Veelgestelde vragen over content security applicaties: hoe voert u een pakketopname uit op een Cisco Content Security applicatie?

Inhoud

Inleiding

Dit document beschrijft hoe u pakketopnamen kunt uitvoeren op de Cisco Content Security-applicaties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco e-mail security applicatie (ESA)
- Cisco Web Security applicatie (WSA)
- Cisco Security Management-applicatie (SMA)
- AsyncOS

Gebruikte componenten

De informatie in dit document is gebaseerd op alle versies van AsyncOS.

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.

Hoe voert u een pakketopname uit op een Cisco Content Security-applicatie?

Voltooi deze stappen om een pakketopname (tcpdump-opdracht) uit te voeren met de GUI:

1. Navigeer om te helpen en te ondersteunen > Packet Capture op de GUI.
2. Bewerk desgewenst de pakketopnameconstellingen, zoals de netwerkinterface waarop de pakketopname wordt uitgevoerd. U kunt een van de vooraf gedefinieerde filters gebruiken, of u kunt een aangepaste filter maken met behulp van een syntaxis die wordt ondersteund door de opdracht Unix tcpdump.
3. Klik op Opname starten om de opname te starten.
4. Klik op Opname stoppen om de opname te beëindigen.
5. Download de pakketopname.

Voltooi deze stappen om een pakketopname (tcpdump-opdracht) met de CLI uit te voeren:

1. Voer deze opdracht in de CLI in:

```
<#root>
wsa.run> packetcapture


Status: No capture running

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     (tcp port 80 or tcp port 3128)
```

2. Kies de bewerking die u wilt uitvoeren:

```
<#root>
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]>
setup
```

3. Voer de maximaal toegestane grootte voor het opnamebestand in (in MB):

<#root>

[200]>

200

Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]>

n

The following interfaces are configured:

1. Management

2. T1

3. T2

4. Voer de naam of het nummer in van een of meer interfaces waaruit om pakketten op te nemen, gescheiden door komma's:

<#root>

[1]>

1

5. Voer het filter in dat u voor de opname wilt gebruiken. Voer het woord CLEAR in om het filter te verwijderen en alle pakketten op de geselecteerde interfaces op te nemen.

<#root>

[(tcp port 80 or tcp port 3128)]>

host 10.10.10.10 && port 80

Status: No capture running

Current Settings:

 Max file size: 200 MB

 Capture Limit: None (Run Indefinitely)

```
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

6. Kies de startbewerking om de opname te starten:

```
<#root>
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]>
start


Status: Capture in progress (Duration: 0s)
File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

7. Kies de stopopdracht om de opname te beëindigen:

```
<#root>
- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.
[]>
stop


Status: No capture running (Capture stopped by user)

Current Settings:
```

```
Max file size:       200 MB

Capture Limit:       None (Run Indefinitely)

Capture Interfaces: Management

Capture Filter:      host 10.10.10.10 && port 80
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.