Configurazione della hairpin sull'appliance ASA

Sommario

Introduzione

In questo documento viene descritto come configurare correttamente Hairpin su una appliance Cisco Adaptive Security (ASA)

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione NAT sull'appliance ASA
- Configurazione ACL su ASA

Componenti usati

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

- Software Cisco Adaptive Security Appliance versione 9.18(4)2

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

La tecnologia NAT (Hairpin Network Address Translation), nota anche come loopback NAT o riflessione NAT, è una tecnica utilizzata nel routing di rete tramite la quale un dispositivo in una rete privata può accedere a un altro dispositivo nella stessa rete privata tramite un indirizzo IP pubblico.

Questa opzione viene utilizzata quando un server è ospitato dietro un router e si desidera consentire ai dispositivi della stessa rete locale del server di accedervi utilizzando l'indirizzo IP pubblico (quello assegnato al router dal provider di servizi Internet) come farebbe una periferica esterna.

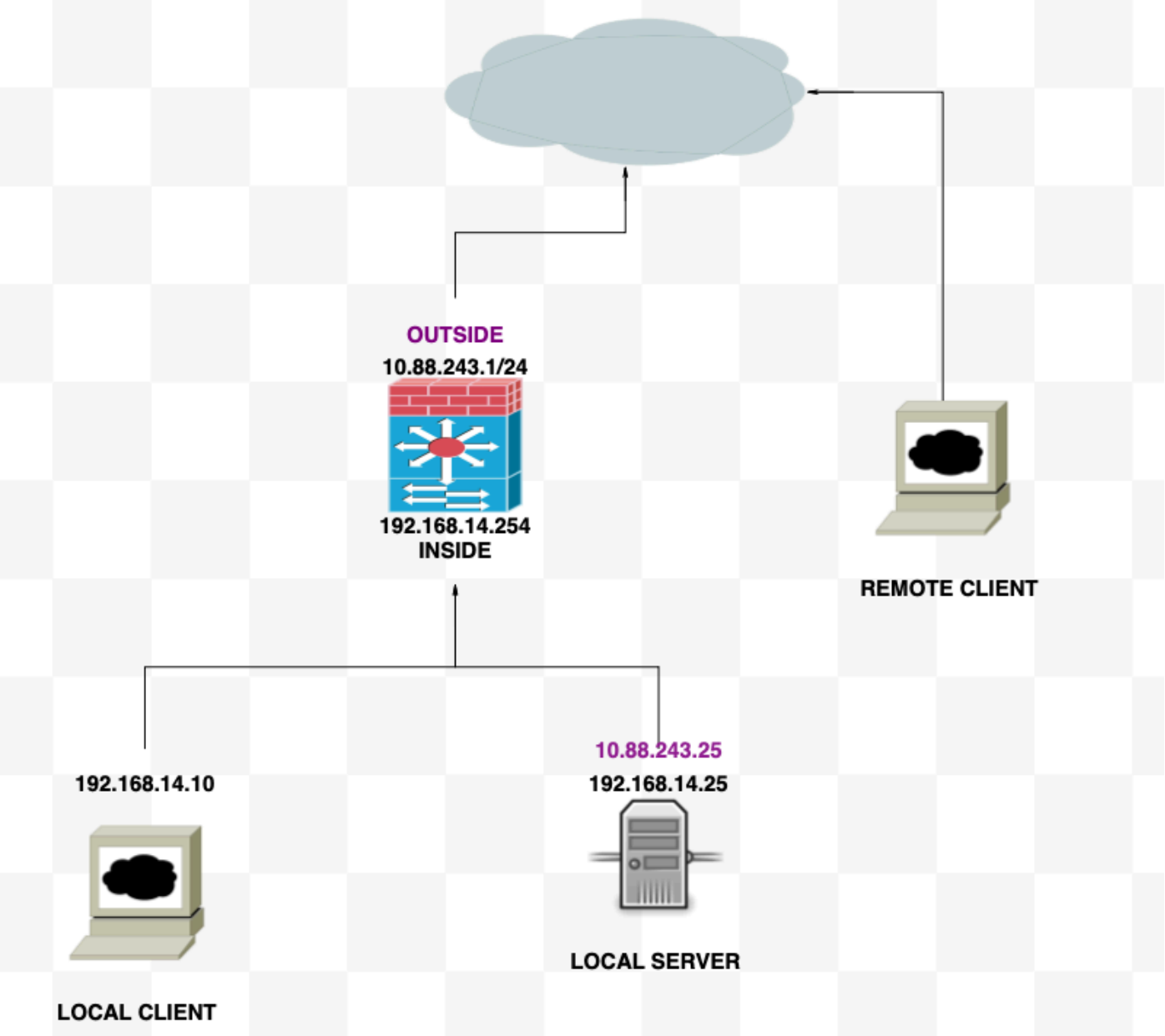
Il termine "hairpin" viene utilizzato perché il traffico proveniente dal client raggiunge il router (o il firewall che implementa NAT) e, dopo la traduzione, viene "girato indietro" come una hairpin alla rete interna per accedere all'indirizzo IP privato del server.

Si supponga, ad esempio, di disporre di un server Web nella rete locale con un indirizzo IP privato. Si desidera accedere a questo server utilizzando il relativo indirizzo IP pubblico o un nome di dominio che viene risolto nell'indirizzo IP pubblico, anche quando ci si trova nella stessa rete locale.

Senza Hairpin NAT, il router non è in grado di comprendere questa richiesta perché prevede che le richieste dell'indirizzo IP pubblico provengano dall'esterno della rete.

Hairpin NAT risolve questo problema consentendo al router di riconoscere che, sebbene la richiesta venga effettuata a un IP pubblico, deve essere instradata a un dispositivo sulla rete locale.

Esempio di rete



Configurazioni

Passaggio 1. Creazione degli oggetti

- Rete interna:192.168.14.10
- Server Web: 192.168.14.25
- Server Web pubblico: 10.88.243.25
- Porta: 80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

Passaggio 2. Creare il NAT

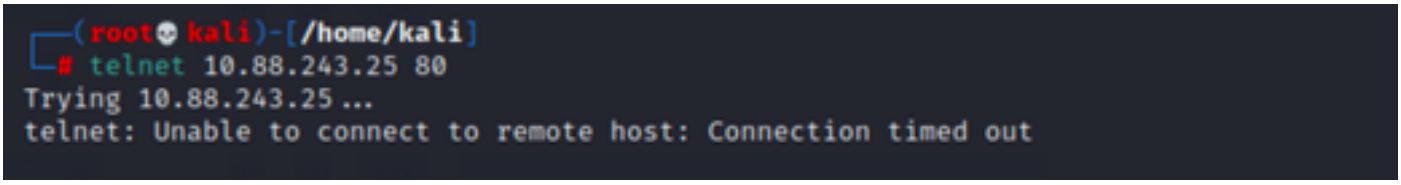
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

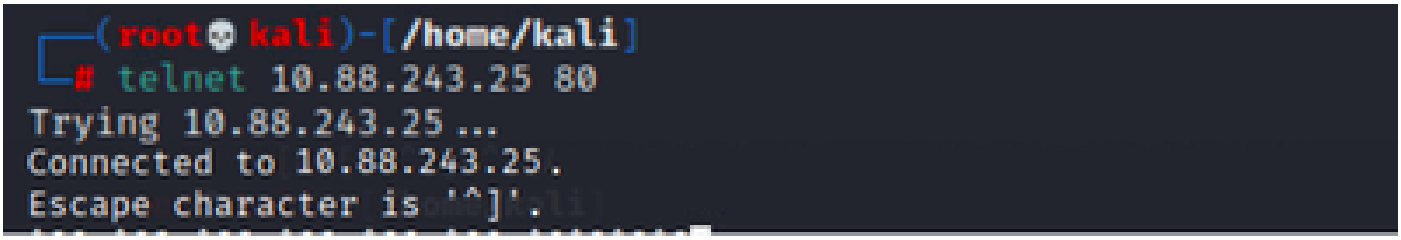
Verifica

Dal client locale eseguire un IP di destinazione telnet con una porta di destinazione:

Se il messaggio "telnet unable to connect to remote host: Connection timed out" (telnet non riesce a connettersi all'host remoto: connessione scaduta) viene visualizzato, si è verificato un errore durante la configurazione.



Ma se dice "Connesso", funziona!



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 della configurazione delle regole NAT

- Esamina regole NAT: verifica che tutte le regole NAT siano configurate correttamente. Verificare che gli indirizzi IP di origine e di destinazione e le porte siano corretti.
- Assegnazione interfaccia: verificare che entrambe 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 alla regola NAT sia assegnata una priorità più alta di qualsiasi altra regola che potrebbe corrispondere allo stesso traffico. Le regole 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 Lists per verificare che siano appropriati per autorizzare il traffico NAT. Gli ACL devono essere configurati in modo da riconoscere gli indirizzi IP tradotti.
- Ordine delle 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 di diagnostica: utilizzare gli strumenti di diagnostica disponibili 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 riconoscono 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.

<#root>

```
ciscoasa(config)#
 clear xlate
```

- Verifica della traduzione: utilizzare comandi quali `show xlate` e `show nat` sulla riga di comando se si utilizzano dispositivi ASA per verificare che le traduzioni NAT vengano eseguite come previsto.

<#root>

ciscoasa(config)#

show xlate

<#root>

ciscoasa(config)#

show nat

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).