Traceroute toestaan via FirePOWER Threat Defence (FTD)

Inhoud

Inleiding

Dit document beschrijft de configuratie om de traceroute toe te staan via Firepower Threat Defence (FTD) via het beleid voor bedreigingsservices.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Dit artikel is van toepassing op alle Firepower platforms.
- Cisco Firepower Threat Defence die softwareversie 6.4.0 uitvoert.
- Cisco Firepower Management Center Virtual, waarop softwareversie 6.4.0 wordt uitgevoerd.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Traceroute om u te helpen de route te bepalen die pakketten naar hun bestemming nemen. Een traceroute werkt door Unified Data Platform (UDP)-pakketten naar een bestemming op een ongeldige poort te verzenden. Omdat de poort niet geldig is, reageren de routers langs de weg naar de bestemming met een ICMP-overschrijding (Internet Control Message Protocol) en melden deze fout aan de adaptieve security applicatie (ASA).

De traceroute toont het resultaat van elke verzonden sonde. Elke uitvoerlijn komt overeen met de waarde Time to Live (TTL) in oplopende volgorde. Deze tabel verklaart de uitvoersymbolen.

Uitvoersymbool	**Beschrijving**
*	Er werd binnen de tijdsduur geen reactie ontvangen op de sonde.
nn msec	Voor elke knoop, de round-trip tijd (in milliseconden) voor het gespecificeerde aantal sondes.
!N	ICMP-netwerk is onbereikbaar.
!H	ICMP-host is onbereikbaar.
!P	ICMP is onbereikbaar.
!A	ICMP is administratief verboden.
?	Onbekende ICMP-fout.

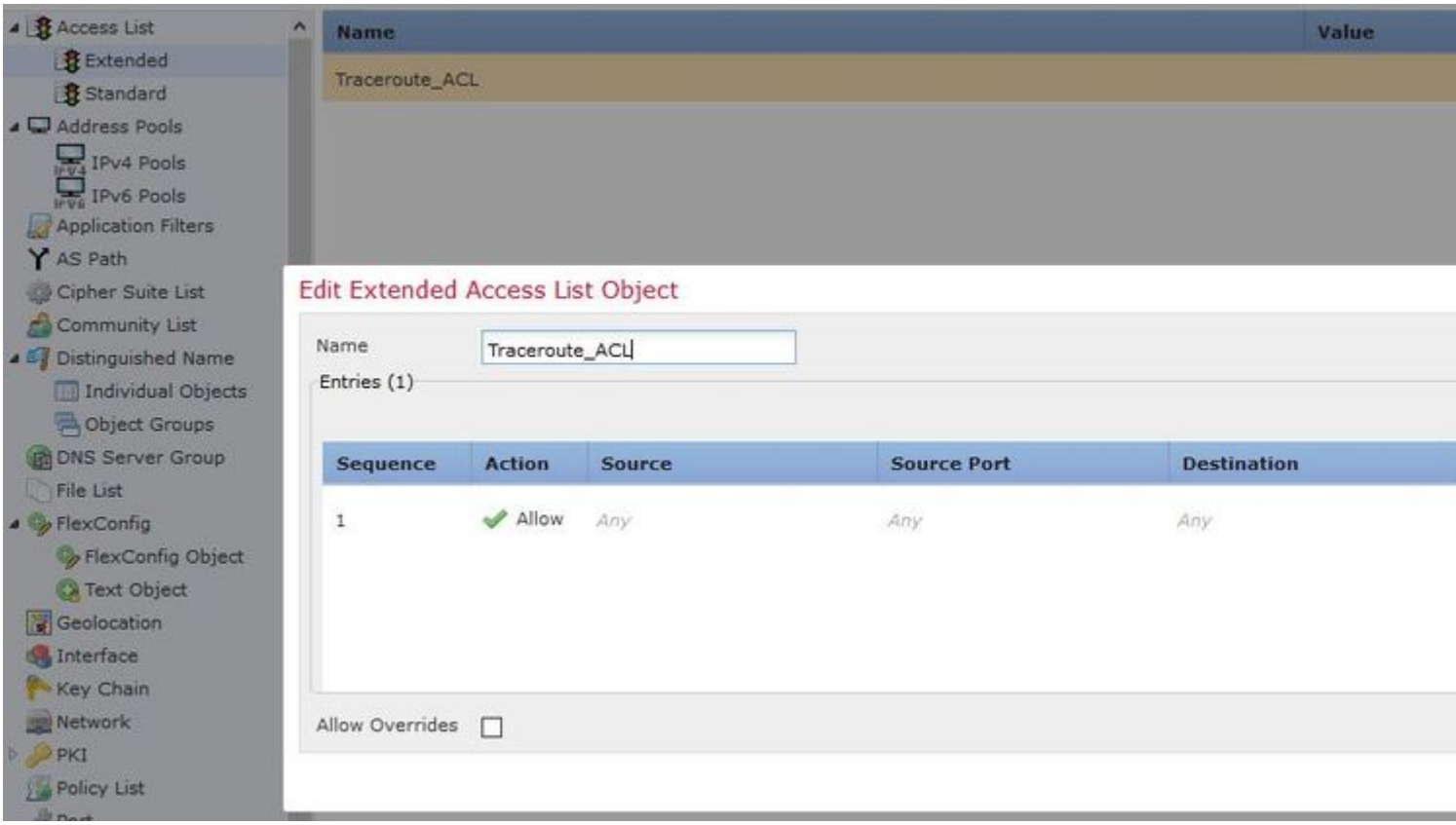
Standaard wordt ASA niet als hop op traceroutes weergegeven. Om het te maken verschijnen, moet u de tijd-aan-leven op pakketten decreteren die door ASA overgaan en de snelheidsgrens op onbereikbare ICMP berichten verhogen.

> **Waarschuwing**: als u de tijd om te leven afneemt, worden pakketten met een TTL van 1 gevallen, maar er wordt een verbinding geopend voor de sessie op basis van de veronderstelling dat de verbinding pakketten met een grotere TTL kan bevatten. Merk op dat sommige pakketten, zoals OSPF hello pakketten, met TTL = 1 worden verzonden, zodat kan de decrementing tijd te leven onverwachte gevolgen hebben. Houd deze overwegingen in gedachten wanneer u uw verkeersklasse definieert.

Configureren

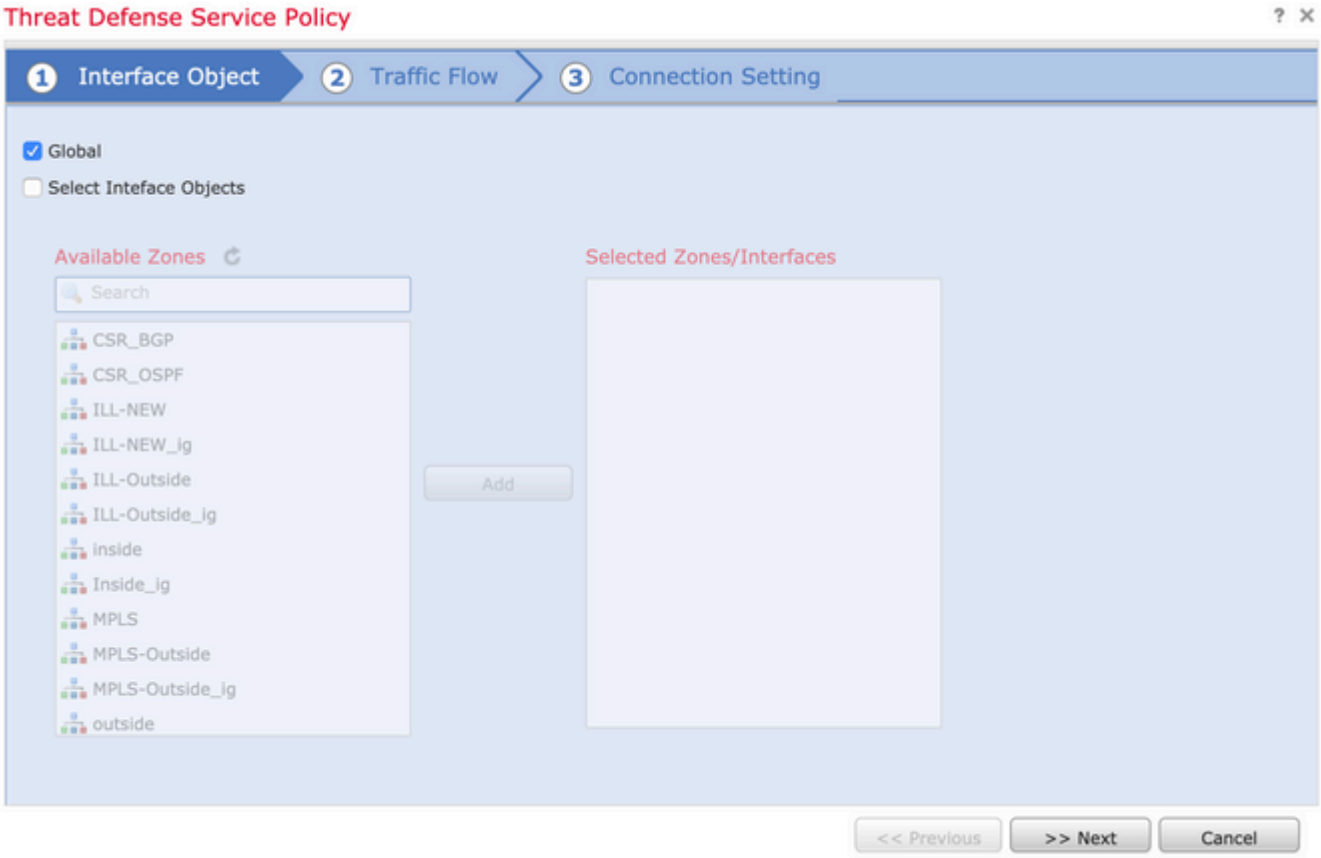
Stap 1. Maak de uitgebreide ACL die de verkeersklasse definieert waarvoor traceroute-rapportage moet worden ingeschakeld.

Log in op **FMC GUI** en navigeer naar **Objecten > Objectbeheer > Toegangslijst**. Selecteer **Uitgebreid** in de inhoudsopgave en **Voeg** een nieuwe uitgebreide toegangslijst toe. Voer een naam voor het object in, bijvoorbeeld onder Traceroute_ACL**, voeg** een regel toe om ICMP-type 3 en 11 toe te staan en **bewaar** het, zoals in de afbeelding:

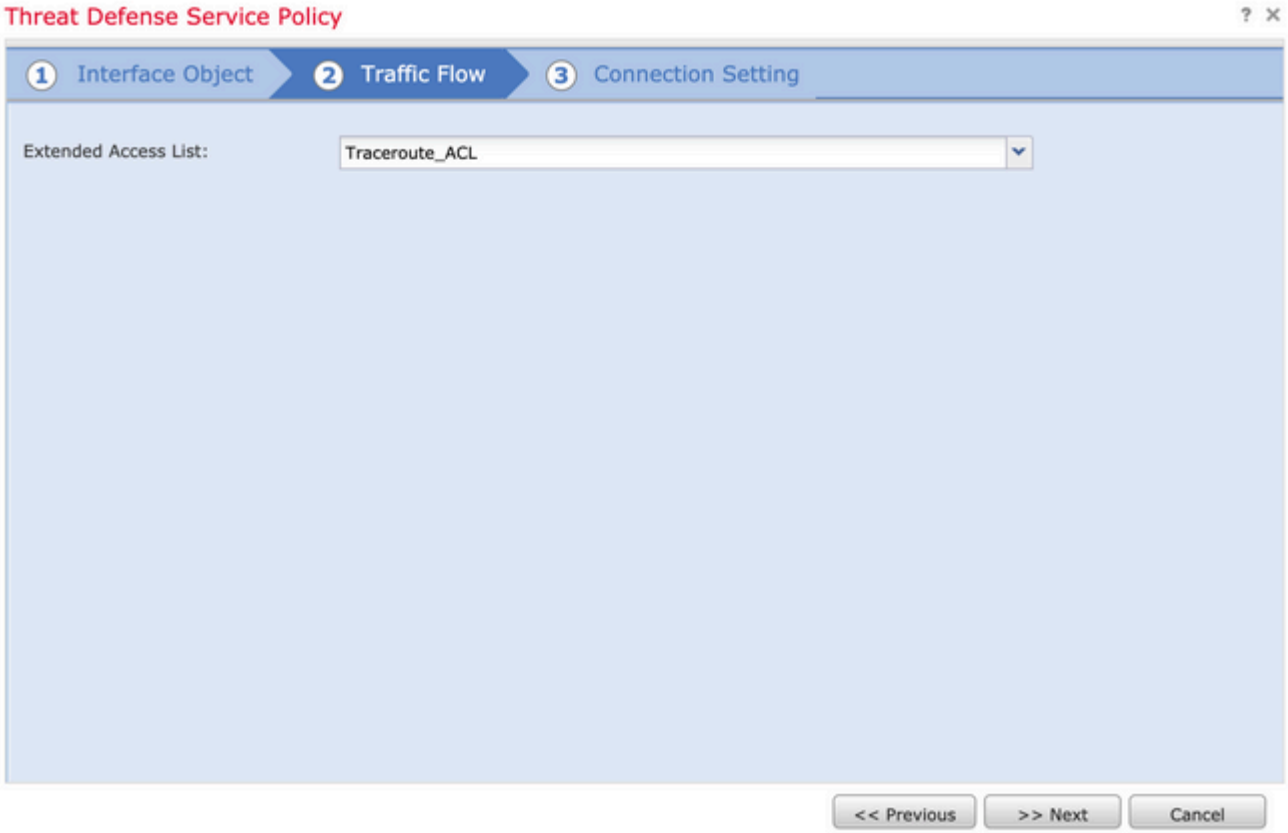


Stap 2. Configureer de regel voor servicebeleid die de waarde van de tijd-tot-leven reduceert.

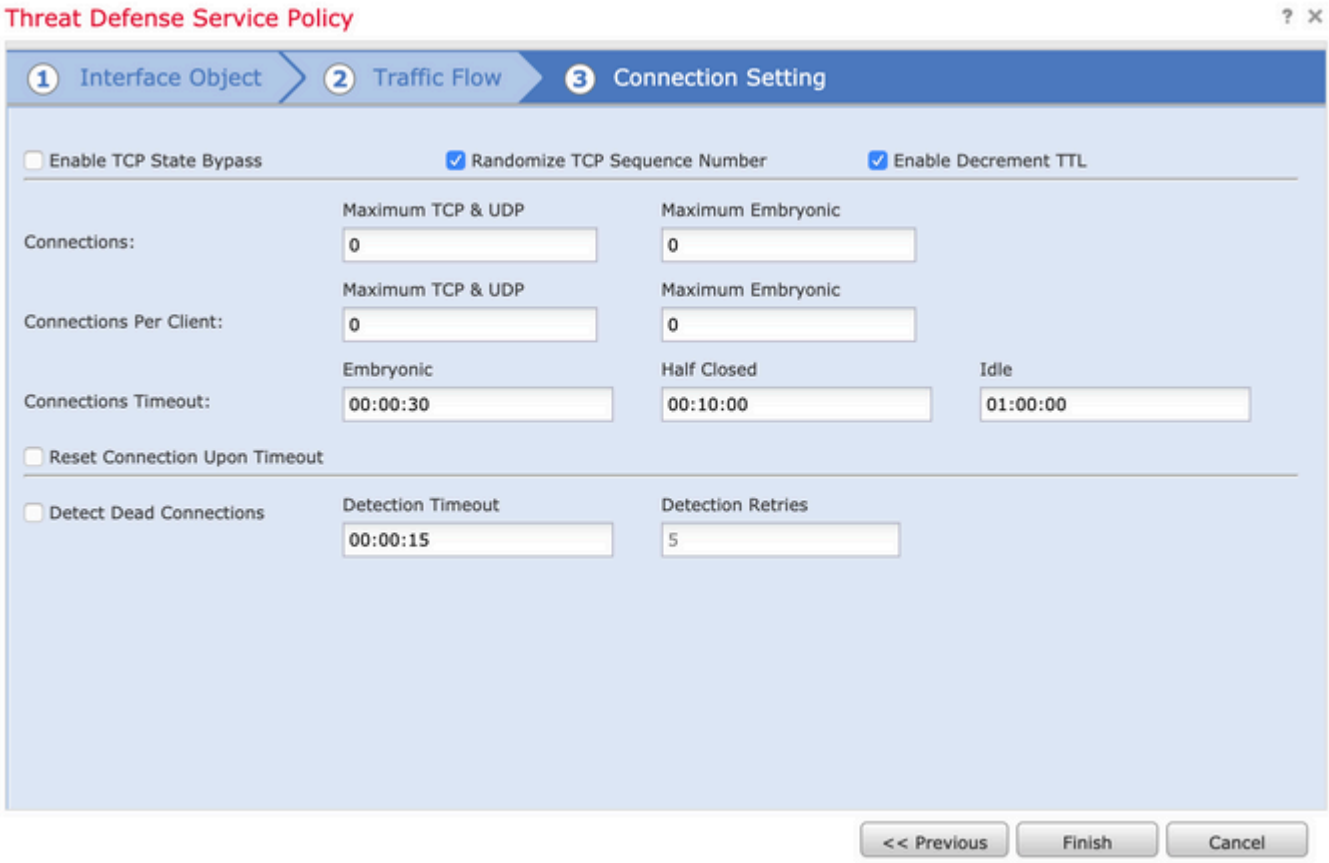
Navigeer naar **Beleid > Toegangsbeheer** en **bewerk** het beleid dat aan het apparaat is toegewezen. Onder het tabblad Geavanceerd, Bewerk het Threat Defense Service Policy en voeg vervolgens een nieuwe regel toe op het tabblad **Regel toevoegen**, kies dan het **aanvinkvakje Global** om het wereldwijd toe te passen en klik op **Volgende**, zoals in de afbeelding wordt getoond:



Navigeer naar **Traffic Flow > Extended Access List** en kies vervolgens **Extended Access List Object** in het vervolgkeuzemenu dat in eerdere stappen is gemaakt. Klik nu op **Volgende,** zoals in de afbeelding:



Kies het selectievakje **Decrement TTL inschakelen** en wijzig de andere verbindingsopties (optioneel). Klik nu op **Voltooien** om de regel toe te voegen, klik vervolgens op **OK** en **Sla** de wijzigingen in het Threat Defense-servicebeleid op, zoals in de afbeelding:

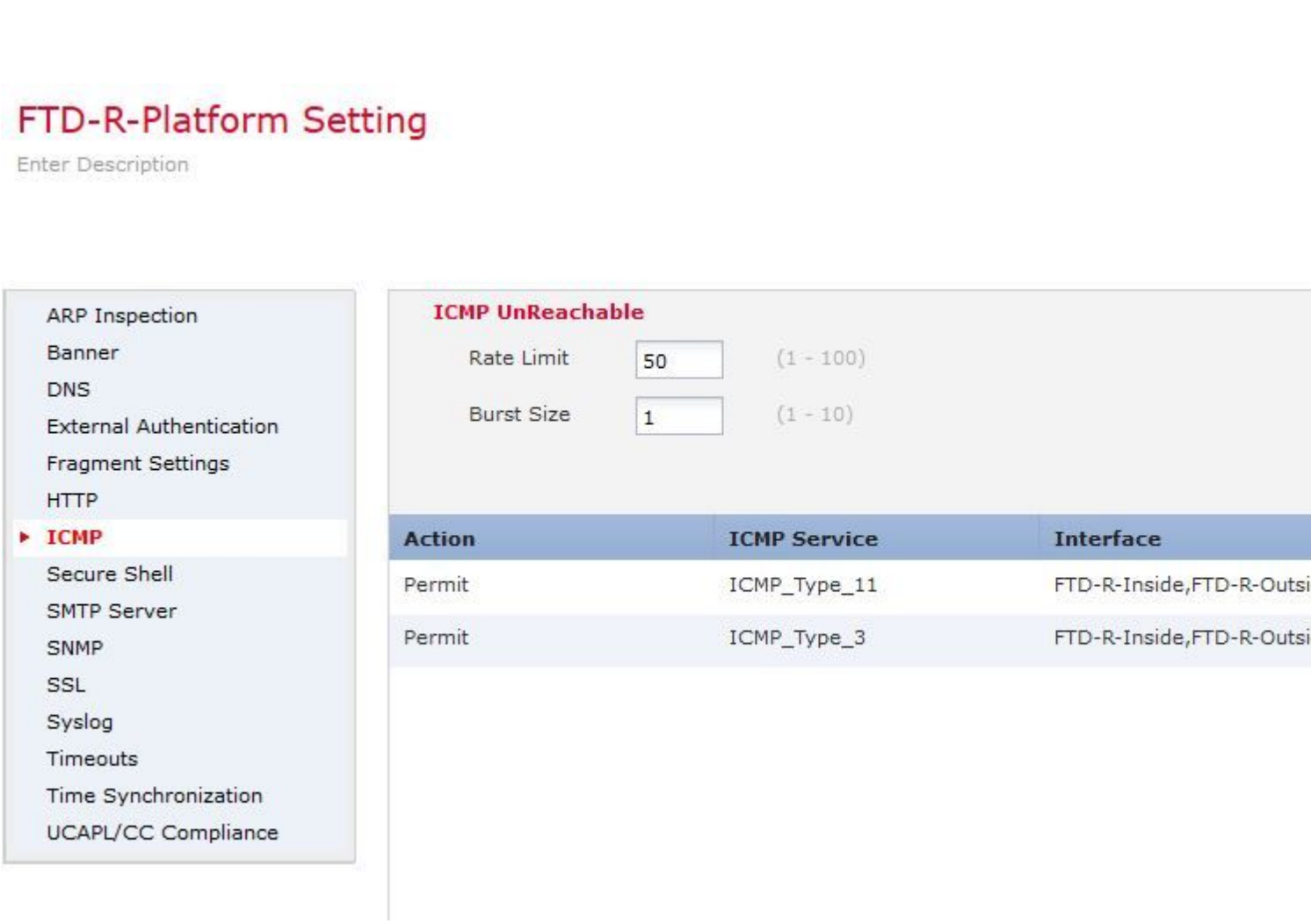


Nadat de vorige stappen zijn voltooid, **slaat u** het toegangscontrolebeleid op.

Stap 3. Laat ICMP toe aan de binnen- en buitenkant en stel de snelheidslimiet in op 50 (optioneel).

Navigeer naar **Apparaten > Platform-instellingen** en **bewerk** of **maak** een nieuw Instellingenbeleid voor Firepower Threat Defence platform en koppel het aan het apparaat. Kies **ICMP** in de inhoudsopgave en verhoog de snelheidslimiet. U kunt bijvoorbeeld op 50 (u kunt de barstgrootte negeren) klikken en vervolgens op **Opslaan** klikken, en **het** beleid **implementeren** op het apparaat, zoals in de afbeelding:

- **Snelheidsbeperking**â€"Hiermee stelt u de snelheidslimiet in van onbereikbare berichten, tussen 1 en 100 berichten per seconde. De standaardinstelling is 1 bericht per seconde.
- **Burst Size**â€"Hiermee stelt u de barstsnelheid in tussen 1 en 10. Deze waarde wordt momenteel niet door het systeem gebruikt.



Waarschuwing: zorg ervoor dat **ICMP-bestemming onbereikbaar (type 3) en ICMP-tijd overschreden (type 11)** is toegestaan van buiten naar binnen in het ACL-beleid of FastPath in het Pre-Filter-beleid.

Verifiëren

Controleer de configuratie van FTD CLI zodra de beleidsontwikkeling is voltooid:

```
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#
```

Problemen oplossen

U kunt opnamen maken op FTD Ingress- en uitgaande interfaces voor het interessante verkeer om het probleem verder op te lossen.

Packet Capture op Lina, terwijl traceroute wordt uitgevoerd, kan als dit tonen voor elke hoop op de route tot het bereikt het doel IP.

```
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
```

Een meer gedetailleerde output kan op Lina CLI worden verkregen als u traceroute met "-I" en "-n" switches zoals vermeld uitvoert.

```
[ 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.
```

> **Tip**: Cisco bug-id CSCvq79913. ICMP-foutpakketten worden gedropt voor Null pdts_info. Zorg ervoor dat u het voorfilter voor ICMP gebruikt, bij voorkeur voor het type 3 en 11 retourverkeer.

Gerelateerde informatie

Technische ondersteuning en documentatie â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.