

Tráfego Multi-Player Online Xbox Live (Teredo Tunnel UDP 3544) Bloqueado por FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema: Tráfego Multi-Player Online Xbox Live \(Teredo Tunnel UDP 3544\) Bloqueado por FTD](#)

[Solução](#)

[Configurar uma regra de pré-filtro normal](#)

[Exemplo 1](#)

[Exemplo 2](#)

[Configurar uma regra de pré-filtro de túnel](#)

[Exemplo 1](#)

[Exemplo 2](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve um problema visto para permitir que os usuários acessem o recurso de vários jogadores online do Xbox ao vivo do Xbox quando conectados por trás de um sensor FTD (FirePower Threat Defense). Sempre que tenta estabelecer uma ligação multijogador online a partir da Xbox, não funciona através do sensor FTD.

Esse problema ocorre após a migração dos serviços de firewall de um Cisco ASA (Adaptive Security Appliance) para um FirePower com FTD.

O principal objetivo deste documento é explicar como permitir que o tráfego Xbox de vários jogadores online (Teredo tunnel UDP 3544) funcione através do FTD.

Contribuído por Christian G. Hernandez R., Engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você conheça a configuração das regras de pré-filtro do Cisco FirePower.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O recurso multiplayer online Xbox estabelece um túnel Teredo que usa a porta UDP 3544, como confirmado no próximo documento do Microsoft Xbox:

[Portas de rede usadas pelo Xbox Live no Xbox One](#)

Problema: Tráfego Multi-Player Online Xbox Live (Teredo Tunnel UDP 3544) Bloqueado por FTD

Confirmado, os sensores FTD bloqueiam o tráfego de multijogadores online Xbox (Teredo tunnel UDP 3544) se você não usar as regras de pré-filtro padrão de fábrica do FMC:

Política de pré-filtro padrão vista na GUI do FMC (Graphic User Interface):

The screenshot displays the Cisco FMC GUI for the 'chherna2-vFTD' device. The 'Policies' tab is active, showing the 'Default Prefilter Policy' for the 'Global' domain. The 'Prefilter Policy Settings' section is highlighted with a red circle, indicating the 'Default Prefilter Policy' is selected for 'Prefilter Policy used before access control'. Other sections include 'General Settings', 'Identity Policy Settings', 'SSL Policy Settings', 'Network Analysis and Intrusion Policies', and 'Files and Malware Settings'.

Política de pré-filtro padrão vista de um sensor FTD CLI (Command 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 4l 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: As regras de pré-filtro acima das linhas 6 e 7 são as regras de pré-filtro padrão destinadas a permitir o tráfego UDP 3544 do túnel Teredo através do FTD.

Mas o problema é que um FTD que não usa a regra de pré-filtro padrão de fábrica, bloqueia ou bloqueia o tráfego UDP 3544 on-line do Xbox que vem do Xbox, isso é confirmado com a ajuda de uma captura de pacote ASP (Accelerated Security Path) aplicada no FTD, da seguinte forma:

```

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: Você pode tentar permitir esse tráfego através do FTD com um ACP (Access Control Policy) configurado para permitir o tráfego UDP 3544; depois disso, você confirmará que as mesmas quedas de ASP serão vistas na CLI do FTD.

Solução

Para permitir o tráfego de vários jogadores online (Teredo tunnel UDP 3544) do Xbox através do FTD, você precisa configurar uma regra de pré-filtro; para isso, você tem 4 opções para configurar a regra de pré-filtro necessária:

Configurar uma regra de pré-filtro normal

Exemplo 1

Configure uma regra de pré-filtro normal com a ação **Analisar** para permitir o tráfego destinado ao UDP 3544 com **Qualquer** como destino:

Teredo-UDP3544 Save Cancel

Enter Description

Rules Add Tunnel Rule Add Prefilter Rule Search Rules

| # | Name | Rule Type | Source Interface Objects | Destination Interface Objects | Source Networks | Destination Networks | Source Port | Destination Port | VLAN Tag | Action | Tunnel Zone |
|---|-----------------------|-----------|--------------------------|-------------------------------|-----------------|----------------------|-------------|------------------|----------|----------|-------------|
| 1 | Allow-Teredo UDP 3544 | Prefilter | inside (Routed) | outside (Routed) | obj-10.1.1.0 | any | any | UDP (17):3544 | any | Fastpath | na |

Non-tunneled traffic is allowed Default Action: Tunnel Traffic Analyze all tunnel traffic

Exemplo 2

Configure uma regra de pré-filtro normal com a ação **Fastpath** para permitir o tráfego destinado ao UDP 3544 com **Any** como destino:



Teredo-UDP3544
Enter Description

| # | Name | Rule Type | Source Interface Objects | Destination Interface Objects | Source Networks | Destination Networks | Source Port | Destination Port | VLAN Tag | Action | Tunnel Zone |
|---|----------------|-----------|--------------------------|-------------------------------|-----------------|----------------------|-------------|------------------------|----------|----------|-------------|
| 1 | Teredo-UDP3544 | Tunnel | inside (Routed) | outside (Routed) | obj-10.1.1.0 | any | any | Teredo (UDP (17)):3544 | any | Fastpath | -- |

Non-tunneled traffic is allowed
Default Action: Tunnel Traffic
Analyze all tunnel traffic

Configurar uma regra de pré-filtro de túnel

Exemplo 1

Configure uma regra de pré-filtro de túnel com a ação **Analisar** para permitir o tráfego destinado ao UDP 3544 com **Qualquer** como destino:



Teredo-UDP3544
Enter Description

| # | Name | Rule Type | Source Interface Objects | Destination Interface Objects | Source Networks | Destination Networks | Source Port | Destination Port | VLAN Tag | Action | Tunnel Zone |
|---|----------------|-----------|--------------------------|-------------------------------|-----------------|----------------------|-------------|------------------------|----------|---------|-------------|
| 1 | Teredo-UDP3544 | Tunnel | inside (Routed) | outside (Routed) | obj-10.1.1.0 | any | any | Teredo (UDP (17)):3544 | any | Analyze | -- |

Non-tunneled traffic is allowed
Default Action: Tunnel Traffic
Analyze all tunnel traffic

Exemplo 2

Configure uma regra de pré-filtro de túnel com ação **Fastpath** para permitir o tráfego destinado ao UDP 3544 com **Any** como destino:



Teredo-UDP3544
Enter Description

| # | Name | Rule Type | Source Interface Objects | Destination Interface Objects | Source Networks | Destination Networks | Source Port | Destination Port | VLAN Tag | Action | Tunnel Zone |
|---|----------------|-----------|--------------------------|-------------------------------|-----------------|----------------------|-------------|------------------------|----------|----------|-------------|
| 1 | Teredo-UDP3544 | Tunnel | inside (Routed) | outside (Routed) | obj-10.1.1.0 | any | any | Teredo (UDP (17)):3544 | any | Fastpath | -- |

Non-tunneled traffic is allowed
Default Action: Tunnel Traffic
Analyze all tunnel traffic

Note: As 4 opções mencionadas acima estão comprovadamente funcionando bem no laboratório do TAC para permitir que o túnel Teredo (UDP 3544) seja estabelecido através do FTD. A principal intenção de usar **Any** como endereço IP de destino para a configuração de regra de pré-filtro é devido aos diferentes endereços IP que o Xbox pode usar para se conectar aos servidores de vários jogadores online da Microsoft.

Informações Relacionadas

- [Configuração e operação das políticas de pré-filtro do FTD](#)
- [Políticas de pré-filtragem e pré-filtro](#)
- [Portas de rede usadas pelo Xbox Live no Xbox One](#)