DNS Guard in Secure Firewall 7.7.0 verstehen

Inhalt

Einleitung

In diesem Dokument wird die Funktion DNS Guard in Secure Firewall 7.7.0 beschrieben. Der Schwerpunkt liegt auf der Funktionalität und Fehlerbehebung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Verständnis von DNS-Protokoll und UDP-Sitzungen
- Vertrautheit mit Snort 3 und dessen Sitzungsmanagement

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure Firewall Threat Defense (FTD) Version 7.7.0
- FirePOWER Management Center (FMC) Version 7.7.0
- Snort Version 3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

DNS ist ein UDP-anforderungsbasiertes Protokoll mit kurzen Sitzungen. Im Gegensatz zu Lina werden die DNS-Sitzungen in Snort 3 nicht unmittelbar nach der DNS-Antwort gelöscht. Stattdessen werden DNS-Sitzungen aufgrund eines Timeouts für den Datenfluss von 120 Sekunden oder mehr abgeschnitten. Dies führt zu unnötiger Sitzungsakkumulation, die andernfalls für andere TCP- oder UDP-Verbindungen verwendet werden könnte.

Vergleich mit der Vorgängerversion

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.

Neue Funktion in 7.7

Neue Funktionen

- Diese Funktion "DNS Guard" löscht den UDP-Fluss sofort nach dem Empfang und der Prüfung des DNS-Antwortpakets.
- Dies ist eine protokollspezifische Erweiterung gegenüber dem aktuellen Design und der aktuellen Architektur von Snort 3.

Grundlagen: Unterstützte Plattformen, Lizenzierung

FTD-Plattformen und -Manager

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

Unterstützte Plattformen

Weitere Support-Aspekte

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

Lizenzierung und Kompatibilität

Problem

In früheren Versionen, insbesondere Secure Firewall 7.6 und niedriger, bleibt die DNS-Sitzung als veralteter Snort 3-Fluss erhalten, bis sie vom UDP-Timeout abgeschnitten wird. Dies führt zu Problemen mit der Sitzungsverwaltung und kann zu einer ineffizienten Ressourcennutzung führen, da sich DNS-Sitzungen unnötig ansammeln.

Schritte zur Neuerstellung des Problems

Um das Problem zu beobachten, führen Sie den Befehl Lina aus, um aktive DNS-Verbindungen von der Lina-Seite aus zu überprüfen:

```
show conn detail
```

Bei Secure Firewall 7.6 und niedriger bleiben DNS-Sitzungen bis zum UDP-Timeout aktiv, was zu Ressourcenineffizienz führt.

Lösung

Die DNS Guard-Funktion in Secure Firewall 7.7.0 löscht das Problem, indem der UDP-Fluss nach dem Empfang und der Prüfung des DNS-Antwortpakets umgehend gelöscht wird. Diese protokollspezifische Erweiterung stellt sicher, dass DNS-Sitzungen in Snort 3 sofort freigegeben werden. Dadurch wird eine unnötige Sitzungsakkumulation verhindert und die Ressourceneffizienz verbessert.

Funktionsüberblick

Die DNS Guard-Funktion löscht den UDP-Fluss sofort nach dem Empfang und der Prüfung des DNS-Antwortpakets. Der Snort-Fluss muss nicht warten, bis ein UDP-Timeout auftritt.

- Wenn ausreichend DNS-Datenverkehr vorhanden ist, führt diese Funktion aufgrund der rechtzeitigen Bereinigung der entsprechenden Snort-Datenflüsse zu weniger aktiven Datenflüssen.
- Mehr TCP/UDP-Verbindungen können von der Box verarbeitet werden, ohne aktive Verbindungen zu entfernen. Dies verbessert die Gesamteffizienz der Box.

Fehlerbehebung

Um die Funktionalität von DNS Guard zu überprüfen, verwenden Sie den Befehl Lina, um sicherzustellen, dass UDP-Sitzungen freigegeben werden, wenn Sie eine DNS-Antwort erhalten:

```
<#root>

>

show snort counters | begin stream_udp
```

Beispielausgabe ohne DNS-Guard-Funktion:

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

```
<#root>

>
```

```
show snort counters | begin stream_udp
```

Beispielausgabe mit DNS Guard-Funktion:

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

Die Ausgaben zeigen an, dass alle erstellten Sitzungen rechtzeitig freigegeben werden, was den ordnungsgemäßen Betrieb der DNS Guard-Funktion bestätigt.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.