Actieve stromen in kleur weergeven

Inhoud

Inleiding

Dit document beschrijft hoe u de opdracht Snel-stromen tonen kunt gebruiken om actieve stromen in Sort te bekijken.

Eerdere versies van deze release contrasteren

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

Overzicht van functies

- De nieuwe CLI toont snortstromen wordt gebruikt om de actieve stromen in het snort 3 flow cache te bekijken.
- Dit geeft details over de actieve stromen in het uitvoeren van Snort 3 proces.
- De uitvoer geeft de status van de gescande stroom, de bron en de bestemming IP en poort.
- Het helpt bij het isoleren en debuggen van problemen in productieomgevingen.

Spoiler (Markeren om te lezen)

OPMERKING: Deze functie is geïntroduceerd om te kunnen kijken naar actieve gesorteerde stromen en client, server statussen van flow, timeout en meer.

OPMERKING: Deze functie is geïntroduceerd om te kunnen kijken naar actieve gesorteerde stromen en client, server statussen van flow, timeout en meer.

Minimale software- en hardwareplatforms

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

Ondersteuning van Snort 3, IPv6, meerdere instanties en HA/Clustering

- Werkt met zowel IPv4 als IPv6.
- Vereist dat Snort 3 de detectiemotor is

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

Andere aspecten van de ondersteuning

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

Beschrijving en doorloop van functies

Deze sectie verstrekt een analyse, met inbegrip van stroomonderbreking, en details over meer eigenschappen.

Nieuw Toon Snelstromen CLI

<#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
```

Dit voorbeeld toont drie stromen:TCP, ICMP en UDP.

Voor de TCP-stroom zijn de waarden:

- Protocol - TCP/ICMP/UDP/IP
- Address Space ID - VRF-id van de interface
- SourceIP/poort: x1,x1,x1,2/38148
- IP-bestemming/poort: x1,x1,x1,1/22
- Clientpakketten/bytes - 9/2323
- Server-pakketten/bytes - 6/2105
- Inactief - tijd sinds laatste pakket in flow
- Uptime - Time sinds flow is ingesteld
- Time-out - Flow time-out
- Clientstatus (alleen TCP-stromen) - EST

- Serverstatus (alleen TCP-stromen) - EST

Stroomstatus van client en server

- De staat van de cliënt en de serverstaat in de output verschijnen slechts als het protocol TCP is.
- Dit zijn mogelijke waarden en wat elk acroniem betekent, voor elke staat:

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

Filteropties

De opdracht Stromen tonen ondersteunt filteropties waarbij alleen de stromen die overeenkomen met de filters worden uitgevoerd. De syntaxis is

snelstromen weergeven <filter optie> <waarde>

De filteropties zijn:

- Proto -TCP/UDP/IP/ICMP

- src_ip - filterstromen per bron ip
- dst_ip - filterstromen per bestemming ip
- src_port - filterstromen per bronpoort
- dst_port - filterstromen per bestemmingshaven

De opdracht > snort flows proto TCP toont alleen TCP-stromen:

```
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 (Markeren om te lezen)

OPMERKING: U kunt ook meer dan één filter in de opdracht gebruiken. Voorbeeld,

> tonen snortstromen proto TCP src_ip x1.x1.x1.2 - outputs TCP stromen die de src ip x1.x1.x1.x1.2 hebben

OPMERKING: U kunt ook meer dan één filter in de opdracht gebruiken. > bijvoorbeeld tonen snortstromen proto TCP src_ip x1.x1.x1.2 - outputs TCP-stromen die de src ip x1.x1.x1.2 hebben

Mogelijke fout respons

- CLI-gebruiker kan een antwoord krijgen "kan de opdracht niet verwerken, probeer het later opnieuw".
- Dit gebeurt bijvoorbeeld als Snort 3 is ingedrukt, als Snort 3 bezet is of als Snort 3 geen besturingstokopdrachten verwerkt (zoals threads in stuck state).
- Voorwaarden waaronder CLI met succes kan worden uitgevoerd:
    - Snuit 3 is actief.
    - Snort 3 reageert op besturingsopdrachten via UNIX domain socket.

CLI/output stoppen

- Als een CLI-opdracht kunt u de opdrachtprompt krijgen door op CTRL +C te drukken, maar de opdracht is al aan alle pakketthreads doorgegeven en wordt in Snort uitgevoerd.
- De opdracht wordt voltooid wanneer beide voorwaarden van toepassing zijn:
    - Alle stromen in het flow cache zijn bekeken
    - Alle stromen die overeenkomen met de filters in de CLI-opdracht zijn naar de bestanden geschreven die als invoer voor de opdracht naar uitvoer in de CLI dienen.

Effect op prestaties

- Dit is een debug CLI. Voor elk pakket dat we doorlopen, kijken we naar ongeveer 100 stromen uit de flowtabel en printen we de stromen die voldoen aan de criteria.
- Het lopen toont korte stromen heeft een prestatieseffect.

Referenties

Veelgestelde vragen

Q: Kunnen we meer dan één filter gebruiken in "Toon snortstromen

A : Ja, de CLI ondersteunt het verstrekken van meer dan één filter tegelijkertijd en outputs die beide filters aanpassen.

Q: Welke protocollen worden ondersteund?

A : IP/TCP/UDP/ICMP

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.