Ferramenta de captura de WebVPN no Cisco ASA 5500 Series Adaptive Security Appliance

Contents

Introduction

O Cisco ASA 5500 Series Adaptive Security Appliance inclui uma ferramenta de captura WebVPN que permite registrar informações sobre sites que não são exibidos corretamente em uma conexão WebVPN. Você pode ativar a ferramenta de captura na CLI (Command Line Interface, interface de linha de comando) do Security Appliance. Os dados registrados por esta ferramenta podem ajudar o representante de suporte ao cliente da Cisco a solucionar problemas.

Observação: quando você habilita a ferramenta de captura WebVPN, ela afeta o desempenho do Security Appliance. Certifique-se de desabilitar a ferramenta de captura depois de gerar os arquivos de saída.

Prerequisites

Requirements

Atenda a estes requisitos antes de tentar esta configuração:

- Use a CLI (Command Line Interface, interface de linha de comando) para configurar o Cisco ASA 5500 Series Adaptive Security Appliance.

Componentes Utilizados

As informações neste documento são baseadas no Cisco ASA 5500 Series Adaptive Security

Appliance com versão 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.

Conventions

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.

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

Arquivos de saída da ferramenta de captura WebVPN

Quando a ferramenta de captura WebVPN está ativada, a ferramenta de captura armazena os dados do primeiro URL visitado nesses arquivos:

- original.000 — Contém os dados trocados entre o Security Appliance e o Servidor Web.
- Mangled.000—Contém os dados trocados entre o Security Appliance e o navegador.

Para cada captura subsequente, a ferramenta de captura gera arquivos originais correspondentes adicionais.<nnn> e gerenciados.<nnn> e incrementa as extensões de arquivos. Neste exemplo, a saída do comando **dir** exibe três conjuntos de arquivos de três 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#
```

Ative a ferramenta de captura WebVPN

Observação: o sistema de arquivos Flash tem limitações quando vários arquivos são abertos para gravação. A ferramenta de captura WebVPN pode possivelmente causar corrupção do sistema de arquivos quando vários arquivos de captura são atualizados simultaneamente. Se essa falha ocorrer com a ferramenta de captura, entre em contato com o Cisco Technical Assistance Center (TAC).

Para ativar a ferramenta de captura WebVPN, use o comando **debug menu webvpn 67** do modo EXEC privilegiado:

```
debug menu webvpn 67
```

Where:

- **cmd** é 0 ou 1. 0 desativa a captura. 1 ativa a captura.
- **usuário** é o nome de usuário a corresponder para a captura de dados.
- **url** é o prefixo de URL a corresponder para a captura de dados. Use um destes formatos de URL:Use /http para capturar todos os dados.Use /http/0/<servidor/caminho> para capturar o tráfego HTTP para o servidor identificado por <servidor/caminho>.Use /https/0/<servidor/caminho> para capturar o tráfego HTTPS para o servidor identificado por <servidor/caminho>.

Use o comando **debug menu webvpn 67 0** para desativar a captura.

Neste exemplo, a ferramenta de captura WebVPN está habilitada para capturar tráfego HTTP para o usuário2 visitando o site 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 de captura WebVPN está desabilitada:

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

Localize e faça o upload dos arquivos de saída da ferramenta de captura WebVPN

Use o comando **dir** para localizar os arquivos de saída da ferramenta de 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 carregar os arquivos de saída da ferramenta de captura WebVPN para outro computador usando o comando **copy flash**. Neste exemplo, os arquivos ORIGINAL.000 e MANGLED.000 são carregados:

```
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#
```

Observação: para evitar possíveis danos no sistema de arquivos, não permita que os arquivos originais.<nnn> e gerenciados.<nnn> das capturas anteriores sejam sobrescritos. Ao desativar a ferramenta de captura, exclua os arquivos antigos para evitar que o sistema de arquivos seja corrompido.

Verificar

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

Troubleshoot

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

Informações Relacionadas

- Guias de configuração do Cisco ASA 5500 Series Adaptive Security Appliance
- Suporte Técnico e Documentação - Cisco Systems