WebVPN Capture Tool op Cisco ASA 5500 Series adaptieve security applicatie

Inhoud

Inleiding

De Cisco ASA 5500 Series adaptieve security applicatie bevat een WebVPN opnamegereedschap waarmee u informatie over websites kunt registreren die niet correct via een WebVPN-verbinding worden weergegeven. U kunt het opnamegereedschap inschakelen via de Opdracht Line Interface (CLI) van het beveiligingsapparaat. De gegevens in deze gereedschaps-bestanden kunnen uw Cisco-klantondersteuning helpen bij problemen met uw vertegenwoordiger voor probleemoplossing.

N.B.: Wanneer u het WebVPN opnamegereedschap inschakelen, heeft dit een invloed op de prestaties van het security apparaat. Vergeet niet het opnamegereedschap uit te schakelen nadat u de uitvoerbestanden hebt gegenereerd.

Voorwaarden

Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereiste worden voldaan:

- Gebruik de Opdracht Line Interface (CLI) om Cisco ASA 5500 Series adaptieve security applicatie te configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA 5500 Series adaptieve security applicatie die versie 7.0 ondersteunt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Uitvoerbestanden van Webex Capture Tool

Wanneer het WebVPN opnamegereedschap is ingeschakeld, slaat het opnamegereedschap de gegevens op van de eerste URL die in deze bestanden wordt bezocht:

- original.000-Bevat de gegevens die tussen het security apparaat en de webserver worden uitgewisseld.
- mangled.000 - Bevat de gegevens die tussen het security apparaat en de browser worden uitgewisseld.

Bij elke volgende opname genereert het opnamegereedschap extra overeenkomend origineel.<nnn> en gemanipuleerd.<nnn> bestanden en worden de bestandsextensies verhoogd. In dit voorbeeld, toont de uitvoer van het **dir** bevel drie reeksen bestanden van drie URL opnamen:

```
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#
```

Activeert het WebVPN Capture Tool

Opmerking: Het Flash File System heeft beperkingen wanneer er meerdere bestanden worden geopend voor het schrijven. Het WebVPN opnamegereedschap kan mogelijk de corruptie van het bestandssysteem veroorzaken wanneer de meerdere opnamekaarten tegelijkertijd worden bijgewerkt. Als deze fout moet optreden met het opnamegereedschap, neem dan contact op met

het Cisco Technical Assistance Center (TAC).

Om het WebVPN opnamegereedschap te activeren, gebruikt u de opdracht **debug menu Web 67** van bevoorrechte EXEC-modus:

```
debug menu webvpn 67
```

Wanneer:

- **cmd** is 0 of 1,0 en blokkeert de opname. 1 maakt het mogelijk te vangen.
- **De gebruiker** is de gebruikersnaam die moet worden aangepast voor de gegevensextractie.
- **url** is het URL-prefix dat moet worden aangepast voor gegevensextractie. Gebruik een van deze URL-formaten:Gebruik /http om alle gegevens op te nemen.Gebruik /http/0/<server/path> om HTTP-verkeer naar de server op te nemen die is geïdentificeerd door <server/pad>.Gebruik /https/0/<server/path> om HTTPS-verkeer naar de server op te nemen die geïdentificeerd is door <server/pad>.

Gebruik de opdracht **debug menu Web 67 0** om opname uit te schakelen.

In dit voorbeeld is het WebVPN opnamegereedschap geactiveerd om HTTP verkeer voor user2 visiting website wwwin.abcd.com/hr/people te vangen:

```
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#
```

In dit voorbeeld is het WebVPN opnamegereedschap uitgeschakeld:

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

De uitvoerbestanden van het WebVPN-Capture Tool zoeken en uploaden

Gebruik de opdracht **dir** om de uitvoerbestanden van het WebVPN-opnamegereedschap te vinden. Dit voorbeeld toont de output van het **dir** bevel en omvat de ORIGINAL.000 en MANGLED.000 bestanden die werden gegenereerd:

```
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#
```

U kunt de uitvoerbestanden van het WebVPN-opnamegereedschap naar een andere computer uploaden met de opdracht **Kopieflitser**. In dit voorbeeld worden de bestanden ORIGINAL.000 en MANGLED.000 geüpload:

```
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#
```

Opmerking: om mogelijke corruptie bij het bestandssysteem te voorkomen, laat het origineel niet toe.<nnn> en gemanipuleerd.<nnn> bestanden van vorige opnamen worden overschreven. Wanneer u het opnamegereedschap uitschakelt, verwijdert u de oude bestanden om corruptie in het bestandssysteem te voorkomen.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicatiehandleidingen
- Technische ondersteuning en documentatie – Cisco Systems