Ingesloten pakket op software configureren en opnemen

Inhoud

Inleiding

In dit document wordt de EPC-functie (Embedded Packet Capture) in Cisco IOS®-software beschreven.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-release 12.4(20)T of hoger
- Cisco IOS XE® release 15.2(4)S - 3.7.0 of hoger

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.

Achtergrondinformatie

Indien ingeschakeld, neemt de router de verzonden en ontvangen pakketten op. De pakketten worden opgeslagen binnen een buffer in DRAM en blijven niet bestaan door herladen. Zodra de gegevens zijn opgenomen, kunnen ze worden onderzocht in een samenvatting of gedetailleerde weergave op de router.

Daarnaast kunnen de gegevens worden geëxporteerd als een pakketopnamebestand (PCAP) om verder onderzoek mogelijk te maken. Het gereedschap is geconfigureerd in de exec-modus en wordt beschouwd als een tijdelijk hulpprogramma. Als gevolg daarvan wordt de gereedschapsconfiguratie niet opgeslagen binnen de routerconfiguratie en blijft deze niet op zijn plaats na een systeemherladen.

De tool Packet Capture Config Generator and Analyzer is beschikbaar voor Cisco-klanten en biedt ondersteuning bij het configureren, vastleggen en extraheren van pakketopnamen.

Configuratievoorbeeld voor Cisco IOS

Basis-EPC-configuratie

1. Definieer een 'opnamebuffer', een tijdelijke buffer waarin de opgenomen pakketten worden opgeslagen.
2. U kunt verschillende opties selecteren nadat de buffer is gedefinieerd, zoals grootte, maximale pakketgrootte en circulair/lineair:

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

3. Een filter is van toepassing om de opname tot het gewenste verkeer te beperken. Definieer een toegangscontrolelijst (ACL) in de configuratiemodus en pas het filter toe op de buffer:

```
ip access-list extended BUF-FILTER
permit ip host 192.168.1.1 host 172.16.1.1
permit ip host 172.16.1.1 host 192.168.1.1

monitor capture buffer BUF filter access-list BUF-FILTER
```

4. Definieer een opnamepunt dat de locatie definieert waar de opname plaatsvindt.
5. Het vastleggingspunt definieert tevens of de vastlegging plaatsvindt voor IPv4 of IPv6 en in welk switchingpad (proces of CEF):

```
monitor capture point ip cef POINT fastEthernet 0 both
```

6. Koppel de buffer aan het vastleggingspunt:

```
monitor capture point associate POINT BUF
```

7. Start de vastlegging:

```
monitor capture point start POINT
```

8. De vastlegging is nu actief. Sta het verzamelen van de benodigde data toe.

9. Stop de vastlegging:

```
monitor capture point stop POINT
```

10. Onderzoek de buffer op het apparaat:

```
show monitor capture buffer BUF dump
```

Opmerking: Deze uitvoer toont alleen de hexadecimale (hex) dump van de pakketvastleggingen. Er zijn twee manieren om deze in door mensen leesbare vorm te bekijken.Exporteer de buffer van de router voor verdere analyse:

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

De vorige methode is niet altijd praktisch aangezien het toegang T/FTP tot de router vereiste. In dergelijke situaties, neem een kopie van de hex dump en gebruik elke online hex-cap convertor om de bestanden te bekijken.

11. Zodra de benodigde data zijn verzameld, verwijdert u het vastleggingspunt en de vastleggingsbuffer:

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

Aanvullende informatie over Cisco IOS-configuratie

- In releases eerder dan Cisco IOS® release 15.0(1)M, was de buffergrootte beperkt tot 512K.
- In releases eerder dan Cisco IOS® release 15.0(1)M, was de opgenomen pakketgrootte beperkt tot 1024 bytes.
- De pakketbuffer wordt opgeslagen in DRAM's en blijft niet bestaan door herladingen.
- De opnameconfiguratie wordt niet opgeslagen in NVRAM en blijft niet bestaan bij herladingen.
- Het vastleggingspunt kan worden gedefinieerd voor vastlegging via het proces- of het CEF-switchingpad.
- Het vastleggingspunt kan zo worden gedefinieerd dat vastlegging alleen op een interface of globaal wordt uitgevoerd.
- Wanneer de vastleggingsbuffer wordt geëxporteerd in PCAP-indeling, blijft L2-informatie (zoals Ethernet-inkapseling) niet behouden.
- Zie Best practices voor zoekopdrachten voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Basis IP-verkeer-export configuratie

De IP Traffic Export is een andere methode om IP-pakketten te exporteren die worden ontvangen op meerdere, gelijktijdige WAN- of LAN-interfaces.

1. Definieer in de configuratiemodus een exportprofiel voor IP-verkeer.

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2. Configuratie van bidirectioneel verkeer in het profiel.

```
Device(config-rite)# bidirectional
```

3. Sluiten

4. Specificeer de interface voor geëxporteerd verkeer.

```
Device(config-if)# interface GigabitEthernet 0/1
```

5. Schakel de export van IP-verkeer op de interface in.

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```

6. Sluiten

7. Start de opname. De vastlegging is nu actief. Sta het verzamelen van de benodigde data toe.

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8. Stop de opname.

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9. Exporteer de opname naar een externe TFTP-server.

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10. Zodra de benodigde gegevens zijn verzameld, verwijdert u het profiel.

```
Device(config)# no ip traffic-export profile mypcap
```

Nadelen bij export van IP-verkeer

IP Traffic Export heeft deze nadelen in vergelijking met de EPC-methode:

- De interface waar het opgenomen verkeer wordt geëxporteerd moet een Ethernet-interface zijn.
- Geen IPv6-ondersteuning.
- Geen Layer 2-informatie, alleen Layer 3 en hoger.

Configuratievoorbeeld voor Cisco IOS-XE

De functie Embedded Packet Capture werd geïntroduceerd in Cisco IOS-XE® release 3.7 - 15.2(4)S. De configuratie van de opname is anders dan Cisco IOS® omdat er meer functies aan zijn toegevoegd.

Basis-EPC-configuratie

1. Bepaal de locatie waar de vangst plaatsvindt:

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. Koppel een filter. Het filter is of gespecifieerd inline, of een ACL of class-map kan als referentie worden gebruikt:

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

3. Start de vastlegging:

```
monitor capture CAP start
```

4. De vastlegging is nu actief. Laat de benodigde data verzamelen.

5. Stop de vastlegging:

```
monitor capture CAP stop
```

6. Bekijk de vastlegging in een overzichtsweergave:

```
show monitor capture CAP buffer brief
```

7. Bestudeer de vastlegging in een gedetailleerde weergave:

```
show monitor capture CAP buffer detailed
```

8. Exporteer bovendien de vastlegging in PCAP-indeling voor verdere analyse:

```
monitor capture CAP export tftp://10.0.0.1/CAP.pcap
```

9. Zodra de benodigde data zijn verzameld, verwijdert u de vastlegging:

```
no monitor capture CAP
```

Aanvullende informatie

- De opname wordt uitgevoerd op fysieke interfaces, subinterfaces en tunnelinterfaces.
- Op Network Based Application Recognition (NBAR) gebaseerde filters (die de **match protocol** commando onder de class-map) momenteel niet ondersteund.
- Zie Best practices voor zoekopdrachten voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Voor EPC die op Cisco IOS-XE® wordt uitgevoerd, wordt deze debug-opdracht gebruikt om er

zeker van te zijn dat EPC op de juiste manier is geïnstalleerd:

```
debug epc provision
debug epc capture-point
```

Gerelateerde informatie

- Embedded Packet Capture – Cisco IOS-XE
- Embedded Packet Capture – Cisco IOS
- Technische ondersteuning en documentatie – Cisco Systems

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.