Permitir Traceroute através do Firepower Threat Defense (FTD)

Contents

Introduction

Este documento descreve a configuração para permitir o traceroute por meio do Firepower Threat Defense (FTD) por meio da Política do Threat Service.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

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

- Este artigo se aplica a todas as plataformas Firepower.
- Cisco Firepower Threat Defense, que executa a versão 6.4.0 do software.
- Cisco Firepower Management Center Virtual que executa a versão 6.4.0 do software.

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

Traceroute para ajudá-lo a determinar a rota que os pacotes seguem até o seu destino. Um traceroute funciona enviando pacotes UDP (Unified Data Platform) para um destino em uma porta inválida. Como a porta não é válida, os roteadores ao longo do caminho até o destino respondem com uma mensagem de tempo excedido do protocolo ICMP (Internet Control Message Protocol) e relatam esse erro ao ASA (Adaptive Security Appliance).

O traceroute mostra o resultado de cada teste enviado. Cada linha de saída corresponde a um valor Time to Live (TTL) em ordem crescente. Esta tabela explica os símbolos de saída.

Símbolo de Saída	**Descrição**
*	Nenhuma resposta foi recebida para o teste dentro do período de tempo limite.
nn msec	Para cada nó, o tempo de ida e volta (em milissegundos) para o número especificado de testes.
!N	A rede ICMP está inacessível.
!H	O host ICMP está inacessível.
!P	ICMP inalcançável.
!A	ICMP administrativamente proibido.
?	Erro de ICMP desconhecido.

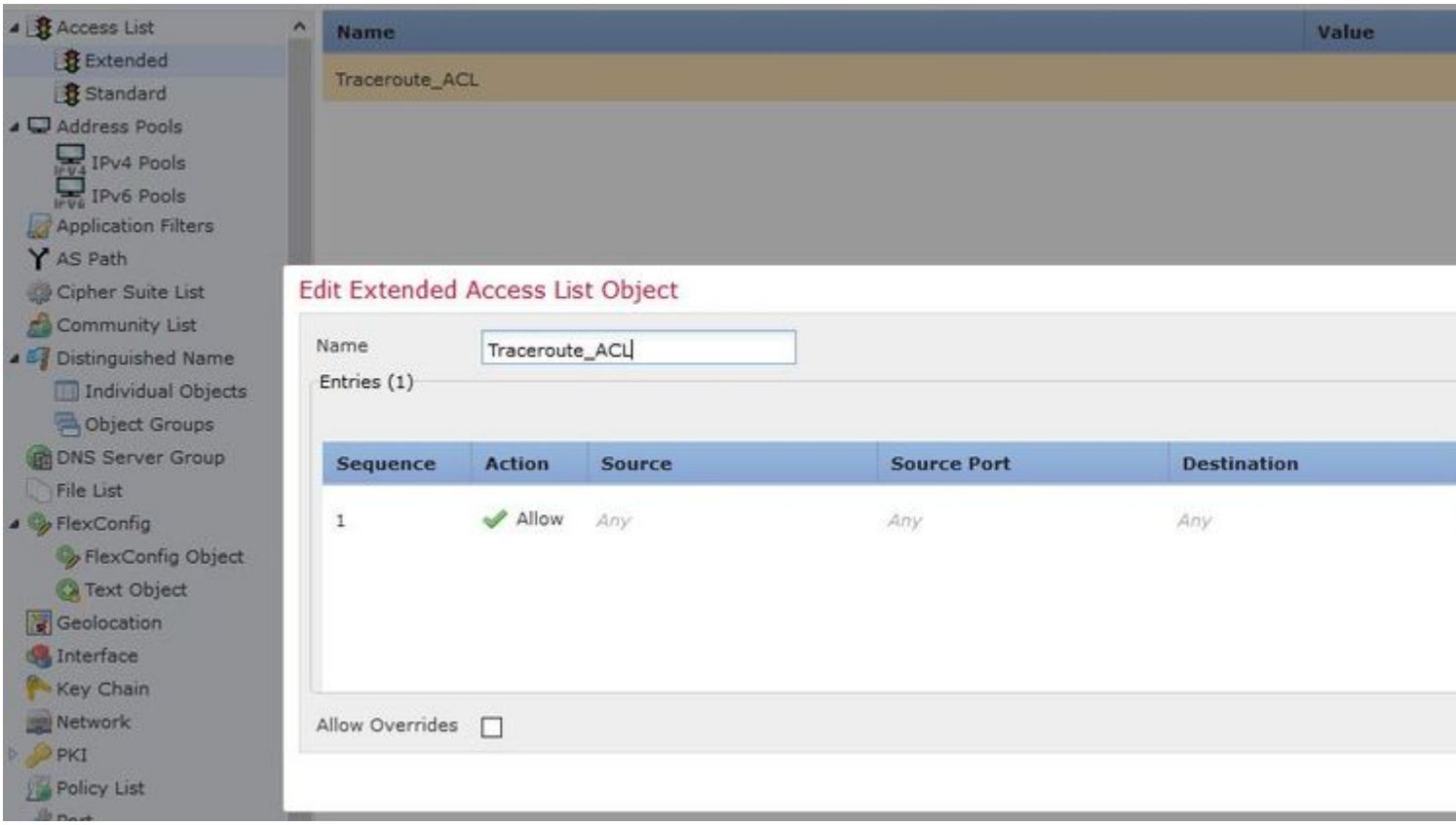
Por padrão, o ASA não aparece em traceroutes como um salto. Para que ele apareça, você precisa diminuir o tempo de vida dos pacotes que passam pelo ASA e aumentar o limite de taxa em mensagens ICMP inalcançáveis.

> **Cuidado**: se você diminuir o tempo de vida, os pacotes com um TTL de 1 serão descartados, mas uma conexão será aberta para a sessão na suposição de que a conexão pode conter pacotes com um TTL maior. Observe que alguns pacotes, como os pacotes hello do OSPF, são enviados com TTL = 1, portanto a redução do tempo de vida pode ter consequências inesperadas. Lembre-se dessas considerações ao definir sua classe de tráfego.

Configurar

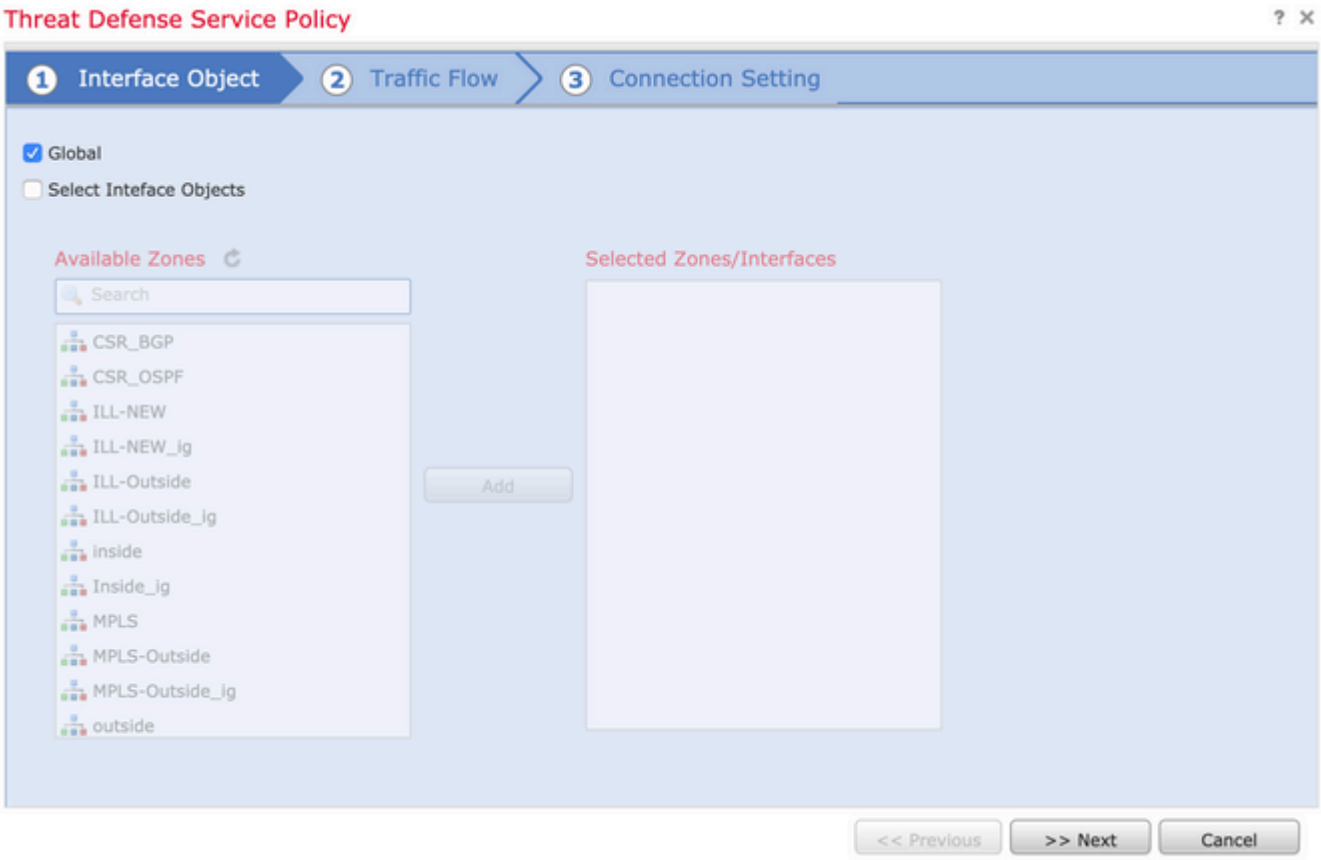
Etapa 1. Crie a ACL estendida que define a classe de tráfego para a qual o relatório de traceroute precisa ser habilitado.

Faça login na **GUI do FMC** e navegue para **Objects > Object Management >** Access List**.** Selecione **Estendido** no sumário e **Adicionar** uma nova Lista de Acesso Estendida.Insira um Nome para o objeto, por exemplo, Em Traceroute_ACL,**Adicionar** uma regra para permitir o tipo ICMP 3 e 11 e **salvá**-lo, como mostrado na imagem:

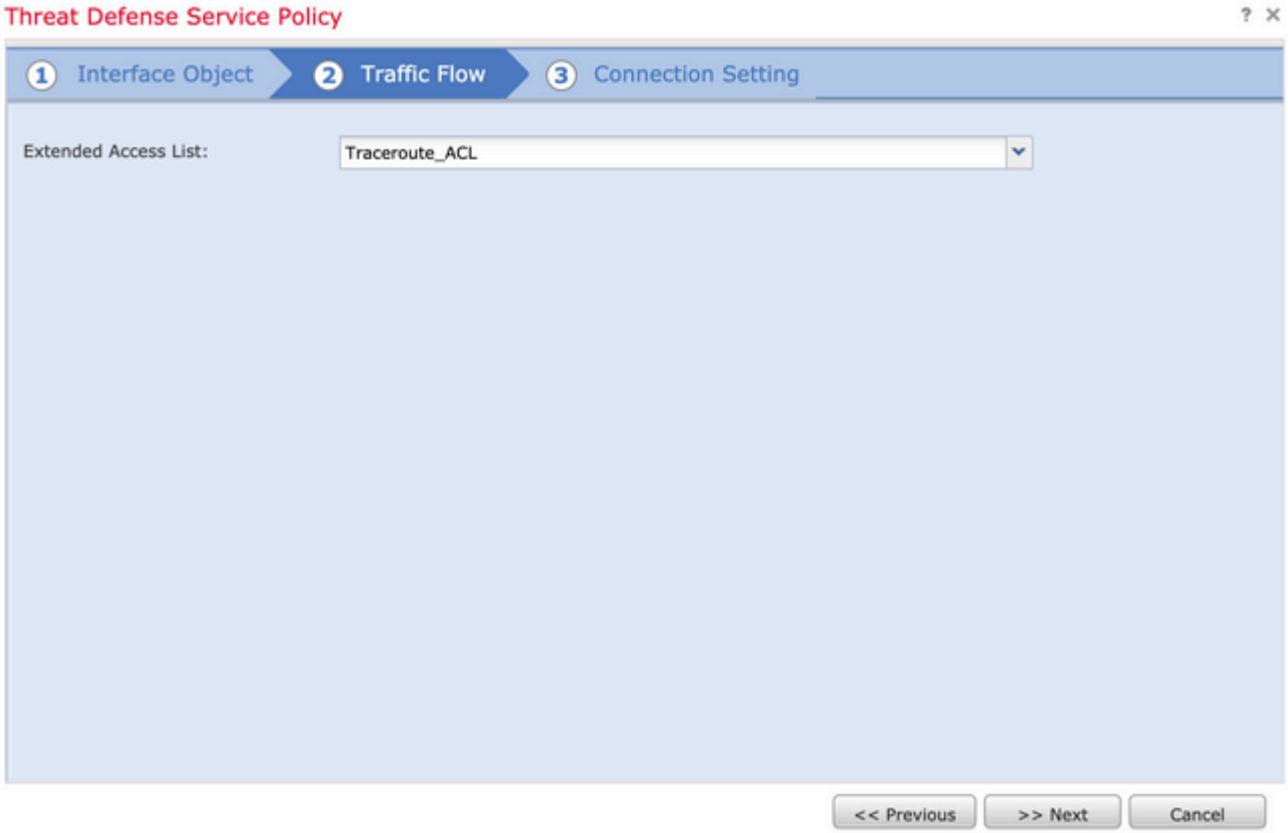


Etapa 2. Configure a regra de política de serviço que reduz o valor do tempo de vida.

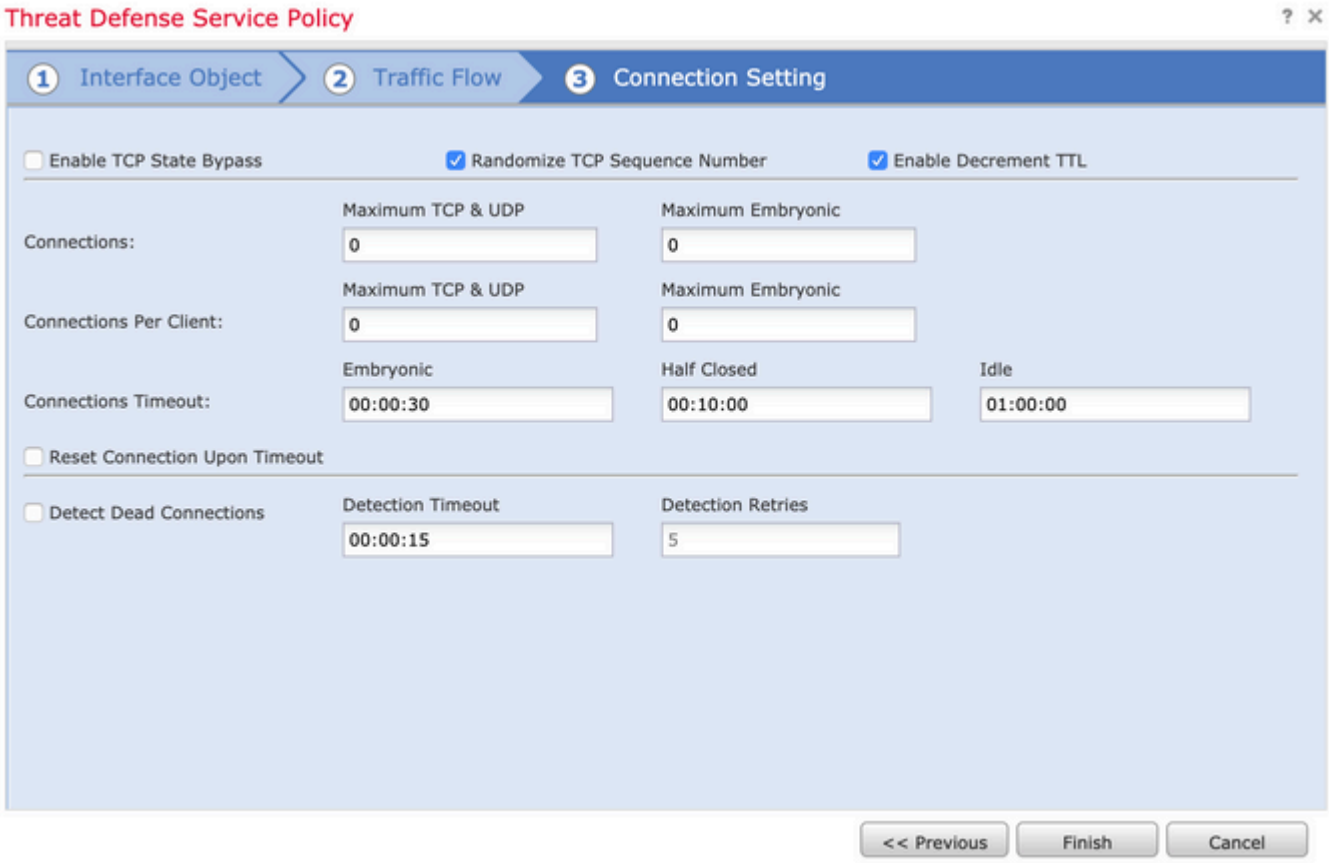
Navegue até **Policies** > **Access Control** e depois **Edit** a política atribuída ao dispositivo. Na guia Avançado, edite a política do Threat Defense Service e, em seguida, adicione uma nova regra da guia **Adicionar regra** e marque a caixa de seleção **Global** para aplicá-la globalmente e clique em **Avançar**, **conforme mostrado na imagem:**



Navegue até **Traffic Flow** > Extended Access List e escolha **Extended Access List Object** no menu suspenso que foi criado nas etapas anteriores. Agora clique em **Avançar** conforme mostrado na imagem:



Marque a caixa de seleção **Habilitar diminuição de TTL** e modifique as outras opções de conexão (Opcional). Agora, clique em **Concluir** para adicionar a regra e, em seguida, clique em **OK**, **e** Salvar **as alterações na política do serviço de defesa contra ameaças, conforme mostrado na imagem:**

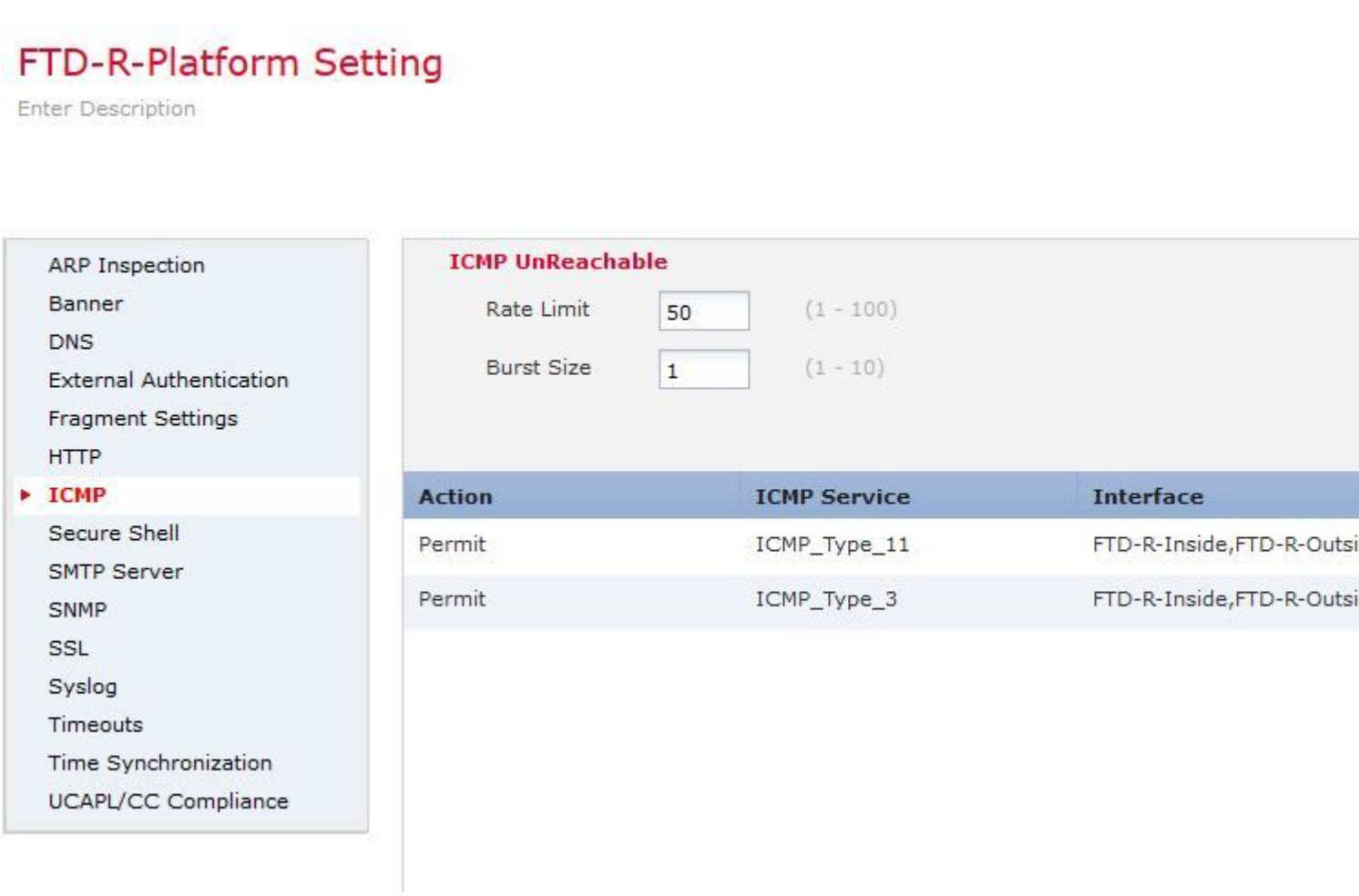


Após concluir as etapas anteriores, **salve** a Política de controle de acesso.

Etapa 3. Permita o ICMP dentro e fora e crie o limite de taxa para 50 (opcional).

Navegue até **Devices > Platform Settings** e **Edit** ou **Create** uma nova política de configurações de plataforma do Firepower Threat Defense e associe-a ao dispositivo. Escolha **ICMP** no índice e Aumente o limite de taxa. Por exemplo, para 50 (Você pode ignorar o Tamanho de Intermitência), clique em **Salvar** e continue em **Implantar** a Diretiva no dispositivo, como mostrado na imagem:

- **Limite de Taxa** â€" Define o limite de taxa de mensagens inalcançáveis, entre 1 e 100 mensagens por segundo. O padrão é 1 mensagem por segundo.
- **Tamanho da intermitência** â€" Define a taxa de intermitência, entre 1 e 10. Este valor não está sendo usado pelo sistema no momento.



Cuidado: verifique se o **destino ICMP inalcançável (Tipo 3) e o tempo ICMP excedido (Tipo 11)** são permitidos de fora para dentro na política de ACL ou caminho rápido na política de pré-filtro.

Verificar

Verifique a configuração da CLI do FTD quando a implantação da política estiver concluída:

```
FTD# show run policy-map
!
policy-map type inspect dns preset_dns_map
---Output omitted---

class class_map_Traceroute_ACL
set connection timeout idle 1:00:00
set connection decrement-ttl
class class-default
!

FTD# show run class-map
!
class-map inspection_default

---Output omitted---

class-map class_map_Traceroute_ACL
match access-list Traceroute_ACL
```

```
!

FTD# show run access-l Traceroute_ACL
access-list Traceroute_ACL extended permit object-group ProxySG_ExtendedACL_30064773500 any any log
FTD#
```

Troubleshoot

Você pode fazer capturas nas interfaces de entrada e saída FTD para que o tráfego interessante solucione o problema ainda mais.

A captura de pacotes em Lina, enquanto traceroute é executado, pode ser mostrada desta forma para cada esperança na rota até alcançar o IP de destino.

```
ftd64# capture icmp interface inside real-time match icmp any any

Warning: using this option with a slow console connection may
         result in an excessive amount of non-displayed packets
         due to performance limitations.

Use ctrl-c to terminate real-time capture


   1: 00:22:04.192800       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   2: 00:22:04.194432       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   3: 00:22:04.194447       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   4: 00:22:04.194981       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   5: 00:22:04.194997       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   6: 00:22:04.201130       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   7: 00:22:04.201146       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   8: 00:22:04.201161       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   9: 00:22:04.201375       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  10: 00:22:04.201420       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  11: 00:22:04.202336       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
  12: 00:22:04.202519       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  13: 00:22:04.216022       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  14: 00:22:04.216038       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  15: 00:22:04.216038       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  16: 00:22:04.216053       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  17: 00:22:04.216297       172.18.127.245 > 10.10.10.11 icmp: 172.18.127.245 udp port 33452 unreachable
  18: 00:22:04.216312       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  19: 00:22:04.216327       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
```

Uma saída mais detalhada pode ser obtida no Lina CLI se você executar traceroute com switches "-I" e "-n" conforme listado.

```
[ On the Client PC ]

# traceroute 10.18.127.245 -I -n

Note: You may not observe any difference between traceroute with or without -I switch. The difference is
```

[On FTD Lina CLI]

```
ftd64# capture icmp interface inside real-time match icmp any any

Warning: using this option with a slow console connection may
         result in an excessive amount of non-displayed packets
         due to performance limitations.

Use ctrl-c to terminate real-time capture


   1: 18:37:33.517307       10.10.10.11 > 172.18.127.245 icmp: echo request
   2: 18:37:33.517642       10.10.10.11 > 172.18.127.245 icmp: echo request
   3: 18:37:33.517658       10.10.10.11 > 172.18.127.245 icmp: echo request
   4: 18:37:33.517658       10.10.10.11 > 172.18.127.245 icmp: echo request
   5: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
   6: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
   7: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
   8: 18:37:33.517749       10.10.10.11 > 172.18.127.245 icmp: echo request
   9: 18:37:33.517749       10.10.10.11 > 172.18.127.245 icmp: echo request
  10: 18:37:33.517764       10.10.10.11 > 172.18.127.245 icmp: echo request
  11: 18:37:33.517764       10.10.10.11 > 172.18.127.245 icmp: echo request
  12: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
  13: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
  14: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
  15: 18:37:33.517932       10.10.10.11 > 172.18.127.245 icmp: echo request
  16: 18:37:33.517932       10.10.10.11 > 172.18.127.245 icmp: echo request
  17: 18:37:33.522464       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
  18: 18:37:33.522510       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
  19: 18:37:33.522510       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
  20: 18:37:33.522632       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
  21: 18:37:33.522647       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
  22: 18:37:33.522647       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
  23: 18:37:33.523852       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  24: 18:37:33.523929       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  25: 18:37:33.523944       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  26: 18:37:33.524066       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  27: 18:37:33.524127       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  28: 18:37:33.524127       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  29: 18:37:33.524142       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  30: 18:37:33.526767       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
  31: 18:37:33.526843       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
  32: 18:37:33.526843       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
  33: 18:37:33.527652       10.10.10.11 > 172.18.127.245 icmp: echo request
  34: 18:37:33.527697       10.10.10.11 > 172.18.127.245 icmp: echo request
  35: 18:37:33.527713       10.10.10.11 > 172.18.127.245 icmp: echo request
  36: 18:37:33.527728       10.10.10.11 > 172.18.127.245 icmp: echo request
  37: 18:37:33.527987       10.10.10.11 > 172.18.127.245 icmp: echo request
  38: 18:37:33.528033       10.10.10.11 > 172.18.127.245 icmp: echo request
  39: 18:37:33.528048       10.10.10.11 > 172.18.127.245 icmp: echo request
  40: 18:37:33.528048       10.10.10.11 > 172.18.127.245 icmp: echo request
  41: 18:37:33.528064       10.10.10.11 > 172.18.127.245 icmp: echo request
  42: 18:37:33.528064       10.10.10.11 > 172.18.127.245 icmp: echo request
  43: 18:37:33.528079       10.10.10.11 > 172.18.127.245 icmp: echo request
  44: 18:37:33.528094       10.10.10.11 > 172.18.127.245 icmp: echo request
  45: 18:37:33.528094       10.10.10.11 > 172.18.127.245 icmp: echo request
  46: 18:37:33.532870       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  47: 18:37:33.532885       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  48: 18:37:33.533679       172.18.127.245 > 10.10.10.11 icmp: echo reply
  49: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
  50: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
```

```
  51: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
  52: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
  53: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
  54: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
  55: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
  56: 18:37:33.533740       10.10.10.11 > 172.18.127.245 icmp: echo request
  57: 18:37:33.533816       10.10.10.11 > 172.18.127.245 icmp: echo request
  58: 18:37:33.533831       10.10.10.11 > 172.18.127.245 icmp: echo request
  59: 18:37:33.537066       172.18.127.245 > 10.10.10.11 icmp: echo reply
  60: 18:37:33.537081       172.18.127.245 > 10.10.10.11 icmp: echo reply
  61: 18:37:33.537081       172.18.127.245 > 10.10.10.11 icmp: echo reply
  62: 18:37:33.538500       172.18.127.245 > 10.10.10.11 icmp: echo reply
  63: 18:37:33.538500       172.18.127.245 > 10.10.10.11 icmp: echo reply
  64: 18:37:33.539217       172.18.127.245 > 10.10.10.11 icmp: echo reply
64 packets shown.
0 packets not shown due to performance limitations.
```

Dica: ID do bug da Cisco CSCvq79913. Pacotes de erro ICMP são descartados para Null pdts_info. Certifique-se de usar o pré-filtro para ICMP, preferencialmente para o tráfego de retorno tipo 3 e 11.

Informações Relacionadas

Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.