Cisco ASA 5500 Series Adaptive Security Appliance의 WebVPN 캡처 툴

목차

소개

Cisco ASA 5500 Series Adaptive Security Appliance에는 WebVPN 연결을 통해 올바르게 표시되지 않는 웹 사이트에 대한 정보를 기록할 수 있는 WebVPN 캡처 도구가 포함되어 있습니다.보안 어플라이언스의 CLI(Command Line Interface)에서 캡처 툴을 활성화할 수 있습니다.이 툴이 기록한 데이터는 Cisco 고객 지원 담당자가 문제를 해결하는 데 도움이 됩니다.

참고: WebVPN 캡처 툴을 활성화하면 보안 어플라이언스의 성능에 영향을 미칩니다.출력 파일을 생성한 후에는 캡처 툴을 비활성화해야 합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 이 요구 사항을 충족해야 합니다.

- Cisco ASA 5500 Series Adaptive Security Appliance를 구성하려면 CLI(Command Line Interface)를 사용합니다.

사용되는 구성 요소

이 문서의 정보는 버전 7.0을 실행하는 Cisco ASA 5500 Series Adaptive Security Appliance를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

WebVPN 캡처 툴 출력 파일

WebVPN 캡처 도구가 활성화된 경우 캡처 툴은 다음 파일에서 방문한 첫 번째 URL의 데이터를 저장합니다.

- original.000 - 보안 어플라이언스와 웹 서버 간에 교환되는 데이터를 포함합니다.
- thrighted.000 - 보안 어플라이언스와 브라우저 간에 교환되는 데이터를 포함합니다.

각 후속 캡처에 대해 캡처 툴은 일치하는 원본 <nnn> 및 잘못된 파일을 추가로 생성하고 파일 확장명을 증가시킵니다.이 예에서 dir 명령의 출력은 3개의 **URL** 캡처에서 3개의 파일 집합을 표시합니다.

```
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#
```

WebVPN 캡처 도구 활성화

참고: 플래시 파일 시스템은 여러 파일을 쓰기 위해 열 때 제한이 있습니다.WebVPN 캡처 툴은 여러 캡처 파일을 동시에 업데이트할 때 파일 시스템이 손상될 수 있습니다.캡처 툴에서 이 오류가 발생하면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

WebVPN 캡처 도구를 활성화하려면 특별 권한 EXEC 모드에서 **debug 메뉴 webvpn 67** 명령을 사용합니다.

```
debug menu webvpn 67
```

위치:

- **cmd**는 0 또는 1입니다. 0은 캡처를 비활성화합니다.1은 캡처를 활성화합니다.
- **user**는 데이터 캡처와 일치시킬 사용자 이름입니다.
- **url**은 데이터 캡처에 대해 매칭할 URL 접두사입니다.다음 URL 형식 중 하나를 사용합니다 ./http를 사용하여 모든 데이터를 캡처합니다./http/0/<server/path>를 사용하여 <server/path>로 식별된 서버에 대한 HTTP 트래픽을 캡처합니다./https/0/<서버/경로>를 사용하여 <server/path>로 식별된 서버에 대한 HTTPS 트래픽을 캡처합니다.

캡처를 비활성화하려면 **debug menu webvpn 67 0** 명령을 사용합니다.

이 예에서 WebVPN 캡처 툴은 wwwin.abcd.com/hr/people 웹 사이트를 방문하는 user2의 HTTP 트래픽을 캡처할 수 있습니다.

```
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#
```

이 예에서는 WebVPN 캡처 도구가 비활성화되어 있습니다.

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

WebVPN 캡처 툴 출력 파일 찾기 및 업로드

WebVPN 캡처 툴 출력 파일을 찾으려면 dir 명령을 사용합니다.다음 예에서는 dir 명령의 출력을 보여 주고 생성된 ORIGINAL.000 및 THRIGHTED.000 파일을 포함합니다.

```
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#
```

copy flash 명령을 사용하여 WebVPN 캡처 도구 출력 파일을 다른 컴퓨터에 업로드할 수 있습니다 .이 예에서는 ORIGINAL.000 및 THRIGHTED.000 파일이 업로드됩니다.

```
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#
```

참고: 파일 시스템 손상을 방지하려면 이전 캡처의 원본.<nnn> 및 실패한.<nnn> 파일을 덮어쓰지 않도록 하십시오.캡처 툴을 비활성화하면 파일 시스템의 손상을 방지하기 위해 이전 파일을 삭제합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems