Windowsでホストスキャンからセキュアファイアウォールポスチャへのアップグレード

内容

はじめに

このドキュメントでは、WindowsでHostScanからセキュアファイアウォールポスチャ（以前のHostScan）にアップグレードする手順について説明します。

前提条件

要件

次の項目に関する専門知識があることが推奨されます。

- Cisco Anyconnectとホストスキャンの設定

使用するコンポーネント

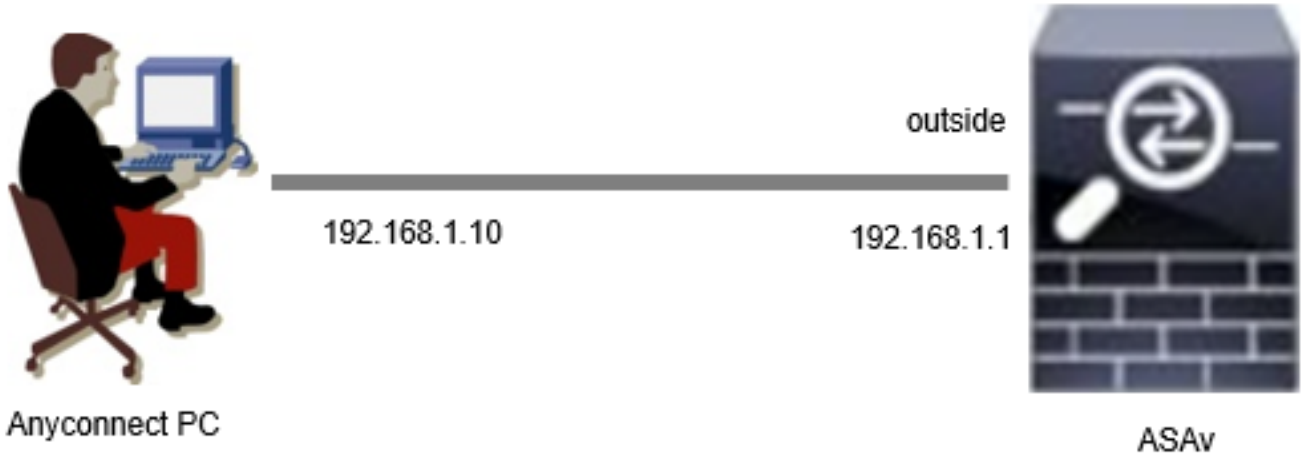
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco適応型セキュリティ仮想アプライアンス9.18(4)
- Cisco Adaptive Security Device Manager(ASDM)7.20(1)
- Cisco AnyConnect セキュア モビリティ クライアント 4.10.07073
- AnyConnectホストスキャン4.10.07073
- Cisco Secureクライアント5.1.2.42
- セキュアなファイアウォールポスチャ5.1.2.42

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。



ネットワーク図

コンフィギュレーション

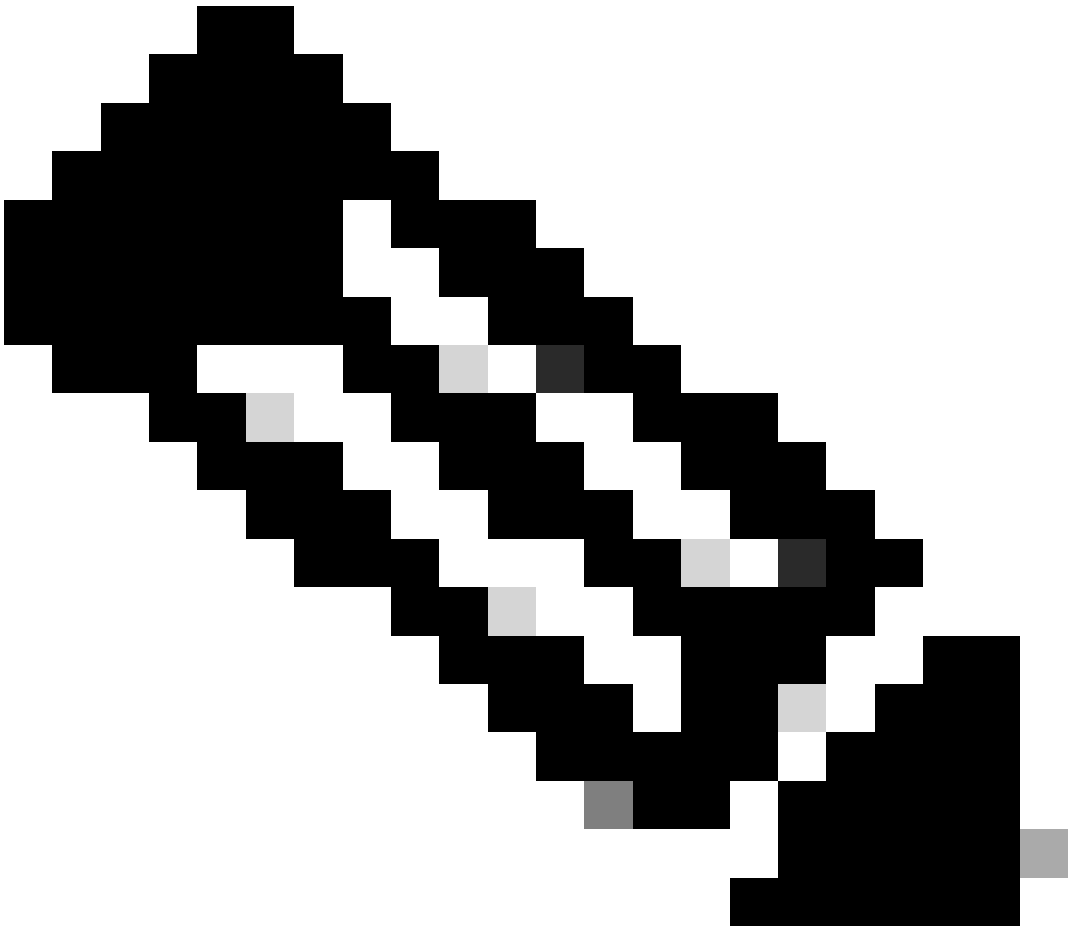
これは、ASA CLIでの最小限の設定です。

```
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
```

アップグレード

このドキュメントでは、Cisco Secure Client（旧称Cisco AnyConnectセキュアモビリティクライアント）のアップグレードとともに、AnyConnect HostScanバージョン4.10.07073からセキュアファイアウォールポスチャバージョン5.1.2.42にアップグレードする方法の例を示します。



注：シスコでは、最新バージョンのSecure Firewall Posture（Cisco Secure Clientと同じバージョン）を実行することを推奨しています。

方式 1.ASA側での導入

ステップ 1：イメージファイルのダウンロード

ソフトウェアのダウンロードから、Cisco Secure ClientおよびSecure Firewall Postureのイメージファイルをダウンロードします。

- Cisco Secure Client:cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
- セキュアファイアウォールポスチャ：secure-firewall-posture-5.1.2.42-k9.pkg

ステップ 2：ASAフラッシュへのイメージファイルの転送

この例では、ASA CLIを使用して、HTTPサーバからASAフラッシュにイメージファイルを転送します。

```
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
```

ステップ 3：ASA CLIからのイメージファイルの指定

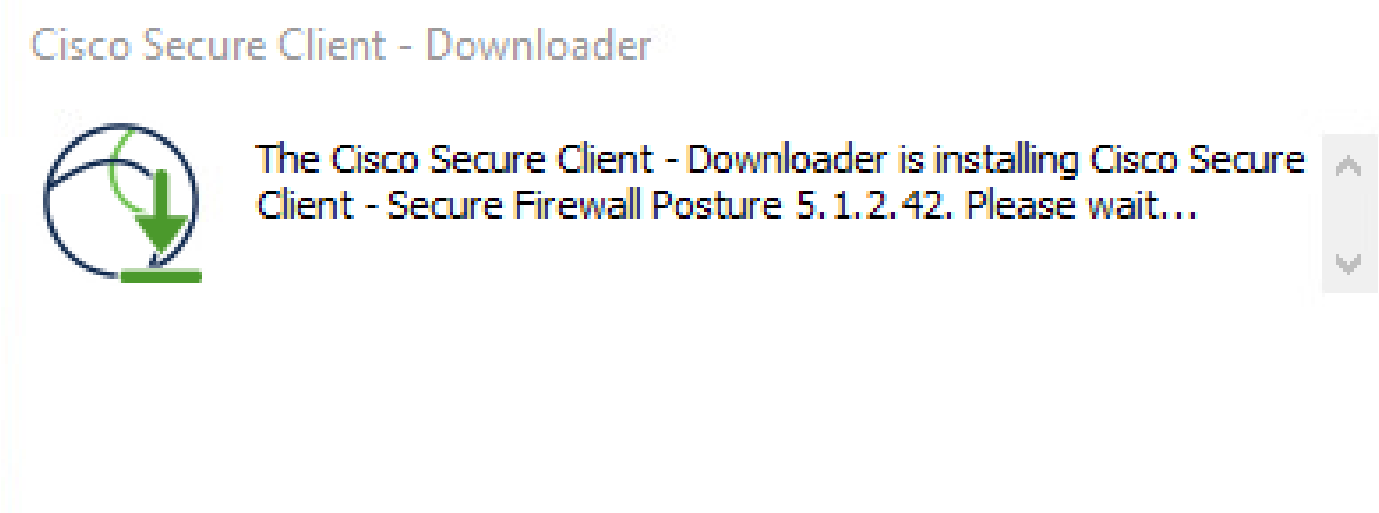
ASA CLIでCisco Secure Client接続に使用する新しいイメージファイルを指定します。

```
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
```

ステップ 4：自動アップグレード

Cisco Secure ClientとSecure Firewall Postureは、どちらも次回クライアントが接続したときに自動的に更新されます。

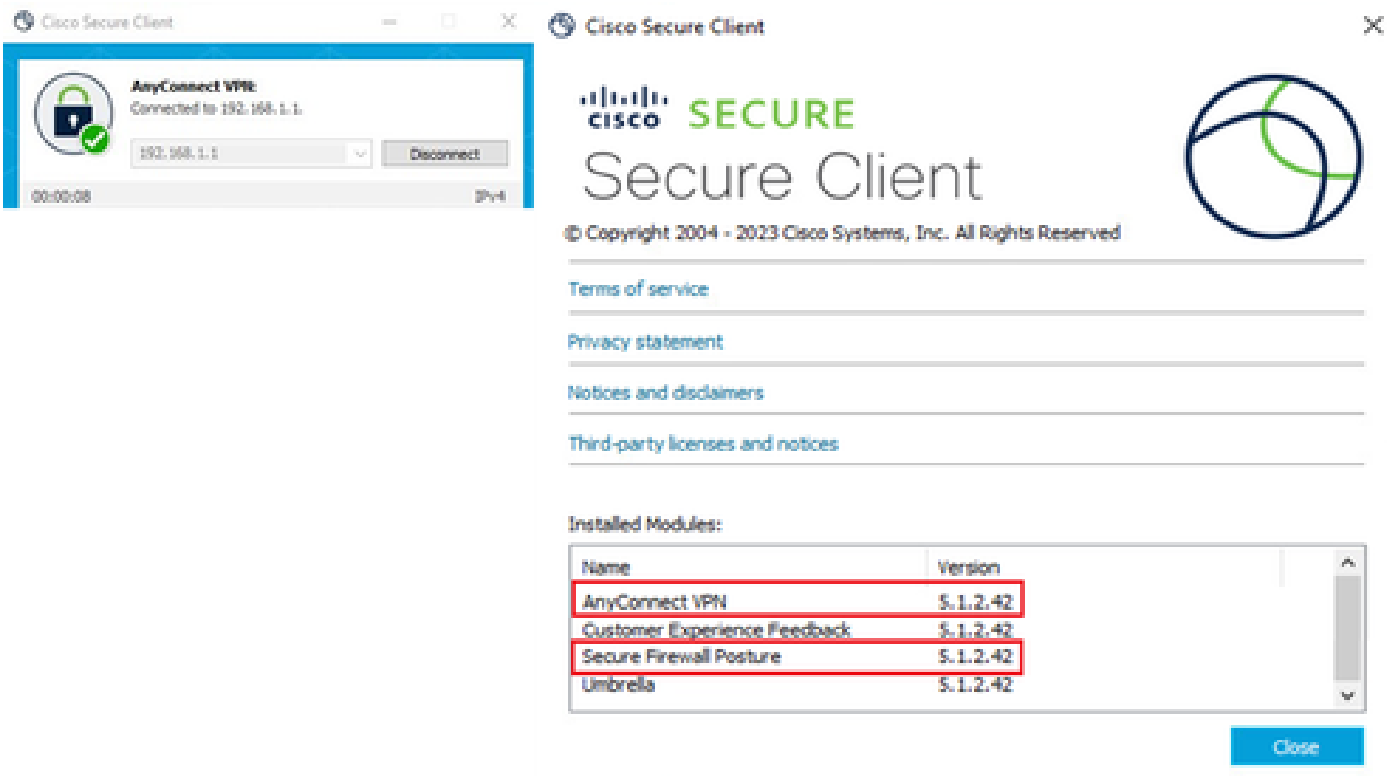
セキュアファイアウォールポスチャモジュールは、図に示すように自動的にアップグレードされます。



自動アップグレード

ステップ 5：新しいバージョンの確認

図に示すように、Cisco Secure ClientとSecure Firewall Postureが正常にアップグレードされたことを確認します。



新バージョン

方式 2.クライアント側でのインストール

ステップ 1：インストーラのダウンロード

ソフトウェアダウンロードからインストーラをダウンロードします。

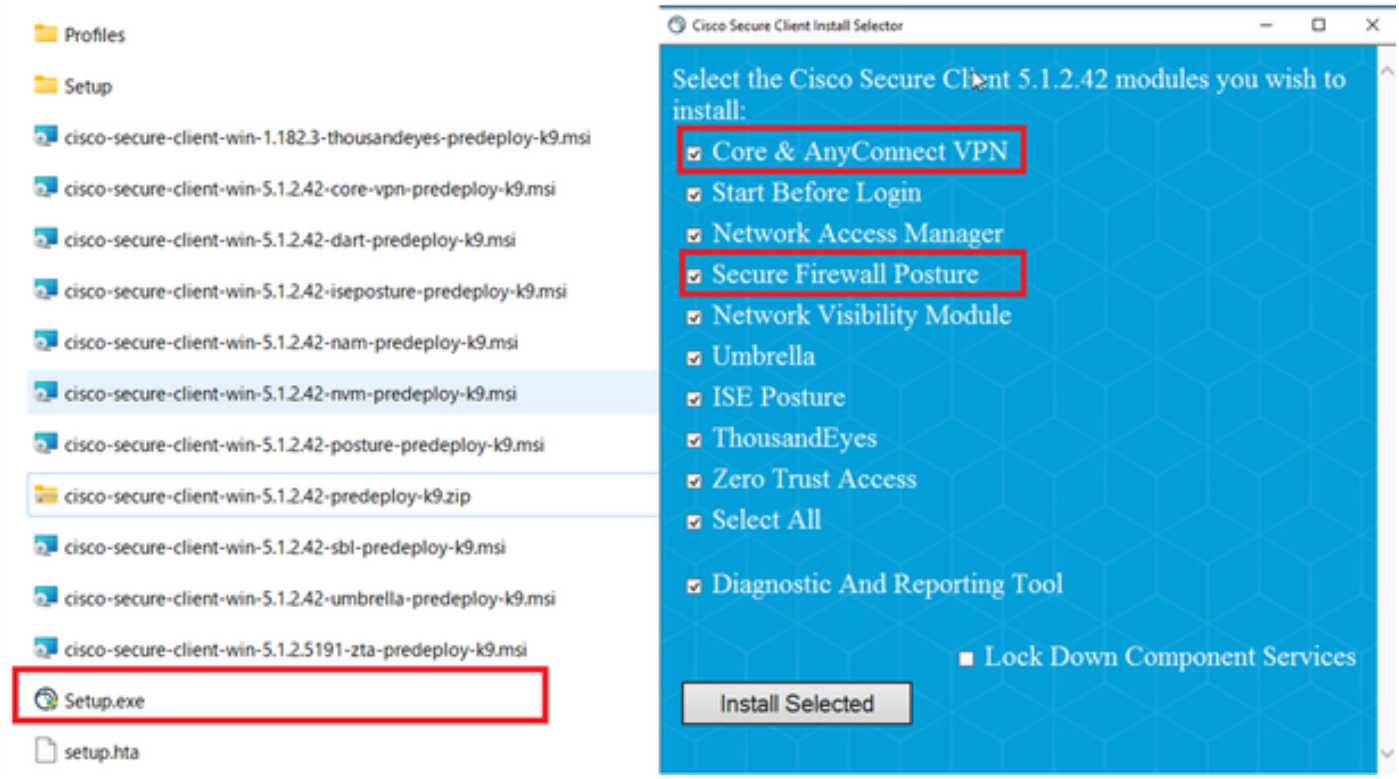
- cisco-secure-client-win-5.1.2.42-predeploy-k9.zip

ステップ 2：ターゲットデバイスへのインストーラの転送

FTP（ファイル転送プロトコル）、USBドライブ、またはその他の方法を使用して、ダウンロードしたインストーラをターゲットデバイスに転送します。

ステップ 3：インストーラの実行

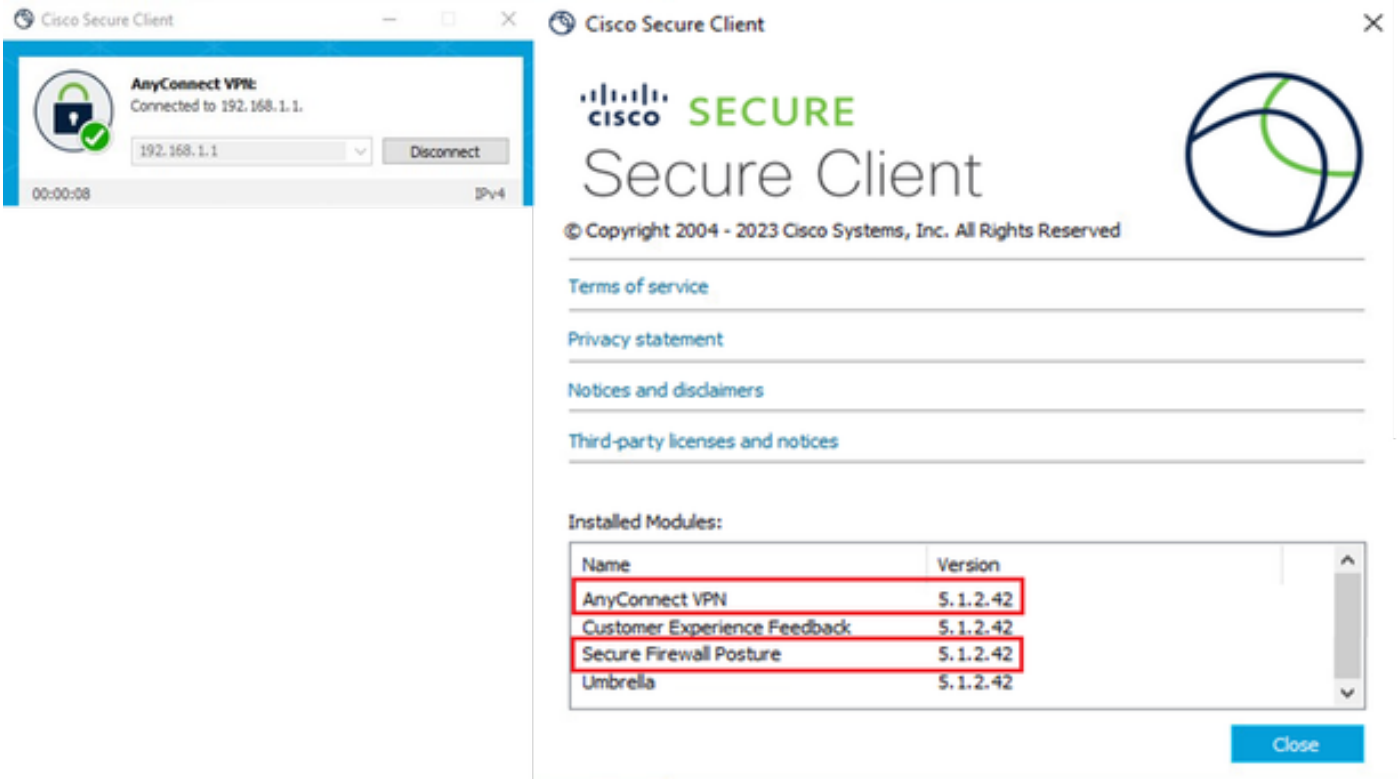
ターゲットデバイスで、圧縮ファイルを展開し、Setup.exeを実行します。



インストーラの実行

ステップ 4：新しいバージョンの確認

図に示すように、Cisco Secure ClientとSecure Firewall Postureが正常にアップグレードされたことを確認します。

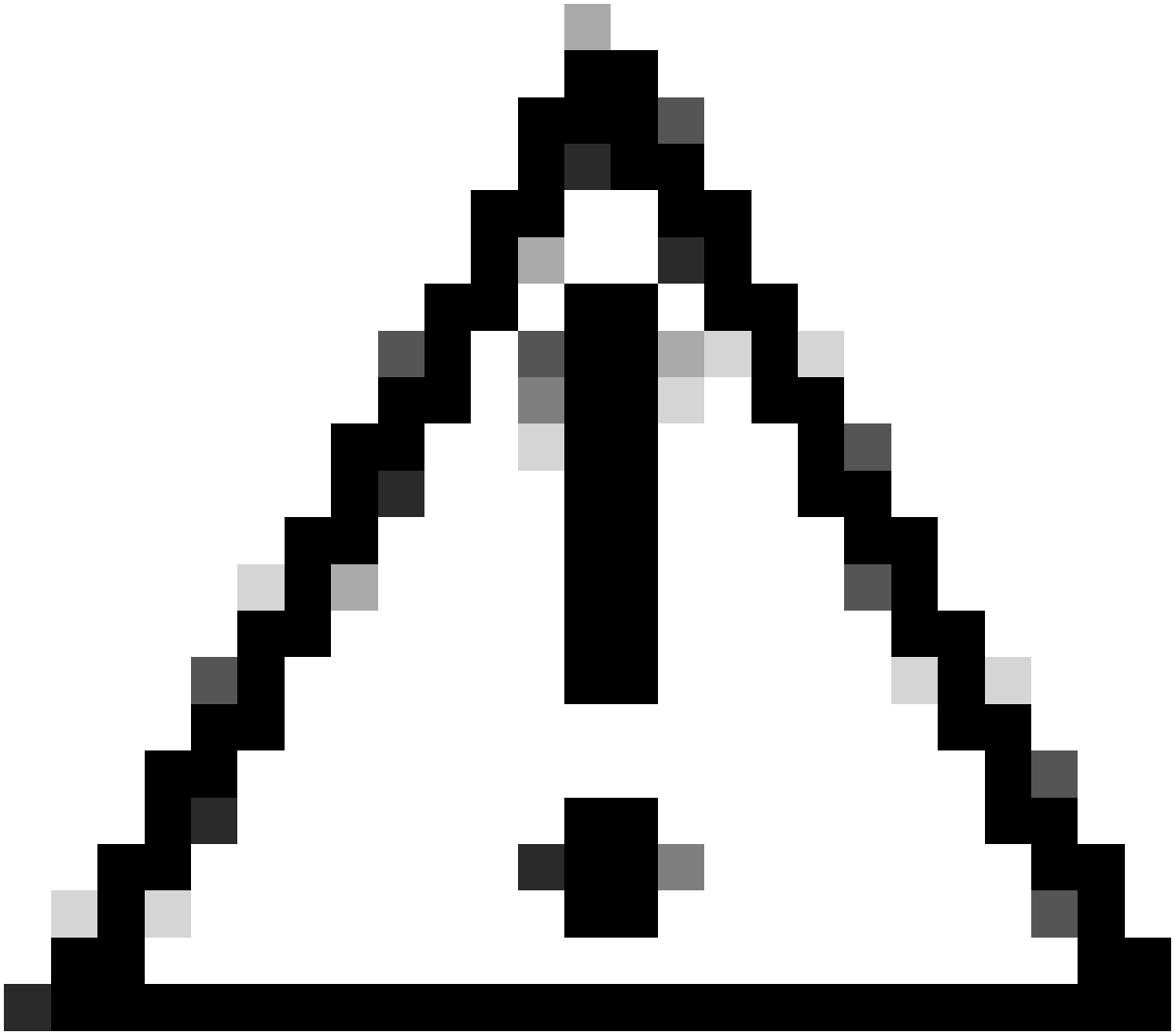


新バージョン

よく寄せられる質問（FAQ）

Q:ASA側で指定されているSecure Firewall Posture（以前のHostScan）のバージョンが、端末にインストールされているバージョンよりも古い場合、正しく動作しますか。

A：はい。次に、DAP(シナリオ3)を使用して特定の端末でHostScanバージョン4.10.07073をセキュアファイアウォールポスチャバージョン5.1.2.42にアップグレードした後の動作確認の例を示します。HostScan 4.10.07073で複数のDAP(Action:Continue)が一致)が設定されている。



注意：動作はSecure Firewall Posture/Cisco Secure Clientのバージョンによって異なる可能性があるため、各バージョンの最新のリリースノートを必ず確認してください。

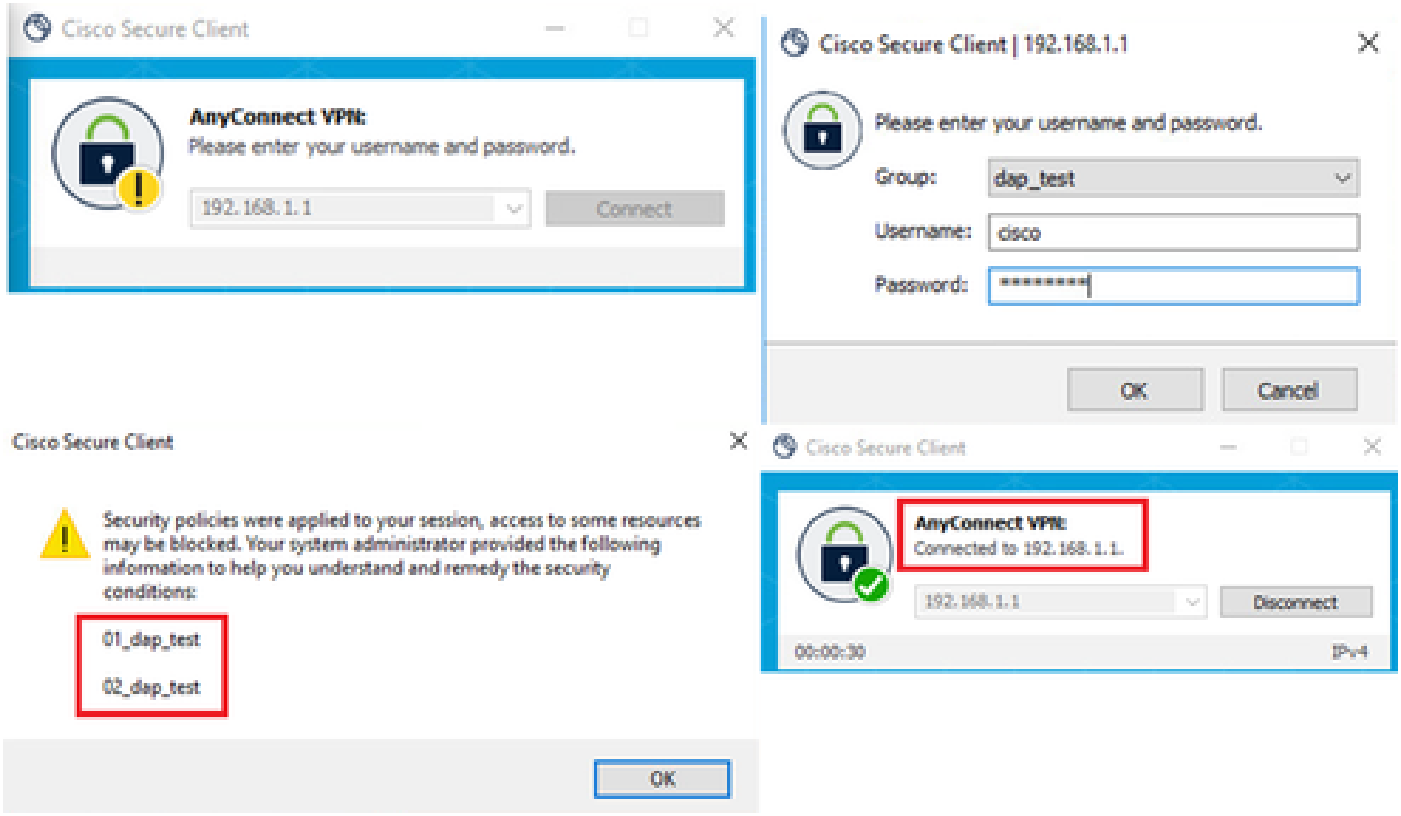
ASA側で設定されているイメージバージョン：

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

ターゲットデバイス上のイメージバージョン：

デバイスのイメージバージョン

Cisco Secure Client接続の例：



Cisco Secureクライアント接続

Q:Cisco Secure Client 5.xはHostScan 4.xと組み合わせて正しく動作しますか。

A：いいえ。Cisco Secure Client 5.xとHostScan 4.xの組み合わせはサポートされていません。

Q:HostScan 4.xからSecure Firewallポスチャ5.xにアップグレードする際、特定のデバイス上でのみアップグレードできますか。

A：はい。前述の方法2を使用して、特定のデバイスをアップグレードできます。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。