Uso de la declaración NAT y de la PALMADITA en el ejemplo seguro de la configuración de escudo de protección de Cisco ASA

Contenido

Introducción

Este documento proporciona las configuraciones del Network Address Translation (NAT) y del Port Address Translation (PAT) de los ejemplos de básico en el Firewall adaptante seguro del dispositivo de seguridad de Cisco (ASA). Este documento también proporciona los diagramas de red simplificada. Consulte la documentación ASA para su versión de software ASA para más información detallada.

Este documento ofrece un análisis personalizado de su dispositivo Cisco.

Refiera a la configuración del NAT en el ASA en los dispositivos de seguridad de las 5500/5500-X Series ASA para más información.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del Firewall seguro de Cisco ASA.

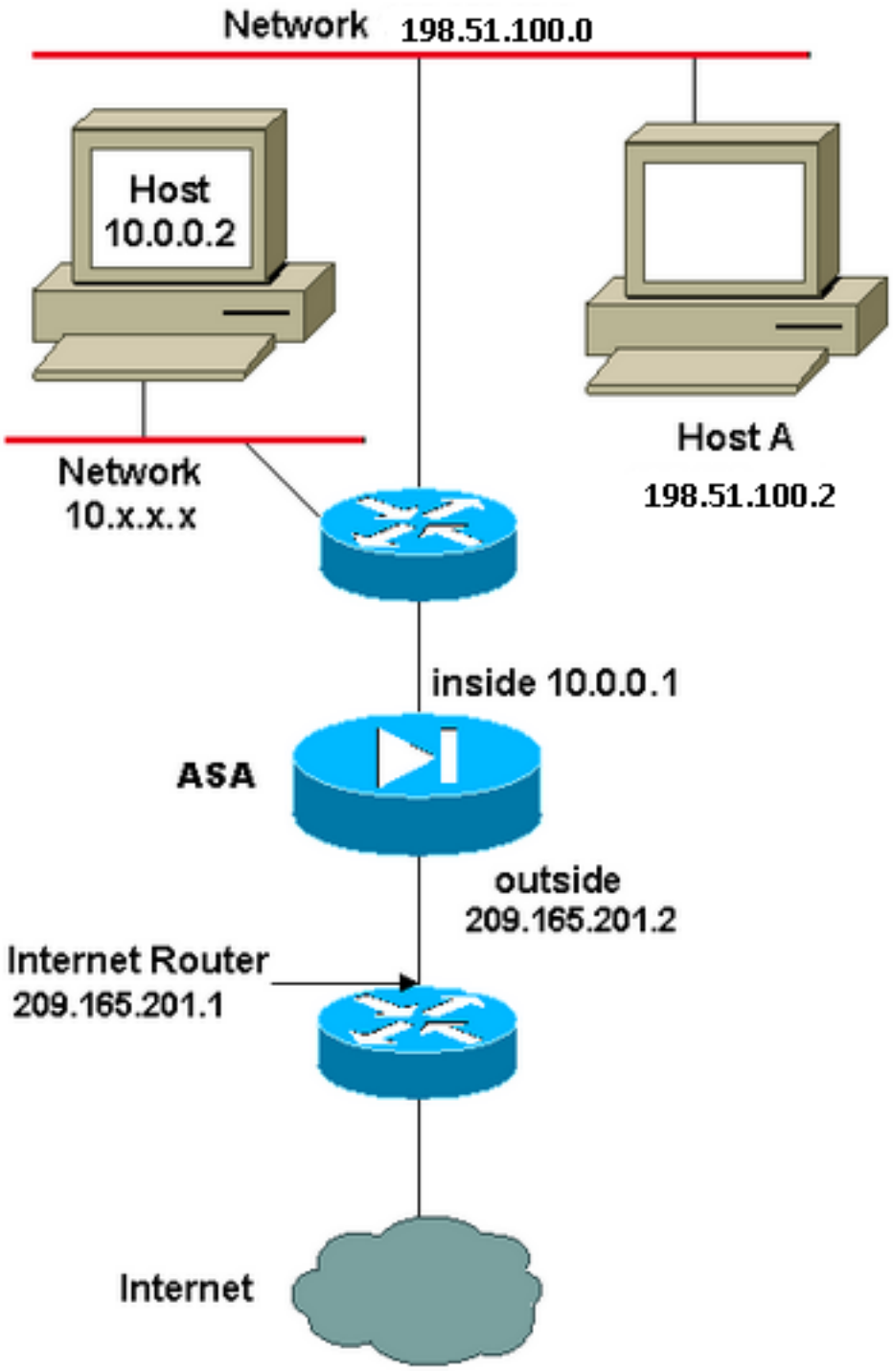
Componentes Utilizados

La información en este documento se basa en la versión 8.4.2 y posterior segura del software de firewall de Cisco ASA.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configuración - Declaraciones de NAT múltiples con el NAT manual y auto

Diagrama de la red



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

El administrador de la red tiene ya un direccionamiento del C de la clase asignado a la red, 198.51.100.0/24, y tiene algunos puestos de trabajo que utilicen estos direccionamientos para acceder Internet. Estos puestos de trabajo no requieren ninguna traducción de la dirección porque tienen ya las direcciones válidas. Sin embargo, las estaciones de trabajo nuevo se asignan los direccionamientos en la red 10.0.0.0/8 y necesitan ser traducidas (porque 10.x.x.x es uno de los espacios de la dirección unroutable por el RFC 1918.

Para acomodar este diseño de red, el administrador de la red debe utilizar dos sentencias NAT y a una agrupación 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 a una dirección de origen en la red 10.0.0.0/8 a un direccionamiento del rango 209.165.201.3 con 209.165.201.30.

> Nota: Cuando usted tiene una interfaz con una política NAT y si no hay agrupación global a otra interfaz, usted necesita utilizar 0 nacional para configurar la excepción NAT.

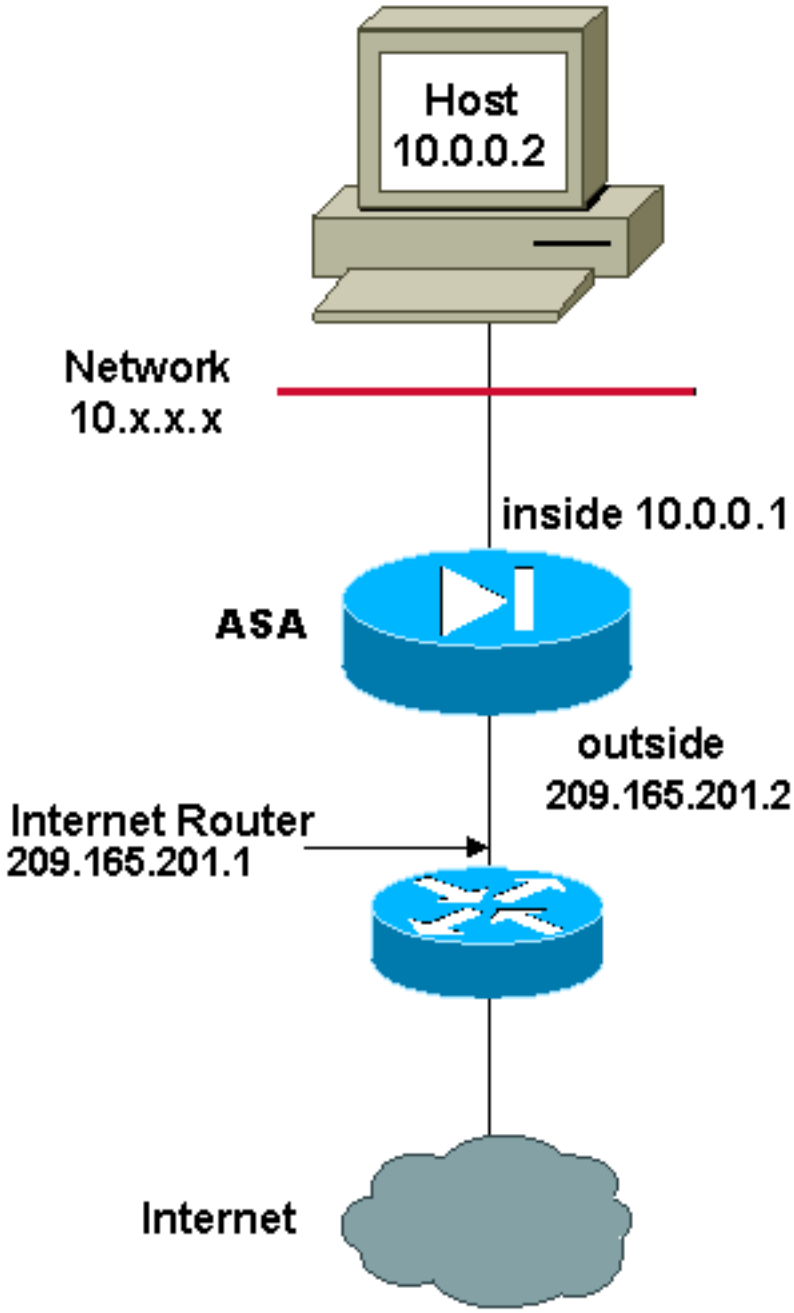
Versión de ASA 8.3 y posterior

Aquí está 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
```

Configuración - Agrupamientos globales múltiples

Diagrama de la red



En este ejemplo, el administrador de la red tiene dos rangos de los IP Addresses que se registren 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 los IP Addresses que el administrador de la red debe utilizar son 209.165.201.1 con 209.165.201.30 y 209.165.200.225 con 209.165.200.254. El administrador de la red puede hacer esto con:

```
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
```

> Nota: Un esquema de direccionamiento comodín se utiliza en la sentencia NAT. Esta declaración dice el ASA traducir a cualquier dirección de origen interna cuando sale a Internet. La dirección de este comando puede ser más específica si se lo desea.

Versión de ASA 8.3 y posterior

Aquí está 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:

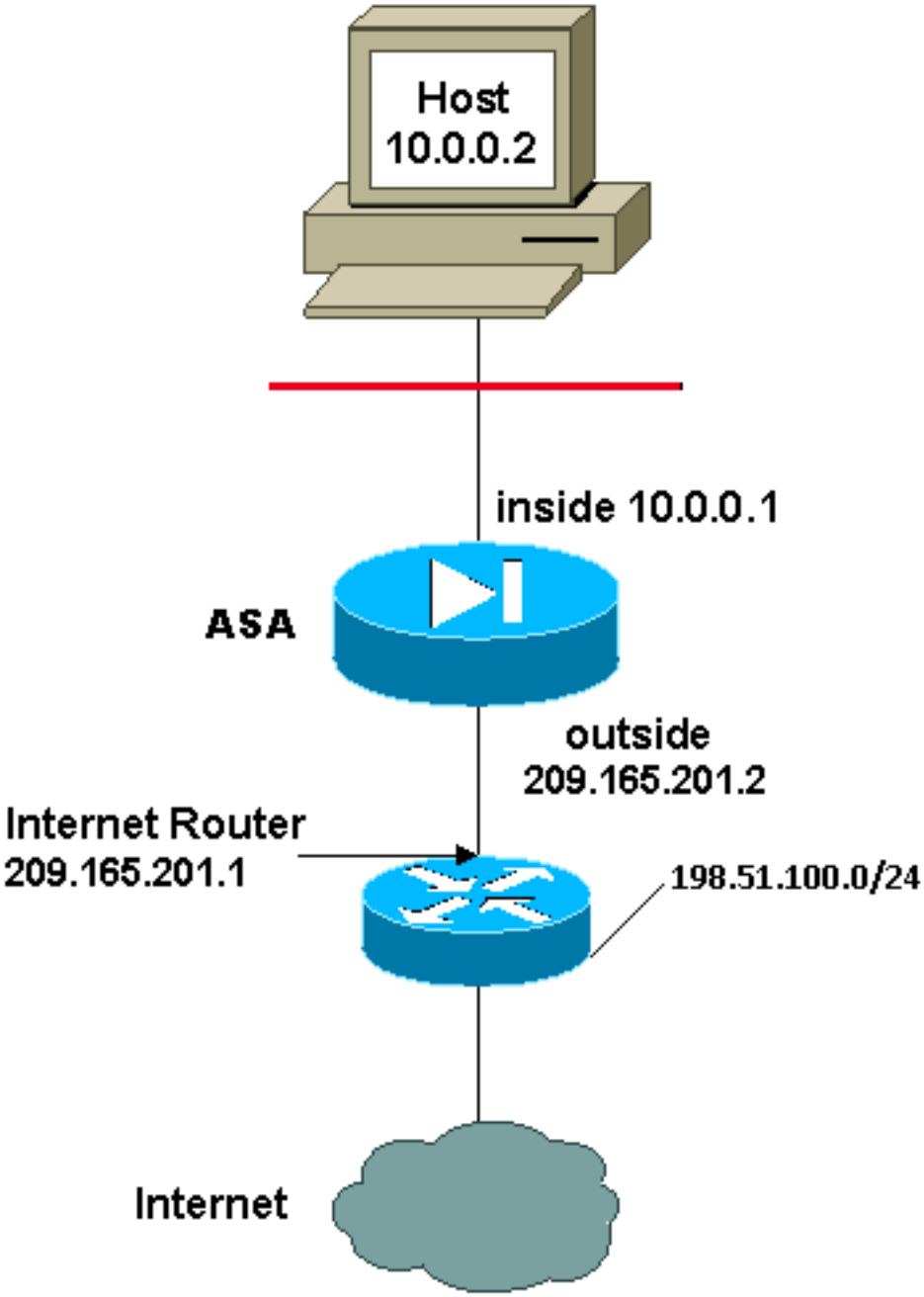
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

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
```

Configuración - Mezcla NAT y declaraciones de la PALMADITA

Diagrama de la red



En este ejemplo, el ISP proporciona al administrador de la red con un rango de direcciones de 209.165.201.1 a 209.165.201.30 para que la compañía utilice. El administrador de la red ha decidido utilizar 209.165.201.1 para la interfaz interior en el router de Internet y 209.165.201.2 para la interfaz exterior en el ASA. Le entonces dejan con 209.165.201.3 con 209.165.201.30 para utilizar para el agrupamiento NAT. Sin embargo, el administrador de la red sabe que, a cualquier momento, puede haber más de 28 personas que intentan salir del ASA. El administrador de la red ha decidido tomar 209.165.201.30 y hacerle un PAT Address de modo que los usuarios múltiples puedan compartir un direccionamiento al mismo tiempo.

Estos comandos dan instrucciones el ASA para traducir a la dirección de origen a 209.165.201.3 con 209.165.201.29 para que los primeros 27 usuarios internos pasen a través del ASA. Después de que se agoten estos direccionamientos, después el ASA traduce a todas las direcciones de origen subsiguientes a 209.165.201.30 hasta que se convierta uno de los direccionamientos en el agrupamiento NAT libremente.

Nota: Un esquema de direccionamiento comodín se utiliza en la sentencia NAT. Esta

declaración dice el ASA traducir a cualquier dirección de origen interna cuando sale a Internet. La dirección de este comando puede ser más específica si se lo desea.

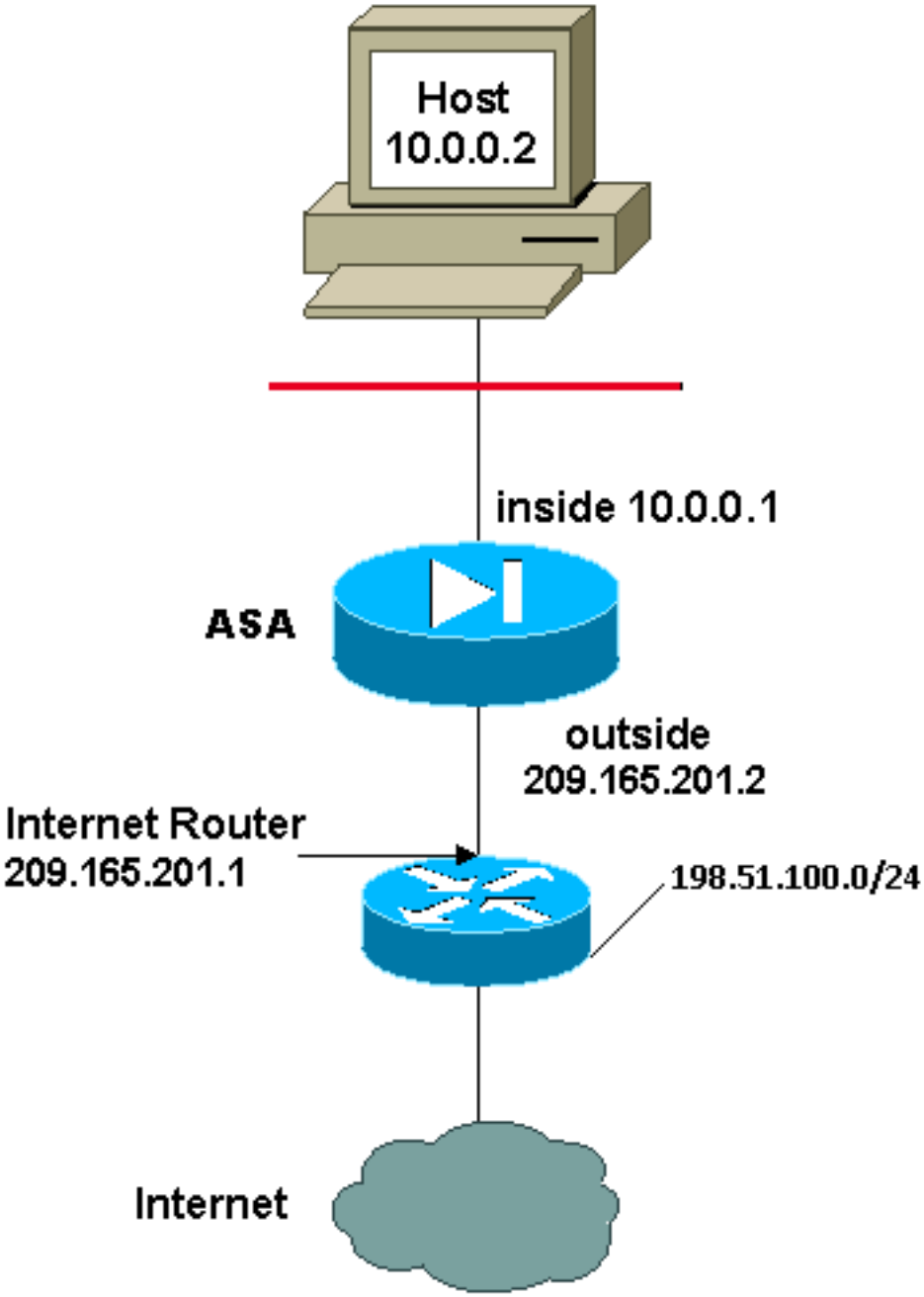
Versión de ASA 8.3 y posterior

Aquí está 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 - Declaraciones de NAT múltiples con las declaraciones manuales

Diagrama de la red



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

Sin embargo, en este escenario, otro segmento de LAN privado se pone apagado del router de Internet. El administrador de la red prefiere no perder los direccionamientos de la agrupación global cuando los host en estas dos redes hablan el uno al otro. El administrador de la red todavía necesita traducir a la dirección de origen para todos los usuarios internos (10.0.0.0/8) cuando sale a Internet.

Esta configuración no traduce esos direccionamientos con una dirección de origen de 10.0.0.0/8 y una dirección destino de 198.51.100.0/24. Traduce a la dirección de origen de cualquier tráfico iniciado dentro de la red 10.0.0.0/8 y destinado para dondequiera con excepción de 198.51.100.0/24 en un direccionamiento 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).

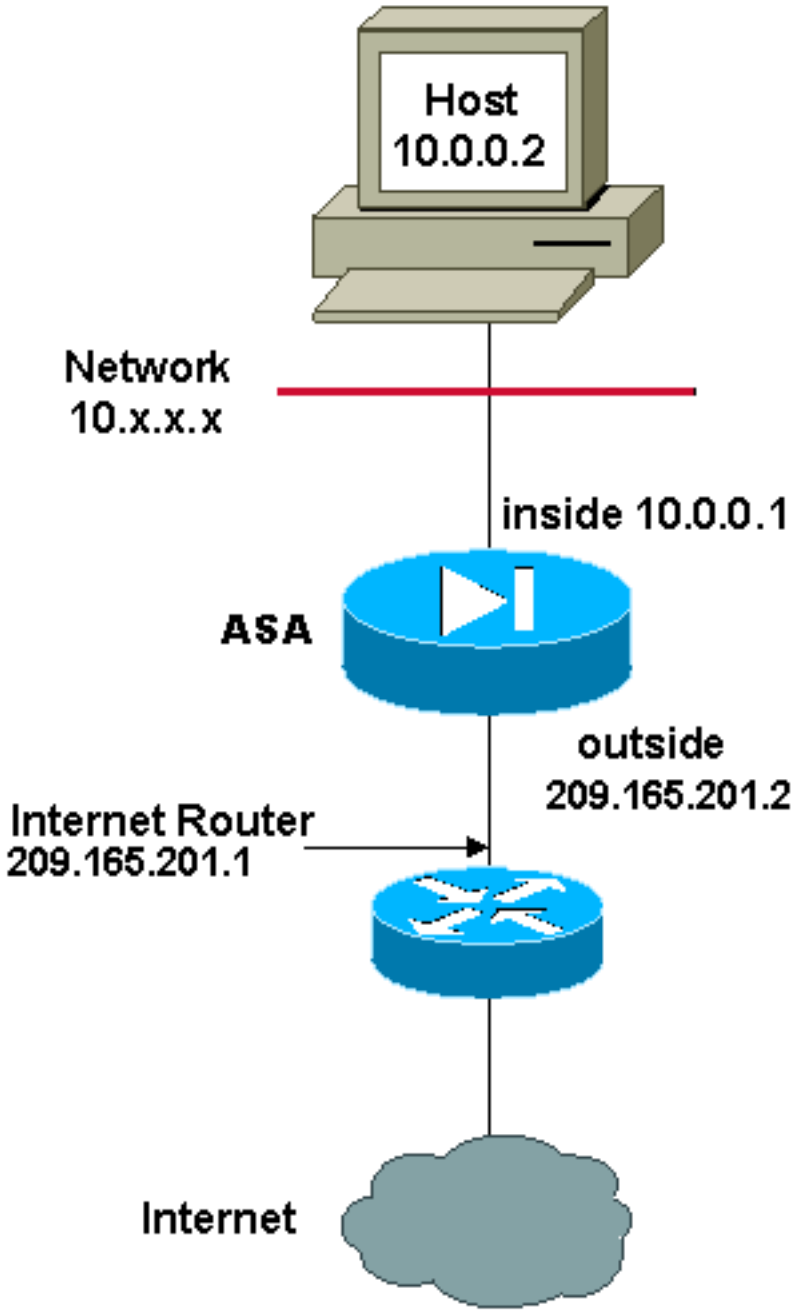
Versión de ASA 8.3 y posterior

Aquí está 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
```

Configuración - Utilice la directiva NAT

Diagrama de la red



Cuando usted utiliza una lista de acceso con el **comando nat** para cualquier IDENTIFICACIÓN NAT con excepción de 0, usted habilita la directiva NAT.

La directiva NAT permite que usted identifique el tráfico local para la traducción de la dirección por la especificación de las direcciones de origen y de destino (o de los puertos) en una lista de acceso. El NAT regular utiliza las direcciones de origen/los puertos solamente. La directiva NAT utiliza ambo las direcciones de origen y de destino/los puertos.

> 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 a las direcciones locales, pero diferencia de la directiva 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 la red tiene que proporcionar el acceso para el IP Address de destino 172.30.1.11 para el puerto 80 (red) y el puerto 23 (Telnet), pero debe utilizar dos diversos IP Addresses como dirección de origen. 209.165.201.3 se utiliza como utilizan a una dirección de origen para la red y 209.165.201.4 para Telnet, y debe convertir a todas las direcciones internas, que están en el rango 10.0.0.0/8. El administrador de la red puede hacer esto con:

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
```

Versión de ASA 8.3 y posterior

Aquí está 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 más información sobre la configuración del NAT y de la PALMADITA en la Versión de ASA 8.4, refiera a la información sobre el NAT.
>
> Para más información sobre la configuración de las Listas de acceso en la Versión de ASA 8.4, refiera a la información sobre las Listas de acceso.

Verificación

Intente acceder un sitio web vía el HTTP con un web browser. Este ejemplo utiliza un sitio que se reciba en 198.51.100.100. Si la conexión es acertada, la salida en la siguiente sección se puede considerar en el ASA CLI.

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 escudo de protección con estado, y el tráfico de retorno del servidor Web se permite detrás con el Firewall porque hace juego una ***conexión*** en la tabla de conexiones del Firewall. Trafique que hace juego una conexión que preexista se permita con el Firewall sin el bloqueo por una interfaz ACL.

En la salida anterior, el cliente en la interfaz interior ha establecido una conexión al host de 198.51.100.100 apagado de la interfaz exterior. Esta conexión se hace con el protocolo TCP y ha estado ociosa por seis segundos. Los indicadores de la conexión indican al estado actual de esta conexión. Más información sobre los indicadores de la conexión se puede encontrar en los indicadores de la conexión TCP 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 ASA genera los Syslog durante el funcionamiento normal. Los Syslog se extienden en la verbosidad basada en la configuración de registro. La salida muestra dos Syslog que se vean en el nivel seis, o el nivel **"informativo"**.

En este ejemplo, hay dos Syslog generados. El primer es un mensaje del registro que indica que el Firewall ha construido una **traducción**, específicamente una traducción dinámica TCP (PALMADITA). Indica la dirección IP de origen y el puerto y la dirección IP y el puerto traducidos mientras que el tráfico atraviesa del interior a las interfaces exteriores.

El segundo Syslog indica que el Firewall ha construido una **conexión** en su tabla de conexiones

para este tráfico específico entre el cliente y servidor. Si el Firewall fuera configurado para bloquear este intento de conexión, o un cierto otro factor inhibiera la creación de esta conexión (las restricciones de recursos o una posible configuración incorrecta), el Firewall no generaría un registro que indica que la conexión fue construida. En lugar registraría una razón de la conexión para ser negado o una indicación sobre qué factor inhibió la conexión de ser creado.

Traducciones de 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, la PALMADITA se configura para traducir los IP Addresses del host interno a los direccionamientos que son routable en Internet. Para confirmar que estas traducciones están creadas, usted puede marcar la tabla del xlate (traducción). El comando show xlate**,** cuando está combinado 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 construida actualmente para este host entre las interfaces interior y exterior. El IP del host interior y el puerto se traducen al direccionamiento de 10.165.200.226 por la configuración.

Los indicadores enumeraron, **r i**, indican que la traducción es **dinámica** y un **portmap**. Más información sobre diversas configuraciones del NAT se puede encontrar en la información sobre el NAT.

Troubleshooting

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