Visualizza flussi attivi in Snort

Sommario

Introduzione

In questo documento viene descritto come usare il comando show snort flows per visualizzare i flussi attivi di Snort.

Contrasto rispetto a questa release

In Secure Firewall 7.4 and Below		New to Secure Firewall 7.6
• No way to look at active flows in Snort		• New CLI `show snort flows` can be used to view active flows in Snort

Panoramica delle funzionalità

- La nuova CLI show snort flow viene utilizzata per visualizzare i flussi attivi nella Snort 3 flow cache.
- Vengono fornite informazioni dettagliate sui flussi attivi durante l'esecuzione del processo Snort 3.
- L'output fornisce lo stato del flusso di dati, dell'IP di origine e di destinazione e della porta.

- Consente di isolare ed eseguire il debug dei problemi negli ambienti di produzione.

Spoiler (Evidenziato da leggere)

NOTA: Questa funzionalità è stata introdotta per consentire di esaminare i flussi di snort attivi e gli stati del client e del server relativi a flusso, timeout e altro ancora.

NOTA: Questa funzionalità è stata introdotta per consentire di esaminare i flussi di snort attivi e gli stati del client e del server relativi a flusso, timeout e altro ancora.

Piattaforme software e hardware minime

Manager(s) and Version (s)	Application (FTD) and Minimum Version of Application	Supported Platforms
• (CLI only)	FTD 7.6.0	All platforms running FTD and Snort 3

Snort 3, IPv6, supporto multi-istanza e HA/clustering

- Funziona sia con IPv4 che con IPv6.
- Richiede che Snort 3 sia il motore di rilevamento

FTD	
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes

Altri aspetti del supporto

Platforms	
FTD	
Licenses Required	Essentials
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes

Descrizione delle funzionalità e procedura dettagliata

In questa sezione viene fornita una procedura dettagliata, incluso il timeout di flusso, e i dettagli su altre funzionalità.

Nuova interfaccia CLI Mostra flussi di snort

<#root>

```
> show snort flows
```

```
TCP 0: x1.x1.x1.2/38148 x1.x1.x1.1/22 pkts/bytes client 9/2323 server 6/2105 idle 7s, uptime 7s, timeou
ICMP 0: x1.x1.x1.2 type 8 x1.x1.x1.1 pkts/bytes client 1/98 server 1/98 idle 0s, uptime 0s, timeout 3m0
UDP 0: x1.x1.x1.1/40101 x1.x1.x1.1/12345 pkts/bytes client 3/141 server 0/0 idle 19s, uptime 58s, timeo
```

Nell'esempio vengono mostrati tre flussi: TCP, ICMP e UDP.

Per il flusso TCP, i valori sono:

- Protocollo - TCP/ICMP/UDP/IP
- ID spazio indirizzi - ID VRF dell'interfaccia
- SourceIP/Port: x1,x1,x1,2/38148
- IP/porta di destinazione: x1,x1,x1,1/22
- Pacchetti/byte client - 9/2323
- Pacchetti/byte server - 6/2105
- Idle - Tempo trascorso dall'ultimo pacchetto nel flusso
- Tempo di attività - Tempo trascorso dall'impostazione del flusso
- Timeout - Timeout flusso
- Stato client (solo flussi TCP) - EST

- Stato server (solo flussi TCP) - EST

Stati di flusso client e server

- Lo stato del client e lo stato del server nell'output vengono visualizzati solo se il protocollo è TCP.
- Questi sono i valori possibili e il significato di ogni acronimo, per ogni stato:

State Acronym	Description
LST	Listen
SYS	SYN Sent
SYR	SYN received
EST	Established
MDS	Midstream Sent
MDR	Midstream Received
FW1	Final Wait 1
FW2	Final Wait 2
CLW	Close Wait
CLG	Closing
LAK	Last ACK
TWT	Time wait
CLD	Closed

Opzioni filtro

Il comando show snort flows supporta le opzioni di filtraggio in cui vengono generati solo i flussi che corrispondono ai filtri. La sintassi è

show snort flows <opzione filtro> <valore>

Le opzioni di filtro sono:

- proto - TCP/UDP/IP/ICMP

- src_ip - filtra i flussi in base all'ip di origine
- dst_ip - filtra i flussi in base all'ip di destinazione
- src_port - filtra i flussi per porta di origine
- dst_port - filtra i flussi in base alla porta di destinazione

Il comando > show snort flows proto TCP elenca solo i flussi TCP:

```
TCP 0: x1.x1.x1.2/45508 x1.x1.x1.1/22 pkts/bytes client 10/2389 server 7/2171 idle
30s, uptime 150s, timeout 59m30s state client CLW server FW2
```

Spoiler (Evidenziato da leggere)

NOTA: è inoltre possibile utilizzare più filtri nel comando. Ad esempio,

> show snort flows proto TCP src_ip x1.x1.x1.2 - genera flussi TCP con src ip x1.x1.x2

NOTA: è inoltre possibile utilizzare più filtri nel comando. Ad esempio, > show snort flows proto TCP src_ip x1.x1.x1.2 - genera flussi TCP con src ip x1.x1.x1.2

Potenziale risposta di errore

- L'utente CLI ha ricevuto una risposta "impossibile elaborare il comando, riprovare più tardi".
- Questo si verifica quando, ad esempio, l'Snort 3 è inattivo, quando l'Snort 3 è occupato o quando l'Snort 3 non elabora i comandi dei socket di controllo (ad esempio, i thread in stato bloccato).
- Condizioni per il corretto funzionamento della CLI:
    - Lo snort 3 è in esecuzione.
    - Lo snort 3 risponde ai comandi di controllo sul socket del dominio UNIX.

Arresto di CLI/Output

- Come per qualsiasi comando CLI, è possibile visualizzare il prompt dei comandi premendo CTRL+C , ma il comando è già stato passato a tutti i thread di pacchetto ed è in esecuzione fino al completamento in Snort.
- Il comando viene completato quando si applicano entrambe le condizioni:
    - Tutti i flussi nella cache di flusso sono stati visualizzati
    - Tutti i flussi che corrispondono ai filtri nel comando CLI sono stati scritti nei file che servono da input per il comando da inviare nella CLI.

Conseguenze sulle prestazioni

- Questa è una CLI di debug. Per ogni pacchetto che esaminiamo, osserviamo circa 100 flussi dalla tabella dei flussi e stampiamo i flussi che corrispondono ai criteri.
- L'esecuzione di show snort flow ha un impatto sulle prestazioni.

Riferimenti

Wireless LAN Controller serie 9800

Q: È possibile utilizzare più di un filtro in "show snort flows"?

A: Sì, la CLI supporta l'uso di più filtri alla volta ed emette flussi corrispondenti a entrambi i filtri.

Q: Quali protocolli sono supportati?

A: IP/TCP/UDP/ICMP

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).