DNS Guard begrijpen in Secure Firewall 7.7.0

Inhoud

Inleiding

In dit document wordt de DNS Guard-functie in Secure Firewall 7.7.0 beschreven, waarbij de nadruk ligt op de functionaliteit en probleemoplossing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Inzicht in DNS-protocol en UDP-sessies
- Bekendheid met Snort 3 en het sessiebeheer ervan

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall Threat Defense (FTD) versie 7.7.0
- Firepower Management Center (FMC) versie 7.7.0
- Snort versie 3

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

DNS is een op UDP-verzoeken gebaseerd protocol met kortdurende sessies. In tegenstelling tot Lina worden de DNS-sessies in Snort 3 niet onmiddellijk na de DNS-reactie gewist. In plaats daarvan worden DNS-sessies gesnoeid op basis van een doorstroomtijd van 120 seconden of meer. Dit leidt tot onnodige sessieaccumulatie, die anders zou kunnen worden gebruikt voor andere TCP- of UDP-verbindingen.

Vergelijking met de vorige release

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• The DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout.		• DNS sessions in Snort 3 are released immediately after the DNS Response is inspected and handled.

Nieuwe functie in 7.7

Nieuwe functies

- Deze "DNS Guard"-functie wist de UDP-stroom onmiddellijk na ontvangst en inspectie van het DNS-responspakket.
- Dit is een protocolspecifieke verbetering ten opzichte van het huidige ontwerp en de architectuur van Snort 3.

Basisprincipes: ondersteunde platforms, licenties

FTD-platforms en -beheerders

FTD Platforms	All
FMC on 7.7.0 FMC Rest API	Yes No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3

Ondersteunde platforms

Andere ondersteunende aspecten

FTD	
Licenses Required	Essentials, URL, Threat, Malware
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

Licenties en compatibiliteit

Probleem

In eerdere releases, met name Secure Firewall 7.6 en lager, blijft de DNS-sessie als een stabiele Snort 3-stroom totdat deze wordt gesnoeid door de UDP-time-out. Dit veroorzaakt problemen met sessiebeheer en kan leiden tot inefficiënt gebruik van bronnen omdat DNS-sessies zich onnodig ophopen.

Stappen om het probleem opnieuw te creëren

Om het probleem te observeren, voert u de opdracht Lina uit om actieve DNS-verbindingen vanaf de Lina-zijde te controleren:

```
show conn detail
```

In Secure Firewall 7.6 en lager blijven DNS-sessies actief tot de UDP-time-out, wat leidt tot inefficiëntie van bronnen.

Oplossing

De DNS Guard-functie in Secure Firewall 7.7.0 lost dit probleem op door de UDP-stroom onmiddellijk te wissen na ontvangst en inspectie van het DNS-reactiepakket. Deze protocolspecifieke verbetering zorgt ervoor dat DNS-sessies in Snort 3 onmiddellijk worden

vrijgegeven, waardoor onnodige sessieaccumulatie wordt voorkomen en de efficiëntie van bronnen wordt verbeterd.

Overzicht van functies

De DNS Guard-functie wist de UDP-stroom onmiddellijk na ontvangst en inspectie van het DNS-reactiepakket. De Snort-stroom hoeft niet te wachten tot de UDP-time-out optreedt.

- Wanneer er voldoende DNS-verkeer op de box staat, leidt deze functie tot minder actieve stromen door tijdige opruiming van de bijbehorende Snort-stromen.
- Meer TCP/UDP-verbindingen kunnen door de doos worden verwerkt zonder actieve verbindingen te snoeien, wat de algehele werkzaamheid van de doos verbetert.

Probleemoplossing

Als u de functionaliteit van de DNS Guard-functie wilt controleren, gebruikt u de opdracht Lina om ervoor te zorgen dat UDP-sessies worden vrijgegeven nadat u een DNS-reactie hebt ontvangen:

<#root>

>

show snort counters | begin stream_udp

Voorbeelduitvoer zonder DNS-bewakingsfunctie:

```
stream_udp sessions: 755
 max: 12
created: 755
released: 0
total_bytes: 124821
```

<#root>

>

show snort counters | begin stream_udp

Voorbeeld van uitvoer met DNS-bewakingsfunctie:

```
stream_udp sessions: 899
max: 14
created: 899
```

```
released: 899
total_bytes: 135671
```

De uitgangen geven aan dat alle gemaakte sessies tijdig worden vrijgegeven, wat de juiste werking van de DNS Guard-functie bevestigt.

Gerelateerde informatie

- Cisco Technical Support en downloads

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.