Trafic multi-joueurs Xbox Live (tunnel Teredo UDP 3544) bloqué par FTD

Contenu

Introduction

Ce document décrit un problème constaté pour permettre aux utilisateurs d'accéder à la fonctionnalité multijoueur en ligne Xbox Live depuis la Xbox lorsqu'ils sont connectés par le biais d'un capteur FTD (FirePower Threat Defense). Chaque fois que vous essayez d'établir une connexion multi-joueurs en ligne à partir de la Xbox, cela ne fonctionne pas avec le capteur FTD.

Ce problème est observé après la migration des services de pare-feu d'un appareil de sécurité adaptatif Cisco ASA vers un appareil FirePower avec FTD.

L'objectif principal de ce document est d'expliquer comment permettre au trafic multi-joueurs en ligne Xbox Live (tunnel Teredo UDP 3544) de fonctionner via le FTD.

Contribué par Christian G. Hernandez R., ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître la configuration des règles de préfiltre Cisco FirePower.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

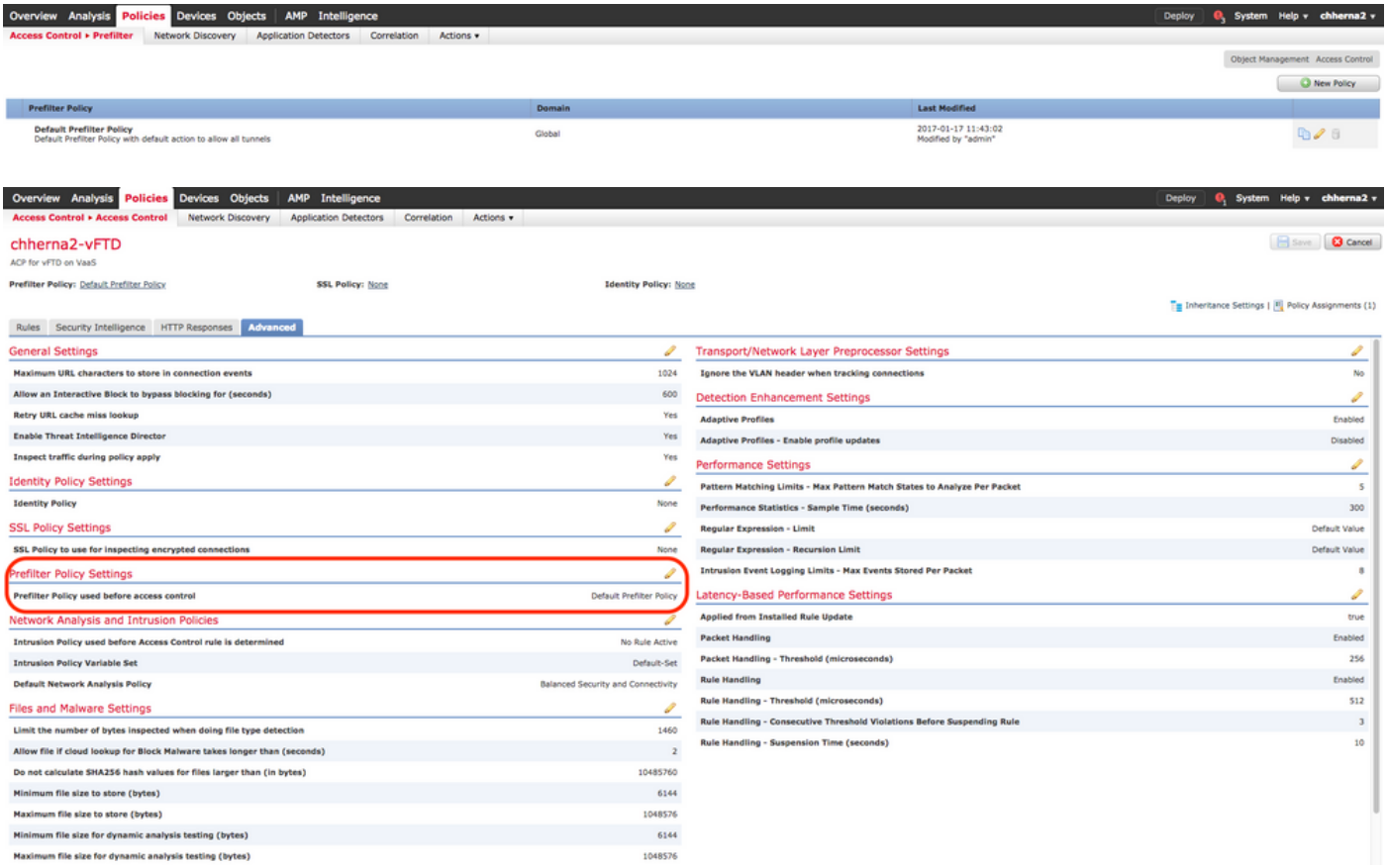
La fonctionnalité multijoueur en ligne Xbox Live pour la Xbox établit un tunnel Teredo qui utilise le port UDP 3544, comme confirmé dans le document Microsoft Xbox suivant :

Ports réseau utilisés par Xbox Live sur Xbox One

Problème : Trafic multi-joueurs Xbox Live (tunnel Teredo UDP 3544) bloqué par FTD

Il est confirmé que les capteurs FTD bloquent le trafic multijoueur en ligne Xbox Live (tunnel Teredo UDP 3544) si vous n'utilisez pas les règles de préfiltre par défaut du FMC :

Stratégie de pré-filtre par défaut vue à partir de l'interface utilisateur graphique FMC :



Stratégie de pré-filtre par défaut vue à partir d'une CLI de capteur FTD (interface de ligne de commande) :

```
> 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
```

> **Note**: Les règles de préfiltre ci-dessus des lignes 6 et 7 sont les règles de préfiltre par défaut destinées à autoriser le trafic UDP 3544 du tunnel Teredo à travers le FTD.

Mais, le problème est qu'un FTD qui n'utilise pas la règle de pré-filtre par défaut, bloque ou met en liste noire ce trafic UDP 3544 multi-joueurs en ligne Xbox Live qui provient de la Xbox, ceci est confirmé à l'aide d'une capture de paquets ASP (Accelerated Security Path) appliquée dans le FTD, comme suit :

```
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
```

> **Note**: Vous pouvez essayer d'autoriser ce trafic à travers le FTD avec un ACP (Access Control Policy) configuré pour autoriser le trafic UDP 3544, après cela, vous confirmerez que les mêmes pertes ASP seront vues sur l'interface de ligne de commande FTD.

Solution

Pour autoriser le trafic multijoueur en ligne Xbox Live (tunnel Teredo UDP 3544) via le FTD, vous devez configurer une règle de pré-filtre, pour cela, vous avez 4 options pour configurer la règle de pré-filtre requise :

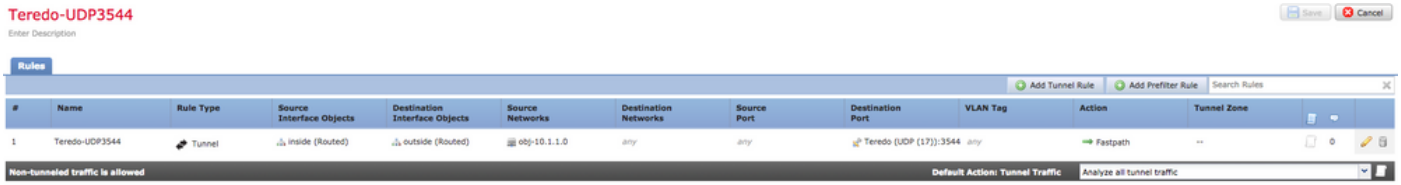
Configurer une règle de pré-filtre normale

Exemple 1

Configurez une règle de préfiltre normale avec l'action **Analyser** pour autoriser le trafic destiné à UDP 3544 avec **Any** comme destination :

Exemple 2

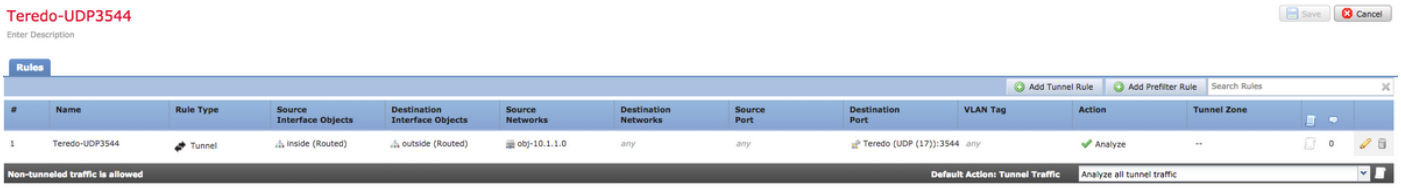
Configurez une règle de préfiltre normale avec l'action **Fastpath** pour autoriser le trafic destiné à UDP 3544 avec **Any** comme destination :



Configurer une règle de préfiltre de tunnel

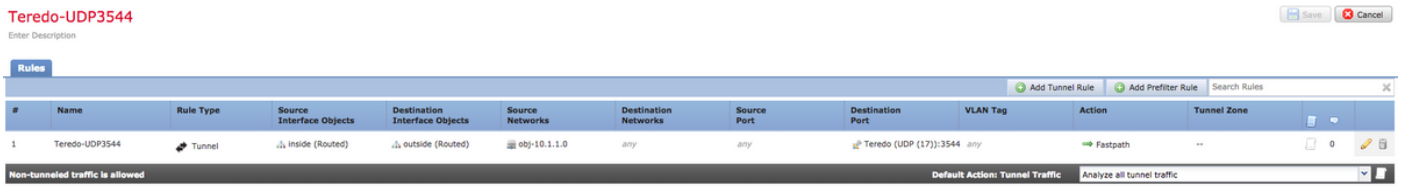
Exemple 1

Configurez une règle de préfiltre de tunnel avec l'action **Analyser** pour autoriser le trafic destiné à UDP 3544 avec **Any** comme destination :



Exemple 2

Configurez une règle de préfiltre de tunnel avec l'action **Fastpath** pour autoriser le trafic destiné à UDP 3544 avec **Any** comme destination :



> **Note**: Les 4 options mentionnées ci-dessus sont des travaux confirmés au laboratoire du TAC pour permettre l'établissement du tunnel Teredo (UDP 3544) par le biais du FTD. L'intention principale d'utiliser **Any** comme adresse IP de destination pour la configuration de la règle de pré-filtre est due aux différentes adresses IP que le Xbox peut utiliser pour se connecter aux serveurs Microsoft en ligne multi-joueurs.

Informations connexes

- Configuration et fonctionnement des stratégies de préfiltre FTD
- Politiques de préfiltrage et de préfiltrage
- Ports réseau utilisés par Xbox Live sur Xbox One