostrado na imagem.

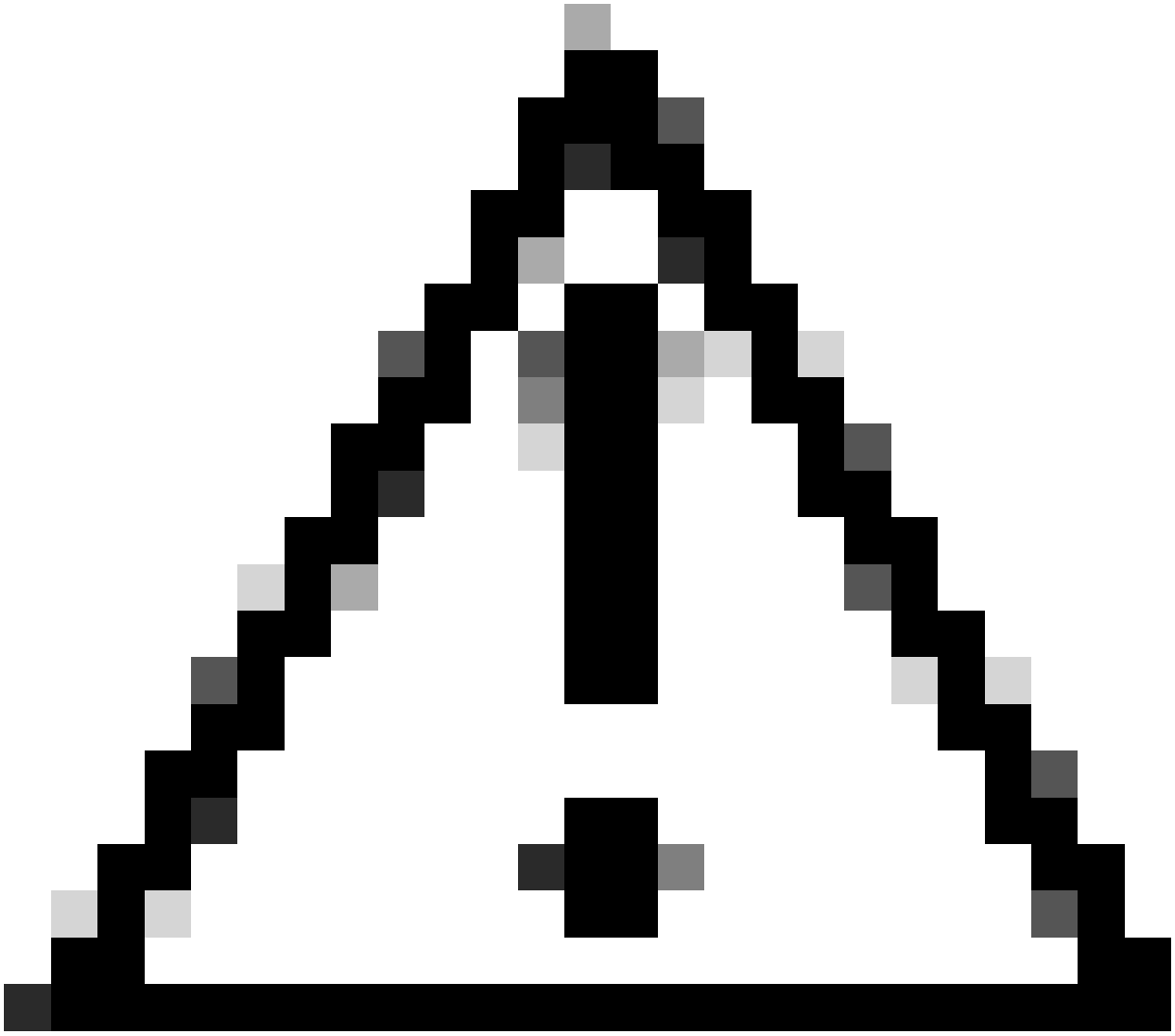


Nova versão

Perguntas frequentes

P: Se a versão do Secure Firewall Posture (anteriormente HostScan) especificada no ASA for mais antiga que a versão instalada no terminal, ela ainda funcionará corretamente?

R: Sim. Este é um exemplo de verificação operacional após a atualização do HostScan versão 4.10.07073 para Secure Firewall Posture versão 5.1.2.42 em um terminal específico, com DAP (Cenário3. Vários DAPs (Ação : Continuar) são correspondidos) configurados no HostScan 4.10.07073.



Cuidado: o comportamento pode depender da versão do Secure Firewall Posture/Cisco Secure Client, portanto verifique as notas de versão mais recentes de cada versão.

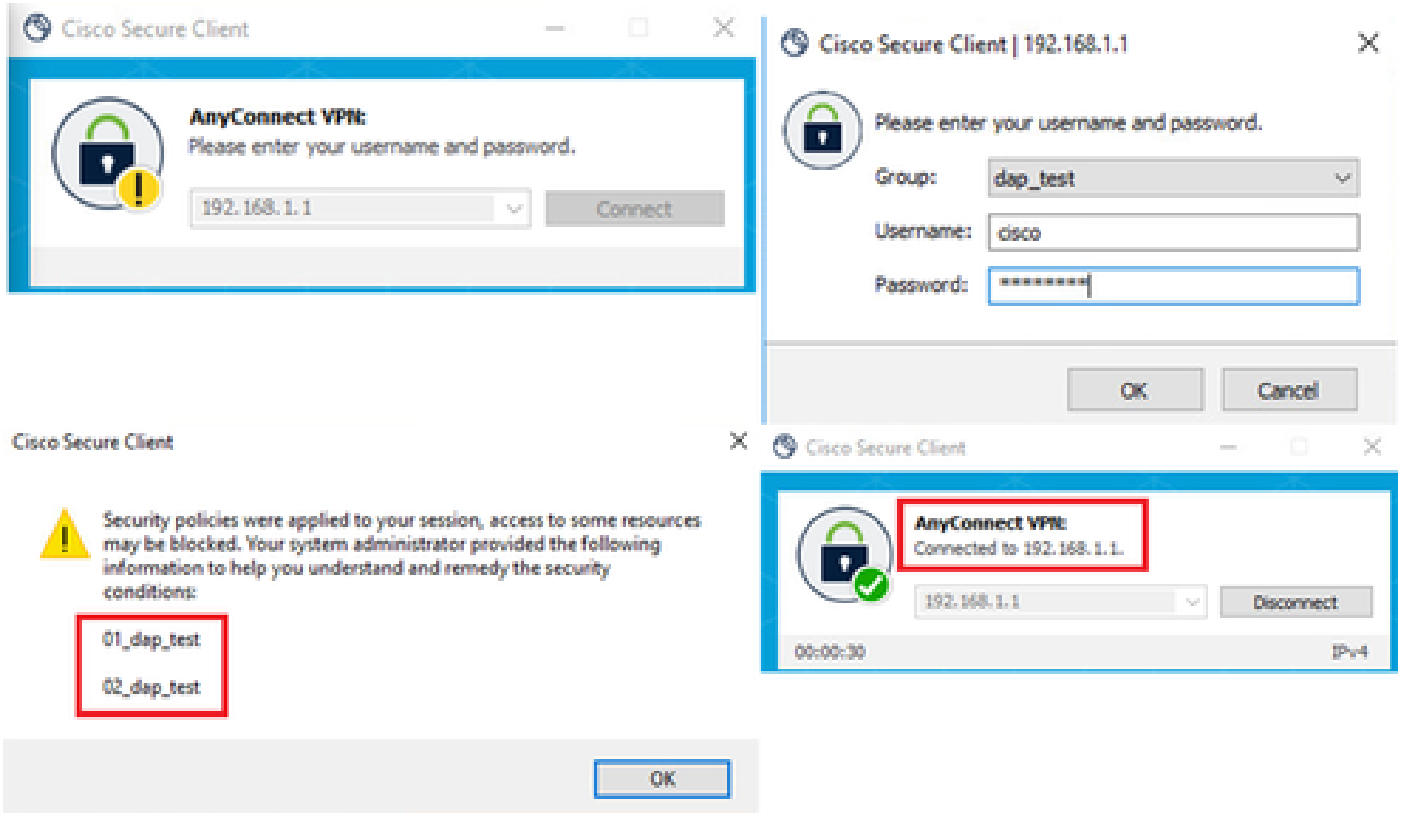
Versão da imagem configurada no ASA:

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

Versão da imagem no dispositivo de destino:

Versão da Imagem no Dispositivo

Exemplo de conexão do Cisco Secure Client :



Cisco Secure Client Connection

P: O Cisco Secure Client 5.x funciona corretamente em combinação com o HostScan 4.x?

R: Não. Não há suporte para a combinação do Cisco Secure Client 5.x e do HostScan 4.x.

P: Ao atualizar do HostScan 4.x para o Secure Firewall Posture 5.x, é possível atualizar somente em determinados dispositivos?

R: Sim. Você pode atualizar dispositivos específicos usando o Método 2 mencionado.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.