Utilizzare le procedure di acquisizione dei pacchetti sulla periferica Firepower

Sommario

Introduzione

In questo documento viene descritto come usare il comando **tcpdump** per acquisire i pacchetti rilevati da un'interfaccia di rete del dispositivo Firepower.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei modelli di dispositivi virtuali e dei dispositivi Cisco Firepower.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. Utilizza la sintassi Berkeley Packet Filter (BPF).

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.

> **Avviso**: l'esecuzione del comando **tcpdump** su un sistema di produzione può influire sulle prestazioni della rete.

Passaggi per l'acquisizione dei pacchetti

Accedere alla CLI del dispositivo Firepower.

Nelle versioni 6.1 e successive, immettere **capture-traffic**. Ad esempio,

<#root>

```
> capture-traffic
```

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

Nelle versioni 6.0.x.x e precedenti, immettere **system support capture-traffic**. Ad esempio,

<#root>

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

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

Dopo aver effettuato una selezione, vengono richieste le opzioni seguenti:

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

Per acquisire dati sufficienti dai pacchetti, è necessario usare l'opzione -s per impostare correttamente la lunghezza dello snapshot. È possibile impostare snaplength su un valore che corrisponde al valore MTU (Maximum Transmission Unit) configurato nella configurazione dell'insieme di interfacce, che assume il valore predefinito di 1518.

> **Avviso**: l'acquisizione del traffico sullo schermo può compromettere le prestazioni del sistema e della rete. Cisco consiglia di usare l'opzione -w <filename> con il comando tcpdump. Cattura i pacchetti in un file. Se si esegue il comando senza l'opzione -w, premere la combinazione di tasti **Ctrl-C** per uscire.

Esempio di opzione -w <nomefile>:

<#root>

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

> **Attenzione**: non utilizzare alcun elemento path quando si specifica il nome file di acquisizione del pacchetto (pcap). È necessario specificare solo il nome del file pcap da creare nell'accessorio.

Se è consigliabile acquisire un numero limitato di pacchetti, è possibile utilizzare il flag -c <packets> per specificare il numero di pacchetti da acquisire. Ad esempio, per acquisire esattamente 5000 pacchetti:

<#root>

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

Inoltre, è possibile aggiungere un filtro BPF alla fine del comando per limitare i pacchetti da acquisire. Ad esempio, per limitare l'acquisizione dei pacchetti a 5000 pacchetti con indirizzo IP di origine o destinazione 192.0.2.1, è possibile usare le seguenti opzioni:

<#root>

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

Quando si acquisisce il traffico contrassegnato come VLAN (Virtual LAN), è necessario specificare la VLAN con la sintassi BPF. In caso contrario, la capsula non contiene nessuno dei pacchetti VLAN con tag. Ad esempio, questo esempio limita l'acquisizione al traffico con tag VLAN da 192.0.2.1:

<#root>

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

Se non si è certi che il traffico sia contrassegnato dalla VLAN, è possibile usare questa sintassi per acquisire il traffico proveniente dalla versione 192.0.2.1 che è o non è contrassegnata dalla VLAN:

<#root>

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

> **Nota**: nell'esempio precedente, le parentesi sono necessarie in modo che 'or' non si applichi solo a 'vlan'. Le virgolette singole sono quindi necessarie per evitare ogni possibile interpretazione errata delle parentesi da parte del guscio.

La specifica di un tag VLAN acquisisce tutto il traffico VLAN che corrisponde al resto del BPF. Tuttavia, se si desidera acquisire un tag VLAN specifico, è possibile specificare il tag VLAN da acquisire nel modo seguente:

<#root>

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

Dopo aver specificato le opzioni desiderate e aver premuto **Invio**, tcpdump inizia a catturare il traffico.

> **Suggerimento**: se l'opzione -c non è stata utilizzata, premere la combinazione di tasti **Ctrl-C** per interrompere l'acquisizione.

Una volta interrotta la cattura, si riceve una conferma. Ad esempio:

<#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.
```

Copiare un file Pcap

Per copiare un file pcap da un accessorio FirePOWER a un altro sistema che accetta connessioni SSH in entrata, utilizzare questo comando:

<#root>

> system file secure-copy hostname username destination_directory pcap_file

Dopo aver premuto **Invio**, viene richiesta la password per il sistema remoto. Il file può essere copiato in rete.

> **Nota**: in questo esempio, il nome host fa riferimento al nome o all'indirizzo IP dell'host remoto di destinazione, il nome utente specifica il nome dell'utente sull'host remoto, la directory di destinazione specifica il percorso di destinazione sull'host remoto e il file pcap specifica il file pcap locale per il trasferimento.

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).