Activer Traceroute via Firepower Threat Defense FTD

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Autoriser ICMP à l'intérieur et à l'extérieur, et augmenter la limite de débit à 50 - Facultatif

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit la configuration pour autoriser traceroute via Firepower Threat Defense (FTD) via la politique de service de défense contre les menaces.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

- Cet article s'applique à toutes les plates-formes Firepower.
- Cisco Firepower Threat Defense qui exécute la version 6.4.0 du logiciel.
- Cisco Firepower Management Center Virtual qui exécute la version logicielle 6.4.0.

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

Traceroute vous aide à déterminer la route que les paquets empruntent pour atteindre leur destination finale. Traceroute fonctionne en envoyant des paquets UDP (User Datagram Protocol) à une destination sur un port non valide. Comme le port n'est pas valide, les routeurs en route vers la destination répondent avec un message ICMP (Internet Control Message Protocol) de dépassement de délai et signalent cette erreur à l'appliance ASA (Adaptive Security Appliance).

La commande traceroute affiche le résultat de chaque sonde envoyée et chaque ligne de sortie correspond à une valeur de durée de vie (TTL) dans l'ordre croissant. Ce tableau explique les symboles de sortie.

Symbole de sortie	Description
*	Aucune réponse n'a été reçue pour la sonde dans le délai imparti.
nn msec	Pour chaque noeud, le temps aller-retour (en millisecondes) pour le nombre spécifié de sondes.
!n	Le réseau ICMP est inaccessible.
!H	L’hôte ICMP est inaccessible.
!P	Le protocole/port ICMP est inaccessible.
!A	ICMP administrativement interdit.

?	Erreur ICMP inconnue.

Par défaut, l'ASA n'apparaît pas sur les traceroutes comme un saut. Pour le faire apparaître, décrémentez la durée de vie sur les paquets qui passent par l'ASA et augmentez la limite de débit sur les messages ICMP inaccessibles.

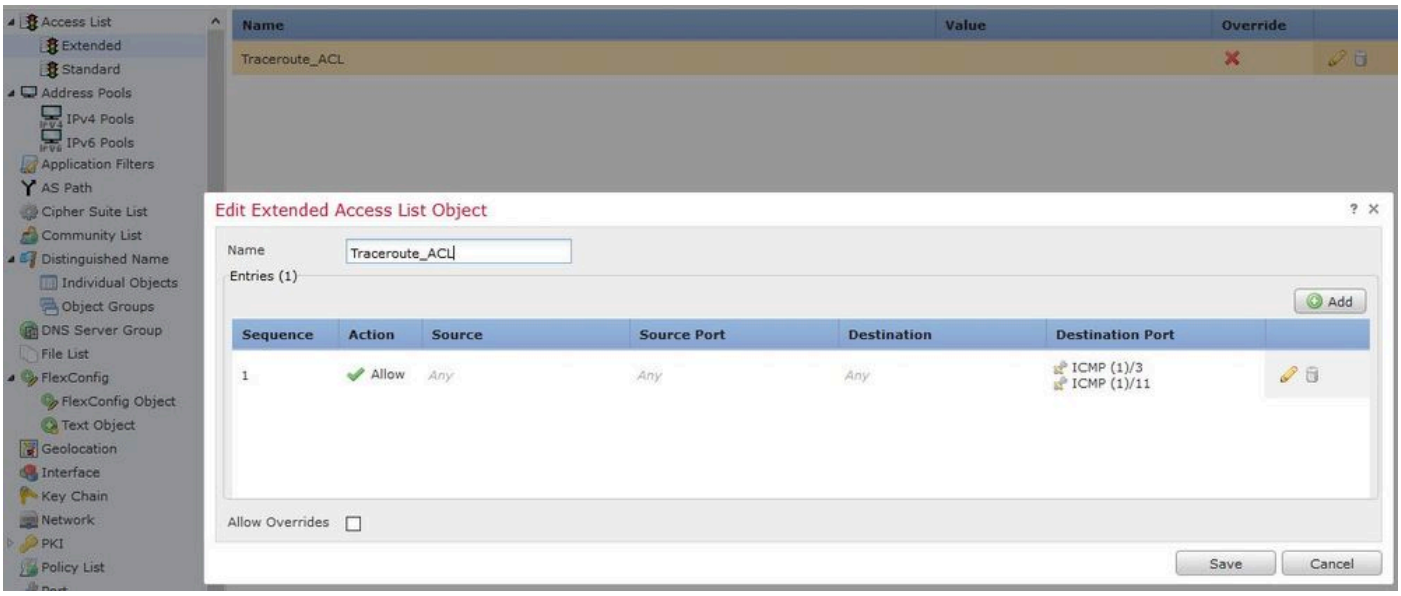
⚠ Mise en garde : Si vous décrémentez le temps de vie, les paquets avec une TTL de 1 sont abandonnés, mais une connexion est ouverte pour la session en supposant que la connexion peut contenir des paquets avec une TTL supérieure. Certains paquets, tels que les paquets Hello OSPF, sont envoyés avec une durée de vie de 1, de sorte que la diminution du temps de vie peut avoir des conséquences inattendues. Gardez ces considérations à l'esprit lorsque vous définissez votre classe de trafic.

Configurer

1. Créez la liste de contrôle d’accès étendue qui définit la classe de trafic pour laquelle le rapport traceroute doit être activé.

2. Connectez-vous à l'interface utilisateur FMC et accédez à Objets > Gestion des objets > Liste d'accès. Sélectionnez Étendue dans la table des matières et ajoutez une nouvelle liste d'accès étendue.

3. Entrez un nom pour l'objet, par exemple, Sous Traceroute_ACL, Ajoutez une règle pour autoriser ICMP de type 3 et 11 et Enregistrez-la, comme indiqué dans l'image :

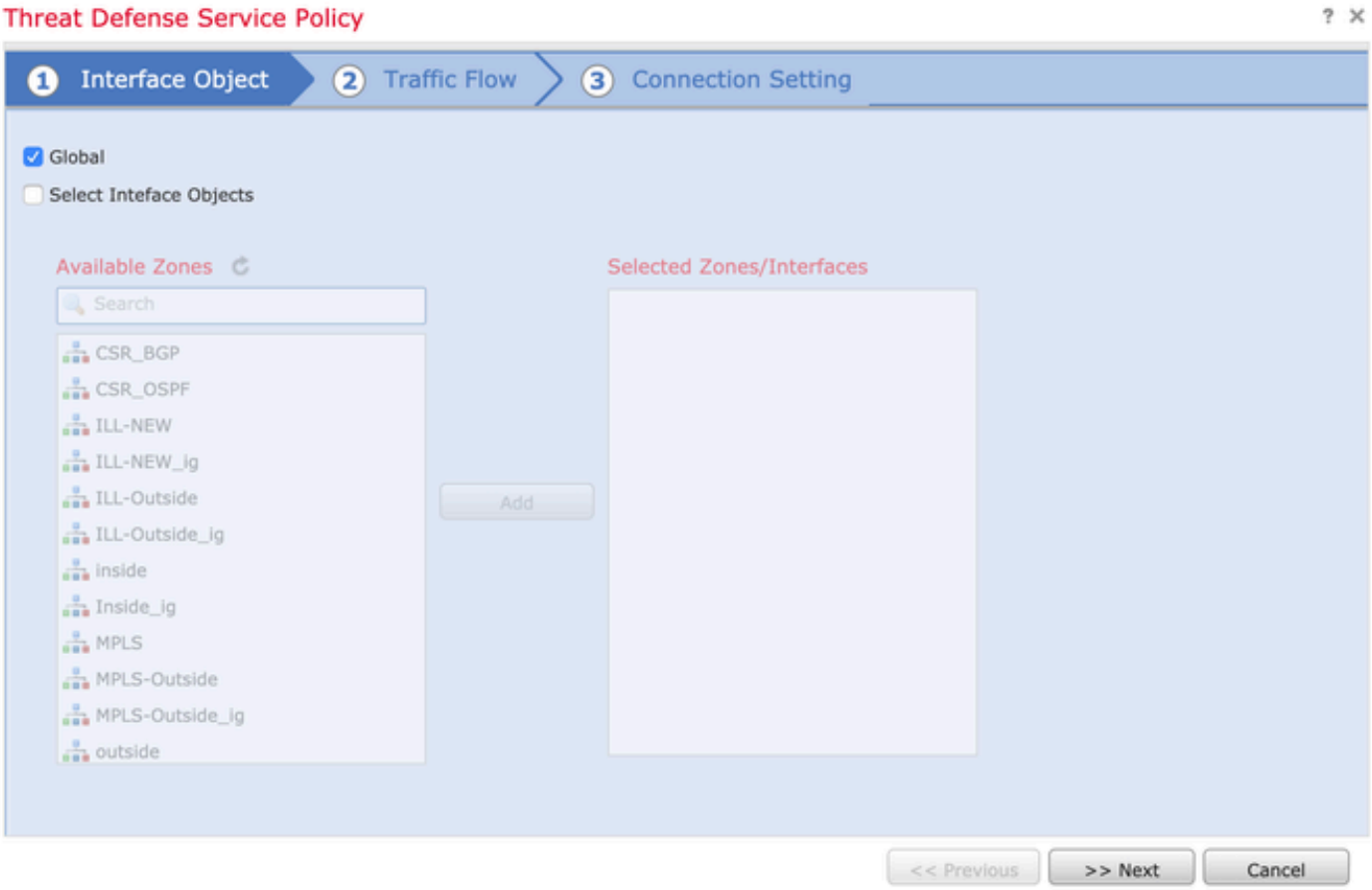


---

4. Configurez la règle de stratégie de service qui décrémente la valeur de durée de vie.

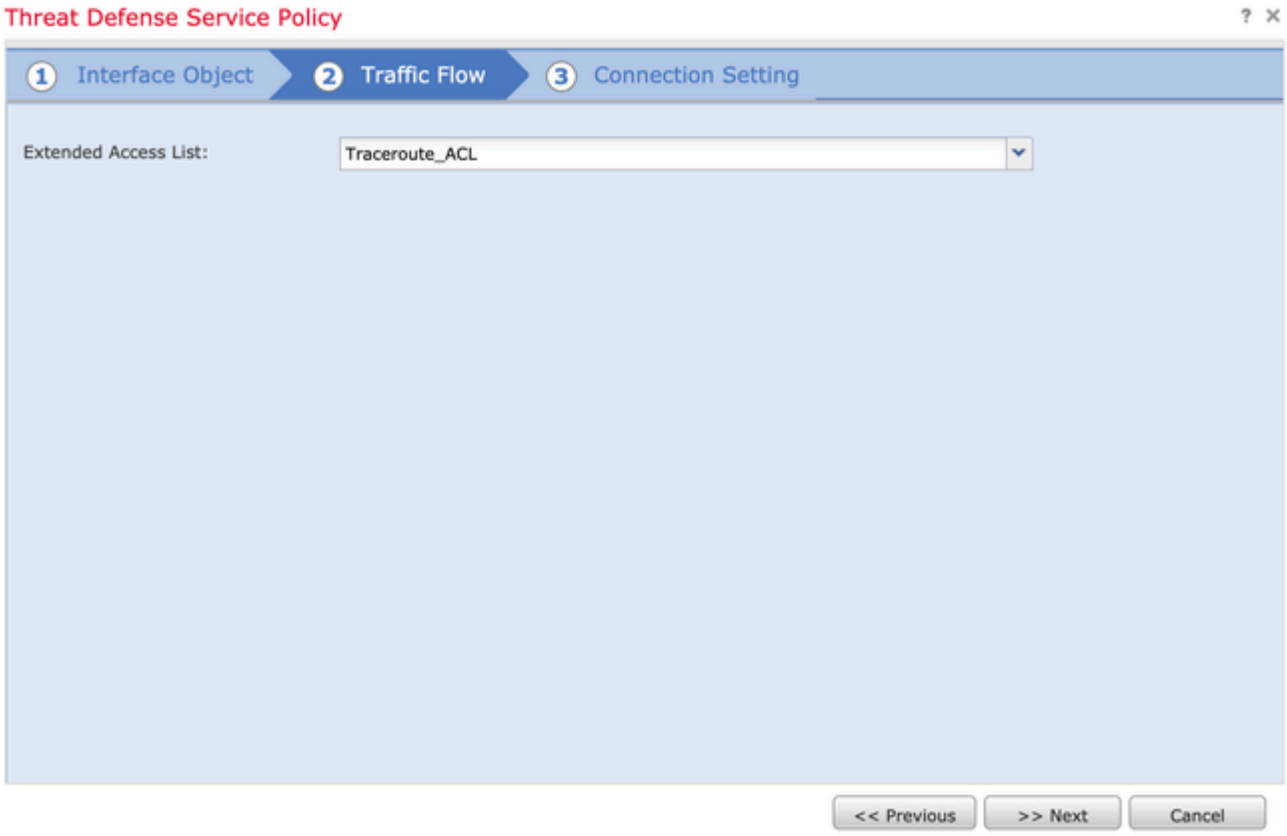
---

5. Accédez à Politiques > Contrôle d'accès et puis Modifier la stratégie attribuée au périphérique. Sous l'onglet Avancé, modifiez la stratégie de service de défense contre les menaces, puis ajoutez une nouvelle règle à partir de l'onglet Ajouter une règle, puis activez la case à cocher Global pour l'appliquer globalement ou sélectionnez des zones particulières où vous souhaitez appliquer le décrément de durée de vie), puis cliquez sur Suivant, comme illustré dans l'image :



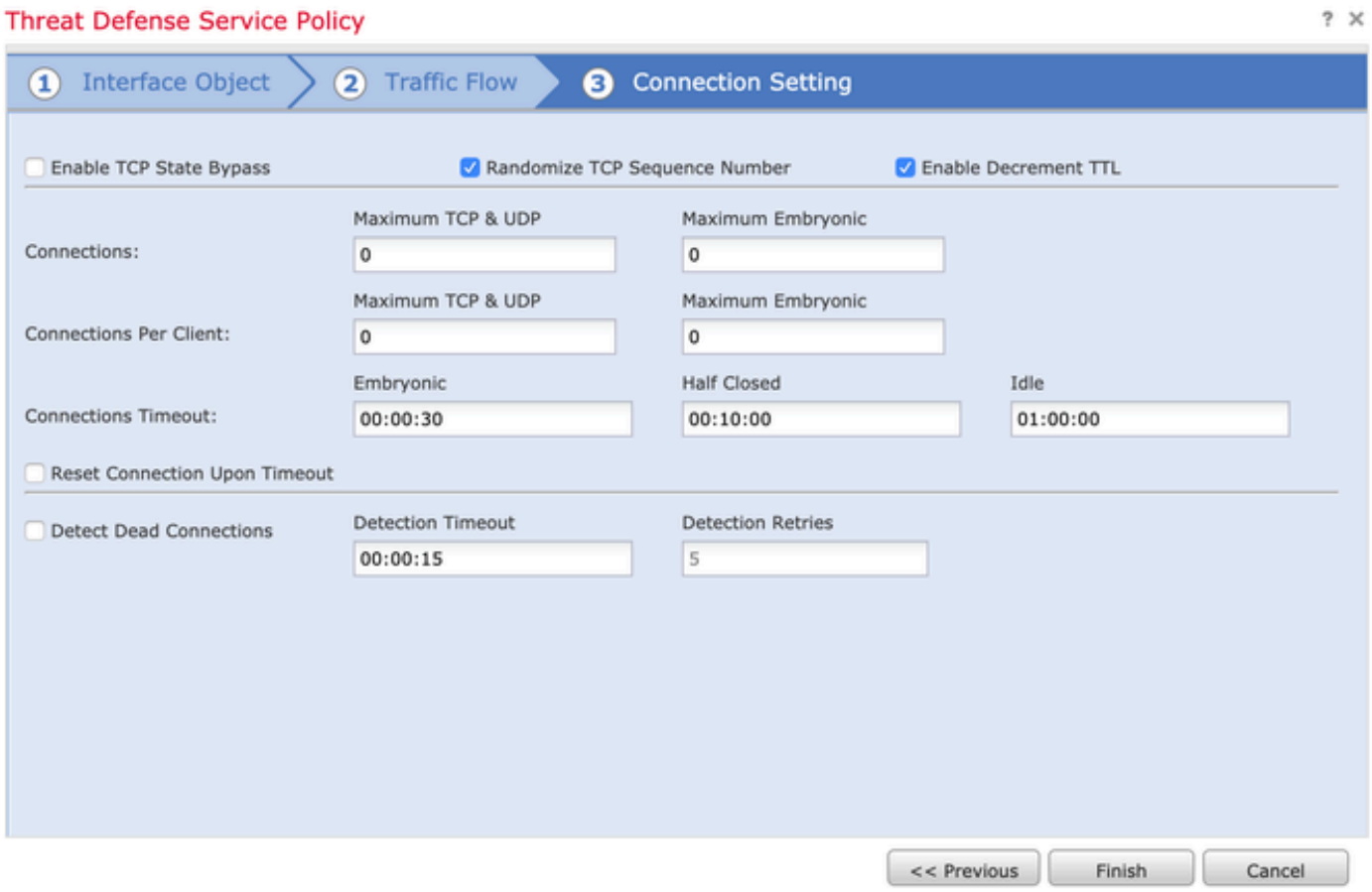
---

6. Accédez à Traffic Flow > Extended Access List et choisissez Extended Access List Object dans le menu déroulant, qui a été créé dans les étapes précédentes. Cliquez maintenant sur Next, comme le montre l'image :



---

7. Cochez la case Enable Decrement TTL et modifiez les autres options de connexion (facultatif). Cliquez à présent sur Finish pour ajouter la règle, puis sur OK, et Save the changes to the Threat Defense Service Policy, comme indiqué dans l'image :



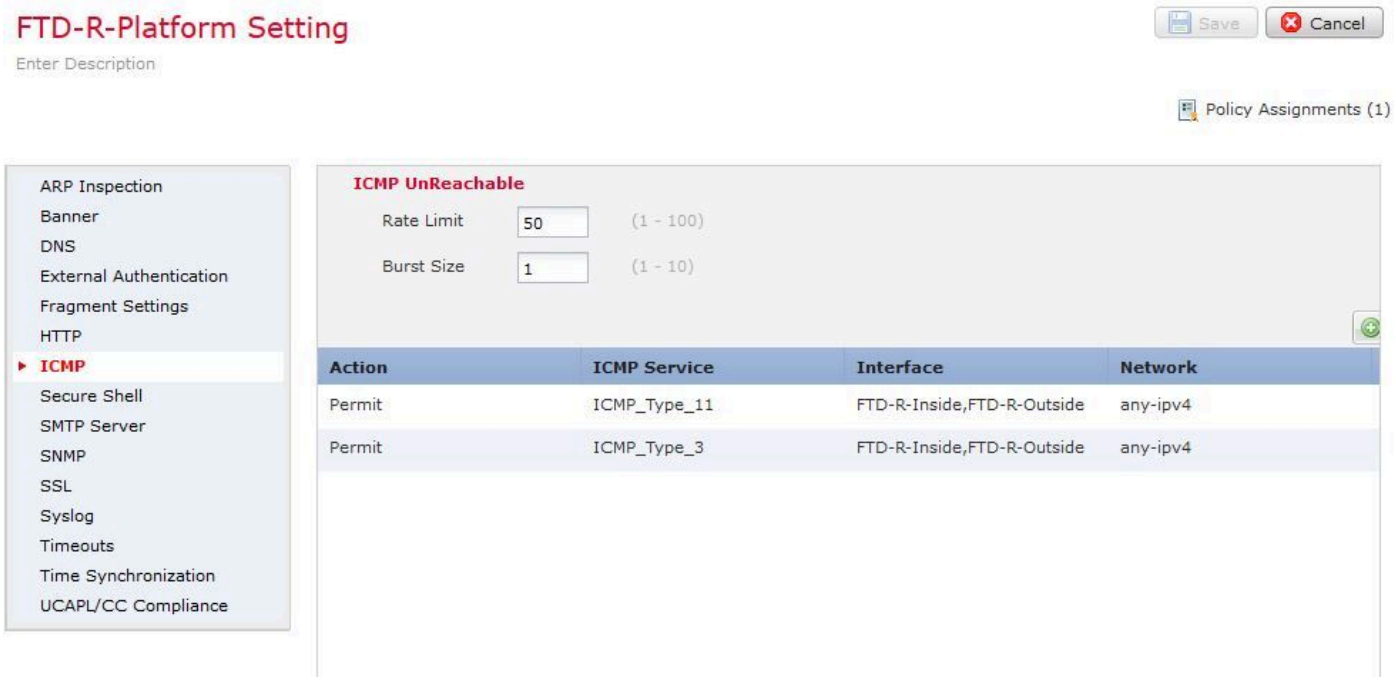
---

8. Une fois les étapes précédentes terminées, enregistrez la stratégie de contrôle d'accès.

Autoriser ICMP à l'intérieur et à l'extérieur, et augmenter la limite de débit à 50 - Facultatif

1. Accédez à Périphériques > Paramètres de la plate-forme, puis Modifier ou Créer une nouvelle stratégie de paramètres de la plate-forme Firepower Threat Defense et associez-la au périphérique. Choisissez ICMP dans la table des matières et Augmentez la limite de débit. Par exemple, à 50 (vous pouvez ignorer la taille de rafale), puis cliquez sur Save, et continuez à Deploy the Policy to the device, comme indiqué dans l'image :

- Rate Limit : définit la limite de débit des messages inaccessibles entre 1 et 100 messages par seconde. La valeur par défaut est 1 message par seconde.
- Burst Size : définit le taux de rafale entre 1 et 10. Cette valeur n'est pas actuellement utilisée par le système.



Mise en garde : Assurez-vous que la destination ICMP inaccessible (type 3) et le délai ICMP dépassé (type 11) sont autorisés de l'extérieur vers l'intérieur dans la stratégie de liste de contrôle d'accès ou via Fastpath dans la stratégie de pré-filtrage pour le trafic intéressant que vous souhaitez tester.

Remarque : Assurez-vous d'ajouter ICMP de type 0 et 8 dans le cadre de la configuration ICMP sous les paramètres de la plate-forme si IP SLA ou PBR est configuré pour un scénario à deux FAI. Dans le cas contraire, le SLA peut échouer et les routes par défaut associées au SLA peuvent être extraites du RIB, ce qui peut entraîner une panne de trafic.

Vérifier

Vérifiez la configuration à partir de l'interface de ligne de commande FTD une fois le déploiement de la stratégie terminé :

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

Dépannage

Vous pouvez effectuer des captures sur les interfaces d'entrée et de sortie FTD pour le trafic unique afin de résoudre le problème. La capture de paquets sur Lina, pendant que la commande traceroute est exécutée à partir de l'hôte, peut afficher ceci pour chaque saut dans la route jusqu'à ce qu'elle atteigne l'IP cible :

```
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 unreachabl
  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
```

Une sortie plus détaillée peut être obtenue sur Lina CLI si vous exécutez traceroute avec les commutateurs "-I" et "-n" comme indiqué :

```
[ 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 i


[ 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.
```



Conseil : ID de bogue Cisco CSCvq79913 - Les paquets d'erreur ICMP sont abandonnés pour Null pdts_info. Veillez à utiliser le préfiltre pour ICMP, de préférence pour le trafic de retour de type 3 et 11.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.