# Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの WebVPN Capture Tool

## 内容



## 概要

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスには、WebVPN の接続上で正しく表示されない Web サイトに関する情報を記録する WebVPN キャプチャ ツールが含まれています。セキュリティ アプライアンスのコマンドライン インターフェイス ( CLI ) からキャプチャ ツールをイネーブルにできます。このツールが記録するデータにより、シスコのカスタマー サポート担当者は問題のトラブルシューティングを行えます。

**注**：WebVPNキャプチャツールを有効にすると、セキュリティアプライアンスのパフォーマンスに影響します。出力ファイルの生成後、必ずキャプチャ ツールを無効にしてください。

## 前提条件

### 要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- コマンド ライン インターフェイス ( CLI ) を使用して、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスを設定します。

### 使用するコンポーネント

このドキュメントの情報は、バージョン 7.0 が稼働する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに基づくものです。

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

**注：このセクションで使用されているコマンドの詳細を調べるには、**Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

## WebVPN キャプチャ ツールの出力ファイル

WebVPN キャプチャ ツールが有効になると、キャプチャ ツールは最初に参照された URL からのデータを次のファイルに保存します。

- original.000：セキュリティアプライアンスとWebサーバ間で交換されるデータが含まれます。
- mangled.000：セキュリティアプライアンスとブラウザの間で交換されるデータが含まれます。

その後の各キャプチャで、キャプチャ ツールは追加一致の original.<nnn> および mangled.<nnn> ファイルを生成し、ファイル拡張子を増やします。次の例では、**dir コマンドの出力が 3 つの URL キャプチャから 3 つのファイルのセットを表示します。**

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6           -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
3399        -rw-        4928            08:32:51 Feb 14 2005 ORIGINAL.001
3400        -rw-        6167            08:32:51 Feb 14 2005 MANGLED.001
3401        -rw-        5264            08:35:23 Feb 14 2005 ORIGINAL.002
3402        -rw-        6503            08:35:23 Feb 14 2005 MANGLED.002
hostname#
```

## WebVPN キャプチャ ツールのアクティブ化

**注：複数のファイルを書き込み用に開く場合、フラッシュファイルシステムには制限があります。**複数のキャプチャ ファイルが同時に更新されると、WebVPN キャプチャ ツールによりファイル システムが破損する可能性があります。キャプチャ ツールでこの障害が発生する場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。

WebVPN キャプチャ ツールをアクティブ化するには、特権 EXEC モードから **debug menu webvpn 67 コマンドを使用します。**

```
debug menu webvpn 67
```

場所：

- **cmd は 0 または 1 です。0 はキャプチャを無効にします。**1 はキャプチャを有効にします。
- **user はデータ キャプチャの対象となるユーザ名です。**
- **url はデータ キャプチャの対象となる URL プレフィクスです。**次に示す URL 形式のいずれかを使用します。/http を使用して、すべてのデータをキャプチャします。/http/0/<サーバ/パス> を使用して、<サーバ/パス> で識別されるサーバへの HTTP トラフィックをキャプチャします。/https/0/<サーバ/パス> を使用して、<サーバ/パス> で識別されるサーバへの HTTPS トラフィックをキャプチャします。

**debug menu webvpn 67 0 コマンドを使用して、キャプチャを無効にします。**

次の例で、WebVPN キャプチャ ツールは有効になり、Web サイト wwwin.abcd.com/hr/people を参照する user2 の HTTP トラフィックをキャプチャします。

```
hostname#debug menu webvpn 67 1 user2 /http/0/wwwin.abcd.com/hr/people
Mangle Logging: ON
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

次の例で、WebVPN キャプチャ ツールは無効になります。

```
hostname#debug menu webvpn 67 0
Mangle Logging: OFF
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

## WebVPN キャプチャ ツールの出力ファイルの特定とアップロード

**dir コマンドを使用して、WebVPN キャプチャ ツールの出力ファイルを特定します。**次の例では、dir コマンドの出力が表示され、生成されたファイル ORIGINAL.000 および MANGLED.000 が含まれます。

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6         -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
hostname#
```

**copy flash コマンドを使用して、WebVPN キャプチャ ツールの出力ファイルを別のコンピュータにアップロードできます。**次の例では、ファイル ORIGINAL.000 および MANGLED.000 がアップロードされます。

```
hostname#copy flash:/original.000 tftp://10/86.194.191/original.000
Source filename [original.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [original.000]?
!!!!!!
21601 bytes copied in 0.370 secs
hostname#copy flash:/mangled.000 tftp://10/86.194.191/mangled.000
Source filename [mangled.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [mangled.000]?
!!!!!!
23526 bytes copied in 0.380 secs
hostname#
```

**注：ファイルシステムの破損の可能性を避けるため**に、以前のキャプチャのオリジナルの。<nnn>およびmangled.<nnn>ファイルを上書きしないでください。キャプチャ ツールを無効にする際、ファイル システムの破損を防ぐために、古いファイルを削除します。

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス設定ガイド
- テクニカル サポートとドキュメント – Cisco Systems