Configuração de NAT básica ASA: Servidor de Web no DMZ na versão ASA 8.3 e mais atrasado

Índice

Introdução

Este documento fornece um exemplo simples e direto de como configurar o Network Address Translation (NAT) e o Access Control Lists (ACLs) em um Firewall ASA a fim permitir a Conectividade de partida assim como de entrada. Este documento foi redigido com um Firewall 5510 adaptável da ferramenta de segurança (ASA) do que a versão de código das corridas ASA 9.1(1), mas este pode facilmente aplicar-se a toda a outra plataforma do Firewall ASA. Se você usa uma plataforma tal como um ASA 5505, que use VLAN em vez de uma interface física, você precisa de mudar os tipos de interface como apropriados.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em um Firewall ASA 5510 que execute a versão de código ASA 9.1(1).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Visão geral

Objetivos

Neste exemplo de configuração, você pode olhar que NAT e configuração ACL será precisada a fim permitir o acesso de entrada a um servidor de Web no DMZ de um Firewall ASA, e permite a Conectividade de partida dos anfitriões internos e DMZ. Isto pode ser resumido como dois objetivos:

1. Permita anfitriões no interior e na Conectividade de partida DMZ ao Internet.
2. Permita que os anfitriões no Internet alcancem um servidor de Web no DMZ com um endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.1.100.

Antes de obter às etapas que devem ser terminadas a fim realizar estes dois objetivos, este documento vai momentaneamente sobre a maneira ACL e o trabalho NAT nas versões mais novas do código ASA (versão 8.3 e mais recente).

Vista geral do Access Control List

As listas de controle de acesso (listas de acesso ou ACL para breve) são o método por que o Firewall ASA determina se o tráfego é permitido ou negado. À revelia, o tráfego que passa de um **mais baixo ao nível de segurança mais elevado** é negado. Isto pode ser cancelado por um ACL aplicado a essa interface de segurança mais baixa. Igualmente o ASA, à revelia, permite o tráfego de **mais altamente às interfaces de segurança mais baixa**. Este comportamento pode igualmente ser cancelado com um ACL.

Nas versões anterior do código ASA (8.2 e mais adiantado), o ASA comparou uma conexão recebida ou um pacote contra o ACL em uma relação sem untranslating o pacote primeiramente. Ou seja o ACL teve que permitir o pacote como se você devia capturar esse pacote na relação. No código da versão 8.3 e mais recente, os untranslates ASA que pacote antes que verificar a relação ACL. Isto significa aquele para 8.3 e o código mais recente, e este documento, tráfego ao IP real do host é permitido e não o IP traduzido do host.

Veja a seção das regras do acesso de livro configurando 2: Guia de configuração de CLI do Series Firewall de Cisco ASA, 9.1 para obter mais informações sobre dos ACL.

Visão geral de NAT

O NAT no ASA na versão 8.3 e mais recente quebra-se em dois tipos conhecidos como **auto NAT (objeto NAT)** e **NAT manual (duas vezes NAT)**. O primeiro dos dois, o **objeto NAT**, é configurado dentro da definição de um objeto de rede. Um exemplo deste é fornecido mais tarde neste documento. Uma vantagem preliminar deste método NAT é que o ASA pede automaticamente as regras processando a fim evitar conflitos. Este é o formulário o mais fácil do NAT, mas com essa

facilidade vem uma limitação na granularidade da configuração. Por exemplo, você não pode fazer uma decisão da tradução baseada no destino no pacote como você poderia com o segundo tipo de NAT, **Nat manual**. **O NAT manual** é mais robusto em sua granularidade, mas exige que as linhas estejam configuradas na ordem correta de modo que possa conseguir o comportamento correto. Isto complica este tipo NAT, e em consequência não será usado neste exemplo de configuração.

Veja a informação sobre a seção NAT de livro 2: Guia de configuração de CLI do Series Firewall de Cisco ASA, 9.1 para obter mais informações sobre do NAT.

Configurar

Obtenha começado

A instalação básica da configuração ASA é três relações conectadas a três segmentos de rede. O segmento da rede ISP é conectado à relação do Ethernet0/0 e etiquetado **fora** com um nível de segurança de 0. A rede interna foi conectada a Ethernet0/1 e etiquetada como **para dentro** com um nível de segurança de 100. O segmento DMZ, onde o servidor de Web reside, é conectado a Ethernet0/2 e etiquetado como o **DMZ** com um nível de segurança dos 50 pés.

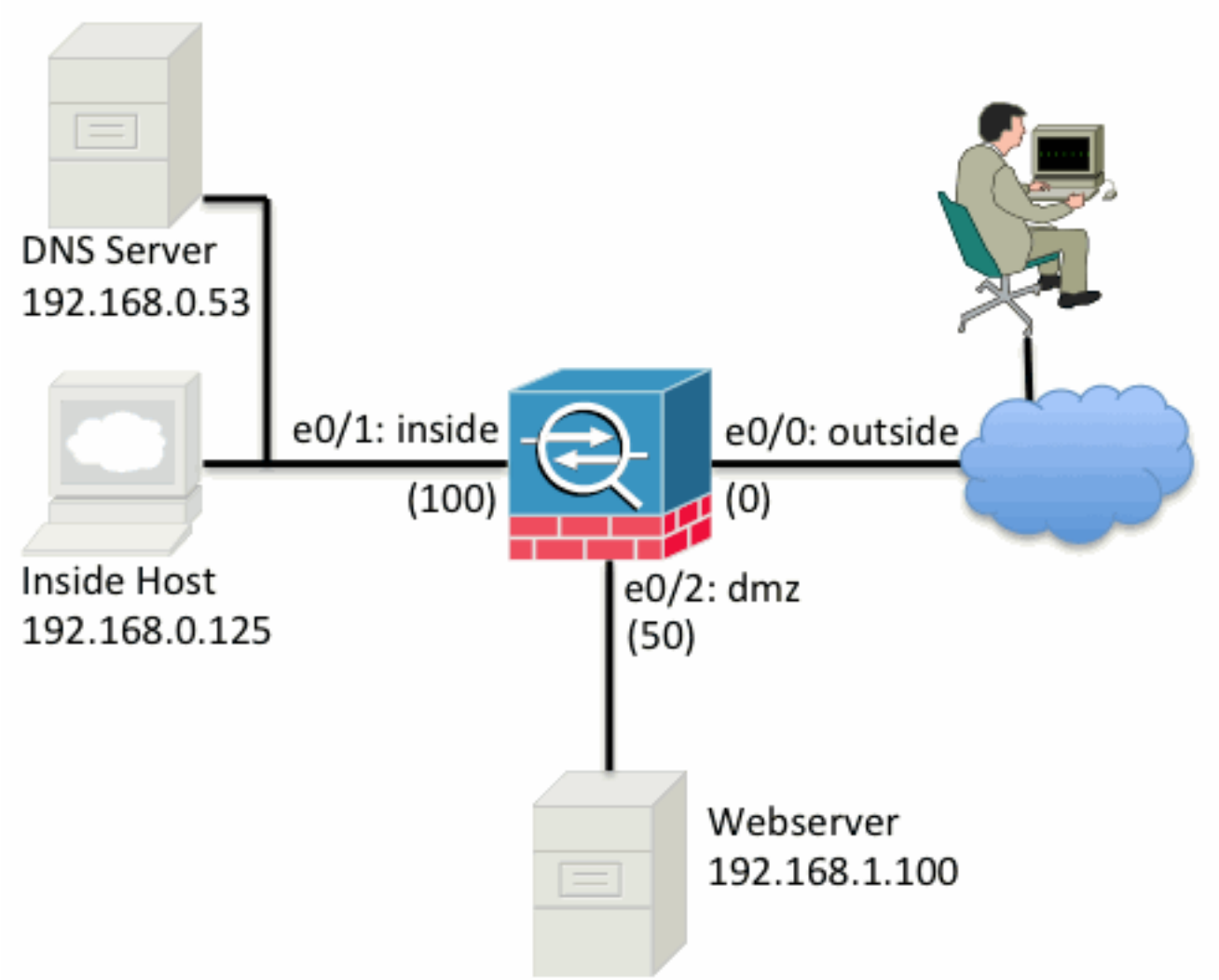
A configuração da interface e os endereços IP de Um ou Mais Servidores Cisco ICM NT para o exemplo são considerados aqui:

```
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
```

Aqui você pode ver que a **interface interna do** ASA está ajustada com o endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.0.1, e é o gateway padrão para os host internos. **A interface externa do** ASA é configurada com um endereço IP de Um ou Mais Servidores Cisco ICM NT obtido do ISP. Há uma rota padrão no lugar, que ajuste o salto seguinte para ser o gateway ISP. Se você usa o DHCP este está fornecido automaticamente. A relação **DMZ** é configurada com o endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.1.1, e é o gateway padrão para anfitriões no segmento da rede do DMZ.

Topologia

Está aqui um olhar visual em como este é cabografado e configurado:



Etapa 1 - Configurar o NAT para permitir que os anfitriões saiam ao Internet

Para este **objeto NAT do** exemplo, igualmente sabido como **AutoNAT**, é usado. A primeira coisa a configurar é as regras NAT que permitem os anfitriões no **interno** e segmentos **DMZ** a conectar ao Internet. Porque estes anfitriões usam endereços IP privados, você precisa de traduzi-los a algo que é roteável no Internet. Neste caso, traduza os endereços de modo que olhem como o endereço IP de Um ou Mais Servidores Cisco ICM NT da **interface externa do** ASA. Se seu IP externo muda frequentemente (talvez devido ao DHCP) esta é a maneira a mais direta de configurar isto.

A fim configurar este NAT, você precisa de criar um objeto de rede que represente a sub-rede **interna** assim como um que representa a **sub-rede DMZ**. Em cada um destes objetos, configurar uma regra **nat dinâmica** que tradução de endereço de porta (PAT) estes clientes enquanto passam de suas interfaces respectivas à **interface externa**.

Esta configuração olha similar a esta:

```
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
```

Se você olha a configuração running neste momento (com a saída do **comando show run**), você

verá que a definição de objeto está rachada em duas porções da saída. A primeira parte indica somente o que está no objeto (host/sub-rede, endereço IP de Um ou Mais Servidores Cisco ICM NT, e assim por diante), quando a segunda seção mostrar que regra NAT amarrada a esse objeto. Se você toma a primeira entrada na saída precedente:

Quando os anfitriões que combinam a travessia de 192.168.0.0/24 sub-redes da ***interface interna à interface externa****, você quiserem os traduzir dinamicamente à* ***interface externa****.*

Etapa 2 - Configurar o NAT para alcançar o servidor de Web do Internet

Agora que os anfitriões nas relações **internas** e **DMZ** podem sair ao Internet, você precisa de alterar a configuração de modo que os usuários no Internet possam alcançar nosso servidor de Web na porta TCP 80. Neste exemplo, a instalação é de modo que os povos no Internet possam conectar a um outro endereço IP de Um ou Mais Servidores Cisco ICM NT que o ISP forneceu, um endereço IP de Um ou Mais Servidores Cisco ICM NT adicional nós *possuímos*. Para este exemplo, use 198.51.100.101. Com esta configuração, os usuários no Internet poderão alcançar o servidor de Web **DMZ por** 198.51.100.101 de acesso na porta TCP 80. Use o **objeto NAT** para esta tarefa, e o ASA traduzirá a porta TCP 80 no servidor de Web (192.168.1.100) para olhar como 198.51.100.101 na porta TCP 80 na **parte externa**. Similarmente ao que foi feito previamente, define um objeto e define Regras de tradução para esse objeto. Também, defina um segundo objeto para representar o IP que você traduzirá este host a.

Esta configuração olha similar a esta:

```
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 apenas o que essa regra NAT significa neste exemplo:

Quando um host que combinem o endereço IP 192.168.1.100 nos segmentos ***DMZ*** *estabelecer uma conexão originado da* ***porta TCP 80 (WWW)*** *e que a conexão sai a* ***interface externa****, você quer traduzir aquele para ser a* ***porta TCP 80 (WWW) na interface externa*** *e para traduzir esse endereço IP de Um ou Mais Servidores Cisco ICM NT para ser* ***198.51.100.101****.*

Aquele parece um pouco impar… “originado da porta TCP 80 (WWW)”, mas do tráfego de web *é destinado à* porta 80. É importante compreender que estas regras NAT são bidirecionais na natureza. Em consequência, você pode lançar o fraseio ao redor a fim reformular esta frase. O resultado faz muito mais o sentido:

Quando os anfitriões na ***parte externa*** *estabelecem uma conexão a* ***198.51.100.101 na porta 80 do*** *TCP destino* ***(WWW)****, você traduzirá o endereço IP de destino para ser* ***192.168.1.100*** *e a porta do destino será a* ***porta TCP 80 (WWW)*** *e enviar-lhe-á para fora o* ***DMZ****.*

Isto faz mais sentido quando fraseado esta maneira. Em seguida, você precisa de estabelecer os ACL.

Etapa 3 - Configurar ACL

O NAT é configurado e o fim desta configuração está próximo. Recorde, ACL no ASA permitem que você cancele o comportamento de segurança do padrão que é como segue:

- Trafique que vai de uma **interface de segurança mais baixa é negado** quando for a uma **interface de segurança mais elevada**.
- Trafique que vai de uma **interface de segurança mais elevada é reservado** quando for a uma **interface de segurança mais baixa**.

Assim sem a adição de todos os ACL à configuração, este tráfego no exemplo trabalha:

- Os anfitriões no **interior** (nível de segurança 100) podem conectar aos anfitriões no **DMZ** (50 pés do nível de segurança).
- Os anfitriões no **interior** (nível de segurança 100) podem conectar aos anfitriões na **parte externa** (nível de segurança 0).
- Os anfitriões no **DMZ** (50 pés do nível de segurança) podem conectar aos anfitriões na **parte externa** (nível de segurança 0).

Contudo, este tráfego é negado:

- Os anfitriões na **parte externa** (nível de segurança 0) não podem conectar aos anfitriões no **interior** (nível de segurança 100).
- Os anfitriões na **parte externa** (nível de segurança 0) não podem conectar aos anfitriões no **DMZ** (50 pés do nível de segurança).
- Os anfitriões no **DMZ** (50 pés do nível de segurança) não podem conectar aos anfitriões no **interior** (nível de segurança 100).

Porque o tráfego da **parte externa à rede do DMZ** é negado pelo ASA com sua configuração atual, os usuários no Internet não podem alcançar o servidor de Web apesar da configuração de NAT em etapa 2. Você precisa de permitir explicitamente este tráfego. Em 8.3 e em código mais recente você deve usar o **IP real do** host no ACL e não no **IP traduzido**. Isto significa que a configuração precisa de permitir o tráfego destinado a 192.168.1.100 e de não traficar destinado a 198.51.100.101 na porta 80. Para a causa da simplicidade, os objetos definidos em etapa 2 serão usados para este ACL também. Uma vez que o ACL é criado, você precisa de aplicá-lo de entrada na interface externa.

Éaqui o que aqueles comandos configuration olham como:

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

A linha estados da lista de acesso:

*Tráfego da licença do **any(where) ao** host representado pelo **web server do** objeto **(192.168.1.100) na** porta 80.*

Éimportante a configuração usa **toda a** palavra-chave aqui. Porque o endereço IP de origem dos clientes não é sabido como ele alcança seu Web site, especifique todos os o significado “quaisquer endereços IP de Um ou Mais Servidores Cisco ICM NT.

Que sobre o tráfego do segmento **DMZ** destinou aos anfitriões no segmento da **rede interna**? Por exemplo, um server na **rede interna a** que os anfitriões na necessidade **DMZ** de conectar. Como pode o ASA reservar somente que específico trafique destinado ao server **interno** e obstrua tudo mais destinado ao segmento **interno do DMZ**?

Neste exemplo supõe-se que há um servidor DNS na rede interna no endereço IP 192.168.0.53 que os anfitriões na necessidade **DMZ** de alcançar para a resolução de DNS. Você cria o ACL necessário e aplica-o à relação **DMZ** assim que o ASA pode cancelar esse comportamento de

segurança do padrão, mencionado mais cedo, para o tráfego que incorpora essa relação.

Éaqui o que aqueles comandos configuration olham como:

```
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
```

O ACL é mais complexo do que simplesmente permitindo esse tráfego ao servidor DNS na porta 53 UDP. Se tudo que nós fizemos é que primeiramente linha da “licença”, a seguir todo o tráfego estaria obstruído do **DMZ aos** anfitriões no Internet. Os ACL têm um “deny ip any any implícito” no fim do ACL. Em consequência, seus anfitriões **DMZ** não poderiam sair ao Internet. Mesmo que o tráfego do **DMZ à parte externa** seja permitido à revelia, com aplicativo de um ACL à relação **DMZ**, aqueles optam por comportamentos de segurança para a relação **DMZ** são já não de fato e você deve explicitamente permitir o tráfego na relação ACL.

Etapa 4 - Teste a configuração com a característica do projétil luminoso do pacote

Agora que a configuração é terminada, você precisa de testá-la a fim certificar-se que trabalha. O método o mais fácil é usar anfitriões reais (se esta é sua rede). Contudo, no interesse de testar isto do CLI e mais adicional explorando algumas das ferramentas do ASA, use o projétil luminoso do pacote a fim testar e debugar potencialmente todos os problemas encontrados.

O projétil luminoso do pacote funciona simulando um pacote baseado em uma série de parâmetros e injetando esse pacote ao trajeto de dados da relação, similar à maneira que um pacote da vida real se foi pegarado fora do fio. Este pacote é seguido com a miríade das verificações e dos processos que estão feitos enquanto passam com o Firewall, e projétil luminoso do pacote nota o resultado. Simule o host interno que sai a um host no Internet. O comando abaixo instrui o Firewall a:

*Simule um **pacote de TCP que** vem na **interface interna do** IP address **192.168.0.125 na** porta de origem **12345** destinada a um IP address de **203.0.113.1 na** porta **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
```

O resultado final é que o tráfego **está permitido**, os whichmeans que passou a todo o NAT e ACL verifica dentro a configuração e foi mandado a interface de saída, **fora**. Note que o pacote esteve traduzido na fase 3 e os detalhes dessa fase mostram o que a regra é batida. O host 192.168.0.125 é traduzido dinamicamente a 198.51.100.100 conforme a configuração.

Agora, execute-o para uma conexão do Internet ao servidor de Web. Recorde, anfitriões no Internet alcançará o servidor de Web conectando a 198.51.100.101 na **interface externa**. Além disso, este comando seguinte traduz a:

*Simule um **pacote de TCP que** vem na **interface externa do** IP address **192.0.2.123 na** porta de origem **12345** destinada a um IP address de **198.51.100.101 na** porta **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
```

Além disso, o resultado é que o pacote está permitido. Os ACL verificam para fora, os olhares da configuração muito bem, e os usuários no Internet (**fora**) devem poder alcançar esse servidor de Web com o IP externo.

Verificar

Os procedimentos de verificação são incluídos em etapa 4 - Configuração de teste com a característica do projétil luminoso do pacote.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Conclusão

A configuração de um ASA para fazer o NAT básico não é aquela desanimaar de uma tarefa. O exemplo neste documento pode ser adaptado a sua encenação específica se você muda os endereços IP de Um ou Mais Servidores Cisco ICM NT e as portas usados nos exemplos de configuração. A configuração final ASA para este, quando combinado, olha similar a isto para um 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
```

Em um ASA 5505, por exemplo, com as relações conectadas como mostrado previamente (**parte externa** conectada ao Ethernet0/0, **dentro do** conectado a Ethernet0/1 e ao **DMZ** conectado 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
```