Domande frequenti sulle appliance di sicurezza dei contenuti: Come è possibile acquisire un pacchetto su un'appliance Cisco Content Security?

Sommario

Introduzione

In questo documento viene descritto come eseguire le acquisizioni di pacchetti sulle appliance Cisco Content Security.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni di questo documento si basano su tutte le versioni di AsyncOS.

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.

Come è possibile acquisire un pacchetto su un'appliance Cisco Content Security?

Per eseguire un'acquisizione del pacchetto (comando **tcpdump**) con la GUI, completare i seguenti passaggi:

1. Selezionare **Help and Support > Packet Capture** (Guida e supporto) sulla GUI.
2. Modificare le impostazioni di acquisizione dei pacchetti in base alle esigenze, ad esempio l'interfaccia di rete su cui viene eseguita l'acquisizione. È possibile utilizzare uno dei filtri predefiniti oppure creare un filtro personalizzato utilizzando qualsiasi sintassi supportata dal comando Unix **tcpdump**.
3. Per avviare l'acquisizione, fare clic su **Start Capture** (Avvia acquisizione).
4. Per terminare l'acquisizione, fare clic su **Stop Capture** (Interrompi acquisizione).
5. Scaricare l'acquisizione del pacchetto.

Completare questi passaggi per eseguire un'acquisizione del pacchetto (comando **tcpdump**) con la CLI:

1. Immettere questo comando nella CLI:

```
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. Scegliere l'operazione da eseguire:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. Immettere la dimensione massima consentita per il file di acquisizione (in MB):

```
[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. Immettere il nome o il numero di una o più interfacce da cui acquisire i pacchetti, separati da virgole:

```
[1]> 1
```

5. Immettere il filtro che si desidera utilizzare per l'acquisizione. Immettere la parola CLEAR per cancellare il filtro e acquisire tutti i pacchetti sulle interfacce selezionate.

```
[(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. Per avviare l'acquisizione, scegliere l'operazione di avvio:

```
- 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. Per terminare l'acquisizione, scegliere l'operazione di **arresto**:

```
- 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
```