Verwenden von Paketerfassungsverfahren auf einem FirePOWER-Gerät

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Befehl **tcpdump** verwenden, um Pakete zu erfassen, die von einer Netzwerkschnittstelle Ihres FirePOWER-Geräts erkannt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco FirePOWER-Geräts und der Modelle für virtuelle Geräte verfügen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt. Es verwendet die Berkeley Packet Filter (BPF)-Syntax.

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 kennen.

> **Warnung**: Wenn Sie den **tcpdump**-Befehl auf einem Produktionssystem ausführen, kann dies die Netzwerkleistung beeinträchtigen.

Schritte zum Erfassen von Paketen

Melden Sie sich bei der CLI Ihres Firepower-Geräts an.

Geben Sie in Version 6.1 und höher **capture-traffic ein**. Beispiele,

<#root>

```
> capture-traffic
```

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

Geben Sie in Version 6.0.x.x und früheren Versionen **system support capture-traffic ein**. Beispiele,

<#root>

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

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

Nachdem Sie eine Auswahl getroffen haben, werden Sie zur Eingabe der folgenden Optionen aufgefordert:

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

Um ausreichend Daten aus den Paketen zu erfassen, muss die -s-Option verwendet werden, um die Snaplength richtig einzustellen. Die Snaplength kann auf einen Wert festgelegt werden, der dem konfigurierten Maximum Transmission Unit (MTU)-Wert der Schnittstellensatz-Konfiguration entspricht, die standardmäßig auf 1518 festgelegt ist.

> **Warnung:** Wenn Sie den Datenverkehr auf dem Bildschirm erfassen, kann dies die Leistung des Systems und des Netzwerks beeinträchtigen. Cisco empfiehlt, die Option -w <Dateiname> mit dem Befehl tcpdump zu verwenden. Es erfasst die Pakete in einer Datei. Wenn Sie den Befehl ohne die Option -w ausführen, drücken Sie die Tastenkombination **Strg-C**, um den Vorgang zu beenden.

Beispiel für die Option -w <Dateiname>:

<#root>

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

> **Achtung**: Verwenden Sie keine Pfadelemente, wenn Sie den Namen der Paketerfassungsdatei (pcap) angeben. Sie müssen nur den pcap-Dateinamen angeben, der in der Appliance erstellt werden soll.

Wenn Sie eine begrenzte Anzahl von Paketen erfassen möchten, können Sie die Anzahl der zu erfassenden Pakete mit dem Flag -c <Pakete> angeben. So erfassen Sie beispielsweise genau 5.000 Pakete:

<#root>

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

Zusätzlich kann am Ende des Befehls ein BPF-Filter hinzugefügt werden, um die Paketerfassung zu begrenzen. Um beispielsweise die Paketerfassung auf 5.000 Pakete mit der Quell- oder Ziel-IP-Adresse 192.0.2.1 zu beschränken, können Sie die folgenden Optionen verwenden:

<#root>

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

Wenn Sie den mit einem virtuellen LAN (VLAN) gekennzeichneten Datenverkehr erfassen, müssen Sie das VLAN mit der BPF-Syntax angeben. Andernfalls enthält pcap keines der markierten VLAN-Pakete. In diesem Beispiel wird die Erfassung auf Datenverkehr beschränkt, der vom VLAN mit 192.0.2.1 markiert ist:

<#root>

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

Wenn Sie sich nicht sicher sind, ob der Datenverkehr VLAN-markiert ist, kann diese Syntax verwendet werden, um den Datenverkehr von 192.0.2.1 zu erfassen, der VLAN-markiert ist und nicht:

<#root>

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

> **Hinweis**: Im vorherigen Beispiel sind die Klammern erforderlich, damit das 'or' nicht nur für 'vlan' gilt. Die einfachen Anführungszeichen werden dann benötigt, um mögliche Fehlinterpretationen der Klammern durch die Shell zu vermeiden.

Die Angabe eines VLAN-Tags erfasst den gesamten VLAN-Datenverkehr, der mit dem Rest der BPF übereinstimmt. Wenn Sie jedoch ein bestimmtes VLAN-Tag erfassen möchten, können Sie angeben, welches VLAN-Tag Sie erfassen möchten:

<#root>

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

Nachdem Sie die gewünschten Optionen festgelegt und die **Eingabetaste** gedrückt haben, beginnt tcpdump mit der Erfassung des Datenverkehrs.

> **Tipp**: Wenn die Option -c nicht verwendet wurde, drücken Sie die Tastenkombination **Strg-C**, um die Erfassung zu beenden.

Sobald Sie die Erfassung beenden, erhalten Sie eine Bestätigung. Beispiele:

<#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.
```

PCAP-Datei kopieren

Um eine pcap-Datei von einer FirePOWER-Appliance auf ein anderes System zu kopieren, das eingehende SSH-Verbindungen akzeptiert, verwenden Sie den folgenden Befehl:

<#root>

> system file secure-copy hostname username destination_directory pcap_file

Nachdem Sie die **Eingabetaste** gedrückt haben, werden Sie zur Eingabe des Kennworts für das Remote-System aufgefordert. Die Datei kann über das Netzwerk kopiert werden.

Hinweis: In diesem Beispiel bezieht sich der Hostname auf den Namen oder die IP-Adresse des Ziel-Remotehosts, der Benutzername gibt den Namen des Benutzers auf dem Remotehost an, das destination_directory gibt den Zielpfad auf dem Remotehost an und die pcap_file gibt die lokale pcap-Datei für die Übertragung an.

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.