Xbox Live線上多玩家流量（Teredo隧道UDP 3544）被FTD阻止

目錄

簡介

本文檔描述了一個問題，當通過FTD（FirePower威脅防禦）感測器進行連線時，允許使用者從Xbox訪問Xbox live線上多玩家功能。每次您嘗試從Xbox建立線上多玩家連線時，它都無法通過FTD感測器工作。

將防火牆服務從Cisco ASA（調適型安全裝置）遷移到FirePower with FTD後會顯示此問題。

本文的主要目的是解釋如何允許Xbox live線上多玩家流量（Teredo隧道UDP 3544）通過FTD。

作者：Christian G. Hernandez R.，思科TAC工程師。

必要條件

需求

思科建議您瞭解Cisco FirePower預過濾器規則配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco FMC（FirePower管理中心）v6.2.3.1
- Cisco FTD v6.2.3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

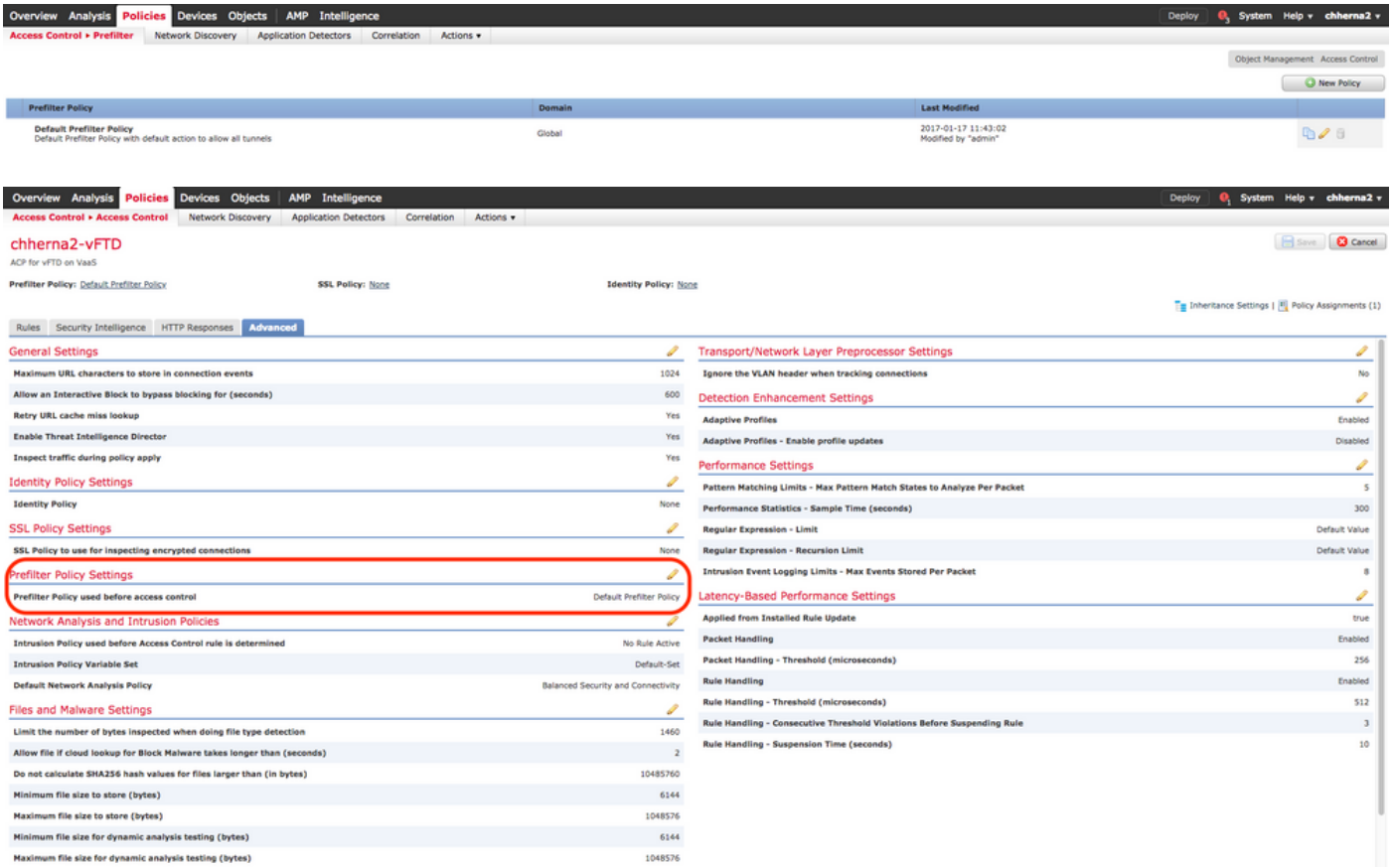
Xbox的Xbox live線上多玩家功能建立了一個Teredo隧道，該隧道使用UDP埠3544，與下一個Microsoft Xbox文檔中確認的一樣：

Xbox Live在Xbox One上使用的網路埠

問題：Xbox Live線上多玩家流量（Teredo隧道UDP 3544）被FTD阻止

如果您未使用FMC的出廠預設預過濾器規則，FTD感測器會阻止Xbox live線上多玩家流量(Teredo tunnel UDP 3544):

從FMC GUI（圖形使用者介面）中看到的預設預過濾器策略：



從FTD感應器CLI（指令行介面）中看到的預設預過濾器原則：

```
> 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
```

附註：來自第6行和第7行的上述預過濾器規則是預設預過濾器規則，用於允許Teredo隧道UDP 3544流量通過FTD。

但是，問題是FTD不使用出廠預設預過濾規則，阻止或黑名單來自Xbox的此Xbox live線上多人UDP 3544流量，這在FTD中應用的ASP（加速安全路徑）資料包捕獲的幫助下得到確認，如下所示：

```
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
```

附註：您可以嘗試允許此流量通過FTD，且將ACP（存取控制原則）設定為允許UDP 3544流量，在此之後，您會確認在FTD CLI上會顯示相同的ASP捨棄專案。

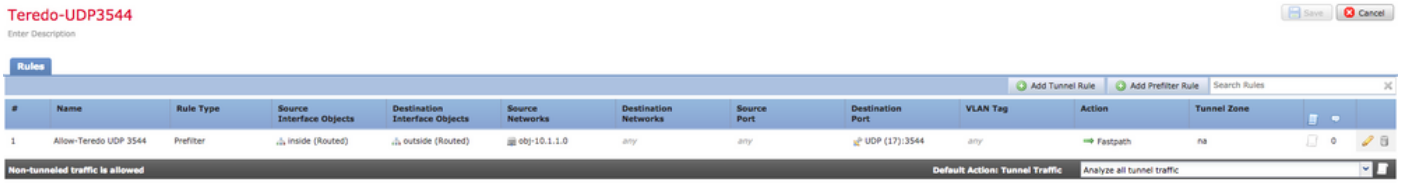
解決方案

要允許Xbox live線上多人流量（Teredo隧道UDP 3544）通過FTD，您需要配置預過濾器規則，為此，您有4個選項來配置所需的預過濾器規則：

配置普通預過濾器規則

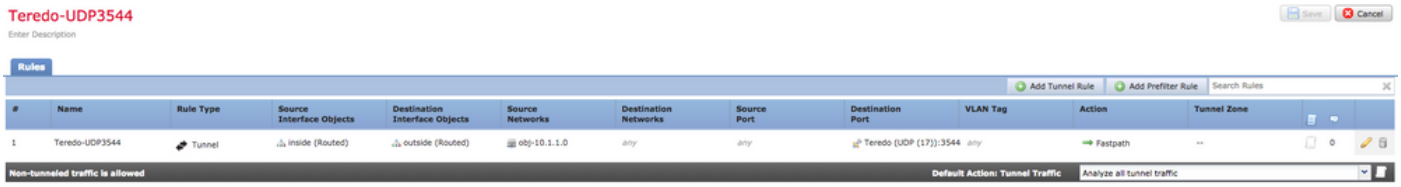
範例 1

使用**Analyze**操作配置普通預過濾器規則，以允許以**Any**作為目的地發往UDP 3544的流量：



範例 2

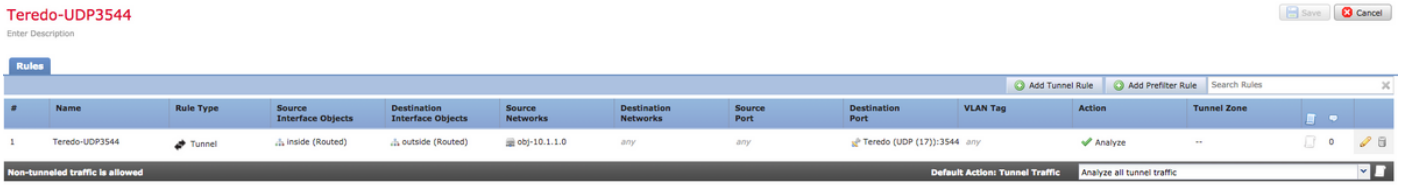
使用**Fastpath**操作配置普通預過濾器規則，以允許以**Any**作為目的地發往UDP 3544的流量：



配置隧道預過濾器規則

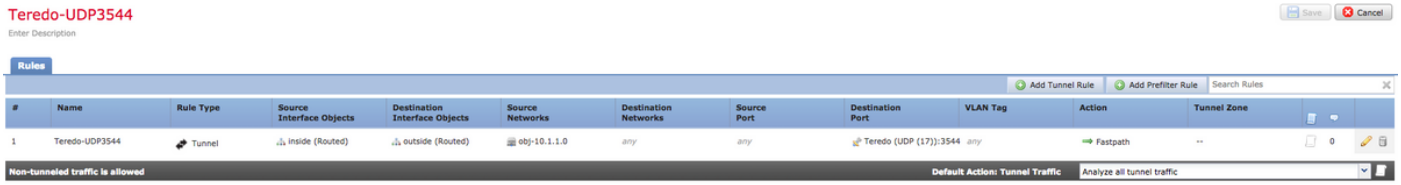
範例 1

使用**Analyze**操作配置隧道預過濾器規則，以允許以**Any**作為目的地發往UDP 3544的流量：



範例 2

使用Fastpath操作配置隧道預**過濾**規則，以允許以**Any**作為目的地發往UDP 3544的流量：



> **附註**：上述4個選項在TAC實驗中確認工作正常，可以允許Teredo通道(UDP 3544)通過FTD建立。使用**Any**作為預過濾器規則配置的目標IP地址的主要意圖是因為Xbox可以使用不同的IP地址連線到Microsoft線上多玩家伺服器。

相關資訊

- [FTD預過濾器策略的設定和操作]
- [預過濾和預過濾策略]
- [Xbox Live在Xbox One上使用的網路埠]