Secure Firewall 7.7.0의 DNS Guard 이해

목차

소개

이 문서에서는 Secure Firewall 7.7.0의 DNS Guard 기능에 대해 설명하며, 기능 및 문제 해결에 중점을 둡니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- DNS 프로토콜 및 UDP 세션 이해
- Snort 3 및 해당 세션 관리에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD(Secure Firewall Threat Defense) 버전 7.7.0
- FMC(firepower Management Center) 버전 7.7.0
- Snort 버전 3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

DNS는 짧은 라이브 세션이 있는 UDP 요청 응답 기반 프로토콜입니다. Lina와 달리 Snort 3의 DNS 세션은 DNS 응답 직후에 지워지지 않습니다. 대신 DNS 세션은 120초 이상의 흐름 시간 초과에 따라 정리됩니다. 그러면 불필요한 세션이 누적되며, 그렇지 않으면 다른 TCP 또는 UDP 연결에 사용될 수 있습니다.

이전 릴리스와 비교

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.

7.7의 새로운 기능

새로운 기능

- 이 "DNS Guard" 기능은 DNS 응답 패킷을 수신 및 검사한 직후 UDP 흐름을 지웁니다.
- 이는 Snort 3의 현재 설계 및 아키텍처에 비해 프로토콜별로 향상된 기능입니다.

기본: 지원되는 플랫폼, 라이센싱

FTD 플랫폼 및 관리자

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

지원되는 플랫폼

기타 지원 측면

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

라이센싱 및 호환성

문제

이전 릴리스, 특히 Secure Firewall 7.6 이하에서 DNS 세션은 UDP 시간 초과로 정리될 때까지 오래된 Snort 3 흐름으로 유지됩니다. 이로 인해 세션 관리 문제가 발생하고 DNS 세션이 불필요하게 누적됨에 따라 리소스를 비효율적으로 사용할 수 있습니다.

문제 재생성 단계

문제를 관찰하려면 Lina 명령을 실행하여 Lina 측의 활성 DNS 연결을 확인합니다.

```
show conn detail
```

Secure Firewall 7.6 이하에서 DNS 세션은 UDP 시간 초과가 될 때까지 활성 상태로 유지되므로 리소스 비효율성이 발생합니다.

솔루션

Secure Firewall 7.7.0의 DNS Guard 기능은 DNS 응답 패킷을 수신하고 검사한 후 즉시 UDP 흐름을 지움으로써 이 문제를 해결합니다. 이러한 프로토콜별 개선을 통해 Snort 3의 DNS 세션이 즉시 해제되어 불필요한 세션 축적을 방지하고 리소스 효율성을 개선할 수 있습니다.

기능 개요

DNS Guard 기능은 DNS 응답 패킷을 수신 및 검사한 직후 UDP 흐름을 지웁니다. Snort 플로우는 UDP 시간 초과가 발생할 때까지 기다리지 않아도 됩니다.

- 박스에 충분한 DNS 트래픽이 있을 경우, 이 기능은 해당 Snort 플로우의 적시 정리로 인해 활성 플로우의 수를 줄입니다.
- 활성 연결을 정리하지 않고도 상자에서 더 많은 TCP/UDP 연결을 처리할 수 있으므로 상자의 전반적인 성능이 향상됩니다.

문제 해결

DNS Guard 기능의 기능을 확인하려면 Lina 명령을 사용하여 DNS 응답을 수신할 때 UDP 세션이 해제되었는지 확인합니다.

<#root>

>

show snort counters | begin stream_udp

DNS 가드 기능이 없는 출력의 예:

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

<#root>

>

show snort counters | begin stream_udp

DNS 가드 기능이 있는 출력의 예:

```
stream_udp sessions: 899
max: 14
created: 899
released: 899
total_bytes: 135671
```

출력은 생성된 모든 세션이 적시에 릴리스되었음을 나타내며, 이는 DNS Guard 기능의 올바른 작동을 확인하는 것입니다.

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.