Routenverfolgung durch FirePOWER Threat Defense (FTD) zulassen

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration beschrieben, die die Traceroute durch Firepower Threat Defense (FTD) via Threat Service Policy ermöglicht.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Dieser Artikel gilt für alle Firepower-Plattformen.
- Cisco Firepower Threat Defense mit der Softwareversion 6.4.0.
- Cisco FirePOWER Management Center Virtual mit Softwareversion 6.4.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Traceroute, um die Route zu ermitteln, über die Pakete an ihr Ziel geleitet werden. Eine Traceroute funktioniert, indem UDP-Pakete (Unified Data Platform) an ein Ziel auf einem ungültigen Port gesendet werden. Da der Port ungültig ist, antworten die Router auf dem Weg zum Ziel mit einer ICMP-Meldung (Internet Control Message Protocol) Time Exceeded Message und melden diesen Fehler an die Adaptive Security Appliance (ASA).

Die Traceroute zeigt das Ergebnis jeder gesendeten Sonde. Jede Ausgabezeile entspricht einem TTL-Wert (Time to Live) in steigender Reihenfolge. In dieser Tabelle werden die Ausgabesymbole erläutert.

Ausgabesymbol	**Beschreibung**
*	Innerhalb des Timeout-Zeitraums wurde keine Antwort für den Test empfangen.
nn ms	Für jeden Knoten die Round-Trip-Zeit (in Millisekunden) für die angegebene Anzahl von Tests.
!N	Das ICMP-Netzwerk ist nicht erreichbar.
!H	Der ICMP-Host ist nicht erreichbar.
!P	ICMP ist nicht erreichbar.
!A	ICMP wurde administrativ untersagt.
?	Unbekannter ICMP-Fehler.

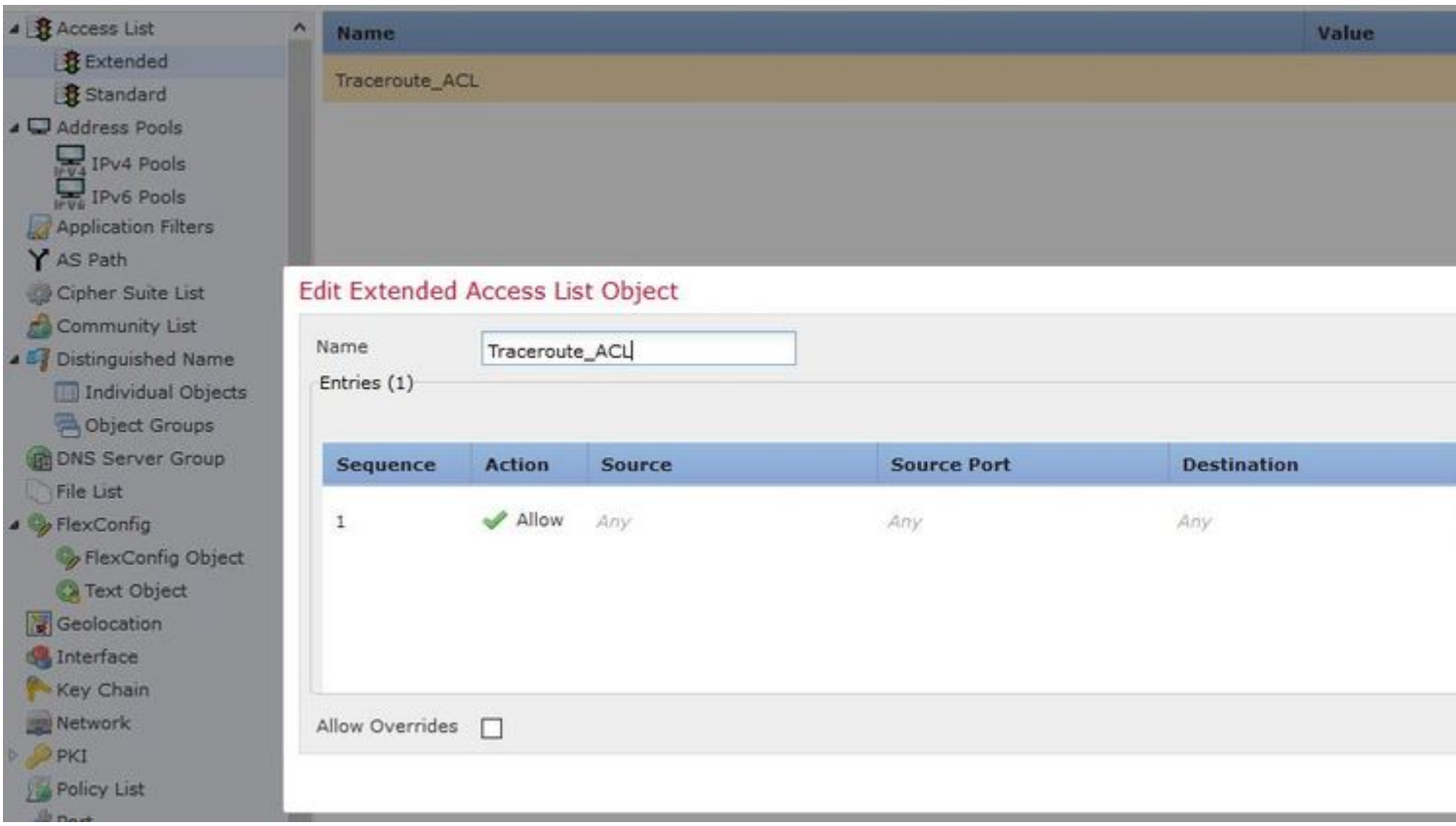
Standardmäßig wird die ASA auf Tracerouten nicht als Hop angezeigt. Damit dies angezeigt wird, müssen Sie die Lebensdauer von Paketen, die die ASA passieren, verkürzen und die Durchsatzgrenze für nicht erreichbare ICMP-Nachrichten erhöhen.

> **Achtung:** Wenn Sie die Lebensdauer reduzieren, werden Pakete mit einer TTL von 1 verworfen, aber eine Verbindung wird für die Sitzung geöffnet, unter der Annahme, dass die Verbindung Pakete mit einer größeren TTL enthalten kann. Beachten Sie, dass einige Pakete, z. B. OSPF-Hello-Pakete, mit TTL = 1 gesendet werden, sodass eine Verkürzung der Lebensdauer unerwartete Folgen haben kann. Beachten Sie diese Überlegungen bei der Definition der Datenverkehrsklasse.

Konfigurieren

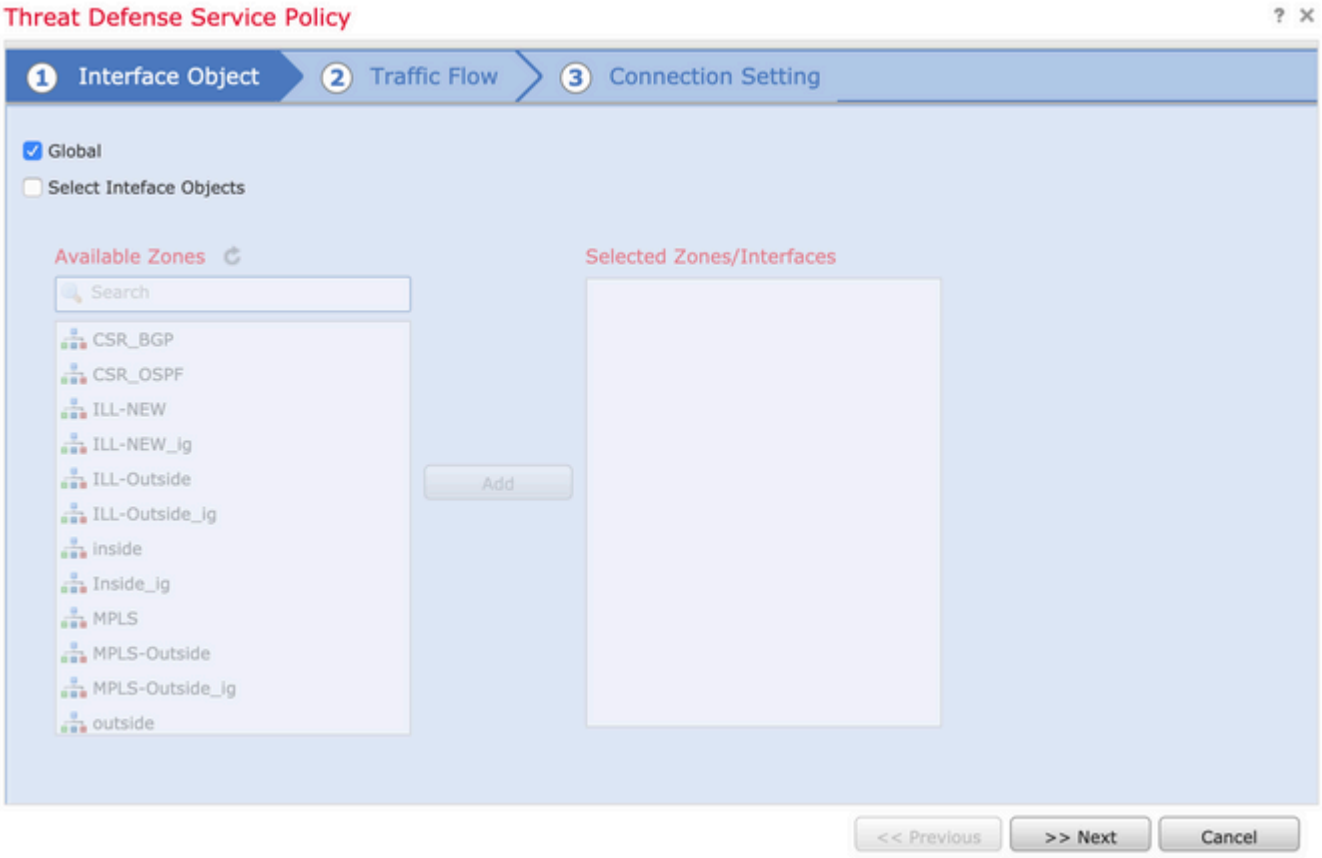
Schritt 1: Erstellen Sie die erweiterte ACL, die die Datenverkehrsklasse definiert, für die die Traceroute-Berichterstellung aktiviert werden muss.

Melden Sie sich bei der **FMC-GUI** an, und navigieren Sie zu **Objects > Object Management > Access List (Objekte > Objektverwaltung > Zugriffsliste)**. Wählen Sie **Erweitert** aus dem Inhaltsverzeichnis aus, und **fügen Sie** eine neue erweiterte Zugriffsliste **hinzu.**Geben Sie einen Namen für das Objekt ein, z. B. unter Traceroute_ACL, **Fügen Sie** eine Regel hinzu, um den ICMP-Typ 3 und 11 zuzulassen und **zu speichern,** wie im Bild gezeigt:

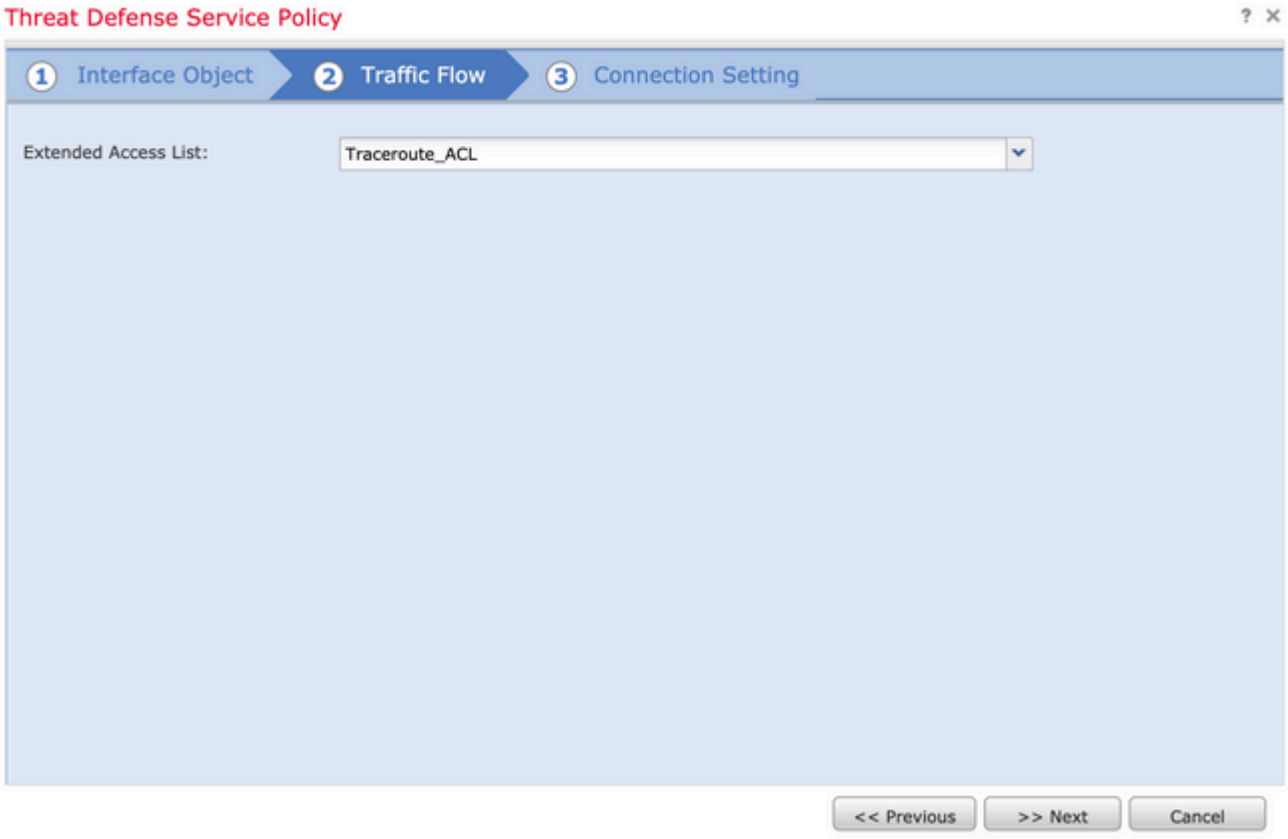


Schritt 2: Konfigurieren Sie die Servicerichtlinien-Regel, die den Time-to-Live-Wert verringert.

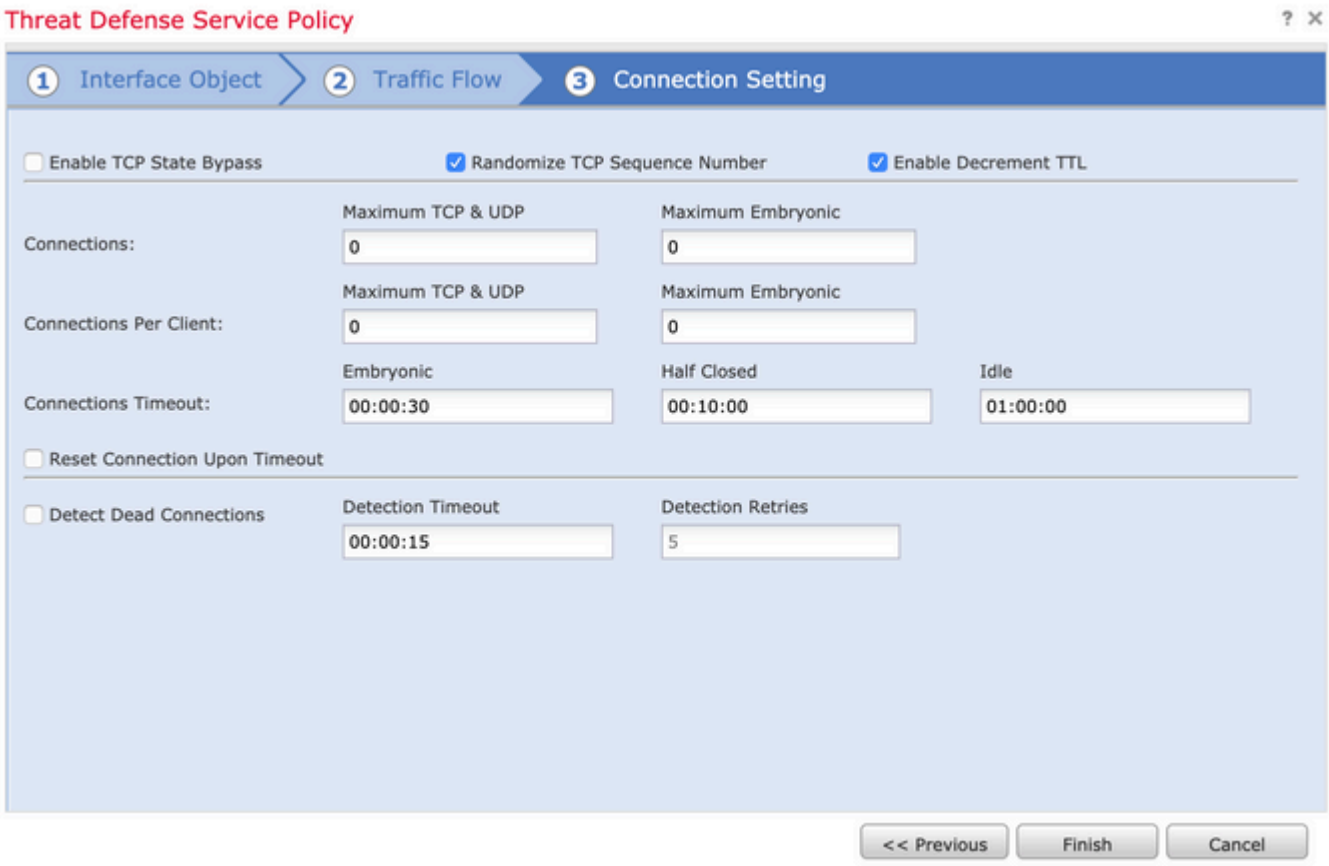
Navigieren Sie zu **Richtlinien > Zugriffskontrolle,** und **bearbeiten Sie** die dem Gerät zugewiesene Richtlinie. Bearbeiten Sie auf der Registerkarte Erweitert die Threat Defense Service-Richtlinie, und fügen Sie dann eine neue Regel von der Registerkarte **Regel hinzufügen hinzu.** Aktivieren Sie dann das Kontrollkästchen **Global,** um sie global anzuwenden, und klicken Sie auf **Weiter**, wie in der folgenden Abbildung gezeigt:



Navigieren Sie zu **Traffic Flow > Extended Access List (Datenverkehrsfluss > Erweiterte Zugriffsliste)**, und wählen Sie im Dropdown-Menü, das mit den vorherigen Schritten erstellt wurde, die Option **Extended Access List Object (Objekt** der erweiterten Zugriffsliste) aus. Klicken Sie nun auf **Weiter**, wie in der Abbildung dargestellt:



Aktivieren Sie das Kontrollkästchen **Dekrement-TTL aktivieren**, und ändern Sie die anderen Verbindungsoptionen (optional). Klicken Sie nun auf **Fertig stellen,** um die Regel hinzuzufügen. Klicken Sie dann auf **OK**, und **speichern Sie** die Änderungen an der Richtlinie für den Schutz vor Bedrohungen, wie in der Abbildung dargestellt:



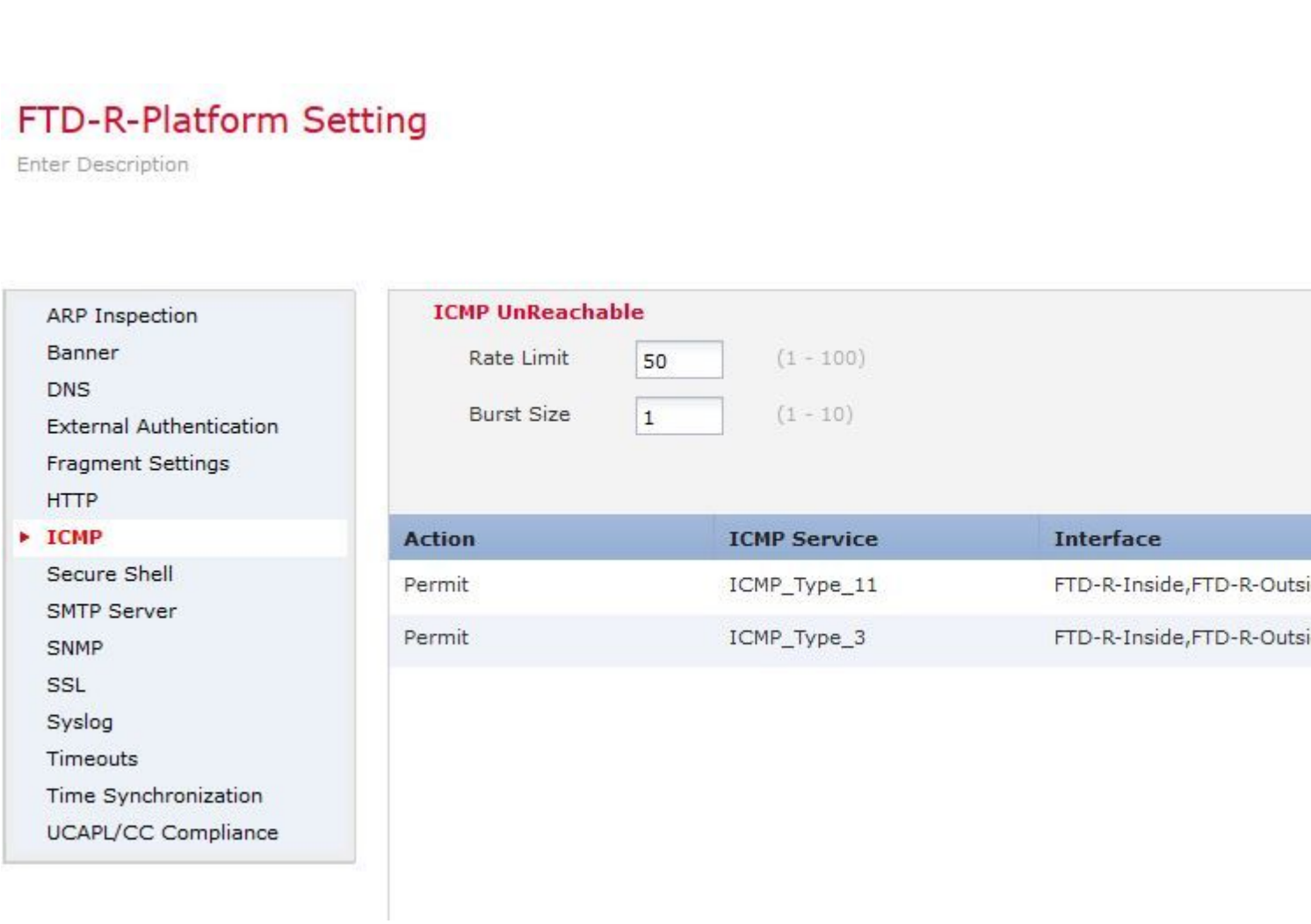
Speichern Sie nach Abschluss der vorherigen Schritte die Zugriffskontrollrichtlinie.

Schritt 3: ICMP intern und extern zulassen und den Ratengrenzwert auf 50 (optional) erhöhen.

Navigieren Sie zu **Geräte > Plattformeinstellungen,** und **bearbeiten** oder **erstellen Sie** eine neue Richtlinie für die Firepower Threat Defense-Plattformeinstellungen, und ordnen Sie diese dem Gerät zu. Wählen Sie **ICMP** aus der Inhaltsübersicht aus, und erhöhen Sie das Durchsatzlimit. Beispiel: bis 50 (Sie können die Burst-Größe ignorieren), dann auf **Speichern** klicken und mit **Bereitstellen** der Richtlinie auf dem Gerät fortfahren, wie im Bild gezeigt:

- **Rate Limit (Übertragungsratenlimit**): Legt die Übertragungsratenbeschränkung für nicht erreichbare Nachrichten fest, die zwischen 1 und 100 Nachrichten pro Sekunde liegt. Der Standardwert ist 1 Nachricht pro Sekunde.

- **Burst Size (Burstgröße**): Legt die Burstrate zwischen 1 und 10 fest. Dieser Wert wird derzeit nicht vom System verwendet.



Vorsicht: Stellen Sie sicher, dass **ICMP-Ziele nicht erreichbar (Typ 3) und ICMP-Zeit überschritten (Typ 11)** in der ACL-Richtlinie von außen nach innen oder in der Vorfilterrichtlinie von FastPath zugelassen sind.

Überprüfung

Überprüfen Sie die Konfiguration von FTD CLI, sobald die Richtlinienbereitstellung abgeschlossen ist:

```
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#
```

Fehlerbehebung

Sie können Aufnahmen von FTD-Eingangs- und -Ausgangsschnittstellen für den interessanten Datenverkehr erstellen, um das Problem weiter zu beheben.

Die Paketerfassung auf Lina kann während der Traceroute für jede Hoffnung auf der Route so lange angezeigt werden, bis die Ziel-IP-Adresse erreicht ist.

```
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
```

Eine detailliertere Ausgabe kann über die Lina CLI bereitgestellt werden, wenn Sie die Traceroute mit den aufgeführten "-I"- und "-n"-Schaltern durchführen.

```
[ 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.
```

Tipp: Cisco Bug-ID CSCvq79913. ICMP-Fehlerpakete werden für Null pdts_info verworfen. Stellen Sie sicher, dass Sie den Vorfilter für ICMP verwenden, vorzugsweise für den Rückverkehr vom Typ 3 und 11.

Zugehörige Informationen

Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.