

O WebVPN captura a ferramenta na ferramenta de segurança adaptável do 5500 Series de Cisco ASA

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[O WebVPN captura arquivos de saída da ferramenta](#)

[Ative a ferramenta da captura WebVPN](#)

[Encontre e transfira arquivos pela rede os arquivos de saída da ferramenta da captura WebVPN](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

A ferramenta de segurança adaptável do 5500 Series de Cisco ASA inclui uma ferramenta da captura WebVPN que o deixe informação de registro sobre os sites que não indicam corretamente sobre uma conexão VPN da Web. Você pode permitir a ferramenta da captura do comando line interface(cli) da ferramenta de segurança. Os dados que esta ferramenta grava podem ajudar seu representante de suporte do cliente Cisco a pesquisar defeitos problemas.

Note: Quando você permite a ferramenta da captura WebVPN, tem um impacto no desempenho da ferramenta de segurança. Seja certo desabilitar a ferramenta da captura depois que você gerencie os arquivos de saída.

[Pré-requisitos](#)

[Requisitos](#)

Assegure-se de que você cumpra esta exigência antes que você tente esta configuração:

- Use o comando line interface(cli) a fim configurar a ferramenta de segurança adaptável do 5500 Series de Cisco ASA.

[Componentes Utilizados](#)

A informação neste documento é baseada na ferramenta de segurança adaptável do 5500 Series de Cisco ASA que executa a versão 7.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

[Configurar](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

[O WebVPN captura arquivos de saída da ferramenta](#)

Quando a ferramenta da captura WebVPN é permitida, a ferramenta da captura armazena os dados da primeira URL visitada nestes arquivos:

- original.000 — Contém os dados trocados entre a ferramenta de segurança e o servidor de Web.
- mangled.000 — Contém os dados trocados entre a ferramenta de segurança e o navegador.

Para cada captura subsequente, a ferramenta da captura gerencie arquivos de harmonização adicionais original.<nnn> e mangled.<nnn> e incrementa as extensões de arquivo. Neste exemplo, a saída dos indicadores do **comando dir** três grupos de arquivos de três 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#
```

[Ative a ferramenta da captura WebVPN](#)

Note: O sistema de arquivo flash tem limitações quando os arquivos múltiplos são abertos para a escrita. A ferramenta da captura WebVPN pode possivelmente causar a corruption do arquivo de sistema quando os arquivos da captura múltipla são atualizados simultaneamente. Se esta falha ocorrer com a ferramenta da captura, contacte o [centro de assistência técnica da Cisco \(TAC\)](#).

A fim ativar a ferramenta da captura WebVPN, use o **comando debug menu webvpn 67** do modo de exec privilegiado:

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

Em que:

- o **Cmd** é 0 ou 1. 0 captções das inutilizações. 1 permite a captura.
- o **usuário** é o username a combinar para a captura de dados.
- a **URL** é o prefixo URL a combinar para a captura de dados. Use um destes formatos
URL: Use /http para capturar todos os dados. Use /http/0/<server/path> para capturar o tráfego de HTTP ao server identificado pelo <server/path>. Use /https/0/<server/path> para capturar o tráfego HTTPS ao server identificado pelo <server/path>.

Use o **comando debug menu webvpn 67 0** a fim desabilitar a captura.

Neste exemplo, a ferramenta da captura WebVPN é permitida de capturar o tráfego de HTTP para user2 o site de 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#
```

Neste exemplo, a ferramenta da captura WebVPN é desabilitada:

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

[Encontre e transfira arquivos pela rede os arquivos de saída da ferramenta da captura WebVPN](#)

Use o **comando dir** a fim encontrar os arquivos de saída da ferramenta da captura WebVPN. Este exemplo mostra a saída do **comando dir** e inclui os arquivos ORIGINAL.000 e MANGLED.000 que foram gerados:

```
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#
```

Você pode transferir arquivos pela rede os arquivos de saída da ferramenta da captura WebVPN a um outro computador usando o **comando copy flash**. Neste exemplo, nos arquivos ORIGINAL.000 e MANGLED.000 são transferidos arquivos pela rede:

```
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#
```

Note: A fim evitar a corruption do arquivo de sistema possível, não permita os arquivos original.<nnn> e mangled.<nnn> das captações precedentes a ser overwritten. Quando você desabilita a ferramenta da captação, suprima dos arquivos velhos a fim impedir a corrupção do sistema de arquivos.

[Verificar](#)

No momento, não há procedimento de verificação disponível para esta configuração.

[Troubleshooting](#)

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

[Informações Relacionadas](#)

- [Manuais de configuração adaptáveis da ferramenta de segurança do 5500 Series de Cisco ASA](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)