Ejemplo de Configuración de NAT y PAT Statement Use en Cisco Secure ASA Firewall

Contenido

Introducción

Este documento proporciona ejemplos de configuraciones básicas de traducción de direcciones de red (NAT) y traducción de direcciones de puerto (PAT) en el firewall Cisco Secure Adaptive Security Appliance (ASA). Este documento también proporciona diagramas de red simplificados. Consulte la documentación de ASA de su versión de software ASA para obtener información más detallada.

Este documento ofrece un análisis personalizado de su dispositivo Cisco.

Refiérase a Configuración de NAT en ASA en ASA 5500/5500-X Series Security Appliances para obtener más información.

Prerequisites

Requirements

Cisco recomienda que conozca el firewall Cisco Secure ASA.

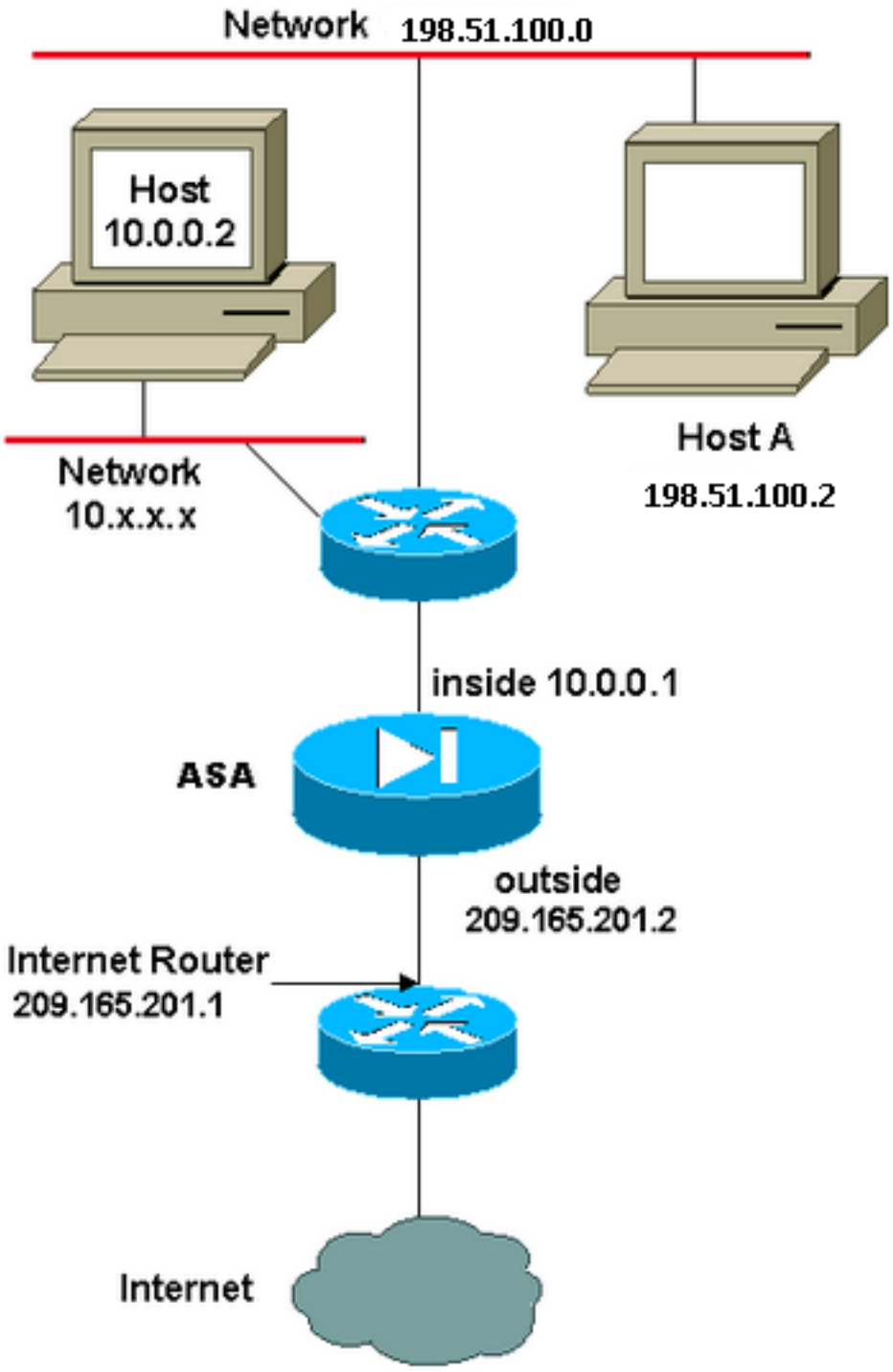
Componentes Utilizados

La información de este documento se basa en la versión 8.4.2 y posteriores del software Cisco Secure ASA Firewall.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuración - Varias sentencias NAT con NAT manual y automática

Diagrama de la red



En este ejemplo, el ISP proporciona al administrador de red un bloque de dirección IP 209.165.201.0/27 que va desde 209.165.201.1 a 209.165.201.30. El administrador de red decide asignar 209.165.201.1 a la interfaz interna en el router de Internet, y 209.165.201.2 a la interfaz exterior del ASA.

El administrador de red ya tiene una dirección de Clase C asignada a la red, 198.51.100.0/24, y tiene algunas estaciones de trabajo que utilizan estas direcciones para acceder a Internet. Estas estaciones de trabajo no requieren traducción de direcciones porque ya tienen direcciones válidas. Sin embargo, a las nuevas estaciones de trabajo se les asignan direcciones en la red 10.0.0.0/8 y deben traducirse (porque 10.x.x.x es uno de los espacios de direcciones no enrutables por RFC 1918 .

Para acomodar este diseño de red, el administrador de red debe utilizar dos sentencias NAT y un conjunto global en la configuración ASA:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Esta configuración no traduce a la dirección de origen de ningún tráfico saliente de la red 198.51.100.0/24. Traduce una dirección de origen en la red 10.0.0.0/8 a una dirección del rango 209.165.201.3 a 209.165.201.30.

> **Nota:** Cuando tiene una interfaz con una política NAT y si no hay un conjunto global a otra interfaz, necesita utilizar nat 0 para configurar la excepción NAT.

ASA Versión 8.3 y Posterior

Esta es la configuración.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

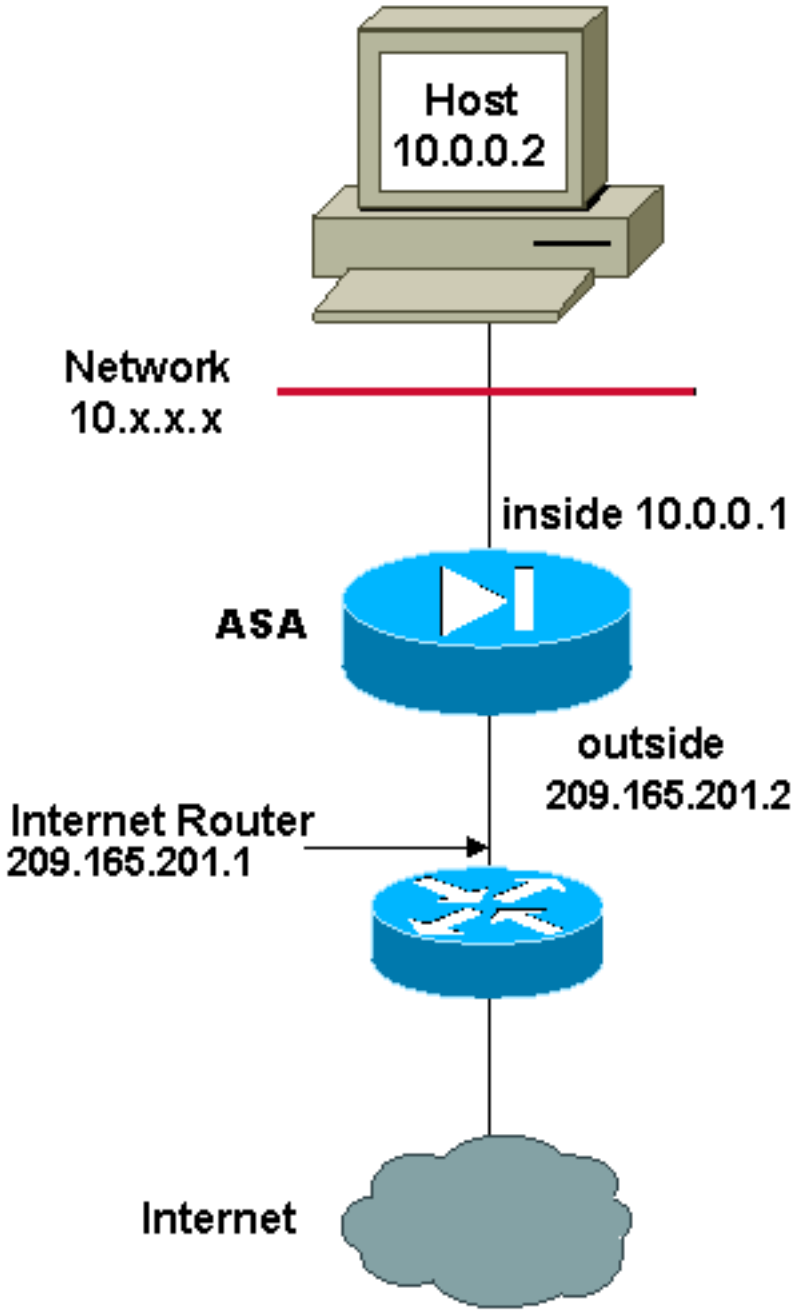
```
nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Configurar - Varios grupos globales

Diagrama de la red



En este ejemplo, el administrador de red tiene dos rangos de direcciones IP registradas en Internet. El administrador de la red debe convertir todas las direcciones internas, que están en el rango 10.0.0.0/8, en direcciones registradas. Los rangos de direcciones IP que debe utilizar el administrador de red son 209.165.201.1 a 209.165.201.30 y 209.165.200.225 a 209.165.200.25 4. El administrador de la red puede hacer esto con:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> **Nota:** Un esquema de direccionamiento comodín se utiliza en la sentencia NAT. Esta instrucción indica al ASA que traduzca cualquier dirección de origen interna cuando salga a Internet. La dirección de este comando puede ser más específica si se lo desea.

ASA Versión 8.3 y Posterior

Esta es la configuración.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

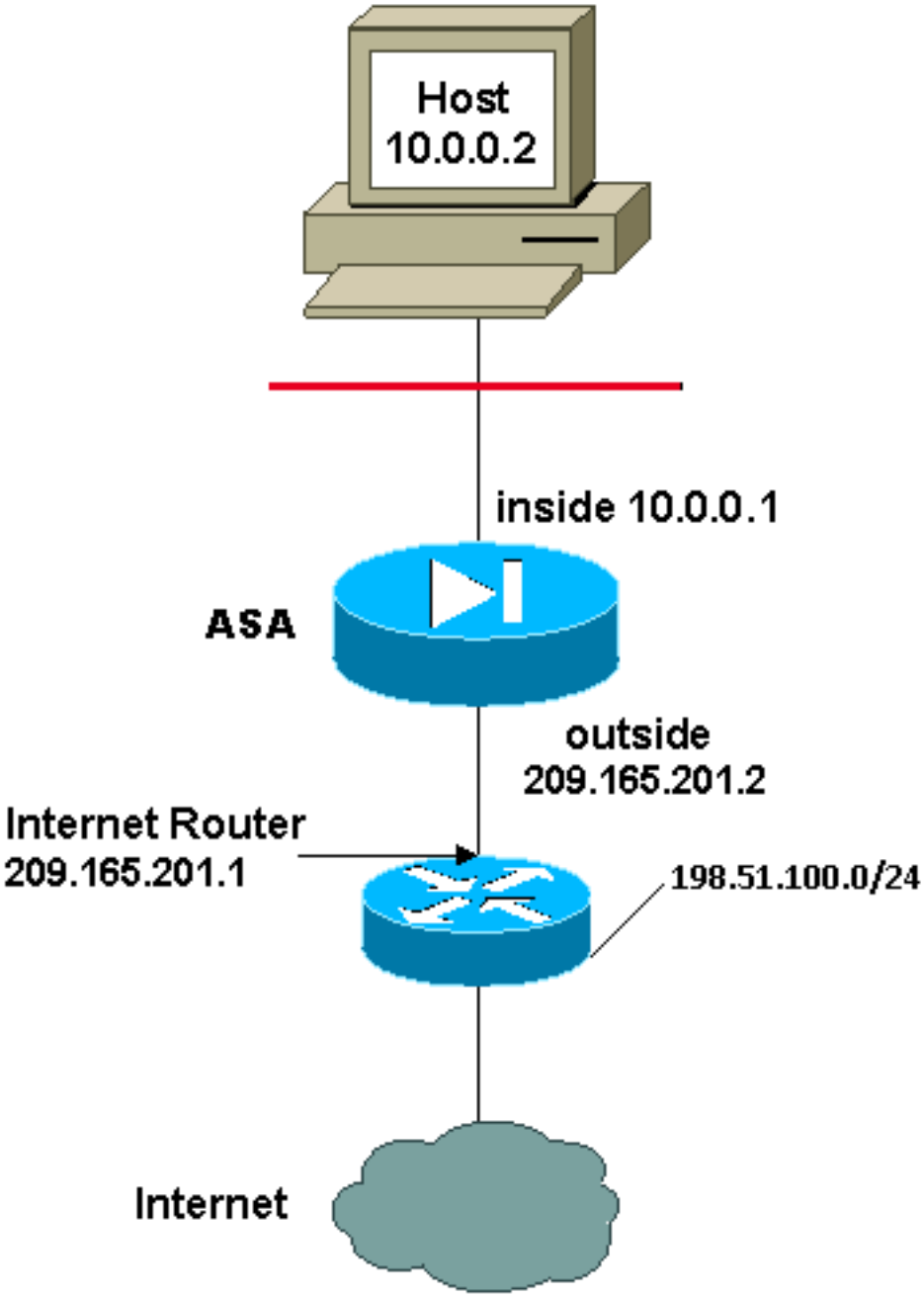
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

Using the Auto Nat statements:

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurar - Combinación de sentencias NAT y PAT

Diagrama de la red



En este ejemplo, el ISP proporciona al administrador de red un rango de direcciones entre 209.165.201.1 y 209.165.201.30 para que la compañía lo utilice. El administrador de red ha decidido utilizar 209.165.201.1 para la interfaz interna en el router de Internet y 209.165.201.2 para la interfaz exterior en el ASA. Luego se queda con 209.165.201.3 a 209.165.201.30 para utilizar para el conjunto NAT. Sin embargo, el administrador de red sabe que, en cualquier momento, puede haber más de 28 personas que intentan salir del ASA. El administrador de red ha decidido tomar 209.165.201.30 y convertirlo en una dirección PAT para que varios usuarios puedan compartir una dirección al mismo tiempo.

Estos comandos indican al ASA que traduzca la dirección de origen a 209.165.201.3 a 209.165.201.29 para que los primeros 27 usuarios internos pasen a través del ASA. Después de agotar estas direcciones, el ASA traduce todas las direcciones de origen subsiguientes a 209.165.201.30 hasta que una de las direcciones en el conjunto NAT se vuelva libre.

> **Nota:** Un esquema de direccionamiento comodín se utiliza en la sentencia NAT. Esta instrucción indica al ASA que traduzca cualquier dirección de origen interna cuando salga a

Internet. La dirección de este comando puede ser más específica si se lo desea.

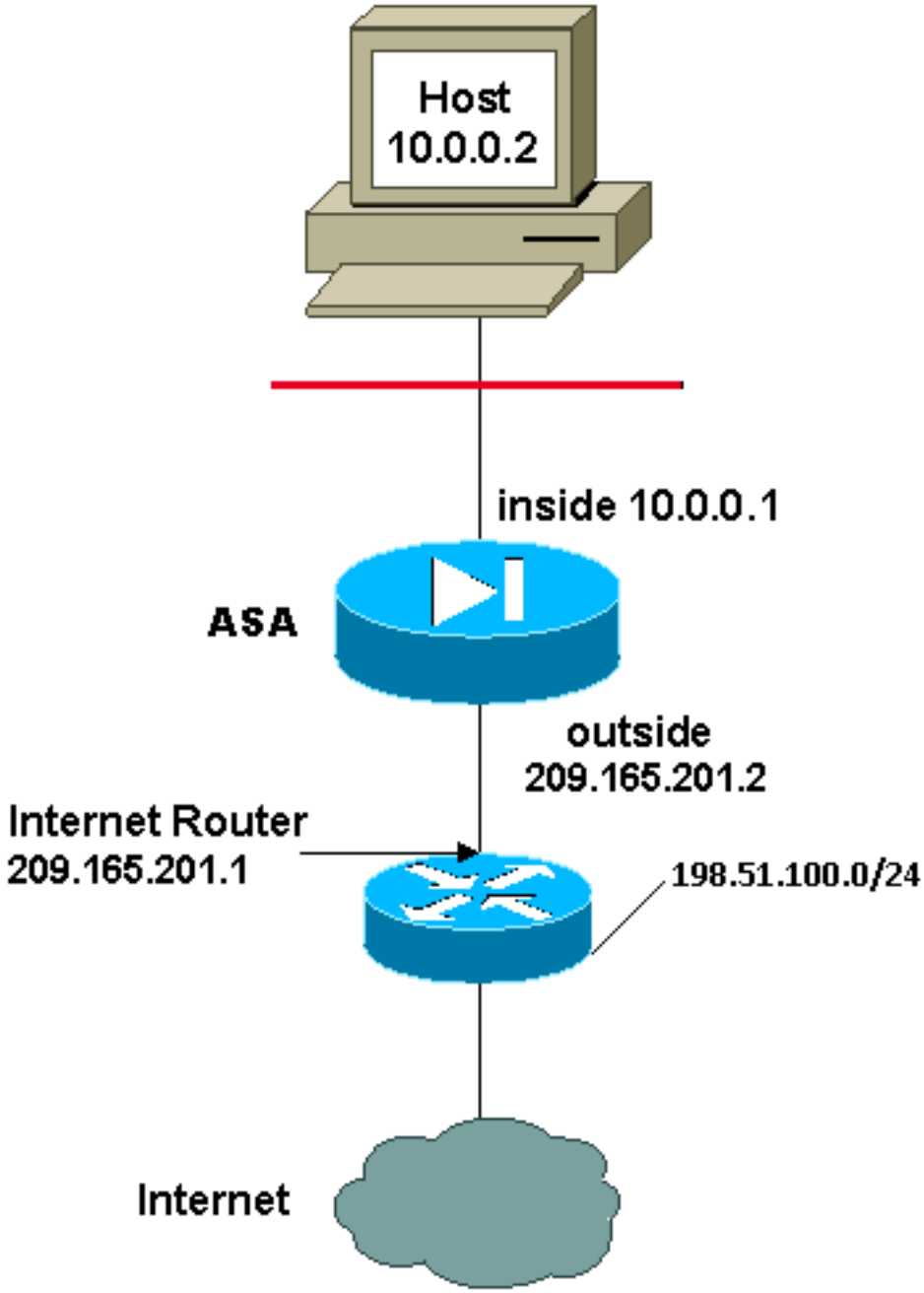
ASA Versión 8.3 y Posterior

Esta es la configuración.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configuración - Varias sentencias NAT con sentencias manuales

Diagrama de la red



En este ejemplo, el ISP proporciona de nuevo al administrador de red un rango de direcciones entre 209.165.201.1 y 209.165.201.30. El administrador de red decide asignar 209.165.201.1 a la interfaz interna en el router de Internet y 209.165.201.2 a la interfaz exterior del ASA.

Sin embargo, en este escenario, otro segmento LAN privado se coloca fuera del router de Internet. El administrador de red prefiere no malgastar las direcciones del conjunto global cuando los hosts de estas dos redes se comunican entre sí. El administrador de la red todavía necesita traducir la dirección de origen para todos los usuarios internos (10.0.0.0/8) cuando sale a Internet.

Esta configuración no traduce las direcciones con una dirección de origen de 10.0.0.0/8 y una dirección de destino de 198.51.100.0/24. Traduce la dirección de origen de cualquier tráfico iniciado dentro de la red 10.0.0.0/8 y destinado para cualquier lugar con excepción de 198.51.100.0/24 en una dirección del rango 209.165.201.3 con 209.165.201.30.

Si tiene la salida de un comando **write terminal de su dispositivo Cisco, puede utilizar Output Interpreter Tool (clientes registrados solamente).**

ASA Versión 8.3 y Posterior

Esta es la configuración.

Using the Manual Nat statements:

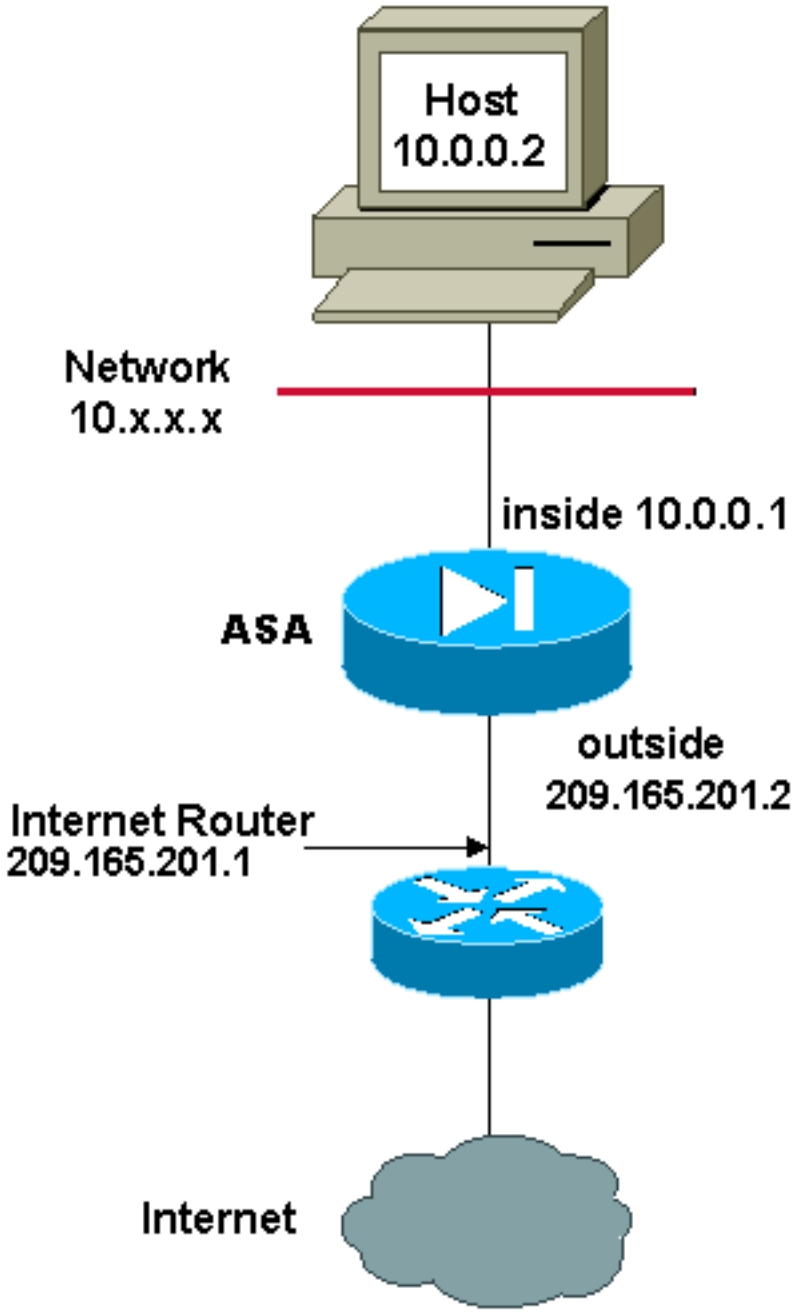
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Configurar - Usar política NAT

Diagrama de la red



Cuando utiliza una lista de acceso con el comando **nat** para cualquier ID NAT que no sea 0, habilita la política NAT.

La política NAT permite identificar el tráfico local para la traducción de direcciones mediante la especificación de las direcciones de origen y de destino (o puertos) en una lista de acceso. La NAT normal utiliza sólo direcciones de origen/puertos. La política NAT utiliza tanto las direcciones de origen como los puertos de destino.

> **Nota:** Todos los tipos de política de soporte NAT a excepción de la exención de NAT (nat 0 access-list). La exención de NAT utiliza una lista de control de acceso (ACL) para identificar las direcciones locales, pero difiere de la política NAT porque los puertos no se consideran.

Con la política NAT, puede crear múltiple NAT o sentencias estáticas que identifican la misma dirección local siempre que las combinaciones origen /puerto y destino /puerto sean únicas para cada sentencia. Puede hacer coincidir diversas direcciones globales a cada par origen /puerto y destino /puerto.

En este ejemplo, el administrador de red debe proporcionar acceso para la dirección IP de destino 172.30.1.11 para el puerto 80 (web) y el puerto 23 (Telnet), pero debe utilizar dos direcciones IP diferentes como dirección de origen. 209.165.201.3 se utiliza como dirección de origen para la Web y 209.165.201.4 se utiliza para Telnet y debe convertir todas las direcciones internas, que se encuentran en el rango 10.0.0.0/8. El administrador de la red puede hacer esto con:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

ASA Versión 8.3 y Posterior

Esta es la configuración.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> **Nota:** Para obtener más información sobre la configuración de NAT y PAT en ASA versión 8.4, consulte Información sobre NAT.
>
> Para obtener más información sobre la configuración de las listas de acceso en ASA versión 8.4, refiérase a Información sobre Listas de Acceso.

Verificación

Intente acceder a un sitio web a través de HTTP con un navegador web. Este ejemplo utiliza un

sitio alojado en 198.51.100.100. Si la conexión se realiza correctamente, se puede ver el resultado de la siguiente sección en la CLI de ASA.

Conexión

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
flags UIO
```

El ASA es un firewall con información de estado y se permite el retorno del tráfico desde el servidor web a través del firewall porque coincide con una ***conexión*** en la tabla de conexión del firewall. El tráfico que coincide con una conexión que existe previamente se permite a través del firewall sin ser bloqueado por una ACL de interfaz.

En la salida anterior, el cliente de la interfaz interna estableció una conexión con el host 198.51.100.100 fuera de la interfaz externa. Esta conexión se realiza con el protocolo TCP y ha estado inactiva durante seis segundos. Los indicadores de conexión indican el estado actual de esta conexión. Puede encontrar más información sobre los indicadores de conexión en Indicadores de conexión TCP de ASA.

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.0.0.2/57431 (209.165.201.3/57431)
```

El firewall de ASA genera syslogs durante el funcionamiento normal. El nivel de detalle de los syslogs depende de la configuración de registro. El resultado muestra dos syslogs que se ven en el nivel seis, o nivel **'informativo'**.

En este ejemplo, se generan dos syslogs. El primero es un mensaje de registro que indica que el firewall ha creado una **traducción**, específicamente una traducción TCP dinámica (PAT). Indica la dirección IP de origen y el puerto y la dirección IP traducida a medida que el tráfico atraviesa desde el interior a las interfaces externas.

El segundo syslog indica que el firewall ha creado una conexión en su tabla de conexiones para este tráfico específico entre el cliente y el servidor. Si el firewall se configuró para bloquear este intento de conexión, o algún otro factor inhibió la creación de esta conexión (restricciones de recursos o una posible configuración incorrecta), el firewall no generaría un registro que indique que la conexión se creó. En su lugar, registraría una razón para que se negara la conexión o una indicación sobre qué factor impedía que se creara la conexión.

Traducciones NAT (Xlate)

```
ASA(config)# show xlate local 10.0.0.2
```

```
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

Como parte de esta configuración, PAT se configura para traducir las direcciones IP del host interno a las direcciones que son enrutables en Internet. Para confirmar que se crean estas traducciones, puede verificar la tabla xlate (translation). El comando **show xlate,** cuando se combina con la palabra clave **local** y la dirección IP del host interno, muestra todas las entradas presentes en la tabla de traducción para ese host. La salida anterior muestra que hay una traducción actualmente construida para este host entre las interfaces interna y externa. La IP y el puerto del host interno se traducen a la dirección 10.165.200.226 por la configuración.

Los indicadores enumerados, **r i** , indican que la traducción es **dinámica** y un **mapa de puertos**. Se puede encontrar más información sobre las diferentes configuraciones de NAT en Información sobre NAT.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.