CHAPTER 80

AnyConnect ホスト スキャンの設定

[Configuration] > [Remote Access VPN] > [Host Scan Image]

AnyConnect ポスチャ モジュールにより、AnyConnect セキュア モビリティ 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、およびアンチウイルス、アンチスパイウェア、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、ホスト スキャン アプリケーションによって収集されます。

Adaptive Security Device Manager（ASDM）で Secure Desktop Manager ツールを使用すると、ホスト スキャンによって識別されるオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを評価するプリログイン ポリシーを作成できます。プリログイン ポリシーの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。

ホスト スキャン サポート表には、プリログイン ポリシーで使用するアンチウイルス、アンチスパイウェア、およびファイアウォール アプリケーションの製品名とバージョン情報が含まれます。シスコでは、ホスト スキャン パッケージにホスト スキャン、ホスト スキャン サポート表、および他のコンポーネントを含めて提供しています。

AnyConnect セキュア モビリティ クライアント リリース 3.0 以降では、ホスト スキャンは CSD とは別に使用できます。これは、CSD をインストールしなくてもホスト スキャンの機能を展開できることを意味します。また、最新のホスト スキャン パッケージに更新することで、ホスト スキャン サポート表を更新できます。

ポスチャ アセスメントおよび AnyConnect テレメトリ モジュールは、ホストにホスト スキャンがインストールされている必要があります。

この章の内容は、次のとおりです。

- 「ホスト スキャンの依存関係およびシステム要件」（P.80-1）
- 「ホスト スキャン パッケージ」（P.80-2）
- 「ASA 上でのホスト スキャンのインストールとイネーブル化」（P.80-3）
- 「ホスト スキャンに関するその他の重要なマニュアル」（P.80-8）

ホスト スキャンの依存関係およびシステム要件

依存関係

AnyConnect Secure Mobility Client をポスチャ 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

次の AnyConnect 機能は、ポスチャ モジュールをインストールする必要があります。

- SCEP 認証
- AnyConnect テレメトリ モジュール

システム要件

ポスチャ モジュールは、次のいずれかのプラットフォームにインストールできます。

- Windows XP（x86 版、および x64 環境で動作する x86 版）
- Windows Vista（x86 版、および x64 環境で動作する x86 版）
- Windows 7（x86 版、および x64 環境で動作する x86 版）
- Mac OS X 10.5、10.6（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Linux（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Windows Mobile

ライセンス

ポスチャ モジュールには、次の AnyConnect ライセンシング要件があります。

- 基本ホスト スキャン用の AnyConnect Premium。
- 次の場合は、Advanced Endpoint Assessment ライセンスが必要です。
  - 修復
  - モバイル デバイス管理

ホスト スキャン パッケージ

ASA へのホスト スキャン パッケージは次のいずれかの方法でロードできます。

- **hostscan-*version*.pkg** は、スタンドアロン パッケージとしてアップロードできます。
- **anyconnect-NGC-win-*version*-k9.pkg** は、AnyConnect セキュア モビリティをアップロードすることによって、アップロードできます。
- **csd_version-k9.pkg** は、Cisco Secure Desktop をアップロードすることによって、アップロードできます。

表 80-1　ASA にロードするホスト スキャン パッケージ

ファイル	説明
hostscan-*version*.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン ライブラリ、およびサポート表が含まれています。
anyconnect-NGC-win-*version*-k9.pkg	このパッケージには、hostscan-*version*.pkg ファイルなど、Cisco AnyConnect セキュア モビリティ クライアントのすべての機能が含まれています。
csd_*version*-k9.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン ライブラリ、サポート表など、Cisco Secure Desktop のすべての機能が含まれています。 この方式には、Cisco Secure Desktop 用の別個のライセンスが必要です。

ASA 上でのホスト スキャンのインストールとイネーブル化

次のタスクでは、ASA 上でのホスト スキャンのインストールとイネーブル化について説明します。

- ホスト スキャンのインストールまたはアップグレード
- ホスト スキャンのイネーブル化またはディセーブル化
- ASA でイネーブルになっているホスト スキャンのバージョンの表示
- ホスト スキャンのアンインストール
- グループ ポリシーへの AnyConnect フィーチャ モジュールの割り当て

ホスト スキャン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ホスト スキャン パッケージをインストールまたはアップグレードし、イネーブルにします。

前提条件

- 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。
- hostscan_version-k9.pkg ファイルまたは anyconnect-NGC-win-version-k9.pkg ファイルを ASA にアップロードします。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn** **例：** `hostname(config)# webvpn`	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**csd hostscan image** path **例：** `ASAName(webvpn)#`**`csd hostscan image disk0:/`***`hostscan-3.6.0-k9.pkg`*** `ASAName(webvpn)#`**`csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg`**	ホスト スキャン 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。ホスト スキャン パッケージとして、スタンドアロンのホスト スキャン パッケージ、または AnyConnect Secure Mobility Client パッケージを指定することができます。 **（注）** Windows、Linux、および Mac OS X のどのオペレーティング システムの場合も、anyconnect-NGC-win-*version*-k9.pkg ファイルをアップロードする必要があります。これは、エンドポイントがホスト スキャンをインストールできるようにするためです。
ステップ 3	**csd enable** **例：** `ASAName(webvpn)#`**`csd enable`**	前の手順で指定したホスト スキャン イメージをイネーブルにします。
ステップ 4	**write memory** **例：** `hostname(webvpn)# write memory`	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。

ホスト スキャンのイネーブル化またはディセーブル化

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ホスト スキャン イメージをイネーブルまたはディセーブルにします。

前提条件

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。

ホスト スキャンをイネーブルにするための詳細な手順

	コマンド	目的
ステップ 1	**webvpn** **例：** `hostname(config)# webvpn`	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**csd enable** **例：** `hostname(config)# csd enable`	スタンドアロンのホスト スキャン イメージ、または AnyConnect Secure Mobility Client パッケージの内のホスト スキャン イメージをイネーブルにします（まだ ASA からアンインストールされていない場合）。このどちらのタイプのパッケージもインストールされておらず、CSD パッケージがインストールされている場合は、この手順を実行すると CSD パッケージ内のホスト スキャン機能がイネーブルになります。

ホスト スキャンをディセーブルにするための詳細な手順

	コマンド	目的
ステップ 1	**webvpn** **例：** `hostname(config)# webvpn`	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**no csd enable** **例：** `hostname(config)# no csd enable`	すべてのインストール済みホスト スキャン パッケージのホスト スキャンをディセーブルにします。 **（注）** イネーブルになっているホスト スキャン 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、ホスト スキャンをディセーブルにする必要があります。

ASA でイネーブルになっているホスト スキャンのバージョンの表示

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、イネーブルになっているホスト スキャンのバージョンを特定します。

前提条件

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。

コマンド	目的

`show webvpn csd hostscan`
 	
例：
`hostname# show webvpn csd hostscan`
	ASA 上でイネーブルになっているホスト スキャンのバージョンを表示します。

ホスト スキャンのアンインストール

ホスト スキャン 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、ホスト スキャンまたは CSD がイネーブルの場合でも ASA によるホスト スキャン パッケージの展開が回避されます。ホスト スキャンをアンインストールしても、フラッシュ ドライブのホスト スキャン パッケージは削除されません。

前提条件

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。ASA のグローバル コンフィギュレーション モードでは、表示されるプロンプトは **hostname(config)#** となります。

手順の詳細

	コマンド	目的
ステップ 1	**webvpn** **例：** `hostname(config)# webvpn`	webvpn コンフィギュレーション モードを開始します。
ステップ 2	**no csd enable** **例：** `ASAName(webvpn)#no csd enable`	アンインストールするホスト スキャン イメージをディセーブルにします。

ステップ 3	**no csd hostscan image** path
	
	例：
	`hostname(webvpn)#no csd hostscan image disk0:/hostscan-3.6.0-k9.pkg`
	`hostname(webvpn)#no csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg`
		アンインストールするホスト スキャン イメージへのパスを指定します。スタンドアロンのホスト スキャン パッケージ、または AnyConnect Secure Mobility Client パッケージがホスト スキャン パッケージとして指定されている場合があります。

	コマンド	目的
ステップ 4	**write memory** **例：** `hostname(webvpn)# write memory`	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。

グループ ポリシーへの AnyConnect フィーチャ モジュールの割り当て

次の手順で、AnyConnect フィーチャ モジュールとグループ ポリシーを関連付けます。VPN ユーザが ASA に接続するときに、ASA はこれらの AnyConnect フィーチャ 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。

前提条件

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。

手順の詳細

	コマンド	目的
ステップ 1	**group-policy** *name* **internal** **例：** `hostname(config)# group-policy PostureModuleGroup internal`	ネットワーク クライアント アクセス用の内部グループ ポリシーの追加
ステップ 2	**group-policy** *name* **attributes** **例：** `hostname(config)# group-policy PostureModuleGroup attributes`	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。
ステップ 3	**webvpn** **例：** `hostname(config-group-policy)# webvpn`	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)#

	コマンド	目的
ステップ 4	hostname(config-group-webvpn)# **anyconnect modules value** AnyConnect Module *Name* **例：** hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture	グループ内のすべてのユーザに AnyConnect フィーチャ 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 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。 **value**　**AnyConnect モジュール名** **dart**　AnyConnect DART（診断およびレポート ツール） **nam**　AnyConnect ネットワーク アクセス マネージャ **vpngina**　AnyConnect SBL（Start Before Logon） **websecurity**　AnyConnect Web セキュリティ モジュール **telemetry**　AnyConnect テレメトリ モジュール **posture**　AnyConnect ポスチャ モジュール **none**　単独で使用され、すべての AnyConnect モジュールをグループ ポリシーから削除します。 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	write memory **例：** hostname(config-group-webvpn)# write memory	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)#

ホスト スキャンに関するその他の重要なマニュアル

ホスト スキャンがエンドポイント 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、ユーザはプリログイン ポリシーの設定、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。

これらの内容については、次のマニュアルで詳しく説明します。

- 『Cisco Secure Desktop Configuration Guides』
- 『Cisco Adaptive Security Device Manager Configuration Guides』

また、AnyConnect クライアントでのホスト スキャンの動作の詳細については、『Cisco *AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*』を参照してください。