Konfigurieren und Erfassen von eingebetteten Paketen auf Software

Inhalt

Einleitung

Dieses Dokument beschreibt die Embedded Packet Capture (EPC)-Funktion in der Cisco IOS®-Software.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS Version 12.4(20)T oder höher
- Cisco IOS XE® Version 15.2(4)S - 3.7.0 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Wenn diese Option aktiviert ist, erfasst der Router die gesendeten und empfangenen Pakete. Die Pakete werden in einem Puffer in DRAM gespeichert und bleiben beim erneuten Laden nicht erhalten. Nachdem die Daten erfasst wurden, können sie auf dem Router in einer Übersicht oder Detailansicht überprüft werden.

Darüber hinaus können die Daten als PCAP-Datei (Packet Capture) exportiert werden, um eine weitere Untersuchung zu ermöglichen. Das Tool wird im EXEC-Modus konfiguriert und gilt als Tool für temporäre Unterstützung. Daher wird die Toolkonfiguration nicht in der Routerkonfiguration gespeichert und bleibt nach einem erneuten Laden des Systems nicht erhalten.

Der Packet Capture Config Generator and Analyzer steht Cisco Kunden zur Verfügung, um die Konfiguration, Erfassung und Extraktion von Paketerfassungen zu unterstützen.

Beispiel für Cisco IOS-Konfiguration

EPC-Basiskonfiguration

1. Definieren Sie einen 'Capture Buffer', einen temporären Puffer, in dem die erfassten Pakete gespeichert werden.
2. Es gibt verschiedene Optionen, die beim Definieren des Puffers ausgewählt werden können. Dazu gehören Größe, maximale Paketgröße und zirkulär/linear:

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

3. Ein Filter ist anwendbar, um die Erfassung auf den gewünschten Datenverkehr zu beschränken. Access Control List (ACL) im Konfigurationsmodus definieren und den Filter auf den Puffer anwenden:

```
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. Definieren Sie einen Erfassungspunkt, der den Ort definiert, an dem die Erfassung erfolgt.
5. Der Erfassungspunkt definiert auch, ob die Erfassung für IPv4 oder IPv6 erfolgt und in welchem Switching-Pfad (Process vs. CEF):

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

6. Puffer an den Erfassungspunkt anhängen:

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

7. Erfassung starten:

```
monitor capture point start POINT
```

8. Die Erfassung ist jetzt aktiv. Gestatten Sie die Erfassung der erforderlichen Daten.

9. Erfassung beenden:

```
monitor capture point stop POINT
```

10. Puffer auf der Einheit untersuchen:

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

Anmerkung: Diese Ausgabe zeigt nur den Hex-Dump der erfassten Pakete. Um sie lesbar zu machen, gibt es zwei Möglichkeiten.Puffer aus dem Router zur weiteren Analyse exportieren:

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

Die vorherige Methode ist nicht immer praktisch, da sie einen T/FTP-Zugriff auf den Router erfordert. In solchen Situationen nehmen Sie eine Kopie des Hex-Dump und verwenden Sie jeden Online-Hex-pcap-Konverter, um die Dateien anzuzeigen.

11. Sobald die erforderlichen Daten erfasst wurden, löschen Sie den „Erfassungspunkt“ und den „Erfassungspuffer“:

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

Zusätzliche Cisco IOS-Konfigurationsinformationen

- In früheren Versionen als Cisco IOS® Version 15.0(1)M war die Puffergröße auf 512.000 begrenzt.
- In früheren Versionen als Cisco IOS® Version 15.0(1)M war die erfasste Paketgröße auf 1024 Byte beschränkt.
- Der Paketpuffer wird im DRAM gespeichert und bleibt nicht durch Neuladen erhalten.
- Die Erfassungskonfiguration wird nicht im NVRAM gespeichert und bleibt auch beim erneuten Laden nicht erhalten.
- Der Erfassungspunkt kann so definiert werden, dass er in den CEF- oder Process-Switching-Pfaden erfasst wird.
- Der Erfassungspunkt kann so definiert werden, dass er nur auf einer Schnittstelle oder global erfasst wird.
- Wenn der Erfassungspuffer im PCAP-Format exportiert wird, werden L2-Informationen (z. B. Ethernet-Kapselung) nicht beibehalten.
- Weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen finden Sie unter Best Practices für Suchbefehle.

Grundlegende Konfiguration für den IP-Datenverkehr-Export

Der Export von IP-Datenverkehr ist eine andere Methode zum Exportieren von IP-Paketen, die über mehrere WAN- oder LAN-Schnittstellen gleichzeitig empfangen werden.

1. Definieren Sie im Konfigurationsmodus ein Exportprofil für IP-Datenverkehr.

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

2. Konfigurieren Sie bidirektionalen Datenverkehr im Profil.

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

3. Beenden

4. Legen Sie die Schnittstelle für den exportierten Datenverkehr fest.

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

5. Aktivieren Sie den Export von IP-Datenverkehr auf der Schnittstelle.

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

6. Beenden

7. Starten Sie die Erfassung. Die Erfassung ist jetzt aktiv. Gestatten Sie die Erfassung der erforderlichen Daten.

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

8. Stoppen Sie die Erfassung.

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

9. Exportieren Sie die Erfassung auf einen externen TFTP-Server.

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

10. Löschen Sie das Profil, sobald die erforderlichen Daten gesammelt wurden.

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

Nachteile beim Export von IP-Datenverkehr

Der Export von IP-Datenverkehr weist gegenüber der EPC-Methode folgende Nachteile auf:

- Bei der Schnittstelle, in die der erfasste Datenverkehr exportiert wird, muss es sich um eine Ethernet-Schnittstelle handeln.
- Keine Unterstützung für IPv6.
- Keine Layer-2-Informationen, nur Layer 3 und höher.

Beispiel für Cisco IOS-XE-Konfiguration

Die Funktion "Embedded Packet Capture" wurde in Cisco IOS-XE® Version 3.7 - 15.2(4)S eingeführt. Die Konfiguration der Erfassung unterscheidet sich von Cisco IOS®, da sie weitere Funktionen hinzufügt.

EPC-Basiskonfiguration

1. Legen Sie den Ort fest, an dem die Erfassung erfolgt:

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

2. Zuordnen eines Filters Der Filter wird entweder inline angegeben, oder es kann auf eine ACL oder Klassenzuordnung verwiesen werden:

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

3. Erfassung starten:

```
monitor capture CAP start
```

4. Die Erfassung ist jetzt aktiv. Erlauben Sie die Erfassung der erforderlichen Daten.

5. Erfassung beenden:

```
monitor capture CAP stop
```

6. Untersuchen der Erfassung in einer Zusammenfassungsansicht:

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

7. Untersuchen der Erfassung in einer detaillierten Ansicht:

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

8. Darüber hinaus können Sie die Erfassung zur weiteren Analyse im PCAP-Format exportieren:

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

9. Sobald die erforderlichen Daten erfasst wurden, entfernen Sie die Erfassung:

```
no monitor capture CAP
```

Zusätzliche Informationen

- Die Erfassung wird an physischen Schnittstellen, Subschnittstellen und Tunnelschnittstellen durchgeführt.
- Network Based Application Recognition (NBAR)-basierte Filter (die die **match protocol** unter class-map) werden derzeit nicht unterstützt.
- Weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen finden Sie unter Best Practices für Suchbefehle.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für EPC, das auf Cisco IOS-XE® ausgeführt wird, wird dieser Debug-Befehl verwendet, um sicherzustellen, dass EPC ordnungsgemäß eingerichtet ist:

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

Zugehörige Informationen

- Embedded Packet Capture – Cisco IOS-XE
- Embedded Packet Capture – Cisco IOS
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.