Configuración del NAT básica ASA: Servidor Web en el DMZ en la Versión de ASA 8.3 y posterior

Contenido

Introducción

Este documento proporciona un ejemplo simple y directo de cómo configurar el Network Address Translation (NAT) y el Listas de control de acceso (ACL) en un Firewall ASA para permitir la Conectividad saliente así como entrante. Este documento fue escrito con un Firewall adaptante 5510 del dispositivo de seguridad (ASA) que la versión del código de los funcionamientos ASA 9.1(1), pero éste puede aplicarse fácilmente a cualquier otra plataforma del Firewall ASA. Si usted utiliza una plataforma tal como un ASA 5505, que utiliza los VLA N en vez de una interfaz física, usted necesita cambiar los tipos de interfaz como apropiados.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un Firewall ASA 5510 que funcione con la versión del código ASA 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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Información general

Metas

En este ejemplo de configuración, usted puede considerar qué NAT y configuración ACL será necesaria para permitir el acceso entrante a un servidor Web en el DMZ de un Firewall ASA, y permite la Conectividad saliente de los host internos y DMZ. Esto se puede resumir como dos metas:

1. Permita los host en el interior y la Conectividad saliente DMZ a Internet.
2. Permita que los host en Internet accedan a un servidor Web en el DMZ con una dirección IP de 192.168.1.100.

Antes de conseguir a los pasos que se deben completar para lograr estas dos metas, este documento pasa abreviadamente la manera ACL y el trabajo NAT sobre las versiones más recientes del código ASA (versión 8.3 y posterior).

Descripción de la lista de control de acceso

Las listas de control de acceso (las listas de acceso o los ACL para corto) son el método por el cual el Firewall ASA determina si se permite o se niega el tráfico. Por abandono, se niega el tráfico que pasa de un **más bajo al mayor nivel de seguridad**. Esto se puede reemplazar por un ACL aplicado a esa interfaz de menor seguridad. También el ASA, por abandono, permite el tráfico de **más arriba a las interfaces de menor seguridad**. Este comportamiento se puede también reemplazar con un ACL.

En las versiones anteriores del código ASA (8.2 y anterior), el ASA comparó una conexión entrante o un paquete contra el ACL en una interfaz sin untranslating el paquete primero. Es decir el ACL tuvo que permitir el paquete como si usted debiera capturar ese paquete en la interfaz. En el código de la versión 8.3 y posterior, los untranslates ASA que paquete antes de que marque la interfaz ACL. Esto significa eso para y posterior el código 8.3, y se permite este documento, tráfico al IP real del host y no el IP traducido del host.

Vea la sección de las reglas de acceso que configura del libro 2: Guía de configuración CLI del Firewall de la serie de Cisco ASA, 9.1 para más información sobre los ACL.

Descripción general de NAT

El NAT en el ASA en la versión 8.3 y posterior está roto en dos tipos conocidos como **NAT auto (objeto NAT)** y **NAT manual (dos veces NAT)**. El primer de los dos, el **objeto NAT**, se configura dentro de la definición de un objeto de red. Un ejemplo de esto se proporciona más adelante en este documento. Una ventaja primaria de este método NAT es que el ASA pide automáticamente las reglas para procesar para evitar los conflictos. Ésta es la forma más fácil de NAT, pero con

esa facilidad viene una limitación en el granularity de la configuración. Por ejemplo, usted no puede tomar una decisión de la traducción basada en el destino en el paquete como usted podría con el segundo tipo de NAT, **nacional manual**. **El NAT manual** es más robusto en su granularity, pero requiere que las líneas estén configuradas en la orden correcta de modo que pueda alcanzar la conducta correcta. Esto complica este tipo NAT, y como consecuencia no será utilizada en este ejemplo de configuración.

Vea la información sobre la sección NAT del libro 2: Guía de configuración CLI del Firewall de la serie de Cisco ASA, 9.1 para más información sobre el NAT.

Configurar

Consiga comenzado

La configuración básica de la configuración ASA es tres interfaces conectadas con tres segmentos de red. El segmento de la red ISP está conectado con la interfaz del Ethernet0/0 y etiquetado **afuera** con un nivel de seguridad de 0. La red interna ha estado conectada con Ethernet0/1 y etiquetada como **dentro** con un nivel de seguridad de 100. El segmento DMZ, donde reside el servidor Web, está conectado con Ethernet0/2 y etiquetado como **DMZ** con un nivel de seguridad de 50.

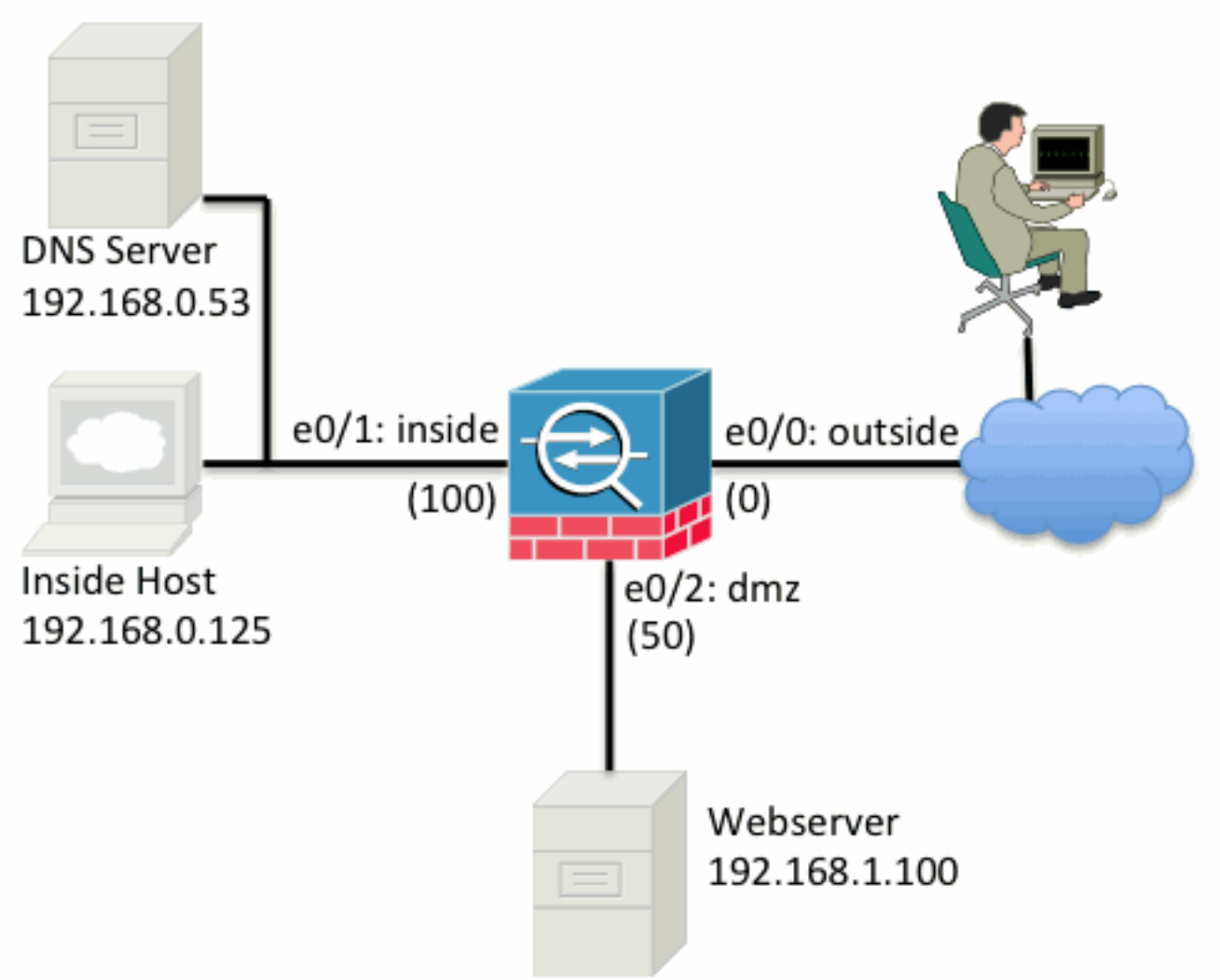
La configuración de la interfaz y los IP Addresses por el ejemplo se consideran aquí:

```
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 usted puede ver que la **interfaz interior** ASA está fijada con la dirección IP de 192.168.0.1, y es el default gateway para los host internos. **La interfaz exterior** ASA se configura con una dirección IP obtenida del ISP. Hay una ruta predeterminado en el lugar, que fija el Next-Hop para ser el gateway ISP. Si usted utiliza el DHCP esto se proporciona automáticamente. La interfaz **DMZ** se configura con la dirección IP de 192.168.1.1, y es el default gateway para los host en el segmento de la red DMZ.

Topología

Aquí está una mirada visual en cómo se telegrafía y se configura esto:



Paso 1 - Configuración NAT para permitir que los host salgan a Internet

Para este **objeto NAT del** ejemplo, también conocido como **AutoNAT**, se utiliza. La primera cosa a configurar es las reglas NAT que permiten los host en el **interior** y segmentos **DMZ** a conectar con Internet. Porque estos host utilizan los IP Address privados, usted necesita traducirlos algo que es routable en Internet. En este caso, traduzca los direccionamientos de modo que parezcan la dirección IP de la **interfaz exterior** ASA. Si su IP externa cambia con frecuencia (quizás debido al DHCP) ésta es la manera más directa de configurar esto.

Para configurar este NAT, usted necesita crear un objeto de red que represente la subred **interior** así como uno que represente la **subred DMZ**. En cada uno de estos objetos, configure una regla **nacional dinámica** que Port Address Translation (PAT) estos clientes mientras que pasan de sus interfaces respectivas a la **interfaz exterior**.

Esta configuración parece similar a esto:

```
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 usted mira la configuración corriente en este momento (con la salida del **comando show run**), usted verá que la definición del objeto está partida en dos partes de la salida. La primera parte

indica solamente cuál está en el objeto (host/subred, dirección IP, y así sucesivamente), mientras que la segunda sección muestra que regla NAT atada a ese objeto. Si usted toma la primera entrada en la salida anterior:

Cuando los host que hacen juego la travesía de 192.168.0.0/24 subredes de la ***interfaz interior a la interfaz exterior****, usted quieren traducirlos dinámicamente a la* ***interfaz exterior****.*

Paso 2 - Configuración NAT para acceder al servidor Web de Internet

Ahora que los host en las interfaces **interiores** y **DMZ** pueden salir a Internet, usted necesita modificar la configuración de modo que los usuarios en Internet puedan acceder a nuestro servidor Web en el puerto TCP 80. En este ejemplo, la configuración es de modo que la gente en Internet pueda conectar con otra dirección IP que el ISP proporcionó, una dirección IP adicional *poseemos*. Por este ejemplo, utilice 198.51.100.101. Con esta configuración, los usuarios en Internet podrán alcanzar al servidor Web **DMZ** accediendo 198.51.100.101 en el puerto TCP 80. Utilice el **objeto NAT** para esta tarea, y el ASA traducirá el puerto TCP 80 en el servidor Web (192.168.1.100) para parecer 198.51.100.101 en el puerto TCP 80 en el **exterior**. Semejantemente a qué fue hecha previamente, define un objeto y define las Reglas de traducción para ese objeto. También, defina un segundo objeto para representar el IP que usted traducirá este host a.

Esta configuración parece similar a esto:

```
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
```

Apenas para resumir lo que significa esa regla NAT en este ejemplo:

Cuando un host que corresponde con a la dirección IP 192.168.1.100 en los segmentos ***DMZ*** *establece una conexión originada del* ***puerto TCP 80 (WWW)*** *y que sale la conexión la* ***interfaz exterior****, usted quiere traducir eso para ser el* ***puerto TCP 80 (WWW)*** *en la* ***interfaz exterior*** *y para traducir ese IP Address para ser* ***198.51.100.101****.*

Ése parece un poco impar… “originado del puerto TCP 80 (WWW)”, solamente del tráfico de la Web *se destina al* puerto 80. Es importante entender que estas reglas NAT son bidireccionales en la naturaleza. Como consecuencia, usted puede mover de un tirón la fraseología alrededor para reformular esta frase. El resultado tiene mucho más sentido:

Cuando los host en el ***exterior*** *establecen una conexión a* ***198.51.100.101*** *en el* ***puerto 80 (WWW) del*** *TCP de destino, usted traducirá el IP Address de destino para ser* ***192.168.1.100*** *y el puerto destino será el* ***puerto TCP 80 (WWW)*** *y le mandará el* ***DMZ****.*

Esto tiene más sentido cuando está expresada esta manera. Después, usted necesita configurar los ACL.

Paso 3 - Configuración ACL

Se configura el NAT y el final de esta configuración está cerca. Recuerde, los ACL en el ASA permiten que usted reemplace la conducta de seguridad predeterminada que es como sigue:

- Trafique **se niega** que va de una **interfaz de menor seguridad** cuando va a una **interfaz de mayor seguridad**.
- Trafique **se permite** que va de una **interfaz de mayor seguridad** cuando va a una **interfaz de menor seguridad**.

Tan sin la adición de cualquier ACL a la configuración, este tráfico en el ejemplo trabaja:

- Los host en el **interior** (nivel de seguridad 100) pueden conectar con los host en el **DMZ** (nivel de seguridad 50).
- Los host en el **interior** (nivel de seguridad 100) pueden conectar con los host en el **exterior** (nivel de seguridad 0).
- Los host en el **DMZ** (nivel de seguridad 50) pueden conectar con los host en el **exterior** (nivel de seguridad 0).

Sin embargo, se niega este tráfico:

- Los host en el **exterior** (nivel de seguridad 0) no pueden conectar con los host en el **interior** (nivel de seguridad 100).
- Los host en el **exterior** (nivel de seguridad 0) no pueden conectar con los host en el **DMZ** (nivel de seguridad 50).
- Los host en el **DMZ** (nivel de seguridad 50) no pueden conectar con los host en el **interior** (nivel de seguridad 100).

Porque el tráfico del **exterior a la red DMZ** es negado por el ASA con su configuración actual, los usuarios en Internet no pueden alcanzar al servidor Web a pesar de la configuración del NAT en el paso 2. Usted necesita permitir explícitamente este tráfico. En y posterior el código 8.3 usted debe utilizar el **IP real del** host en el ACL y no el **IP traducido**. Esto significa que la configuración necesita permitir el tráfico destinado a 192.168.1.100 y no traficar destinado a 198.51.100.101 en el puerto 80. Para el motivo de la simplicidad, los objetos definidos en el paso 2 serán utilizados para este ACL también. Una vez que se crea el ACL, usted necesita aplicarlo entrante en la interfaz exterior.

Aquí es lo que parecen esos comandos configuration:

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

La línea estados de la lista de acceso:

*Tráfico del permiso del **any(where) al** host representado por el **web server del** objeto **(192.168.1.100)** en el puerto 80.*

Es importante la configuración utiliza la **cualquier** palabra clave aquí. Porque la dirección IP de origen de los clientes no se conoce como él alcanza su sitio web, especifique cualquier el significado “cualquier dirección IP.

¿Qué sobre el tráfico del segmento **DMZ** destinó a los host en el segmento de la **red interna**? Por ejemplo, un servidor en la **red interna a** la cual los host en la necesidad **DMZ** de conectar. ¿Cómo puede el ASA permitir solamente que específico trafique destinado al servidor **interior** y bloquee todo lo demás destinada al segmento **interior del DMZ**?

En este ejemplo se asume que hay servidor DNS en la red interna en la dirección IP 192.168.0.53 que los host en la necesidad **DMZ** de acceder para la resolución de DNS. Usted crea el ACL necesario y lo aplica a la interfaz **DMZ** así que el ASA puede reemplazar esa conducta de

seguridad predeterminada, mencionada anterior, para el tráfico que ingresa esa interfaz.

Aquí es lo que parecen esos comandos configuration:

```
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
```

El ACL es más complejo que simplemente permitiendo ese tráfico al servidor DNS en el puerto 53 UDP. Si todo lo que lo hicimos es que primero línea del “permiso”, después todo el tráfico sería bloqueado del **DMZ a los** host en Internet. Los ACL tienen un “deny ip any any implícito” en el final del ACL. Como consecuencia, sus host **DMZ** no podrían salir a Internet. Aunque el tráfico del **DMZ al exterior** se permite por abandono, con la aplicación de un ACL a la interfaz **DMZ**, ésos omiten las conductas de seguridad para la interfaz **DMZ** están no más en efecto y usted debe permitir explícitamente el tráfico en la interfaz ACL.

Paso 4 - Pruebe la configuración con la característica del trazalíneas del paquete

Ahora que se completa la configuración, usted necesita probarla para aseegurarse la trabaja. El método más fácil es utilizar los host reales (si ésta es su red). Sin embargo, en interés de probar esto del CLI y más futuro explorando algunas de las herramientas ASA, utilice el trazalíneas del paquete para probar y potencialmente hacer el debug de cualquier problema encontrado.

El trazalíneas del paquete trabaja simulando un paquete basado en una serie de parámetros e inyectando ese paquete al trayecto de datos de la interfaz, similar a la manera que un paquete de la vida real si fue cogido del alambre. Este paquete se sigue con la miríada de los controles y de los procesos se hacen que mientras que pasan con el Firewall, y trazalíneas del paquete observa el resultado. Simule el host interno que sale a un host en Internet. El comando abajo da instrucciones el Firewall a:

*Simule un **paquete TCP** que viene en la **interfaz interior del** IP address **192.168.0.125** en el puerto de origen **12345** destinado a un IP address de **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 el tráfico **está permitido**, los whichmeans que pasó todos los incorporares NAT y ACL la configuración y fue enviado la interfaz de egreso, **afuera**. Observe que el paquete fue traducido en la fase 3 y los detalles de esa fase muestran lo que se golpea la regla. El host 192.168.0.125 se traduce dinámicamente a 198.51.100.100 según la configuración.

Ahora, ejecútelo para una conexión de Internet al servidor Web. Recuerde, los host en Internet accederá al servidor Web conectando con 198.51.100.101 en la **interfaz exterior**. Una vez más este comando siguiente traduce a:

*Simule un **paquete TCP** que viene en la **interfaz exterior del** IP address **192.0.2.123** en el puerto de origen **12345** destinado a un IP address de **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 que el paquete está permitido. Los ACL marcan hacia fuera, las miradas de la configuración muy bien, y los usuarios en Internet (**afuera**) deben poder acceder a ese servidor Web con IP externa.

Verificación

Los procedimientos de verificación se incluyen en el paso 4 - Configuración de prueba con la característica del trazalíneas del paquete.

Troubleshooting

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

Conclusión

La configuración de un ASA para hacer el NAT básico no es ésa el desanimar de una tarea. El ejemplo en este documento se puede adaptar a su escenario específico si usted cambia los IP Addresses y los puertos usados en los ejemplos de configuración. La configuración final ASA para esto, cuando está combinado, parece similar a esto para un 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 un ASA 5505, por ejemplo, con las interfaces conectadas como se muestra previamente (**exterior** conectado con el Ethernet0/0, **dentro de** conectado con Ethernet0/1 y el **DMZ** conectado con 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
```