Häufig gestellte Fragen zu Content Security Appliances: Wie erfolgt die Paketerfassung auf einer Cisco Content Security Appliance?

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Paketerfassungen auf den Cisco Content Security Appliances durchgeführt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco E-Mail Security Appliance (ESA)
- Cisco Web Security Appliance (WSA)
- Cisco Security Management Appliance (SMA)
- AsyncOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Versionen von AsyncOS.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Wie erfolgt die Paketerfassung auf einer Cisco Content Security Appliance?

Führen Sie die folgenden Schritte aus, um mithilfe der GUI eine Paketerfassung (**tcpdump**-Befehl) durchzuführen:

1. Navigieren Sie in der Benutzeroberfläche zu **Hilfe und Unterstützung > Paketerfassung**.
2. Bearbeiten Sie die Paketerfassungseinstellungen nach Bedarf, z. B. die Netzwerkschnittstelle, auf der die Paketerfassung ausgeführt wird. Sie können einen der vordefinierten Filter verwenden oder einen benutzerdefinierten Filter mit einer beliebigen Syntax erstellen, die vom Unix **tcpdump**-Befehl unterstützt wird.
3. Klicken Sie auf **Erfassung starten**, um mit der Erfassung zu beginnen.
4. Klicken Sie auf **Erfassung beenden**, um die Erfassung zu beenden.
5. Laden Sie die Paketerfassung herunter.

Führen Sie die folgenden Schritte aus, um eine Paketerfassung (**tcpdump-**Befehl) mit der CLI durchzuführen:

1. Geben Sie diesen Befehl in die CLI ein:

```
wsa.run> packetcapture

Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     (tcp port 80 or tcp port 3128)
```

2. Wählen Sie den Vorgang aus, den Sie ausführen möchten:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. Geben Sie die maximal zulässige Größe für die Erfassungsdatei (in MB) ein:

```
[200]> 200

Do you want to stop the capture when the file size is reached? (If not, a new
```

```
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:

1. Management

2. T1

3. T2
```

4. Geben Sie den Namen oder die Anzahl einer oder mehrerer Schnittstellen ein, von denen Pakete erfasst werden sollen, getrennt durch Kommas:

```
[1]> 1
```

5. Geben Sie den Filter ein, den Sie für die Erfassung verwenden möchten. Geben Sie das Wort **CLEAR ein**, um den Filter zu löschen und alle Pakete an den ausgewählten Schnittstellen zu erfassen.

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80


Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```

6. Wählen Sie den **Start-**Vorgang aus, um mit der Erfassung zu beginnen:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> start


Status: Capture in progress (Duration: 0s)

File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```

7. Wählen Sie den **Stopp-**Vorgang aus, um die Erfassung zu beenden:

```
- STOP - Stop packet capture.

- STATUS - Display current capture status.

- SETUP - Change packet capture settings.

[]> stop


Status: No capture running (Capture stopped by user)


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```