Solucionar problemas de configuración de traducción de direcciones de red (NAT) ASA

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Resolución de problemas de configuración de NAT en ASA
- Cómo se Utiliza la Configuración ASA para Construir la Tabla de Políticas NAT
- Cómo resolver problemas de NAT
  - Uso de la utilidad Packet Tracer
  - Ver el resultado del comando Show Nat
  - Metodología de Troubleshooting de NAT
- Problemas comunes con las configuraciones NAT
  - Problema: el tráfico falla debido a un error de ruta inversa (RPF) de NAT Error: reglas NAT asimétricas coincidentes para flujos de reenvío e inverso
  - Problema: las reglas NAT manuales están desordenadas, lo que provoca coincidencias incorrectas de paquetes
  - Problema
  - Problema
  - Problema: Una regla NAT hace que ASA Proxy Address Resolution Protocol (ARP) para el tráfico en la interfaz asignada

Introducción

Este documento describe cómo resolver problemas de configuración de traducción de direcciones de red (NAT) en la plataforma Cisco Adaptive Security Appliance (ASA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

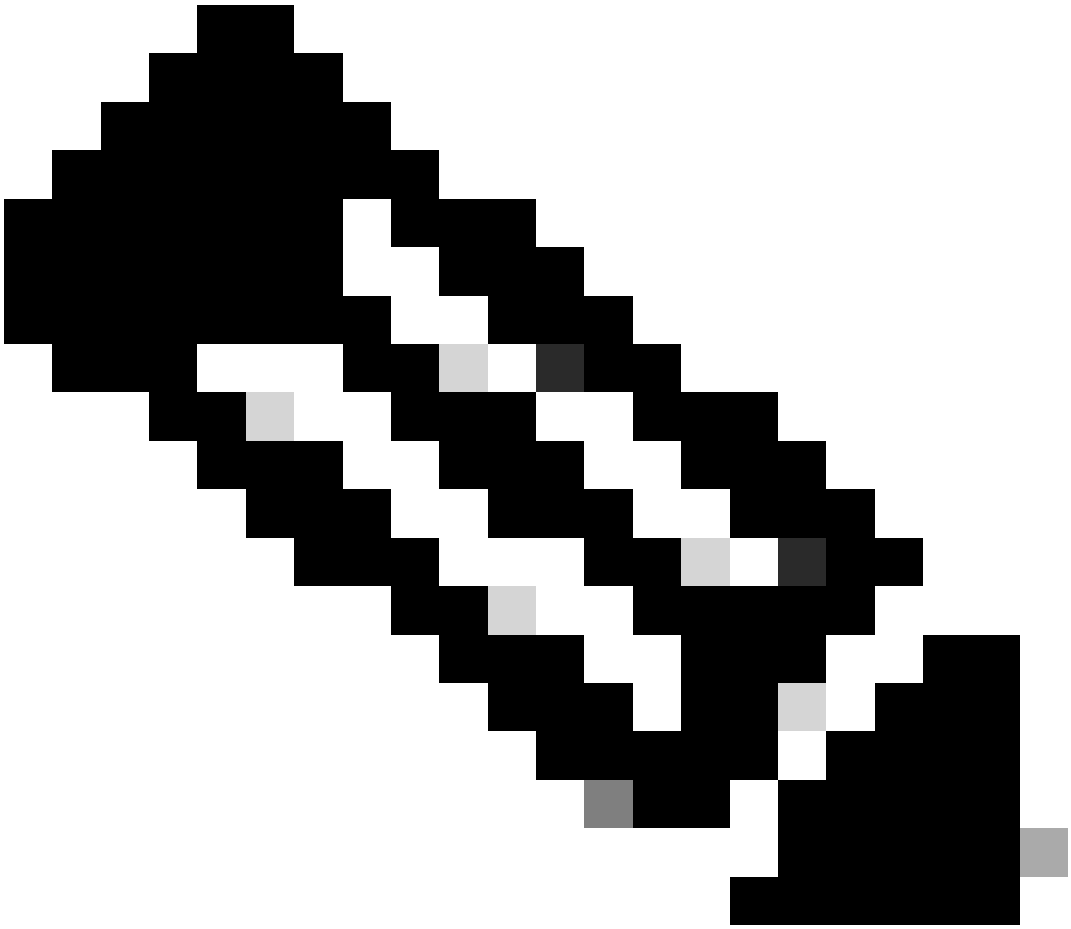
Componentes Utilizados

La información de este documento se basa en ASA versión 8.3 y posteriores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

Resolución de problemas de configuración de NAT en ASA



> Nota: Para ver algunos ejemplos básicos de configuraciones de NAT, que incluyen un video que muestra una configuración básica de NAT, vea la sección Información Relacionada en la parte inferior de este documento.

Al resolver problemas de configuraciones de NAT, es importante entender cómo se utiliza la configuración de NAT en el ASA para construir la tabla de políticas de NAT.

Estos errores de configuración explican la mayoría de los problemas de NAT que encuentran los administradores de ASA:

- Las reglas de configuración de NAT están fuera de servicio. Por ejemplo, una regla NAT manual se coloca en la parte superior de la tabla NAT, lo que hace que nunca se alcancen reglas más específicas ubicadas más abajo de la tabla NAT.

- Los objetos de red utilizados en la configuración de NAT son demasiado amplios, lo que hace que el tráfico coincida inadvertidamente con estas reglas de NAT, y que omita reglas de NAT más específicas.

La utilidad packet tracer se puede utilizar para diagnosticar la mayoría de los problemas relacionados con NAT en el ASA. Vea la siguiente sección para obtener más información sobre cómo se utiliza la configuración de NAT para crear la tabla de políticas de NAT y cómo resolver problemas específicos de NAT.

Además, el comando show nat detail se puede utilizar para comprender qué reglas NAT son afectadas por las nuevas conexiones.

Cómo se Utiliza la Configuración ASA para Construir la Tabla de Políticas NAT

Todos los paquetes procesados por el ASA se evalúan en función de la tabla NAT. Esta evaluación comienza en la parte superior (Sección 1) y funciona hacia abajo hasta que se iguala una regla NAT.

En general, una vez que una regla NAT coincide, esa regla NAT se aplica a la conexión y no se verifican más políticas NAT en el paquete, pero hay algunas advertencias que se explican a continuación.

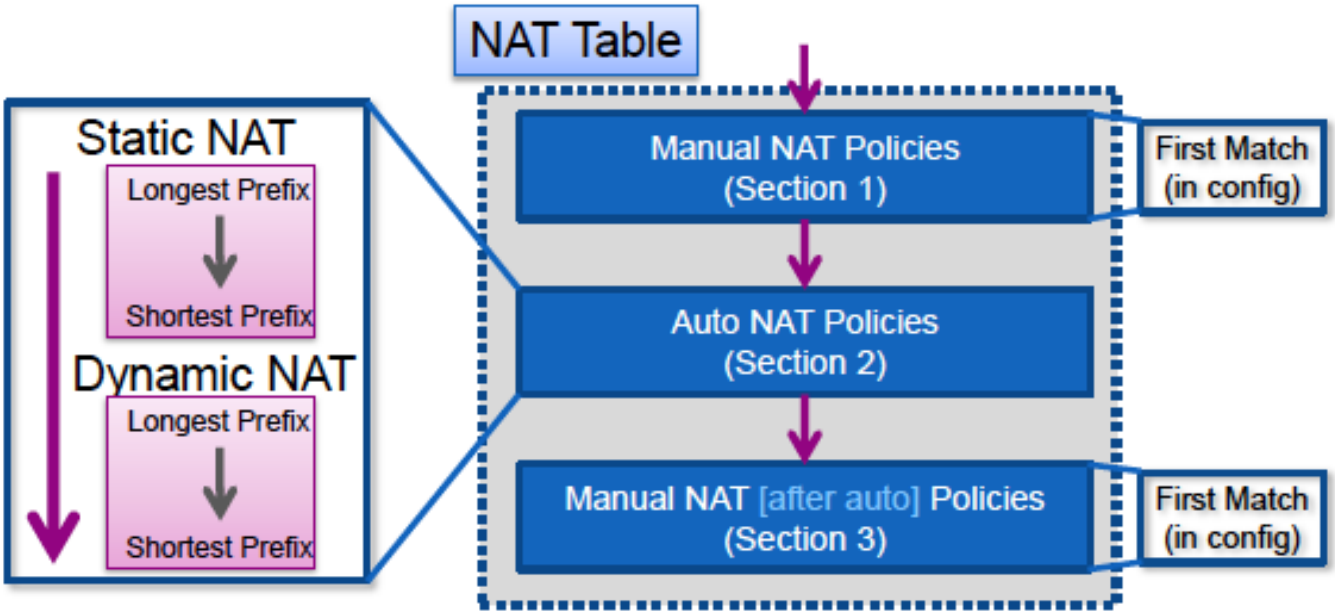
La Tabla de Políticas NAT

La política NAT en el ASA se construye a partir de la configuración NAT.

Las tres secciones de la tabla NAT de ASA son:

Sección 1	Políticas NAT manuales Se procesan en el orden en que aparecen en la configuración.
Sección 2	Políticas NAT automáticas Se procesan en función del tipo de NAT (estática o dinámica) y de la longitud del prefijo (máscara de subred) del objeto.
Sección 3	Políticas NAT manuales después de la activación automática Se procesan en el orden en que aparecen en la configuración.

Este diagrama muestra las diferentes secciones de NAT y cómo se ordenan:



Coincidencia de regla NAT

Sección 1

- Un flujo se evalúa primero en relación con la sección 1 de la tabla NAT que comienza con la primera regla.
    - Si la IP de origen y de destino del paquete coinciden con los parámetros de la regla NAT manual, se aplica la traducción y el proceso se detiene y no se evalúan más reglas NAT en ninguna sección.
    - Si no coincide ninguna regla NAT, el flujo se evalúa en función de la sección 2 de la tabla NAT.

Sección 2

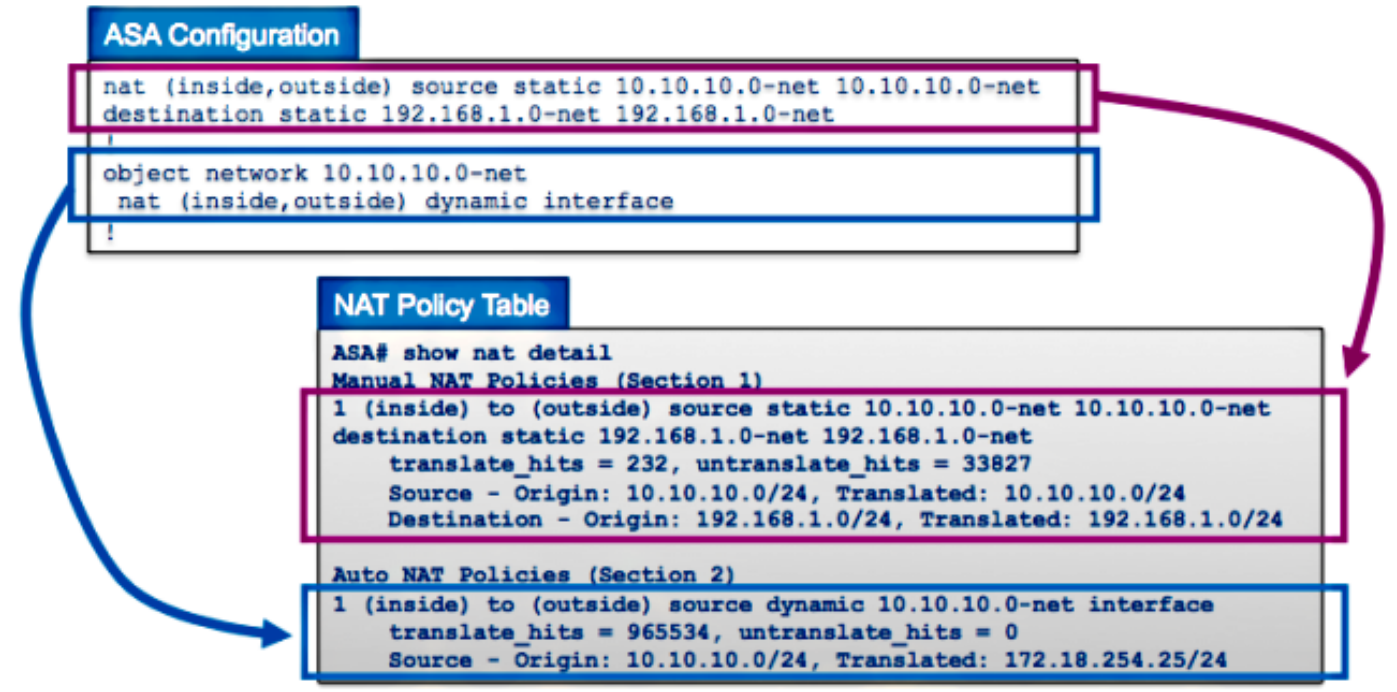
- Un flujo se evalúa en función de las reglas NAT de la sección 2 en el orden especificado anteriormente, primero las reglas NAT estáticas y, a continuación, las reglas NAT dinámicas.
    - Si una regla de traducción coincide con la IP de origen o de destino del flujo, se puede aplicar la traducción y se puede seguir evaluando el resto de las reglas para ver si coinciden con la otra IP del flujo. Por ejemplo, una regla de NAT automática podría traducir la IP de origen y otra regla de NAT automática podría traducir el destino.
    - Si el flujo coincide con una regla de NAT automática, cuando se alcanza el final de la sección 2, se detiene la búsqueda de NAT y no se evalúan las reglas de la sección 3.
    - Si ninguna regla NAT de la sección 2 coincide con el flujo, la búsqueda continúa con la sección 3

Sección 3

- El proceso de la sección 3 es esencialmente el mismo que el de la sección 1. Si la IP de origen y de destino del paquete coinciden con los parámetros de la regla NAT manual, se aplica la traducción y el proceso se detiene y no se evalúan más reglas NAT en ninguna

sección.

Este ejemplo muestra cómo se representa la configuración NAT de ASA con dos reglas (una instrucción NAT manual y una configuración NAT automática) en la tabla NAT:



Cómo resolver problemas de NAT

Uso de la utilidad Packet Tracer

Para resolver problemas con las configuraciones NAT, utilice la utilidad packet tracer para verificar que un paquete llegue a la política NAT. Packet Tracer le permite especificar un paquete de muestra que ingresa al ASA, y el ASA indica qué configuración se aplica al paquete y si se permite o no.

En el siguiente ejemplo, se proporciona un paquete TCP de ejemplo que entra en la interfaz interna y se dirige a un host en Internet. La utilidad packet tracer muestra que el paquete coincide con una regla NAT dinámica y se traduce a la dirección IP externa de 172.16.123.4:

<#root>

ASA#

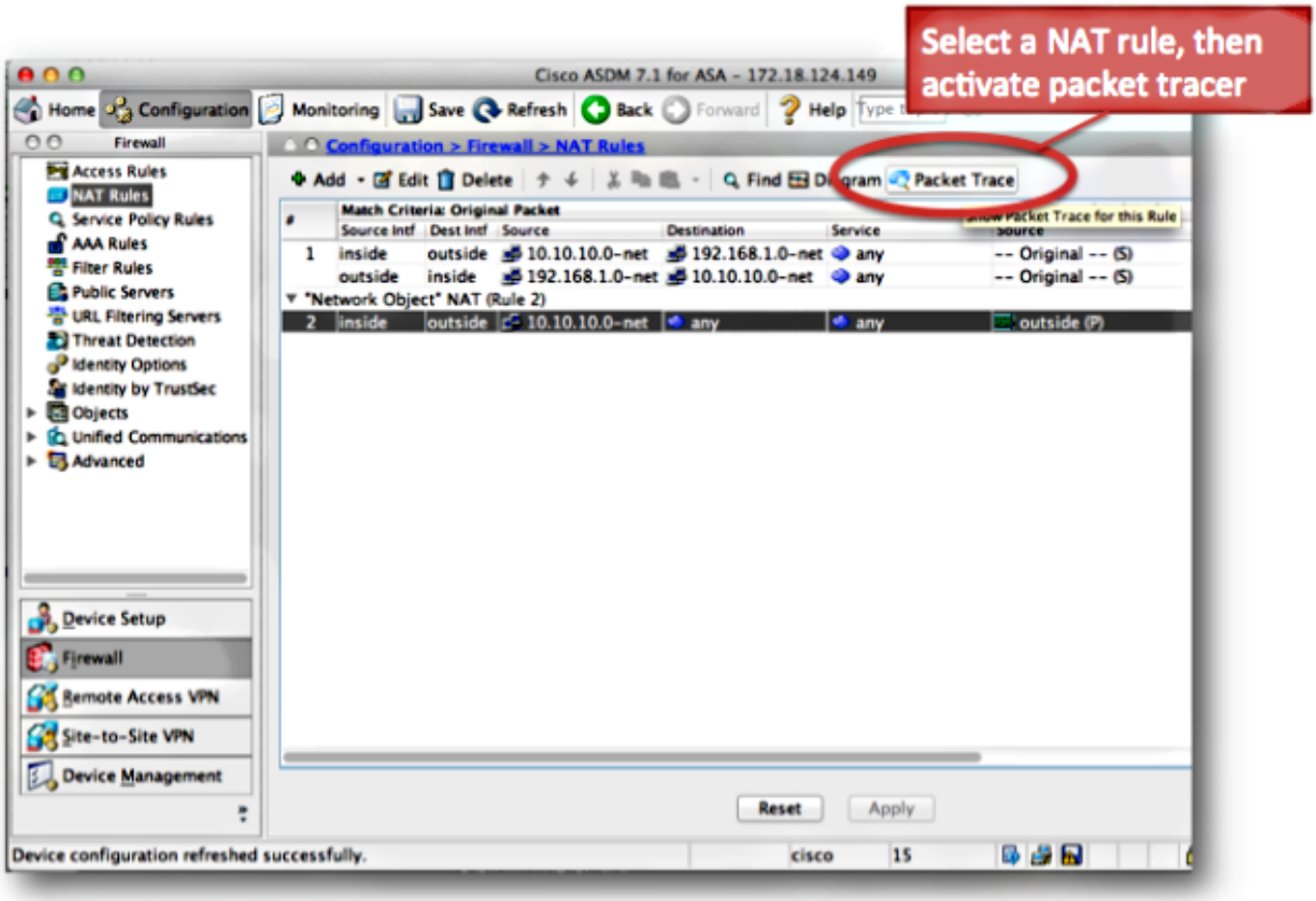
packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80

...(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#
```

Elija la regla NAT y haga clic en Rastreo de paquetes para activar el rastreador de paquetes desde el Administrador adaptable de dispositivos de seguridad de Cisco (ASDM). Esto utiliza las direcciones IP especificadas en la regla NAT como entradas para la herramienta de seguimiento de paquetes:

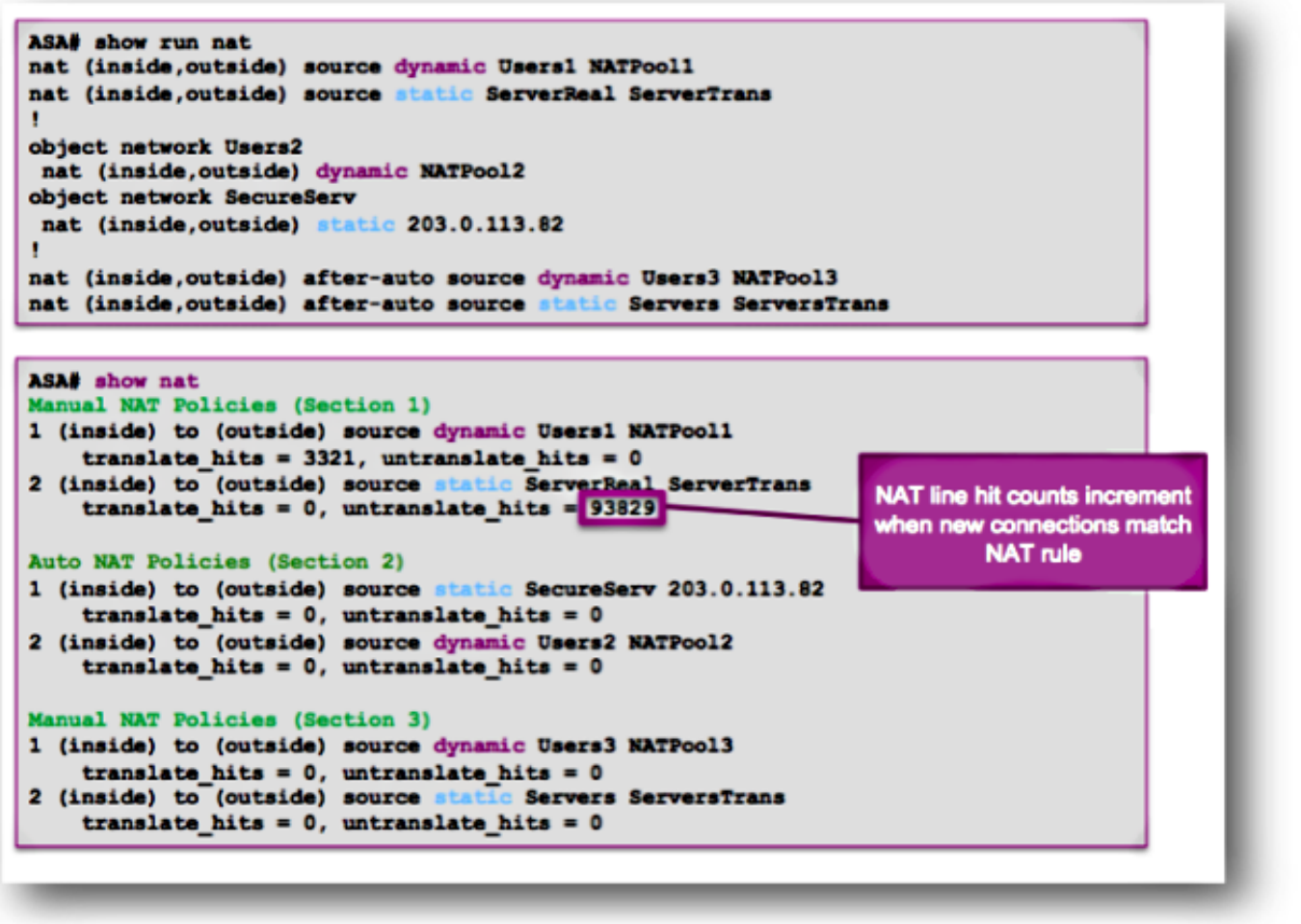


Ver el resultado del comando Show Nat

La salida del comando show nat detail se puede utilizar para ver la tabla de políticas de NAT. Específicamente, los contadores translate_hits y untranslate_hits se pueden utilizar para determinar qué entradas NAT se utilizan en el ASA.

Si observa que su nueva regla NAT no tiene translate_hits ni untranslate_hits, eso significa que el tráfico no llega al ASA, o quizás una regla diferente que tiene una prioridad más alta en la tabla NAT coincida con el tráfico.

Aquí está la configuración NAT y la tabla de política NAT de una configuración ASA diferente:



En el ejemplo anterior, hay seis reglas NAT configuradas en este ASA. El resultado de show nat muestra cómo se utilizan estas reglas para construir la tabla de política NAT, así como el número de translate_hits y untranslate_hits para cada regla.

Estos contadores de visitas se incrementan sólo una vez por conexión. Después de que la conexión se construye a través del ASA, los paquetes subsiguientes que coinciden con esa conexión actual no incrementan las líneas NAT (de manera muy similar a como funciona el conteo de visitas a la lista de acceso en el ASA).

Translate_hits: El número de nuevas conexiones que coinciden con la regla NAT en la dirección de reenvío.

"Dirección de reenvío" significa que la conexión se construyó a través del ASA en la dirección de las interfaces especificadas en la regla NAT.

Si una regla NAT especificó que el servidor interno se traduce a la interfaz externa, el orden de las interfaces en la regla NAT es "nat (inside,outside)..."; si ese servidor inicia una nueva conexión a un host en el exterior, el contador translate_hit aumenta.

Untranslate_hits: El número de nuevas conexiones que coinciden con la regla NAT en la dirección inversa.

Si una regla NAT especifica que el servidor interno se traduce a la interfaz externa, el orden de las interfaces en la regla NAT es "nat (inside,outside)..."; si un cliente en el exterior del ASA inicia una nueva conexión con el servidor en el interior, el contador untranslate_hit aumenta.

De nuevo, si ve que su nueva regla NAT no tiene translate_hits ni untranslate_hits, eso significa que el tráfico no llega al ASA, o quizás una regla diferente que tiene una prioridad más alta en la tabla NAT coincida con el tráfico.

Metodología de Troubleshooting de NAT

Utilice el rastreador de paquetes para confirmar que un paquete de muestra coincide con la regla de configuración NAT adecuada en el ASA. Utilice el comando show nat detail para comprender qué reglas de política NAT se aplican. Si una conexión coincide con una configuración de NAT diferente a la esperada, solucione los problemas con estas preguntas:

- ¿Existe una regla de NAT diferente que tenga prioridad sobre la regla de NAT a la que pretendía que llegue el tráfico?
- ¿Existe una regla NAT diferente con definiciones de objeto demasiado amplias (la máscara de subred es demasiado corta, como 255.0.0.0) que hace que este tráfico coincida con la regla incorrecta?
- ¿Están las políticas NAT manuales fuera de servicio, lo que hace que el paquete coincida con la regla incorrecta?
- ¿Su regla NAT está configurada incorrectamente, lo que hace que la regla no coincida con su tráfico?

Consulte la siguiente sección para ver ejemplos de problemas y soluciones.

Problemas comunes con las configuraciones NAT

A continuación, se detallan algunos problemas comunes que se experimentan al configurar NAT en ASA.

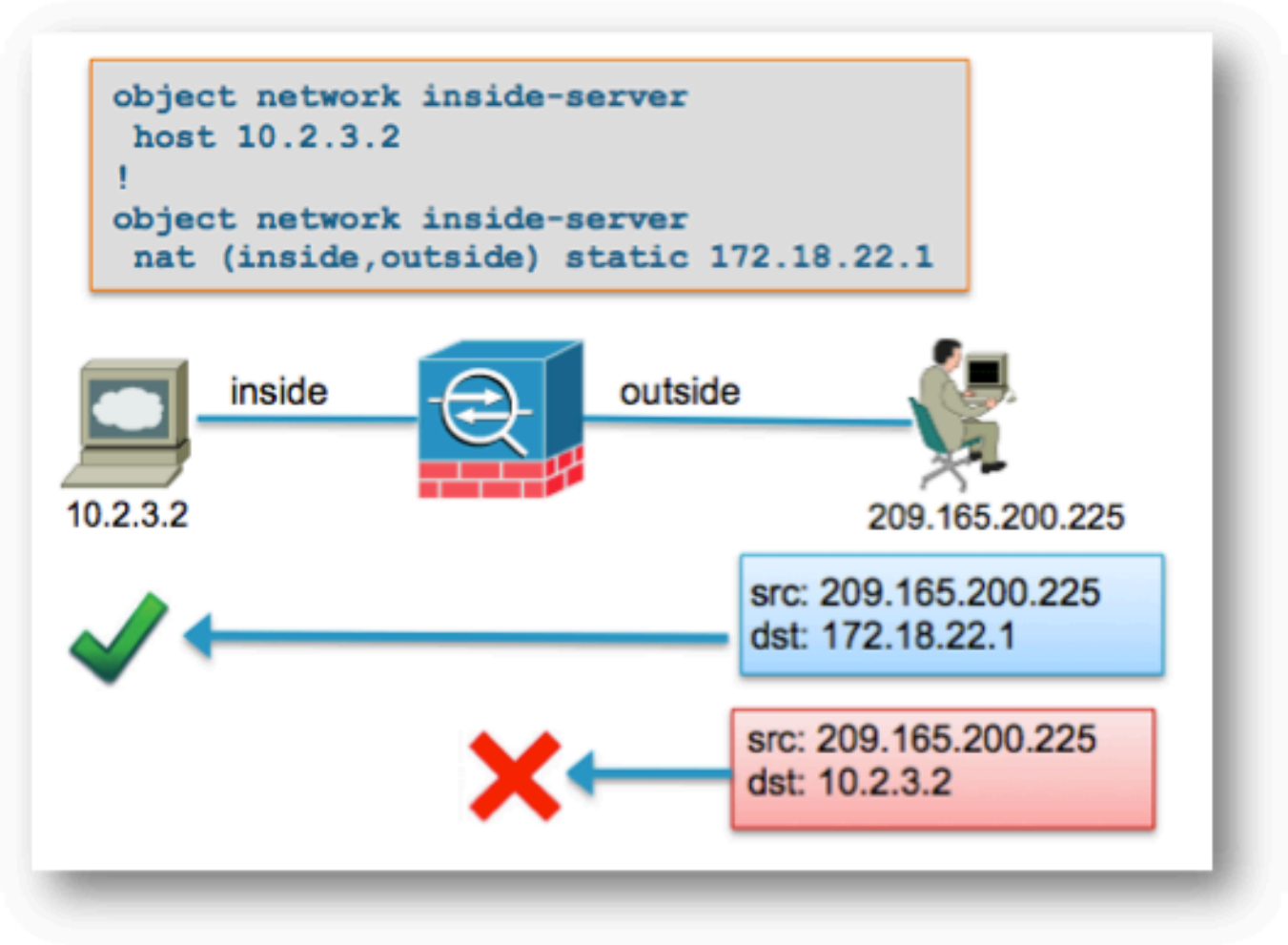
Problema: el tráfico falla debido a un error de ruta inversa (RPF) de NAT Error: reglas NAT asimétricas coincidentes para flujos de reenvío e inverso

La verificación NAT RPF garantiza que una conexión traducida por el ASA en la dirección de reenvío, como la sincronización TCP (SYN), sea traducida por la misma regla NAT en la dirección

inversa, como la confirmación TCP SYN (ACK).

Generalmente, este problema es causado por conexiones entrantes destinadas a la dirección local (sin traducir) en una sentencia NAT. En un nivel básico, NAT RPF verifica que la conexión inversa del servidor al cliente coincida con la misma regla NAT; si no lo hace, la verificación NAT RPF falla.

Ejemplo: 209.165.200.225



Cuando el host externo en 192.168.200.225 envía un paquete destinado directamente a la dirección IP local (sin traducir) de 10.2.3.2, el ASA descarta el paquete y registra este 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
```

Solución:

Primero, asegúrese de que el host envíe los datos a la dirección NAT global correcta. Si el host envía paquetes destinados a la dirección correcta, verifique las reglas NAT que son alcanzadas

por la conexión.

Verifique que las reglas NAT estén definidas correctamente y que los objetos a los que se hace referencia en las reglas NAT sean correctos. También verifique que el orden de las reglas NAT sea apropiado.

Utilice la utilidad packet tracer para especificar los detalles del paquete denegado. El rastreador de paquetes debe mostrar el paquete descartado debido a la falla de verificación RPF.

A continuación, observe la salida de packet tracer para ver qué reglas NAT se aplican en la fase NAT y en la fase NAT-RPF.

Si un paquete coincide con una regla NAT en la fase de verificación NAT RPF, que indica que el flujo inverso alcanzaría una traducción NAT, pero no coincide con una regla en la fase NAT, que indica que el flujo de reenvío NO alcanzaría una regla NAT, el paquete se descarta.

Este resultado coincide con el escenario mostrado en el diagrama anterior, donde el host externo envía tráfico incorrectamente a la dirección IP local del servidor y no a la dirección IP global (traducida):

```
<#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)#
```

Cuando el paquete está destinado a la dirección IP asignada correcta de 172.18.22.1, el paquete coincide con la regla NAT correcta en la fase UN-NAT en la dirección de reenvío, y la misma regla en la fase NAT RPF-check:

```
<#root>

ASA(config)#
```

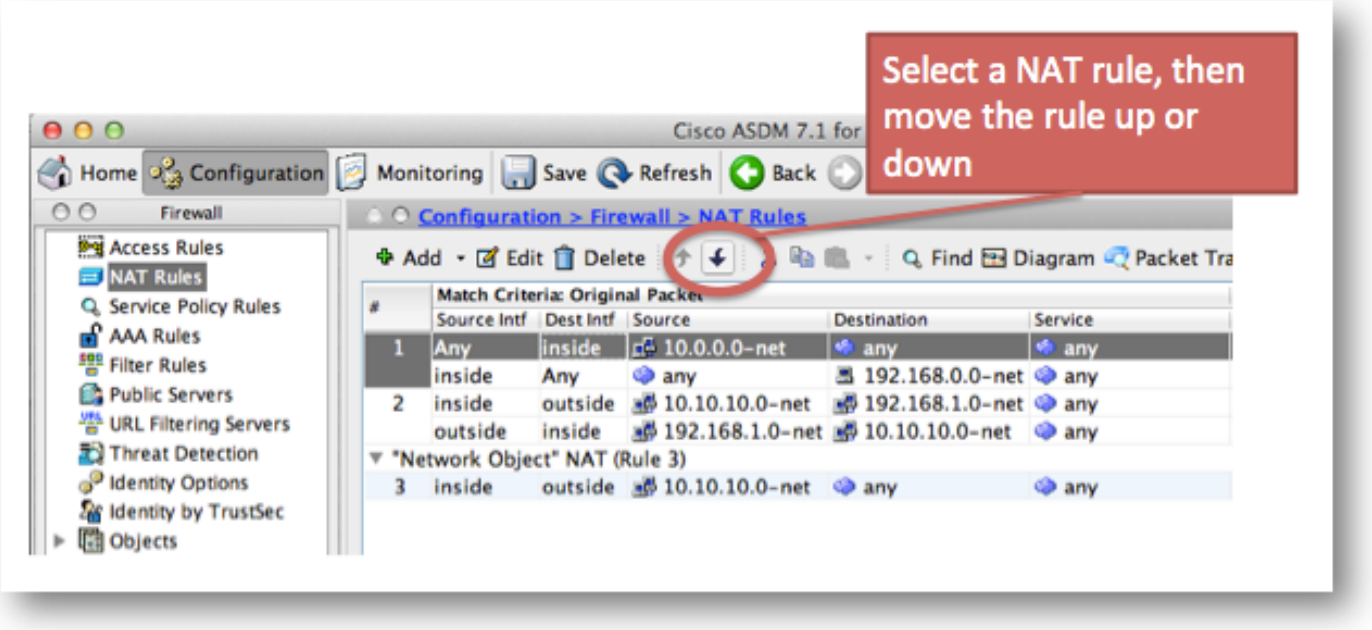
```
packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80


...
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: las reglas NAT manuales están desordenadas, lo que provoca coincidencias incorrectas de paquetes

Las reglas NAT manuales se procesan en función de su apariencia en la configuración. Si una regla NAT muy amplia aparece primero en la configuración, puede invalidar otra regla más específica más abajo en la tabla NAT. Utilice el rastreador de paquetes para verificar qué regla NAT afecta su tráfico; puede ser necesario reorganizar las entradas manuales de NAT a un orden diferente.

Solución:

Reordenar las reglas NAT con ASDM.



Solución:

Las reglas NAT se pueden reordenar con la CLI si elimina la regla y la vuelve a insertar en un número de línea específico. Para insertar una nueva regla en una línea específica, ingrese el número de línea justo después de que se especifiquen las interfaces.

Ejemplo:

<#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 regla NAT es demasiado amplia y coincide con cierto tráfico de forma inadvertida. A veces se crean reglas NAT que utilizan objetos demasiado amplios. Si estas reglas se colocan cerca de la parte superior de la tabla NAT (en la parte superior de la Sección 1, por ejemplo), pueden coincidir con más tráfico del esperado y hacer que las reglas NAT más abajo de la tabla nunca sean alcanzadas.

Solución

Utilice packet tracer para determinar si su tráfico coincide con una regla con definiciones de objeto que son demasiado amplias. Si este es el caso, debe reducir el alcance de esos objetos, o mover las reglas más abajo en la tabla NAT, o a la sección post-auto (Sección 3) de la tabla NAT.

Problema

Una regla NAT desvía el tráfico a una interfaz incorrecta. Las reglas NAT pueden tener precedencia sobre la tabla de ruteo cuando determinan qué interfaz un paquete egresa del ASA. Si un paquete entrante coincide con una dirección IP traducida en una sentencia NAT, se utiliza la regla NAT para determinar la interfaz de salida.

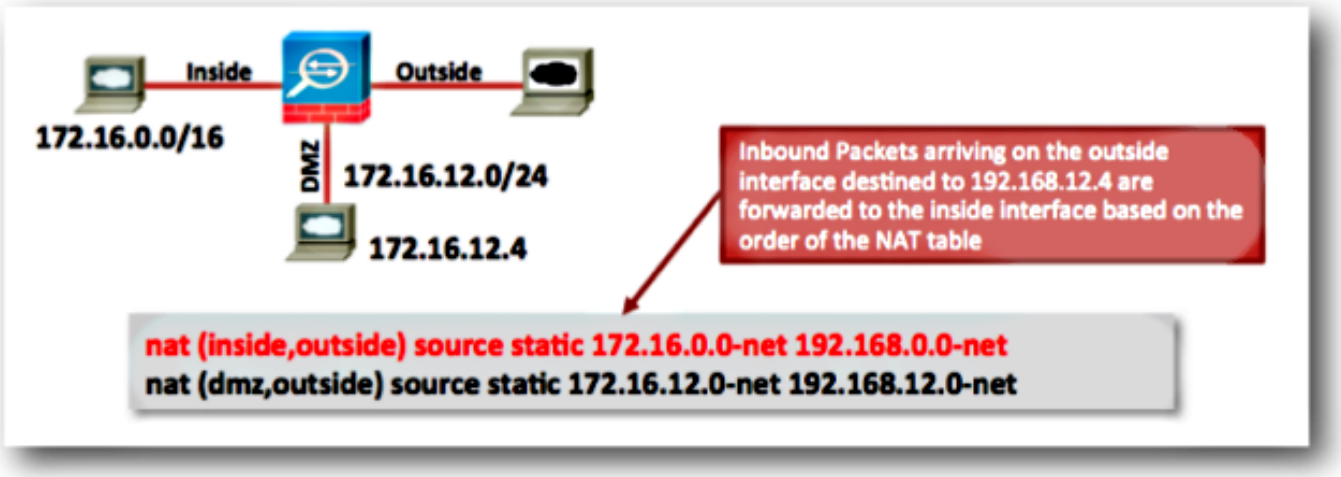
La verificación de desvío de NAT (que es lo que puede invalidar la tabla de ruteo) verifica si hay alguna regla NAT que especifique la traducción de dirección de destino para un paquete entrante que llega a una interfaz.

Si no hay ninguna regla que especifique explícitamente cómo traducir esa dirección IP de destino del paquete, se consulta la tabla de ruteo global para determinar la interfaz de salida.

Si hay una regla que especifica explícitamente cómo traducir la dirección IP de destino del paquete, la regla NAT extrae el paquete a la otra interfaz en la traducción y la tabla de ruteo global se omite de manera efectiva.

Este problema se observa con mayor frecuencia en el tráfico entrante, que llega a la interfaz externa, y suele deberse a reglas NAT fuera de orden que desvían el tráfico a interfaces no deseadas.

Ejemplo:



Soluciones:

Este problema se puede resolver con cualquiera de estas acciones:

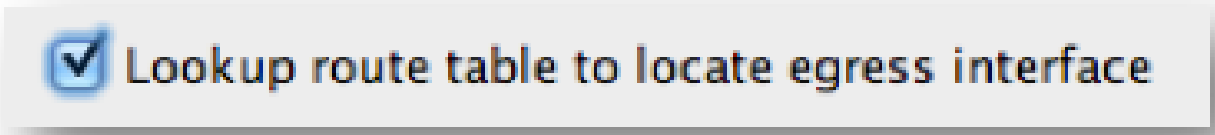
- Reordene la tabla NAT de modo que la entrada más específica aparezca en primer lugar.
- Utilice rangos de direcciones IP globales no superpuestos para las sentencias NAT.

Tenga en cuenta que si la regla NAT es una regla de identidad (lo que significa que la regla no cambia las direcciones IP), se puede utilizar la palabra clave route-lookup (esta palabra clave no es aplicable al ejemplo anterior, ya que la regla NAT no es una regla de identidad).

La palabra clave route-lookup hace que ASA realice una verificación adicional cuando coincide con una regla NAT. Comprueba que la tabla de ruteo del ASA reenvía el paquete a la misma interfaz de salida a la que esta configuración de NAT desvía el paquete.

Si la interfaz de salida de la tabla de ruteo no coincide con la interfaz de desvío NAT, la regla NAT no coincide (la regla se omite) y el paquete continúa hacia abajo en la tabla NAT para ser procesado por una regla NAT posterior.

La opción route-lookup sólo está disponible si la regla NAT es una regla de identidad NAT, lo que significa que la regla no cambia las direcciones IP. La opción route-lookup se puede habilitar por regla NAT si agrega route-lookup al final de la línea NAT, o si marca la casilla de verificación Lookup route table to locate egress interface en la configuración de regla NAT en ASDM:



Problema: Una regla NAT hace que ASA Proxy Address Resolution Protocol (ARP) para el tráfico en la interfaz asignada

Los ARP de proxy ASA para el rango de direcciones IP globales en una sentencia NAT en la interfaz global. Esta funcionalidad ARP de proxy se puede inhabilitar según la regla por NAT si agrega la palabra clave no-proxy-arp a la instrucción NAT.

Este problema también se observa cuando la subred de la dirección global se crea inadvertidamente para ser mucho más grande de lo que se pretendía.

Solución

Agregue la palabra clave no-proxy-arp a la línea NAT si es posible.

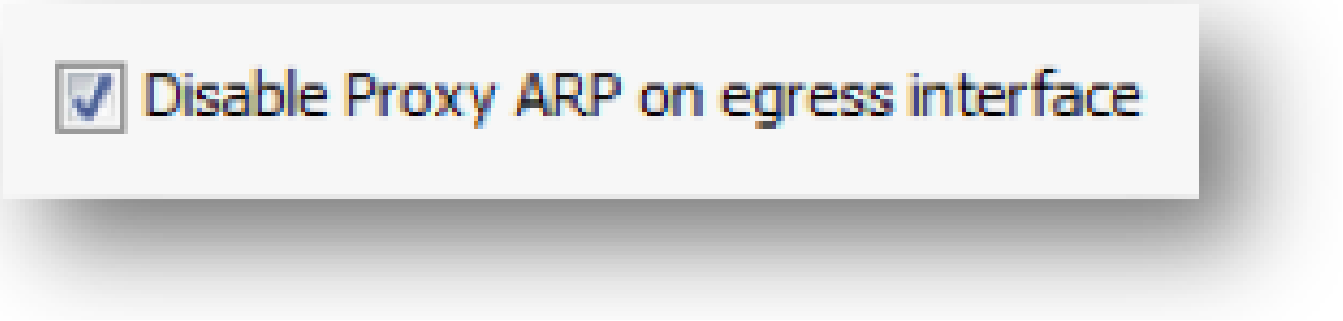
Ejemplo:

<#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#
```

Esto también se puede lograr con ASDM. Dentro de la regla NAT, marque la casilla de verificación Disable Proxy ARP on egress interface.



.

Información Relacionada

- VÍDEO: Reenvío de puertos ASA para acceso al servidor DMZ (versiones 8.3 y 8.4)
- Configuración básica de NAT de ASA: servidor web en la DMZ en ASA versión 8.3 y posteriores
- Libro 2: Guía de configuración CLI del firewall de la serie Cisco ASA, 9.1
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).