Troubleshooting de la configuración de la traducción de dirección de red ASA

Contenido

Introducción

Este documento describe cómo resolver problemas la configuración del Network Address Translation (NAT) en la plataforma adaptante del dispositivo de seguridad de Cisco (ASA). Este documento es válido para la Versión de ASA 8.3 y posterior.

> Nota: Para algunos ejemplos básicos de las configuraciones del NAT, que incluyen un vídeo que muestre una configuración del NAT básica, vea la información relacionada de la sección en la parte inferior de este documento.

Resuelva problemas la configuración del NAT en el ASA

Cuando usted resuelve problemas las configuraciones del NAT, es importante entender cómo la configuración del NAT en el ASA se utiliza para construir la tabla de la política NAT.

Estos errores de configuración explican a la mayoría de los problemas del NAT encontrados por los administradores ASA:

- Las reglas de la configuración del NAT están fuera de servicio. Por ejemplo, una regla manual NAT se pone en la cima de la tabla NAT, que causa reglas más específicas puso un plumón más lejano la tabla NAT nunca que se golpeará.
- Los objetos de red usados en la configuración del NAT son reglas más específicas demasiado amplias, que hace el tráfico hacer juego inadvertidamente estas reglas NAT, y falta NAT.

La utilidad del **trazalíneas del paquete** se puede utilizar para diagnosticar la mayoría de los problemas NAT-relacionados en el ASA. Vea la siguiente sección para más información sobre cómo la configuración del NAT se utiliza para construir la tabla de la política NAT, y cómo resolver problemas y resolver los problemas del NAT específicos.

Además, el **comando detail nacional de la demostración** puede ser utilizado para entender qué reglas NAT son golpeadas por las nuevas conexiones.

Cómo la configuración ASA se utiliza para construir la tabla de la política NAT

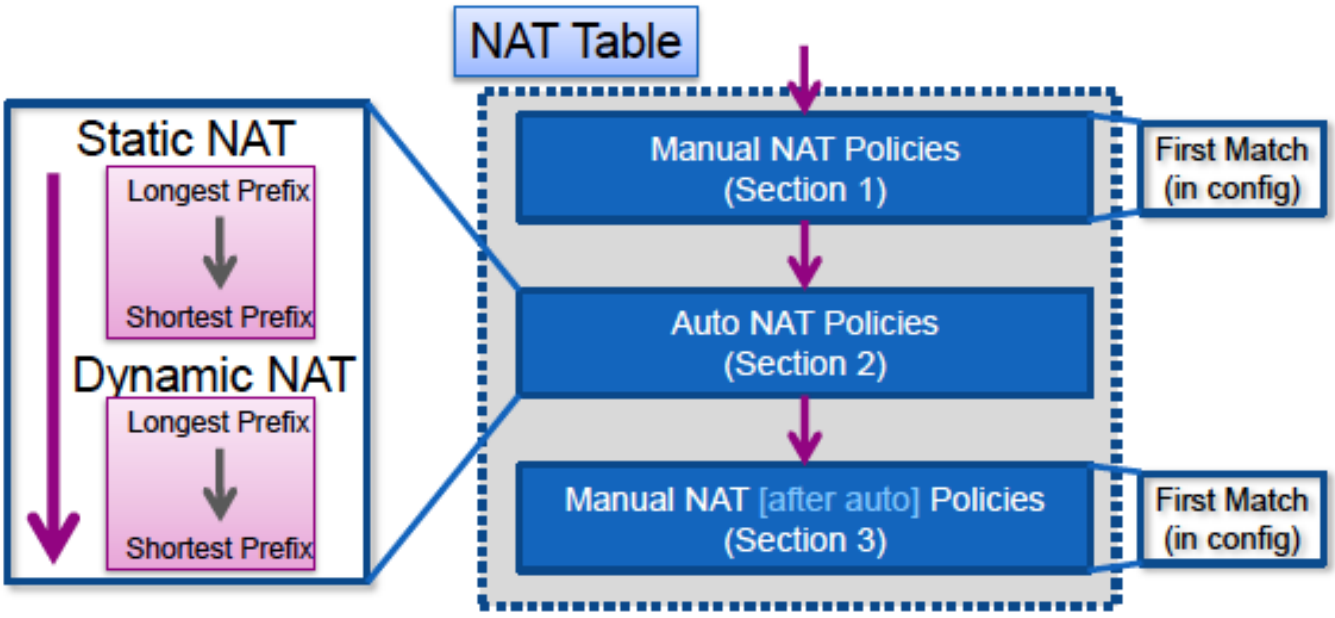
Todos los paquetes procesados por el ASA se evalúan contra la tabla NAT. Esta evaluación comienza en el top (sección 1) y trabajos abajo hasta que se corresponda con una regla NAT. Una vez que se corresponde con una regla NAT, esa regla NAT se aplica a la conexión y no más de políticas NAT se marcan contra el paquete.

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

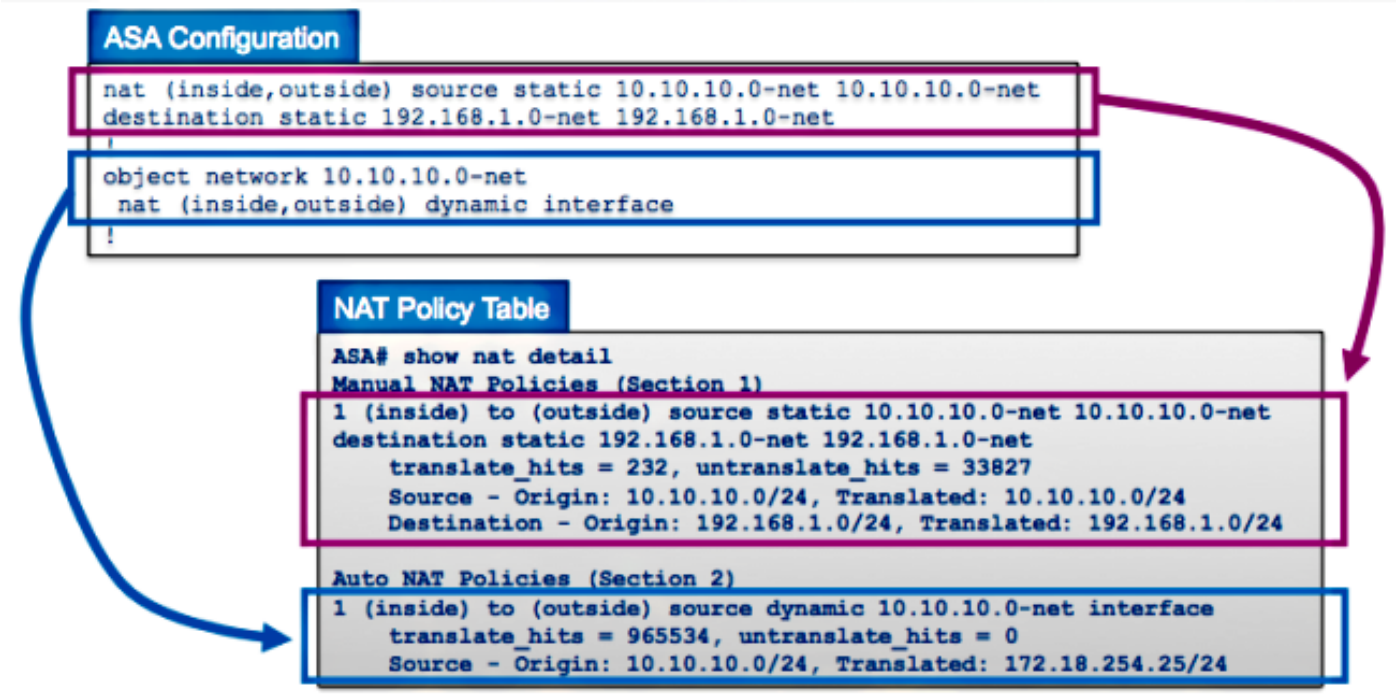
Las tres secciones de la tabla ASA NAT son:

Sección 1	**Políticas NAT manuales** Éstos se procesan en la orden en la cual aparecen en la configuración.
Sección 2	**Políticas NAT autos** Se procesan éstos basaron en el tipo NAT (estático o dinámico) y la longitud del prefijo (máscar subred) en el objeto.
Sección 3	**políticas NAT manuales Después-autos** Éstos se procesan en la orden en la cual aparecen en la configuración.

Este diagrama muestra las diversas secciones NAT y cómo se piden:



Este ejemplo muestra cómo la configuración del NAT ASA con dos reglas (una sentencia NAT manual y una configuración del NAT auto) se representa en la tabla NAT:



Cómo resolver problemas los problemas del NAT

Utilice la utilidad del trazalíneas del paquete

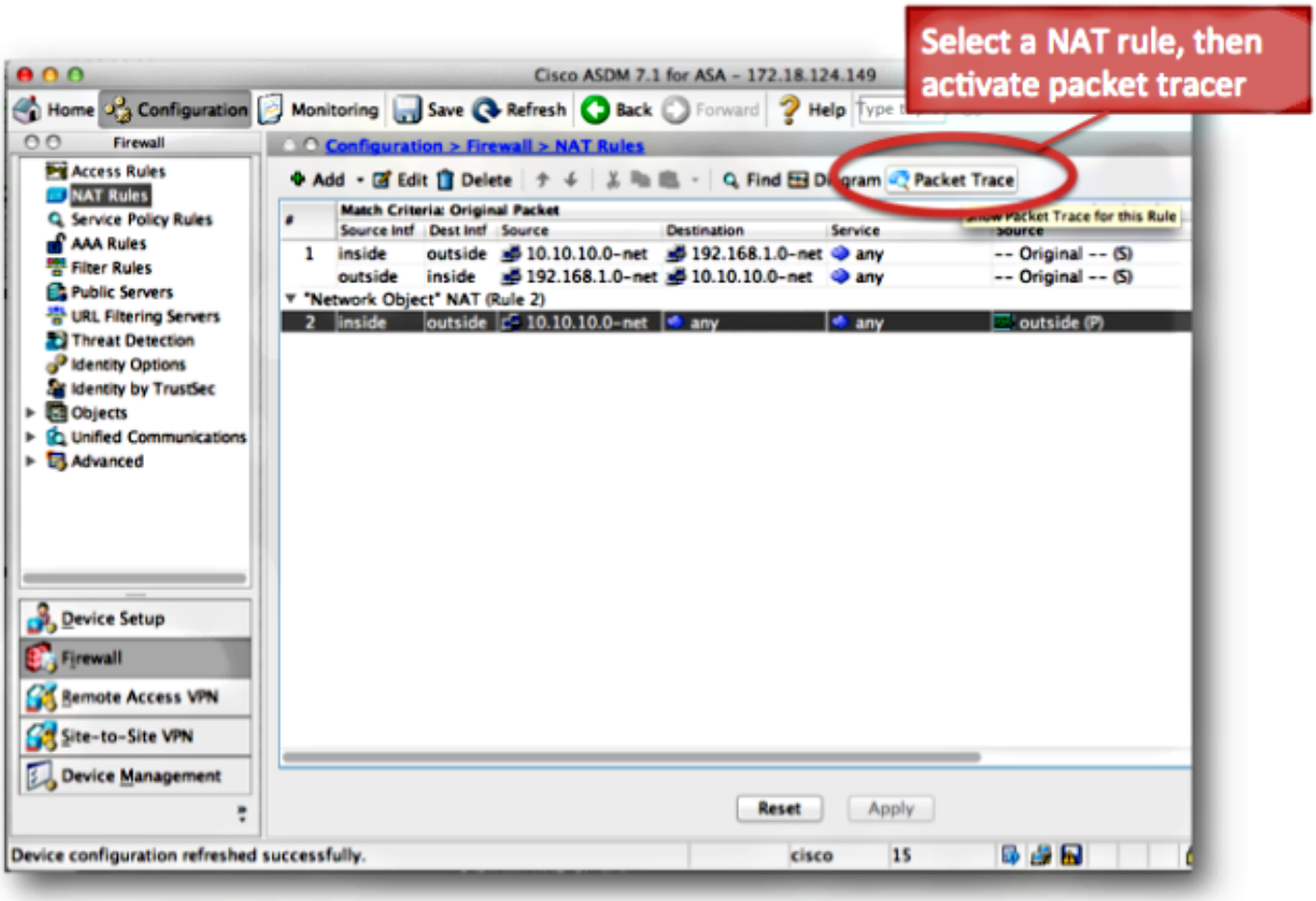
Para resolver problemas los problemas con las configuraciones del NAT, utilice la utilidad del **trazalíneas del paquete** para verificar que un paquete golpea la política NAT. El trazalíneas del paquete permite que usted especifique un paquete de la muestra que ingrese el ASA, y el ASA indica lo que se aplica la configuración al paquete y si se permite o no.

En el ejemplo abajo, se da un paquete TCP de la muestra que ingresa la interfaz interior y se

destina a un host en el Internet. La utilidad del trazalíneas del paquete muestra que el paquete hace juego una regla dinámica NAT y está traducido al IP Address externo de **172.16.123.4**:

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 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#
```

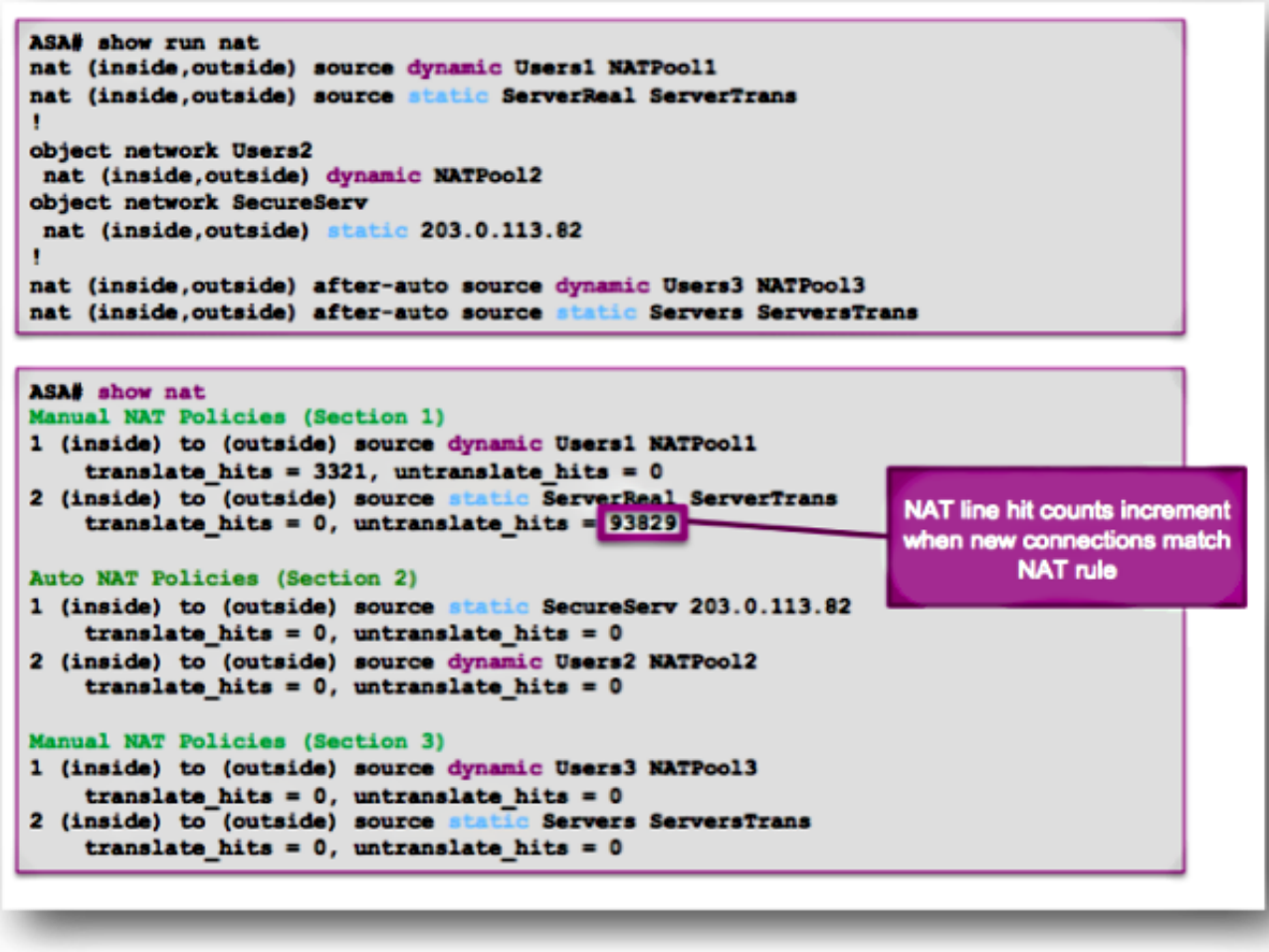
Elija la **regla NAT** y haga clic la **traza del paquete** para activar el trazalíneas del paquete del Cisco Adaptive Security Device Manager (ASDM). Esto utiliza los IP Addresses especificados en la regla NAT como las entradas para la herramienta del trazalíneas del paquete:



Vea la salida del comando show nat

La salida del **comando detail nacional de la demostración** se puede utilizar para ver la tabla de la política NAT. Específicamente, los **translate_hits** y los contadores de los **untranslate_hits** se pueden utilizar para determinar qué entradas de NAT se utilizan en el ASA. Si usted ve que su nueva regla NAT no tiene ningunos **translate_hits** o **untranslate_hits**, esos significa que o el tráfico no llega el ASA, o quizás una diversa regla que tiene una prioridad más alta en la tabla NAT hace juego el tráfico.

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



En el ejemplo anterior, hay seis reglas NAT configuradas en este ASA. La salida **nacional de la demostración** muestra cómo estas reglas se utilizan para construir la tabla de la política NAT, así como el número de **translate_hits** y de **untranslate_hits** para cada regla. Estos contadores de aciertos incrementan solamente una vez por la conexión. Después de que la conexión se construya con el ASA, los paquetes subsiguientes que hacen juego esa conexión actual no incrementan las líneas NAT (como las cuentas del golpe de la lista de acceso de la manera trabaje en el ASA).

Translate_hits: El número de nuevas conexiones que hacen juego la regla NAT en la dirección delantera.

La “dirección delantera” significa que la conexión fue construida con el ASA en dirección de las interfaces especificadas en la regla NAT. Si una regla NAT especificó que el servidor interior está traducido a la interfaz exterior, la pedido de las interfaces en la regla NAT es “nacional (dentro, afuera)…”; si ese servidor inicia una nueva conexión a un host en el exterior, el contador del **translate_hit** incrementa.

Untranslate_hits: El número de nuevas conexiones que hacen juego la regla NAT en la dirección inversa.

Si una regla NAT especifica que el servidor interior está traducido a la interfaz exterior, la pedido de las interfaces en la regla NAT es “nacional (dentro, afuera)…”; si un cliente en el exterior del ASA inicia una nueva conexión al servidor en el interior, el contador del **untranslate_hit** incrementa.

Una vez más si usted ve que su nueva regla NAT no tiene ningunos **translate_hits** o

untranslate_hits, ese significa que o el tráfico no llega el ASA, o quizás una diversa regla que tiene una prioridad más alta en la tabla NAT hace juego el tráfico.

Metodología de Troubleshooting del problema del NAT

Utilice el trazalíneas del paquete para confirmar que un paquete de la muestra hace juego la regla apropiada de la configuración del NAT en el ASA. Utilice el **comando detail nacional de la demostración** para entender se golpean qué reglas de la política NAT. Si una conexión hace juego una diversa configuración del NAT que esperada, resuelva problemas con estas preguntas:

- ¿Hay una diversa regla NAT que tome la precedencia sobre la regla NAT que usted pensó el tráfico para golpear?
- ¿Hay una diversa regla NAT con las definiciones del objeto que son demasiado amplias (la máscara de subred es demasiado corta, por ejemplo 255.0.0.0) que hace este tráfico hacer juego la regla incorrecta?
- ¿Son las políticas NAT manuales fuera de servicio, que las causas el paquete para hacer juego la regla incorrecta?
- ¿Es su regla NAT configurada incorrectamente, que las causas la regla para no hacer juego su tráfico?

Vea la siguiente sección para los problemas de ejemplo y las soluciones.

Problemas comunes con las configuraciones del NAT

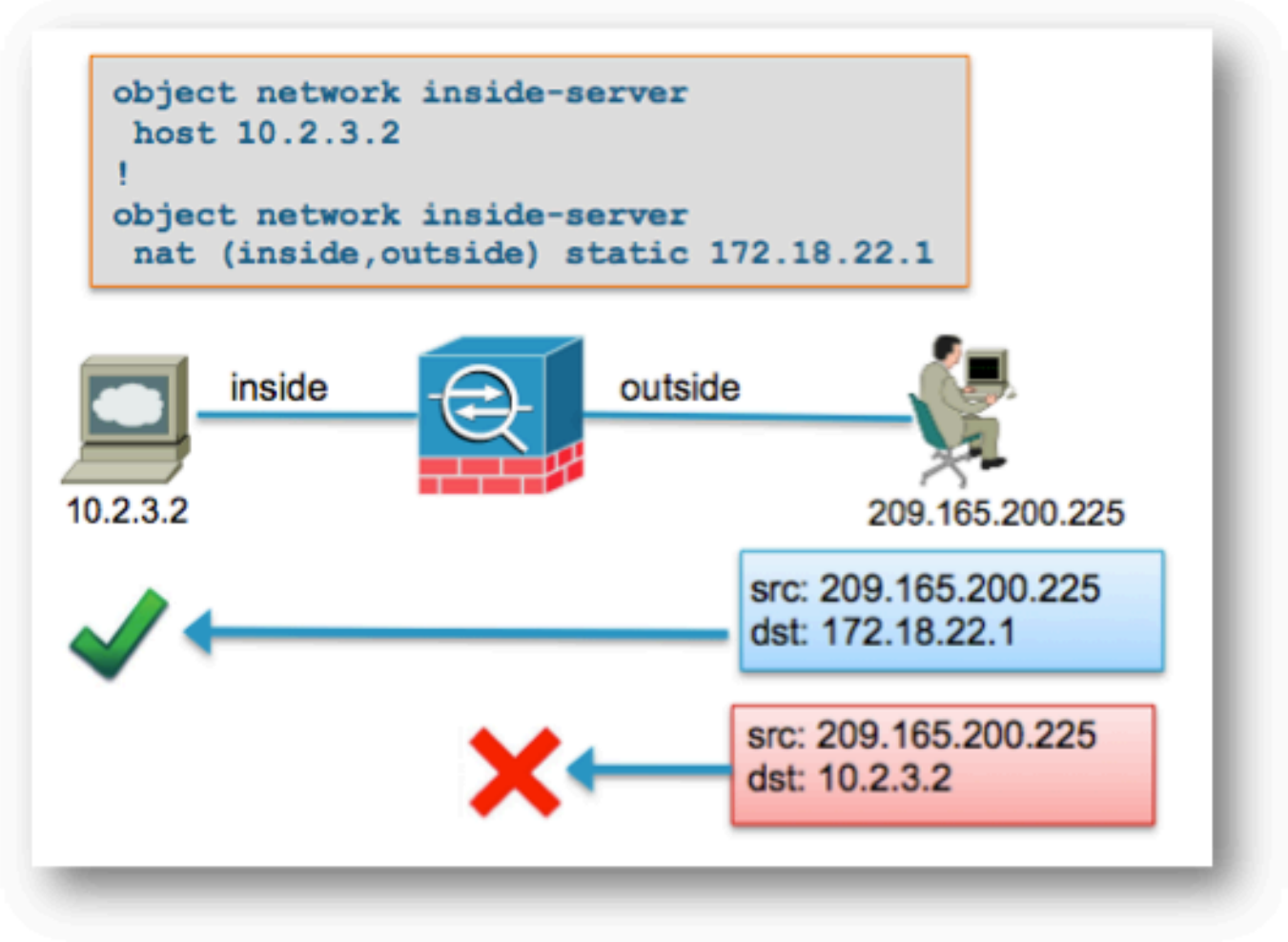
Aquí están algunos problemas comunes experimentados cuando usted configura el NAT en el ASA.

Problema: El tráfico falla debido al error del error del trayecto inverso NAT (RPF): Reglas asimétricas NAT correspondidas con para delantero y los flujos inversos

El NAT revisión de "RPF" se asegura de que una conexión que es traducida por el ASA en la dirección delantera, tal como el TCP sincronice (SYN), es traducido por la misma regla NAT en la dirección inversa, tal como el TCP SYN/acknowledge (ACK).

Lo más comúnmente posible, este problema es causado por las conexiones hacia adentro destinadas al direccionamiento (sin traducir) local en una sentencia NAT. En un nivel básico, el NAT RPF verifica que la conexión inversa del servidor al cliente haga juego la misma regla NAT; si no hace, el NAT revisión de "RPF" falla.

Ejemplo:



Cuando el host exterior en **209.165.200.225** envía un paquete destinado directamente a la dirección IP (sin traducir) local de **10.2.3.2**, el ASA cae el paquete y registra este Syslog:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:209.165.200.225 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 al direccionamiento global correcto NAT. Si el host envía los paquetes destinados a la dirección correcta, marque las reglas NAT que son golpeadas por la conexión. Verifique que las reglas NAT estén definidas correctamente, y que los objetos referidos a las reglas NAT están correctos. También verifique que la orden de las reglas NAT sea apropiada.

Utilice la utilidad del trazalíneas del paquete para especificar los detalles del paquete negado. El trazalíneas del paquete debe mostrar el paquete perdidos debido revisión de "RPF" al error. Después, la mirada en la salida del trazalíneas del paquete para considerar qué NAT gobierna se golpea en la fase NAT y la fase NAT-RPF.

Si un paquete hace juego una regla NAT en la fase NAT revisión de "RPF", que indica que el flujo inverso golpearía una traducción de NAT, pero no hace juego una regla en la fase NAT, que indica que el flujo delantero no golpearía una regla NAT, se cae el paquete.

Esta salida hace juego el escenario mostrado en el diagrama anterior, donde el host exterior envía incorrectamente el tráfico al IP Address local del servidor y no de la dirección IP (traducida) global:

```
ASA# packet-tracer input outside tcp 209.165.200.225 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 se destina a la dirección IP asociada correcta de 172.18.22.1, el paquete hace juego la regla correcta NAT en la fase UN-NAT en la dirección delantera, y la misma regla en la fase NAT revisión de "RPF":

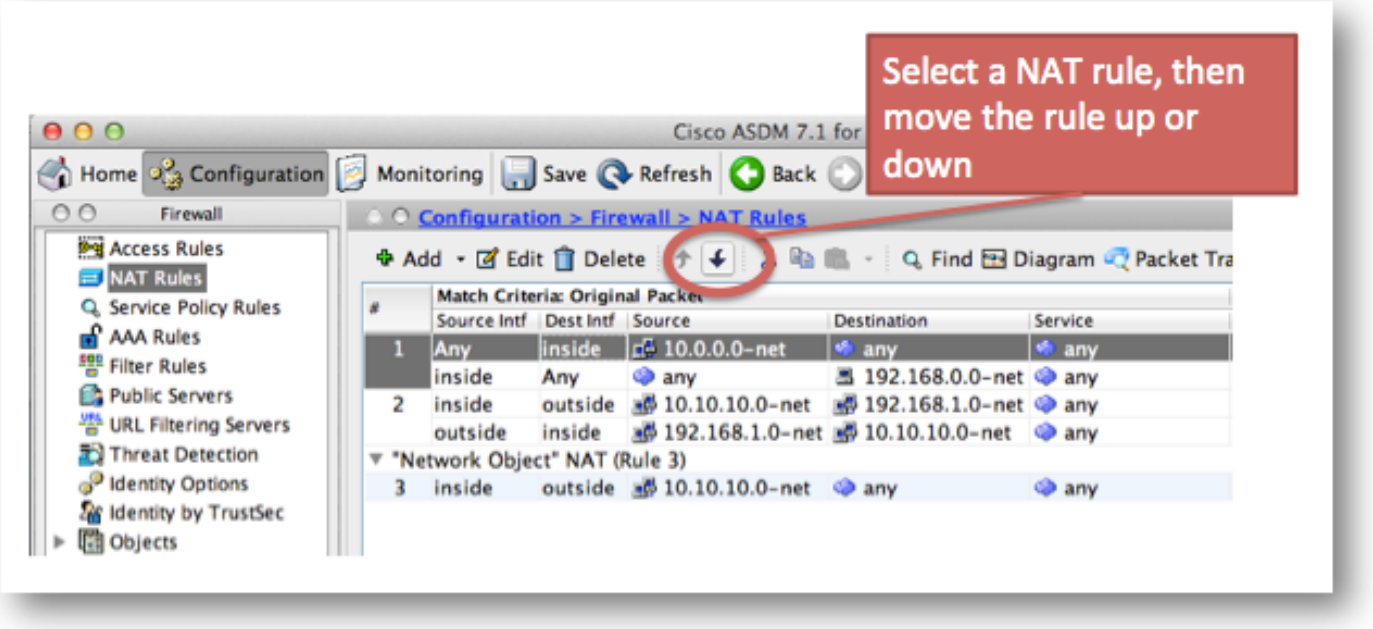
```
ASA(config)# packet-tracer input outside tcp 209.165.200.225 1234 172.18.22.1 80
...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 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 manuales NAT están fuera de servicio, que causa las coincidencias del paquete incorrecto

Se procesan las reglas manuales NAT basaron en su aspecto en la configuración. Si una regla muy amplia NAT se enumera primero en la configuración, puede ser que reemplace otra, una regla más específica más lejos abajo en la tabla NAT. Utilice el trazalíneas del paquete para verificar que la regla NAT su tráfico golpea; puede ser que sea necesario cambiar las entradas de NAT manuales a una diversa orden.

Solución:

Reordene las reglas NAT con el ASDM.



Solución:

Las reglas NAT se pueden reordenar con el CLI si usted quita la regla y la reinserta en un número de línea específico. Para insertar una nueva regla en una línea específica, ingrese el número de línea enseguida después que se especifican las interfaces.

Ejemplo:

```
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 hace juego un cierto tráfico inadvertidamente

Las reglas NAT se crean a veces que utilizan los objetos que son demasiado amplios. Si estas reglas se ponen cerca del top de la tabla NAT (en la cima de la sección 1, por ejemplo), puede ser que hagan juego más tráfico que previsto y hagan las reglas NAT más lejos abajo de la tabla nunca ser golpeadas.

Solución:

Utilice el trazalíneas del paquete para determinar si su tráfico corresponde con una regla con las definiciones del objeto que son demasiado amplias. Si éste es el caso, usted debe reducir el alcance de esos objetos, o mueva las reglas más lejos abajo de la tabla NAT, o a la sección después-auto (sección 3) de la tabla NAT.

Problema: Una regla NAT desvía el tráfico a una interfaz incorrecta

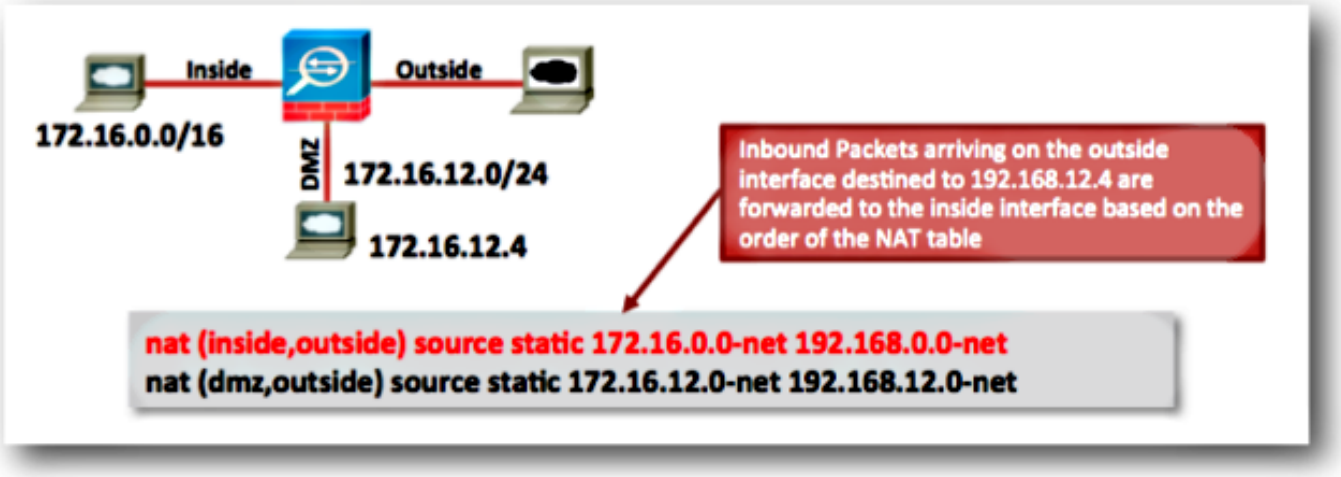
Las reglas NAT pueden tomar la precedencia sobre la tabla de ruteo cuando determinan que interconectan un paquete salida el ASA. Si un paquete de entrada corresponde con un IP Address traducido en una sentencia NAT, la regla NAT se utiliza para determinar la interfaz de egreso.

El NAT desvía los controles del control (que es qué puede reemplazar la tabla de ruteo) para ver

si hay cualquier regla NAT que especifique la traducción de la dirección destino para un paquete de entrada que llegue en una interfaz. Si hay no se consulta ninguna regla que especifica explícitamente cómo traducir el IP Address de destino, después la tabla de Global Routing de ese paquete para determinar la interfaz de egreso. Si hay una regla que especifica explícitamente cómo traducir el IP Address de destino de los paquetes, después la regla NAT "tira" del paquete a la otra interfaz en la traducción y la tabla de Global Routing se desvía con eficacia.

Este problema se considera lo más a menudo posible para el tráfico entrante, que llega en la interfaz exterior, y es generalmente debido a las reglas fuera de servicio NAT que desvían el tráfico a las interfaces involuntarias.

Ejemplo:



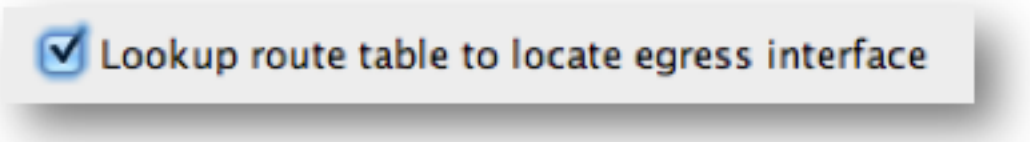
Soluciones:

Este problema se puede resolver con cualquiera de estas acciones:

- Reordene la tabla NAT para enumerar más la entrada específica primero.
- Utilice los rangos de IP Address global sin traslapo para las sentencias NAT.

Observe que si la regla NAT es una regla de la identidad, (que significa que los IP Addresses no son cambiados por la regla) entonces la palabra clave de las ruta-**operaciones de búsqueda** puede ser utilizada (esta palabra clave es no corresponde al ejemplo anterior puesto que la regla NAT no es una regla de la identidad). La palabra clave de las ruta-**operaciones de búsqueda** hace el ASA realizar un control adicional cuando hace juego una regla NAT. Marca que la tabla de ruteo del ASA adelante el paquete a la misma interfaz de egreso a la cual esta configuración del NAT desvía el paquete. Si la interfaz de egreso de la tabla de ruteo no hace juego el NAT desvía la interfaz, se salta la regla NAT no se corresponde con (la regla) y el paquete continúa abajo de la tabla NAT que se procesará por una regla posterior NAT.

La opción de las ruta-operaciones de búsqueda está solamente disponible si la regla NAT es una regla NAT de la "identidad", así que significa que los IP Addresses no son cambiados por la regla. La opción de las ruta-**operaciones de búsqueda** se puede habilitar por la regla NAT si usted agrega las ruta-**operaciones de búsqueda** al final de la línea NAT, o si usted marca la **tabla de ruta de las operaciones de búsqueda para localizar la** casilla de verificación de la **interfaz de egreso** en la configuración de la regla NAT en el ASDM:



Problema: Una regla NAT causa el ASA al (ARP) del protocolo proxy address resolution para el tráfico en la interfaz asociada

El proxy ARP ASA para el rango de IP Address global en una sentencia NAT en la interfaz global. Estas funciones del proxy ARP se pueden inhabilitar sobre una base de la regla por-NAT si usted agrega la palabra clave ninguno-proxy-**ARP a la** sentencia NAT.

Este problema también se considera cuando la subred de la dirección global se crea inadvertidamente para ser mucho más grande que él fue pensado ser.

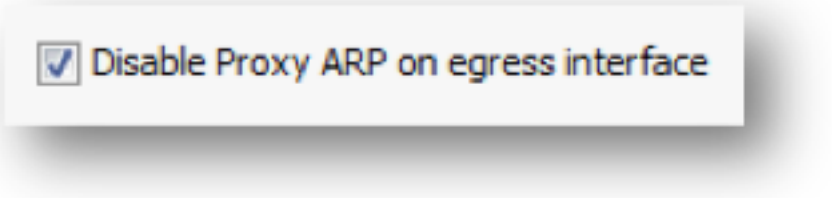
Solución:

Agregue la palabra clave ninguno-proxy-**ARP a la** línea NAT si es posible.

Ejemplo:

```
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 se puede también lograr con el ASDM. Dentro de la regla NAT, marque el **proxy ARP de la neutralización en la** casilla de verificación de la **interfaz de egreso**.



Información Relacionada

- VÍDEO: Expedición del puerto ASA para el acceso del servidor DMZ (versiones 8.3 y 8.4)
- Configuración del NAT básica ASA: Web server en el DMZ en la Versión de ASA 8.3 y posterior
- Libro 2: Guía de configuración CLI del Firewall de la serie de Cisco ASA, 9.1
- Soporte Técnico y Documentación - Cisco Systems