

Herramienta de la captura del WebVPN en el dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Archivos salientes de la herramienta de la captura del WebVPN](#)

[Active la herramienta de la captura del WebVPN](#)

[Localice y cargue los archivos salientes de la herramienta de la captura del WebVPN](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

El dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA incluye una herramienta de la captura del WebVPN que le deje información de registro sobre los sitios web que no visualizan correctamente sobre una conexión WebVPN. Usted puede habilitar la herramienta de la captura del comando line interface(cli) del dispositivo de seguridad. Los datos que esta herramienta registra pueden ayudar a su representante de servicio técnico del cliente de Cisco a resolver problemas los problemas.

Nota: Cuando usted habilita la herramienta de la captura del WebVPN, tiene un impacto en el funcionamiento del dispositivo de seguridad. Esté seguro de inhabilitar la herramienta de la captura después de que usted genere los archivos salientes.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir este requisito antes de intentar esta configuración:

- Utilice el comando line interface(cli) para configurar el dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA.

[Componentes Utilizados](#)

La información en este documento se basa en el dispositivo de seguridad adaptante de las 5500

Series de Cisco ASA que funciona con la versión 7.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

[Archivos salientes de la herramienta de la captura del WebVPN](#)

Cuando se habilita la herramienta de la captura del WebVPN, la herramienta de la captura salva los datos del primer URL visitada en estos archivos:

- original.000 — Contiene los datos intercambiados entre el dispositivo de seguridad y el servidor Web.
- mangled.000 — Contiene los datos intercambiados entre el dispositivo de seguridad y el navegador.

Para cada captura subsiguiente, la herramienta de la captura genera los archivos adicionales original.<nnn> que corresponden con y mangled.<nnn> y incrementa las extensiones de archivo. En este ejemplo, la salida de las visualizaciones del **comando dir** tres conjuntos de los archivos a partir de tres capturas URL:

```
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#
```

[Active la herramienta de la captura del WebVPN](#)

Nota: El sistema de archivos Flash tiene limitaciones cuando los Archivos múltiples se abren para la escritura. La herramienta de la captura del WebVPN puede causar posiblemente la corrupción del sistema de archivos cuando los archivos de la captura múltiple se ponen al día en paralelo. Si este error ocurre con la herramienta de la captura, entre en contacto el [Centro de Asistencia Técnica de Cisco \(TAC\)](#).

Para activar la herramienta de la captura del WebVPN, utilice el **comando debug menu webvpn 67** del modo EXEC privilegiado:

```
debug menu webvpn 67 <cmd> <user> <url>
```

Donde:

- **el cmd** es 0 o 1. 0 capturas de las neutralizaciones. 1 captura de los permisos.
- **el usuario** es el nombre de usuario a hacer juego para la captura de datos.
- **el URL** es el prefijo URL a hacer juego para la captura de datos. Utilice uno de estos formatos URL: Utilice /http para capturar todos los datos. Utilice /http/0/<server/path> para capturar el tráfico HTTP al servidor identificado por el <server/path>. Utilice /https/0/<server/path> para capturar el tráfico HTTPS al servidor identificado por el <server/path>.

Utilice el **comando debug menu webvpn 67 0** para inhabilitar la captura.

En este ejemplo, la herramienta de la captura del WebVPN se habilita para capturar el tráfico HTTP para user2 el sitio web que visita wwwin.abcd.com/hr/people:

```
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#
```

En este ejemplo, se inhabilita la herramienta de la captura del WebVPN:

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

[Localice y cargue los archivos salientes de la herramienta de la captura del WebVPN](#)

Utilice el **comando dir** para localizar los archivos salientes de la herramienta de la captura del WebVPN. Este ejemplo muestra la salida del **comando dir** e incluye ORIGINAL.000 y MANGLED.000 los archivos que fueron generados:

```
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#
```

Usted puede cargar los archivos salientes de la herramienta de la captura del WebVPN a otro ordenador usando el **comando copy flash**. En este ejemplo, ORIGINAL.000 y MANGLED.000 los archivos están cargados:

```
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#
```

Nota: Para evitar la corrupción del sistema de archivos posible, no permita los archivos original.<nnn> y mangled.<nnn> de las capturas anteriores que se sobregrabarán. Cuando usted inhabilita la herramienta de la captura, borre los viejos archivos para prevenir la corrupción del sistema de archivos.

[Verificación](#)

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

[Troubleshooting](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Guías de configuración adaptantes del dispositivo de seguridad de las 5500 Series de Cisco ASA](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)