Herramienta de captura de WebVPN en el dispositivo de seguridad adaptable Cisco ASA serie 5500

Contenido

Introducción

Cisco ASA 5500 Series Adaptive Security Appliance incluye una herramienta de captura WebVPN que le permite registrar información sobre sitios Web que no se muestran correctamente a través de una conexión WebVPN. Puede activar la herramienta de captura desde la interfaz de línea de comandos (CLI) del dispositivo de seguridad. Los datos que esta herramienta registra pueden ayudar a su representante de atención al cliente de Cisco a resolver problemas.

Nota: Cuando habilita la herramienta de captura de WebVPN, tiene un impacto en el rendimiento del dispositivo de seguridad. Asegúrese de inhabilitar la herramienta de captura después de generar los archivos de salida.

Prerequisites

Requirements

Asegúrese de cumplir este requisito antes de intentar esta configuración:

- Utilice la interfaz de línea de comandos (CLI) para configurar el dispositivo de seguridad adaptable Cisco ASA serie 5500.

Componentes Utilizados

La información de este documento se basa en el Cisco ASA 5500 Series Adaptive Security Appliance que ejecuta la versión 7.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco 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 (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Archivos de salida de la herramienta de captura WebVPN

Cuando se habilita la herramienta de captura WebVPN, la herramienta de captura almacena los datos de la primera 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 explorador.

Para cada captura subsiguiente, la herramienta de captura genera archivos originales.<nnn> y manipulados.<nnn> e incrementa las extensiones de archivo. En este ejemplo, el resultado del comando **dir** muestra tres conjuntos de archivos de tres capturas de 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#
```

Activar la herramienta de captura WebVPN

Nota: El sistema de archivos Flash tiene limitaciones cuando se abren varios archivos para su escritura. La herramienta de captura de WebVPN puede provocar la corrupción del sistema de archivos cuando se actualizan varios archivos de captura simultáneamente. Si este fallo se produce con la herramienta de captura, póngase en contacto con el Centro de asistencia técnica de Cisco (TAC).

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

```
debug menu webvpn 67
```

Where:

- **cmd** es 0 o 1. 0 inhabilita la captura. 1 habilita la captura.
- **user** es el nombre de usuario que debe coincidir para la captura de datos.
- **url** es el prefijo URL que debe coincidir para la captura de datos. Utilice uno de estos formatos de URL:Utilice /http para capturar todos los datos.Utilice /http/0/<server/path> para capturar el tráfico HTTP al servidor identificado por <server/path>.Utilice /https/0/<server/path> para capturar el tráfico HTTPS al servidor identificado por <server/path>.

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

En este ejemplo, la herramienta de captura WebVPN está habilitada para capturar tráfico HTTP para el usuario2 que visita el sitio Web 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, la herramienta de captura WebVPN está inhabilitada:

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

Localizar y cargar los archivos de salida de la herramienta de captura WebVPN

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

```
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#
```

Puede cargar los archivos de salida de la herramienta de captura WebVPN en otro equipo mediante el comando **copy flash**. En este ejemplo, se cargan los archivos ORIGINAL.000 y

MANGLED.000:

```
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 posibles daños en el sistema de archivos, no permita que se sobrescriban los archivos originales.<nnn> y manipulados.<nnn> de capturas anteriores. Cuando desactive la herramienta de captura, elimine los archivos antiguos para evitar la corrupción del sistema de archivos.

Verificación

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

Troubleshoot

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

Información Relacionada

- Guías de Configuración de Cisco ASA 5500 Series Adaptive Security Appliance
- Soporte Técnico y Documentación - Cisco Systems