Configuración de traducción de direcciones de red y ACL en un firewall ASA

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Overview

- Objetivos
- Descripción general de la lista de control de acceso
- Descripción general de NAT

Configurar

- Introducción
- Topología
- Paso 1. Configuración de NAT para permitir que los hosts salgan a Internet
- Paso 2. Configuración de NAT para acceder al servidor web desde Internet
- Paso 3. Configurar ACL
- Paso 4. Probar configuración con la función Packet Tracer

Verificación

Troubleshoot

Conclusión

Introducción

Este documento describe cómo configurar la traducción de direcciones de red (NAT) y las listas de control de acceso (ACL) en un firewall ASA.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un firewall ASA 5510 que ejecuta código ASA versión 9.1(1).

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.

Antecedentes

Este documento describe un ejemplo simple y directo de cómo configurar NAT y ACL en un Firewall ASA para permitir la conectividad saliente y entrante. Se ha escrito con un firewall Adaptive Security Appliance (ASA) 5510 que ejecuta la versión de código ASA 9.1(1), pero esto se puede aplicar fácilmente a cualquier otra plataforma de firewall ASA. Si utiliza una plataforma como ASA 5505, que utiliza VLAN en lugar de una interfaz física, necesita cambiar los tipos de interfaz según corresponda.

Overview

Objetivos

En este ejemplo de configuración, puede ver qué configuraciones de NAT y ACL son necesarias para permitir el acceso entrante a un servidor web en la DMZ de un firewall ASA, y permitir la conectividad saliente desde hosts internos y DMZ. Esto puede resumirse en dos objetivos:

1. Permitir hosts en el interior y conectividad saliente de DMZ a Internet.
2. Permitir que hosts en Internet tengan acceso a un servidor web en la DMZ con una dirección IP 192.168.1.100.

Antes de realizar los pasos que deben completarse para lograr estos dos objetivos, este documento repasa brevemente la forma en que las ACL y NAT funcionan en las versiones más recientes del código ASA (versión 8.3 y posteriores).

Descripción general de la lista de control de acceso

Las listas de control de acceso (listas de acceso o ACL) son el método por el cual el firewall ASA determina si se autoriza o rechaza el tráfico. De manera predeterminada, se rechaza el tráfico que circula de un nivel de seguridad inferior a uno superior. Es posible anular esto aplicando una ACL a la interfaz de seguridad inferior. También de manera predeterminada, ASA permite el tráfico de interfaces de seguridad superiores a inferiores. También es posible anular este comportamiento con una ACL.

En versiones anteriores de código ASA (8.2 y anteriores), ASA comparaba una conexión o paquete entrante con la ACL en una interfaz, sin eliminar primero la traducción del paquete. En otras palabras, la ACL debía autorizar el paquete como si fuera a capturarse en la interfaz. A partir de la versión 8.3 del código, ASA elimina la traducción del paquete antes de que llegue a la ACL de la interfaz. Esto significa que, a partir del código 8.3 (y para este documento), se autoriza el tráfico al IP real del host, y no al IP traducido del host.

Consulte la sección Configuración de las Reglas de Acceso del Libro 2: Guía de Configuración de la CLI del Firewall de la Serie ASA de Cisco, 9.1 para obtener más información sobre las ACL.

Descripción general de NAT

A partir de la versión 8.3 de ASA, NAT se divide en dos tipos conocidos como NAT automática (NAT de objeto) y NAT manual (NAT doble). La primera de los dos (NAT de objeto) se configura en la definición de un objeto de red. Más adelante en este documento, se incluye un ejemplo de esto. Una ventaja principal de este método de NAT es que ASA ordena automáticamente las reglas de procesamiento para evitar conflictos. Esta es la forma más sencilla de NAT, pero esa facilidad conlleva una limitación en la granularidad de configuración. Por ejemplo, no es posible tomar una decisión de traducción en función del destino en el paquete, algo que sí es posible con el segundo tipo de NAT (NAT manual). La NAT manual es más sólida en su granularidad, pero requiere que las líneas estén configuradas en el orden correcto para que sea posible lograr el comportamiento adecuado. Esto complica este tipo de NAT y, como resultado, no se puede utilizar en este ejemplo de configuración.

Consulte la sección Información sobre NAT del Libro 2: Guía de configuración de la CLI del firewall de la serie Cisco ASA, 9.1 para obtener más información sobre NAT.

Configurar

Introducción

La configuración básica de ASA son tres interfaces conectadas a tres segmentos de red. El segmento de red del proveedor de internet (ISP) se conecta a la interfaz Ethernet0/0 y se etiqueta como externa con un nivel de seguridad de 0. La red interna se conecta a Ethernet0/1 y se etiqueta como interna con un nivel de seguridad de 100. El segmento DMZ, donde reside el servidor web, se conecta a Ethernet0/2 y se etiqueta como DMZ con un nivel de seguridad de 50.

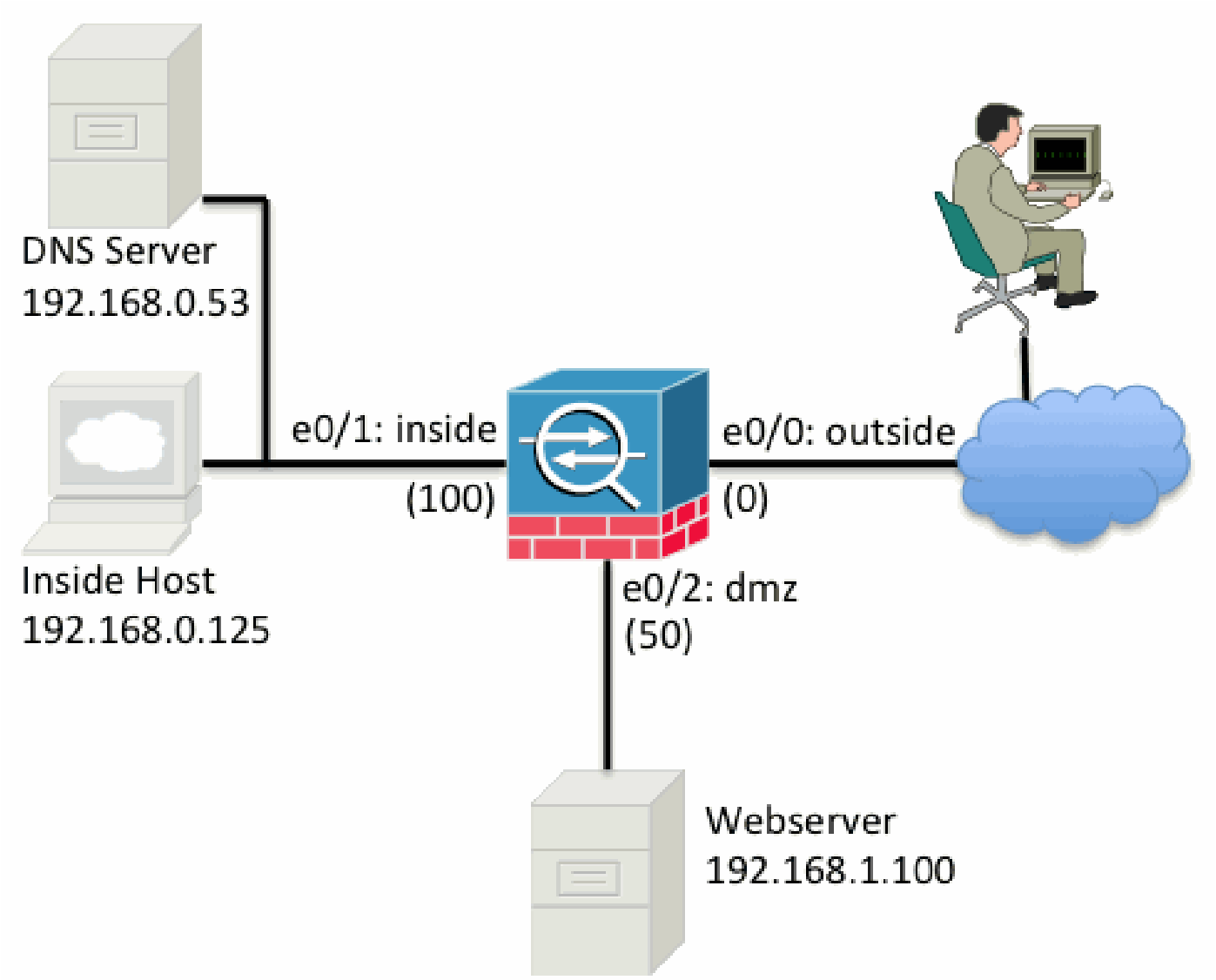
A continuación, es posible ver la configuración de la interfaz y las direcciones IP para el ejemplo:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

Aquí se puede ver que la interfaz interna de ASA se configura con la dirección IP 192.168.0.1 y es el gateway predeterminado para los hosts internos. La interfaz externa de ASA está configurada con una dirección IP obtenida del ISP. Existe también una ruta predeterminada, que configura el siguiente salto como gateway del ISP. Si utiliza el protocolo de configuración dinámica de host (DHCP), esto se suministra automáticamente. La interfaz de DMZ está configurada con la dirección IP 192.168.1.1 y es el gateway predeterminado para los hosts en el segmento de red de DMZ.

Topología

A continuación, es posible ver una ilustración del cableado y la configuración:



Paso 1. Configuración de NAT para permitir que los hosts salgan a Internet

Para este ejemplo, se utiliza el objeto NAT, también conocido como AutoNAT. Lo primero que debemos configurar son las reglas de NAT que permiten que los hosts de los segmentos en el interior y en DMZ se conecten a Internet. Debido a que estos hosts utilizan direcciones IP privadas, es necesario traducirlos a un elemento que pueda someterse a routing en Internet. En este caso, traduzca las direcciones de modo que se parezcan a la dirección IP de la interfaz

externa de ASA. Si su IP externo cambia con frecuencia (quizá debido a DHCP), esta es la manera más sencilla de realizar la configuración.

Para configurar esta NAT, es necesario crear un objeto de red que represente la subred interna y otro que represente la subred de DMZ. En cada uno de estos objetos, configure una regla nat dinámica que pueda traducir la dirección de puerto (PAT) a estos clientes a medida que pasan de sus respectivas interfaces a la interfaz externa.

Esta configuración es similar a la siguiente:

```
object network inside-subnet
 subnet 192.168.0.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
object network dmz-subnet
 subnet 192.168.1.0 255.255.255.0
 nat (dmz,outside) dynamic interface
```

Si observa la configuración en ejecución en este punto (con el resultado del comando show run), puede ver que la definición de objeto se divide en dos partes del resultado. La primera parte solamente indica qué hay en el objeto (host/subred, dirección IP, etc.), mientras que la segunda sección muestra la regla de NAT vinculada a ese objeto. Si observamos la primera entrada en la salida anterior:

Cuando los hosts que coinciden con la subred 192.168.0.0/24 pasan de la interfaz interna a la interfaz externa, es recomendable traducirlos dinámicamente a lainterfaz externa.

Paso 2. Configuración de NAT para acceder al servidor web desde Internet

Ahora que los hosts en las interfaces interna y de DMZ pueden conectarse a Internet, es necesario modificar la configuración para que los usuarios de Internet puedan tener acceso a nuestro servidor web en el puerto TCP 80. En este ejemplo, la configuración es para que las personas en Internet puedan conectarse a otra dirección IP que proporcione el ISP y a una dirección IP adicional propia . Para este ejemplo, utilice 198.51.100.101. Con esta configuración, los usuarios de Internet pueden alcanzar el servidor web DMZ accediendo a 198.51.100.101 en el puerto TCP 80. Utilice el objeto NAT para esta tarea, y el ASA puede traducir el puerto TCP 80 en el servidor web (192.168.1.100) para que se vea como 198.51.100.101 en el puerto TCP 80 en el exterior. De manera similar a lo que hizo anteriormente, defina un objeto y las reglas de traducción para ese objeto. Además, defina un segundo objeto para representar la IP a la que puede traducir este host.

Esta configuración es similar a la siguiente:

```
object network webserver-external-ip
 host 198.51.100.101
!
```

```
object network webserver
 host 192.168.1.100
 nat (dmz,outside) static webserver-external-ip service tcp www www
```

Para resumir lo que esa regla de NAT significa en este ejemplo:

Cuando un host que coincide con la dirección IP 192.168.1.100 en los segmentos de DMZ establece una conexión originada en el puerto TCP 80 (www) y dicha conexión sale de la interfaz externa, se recomienda traducir esto para que sea el puerto TCP 80 (www) en la interfaz externa y traducir la dirección IP para que sea 198.51.100.101.

Eso parece un poco extraño... "originado en el puerto TCP 80 (www)", pero el tráfico web está destinado al puerto 80. Es importante comprender que estas reglas de NAT son bidireccionales por naturaleza. Como resultado, puede invertir el texto para reformular esta oración. El resultado tiene mucho más sentido:

Cuando los hosts en el exterior establecen una conexión a 198.51.100.101 en el puerto TCP de destino 80 (www), puede traducir la dirección IP de destino a 192.168.1.100 y el puerto de destino puede ser el puerto TCP 80 (www) y enviarlo a la DMZ.

Tiene más sentido cuando se expresa de esta manera. A continuación, debe configurar las ACL.

Paso 3. Configurar ACL

Ya se configuró la NAT y estamos por finalizar toda la configuración. Recuerde que las ACL en ASA le permiten anular el comportamiento de seguridad predeterminado, que es el siguiente:

- El tráfico que circula desde una interfaz de seguridad inferior es rechazado cuando se dirige a una interfaz de seguridad superior.
- El tráfico que circula desde una interfaz de seguridad superior es permitido cuando se dirige a una interfaz de seguridad inferior.

Por lo tanto, si no se agrega ninguna ACL a la configuración, el tráfico de este ejemplo funciona del siguiente modo:

- Los hosts en el interior (nivel de seguridad 100) pueden conectarse a los hosts en la DMZ (nivel de seguridad 50).
- Los hosts en el interior (nivel de seguridad 100) pueden conectarse a los hosts en el exterior (nivel de seguridad 0).
- Los hosts en la DMZ (nivel de seguridad 50) pueden conectarse a los hosts en el exterior (nivel de seguridad 0).

Sin embargo, este tráfico se rechaza:

- Los hosts en el exterior (nivel de seguridad 0) no pueden conectarse a los hosts en el interior (nivel de seguridad 100).
- Los hosts en el exterior (nivel de seguridad 0) no pueden conectarse a los hosts en la DMZ (nivel de seguridad 50).

- Los hosts en la DMZ (nivel de seguridad 50) no pueden conectarse a los hosts en el interior (nivel de seguridad 100).

Debido a que ASA rechaza el tráfico del exterior a la red DMZ con la configuración actual, los usuarios de Internet no pueden comunicarse con el servidor web a pesar de la configuración de NAT en el paso 2. Se debe autorizar explícitamente este tráfico. A partir del código 8.3, se debe utilizar la dirección IP real del host en la ACL, no la dirección IP traducida. Esto significa que la configuración debe permitir el tráfico destinado a 192.168.1.100 yNO el tráfico destinado a 198.51.100.101 en el puerto 80. Por motivos de simplicidad, los objetos definidos en el paso 2 también se pueden utilizar para esta ACL. Una vez que se crea la ACL, es necesario aplicarla internamente en la interfaz externa.

Así se ven esos comandos de configuración:

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

La línea de la lista de acceso establece lo siguiente:

Permitir el tráfico desde any (cualquier lugar) al host representado por el objeto servidor web (192.168.1.100) en el puerto 80.

Es importante que la configuración utilice la palabra clave any aquí. Debido a que la dirección IP de origen de los clientes no se conoce cuando llega a su sitio web, especifique cualquier significado, Cualquier dirección IP.

¿Qué ocurre con el tráfico del segmento DMZ destinado a los hosts en el segmento de red interna? Por ejemplo, un servidor de la red interna al que necesitan conectarse los hosts de la DMZ. ¿Cómo puede ASA permitir solo ese tráfico específico destinado al servidor interno y bloquear todo lo demás destinado al segmento interno de la DMZ?

En este ejemplo, se supone que hay un servidor DNS en la red interna, en la dirección IP 192.168.0.53, al que los hosts de la DMZ necesitan tener acceso para la resolución de DNS. Debe crear la ACL necesaria y aplicarla a la interfaz de DMZ para que ASA pueda anular ese comportamiento de seguridad predeterminado, mencionado anteriormente, para el tráfico que ingresa en esa interfaz.

Así se ven esos comandos de configuración:

```
object network dns-server
 host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
```

```
access-group dmz_acl in interface dmz
```

La ACL no solo permite el tráfico al servidor DNS en el puerto UDP 53, sino que es más compleja. Si lo único que hiciéramos fuera permitir la primera línea, se bloquearía todo el tráfico desde la DMZ a los hosts de Internet. Las ACL tienen una negación implícita de IP any any al final de la ACL. Como resultado, los hosts de su DMZ no podrán conectarse a Internet. Aun cuando el tráfico desde la DMZ al exterior se permita de manera predeterminada, si se aplica una ACL a la interfaz de DMZ, los comportamientos de seguridad predeterminados para la interfaz de DMZ pierden vigor y debe permitirse explícitamente el tráfico en la ACL de la interfaz.

Paso 4. Probar configuración con la función Packet Tracer

Ahora que se ha completado la configuración, es necesario probarla para asegurarse de que funciona. El método más fácil es utilizar hosts reales (si la red es suya). Sin embargo, para probar esto desde la CLI y explorar más a fondo algunas de las herramientas de ASA, utilice el rastreador de paquetes para probar y, potencialmente, depurar cualquier problema encontrado.

Packet Tracer funciona simulando un paquete con una serie de parámetros e inyectándolo a la ruta de datos de la interfaz, de manera similar a como lo haría un paquete real proveniente de la red. Se realiza un seguimiento de este paquete a través de la inmensidad de controles y procesos que se realizan mientras pasa por el firewall, y Packet Tracer registra el resultado. Simule el host interno conectándose a un host en Internet. Este comando indica al firewall que:

Simular un paquete TCP que ingresa a la interfaz interna desde la dirección IP 192.168.0.125 en el puerto de origen 12345 y se dirige a una dirección IP 203.0.113.1 en el puerto 80.

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0         0.0.0.0         outside

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
```

```
 nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

El resultado final es que se permite el tráfico, lo que significa que aprobó todos los controles de NAT y ACL en la configuración y abandonó la interfaz de salida hacia el exterior. Tenga en cuenta que el paquete se tradujo en la etapa 3 y los detalles de esa etapa muestran qué regla se aplica. El host 192.168.0.125 se traduce dinámicamente a 198.51.100.100 según la configuración.

Ahora, ejecútelo para obtener una conexión de Internet al servidor web. Recuerde que los hosts en Internet pueden acceder al servidor web conectándose a 198.51.100.101 en la interfaz externa. Nuevamente, el siguiente comando se traduce a lo siguiente:

Simular un paquete TCP que ingresa a la interfaz externa desde la dirección IP 192.0.2.123 en el puerto de origen 12345 y se dirige a una dirección IP 198.51.100.101 en el puerto 80.

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
```

```
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Una vez más, el resultado es la autorización del paquete. Las ACL se desprotegen, la configuración parece correcta y los usuarios de Internet (externos) pueden acceder a ese servidor web con la IP externa.

Verificación

Los procedimientos de verificación están incluidos en el Paso 4: Pruebe la configuración con la función Packet Tracer.

Troubleshoot

Actualmente no hay información específica disponible sobre cómo resolver problemas de esta configuración.

Conclusión

La configuración de un ASA para hacer NAT básico no es tan difícil de una tarea. El ejemplo incluido en este documento se puede adaptar a su situación específica si cambia las direcciones IP y los puertos utilizados en los ejemplos de configuraciones. La configuración final de ASA en este caso, cuando se combina, es similar a la siguiente para ASA 5510:

```
ASA Version 9.1(1)
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
 nameif inside
```

```
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
 subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
 subnet 192.168.1.0 255.255.255.0
object network webserver
 host 192.168.1.100
object network webserver-external-ip
 host 198.51.100.101
object network dns-server
 host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
 nat (inside,outside) dynamic interface
object network dmz-subnet
 nat (dmz,outside) dynamic interface
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

En ASA 5505, por ejemplo, con las interfaces conectadas como se muestra anteriormente (la externa conectada a Ethernet0/0, la interna conectada a Ethernet0/1 y la DMZ conectada a Ethernet0/2):

```
ASA Version 9.1(1)
!
interface Ethernet0/0
 description Connected to Outside Segment
 switchport access vlan 2
!
interface Ethernet0/1
 description Connected to Inside Segment
 switchport access vlan 1
!
interface Ethernet0/2
 description Connected to DMZ Segment
 switchport access vlan 3
!
interface Vlan2
 nameif outside
 security-level 0
```

```
 ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
 nameif dmz
 security-level 50
 ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
 subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
 subnet 192.168.1.0 255.255.255.0
object network webserver
 host 192.168.1.100
object network webserver-external-ip
 host 198.51.100.101
object network dns-server
 host 192.168.0.53



!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
 nat (inside,outside) dynamic interface
object network dmz-subnet
 nat (dmz,outside) dynamic interface
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

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).