Configurazione e acquisizione di pacchetti integrati sul software

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Esempio di configurazione di Cisco IOS](#)
[Configurazione EPC di base](#)
[Informazioni aggiuntive sulla configurazione di Cisco IOS](#)
[Configurazione base traffico IP-esportazione](#)
[Svantaggi dell'esportazione del traffico IP](#)
[Esempio di Cisco IOS-XEConfiguration](#)
[Configurazione EPC di base](#)
[Ulteriori informazioni](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la funzione Embedded Packet Capture (EPC) nel software Cisco IOS®.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS release 12.4(20)T o successive
- Cisco IOS XE release 15.2(4)S - 3.7.0 o successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando abilitato, il router acquisisce i pacchetti inviati e ricevuti. I pacchetti vengono memorizzati in un buffer nella DRAM e non vengono caricati nuovamente in modo permanente. Dopo aver acquisito i dati, è possibile esaminarli in una visualizzazione di riepilogo o dettagliata sul router.

Inoltre, i dati possono essere esportati come file PCAP (Packet Capture) per consentire un ulteriore esame. Lo strumento è configurato in modalità di esecuzione ed è considerato uno strumento di assistenza temporanea. Di conseguenza, la configurazione dello strumento non viene memorizzata nella configurazione del router e non rimane tale dopo un ricaricamento del sistema.

Lo strumento Packet Capture Config Generator and Analyzer è disponibile per i clienti Cisco per semplificare la configurazione, l'acquisizione e l'estrazione delle acquisizioni dei pacchetti.

Esempio di configurazione di Cisco IOS

Configurazione EPC di base

1. Definire un 'buffer di acquisizione', ovvero un buffer temporaneo in cui vengono archiviati i pacchetti acquisiti.
2. Quando si definisce il buffer, è possibile selezionare diverse opzioni, ad esempio dimensioni, dimensioni massime del pacchetto e circolare/lineare:

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

3. È possibile applicare un filtro per limitare l'acquisizione al traffico desiderato. Definire un Access Control List (ACL) in modalità di configurazione e applicare il filtro al 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. Definire un punto di acquisizione che definisca la posizione in cui viene eseguita l'acquisizione.

5. Il punto di acquisizione definisce anche se l'acquisizione avviene per IPv4 o IPv6 e in quale percorso di commutazione (processo o cef):

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

6. Collegare il buffer al punto di acquisizione:

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

7. Avviare l'acquisizione:

```
monitor capture point start POINT
```

8. L'acquisizione è ora attiva. Consente la raccolta dei dati necessari.
9. Interrompere l'acquisizione:

```
monitor capture point stop POINT
```

10. Esaminare il buffer sull'unità:

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

> Nota: questo output mostra solo il dump esadecimale delle acquisizioni dei pacchetti. Per vederli in chiaro ci sono due modi.

Esportare il buffer dal router per un'ulteriore analisi:

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

Il metodo precedente non è sempre pratico in quanto richiedeva l'accesso T/FTP al router. In tali situazioni, prendere una copia del dump esadecimale e utilizzare qualsiasi convertitore hex-cap in linea per visualizzare i file.

11. Una volta raccolti i dati necessari, eliminare il 'punto di acquisizione' e il 'buffer di

acquisizione':

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

Informazioni aggiuntive sulla configurazione di Cisco IOS

- Nelle versioni precedenti a Cisco IOS versione 15.0(1)M, le dimensioni del buffer erano limitate a 512K.
- Nelle versioni precedenti a Cisco IOS versione 15.0(1)M, le dimensioni del pacchetto acquisito erano limitate a 1024 byte.
- Il buffer del pacchetto è memorizzato nella DRAM e non persiste durante i ricaricamenti.
- La configurazione di acquisizione non è memorizzata nella NVRAM e non viene mantenuta durante i ricaricamenti.
- Il punto di acquisizione può essere definito per l'acquisizione nel cef o nei percorsi di commutazione del processo.
- Il punto di acquisizione può essere definito per l'acquisizione solo su un'interfaccia o globalmente.
- Quando il buffer di acquisizione viene esportato in formato PCAP, le informazioni L2 (ad esempio l'incapsulamento Ethernet) non vengono mantenute.
- Per ulteriori informazioni sui comandi menzionati in questa sezione, vedere Procedure ottimali per i comandi di ricerca.

Configurazione base traffico IP-esportazione

L'esportazione del traffico IP è un metodo diverso per esportare pacchetti IP che vengono ricevuti su più interfacce WAN o LAN simultanee.

1. In modalità di configurazione, definire un profilo di esportazione del traffico IP.

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

2. Configurare il traffico bidirezionale nel profilo.

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

3. Esci

4. Specificare l'interfaccia per il traffico esportato.

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

5. Abilitare l'esportazione del traffico IP sull'interfaccia.

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

6. Uscita

7. Avviare l'acquisizione. L'acquisizione è ora attiva. Consente la raccolta dei dati necessari.

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

8. Interrompere l'acquisizione.

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

9. Esportare l'acquisizione su un server TFTP esterno.

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

10. Una volta raccolti i dati necessari, eliminare il profilo.

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

Svantaggi dell'esportazione del traffico IP

L'esportazione del traffico IP presenta i seguenti svantaggi rispetto al metodo EPC:

- L'interfaccia su cui viene esportato il traffico acquisito deve essere Ethernet.
- Nessun supporto per IPv6.
- Nessuna informazione sul livello 2, solo il livello 3 e superiore.

Esempio di configurazione di Cisco IOS-XE

La funzione Embedded Packet Capture è stata introdotta in Cisco IOS XE versione 3.7 -

15.2(4)S. La configurazione dell'acquisizione è diversa da Cisco IOS perché aggiunge più funzionalità.

Configurazione EPC di base

1. Definire il percorso in cui viene eseguita l'acquisizione:

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

2. Associare un filtro. È possibile specificare il filtro in linea oppure fare riferimento a un ACL o a una mappa di classe:

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

3. Avviare l'acquisizione:

```
monitor capture CAP start
```

4. L'acquisizione è ora attiva. Consentire la raccolta dei dati necessari.

5. Interrompere l'acquisizione:

```
monitor capture CAP stop
```

6. Esaminare l'acquisizione in una visualizzazione di riepilogo:

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

7. Esaminate l'acquisizione in una vista dettagliata:

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

8. Inoltre, esportate l'acquisizione in formato PCAP per un'ulteriore analisi:

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

9. Una volta raccolti i dati necessari, rimuovere l'acquisizione:

```
no monitor capture CAP
```

Ulteriori informazioni

- L'acquisizione viene eseguita su interfacce fisiche, sottointerfacce e interfacce tunnel.
- Filtri basati su NBAR (Network Based Application Recognition) che utilizzano **match protocol** sotto la mappa-classi) non sono attualmente supportati.
- Per ulteriori informazioni sui comandi menzionati in questa sezione, vedere Procedure ottimali per i comandi di ricerca.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Per l'EPC eseguito su Cisco IOS-XE®, questo comando di debug viene usato per garantire la corretta configurazione dell'EPC:

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

Informazioni correlate

- Acquisizione pacchetti integrata - Cisco IOS-XE
- Embedded Packet Capture - Cisco IOS
- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).