



セキュアクライアント HostScan

AnyConnect ポスチャモジュールにより、セキュアクライアントは、ホストにインストールされているオペレーティングシステム、アンチマルウェア、ファイアウォールの各ソフトウェアを識別できます。この情報は、HostScan アプリケーションによって収集されます。ポスチャアセスメントでは、ホストに HostScan がインストールされている必要があります。

- [HostScan/Secure Firewall ポスチャの前提条件](#) (1 ページ)
- [HostScan のライセンス](#) (2 ページ)
- [HostScan パッケージ](#) (2 ページ)
- [HostScan/Secure Firewall ポスチャのインストールまたはアップグレード](#) (2 ページ)
- [HostScan の有効化または無効化](#) (3 ページ)
- [ASA で有効になっている HostScan/Secure Firewall ポスチャバージョンの表示](#) (4 ページ)
- [HostScan/Secure Firewall ポスチャのアンインストール](#) (5 ページ)
- [グループポリシーへの セキュアクライアント 機能モジュールの割り当て](#) (6 ページ)
- [HostScan/Secure Firewall ポスチャ関連資料](#) (7 ページ)

HostScan/Secure Firewall ポスチャの前提条件

セキュアクライアントを Secure Firewall Posture/HostScan モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

SCEP 認証機能を使用するには、Secure Firewall Posture/HostScan をインストールする必要があります。

Secure Firewall Posture/HostScan のインストールでサポートされるオペレーティングシステムについては、『[Supported VPN Platforms, Cisco ASA Series](#)』を参照してください。

HostScan のライセンス

次に、HostScan の セキュアクライアント ライセンス要件を示します。

- AnyConnect Apex
- AnyConnect VPN Only

HostScan パッケージ

HostScan パッケージを ASA にスタンドアロンパッケージ **hostscan-version.pkg** としてロードすることができます。このファイルには、HostScan ソフトウェアとともに、HostScan ライブラリおよびサポート表が含まれています。

HostScan/Secure Firewall ポスチャのインストールまたはアップグレード

この手順では、ASA のコマンドライン インターフェイスを使用して HostScan または Secure Firewall ポスチャパッケージをインストールまたはアップグレードし、有効にします。

始める前に



- (注) HostScan バージョン 4.3.x 以前から 4.6.x 以降にアップグレードしようとしている場合、以前に確立した既存の AV/AS/FW DAP ポリシーおよび LUA スクリプトがすべて HostScan 4.6.x 以降と非互換であるという事実に起因するエラー メッセージが表示されます。

設定を適応させるために実行する必要があるワнтаイム移行手順が存在します。この手順では、このダイアログボックスを閉じて、この設定を保存する前に HostScan 4.4.x と互換になるように設定を移行します。この手順を中止し、『[セキュアクライアント HostScan 4.3.x to 4.6.x Migration Guide](#)』で詳細な手順を参照してください。つまり、移行するには ASDM DAP のポリシーページに移動して、互換性のない AV/AS/FW 属性を確認して手動で削除してから、LUA スクリプトを確認し、書き換える必要があります。

- ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。
- `secure-firewall-posture-version-k9.pkg` を ASA にアップロードします。HostScan 4.x バージョンを使用している場合は、`hostscan_version-k9.pkg` ファイルをアップロードする必要があります。

手順

ステップ 1 webvpn コンフィギュレーション モードを開始します。

例：

```
hostname(config)# webvpn
```

ステップ 2 ASDM を開いて [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [Cisco Secure Firewall用ポスチャ (Posture (for Secure Firewall))] > [ポスチャイメージ (Posture Image)] を選択します。HostScan 4.x バージョンを使用している場合、パスは [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [Secure Desktop Manager] > [ホストスキャンイメージ (Host Scan Image)] になります。

ステップ 3 HostScan/Secure Firewall ポスチャイメージとして指定するパッケージのパスを指定します。スタンドアロンのパッケージ、またはセキュアクライアント パッケージを指定することができます。

hostscan image path

例：

HostScan 4.x バージョンを使用している場合は、

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081.pkg
```

Secure Firewall ポスチャ 5.x バージョンを使用している場合は、

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture5.0.00556.pkg
```

ステップ 4 前の手順で指定した HostScan/Secure Firewall ポスチャイメージを有効にします。

例：

```
ASAName(webvpn)#hostscan enable
```

ステップ 5 実行コンフィギュレーションをフラッシュメモリに保存します。新しいコンフィギュレーションがフラッシュメモリに正常に保存されると、[OK] メッセージが表示されます。

例：

```
hostname(webvpn)# write memory
```

ステップ 6

HostScan の有効化または無効化

これらのコマンドは、ASA のコマンドライン インターフェイスを使用して、インストール済みの HostScan イメージを有効または無効にします。

始める前に

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。

手順

ステップ 1 `webvpn` コンフィギュレーション モードを開始します。

例 :

`webvpn`

ステップ 2 ASA からスタンドアロンの HostScan イメージがアンインストールされていない場合、このイメージを有効にします。

`hostscan enable`

ステップ 3 インストールされているすべての HostScan パッケージの HostScan を無効にします。

(注)

有効になっている HostScan イメージをアンインストールする前に、このコマンドを使用して、HostScan を無効にする必要があります。

`no hostscan enable`

ASA で有効になっている HostScan/Secure Firewall ポスチャバージョンの表示

この手順では、ASA のコマンドライン インターフェイスを使用して、有効になっている HostScan/Secure Firewall ポスチャのバージョンを特定します。

始める前に

ASA にログインし、特権 EXEC モードを開始します。ASA の特権 EXEC モードでは、表示されるプロンプトは `hostname#` となります。

手順

ASA で有効になっている HostScan/Secure Firewall ポスチャバージョンを表示します。

`show webvpn hostscan`

HostScan/Secure Firewall ポスチャのアンインストール

HostScan/Secure Firewall ポスチャパッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、HostScan/Secure Firewall ポスチャが有効になっている場合でも ASA による HostScan/Secure Firewall ポスチャパッケージの展開が回避されます。HostScan/Secure Firewall ポスチャをアンインストールしても、HostScan/Secure Firewall ポスチャパッケージはフラッシュドライブから削除されません。

始める前に

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。

手順

ステップ 1 webvpn コンフィギュレーション モードを開始します。

webvpn

ステップ 2 アンインストールする HostScan/Secure Firewall ポスチャイメージを無効にします。

no hostscanenable

ステップ 3 アンインストールする HostScan/Secure Firewall ポスチャイメージのパスを指定します。スタンドアロンのパッケージが HostScan/Secure Firewall ポスチャパッケージとして指定されている場合があります。

no hostscan image path

例 :

HostScan 4.x バージョンを使用している場合は、

`ASAName (webvpn) #hostscan image disk0:/hostscan_4.10.06081-k9.pkg`

Secure Firewall ポスチャ 5.x バージョンを使用している場合は、

`ASAName (webvpn) #hostscan image disk0:/secure-firewall-posture-5.0.00556-k9.pkg`

ステップ 4 実行コンフィギュレーションをフラッシュメモリに保存します。新しいコンフィギュレーションがフラッシュメモリに正常に保存されると、[OK] メッセージが表示されます。

write memory

グループポリシーへの セキュアクライアント 機能モジュールの割り当て

次の手順で、セキュアクライアント機能モジュールとグループポリシーを関連付けます。VPN ユーザーが ASA に接続するときに、ASA はこれらのセキュアクライアント機能モジュールをエンドポイントコンピュータにダウンロードしてインストールします。

始める前に

ASA にログオンし、グローバル コンフィギュレーションモードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。

手順

ステップ 1 ネットワーク クライアント アクセス用の内部グループ ポリシーを追加します。

group-policy name internal

例 :

```
hostname(config)# group-policy PostureModuleGroup internal
```

ステップ 2 新しいグループ ポリシーを編集します。このコマンドを入力した後は、グループ ポリシー コンフィギュレーション モードのプロンプト `hostname(config-group-policy)#` が表示されます。

group-policy name attributes

例 :

```
hostname(config)# group-policy PostureModuleGroup attributes
```

ステップ 3 グループポリシー webvpn コンフィギュレーションモードを開始します。このコマンドを入力した後は、次に示す ASA のプロンプトが表示されます。 `hostname(config-group-webvpn)#`

webvpn

ステップ 4 グループ内のすべてのユーザーに セキュアクライアント 機能モジュールがダウンロードされるように、グループポリシーを設定します。

anyconnect modules value Secure Firewall モジュール 名

`anyconnect module` コマンドの `value` には、次の値の 1 つ以上を指定することができます。複数のモジュールを指定する場合は、値をカンマで区切ります。

値	Secure Firewall モジュール/機能名
dart	Secure Client DART (診断およびレポートツール)
vpngina	Secure Client SBL (ログイン前の起動)

値	Secure Firewall モジュール/機能名
ポスチャ	Secure Firewall ポスチャ/HostScan
nam	Secure Client ネットワーク アクセス マネージャ
none	グループ ポリシーからすべての AnyConnect モジュールを削除する場合に使用します。
profileMgmt	Secure Client 管理トンネル VPN

例：

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

モジュールの1つを削除するには、保持したいモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドは Web セキュリティ モジュールを削除します。

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

ステップ5 実行コンフィギュレーションをフラッシュ メモリに保存します。

新しいコンフィギュレーションが正常にフラッシュ メモリに保存されると、[OK] というメッセージが表示され、次に示す ASA のプロンプトが表示されます。hostname(config-group-webvpn)# write memory

HostScan/Secure Firewall ポスチャ関連資料

HostScan/Secure Firewall ポスチャがエンドポイントコンピュータからポスチャクレデンシャルを収集した後は、情報を活用するために、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらのトピックの詳細については、『[Cisco Adaptive Security Device Manager Configuration Guides](#)』を参照してください。また、セキュアクライアントでの HostScan/Secure Firewall ポスチャの動作の詳細については、『[Cisco Secure Client \(including AnyConnect\) Administrator Guide](#)』を参照してください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。