# Risoluzione dei problemi di traffico sulla CLI di CSF

## Sommario



## Introduzione

In questo documento viene descritto come usare Cisco Secure Firewall CLI per risolvere i problemi di traffico convalidando il routing, il flusso di pacchetti e il comportamento degli script.

## Prerequisiti

Nessun requisito specifico previsto per questo documento.

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Criteri e configurazione degli oggetti di Firepower Management Center (FMC)
- Routing Cisco Secure Firewall (CSF) e logica di interfaccia

- Concetti relativi all'ispezione dei pacchetti e alla risoluzione dei problemi del firewall

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware per CSF. Il dispositivo utilizzato nel documento esegue il codice 7.6.5.

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.

### Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Centro gestione firewall protetto (FMC)
- Cisco Secure Firewall (CSF)
- Strumenti CLI Firepower Threat Defense

### Informazioni importanti

Quando un dispositivo utilizza CPU, memoria o I/O in modo elevato, l'esecuzione dei comandi di risoluzione dei problemi può peggiorare il peggioramento delle prestazioni. È consigliabile analizzare e risolvere prima la condizione di esaurimento delle risorse, quindi procedere con la diagnosi dei problemi di traffico. I comandi di diagnostica utilizzano ulteriori risorse di sistema, che possono ridurre ulteriormente la disponibilità e prolungare i tempi di ripristino.

## Premesse

La risoluzione dei problemi di traffico su CSF spesso inizia con la conferma del percorso logico che un pacchetto deve passare attraverso il firewall. Dopo aver compreso il mapping di route e interfaccia, il passaggio successivo consiste nel confrontare il percorso previsto con il flusso di pacchetto effettivo. Questa operazione può essere eseguita utilizzando ricerche di route, simulazione packet-tracer, acquisizioni di pacchetti e traccia del motore Snort.

Ogni strumento offre un livello di visibilità diverso:

- show route conferma il percorso di routing del pacchetto e l'identità dell'interfaccia.
- packet-tracer simula il flusso del traffico e identifica le decisioni di ACL, NAT e interfaccia.
- il pacchetto acquisisce il traffico inspect live che attraversa il firewall.
- la traccia di supporto del sistema espone il processo decisionale Snort per blocchi correlati a policy o eventi di ispezione.

---

Suggerimento: Prima di acquisire il traffico, iniziare con la convalida del routing e del tracer dei pacchetti per verificare se le decisioni sul percorso e sul controllo dell'accesso previste sono corrette prima di analizzare il traffico in tempo reale.

---

## Problema

Un flusso di traffico non funziona nel modo previsto e l'amministratore deve determinare se il pacchetto sta seguendo il percorso corretto, se il firewall consente o nega la connessione e se il traffico è bloccato dall'intercettazione o dal controllo delle policy.

## Passaggio 1: Trova il percorso

Identificare il percorso di routing e determinare i nomi delle interfacce logiche associate agli indirizzi IP di origine e di destinazione. I nomi delle interfacce logiche sono richiesti dalla maggior parte dei comandi di risoluzione dei problemi, pertanto questo deve essere il primo passaggio del flusso di lavoro di risoluzione dei problemi.

Eseguire il comando per l'indirizzo IP di origine e di destinazione:

```
show route <IP>
```

Il traffico destinato a Internet che si basa sul percorso predefinito richiede l'identificazione dell'interfaccia di uscita logica. È possibile determinare il nome dell'interfaccia logica eseguendo questo passaggio:

```
show route 0.0.0.0
```

Output di esempio:

```
FTD1# show route 192.168.0.11


Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

---

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

In questo esempio, l'interfaccia in entrata logica è Interna (Inside) e l'interfaccia in uscita è Esterna (Outside).

---

Attenzione: Network Address Translation (NAT) può reindirizzare il traffico tramite interfacce diverse da quelle indicate dalla tabella di routing quando i criteri NAT corrispondono al flusso di traffico. Per risolvere i problemi di connettività, verificare che la configurazione NAT sia allineata al percorso del traffico previsto.

---

Suggerimento: I nomi delle interfacce logiche vengono utilizzati nei comandi di risoluzione dei problemi della CLI. Prendere nota del nome logico per riferimento futuro.

---

## Passaggio 2: Esegui Packet-Tracer

Usare packet-tracer per simulare il modo in cui il firewall valuta un flusso del traffico specifico. Questo strumento aiuta a confermare quali interfacce vengono usate, se si applica un criterio NAT e se un ACL permette o nega il traffico.

Utilizzare la seguente sintassi del comando:

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

Comando di esempio:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

Esaminare l'output per verificare che il pacchetto segua il percorso previsto e sia autorizzato durante la simulazione. Questa opzione è utile quando è necessario determinare se il problema è correlato al routing, al NAT o alla corrispondenza alle policy prima di procedere all'analisi dei pacchetti live.

La parola chiave transmission in packet-tracer fa sì che il pacchetto simulato venga iniettato sull'interfaccia in entrata, consentendo di attraversare tutte le fasi di elaborazione del firewall anziché rimanere una simulazione.

Comando di esempio:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

## Passaggio 3: Esegui acquisizioni

Usare le acquisizioni dei pacchetti per ispezionare il traffico in tempo reale mentre attraversa il firewall. Le acquisizioni dei pacchetti sono diverse da quelle del tracer, in quanto acquisiscono il traffico effettivo e devono quindi corrispondere al flusso reale che attraversa il firewall nel momento in cui l'acquisizione è attiva. Le acquisizioni dei pacchetti sono bidirezionali e documentano entrambi i lati della connessione.

Per la maggior parte degli scenari di risoluzione dei problemi di traffico, configurare le seguenti clip:

- Ingress Capture: acquisisce il traffico in arrivo sull'interfaccia sul lato origine
- Esci da acquisizione: acquisisce il traffico in uscita sull'interfaccia di destinazione
- ASP Drop Capture: acquisisce i pacchetti scartati dal firewall e che corrispondono ai criteri configurati

Sintassi generale di acquisizione:

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

Esempio di acquisizione in ingresso:

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

Esempio di acquisizione in uscita:

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

Esempio di drop capture ASP:

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

Le acquisizioni dei pacchetti sono bidirezionali, ossia è possibile acquisire sia il traffico di inoltro che quello di ritorno in base ai criteri di corrispondenza definiti. La funzionalità di traccia consente di visualizzare le decisioni prese dal firewall sul traffico effettivo.

---

⚠ Attenzione: Se si sta eseguendo NAT, l'acquisizione in uscita deve utilizzare l'IP di origine tradotto, non l'IP di origine originale, per acquisire correttamente il traffico post-NAT.

---

## Passaggio 4: Esegui traccia supporto di sistema

Utilizzare la traccia di supporto del sistema per visualizzare il processo di ispezione Snort in tempo reale per un flusso di traffico specifico. Ciò è particolarmente utile quando il traffico soddisfa una regola di autorizzazione ACL ma è ancora bloccato dall'ispezione dei criteri. Le acquisizioni di pacchetti standard mostrano che un pacchetto è stato bloccato, ma la traccia di supporto del sistema permette di capire perché il pacchetto è stato gestito in questo modo. La traccia di supporto del sistema è bidirezionale, ovvero riceve traffico da entrambi i lati. Ciò significa che l'ordine in cui gli IP vengono aggiunti allo strumento non ha importanza.

Eseguire questo comando e rispondere ai prompt:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

Questo strumento è particolarmente utile quando l'ambiente utilizza regole di applicazione o URL, regole basate sull'identità, criteri di file o criteri di intrusione. Queste funzionalità vengono valutate dopo la corrispondenza dell'ACL, quindi un pacchetto può essere autorizzato dai criteri di controllo di accesso ma bloccato dall'ispezione Snort.

---

Nota: La porta del client può essere lasciata vuota se la porta di origine esatta è sconosciuta.

---

## Verifica

Usare l'output della ricerca route, della simulazione packet-tracer, delle acquisizioni pacchetti e della traccia di supporto del sistema insieme per confermare il comportamento del flusso di traffico. L'obiettivo è quello di determinare se il pacchetto sta seguendo il percorso corretto, se il firewall lo permette o lo nega, e se il pacchetto viene bloccato da Snort a seguito di un'ispezione più approfondita.

Un flusso di risoluzione dei problemi completo in genere conferma:

- La ricerca route mostra le interfacce logiche in entrata e in uscita.
- Packet-tracer conferma il percorso di inoltro e la valutazione dei criteri previsti.
- Le acquisizioni dei pacchetti confermano se il traffico sta arrivando e partendo come previsto.
- La traccia di supporto del sistema conferma se il blocco è causato da un'operazione Snort o da un'ispezione dei criteri.

## Risoluzione dei problemi

Se il problema persiste, esaminare le seguenti aree:

- Verificare se la ricerca route corrisponde alle interfacce di origine e di destinazione previste.
- Verificare se l'output del comando packet-tracer visualizza il traffico negato in fase ACL o

NAT.

- Esaminare le acquisizioni dei pacchetti in entrata e in uscita per verificare che il traffico stia raggiungendo il firewall e partendo dall'interfaccia corretta.
- Usare le acquisizioni di rilascio ASP per confermare se il firewall sta interrompendo il traffico internamente.
- Usare la traccia di supporto del sistema per determinare se Snort sta bloccando il traffico dopo la decisione di autorizzazione dell'ACL.

## Informazioni correlate

- Analisi delle acquisizioni di Firepower Firewall per la risoluzione dei problemi di rete
- Uso di Firepower Threat Defense Capture e Packet Tracer

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).