Risoluzione dei problemi di configurazione di ASA Network Address Translation (NAT)

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Risoluzione dei problemi di configurazione NAT sull'appliance ASA
- Modalità di utilizzo della configurazione ASA per compilare la tabella dei criteri NAT
- Come risolvere i problemi NAT
  - Uso dell'utility Packet Tracer
  - Visualizza l'output del comando Show Nat
  - Metodologia di risoluzione dei problemi NAT
- Problemi comuni delle configurazioni NAT
  - Problema: il traffico non riesce a causa di un errore RPF (NAT Reverse Path Failure). Errore: regole NAT asimmetriche corrispondenti per i flussi in avanti e all'indietro
  - Problema: le regole NAT manuali non sono ordinate, il che provoca corrispondenze errate ai pacchetti
  - Problema
  - Problema
  - Problema: in seguito a una regola NAT, l'ASA passa al protocollo ARP (Proxy Address Resolution Protocol) per il traffico sull'interfaccia mappata

Introduzione

In questo documento viene descritto come risolvere i problemi di configurazione di Network Address Translation (NAT) sulla piattaforma Cisco Adaptive Security Appliance (ASA).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

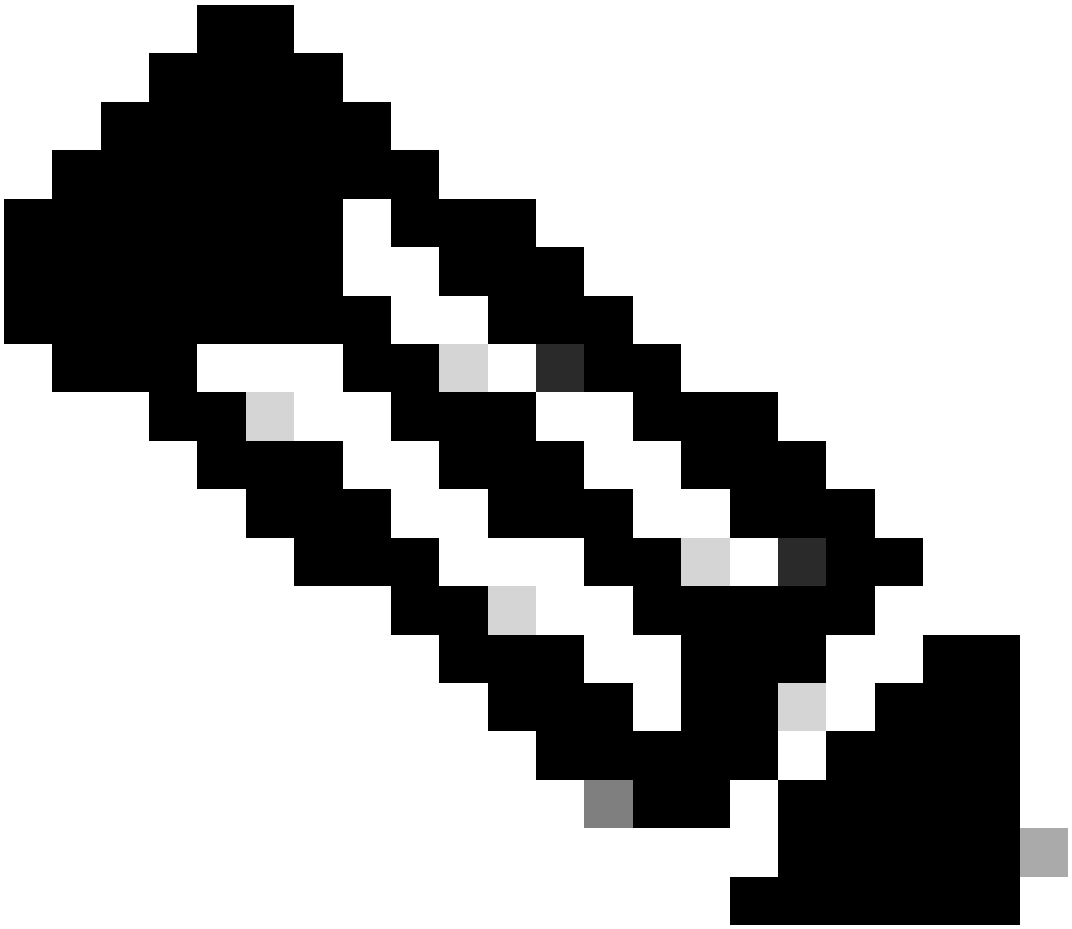
Componenti usati

Il riferimento delle informazioni contenute in questo documento è ASA versione 8.3 e successive.

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.

Risoluzione dei problemi di configurazione NAT sull'appliance ASA



> Nota: per alcuni esempi base di configurazioni NAT, che includono un video che mostra una configurazione NAT di base, vedere la sezione Informazioni correlate in fondo a questo documento.

Quando si risolvono i problemi relativi alle configurazioni NAT, è importante capire come la configurazione NAT sull'appliance ASA viene utilizzata per compilare la tabella dei criteri NAT.

Questi errori di configurazione costituiscono la maggior parte dei problemi NAT incontrati dagli amministratori ASA:

- Le regole di configurazione NAT non sono funzionanti. Ad esempio, una regola NAT manuale viene posizionata nella parte superiore della tabella NAT, in modo che le regole più

specifiche posizionate più in basso nella tabella NAT non vengano mai trovate.
- Gli oggetti di rete utilizzati nella configurazione NAT sono troppo ampi, il traffico corrisponde inavvertitamente a queste regole NAT, e mancano regole NAT più specifiche.

L'utilità packet tracer può essere usata per diagnosticare la maggior parte dei problemi NAT sull'appliance ASA. Vedere la sezione successiva per ulteriori informazioni su come la configurazione NAT viene utilizzata per creare la tabella dei criteri NAT e su come risolvere e risolvere problemi NAT specifici.

Inoltre, è possibile usare il comando show nat detail per capire quali regole NAT vengono interessate dalle nuove connessioni.

Modalità di utilizzo della configurazione ASA per compilare la tabella dei criteri NAT

Tutti i pacchetti elaborati dall'ASA vengono valutati sulla base della tabella NAT. Questa valutazione inizia in alto (Sezione 1) e funziona fino a quando non viene trovata una corrispondenza con una regola NAT.

In generale, una volta trovata una corrispondenza con una regola NAT, questa regola NAT viene applicata alla connessione e non vengono più controllati i criteri NAT in base al pacchetto, ma vengono illustrate alcune avvertenze.

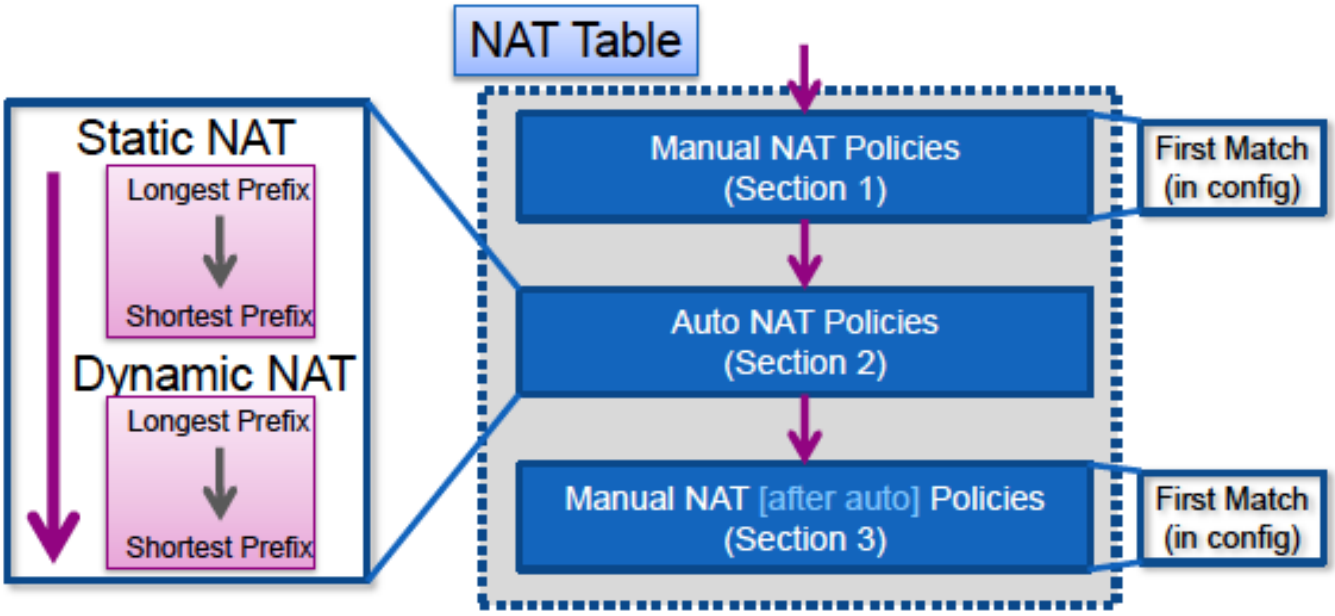
Tabella dei criteri NAT

La policy NAT sull'appliance ASA è costruita dalla configurazione NAT.

Le tre sezioni della tabella ASA NAT sono:

Sezione 1	Criteri NAT manuali Questi vengono elaborati nell'ordine in cui appaiono nella configurazione.
Sezione 2	Criteri NAT automatici Questi vengono elaborati in base al tipo NAT (statico o dinamico) e alla lunghezza del prefisso (subnet mask) nell'oggetto.
Sezione 3	Criteri NAT manuali post-automatici Questi vengono elaborati nell'ordine in cui appaiono nella configurazione.

Il diagramma mostra le diverse sezioni NAT e il loro ordine:



Corrispondenza regola NAT

Sezione 1

- Un flusso viene prima valutato in base alla sezione 1 della tabella NAT che inizia con la prima regola.
  - Se l'IP di origine e di destinazione del pacchetto corrisponde ai parametri della regola NAT manuale, la traduzione viene applicata e il processo si arresta e non vengono valutate ulteriori regole NAT in alcuna sezione.
  - Se non viene trovata una corrispondenza per una regola NAT, il flusso viene valutato rispetto alla sezione 2 della tabella NAT.

Sezione 2

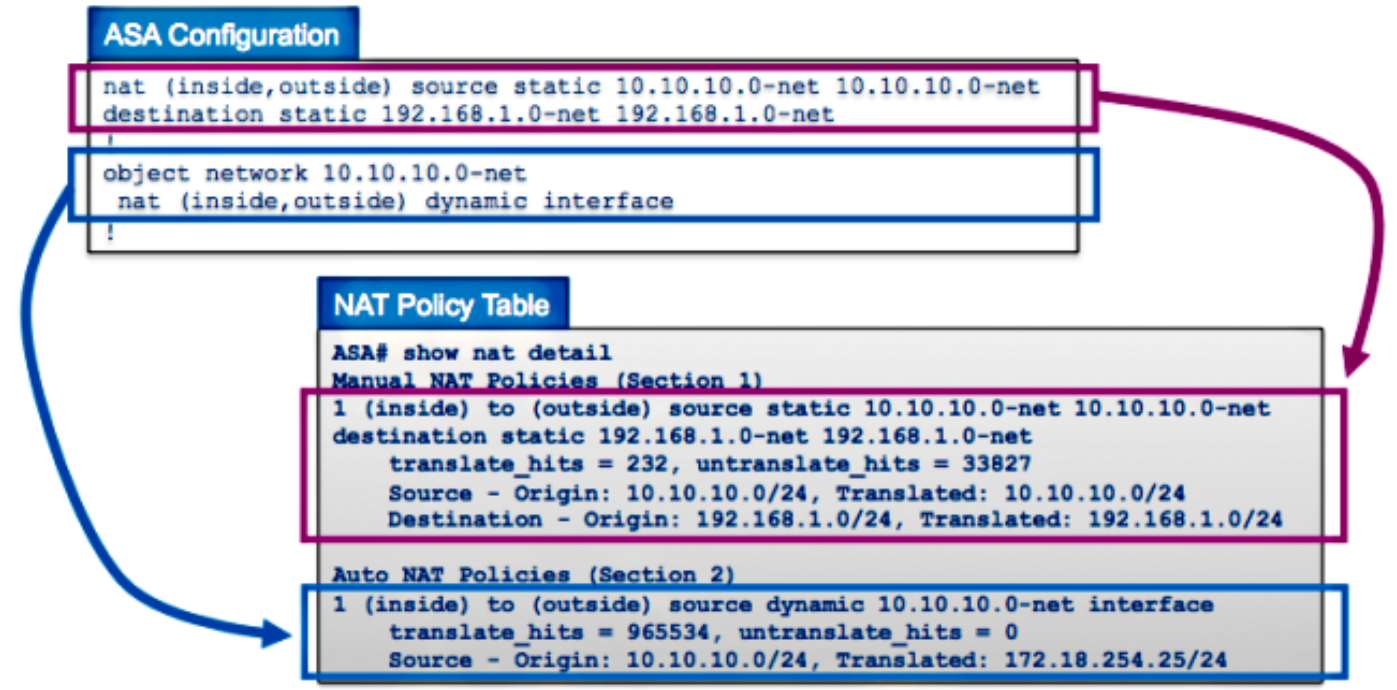
- Un flusso viene valutato in base alle regole NAT della sezione 2 nell'ordine specificato in precedenza, prima le regole NAT statiche, quindi le regole NAT dinamiche.
  - Se una regola di conversione corrisponde all'indirizzo IP di origine o di destinazione del flusso, è possibile applicare la conversione e continuare a valutare le altre regole per verificare se corrispondono all'altro indirizzo IP del flusso. Ad esempio, una regola auto-NAT potrebbe tradurre l'IP di origine, mentre un'altra regola auto-NAT potrebbe tradurre la destinazione.
  - Se il flusso soddisfa una regola NAT automatica, quando viene raggiunta la fine della sezione 2 la ricerca NAT viene interrotta e le regole nella sezione 3 non vengono valutate.
  - Se nessuna regola NAT della sezione 2 viene confrontata con il flusso, la ricerca procede alla sezione 3

Sezione 3

- La procedura di cui alla sezione 3 è essenzialmente la stessa della sezione 1. Se l'IP di origine e di destinazione del pacchetto corrisponde ai parametri della regola NAT manuale,

la traduzione viene applicata e il processo si arresta e non vengono valutate ulteriori regole NAT in alcuna sezione.

Nell'esempio viene mostrato come rappresentare la configurazione ASA NAT con due regole (un'istruzione NAT manuale e una configurazione NAT automatica) nella tabella NAT:



Come risolvere i problemi NAT

Uso dell'utility Packet Tracer

Per risolvere i problemi con le configurazioni NAT, usare l'utilità packet tracer per verificare che un pacchetto raggiunga la policy NAT. Il servizio di traccia dei pacchetti consente di specificare un pacchetto di esempio che entra nell'ASA. L'ASA indica la configurazione applicata al pacchetto e se è consentita o meno.

Nell'esempio successivo, viene fornito un pacchetto TCP di esempio che entra nell'interfaccia interna e è destinato a un host su Internet. L'utilità di traccia dei pacchetti mostra che il pacchetto soddisfa una regola NAT dinamica e viene convertito nell'indirizzo IP esterno di 172.16.123.4:

<#root>

ASA#

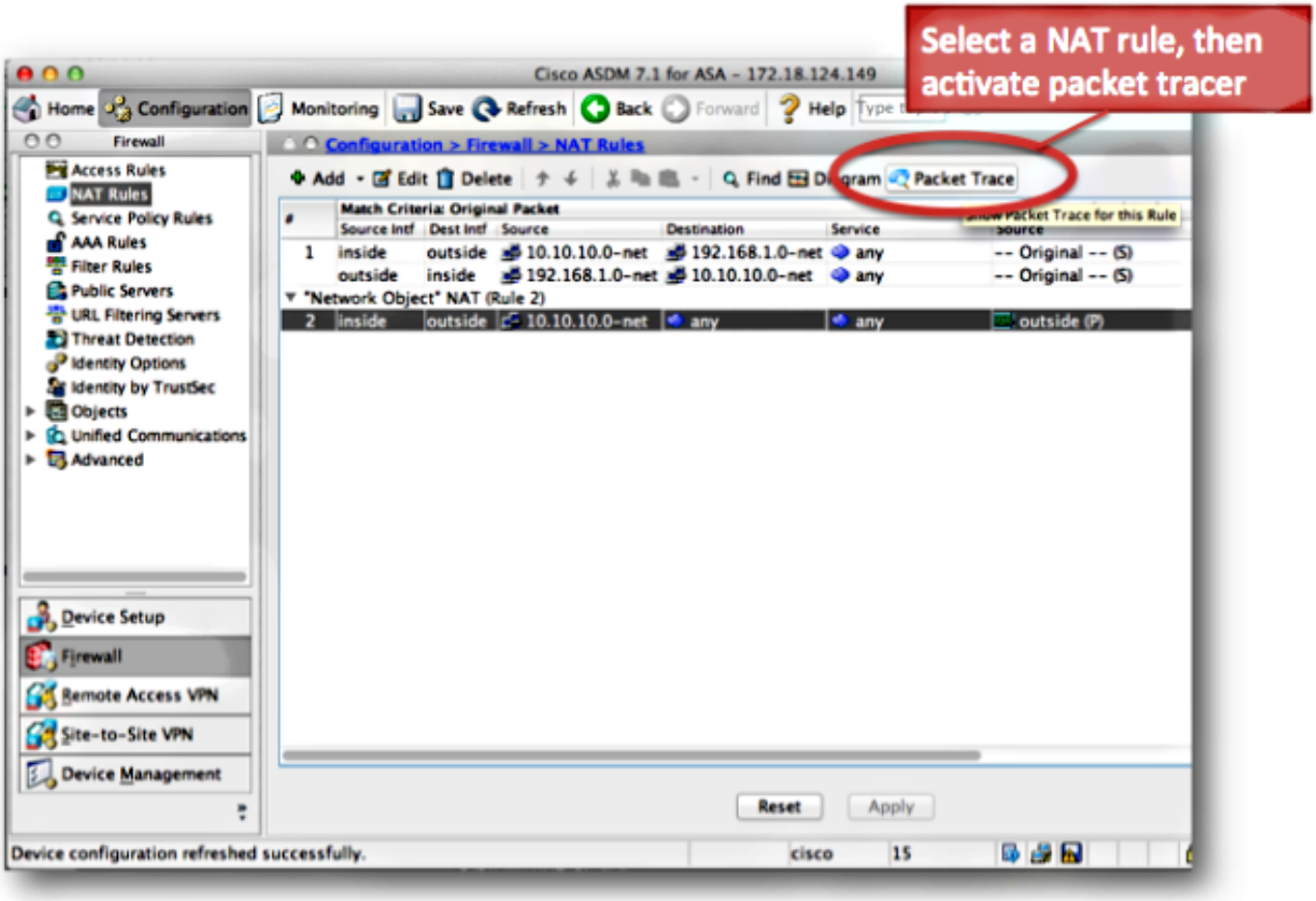
packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80

...(output omitted)...

Phase: 2
Type: NAT
Subtype:

```
Result: ALLOW
Config:

object network 10.10.10.0-net
 nat (inside,outside) dynamic interface


Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up

Action: allow



ASA#
```

Scegliere la regola NAT e fare clic su Packet Trace per attivare il tracer dei pacchetti da Cisco Adaptive Security Device Manager (ASDM). In questo modo vengono utilizzati gli indirizzi IP specificati nella regola NAT come input per lo strumento di traccia dei pacchetti:

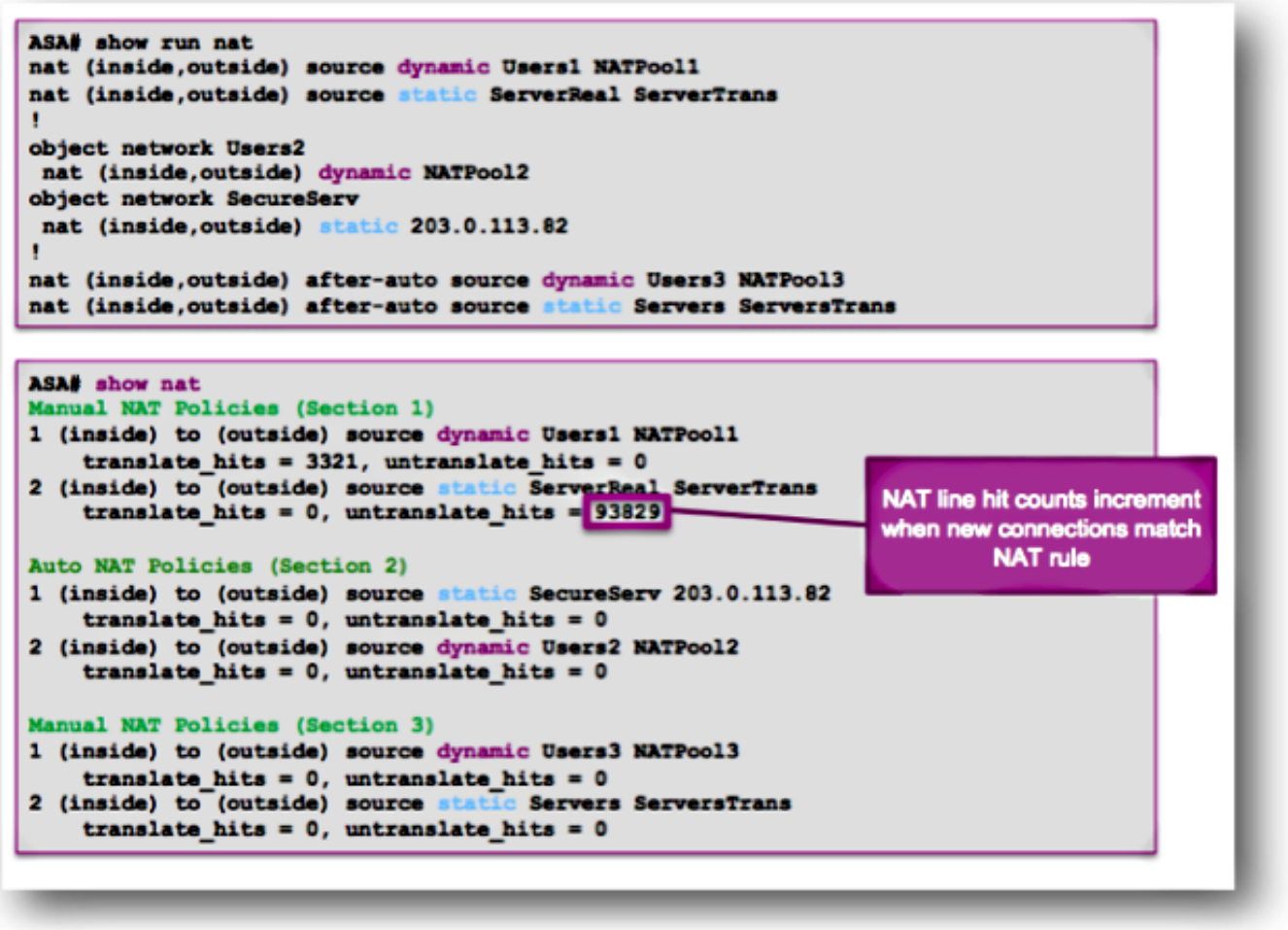


Visualizza l'output del comando Show Nat

L'output del comando show nat detail può essere utilizzato per visualizzare la tabella dei criteri NAT. In particolare, è possibile usare i contatori translate_hits e untranslate_hits per determinare le voci NAT da usare sull'appliance ASA.

Se la nuova regola NAT non ha translate_hits o untranslate_hits, il traffico non arriva all'ASA o forse una regola diversa con una priorità più alta nella tabella NAT corrisponde al traffico.

Di seguito vengono riportati la configurazione NAT e la tabella dei criteri NAT di una configurazione ASA diversa:



Nell'esempio precedente, sull'appliance ASA sono configurate sei regole NAT. L'output show nat mostra come queste regole vengono utilizzate per creare la tabella dei criteri NAT, nonché il numero di translate_hits e untranslate_hits per ciascuna regola.

Questi contatori vengono incrementati una sola volta per connessione. Dopo aver creato la connessione tramite l'ASA, i pacchetti successivi che corrispondono alla connessione corrente non incrementano le linee NAT (in modo simile al funzionamento del numero di accessi all'elenco sull'ASA).

Translate_hits: numero di nuove connessioni che soddisfano la regola NAT nella direzione in avanti.

Per "direzione di inoltro" si intende che la connessione è stata costruita attraverso l'ASA nella direzione delle interfacce specificate nella regola NAT.

Se una regola NAT specifica che il server interno viene convertito nell'interfaccia esterna, l'ordine delle interfacce nella regola NAT è "nat (inside,outside)..."; se il server avvia una nuova connessione a un host all'esterno, il contatore translate_hit viene incrementato.

Untranslate_hits: Il numero di nuove connessioni che corrispondono alla regola NAT nella direzione inversa.

Se una regola NAT specifica che il server interno viene convertito nell'interfaccia esterna, l'ordine

delle interfacce nella regola NAT è "nat (inside,outside)..."; se un client all'esterno dell'ASA avvia una nuova connessione al server all'interno, il contatore untranslate_hit viene incrementato.

Anche in questo caso, se si rileva che la nuova regola NAT non ha translate_hits o untranslate_hits, il traffico non arriva all'ASA o forse una regola diversa con una priorità più alta nella tabella NAT corrisponde al traffico.

Metodologia di risoluzione dei problemi NAT

Usare il tracciatore dei pacchetti per verificare che un pacchetto di esempio corrisponda alla regola di configurazione NAT corretta sull'appliance ASA. Per capire quali regole dei criteri NAT sono state trovate, usare il comando show nat detail. Se una connessione corrisponde a una configurazione NAT diversa da quella prevista, risolvere le seguenti domande:

- Esiste una regola NAT diversa che ha la precedenza sulla regola NAT che intendevi bloccare il traffico?
- È presente una regola NAT diversa con definizioni dell'oggetto troppo ampie (la subnet mask è troppo corta, ad esempio 255.0.0.0) che fa sì che il traffico corrisponda alla regola errata?
- Le policy NAT manuali non sono ordinate, il che fa sì che il pacchetto soddisfi la regola errata?
- La regola NAT è configurata in modo errato. La regola non corrisponde al traffico?

Vedere la sezione successiva per esempi di problemi e soluzioni.

Problemi comuni delle configurazioni NAT

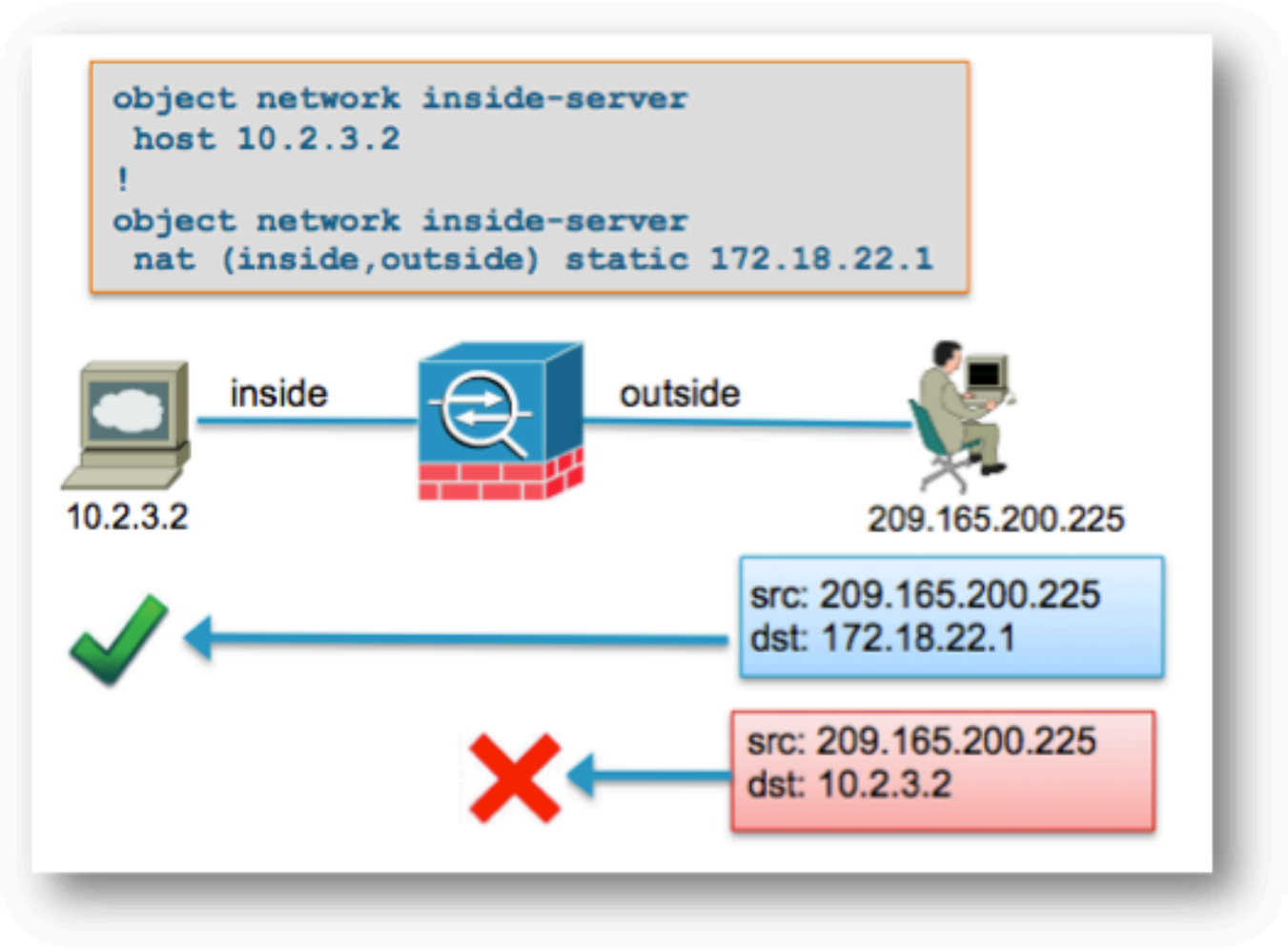
Di seguito sono riportati alcuni problemi comuni riscontrati quando si configura NAT sull'appliance ASA.

Problema: il traffico non riesce a causa di un errore RPF (NAT Reverse Path Failure). Errore: regole NAT asimmetriche corrispondenti per i flussi in avanti e all'indietro

Il controllo NAT RPF assicura che una connessione convertita dall'ASA in direzione diretta, ad esempio la sincronizzazione TCP (SYN), venga convertita dalla stessa regola NAT in direzione inversa, ad esempio la sintassi TCP SYN/acknowledledge (ACK).

Nella maggior parte dei casi, questo problema è causato da connessioni in entrata destinate all'indirizzo locale (non tradotto) in un'istruzione NAT. A livello di base, NAT RPF verifica che la connessione inversa dal server al client corrisponda alla stessa regola NAT; in caso contrario, il controllo NAT RPF non riesce.

Esempio: 209.165.200.225



Quando l'host esterno al numero 192.168.200.225 invia un pacchetto destinato direttamente all'indirizzo IP locale (non tradotto) 10.2.3.2, l'ASA scarta il pacchetto e registra questo syslog:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

Soluzione:

In primo luogo, accertarsi che l'host invii i dati all'indirizzo NAT globale corretto. Se l'host invia i pacchetti destinati all'indirizzo corretto, controllare le regole NAT interessate dalla connessione.

Verificare che le regole NAT siano definite correttamente e che gli oggetti a cui si fa riferimento nelle regole NAT siano corretti. Verificare inoltre che l'ordine delle norme NAT sia appropriato.

Usare l'utility packet tracer per specificare i dettagli del pacchetto negato. Nell'utilità di traccia dei pacchetti deve essere visualizzato il pacchetto ignorato a causa di un errore di controllo RPF.

Quindi, guardate l'output del packet tracer per vedere quali regole NAT vengono colpite nella fase NAT e nella fase NAT-RPF.

Se un pacchetto soddisfa una regola NAT nella fase di controllo RPF NAT, che indica che il flusso inverso influirebbe su una traduzione NAT, ma non corrisponde a una regola nella fase NAT, che indica che il flusso in avanti NON influirebbe su una regola NAT, il pacchetto viene scartato.

Questo output corrisponde allo scenario illustrato nel diagramma precedente, in cui l'host esterno invia in modo non corretto il traffico all'indirizzo IP locale del server e non all'indirizzo IP globale (convertito):

```
<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 1234 10.2.3.2 80



    .....

Phase: 8
Type: NAT
Subtype: rpf-check
Result:

DROP


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

Quando il pacchetto è destinato all'indirizzo IP mappato corretto di 172.18.22.1, il pacchetto soddisfa la regola NAT corretta nella fase UN-NAT nella direzione di inoltro e la stessa regola nella fase di controllo NAT RPF:

```
<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80


...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
```

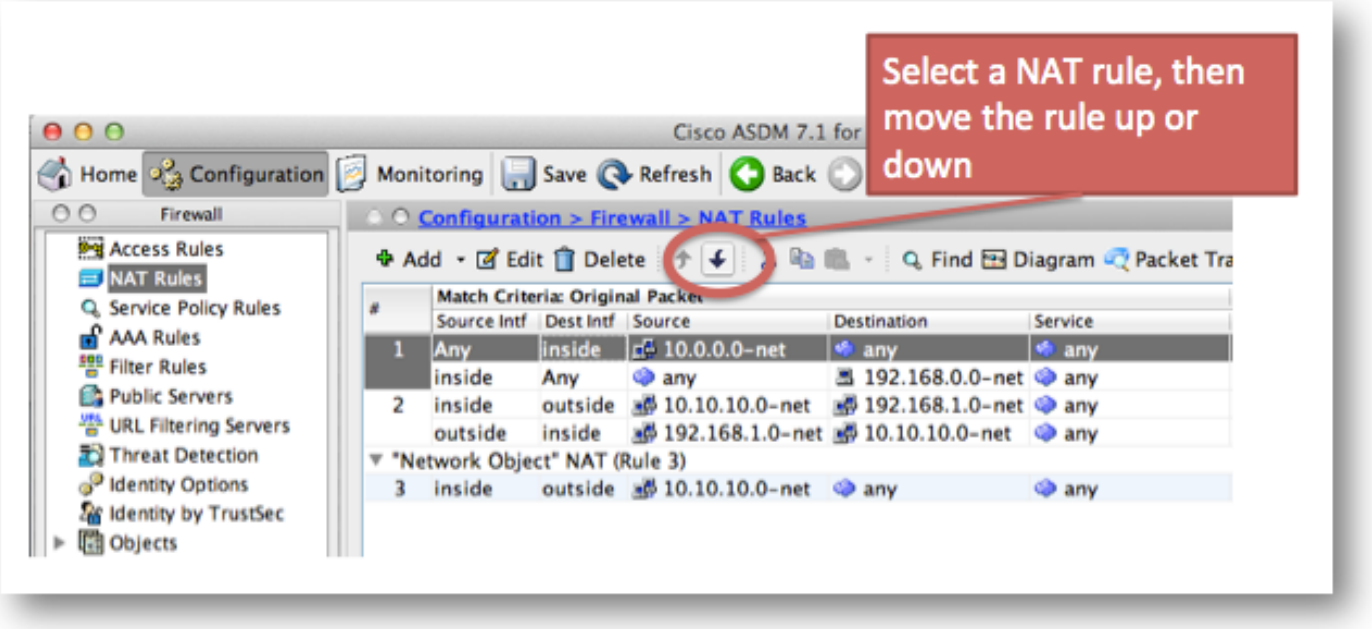
```
Phase: 8
Type: NAT
Subtype: rpf-check
Result:

ALLOW


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

Problema: le regole NAT manuali non sono ordinate, il che provoca corrispondenze errate ai pacchetti

Le regole NAT manuali vengono elaborate in base al relativo aspetto nella configurazione. Se una regola NAT molto ampia è elencata per prima nella configurazione, può eseguire l'override di un'altra regola più specifica più in basso nella tabella NAT. Usa il tracciatore dei pacchetti per verificare quale regola NAT colpisce il traffico. Può essere necessario riorganizzare le voci NAT manuali in un ordine diverso.

Soluzione:

Riordinare le regole NAT con ASDM.



Soluzione:

Le regole NAT possono essere riordinate con la CLI se si rimuove la regola e la si reinserisce con un numero di riga specifico. Per inserire una nuova regola in corrispondenza di una riga specifica,

immettere il numero di riga subito dopo aver specificato le interfacce.

Esempio:

<#root>

ASA(config)#

**nat (inside,outside) *1* source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net**

Problema

Una regola NAT è troppo ampia e corrisponde inavvertitamente ad alcuni tipi di traffico. A volte vengono create regole NAT che utilizzano oggetti troppo ampi. Se queste regole vengono posizionate vicino alla parte superiore della tabella NAT (all'inizio della Sezione 1, ad esempio), possono corrispondere a più traffico di quanto previsto e fare in modo che le regole NAT più in basso nella tabella non vengano mai trovate.

Soluzione

Usare l'analisi dei pacchetti per determinare se il traffico soddisfa una regola con definizioni dell'oggetto troppo ampie. In questo caso, è necessario ridurre l'ambito di tali oggetti o spostare le regole più in basso nella tabella NAT o nella sezione after-auto (Sezione 3) della tabella NAT.

Problema

Una regola NAT devia il traffico a un'interfaccia errata. Le regole NAT possono avere la precedenza sulla tabella di routing quando determinano l'interfaccia che il pacchetto invia all'ASA. Se un pacchetto in entrata corrisponde a un indirizzo IP tradotto in un'istruzione NAT, viene utilizzata la regola NAT per determinare l'interfaccia di uscita.

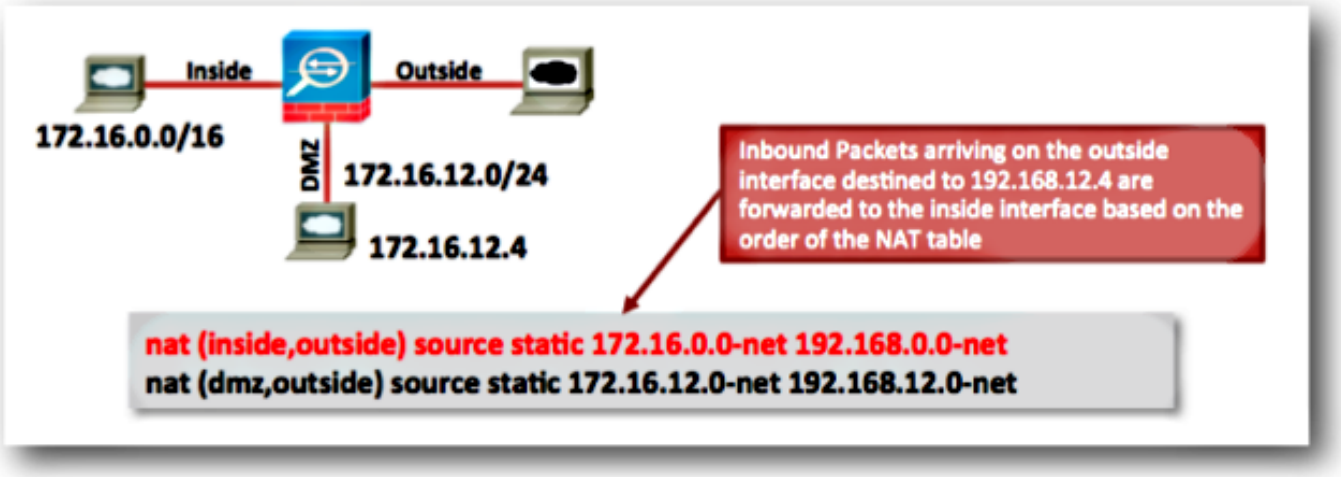
Il controllo deviazione NAT (che può ignorare la tabella di routing) verifica se sono presenti regole NAT che specificano la traduzione dell'indirizzo di destinazione per un pacchetto in entrata che arriva su un'interfaccia.

Se non esiste una regola che specifica in modo esplicito come convertire l'indirizzo IP di destinazione del pacchetto, viene consultata la tabella di routing globale per determinare l'interfaccia di uscita.

Se esiste una regola che specifica in modo esplicito come tradurre l'indirizzo IP di destinazione del pacchetto, la regola NAT estrae il pacchetto verso l'altra interfaccia nella conversione e la tabella di routing globale viene effettivamente ignorata.

Questo problema si verifica più spesso per il traffico in entrata, che arriva all'interfaccia esterna, ed è in genere causato da regole NAT non ordinate che deviano il traffico a interfacce non intenzionali.

Esempio:



Soluzioni:

Il problema può essere risolto tramite una delle azioni seguenti:

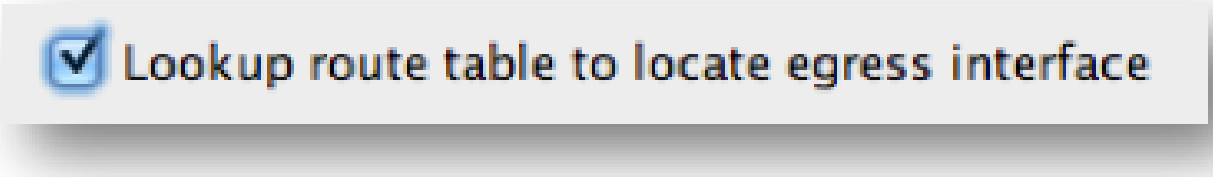
- Riordinare la tabella NAT in modo che la voce più specifica venga elencata per prima.
- Usa intervalli di indirizzi IP globali non sovrapposti per le istruzioni NAT.

Si noti che se la regola NAT è una regola di identità, ovvero gli indirizzi IP non vengono modificati dalla regola, è possibile utilizzare la parola chiave route-lookup (questa parola chiave non è applicabile all'esempio precedente poiché la regola NAT non è una regola di identità).

La parola chiave route-lookup determina l'esecuzione di un controllo aggiuntivo da parte dell'ASA quando viene soddisfatta una regola NAT. Controlla che la tabella di routing dell'ASA inoltri il pacchetto alla stessa interfaccia in uscita a cui la configurazione NAT devia il pacchetto.

Se l'interfaccia di uscita della tabella di routing non corrisponde all'interfaccia di deviazione NAT, la regola NAT non viene soddisfatta (la regola viene ignorata) e il pacchetto continua verso il basso nella tabella NAT per essere elaborato da una regola NAT successiva.

L'opzione route-lookup è disponibile solo se la regola NAT è una regola NAT di identità, ovvero gli indirizzi IP non vengono modificati dalla regola. L'opzione route-lookup può essere abilitata per ogni regola NAT se si aggiunge route-lookup alla fine della riga NAT o se si seleziona la casella di controllo Cerca tabella di route per individuare l'interfaccia di uscita nella configurazione della regola NAT in ASDM:



Problema: in seguito a una regola NAT, l'ASA passa al protocollo ARP (Proxy Address Resolution Protocol) per il traffico sull'interfaccia mappata

Gli ARP proxy ASA per l'intervallo di indirizzi IP globali in un'istruzione NAT sull'interfaccia globale. La funzionalità ARP proxy può essere disabilitata in base alle regole NAT se si aggiunge la parola chiave no-proxy-arp all'istruzione NAT.

Questo problema si verifica anche quando la subnet dell'indirizzo globale viene inavvertitamente creata in modo da essere molto più grande di quanto previsto.

Soluzione

Se possibile, aggiungere la parola chiave no-proxy-arp alla riga NAT.

Esempio:

<#root>

```
ASA(config)#
object network inside-server

ASA(config-network-object)#
nat (inside,outside) static 172.18.22.1 no-proxy-arp

ASA(config-network-object)#
end

ASA#
  ASA#
 show run nat

object network inside-server
 nat (inside,outside) static 172.18.22.1
no-proxy-arp

ASA#
```

Questa operazione può essere effettuata anche con ASDM. All'interno della regola NAT, selezionare la casella di controllo Disabilita ARP proxy sull'interfaccia di uscita.

.

Informazioni correlate

- VIDEO: ASA port forwarding per l'accesso al server DMZ (versioni 8.3 e 8.4)
- Configurazione di base di ASA NAT: server Web nella DMZ in ASA versione 8.3 e successive
- Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1
- Supporto tecnico Cisco e download

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).