FirePOWER Management Center geeft bepaalde TCP-verbindingsgebeurtenissen in de verkeerde richting weer

Inhoud

Inleiding

Dit document beschrijft de redenen en limiteringsstappen voor FirePOWER Management Center (FMC), waarbij TCP-verbindingsgebeurtenissen in de omgekeerde richting worden weergegeven: IP van de Initiator is de IP van de TCP-verbinding en IP van de Responder is de client van de TCP-verbinding.

> Opmerking: Er zijn meerdere redenen voor het optreden van dergelijke gebeurtenissen. Deze documenten verklaren de meest voorkomende oorzaak van dit symptoom.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FirePOWER-technologie
- Basiskennis van adaptieve security applicatie (ASA)
- Understanding of Transmission Control Protocol (TCP) tijdmechanisme

Gebruikte componenten

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

- ASA Firepower Threat Defense (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) die software versie 6.0.1 en hoger heeft
- ASA Firepower Threat Defense (5512-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-

X,FP9300,FP4100) die softwareversie 6.0.1 en hoger uitvoert
- ASA met FirePOWER-modules (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 softwareversies 6.0.0 en hoger uitvoert
- Firepower Management Center (FMC) versie 6.0.0 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, begonnen met een duidelijke (standaard) configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrond

In een TCP verbinding verwijst **client** naar het IP dat het eerste pakket verstuurt. FirePOWER Management Center genereert een verbindingsgebeurtenis wanneer het beheerde apparaat (sensor of FTD) het oorspronkelijke TCP-pakket van een verbinding ziet.

Apparaten die de status van een TCP-verbinding volgen, hebben een **stille tijd** gedefinieerd om er zeker van te zijn dat verbindingen die door endpoints niet onjuist worden gesloten, het beschikbare geheugen lange tijd niet gebruiken. De standaard inactiviteitstimer voor ingestelde TCP-verbindingen op FirePOWER is **drie minuten**. Een TCP-verbinding die drie minuten of langer onklaar is gebleven, wordt niet gevolgd door de FirePOWER IPS-sensor.

Het volgende pakket na de tijdelijke versie wordt behandeld als een nieuwe TCP-stroom en de verzendingsbeslissing wordt genomen volgens de regel die met dit pakket overeenkomt. Wanneer het pakket van de server komt, wordt IP van de server opgenomen als initiator van deze nieuwe stroom. Wanneer houtkap voor de regel is ingeschakeld, wordt er een verbindingsgebeurtenis gegenereerd op het FirePOWER Management Center.

> Opmerking: Zoals per gevormd beleid, is de het verzenden beslissing voor het pakket dat na de tijd komt anders dan de beslissing voor het eerste TCP pakket. Als de ingestelde standaardoptie "Blok" is, wordt het pakje ingetrokken.

Een voorbeeld van dit symptoom is zoals in het hieronder weergegeven scherm:

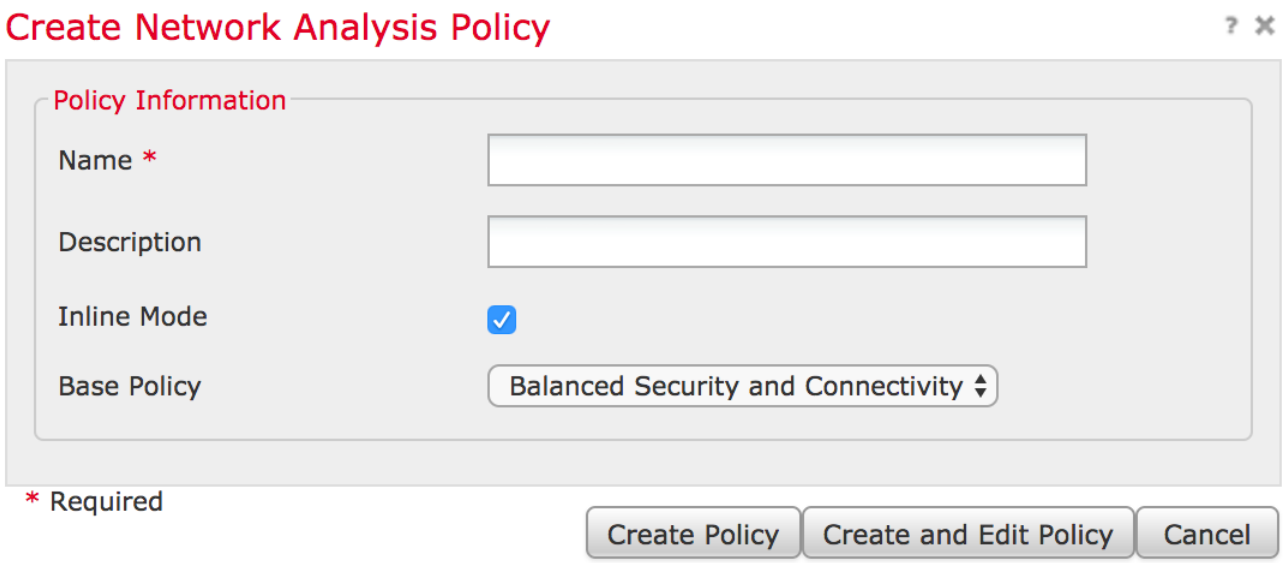
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13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

Oplossing

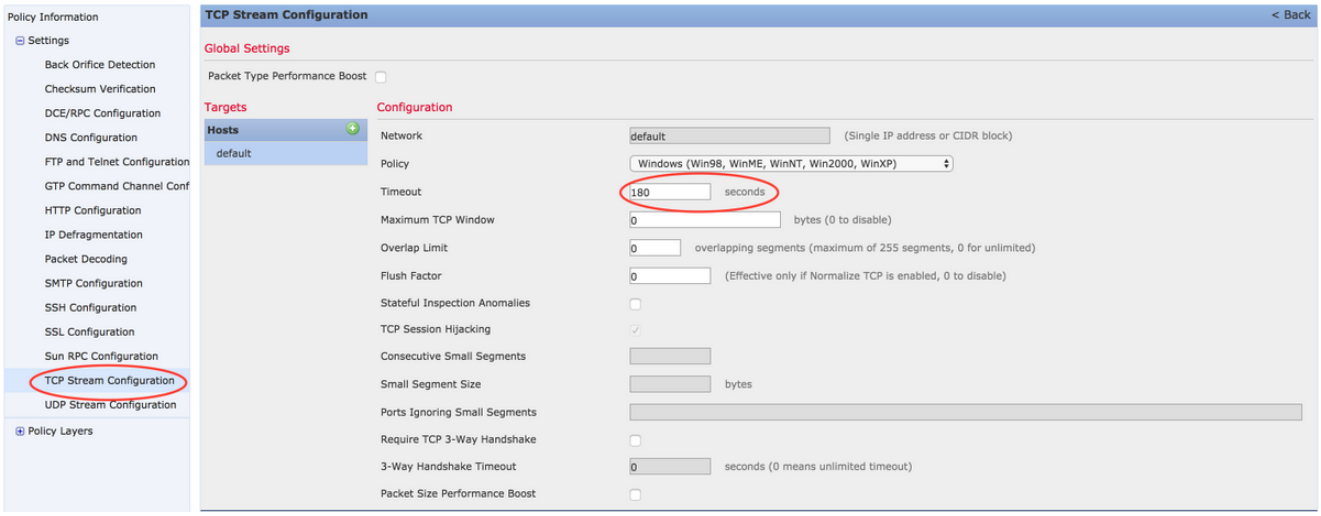
Het bovenstaande probleem wordt verzacht door de **Time-out** van TCP-verbindingen te verhogen. Zo wijzigt u de tijd:

1. Navigeren in op **beleid > Toegangsbeheer > Inbraakcontrole**.
2. Blader naar de rechterbovenhoek en selecteer **Netwerktoegangsbeleid**.

3. Selecteer **Beleid maken** , kies een naam en klik op **Beleid maken en bewerken**. Wijzig het **basisbeleid** niet.

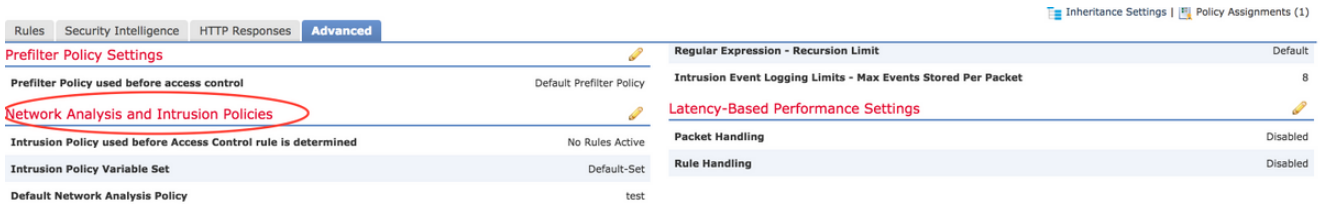


4. Vul de optie **Instellingen** uit en kies **TCP-stroomconfiguratie**.
5. Navigeer naar het configuratie gedeelte en verander de waarde van de **Time-out** naar wens.



6. Navigeren in op **beleid > Toegangsbeheer > Toegangsbeheer**.
7. Selecteer de optie **Bewerken** om het beleid te bewerken dat op een relevant beheerd apparaat is toegepast of om een nieuw beleid te maken.

8. Selecteer het tabblad **Geavanceerd** in het kader van het toegangsbeleid.
9. Selecteer **de** sectie **Netwerkanalyse en inbraakbeleid** lokaliseren en klik op het pictogram **Bewerken**.



10. Kies in het vervolgkeuzemenu van het **beleid voor netwerkanalyse** het beleid dat in stap 2 is gemaakt.
11. Klik op **OK** en **Sla** de wijzigingen op.
12. Klik op de optie **implementeren** om het beleid in te stellen op relevante beheerde apparaten.

Voorzichtig: De stijgende tijd zal naar verwachting een hoger geheugengebruik veroorzaken, moet FirePOWER stromen volgen die niet door endpoints voor een langere tijd worden gesloten. De eigenlijke toename in geheugengebruik is verschillend voor elk uniek netwerk aangezien het van de lange tijd van de netwerktoepassingen de verbindingen van TCP ongebruikt houdt afhangt.

Conclusie

De benchmark van elk netwerk voor het onklaar maken van TCP connecties is anders. Het is volledig afhankelijk van de gebruikte toepassingen. Een optimale waarde moet worden vastgesteld door te observeren hoe lang de netwerktoepassingen TCP verbindingen nutteloos houden. Voor kwesties die betrekking hebben op FirePOWER-servicemodule op een Cisco ASA, wanneer een optimale waarde niet kan worden afgetrokken, kan de tijdelijke versie worden aangepast door deze in stappen te verhogen tot de waarde van ASA.

Gerelateerde informatie

- Cisco Firepower Threat Defense Quick Start-gids voor de ASA
- Technische ondersteuning en documentatie – Cisco Systems
- ASA Firepower Quick Start-gids