Xbox Liveオンラインマルチプレーヤートラフィック（TeredoトンネルUDP 3544）がFTDでブロックされました

内容

概要

このドキュメントでは、FTD (FirePower Threat Defense)センサーの背後で接続した場合に、XboxからXbox liveオンラインマルチプレーヤー機能にアクセスできる問題について説明します。Xboxからオンラインマルチプレーヤー接続を確立しようとするたびにFTDセンサーをを使用できません。

この問題は、ファイアウォールサービスをCisco ASA（適応型セキュリティアプライアンス）からFTDを使用するFirePowerに移行した後に発生します。

このドキュメントの主な目的は、Xbox liveオンラインマルチプレーヤートラフィック(Teredo tunnel UDP 3544)をFTD経由で動作させる方法を説明することです。

著者：Cisco TACエンジニア、Christian G. Hernandez R.

前提条件

要件

Cisco FirePowerのフィルタ前ルール設定に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

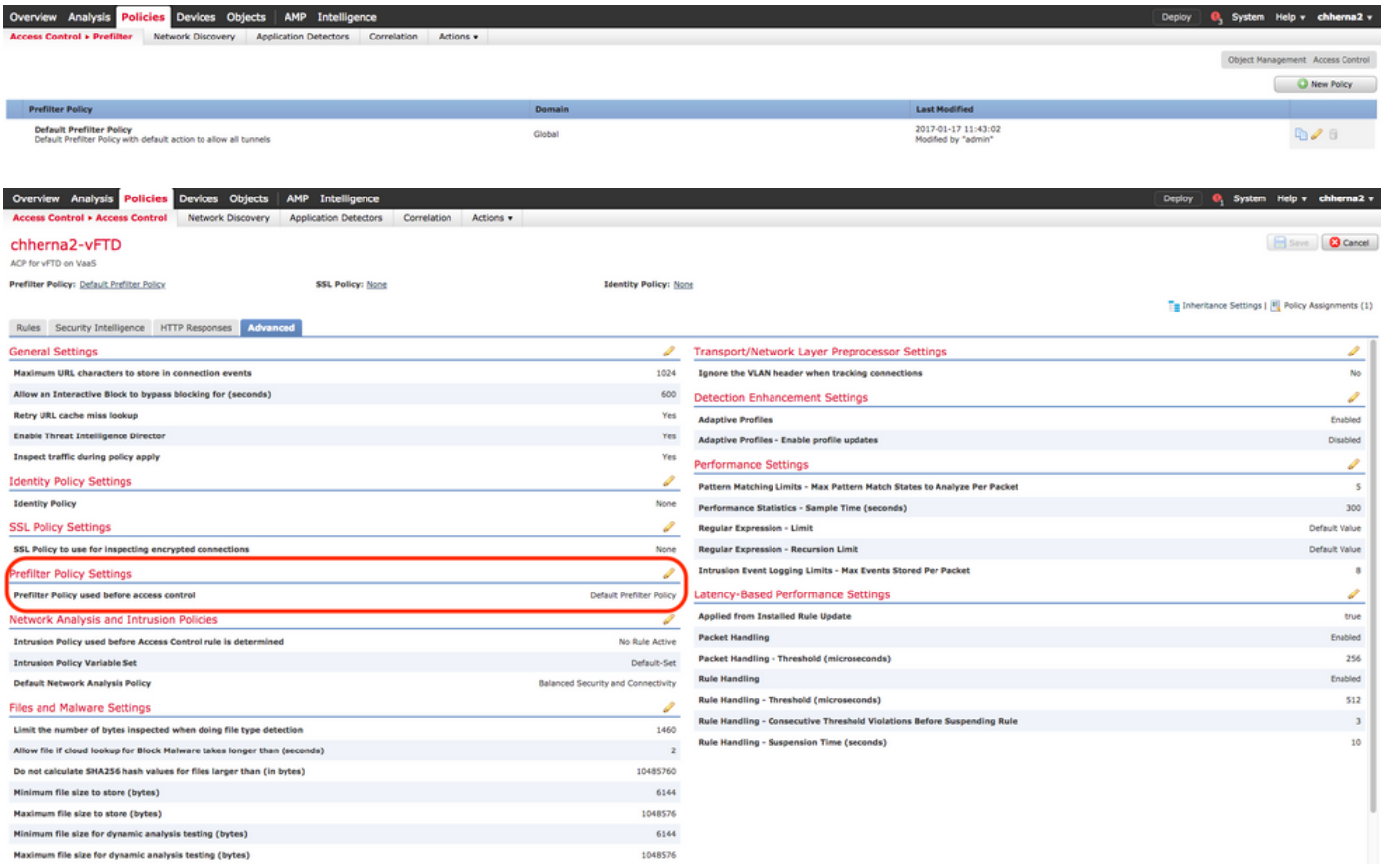
XboxのXbox liveオンラインマルチプレーヤー機能は、次のMicrosoft Xboxドキュメントで確認したように、UDPポート3544を使用するTeredoトンネルを確立します。

[Xbox OneでXbox Liveで使用されるネットワークポート]

問題： Xbox Liveオンラインマルチプレーヤートラフィック（TeredoトンネルUDP 3544）がFTDでブロックされました

FMCから工場出荷時のデフォルトのプレフィルタルールを使用しない場合、FTDセンサーがXbox liveオンラインマルチプレーヤートラフィック(Teredo tunnel UDP 3544)をブロックすることが確認されています。

FMC GUI（グラフィックユーザインターフェイス）から表示されるデフォルトのプレフィルタポリシー：



FTDセンサーのCLI（コマンドラインインターフェイス）から表示されるデフォルトのプレフィルタポリシー：

```
> 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
```

注：上記の6行目と7行目のプレフィルタルールは、TeredoトンネルUDP 3544トラフィックがFTDを通過することを許可するデフォルトのプレフィルタルールです。

しかし、問題は、工場出荷時のデフォルトのプレフィルタ規則を使用しないFTDは、Xboxから着信するXbox liveオンラインマルチプレーヤーUDP 3544トラフィックをブロックまたはブラックリストに載せていないことです。

```
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
```

注：UDP 3544トラフィックを許可するように設定されたACP(Access Control Policy)を使用して、このトラフィックをFTD経由で許可してみてください。その後、FTD CLIで同じASPドロップが表示されることを確認します。

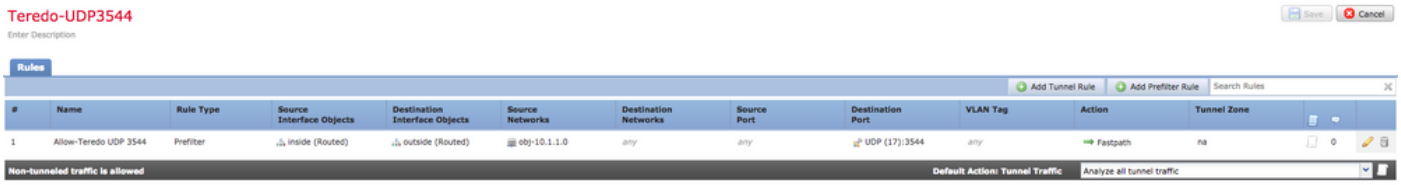
解決方法

FTDを介してXbox liveオンラインマルチプレーヤートラフィック(Teredo tunnel UDP 3544)を許可するには、プレフィルタルールを設定する必要があります。これには、次の4つのオプションが必要です。

通常のプレフィルタルールの設定

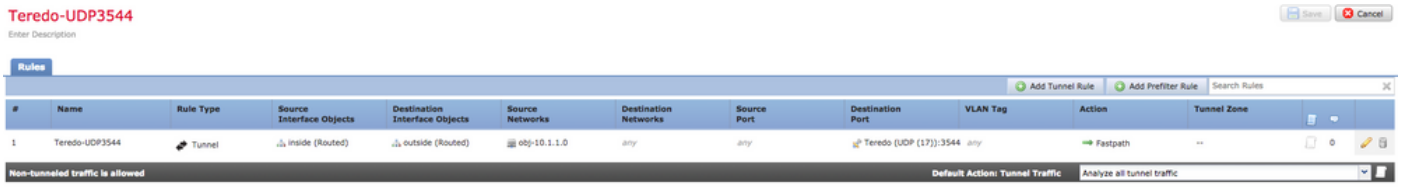
例 1

Analyzeアクションを使用して、宛先が**Any**のUDP 3544宛てのトラフィックを許可するように、通常のプレフィルタ規則を設定します。



例 2

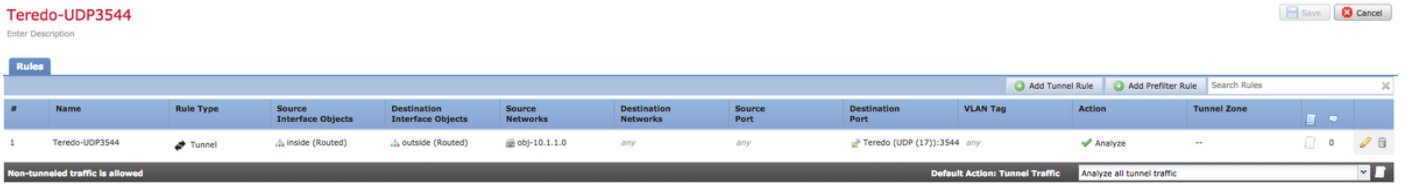
Fastpathアクションを使用して通常のプレフィルタルールを設定し、宛先が**Any**の**UDP 3544**宛てのトラフィックを許可します。



トンネルプレフィルタルールの設定

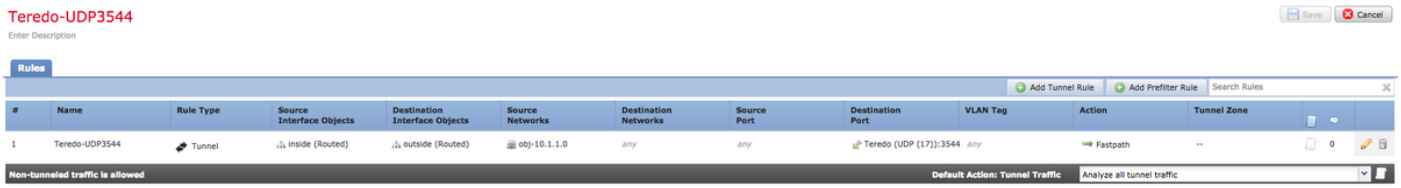
例 1

Analyzeアクションを使用して、宛先が**Any**のUDP 3544宛てのトラフィックを許可するように、トンネルのプレフィルタルールを設定します。



例 2

Fastpathアクションを使用してトンネルのプレフィルタルールを設定し、宛先が**Any**の**UDP 3544**宛てのトラフィックを許可します。



> **注**：上記の4つのオプションは、TACラボで問題なく動作することが確認されており、Teredoトンネル(UDP 3544)をFTD経由で確立できます。プレフィルタ規則の設定に**Any**を宛先IPアドレスとして使用する主な目的は、XboxがMicrosoftオンラインマルチプレイヤーサーバーに接続するために使用できるIPアドレスが異なることです。

関連情報

- [FTDプレフィルタポリシーの設定と操作]

- プレフィルタリングおよびプレフィルタポリシー
- Xbox OneでXbox Liveで使用されるネットワークポート