# Configurare l'hairpin con Firepower Management Center

## Sommario



## Introduzione

In questo documento vengono descritti i passaggi necessari per configurare correttamente Hairpin su Firepower Threat Defense (FTD) con Firepower Management Center (FMC).

## 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:

- Firepower Management Center Virtual 7.2.4.1
- Firepower Threat Defense Virtual 7.2.4.1

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.

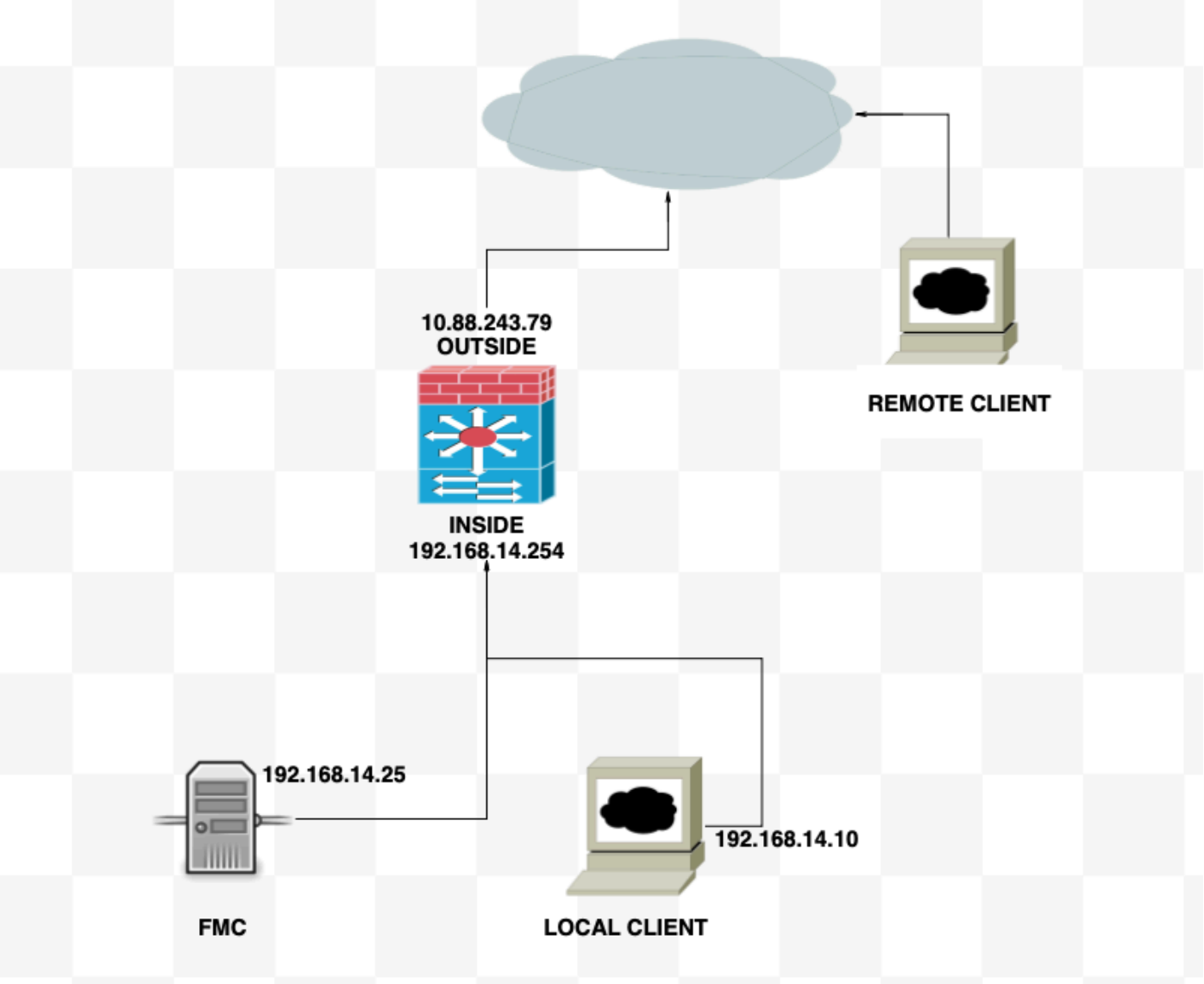
# Configurazione

Il termine hairpin viene utilizzato perché il traffico proveniente dal client raggiunge il router (o il firewall che implementa NAT) e, dopo la traduzione, viene restituito alla rete interna come un hairpin per accedere all'indirizzo IP privato del server.

Questa funzione è utile per i servizi di rete come l'hosting Web all'interno di una rete locale, in cui gli utenti della rete locale devono accedere al server interno utilizzando lo stesso URL o indirizzo IP utilizzato dagli utenti esterni. Garantisce un accesso uniforme alle risorse indipendentemente dal fatto che la richiesta provenga dall'interno o dall'esterno della rete locale.

Nell'esempio, è necessario accedere a un CCP tramite l'indirizzo IP dell'interfaccia esterna dell'FTD

## Diagramma

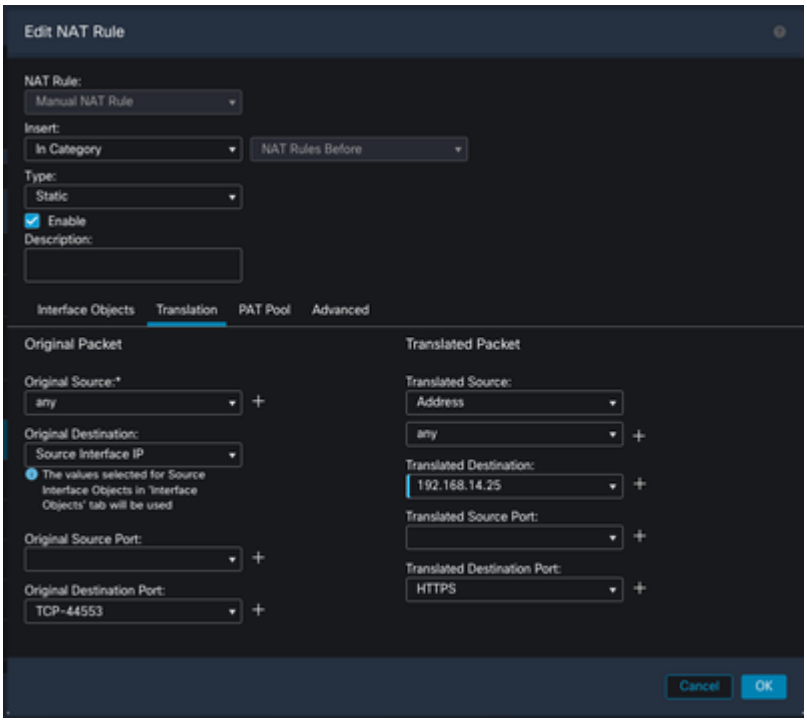



## Passaggio 1. Configurare Il Nat Esterno-Interno

Come primo passo, occorre configurare un NAT statico; nell'esempio, l'IP di destinazione e la porta di destinazione vengono convertiti utilizzando l'IP dell'interfaccia esterna e la destinazione della porta è 44553.

Dal FMC passare a Periferica > NAT per creare o modificare la policy esistente, quindi fare clic sulla casella Aggiungi regola.

- Regola NAT: Regola Nat Manuale
- Origine: Qualsiasi
- Destinazione originale: Source Interface IP
- Porta di destinazione originale: 44553
- Destinazione tradotta: 192.168.14.25
- Porta di destinazione tradotta: 443




Configurare il criterio. Passare a Criteri > Controllo di accesso per creare o modificare il criterio esistente, quindi fare clic sulla casella Aggiungi regola.

Zona di origine: Esterno

Zona di destinazione: Interno

Rete di origine: Qualsiasi

Rete di destinazione: 10.88.243.79

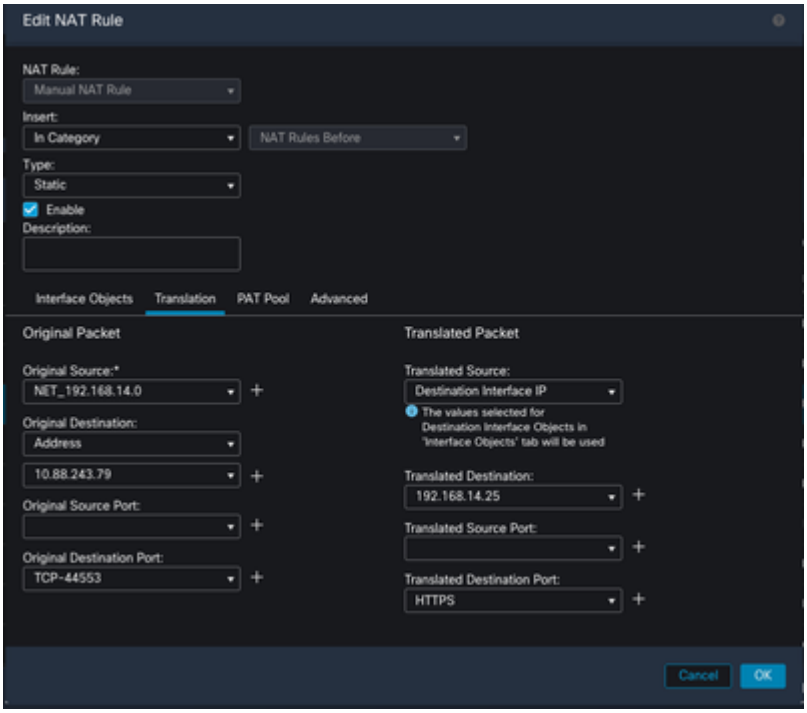

## Passaggio 2. Configurare Il Nat Interno (Hairpin)

Come secondo passo, un NAT statico deve essere configurato dall'interno all'interno; nell'esempio, l'IP di destinazione e la porta di destinazione vengono convertiti utilizzando un oggetto con l'IP dell'interfaccia esterna e la porta di destinazione è 44553.

Dal FMC passare a Periferica > NAT per modificare la policy esistente, quindi fare clic sulla casella Aggiungi regola.

- Regola NAT: Regola Nat Manuale

- Origine: 192.168.14.0/24
- Destinazione originale: Indirizzo 10.88.243.79
- Porta di destinazione originale: 44553
- Origine tradotta: IP interfaccia di destinazione
- Destinazione tradotta: 192.168.14.25
- Porta di destinazione tradotta: 443




Configurare il criterio. Passare a Criteri > Controllo d'accesso per modificare il criterio esistente, quindi fare clic sulla casella Aggiungi regola.

Zona di origine: Qualsiasi

Zona di destinazione: Qualsiasi

Rete di origine: 192.168.14.0/24

Rete di destinazione: 10.88.243.79

| # | Name | Source Zones | Dest Zones | Source Networks | Dest Networks |
|---|---|---|---|---|---|
| Mandatory - la primera (1-4) | | | | | |
| 1 | nat-fmc | OUTSIDE | INSIDE | any | Any |
| 2 | Hairpin | Any | Any | NET_192.168.14 | 10.88.243.79 |

## Verifica

Dal client locale, eseguire una connessione telnet con l'IP di destinazione e la porta di destinazione:

Se viene visualizzato il messaggio di errore "telnet cannot connect to remote host: "Connessione scaduta". Si è verificato un errore durante la configurazione.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

Se invece il messaggio è Connesso, la configurazione è riuscita.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

# Risoluzione dei problemi

In caso di problemi con Network Address Translation (NAT), utilizzare questa guida dettagliata per la risoluzione dei problemi più comuni.

## Passaggio 1: Controllo configurazione regole NAT

- Verifica regole NAT: Verificare che tutte le regole NAT siano configurate correttamente in FMC. Verificare che gli indirizzi IP di origine e di destinazione e le porte siano corretti.
- Assegnazione interfaccia: Confermare che le interfacce di origine e di destinazione siano assegnate correttamente nella regola NAT. Un mapping non corretto può causare la conversione o il routing non corretto del traffico.
- Priorità regola NAT: Verificare che la regola NAT sia posizionata all'inizio di qualsiasi altra regola che può corrispondere allo stesso traffico. Le regole in FMC vengono elaborate in ordine sequenziale, pertanto una regola posizionata più in alto ha la precedenza.

## Passaggio 2: Verifica delle regole di controllo di accesso (ACL)

- Revisione degli ACL: Controllare gli Access Control List per assicurarsi che siano appropriati per autorizzare il traffico NAT. Gli ACL devono essere configurati in modo da riconoscere gli indirizzi IP tradotti.
- Ordine regole: Verificare che l'elenco di controllo di accesso sia nell'ordine corretto. Come le regole NAT, gli ACL vengono elaborati dall'alto verso il basso e la prima regola che corrisponde al traffico è quella applicata.
- Autorizzazioni traffico: Verificare che esista un elenco di controllo di accesso appropriato per consentire il traffico dalla rete interna alla destinazione tradotta. Se una regola non è presente o non è configurata correttamente, il traffico desiderato potrebbe essere bloccato.

## Passaggio 3: Diagnostica aggiuntiva

- Utilizzare gli strumenti diagnostici: Utilizzare gli strumenti di diagnostica disponibili in FMC per monitorare ed eseguire il debug del traffico che attraversa il dispositivo. Ciò

include la visualizzazione in tempo reale dei registri e degli eventi di connessione.

- Riavvia connessioni: In alcuni casi, le connessioni esistenti non possono riconoscere le modifiche apportate alle regole NAT o agli ACL finché non vengono riavviate. Valutare l'opportunità di cancellare le connessioni esistenti per forzare l'applicazione di nuove regole.

Da LINA:

```
<#root>

firepower#

 clear xlate
```

- Verifica traduzione: Usare comandi come show xlate e show nat sulla riga di comando se si lavora con dispositivi FTD per verificare che le conversioni NAT vengano eseguite come previsto.

Da LINA:

```
<#root>

firepower#

 show nat
```

```
<#root>

firepower#

 show xlate
```

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).