FirePOWER Management Center zeigt einige TCP-Verbindungsereignisse in die falsche Richtung an

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrund](#)
[Lösung](#)
[Schlussfolgerung](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die Gründe und Abhilfemaßnahmen für FirePOWER Management Center (FMC) beschrieben, die TCP-Verbindungsereignisse in umgekehrter Richtung anzeigen, wobei die Initiator-IP die Server-IP der TCP-Verbindung und die Responder-IP die Client-IP der TCP-Verbindung ist.

> **Hinweis**: Es gibt mehrere Gründe für solche Ereignisse. In diesen Dokumenten wird die häufigste Ursache dieses Symptoms erläutert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FirePOWER-Technologie
- Grundkenntnisse der Adaptive Security Appliance (ASA)
- Verständnis des Transmission Control Protocol (TCP)-Timing-Mechanismus

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER Threat Defense (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 6.0.1 und höher

- ASA Firepower Threat Defense (5512-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X, FP9300, FP4100) mit Softwareversion 6.0.1 und höher
- ASA mit FirePOWER-Modulen (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X, 5515-X, ASA 5525-X, ASA 5545-X 5-X, ASA 5585-X), die Softwareversionen 6.0.0 und höher ausführt
- FirePOWER Management Center (FMC) Version 6.0.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer klaren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrund

Bei einer TCP-Verbindung bezieht sich **Client** auf die IP, die das ursprüngliche Paket sendet. Das FirePOWER Management Center generiert ein Verbindungsereignis, wenn das verwaltete Gerät (der Sensor oder FTD) das ursprüngliche TCP-Paket einer Verbindung erkennt.

Auf Geräten, die den Status einer TCP-Verbindung verfolgen, ist eine **Leerlaufzeitüberschreitung** definiert, um sicherzustellen, dass Verbindungen, die irrtümlicherweise nicht von Endpunkten geschlossen werden, den verfügbaren Speicher über längere Zeiträume nicht verbrauchen. Der Standard-Timeout für Inaktivität bei etablierten TCP-Verbindungen auf FirePOWER beträgt **drei Minuten**. Eine TCP-Verbindung, die drei Minuten oder länger inaktiv geblieben ist, wird nicht vom FirePOWER IPS-Sensor verfolgt.

Das nachfolgende Paket nach dem Timeout wird als neuer TCP-Fluss behandelt, und die Weiterleitungsentscheidung wird gemäß der Regel getroffen, die diesem Paket entspricht.Wenn das Paket vom Server stammt, wird die IP-Adresse des Servers als Initiator dieses neuen Flusses aufgezeichnet. Wenn die Protokollierung für die Regel aktiviert ist, wird im FirePOWER Management Center ein Verbindungsereignis generiert.

> **Hinweis**: Gemäß konfigurierten Richtlinien unterscheidet sich die Weiterleitungsentscheidung für das Paket nach dem Timeout von der Entscheidung für das ursprüngliche TCP-Paket. Wenn die konfigurierte Standardaktion "Block" (Blockieren) lautet, wird das Paket verworfen.

Ein Beispiel für dieses Symptom ist der folgende Screenshot:

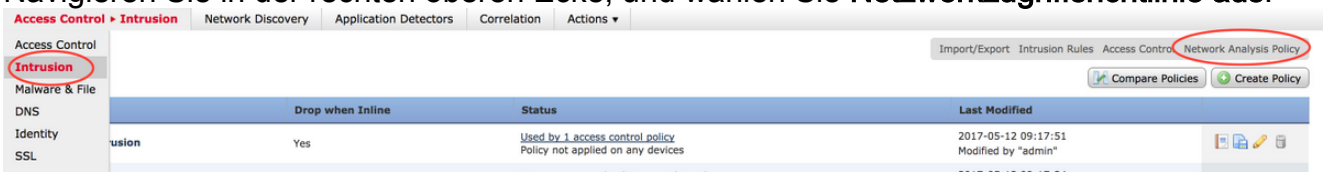
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

Lösung

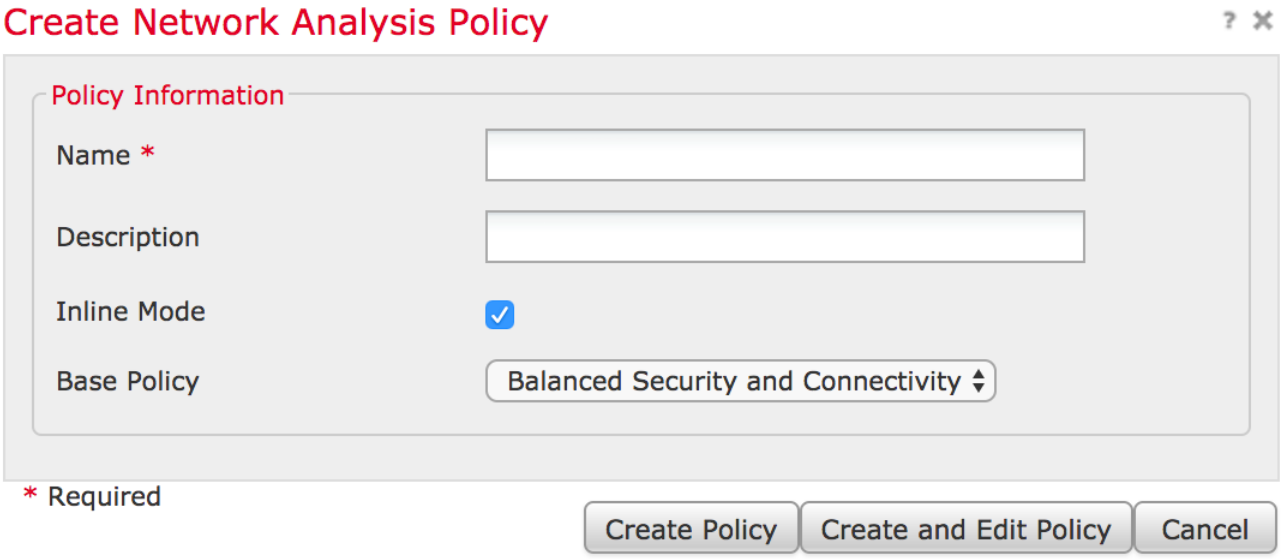
Das oben genannte Problem wird durch die Erhöhung der **Timeout** von TCP-Verbindungen gemindert. Um das Timeout zu ändern,

1. Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle**.

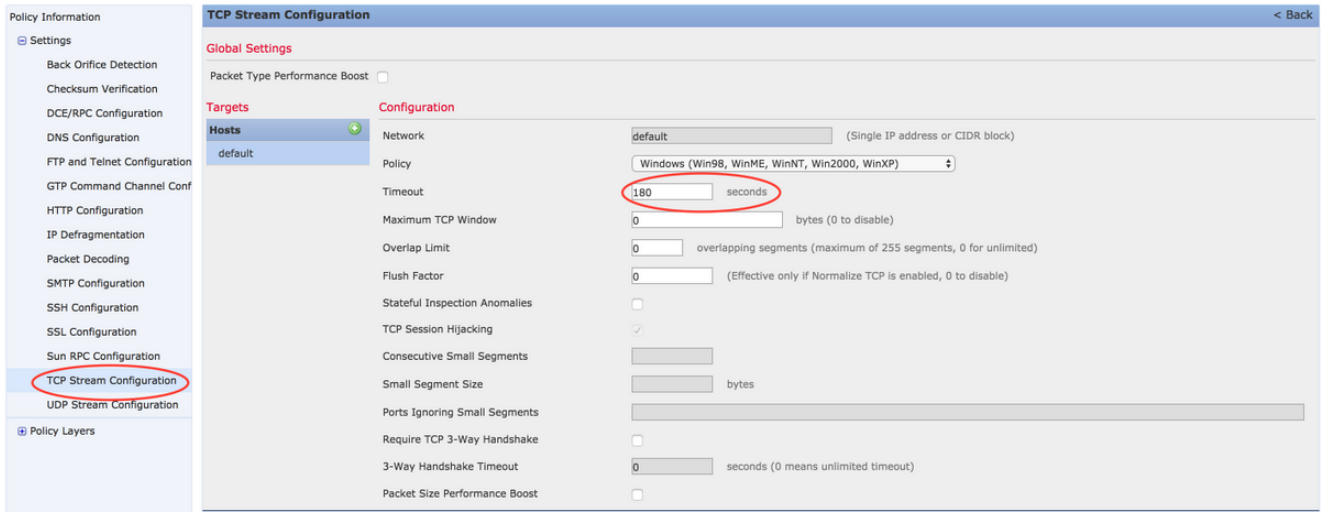
2. Navigieren Sie in der rechten oberen Ecke, und wählen Sie **Netzwerkzugriffsrichtlinie aus**.



3. Wählen Sie **Create Policy (Richtlinie erstellen)** aus, wählen Sie einen Namen aus, und klicken Sie auf **Create and Edit Policy (Richtlinie erstellen und bearbeiten)**. Ändern Sie die **Basisrichtlinie**
nicht.



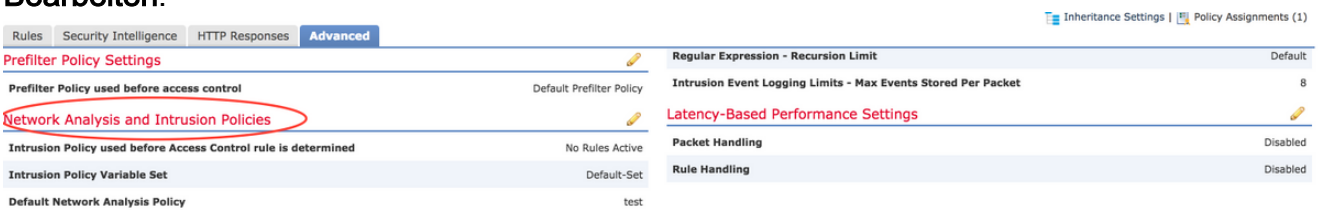
4. Erweitern Sie die Option **Einstellungen**, und wählen Sie **TCP Stream Configuration aus**.
5. Navigieren Sie zum Konfigurationsabschnitt, und ändern Sie den Wert von **Timeout** nach Bedarf.



6. Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle**.
7. Wählen Sie die Option **Bearbeiten** aus, um die auf das entsprechende verwaltete Gerät angewendete Richtlinie zu bearbeiten oder eine neue Richtlinie zu
erstellen.

8. Wählen Sie die Registerkarte **Erweitert** in der Zugriffsrichtlinie aus.
9. Suchen Sie den Abschnitt **"Netzwerkanalyse und Zugriffsrichtlinien"**, und klicken Sie auf das Symbol

Bearbeiten.



10. Wählen Sie aus dem Dropdown-Menü **Standard Network Analysis Policy** (Standardnetzwerkanalyserichtlinie) die in Schritt 2 erstellte Richtlinie aus.
11. Klicken Sie auf **OK** und **Speichern** der Änderungen.
12. Klicken Sie auf die Option **Bereitstellen**, um die Richtlinien auf relevanten verwalteten Geräten bereitzustellen.

Vorsicht: Die zunehmende Zeitüberschreitung dürfte zu einer höheren Speichernutzung führen. FirePOWER muss Datenflüsse verfolgen, die von Endpunkten über einen längeren Zeitraum nicht geschlossen werden. Die tatsächliche Steigerung der Speichernutzung ist für jedes einzelne Netzwerk unterschiedlich, da sie davon abhängt, wie lange die TCP-Verbindungen von den Netzwerkanwendungen im Leerlauf gehalten werden.

Schlussfolgerung

Die Benchmark für Leerlaufzeitüberschreitungen bei TCP-Verbindungen ist unterschiedlich. Es hängt komplett von den verwendeten Anwendungen ab. Es muss ein optimaler Wert ermittelt werden, indem überwacht wird, wie lange TCP-Verbindungen durch Netzwerkanwendungen deaktiviert bleiben. Bei Problemen, die sich auf das FirePOWER-Servicemodul bei einer Cisco ASA beziehen, kann der Timeout angepasst werden, indem dieser schrittweise bis zum Zeitüberschreitungswert der ASA erhöht wird, wenn kein optimaler Wert abgezogen werden kann.

Zugehörige Informationen

- Cisco FirePOWER Threat Defense - Kurzanleitung für die ASA
- Technischer Support und Dokumentation - Cisco Systems
- ASA FirePOWER Schnellstartanleitung