Consenti tracciamento routing tramite Firepower Threat Defense (FTD)

Sommario

Introduzione

Questo documento descrive la configurazione per consentire il traceroute tramite Firepower Threat Defense (FTD) tramite i criteri del servizio minacce.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Questo articolo è applicabile a tutte le piattaforme Firepower.
- Cisco Firepower Threat Defense con software versione 6.4.0.
- Cisco Firepower Management Center Virtual con software versione 6.4.0.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il comando traceroute permette di determinare il percorso dei pacchetti verso la destinazione. Il comando traceroute invia pacchetti UDP (Unified Data Platform) a una destinazione su una porta non valida. Poiché la porta non è valida, i router diretti alla destinazione rispondono con un messaggio ICMP (Internet Control Message Protocol) "Time Exceeded" (Tempo scaduto) e segnalano l'errore all'appliance ASA (Adaptive Security Appliance).

Il comando traceroute visualizza il risultato di ciascuna sonda inviata. Ogni riga di output corrisponde a un valore TTL (Time to Live) in ordine crescente. In questa tabella vengono descritti i simboli di output.

Simbolo di output	Descrizione
*	Nessuna risposta ricevuta per la sonda entro il periodo di timeout.
nn msec	Per ogni nodo, il tempo di andata e ritorno (in millisecondi) per il numero specificato di richieste.
!N	Rete ICMP irraggiungibile.
!H	Host ICMP non raggiungibile.
!P	ICMP non raggiungibile.
!A	ICMP non consentito a livello amministrativo.
?	Errore ICMP sconosciuto.

Per impostazione predefinita, l'ASA non viene visualizzata sui percorsi di traccia come hop. Per visualizzarla, è necessario diminuire il tempo di trasmissione sui pacchetti che passano attraverso l'ASA e aumentare il limite di velocità sui messaggi ICMP "destinazione irraggiungibile".

⚠ Attenzione: se si riduce il tempo di durata, i pacchetti con un valore TTL pari a 1 vengono scartati, ma viene aperta una connessione per la sessione sul presupposto che la connessione possa contenere pacchetti con un valore TTL superiore. Si noti che alcuni pacchetti, ad esempio i pacchetti hello OSPF, vengono inviati con TTL = 1, quindi la riduzione del tempo di durata può avere conseguenze impreviste. Quando si definisce la

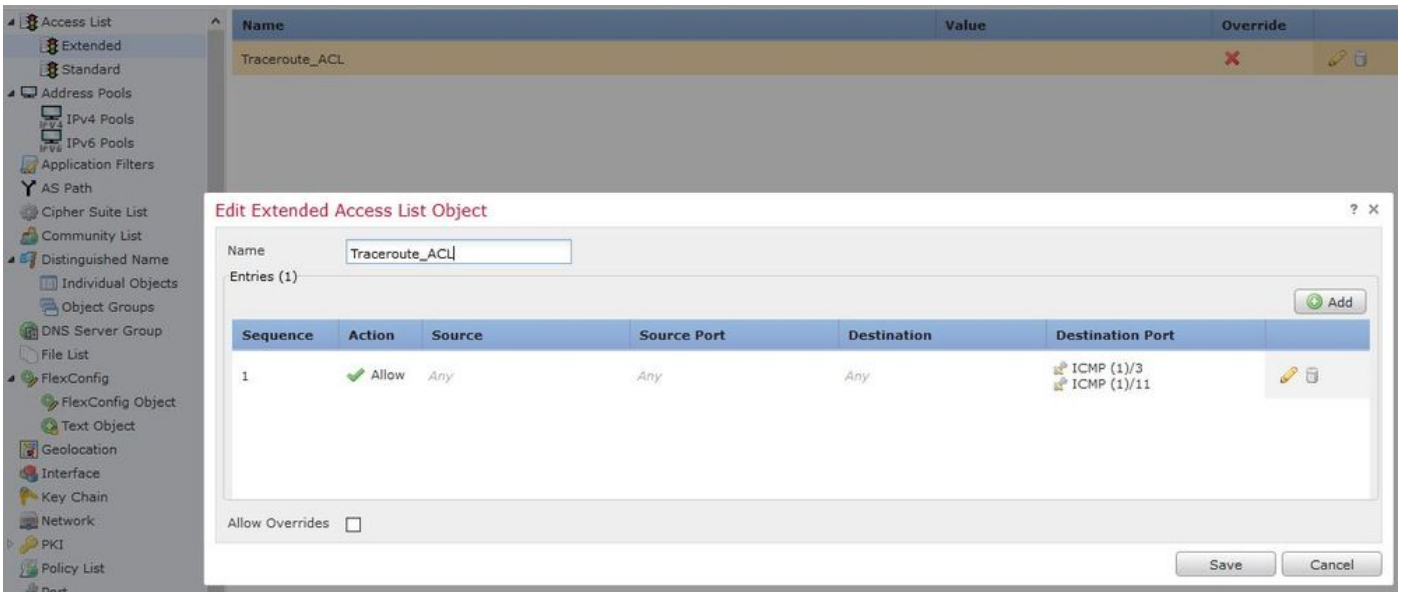
---

⚠ classe del traffico, tenere presenti queste considerazioni.

Configurazione

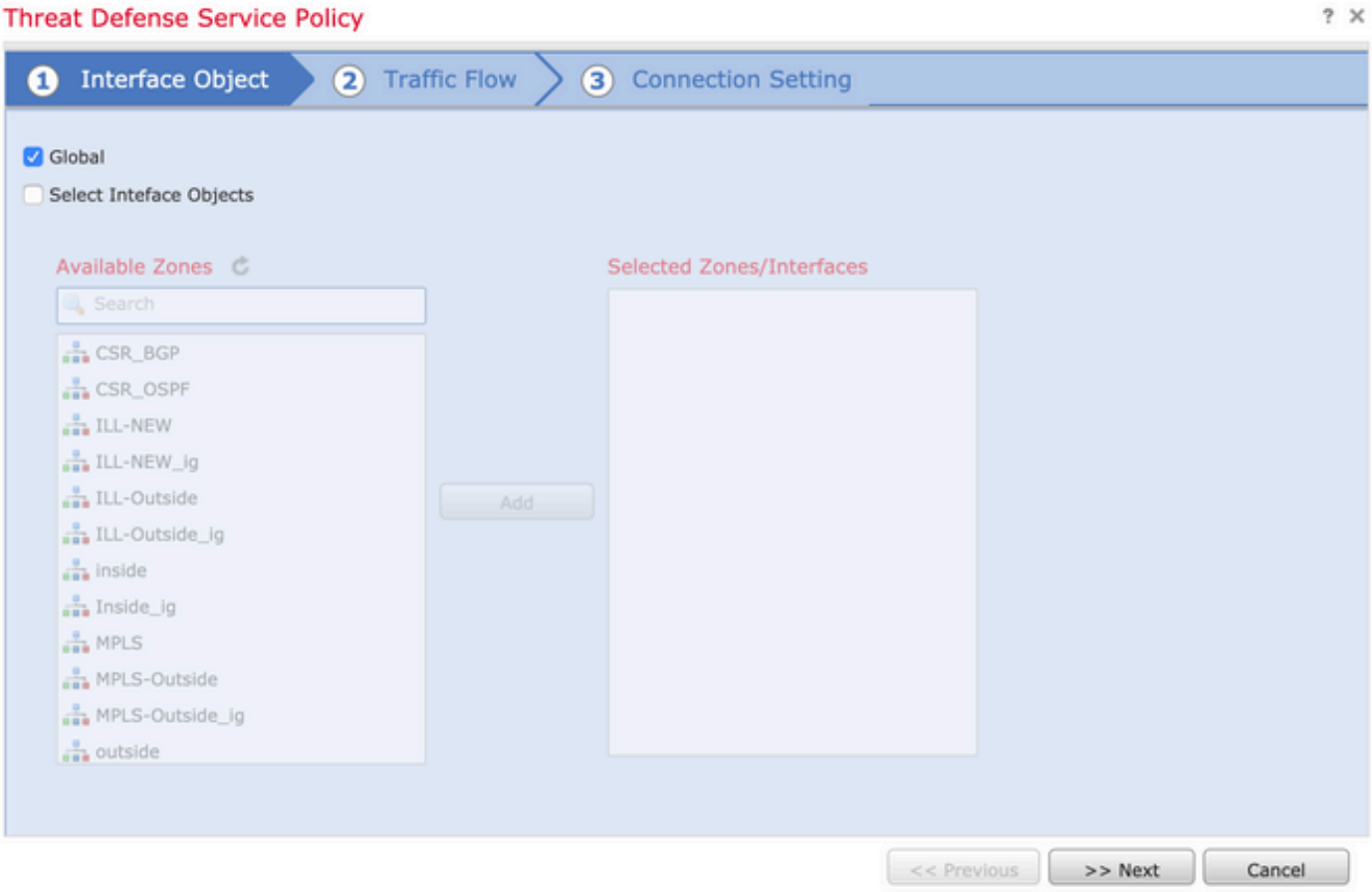
Passaggio 1. Creare l'ACL esteso che definisce la classe di traffico per cui deve essere abilitata la segnalazione di traceroute.

Accedere alla GUI di FMC e selezionare Oggetti > Gestione oggetti > Elenco accessi. Selezionare Extended (Esteso) dal sommario e Aggiungere un nuovo elenco degli accessi esteso.Immettere un nome per l'oggetto, ad esempio, in Traceroute_ACL,Aggiungere una regola per consentire il tipo ICMP 3 e 11 e salvarla, come mostrato nell'immagine:

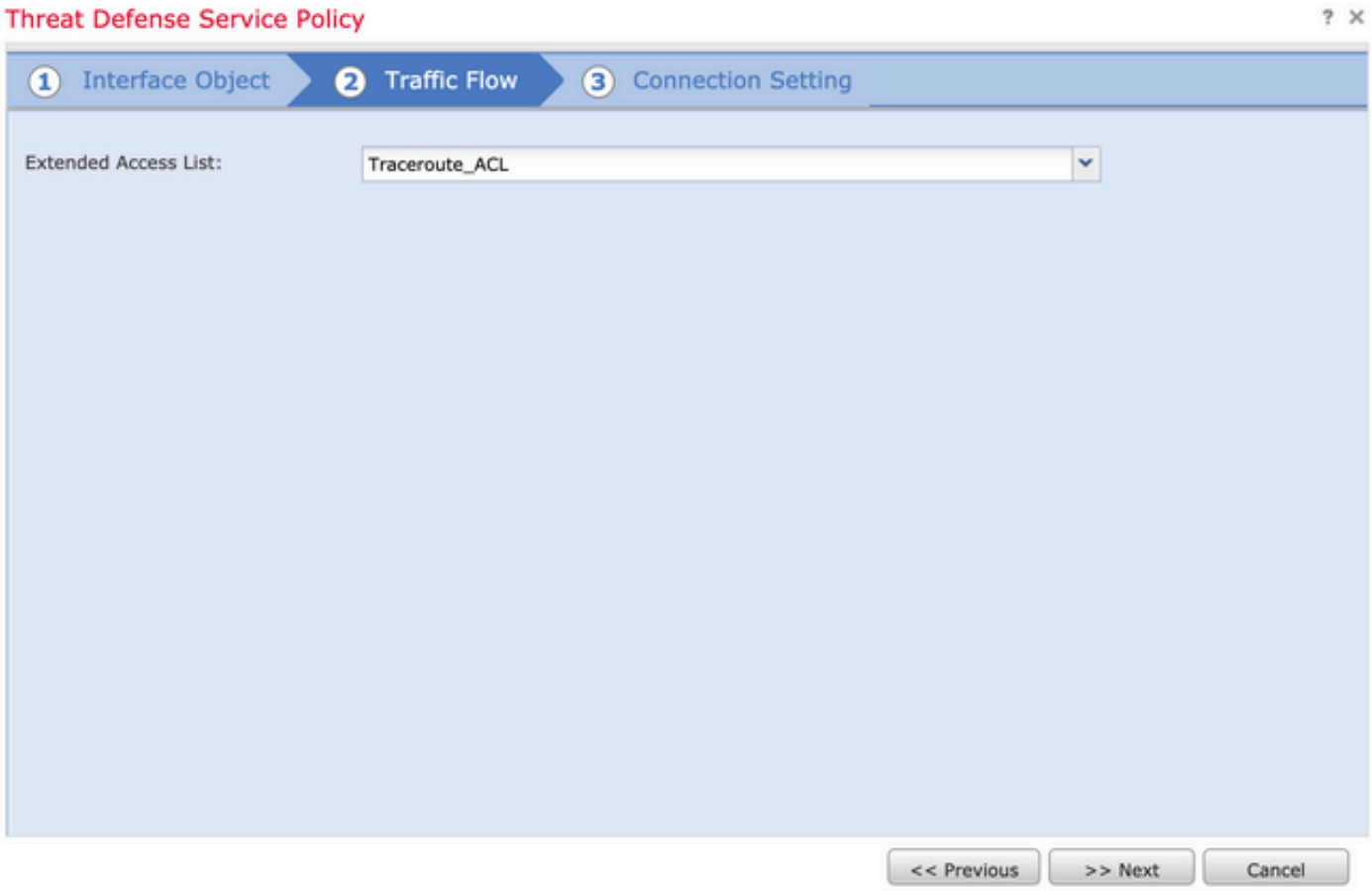


Passaggio 2. Configurare la regola dei criteri del servizio che decrementa il valore di durata.

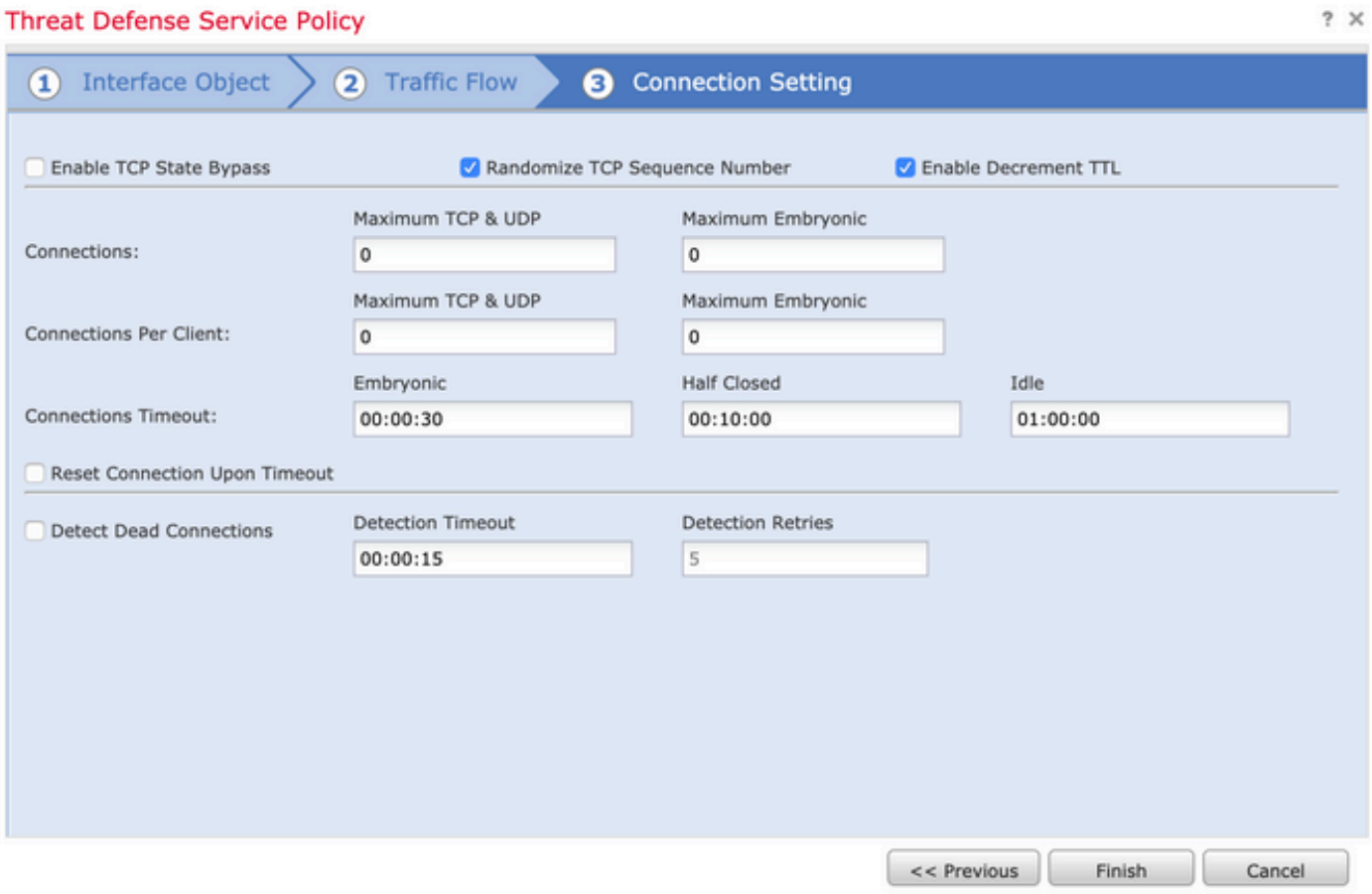
Passare a Criteri > Controllo di accesso e quindi Modificare i criteri assegnati al dispositivo. Nella scheda Avanzate modificare i criteri del servizio di difesa delle minacce e quindi aggiungere una nuova regola dalla scheda Aggiungi regola, selezionare la casella di controllo Globale per applicarla globalmente e fare clic su Avanti, come mostrato nell'immagine:



Passare a Flusso di traffico > Elenco accessi esteso e quindi scegliere Oggetto elenco accessi esteso dal menu a discesa creato nei passaggi precedenti. Fare clic su Next (Avanti), come mostrato nell'immagine:



Selezionate la casella di controllo Attiva TTL decremento (Enable Decrement TTL) e modificate le altre opzioni di connessione (Facoltativo). A questo punto, fare clic su Fine per aggiungere la regola, quindi su OK e salvare le modifiche apportate al criterio del servizio di difesa delle minacce, come mostrato nell'immagine:

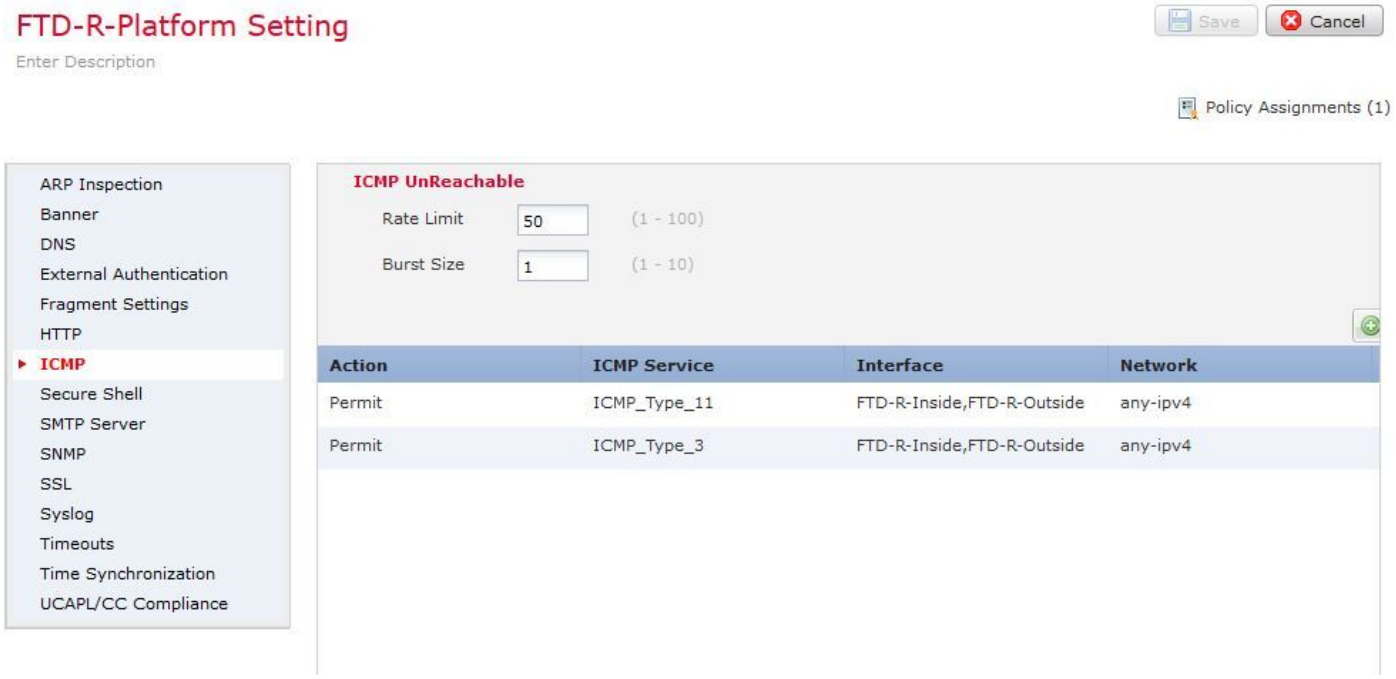


Una volta completati i passaggi precedenti, salvare i criteri di controllo di accesso.

Passaggio 3. Consentire l'uso di ICMP su interni ed esterni e non creare il limite di velocità a 50 (facoltativo).

Passare a Dispositivi > Impostazioni piattaforma, quindi Modificare o Creare un nuovo criterio di impostazioni della piattaforma Firepower Threat Defense e associarlo al dispositivo. Selezionare ICMP dal sommario e aumentare il limite di velocità. Ad esempio, su 50 (è possibile ignorare la dimensione della frammentazione), quindi fare clic su Salva e procedere alla distribuzione del criterio sul dispositivo, come mostrato nell'immagine:

- Limite di velocità—Imposta il limite di velocità per i messaggi non raggiungibili, compreso tra 1 e 100 messaggi al secondo. Il valore predefinito è 1 messaggio al secondo.
- Dimensione burst (Burst Size) - Imposta la velocità di burst su un valore compreso tra 1 e 10. Valore attualmente non utilizzato dal sistema.



⚠ Attenzione: verificare che la destinazione ICMP non sia raggiungibile (tipo 3) e che il tempo ICMP scaduto (tipo 1) sia consentito dall'esterno all'interno nei criteri ACL o nel criterio Fastpath's in Pre-filter.

Verifica

Controllare la configurazione dalla CLI FTD al termine della distribuzione dei criteri:

```
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#
```

Risoluzione dei problemi

È possibile acquisire le immagini sulle interfacce FTD in entrata e in uscita per il traffico interessato, al fine di risolvere ulteriormente il problema.

L'acquisizione del pacchetto su Lina, durante il processo di traceroute, può essere usata per ciascuna speranza sul percorso fino a che non raggiunge l'IP di destinazione.

```
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
```

Per ottenere un output più dettagliato sulla CLI di Lina, è possibile eseguire il traceroute con gli switch "-I" e "-n" elencati.

```
[ 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.
```

Suggerimento: ID bug Cisco CSCvq79913. I pacchetti di errore ICMP vengono scartati per pdts_info Null. Accertarsi di usare il prefiltro per il protocollo ICMP, preferibilmente per il traffico di ritorno di tipo 3 e 11.

Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).