Xbox Live在线多用户流量（Teredo隧道UDP 3544）被FTD阻止

目录

简介

本文档介绍当用户在FTD（FirePower威胁防御）传感器后面连接时，允许用户从Xbox访问Xbox live在线多玩家功能。每次您尝试从Xbox建立在线多玩家连接时，它都无法通过FTD传感器工作。

将防火墙服务从Cisco ASA（自适应安全设备）迁移到带FTD的FirePower后，会出现此问题。

本文档的主要目的是说明如何允许Xbox live在线多用户流量（Teredo隧道UDP 3544）通过FTD工作。

作者：Cisco TAC工程师Christian G. Hernandez R.。

先决条件

要求

思科建议您了解Cisco FirePower预过滤器规则配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

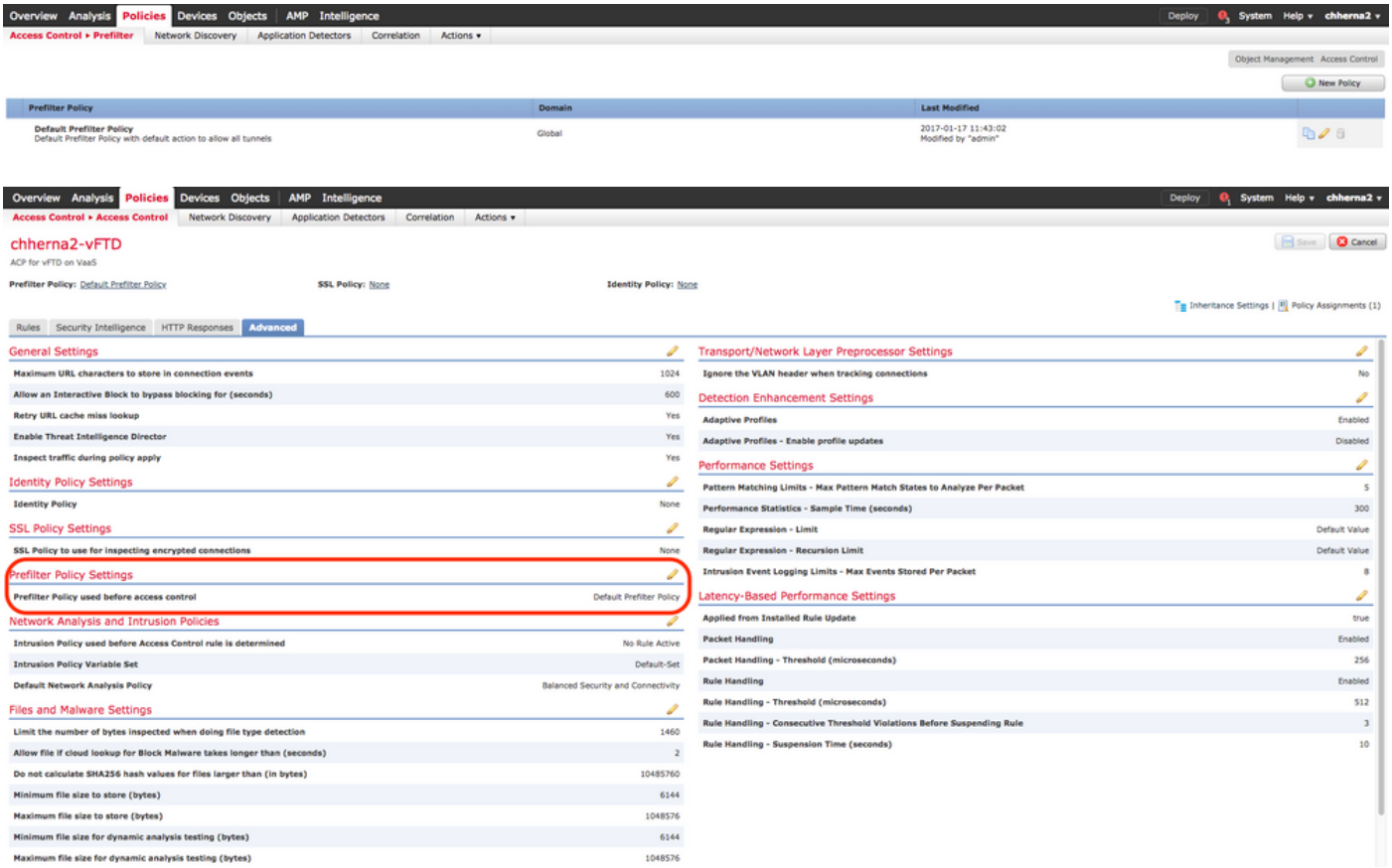
Xbox live在线多玩家功能为Xbox建立了一个使用UDP端口3544的Teredo隧道，正如在下一个Microsoft Xbox文档中确认的那样：

Xbox Live在Xbox One上使用的网络端口

问题：Xbox Live在线多用户流量（Teredo隧道UDP 3544）被FTD阻止

如果您不使用FMC的出厂默认预过滤规则，FTD传感器会阻止Xbox live在线多用户流量（Teredo隧道UDP 3544）：

从FMC GUI（图形用户界面）中看到的默认预过滤策略：



从FTD传感器CLI（命令行界面）中看到的默认预过滤策略：

```
> 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
```

注意：上述第6行和第7行的预过滤规则是默认的预过滤规则，旨在允许Teredo隧道UDP 3544流量通过FTD。

但是，问题是，如果FTD不使用出厂默认预过滤规则、阻止或黑名单此Xbox Live在线多用户UDP 3544流量来自Xbox，请借助FTD中应用的ASP（加速安全路径）数据包捕获来确认，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
```

注意：您可以尝试通过FTD允许此流量，其中ACP（访问控制策略）配置为允许UDP 3544流量，在此之后，您将确认在FTD CLI上看到相同的ASP丢弃。

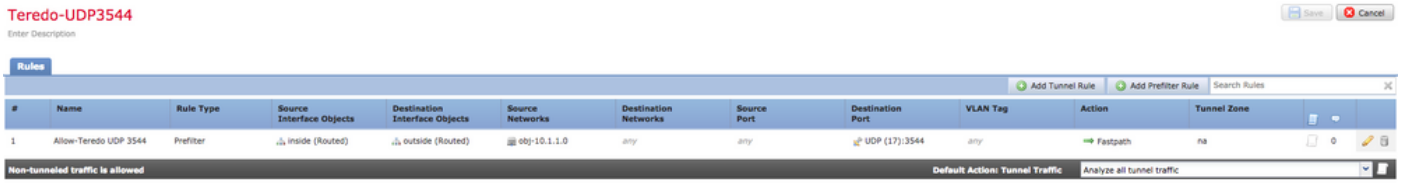
解决方案

要允许Xbox Live在线多用户流量（Teredo隧道UDP 3544）通过FTD，您需要配置预过滤规则，为此，您有4个选项来配置所需的预过滤规则：

配置普通预过滤器规则

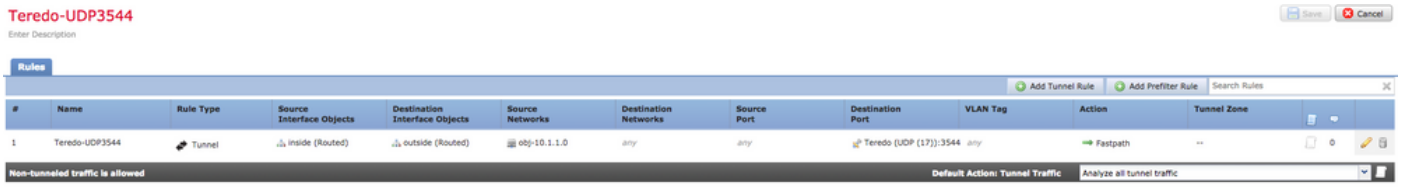
示例 1

使用Analyze操作配置普通的预过滤器规则，以允许以Any作为目的地址发往UDP 3544的流量：



示例 2

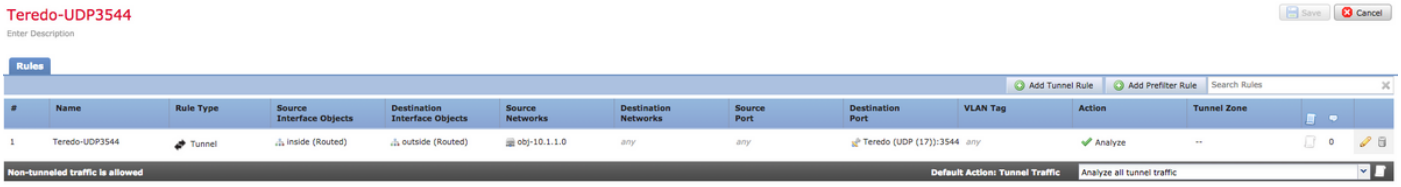
使用Fastpath操作配置普通预过滤器规则，以允许以Any作为目的地发往UDP 3544的流量：



配置隧道预过滤器规则

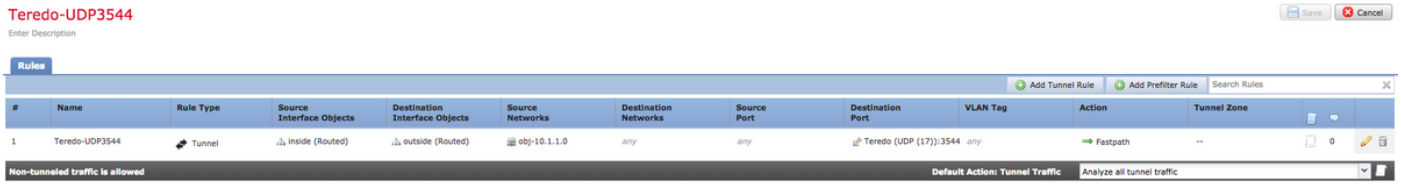
示例 1

使用**Analyze**操作配置隧道预过滤器规则，以允许以Any作为目标发往UDP 3544的**流量**:



示例 2

使用Fastpath操作配置隧道预过滤器规则，以允许以Any作为目标的发往UDP 3544的**流量**:



> **注意**：上述4个选项在TAC实验室中已确认工作正常，可通过FTD建立Teredo隧道(UDP 3544)。将**Any**用作预过滤规则配置的目标IP地址的主要意图是由于Xbox可用于连接到Microsoft在线多用户服务器的不同IP地址。

相关信息

- [FTD预过滤器策略的配置和操作]
- [预过滤和预过滤策略]
- [Xbox Live在Xbox One上使用的网络端口]