^Live online verkeer met meerdere deelnemers (Teredo Tunnel UDP 3544) geblokkeerd door FTD

Inhoud

Inleiding

In dit document wordt een probleem beschreven waarmee gebruikers toegang kunnen krijgen tot de gratis-live-multiplayer-functie van de gratis-gebruiker wanneer deze verbonden is achter een FTD-sensor (FirePower Threat Defense Defense). Telkens wanneer u probeert een online-verbinding van meerdere spelers op te zetten, werkt deze niet via de FTD-sensor.

Dit probleem wordt gezien nadat u de firewallservices van een Cisco ASA (adaptieve security applicatie) naar een FirePOWER met FTD migreert.

Het belangrijkste doel van dit document is uit te leggen hoe het mogelijk is dat de "Giolive"-on-multiplayer-verkeer (Teredo-tunnel UDP 3544) door de FTD wordt gebruikt.

Bijgedragen door Christian G. Hernandez R., Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Cisco FirePower-voorfilter configuratie.

Gebruikte componenten

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

- Cisco FMC (FirePower Management Center) v6.2.3.1
- Cisco FTD v6.2.3.1

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

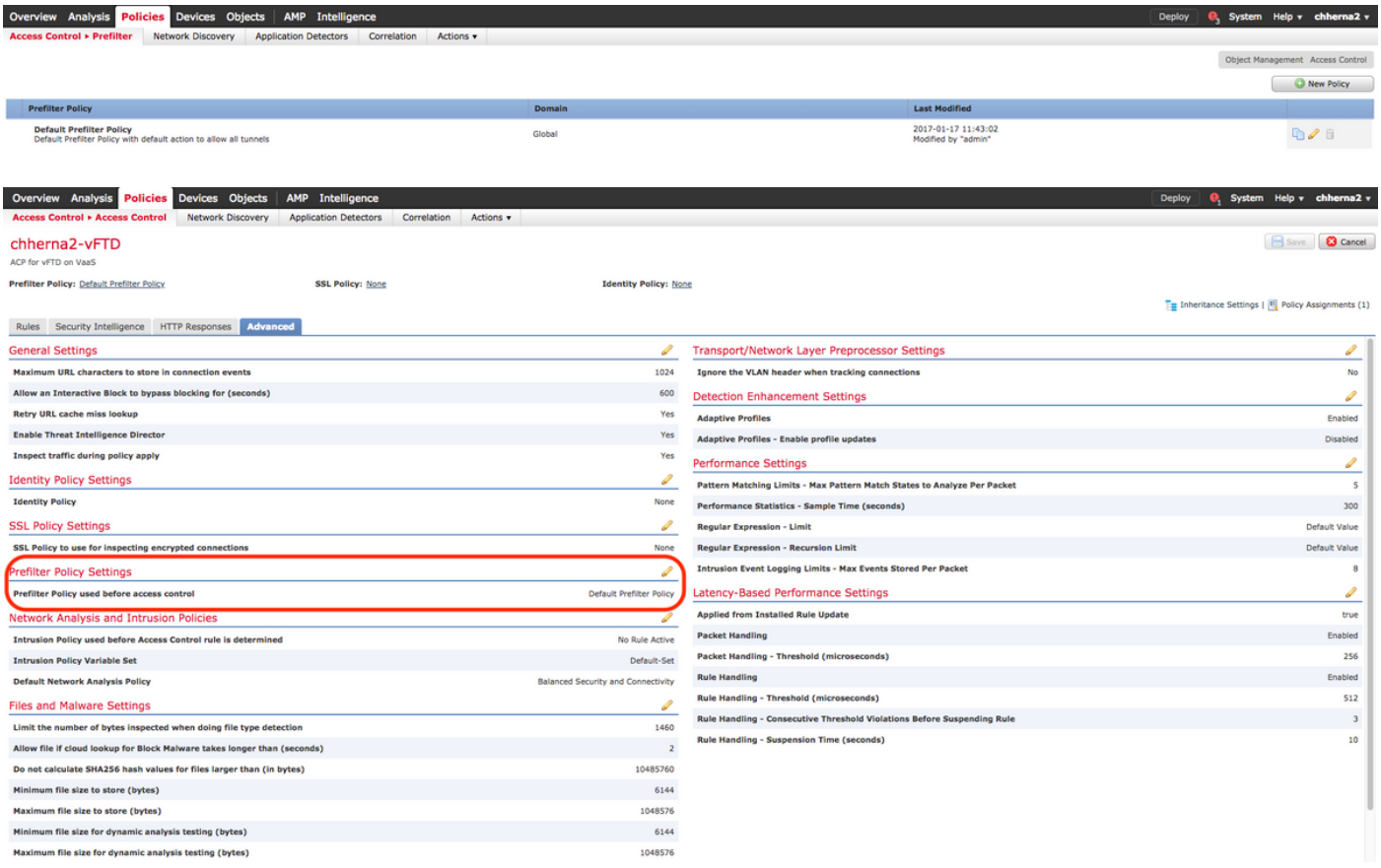
De gratis online multiplayer-optie voor de gratis-gebruiker breekt een Teredo-tunnel op die gebruikmaakt van de UDP-poort 3544, zoals bevestigd in het volgende Microsoft-document:

Netwerkpoorten die worden gebruikt door de gratis op de

Probleem: gratis online verkeer met meerdere deelnemers (Teredo Tunnel UDP 3544) geblokkeerd door FTD

Het wordt bevestigd dat de FTD-sensoren het gratis online verkeer met meerdere spelers blokkeren (Teredo-tunnel UDP 3544) als u de standaard-voorfilterregels van het FMC niet gebruikt:

Standaard voorfilterbeleid op basis van de FMC GUI (grafische gebruikersinterface):



Standaard pre-filter beleid gezien vanaf een FTD Sensor CLI (Opdracht Line Interface):

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list CSM_FW_ACL_; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and
Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
(hitcnt=0) 0x46d7839e access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535
any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
```

> Opmerking: De bovenstaande voorfilterregels van de lijnen 6 en 7 zijn de standaard voorfilterregels die bedoeld zijn om het verkeer van de Teredo-tunnel UDP 3544 door de FTD mogelijk te maken.

Maar het probleem is dat een FTD die geen gebruik maakt van de standaard-voorfilterregel, blokken of zwarte lijsten van dit live online UDP 3544-verkeer van meerdere spelers die afkomstig is van de gratis, dit wordt bevestigd met de hulp van een ASP (Accelerated Security Path)-pakketvastlegging die in de FTD wordt toegepast, net als volgt:

```
firepower# capture asp type asp-drop all
firepower# show cap asp | i x.x.x.x
50243: 16:23:03.023054 x.x.x.x.3074 > y.y.y.y.3544: udp 61 Drop-reason: (session) Blocked or
blacklisted by the session preprocessor
51622: 16:23:04.023253 x.x.x.x.3074 > y.y.y.y.3544: udp 61 Drop-reason: (session) Blocked or
blacklisted by the session preprocessor
53990: 16:23:06.023588 x.x.x.x.3074 > y.y.y.y.3544: udp 61 Drop-reason: (session) Blocked or
blacklisted by the session preprocessor
58785: 16:23:10.024367 x.x.x.x.3074 > y.y.y.y.3544: udp 61 Drop-reason: (session) Blocked or
blacklisted by the session preprocessor
69006: 16:23:18.025145 x.x.x.x.3074 > y.y.y.y.3544: udp 61
89783: 16:23:34.026716 x.x.x.x.3074 > y.y.y.y.3544: udp 61
```

> Opmerking: U kunt proberen dit verkeer door de FTD toe te staan met een ACS (Access Control Policy), ingesteld om het UDP 3544-verkeer mogelijk te maken. Daarna bevestigt u dat dezelfde ASP-druppels op de FTD CLI zullen worden gezien.

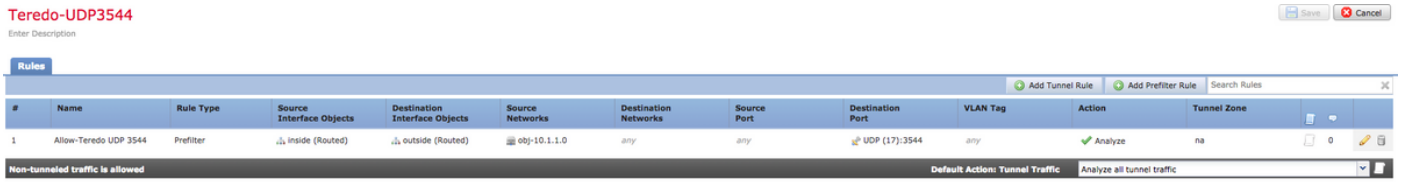
Oplossing

Om het gratis online verkeer van meerdere spelers (Teredo-tunnel UDP 3544) via de FTD mogelijk te maken, moet u een pre-filter regel configureren. U hebt dan vier opties om de vereiste voorfilterregel te configureren:

Normaal gefilterde regel configureren

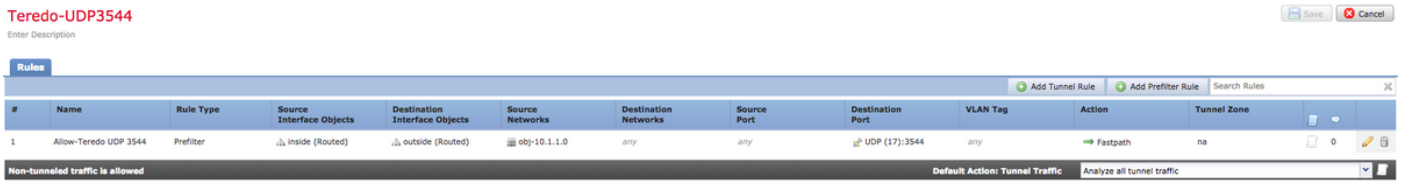
Voorbeeld 1

Configureer een normale voorfilterregel met **Analyse-**actie om het verkeer dat is bestemd voor UDP 3544 met **Any**-filter als bestemming toe te staan:



Voorbeeld 2

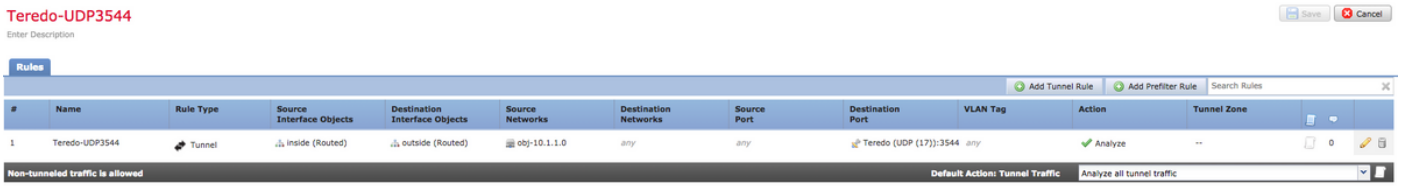
Configureer een normale voorfilterregel met **Fastpath**-actie om het verkeer dat is bestemd voor UDP 3544 met **Any** als bestemming toe te staan:



Een tunnelvoorfilterregel configureren

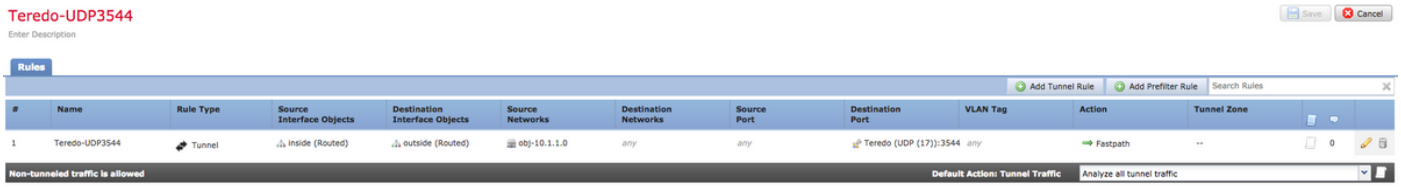
Voorbeeld 1

Configureer een regel voor tunnelvoorfilter met **Analyse** actie om het verkeer dat bestemd is voor UDP 3544 met **Any** als bestemming toe te staan:



Voorbeeld 2

Configureer een vooraf filter regel met de **Fastpath**-actie om het verkeer dat is bestemd voor UDP 3544 met **Any** als bestemming toe te staan:



> Opmerking: De vier hierboven genoemde opties zijn bevestigd werk fijn in het TAC-laboratorium om de Teredo-tunnel (UDP 3544) door de FTD te laten opzetten. De belangrijkste intentie om **Any** als bestemming IP-adres te gebruiken voor de configuratie van de voorfilterregel is het gevolg van de verschillende IP-adressen die de gratis kan gebruiken om verbinding te maken met de Microsoft online multi-player servers.

Gerelateerde informatie

- Configuratie en werking van het FTD-prefilterbeleid

- Prefilterbeleid en prefilterbeleid
- Netwerkpoorten die worden gebruikt door de gratis op de