Permitir Traceroute mediante Firepower Threat Defence (FTD)

Contenido

Introducción

Este documento describe la configuración para permitir el traceroute a través de Firepower Threat Defence (FTD) mediante la política de servicio de amenazas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Este artículo es aplicable a todas las plataformas Firepower.
- Cisco Firepower Threat Defence, que ejecuta la versión de software 6.4.0.
- Cisco Firepower Management Center Virtual, que ejecuta la versión de software 6.4.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Traceroute para ayudarle a determinar la ruta que toman los paquetes hacia su destino. Un traceroute funciona enviando paquetes de Unified Data Platform (UDP) a un destino en un puerto no válido. Debido a que el puerto no es válido, los routers en el camino hacia el destino responden con un mensaje de tiempo excedido del protocolo de mensajes de control de Internet (ICMP) e informan de ese error al dispositivo de seguridad adaptable (ASA).

El traceroute muestra el resultado de cada sondeo enviado. Cada línea de salida corresponde a un valor de Tiempo de vida (TTL) en orden creciente. Esta tabla explica los símbolos de salida.

Símbolo de salida	**Descripción**
*	No se recibió ninguna respuesta para la sonda dentro del período de tiempo de espera.
nn msec	Para cada nodo, el tiempo de ida y vuelta (en milisegundos) para el número especificado de sondeos.
!N	La red ICMP es inalcanzable.
!H	El host ICMP es inalcanzable.
!P	ICMP es inalcanzable.
!A	ICMP está prohibido administrativamente.
?	Error ICMP desconocido.

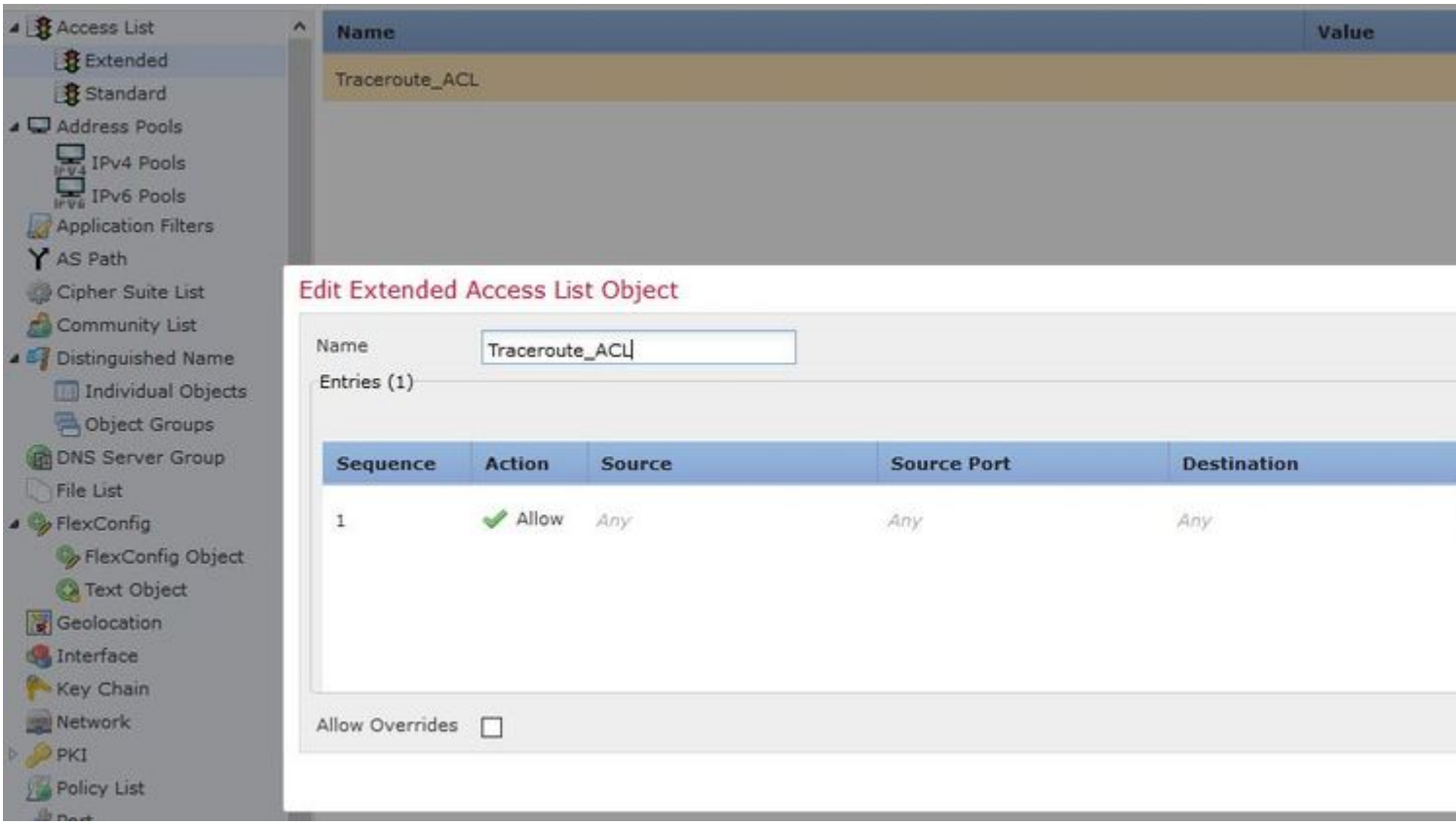
De forma predeterminada, ASA no aparece en los traceroutes como un salto. Para que aparezca, debe disminuir el tiempo de vida de los paquetes que pasan a través del ASA y aumentar el límite de velocidad en los mensajes ICMP inalcanzables.

> **Precaución**: si reduce el tiempo de vida, los paquetes con un TTL de 1 se descartan, pero se abre una conexión para la sesión en el supuesto de que la conexión puede contener paquetes con un TTL mayor. Tenga en cuenta que algunos paquetes, como los paquetes de saludo OSPF, se envían con TTL = 1, por lo que reducir el tiempo de vida puede tener consecuencias inesperadas. Tenga en cuenta estas consideraciones cuando defina su clase de tráfico.

Configurar

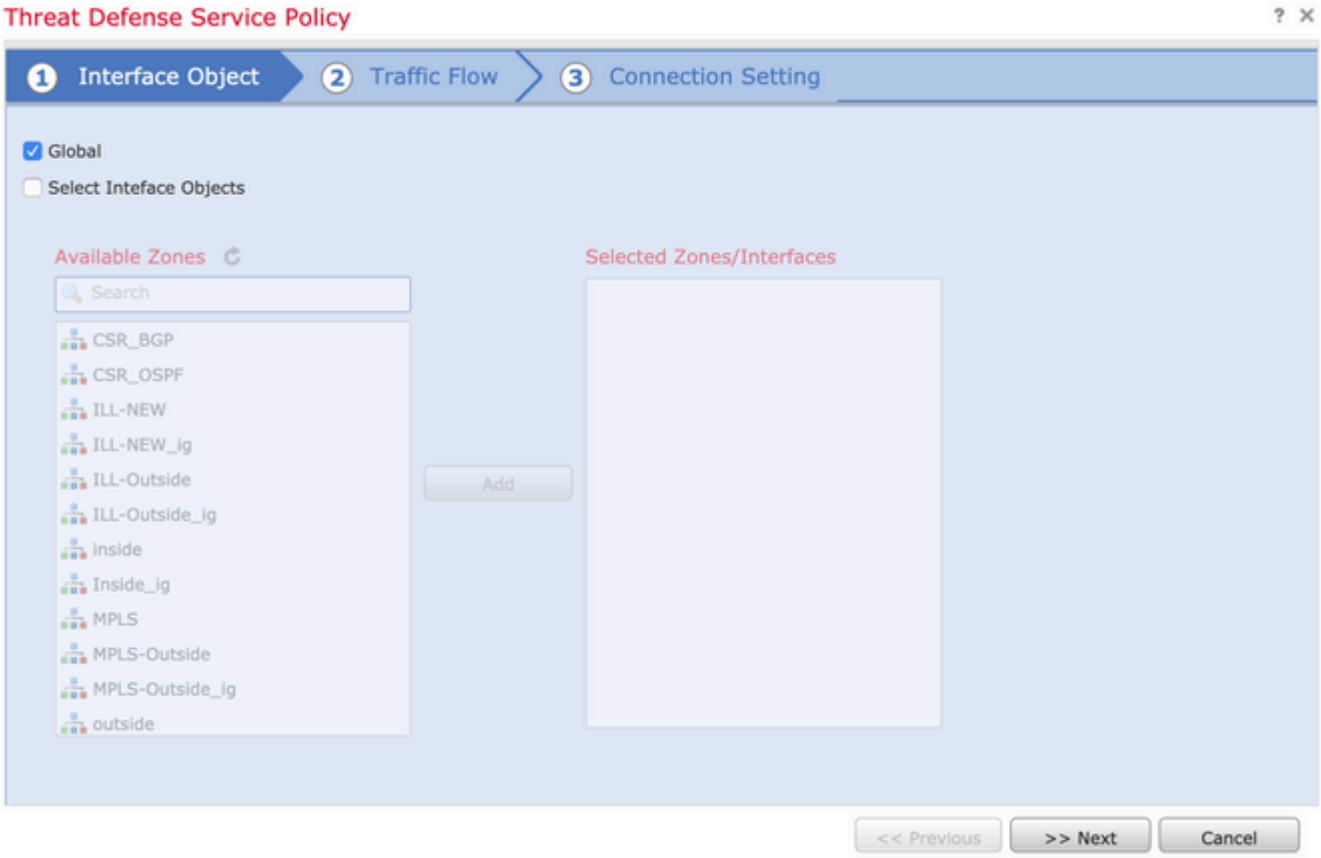
Paso 1. Cree la ACL extendida que define la clase de tráfico para la que se deben habilitar los informes de traceroute.

Inicie sesión en la **GUI de FMC** y navegue hasta **Objetos > Administración de objetos > Lista de acceso**. Seleccione **Extended** en la tabla de contenido y **Add** a new Extended Access List. Introduzca un nombre para el objeto, por ejemplo, en Traceroute_ACL,**Add** a rule to permit ICMP type 3 and 11 and **save**, como se muestra en la imagen:

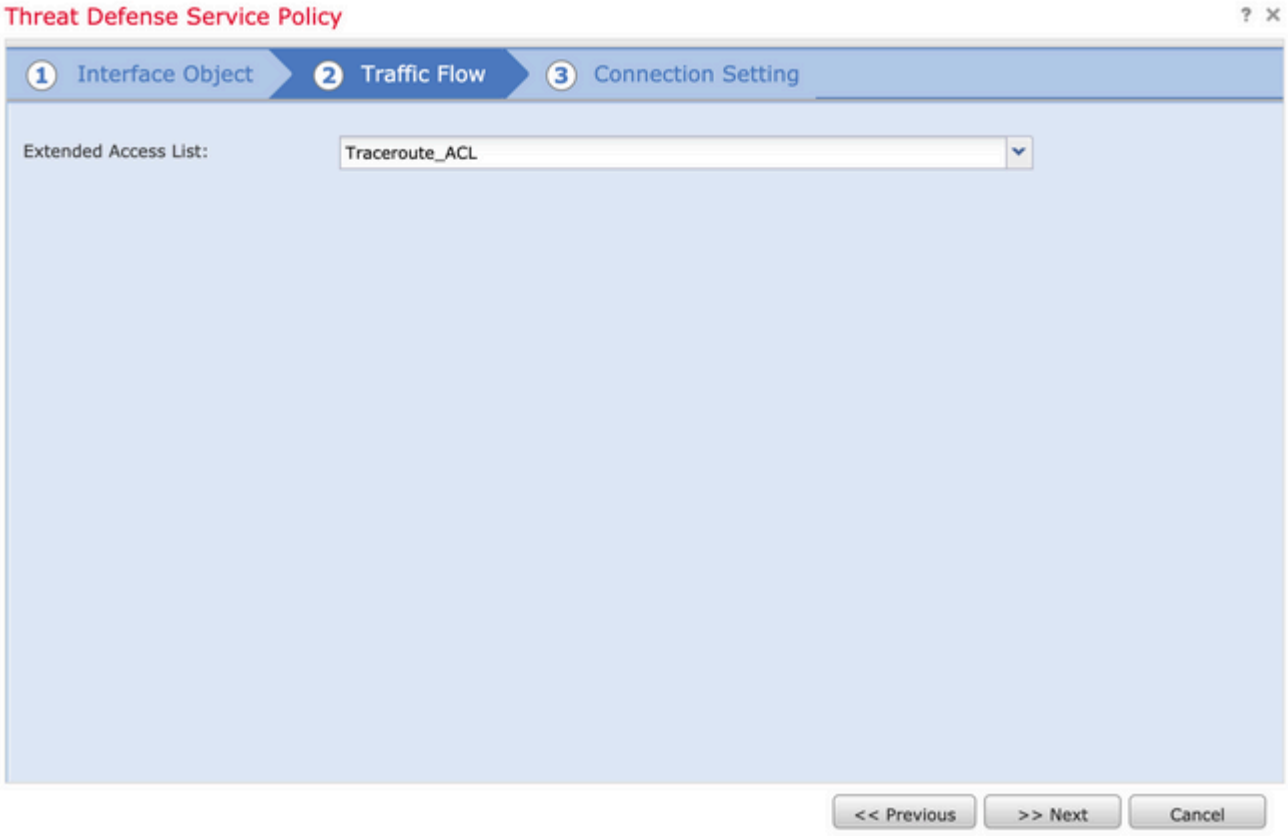


Paso 2. Configure la regla de política de servicio que reduce el valor de tiempo de vida.

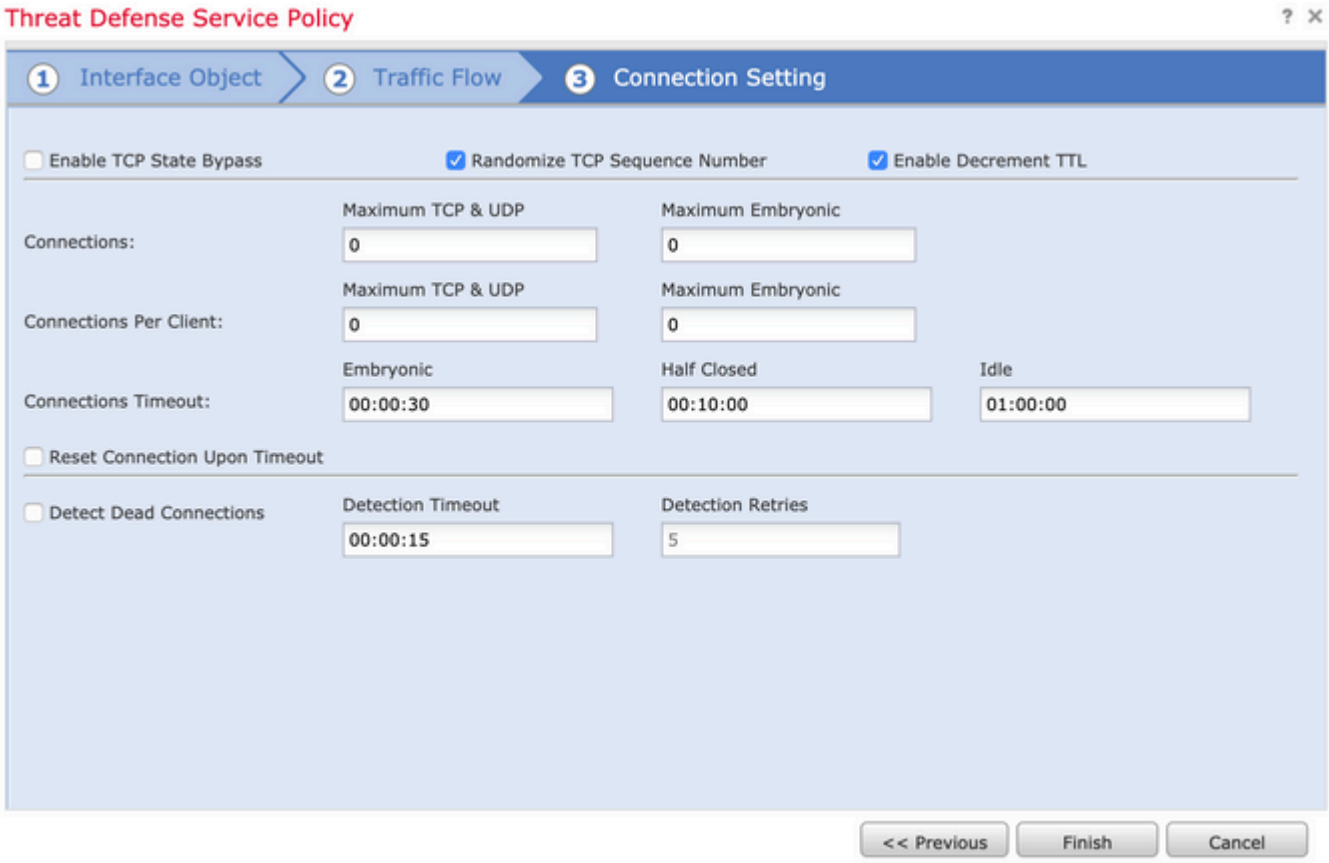
Navegue hasta **Políticas** > **Control de acceso** y luego **Editar** la política asignada al dispositivo. En la ficha Avanzadas, edite la directiva del servicio de Threat Defence y, a continuación, agregue una nueva regla desde la ficha **Agregar regla**, marque la casilla de verificación **Global** para aplicarla globalmente y haga clic en **Siguiente**, como se muestra en la imagen:



Navegue hasta **Traffic Flow** > Extended Access List y luego elija **Extended Access List Object** del menú desplegable que se creó en pasos anteriores. Ahora haga clic en **Next,** como se muestra en la imagen:



Seleccione la casilla de verificación **Enable Decrement TTL** y modifique las otras opciones de conexión (Opcional). Ahora, haga clic en **Finish** para agregar la regla, luego haga clic en **OK**, **y** Save **los cambios a la política del servicio Threat Defence, como se muestra en la imagen:**

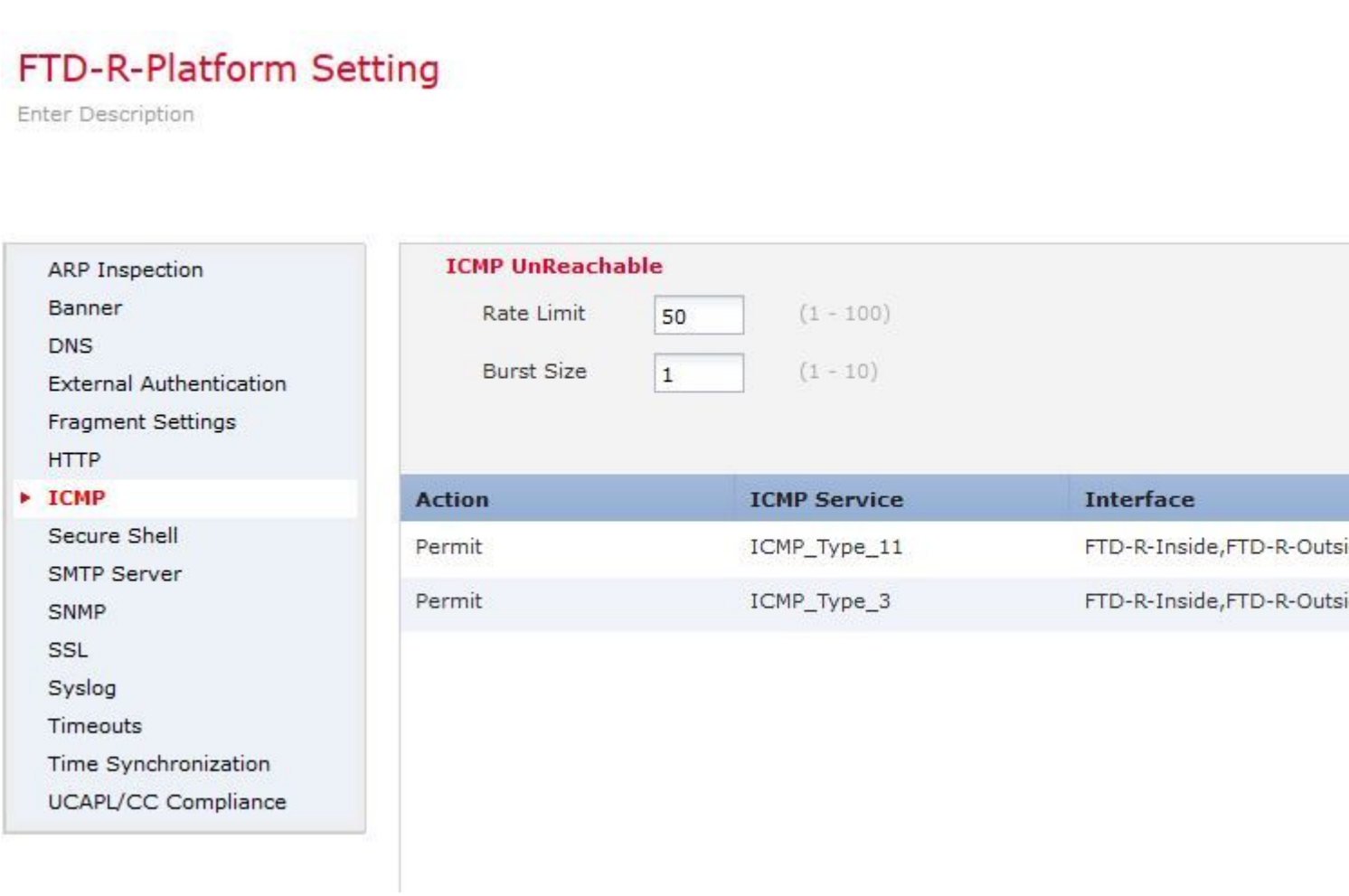


Una vez completados los pasos anteriores, **guarde** la directiva de control de acceso.

Paso 3. Permita ICMP en el Interior y el Exterior, e Incree el Límite de Velocidad a 50 (opcional).

Navegue hasta **Devices > Platform Settings** y luego **Edit** o **Create** una nueva política de configuración de la plataforma Firepower Threat Defence y asóciela al dispositivo. Elija **ICMP** de la tabla de contenido y Aumente el Límite de Velocidad. Por ejemplo, a 50 (puede ignorar el tamaño de ráfaga) y luego haga clic en **Save**, y continúe con **Deploy** the Policy to the device, como se muestra en la imagen:

- **Límite de velocidad**: establece el límite de velocidad de los mensajes inalcanzables, entre 1 y 100 mensajes por segundo. El valor predeterminado es 1 mensaje por segundo.
- **Tamaño de ráfaga (Burst Size)**: permite definir la velocidad de ráfaga, entre 1 y 10. Este valor no está siendo utilizado actualmente por el sistema.



Precaución: asegúrese de que **ICMP Destination Unreachable (Tipo 3) y ICMP Time Exceeded (Tipo 11)** estén permitidos de afuera hacia adentro en la política ACL o Fastpath'ed en la política de prefiltro.

Verificación

Verifique la configuración desde la CLI de FTD una vez que se haya completado la implementación de políticas:

```
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

Puede tomar capturas en las interfaces de ingreso y egreso de FTD para el tráfico interesante para resolver el problema con mayor profundidad.

La captura de paquetes en Lina, mientras se realiza el traceroute, puede mostrarse así para cada esperanza en la ruta hasta que alcanza la 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
```

Se puede obtener un resultado más detallado en la CLI de Lina si realiza traceroute con los switches "-I" y "-n" enumerados.

```
[ 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.
```

Sugerencia: Id. de error de Cisco CSCvq79913. Los paquetes de error ICMP se descartan para Null pdts_info. Asegúrese de utilizar el prefiltro para ICMP, preferiblemente para el tráfico de retorno de tipo 3 y 11.

Información Relacionada

Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).