Средство WebVPN Capture Tool устройства адаптивной защиты Cisco ASA 5500 Series

Содержание

Введение

Многофункциональное устройство защиты Cisco ASA серии 5500 включает Инструмент захвата данных WebVPN, который позволяет вам информация журнала о веб-сайтах, которые не отображаются должным образом по подключению WebVPN. Можно включить программное средство перехвата от Интерфейса командной строки (CLI) устройства безопасности. Данные это программное средство записи могут помочь вашим представителям службы поддержки Клиента Cisco устранять проблемы.

Примечание: При включении Инструмента захвата данных WebVPN он оказывает влияние на производительность устройства безопасности. Обязательно отключите программное средство перехвата после генерации выходных файлов.

Предварительные условия

Требования

Перед попыткой применения конфигурации убедитесь в том, что следующие требования выполняются:

- Используйте Интерфейс командной строки (CLI) для настройки многофункционального устройства защиты Cisco ASA серии 5500.

Используемые компоненты

Сведения в этом документе основываются на многофункциональном устройстве защиты Cisco ASA серии 5500, которое выполняет версию 7.0.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Выходные файлы инструмента захвата данных WebVPN

Когда Инструмент захвата данных WebVPN включен, программное средство перехвата хранит данные от первого URL, который посещают в этих файлах:

- исходный 000 — Содержит данные, переданные между устройством безопасности и Web-сервером.
- искаженный 000 — Содержит данные, переданные между устройством безопасности и браузером.

Для каждого последующего перехвата программное средство перехвата генерирует дополнительное исходное соответствие. <nnn> и искаженный. <nnn> файлы и инкременты расширения файла. В данном примере выходные данные **команды dir** отображают три набора файлов от трех перехватов 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#
```

Активируйте инструмент захвата данных WebVPN

Примечание: Когда множественные файлы открыты для записи, Файловая система флэш-устройства имеет ограничения. Когда файлы множественного заголовка обновлены одновременно, Инструмент захвата данных WebVPN может возможно вызвать повреждение файловой системы. Если этот сбой должен произойти с программным средством перехвата, свяжитесь с Центром технической поддержки Cisco (TAC).

Для активации Инструмента захвата данных WebVPN используйте **команду debug menu webvpn 67** от привилегированного режима EXEC:

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

Где:

- **cmd** 0 или 1. 0 отключает перехват. 1 включает перехват.
- **пользователь** является именем пользователя для соответствия для перехвата данных.
- **URL** является префиксом URL для соответствия для перехвата данных. Используйте один из этих Форматов ссылки:Используйте / http для получения всех данных.Используйте/http/0 / <server/path> для получения трафика HTTP к серверу, определенному <server/path>.Используйте/https/0 / <server/path> для получения Трафика HTTPS к серверу, определенному <server/path>.

Используйте **команду debug menu webvpn 67 0** для отключения перехвата.

В данном примере Инструменту захвата данных WebVPN позволяют перехватить трафик HTTP для user2, посещающего веб-сайт 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#
```

В данном примере отключен Инструмент захвата данных WebVPN:

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

Найдите и загрузите выходные файлы инструмента захвата данных WebVPN

Используйте **команду dir** для определения местоположения выходных файлов Инструмента захвата данных WebVPN. Данный пример показывает выходные данные **команды dir** и включает Исходные 000 и Искаженные 000 файлы, которые генерировались:

```
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#
```

Можно загрузить выходные файлы Инструмента захвата данных WebVPN другому использующему компьютеры команда **copy flash**. В данном примере загружены Исходные 000 и Искаженные 000 файлы:

```
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#
```

Примечание: Во избежание возможного повреждения файловой системы не позволяйте оригинал. <nnn> и искаженный. <nnn> файлы от предыдущих перехватов, которые будут перезаписаны. Когда вы отключаете программное средство перехвата, удаляете старые файлы для предотвращения повреждения файловой системы.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Руководства по конфигурации многофункционального устройства защиты Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация