Packet Capture Procedures gebruiken op FirePOWER-apparaat

Inhoud

Inleiding

Dit document beschrijft hoe de opdracht **tcpdump** moet worden gebruikt om pakketten op te nemen die worden gezien door een netwerkinterface van uw FirePOWER-apparaat.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van het Cisco Firepower-apparaat en de modellen van virtuele apparaten.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies. Het gebruikt de syntaxis van Berkeley Packet Filter (BPF).

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

> **Waarschuwing**: als u **tcpdump** commando op een productiesysteem uitvoert, kan dit van invloed zijn op de netwerkprestaties.

Stappen om pakketten op te nemen

Log in op de CLI van uw FirePOWER-apparaat.

Voer in versie 6.1 en hoger **opnameverkeer in**. Voorbeeld,

<#root>

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

In versies 6.0.x.x en hoger voert u **systeemondersteuning en opnameverkeer in**. Voorbeeld,

<#root>

```
> system support capture-traffic
```

```
Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

Nadat u een selectie hebt gemaakt, wordt u gevraagd om opties:

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

Om voldoende gegevens van de pakketten te kunnen opnemen, moet de optie -s worden gebruikt om de lengte van de snaplength correct in te stellen. De snaplength kan worden ingesteld op een waarde die overeenkomt met de geconfigureerde maximale transmissie-unit (MTU) waarde van de Interface Set-configuratie, die standaard op 1518 staat.

> **Waarschuwing**: wanneer u verkeer op het scherm opneemt, kan dit de prestaties van het systeem en netwerk nadelig beïnvloeden. Cisco raadt u aan de -w <filename>optie met de opdracht tcpdump te gebruiken. De pakketten worden in een bestand opgenomen. Als u de opdracht zonder de -w-optie uitvoert, drukt u op de toetsencombinatie **Ctrl-C** om de opdracht te beëindigen.

Voorbeeld van -w <filename>optie:

<#root>

```
-w capture.pcap -s 1518
```

> **Waarschuwing**: gebruik geen pad elementen wanneer u de bestandsnaam voor pakketopname (pcap) specificeert. U moet alleen de bestandsnaam voor de dop opgeven die in het apparaat moet worden gemaakt.

Als het wenselijk is om een beperkt aantal pakketten op te nemen, kunt u de vlag -c <packets> gebruiken om het aantal op te nemen pakketten te specificeren. Bijvoorbeeld, om precies 5000 pakketten te vangen:

<#root>

```
-w capture.pcap -s 1518 -c 5000
```

Daarnaast kan er een BPF-filter worden toegevoegd aan het einde van de opdracht om te beperken welke pakketten worden opgenomen. U kunt bijvoorbeeld deze opties gebruiken om de pakketopname te beperken tot 5000 pakketten met een IP-adres voor bron of bestemming van 192.0.2.1:

<#root>

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

Wanneer u verkeer opneemt dat is gelabeld voor Virtual LAN (VLAN), moet u het VLAN opgeven met de BPF-syntaxis. Anders bevat de pcap geen van de VLAN getagde pakketten. Dit voorbeeld beperkt de opname bijvoorbeeld tot verkeer dat VLAN-tags vanaf 192.0.2.1 bevat:

<#root>

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

Als u niet zeker weet of verkeer VLAN-tags heeft, kan deze syntaxis worden gebruikt om verkeer vanaf 192.0.2.1 op te nemen dat VLAN-tags is en niet is:

<#root>

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

> **Opmerking**: In het vorige voorbeeld zijn de haakjes nodig, zodat de 'of' niet alleen van toepassing is op 'vlan'. De enkele noteringen zijn dan nodig om mogelijke verkeerde interpretatie van de haakjes door de schelp te voorkomen.

Specificatie van een VLAN-tag legt al het VLAN-verkeer vast dat overeenkomt met de rest van uw BPF. Als u echter een specifieke VLAN-tag wilt vastleggen, kunt u opgeven welke VLAN-tag u als volgt wilt vastleggen:

<#root>

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

Nadat u de gewenste opties hebt gespecificeerd en op **Enter** hebt gedrukt, begint tcpdump verkeer op te nemen.

> **Tip**: Als de -c-optie niet is gebruikt, druk dan op de toetscombinatie **Ctrl-C** om de opname te stoppen.

Zodra u de opname stopt, ontvangt u bevestiging. Voorbeeld:

<#root>

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

-w capture.pcap -s 1518 -c 5000 host 192.0.2.1

```
Cleaning up.
Done.
```

Een PCAP-bestand kopiëren

Gebruik deze opdracht om een pcap-bestand van een FirePOWER-applicatie te kopiëren naar een ander systeem dat inkomende SSH-verbindingen accepteert:

<#root>

> system file secure-copy hostname username destination_directory pcap_file

Nadat u op **Enter** hebt gedrukt, wordt u gevraagd het wachtwoord op te geven naar het externe systeem. Het bestand kan worden gekopieerd naar het netwerk.

> **Opmerking**: in dit voorbeeld verwijst de hostnaam naar de naam of het IP-adres van de externe doelhost, de gebruikersnaam specificeert de naam van de gebruiker op de externe host, de destination_directory specificeert het bestemmingspad op de externe host, en het pcap_bestand specificeert het lokale pcap-bestand voor overdracht.

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.