# Configurar a conversão de endereço de rede e ACLs em um firewall ASA

## Contents


[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Overview](#)
[Metas](#)
[Resumo da lista de controle de acesso](#)
[Visão geral de NAT](#)
[Configurar](#)
[Comece já](#)
[Topologia](#)
[Etapa 1. Configurar o NAT para permitir que os hosts acessem a Internet](#)
[Etapa 2. Configure o NAT para acessar o servidor Web da Internet](#)
[Etapa 3. Configurar ACLs](#)
[Etapa 4. Testar a configuração com o recurso Packet Tracer](#)
[Verificar](#)
[Troubleshoot](#)
[Conclusão](#)


## Introduction

Este documento descreve como configurar a Tradução de Endereço de Rede (NAT - Network Address Translation) e as Listas de Controle de Acesso (ACLs - Access Control Lists) em um Firewall ASA.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações contidas neste documento baseiam-se em um firewall ASA 5510 que executa o ASA versão 9.1(1).

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

Este documento descreve um exemplo simples e direto de como configurar NAT e ACLs em um firewall ASA para permitir conectividade de saída e de entrada. Ele foi criado com um firewall Adaptive Security Appliance (ASA) 5510 que executa a versão 9.1(1) do código ASA, mas isso pode ser facilmente aplicado a qualquer outra plataforma de firewall ASA. Se você usar uma plataforma como um ASA 5505, que usa VLANs em vez de uma interface física, você precisará alterar os tipos de interface, conforme apropriado.

# Overview

## Metas

Nesta configuração de exemplo, você pode ver quais configurações de NAT e ACL são necessárias para permitir acesso de entrada a um servidor Web na DMZ de um firewall ASA e permitir conectividade de saída de hosts internos e DMZ. Isso pode ser resumido como duas metas:

1. Permitir hosts no interior e conectividade de saída DMZ para a Internet.
2. Permitir que hosts na Internet acessem um servidor Web no DMZ com um endereço IP 192.168.1.100.

Antes de executar as etapas que devem ser concluídas para atingir esses dois objetivos, este documento aborda brevemente a forma como as ACLs e a NAT funcionam nas versões mais recentes do código ASA (versão 8.3 e posterior).

## Resumo da lista de controle de acesso

As listas de controle de acesso (listas de acesso ou ACLs) são o método pelo qual o firewall ASA determina se o tráfego é permitido ou negado. Por padrão, o tráfego que passa de um nível de segurança inferior para um nível mais elevado é negado. Isso pode ser anulado por uma ACL aplicada a essa interface de segurança inferior. Por padrão, o ASA também permite o tráfego de interfaces de segurança de níveis mais elevados para níveis inferiores. Esse comportamento também pode ser cancelado com uma ACL.

Em versões anteriores do ASA (8.2 e anterior), o ASA era comparável com uma conexão de entrada ou pacote em relação à ACL em uma interface sem desconverter o pacote primeiro. Em outras palavras, a ACL tinha que dar permissão ao pacote como se fosse capturá-lo na interface. Na versão 8.3 e superiores, o ASA desconverte esse pacote antes que ele verifique a ACL de interface. Isso significa que, para as versões 8.3 e posteriores, e para este documento, o tráfego até o IP real do host, não o IP convertido do host, é permitido.

Consulte a seção Configuração de regras de acesso do Livro 2: Guia de configuração da CLI do Cisco ASA Series Firewall, 9.1 para obter mais informações sobre ACLs.

## Visão geral de NAT

A NAT no ASA na versão 8.3 e posterior é dividida em dois tipos conhecidos como NAT automática (NAT objeto) e NAT manual (NAT dupla). A primeira das duas, a NAT objeto, é configurada na definição de um objeto de rede. Um exemplo disso é apresentado ao final deste documento. Uma das principais vantagens desse método de NAT é que o ASA pede automaticamente as regras de processamento, para evitar conflitos. Essa é a forma mais simples da NAT, mas com essa facilidade vem uma limitação na granularidade de configuração. Por exemplo, você não pode tomar uma decisão de conversão de acordo com o destino do pacote como faria com o segundo tipo de NAT, a Nat manual. A NAT manual tem granularidade mais resistente, mas exige que as linhas sejam configuradas na ordem correta para que seja possível atingir o comportamento correto. Isso complica esse tipo de NAT e, como resultado, ele não pode ser usado neste exemplo de configuração.

Consulte a seção Information About NAT do Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1 para obter mais informações sobre o NAT.

# Configurar

## Comece já

A configuração básica do ASA conta com três interfaces conectadas a três segmentos de rede. O segmento de rede do ISP é conectado à interface Ethernet0/0 e é rotulado como fora com um nível de segurança de 0. A rede interna foi conectada à Ethernet0/1 e rotulada como dentro com um nível de segurança de 100. O segmento de DMZ, onde reside o servidor Web, é conectado à Ethernet0/2 e rotulado como DMZ com um nível de segurança de 50.

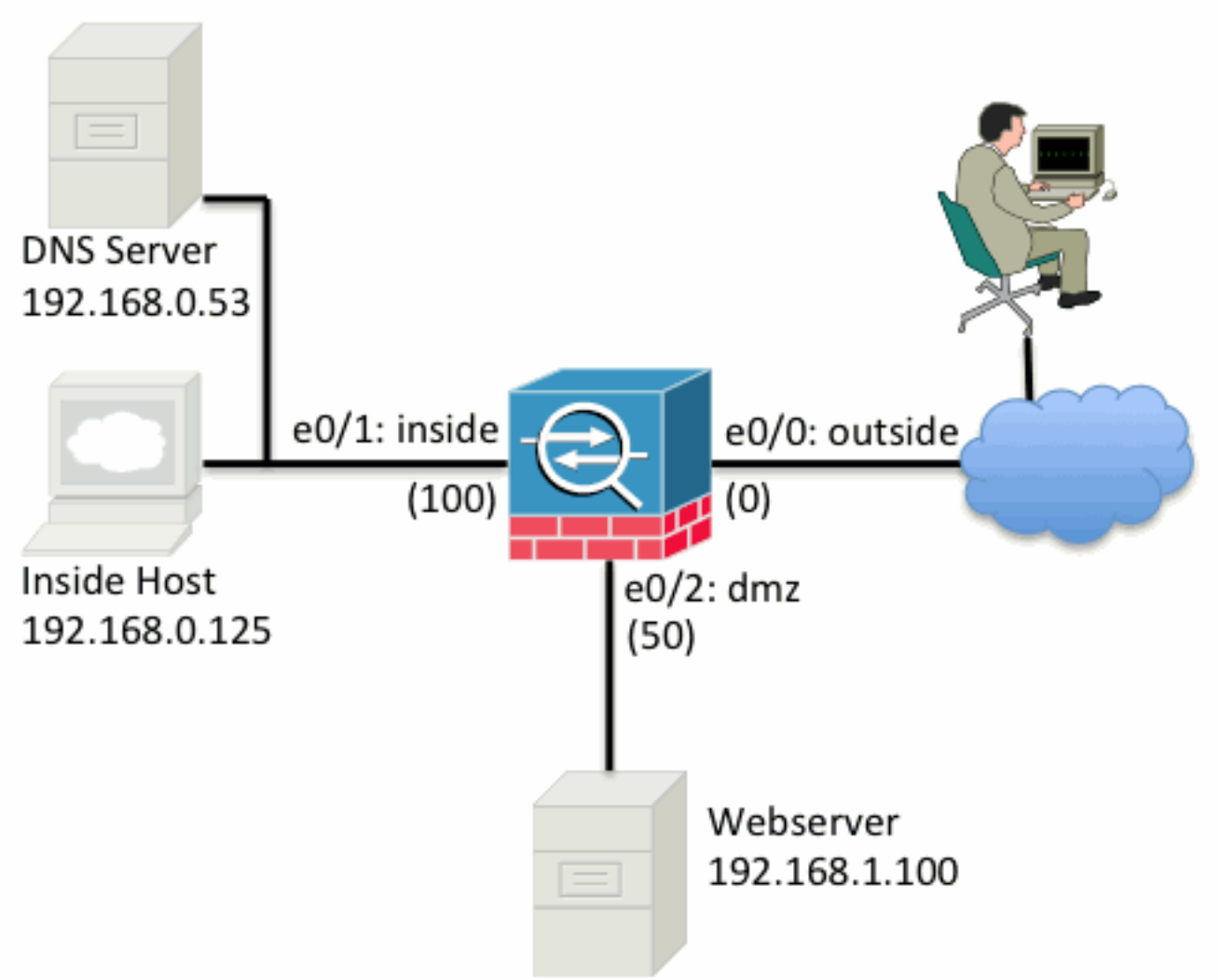
A configuração de interface e os endereços IP do exemplo são exibidos a seguir:

```
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 é definida com o endereço IP 192.168.0.1 e é o gateway padrão para os hosts internos. A interface externa do ASA é configurada com um endereço IP obtido a partir do ISP. É estabelecida uma rota padrão, que define o próximo salto para ser o gateway ISP. Se você usar DHCP, essa informação é fornecida automaticamente. A interface do DMZ é configurada com o endereço IP 192.168.1.1 e é o gateway padrão para hosts no segmento de rede do DMZ.

## Topologia

Veja a seguir como tudo é cabeado e configurado:




## Etapa 1. Configurar o NAT para permitir que os hosts acessem a Internet

Para este exemplo, NAT de objeto, também conhecido como AutoNAT, é usado. A primeira ação é configurar as regras da NAT que permitem que os hosts nos segmentos interno e DMZ se conectem à Internet. Como esses hosts usam endereços IP privados, você precisa traduzi-los para algo roteável na Internet. Nesse caso, converta os endereços para que eles se pareçam com os endereços IP da interface externa do ASA. Se o IP externo mudar com frequência (talvez devido ao DHCP), esta é a maneira mais simples de fazer a configuração.

Para configurar esta NAT, você precisa criar um objeto de rede que represente a sub-rede interna e um que represente a sub-rede DMZ. Em cada um desses objetos, configure uma regra de nat dinâmica que possa fazer a conversão de endereço de porta (PAT - Port Address Translation) nesses clientes à medida que eles passam de suas respectivas interfaces para a interface externa.

Essa configuração é semelhante a:

```
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 observar a configuração de execução nesse ponto (com a saída do comando show run), poderá ver que a definição do objeto é dividida em duas partes da saída. A primeira parte apenas indica o que está no objeto (host/sub-rede, endereço IP etc.), enquanto a segunda seção mostra a regra da NAT ligada a esse objeto. Se você tomar a primeira entrada na saída anterior:

Quando os hosts que correspondem à sub-rede 192.168.0.0/24 atravessam a interface interna em direção à interface externa, é desejável convertê-los dinamicamente para a interface externa.

## Etapa 2. Configure o NAT para acessar o servidor Web da Internet

Agora que os hosts nas interfaces interna e DMZ podem sair para a Internet, você precisará modificar a configuração para que usuários da Internet possam acessar o nosso servidor Web na porta TCP 80. Nesse exemplo, a instalação é feita de forma que as pessoas na Internet possam se conectar a outro endereço IP fornecido pelo ISP, um endereço IP adicional de nossa *propriedade*. Para esse exemplo, use 198.51.100.101. Com essa configuração, os usuários na Internet podem acessar o servidor Web DMZ acessando 198.51.100.101 na porta TCP 80. Use NAT de objeto para esta tarefa, e o ASA pode converter a porta TCP 80 no servidor web (192.168.1.100) para parecer com 198.51.100.101 na porta TCP 80 no exterior. Semelhante ao que foi feito anteriormente, defina um objeto e as regras de conversão para esse objeto. Além disso, defina um segundo objeto para representar o IP para o qual você pode converter esse host.

Essa configuração é semelhante a:

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

Quando um host que coincide com o endereço IP 192.168.1.100 nos segmentos do DMZ estabelece uma conexão originária da porta TCP 80 (www) e essa conexão sai da interface externa, recomenda-se convertê-la para a porta TCP 80 (www) na interface externa e converter esse endereço IP para 198.51.100.101.

Isso parece um pouco estranho... "originado da porta TCP 80 (www)", mas o tráfego da Web é destinado à porta 80. É importante compreender que essas regras de NAT são bidirecionais por natureza. Como resultado, você pode inverter o texto ao redor para reformular essa frase. O resultado faz muito mais sentido:

Quando os hosts externos estabelecem uma conexão com 198.51.100.101 na porta TCP 80 (www) de destino, você pode converter o endereço IP de destino em 192.168.1.100 e a porta de destino pode ser a porta TCP 80 (www) e enviá-lo pela DMZ.

Assim a frase faz mais sentido. Em seguida, você precisa configurar as ACLs.

## Etapa 3. Configurar ACLs

A NAT está configurada e estamos chegando ao fim desta configuração. Lembre-se, as ACLs no ASA permitem substituir o comportamento de segurança padrão que é o seguinte:

- O tráfego que vai de uma interface de segurança de nível inferior é negado quando ele vai para uma interface de segurança de nível mais elevado.
- O tráfego que vai de uma interface de segurança de nível mais elevado é permitido quando ele vai para uma interface de segurança de nível inferior.

Então, sem adição de qualquer ACL à configuração, esse tráfego no exemplo funciona:

- Hosts no interior (nível de segurança 100) podem se conectar a hosts no DMZ (nível de segurança de 50).
- Hosts no interior (nível de segurança 100) podem se conectar a hosts no exterior (nível de segurança de 0).
- Hosts no DMZ (nível de segurança 50) podem se conectar a hosts no exterior (nível de segurança de 0).

No entanto, este tráfego é negado:

- Hosts no exterior (nível de segurança 0) não podem se conectar a hosts no interior (nível de segurança de 100).
- Hosts no exterior (nível de segurança 0) não podem se conectar a hosts no DMZ (nível de segurança de 50).
- Hosts no DMZ (nível de segurança 50) não podem se conectar a hosts no interior (nível de segurança de 100).

Como o tráfego do exterior para a rede DMZ é negado pelo ASA com sua configuração atual, os usuários da Internet não podem alcançar o servidor Web, apesar da configuração de NAT na etapa 2. Você precisa permitir explicitamente este tráfego. No 8.3 e posteriores, você deve usar o IP real do host na ACL e não o IP convertido. Isso significa que a configuração precisa permitir o tráfego destinado a 192.168.1.100 e NÃO o tráfego destinado a 198.51.100.101 na porta 80. Para simplificar, os objetos definidos na etapa 2 também podem ser usados para essa ACL. Uma vez que a ACL é criada, você precisa aplicá-la de entrada na interface externa.

Os comandos de configuração têm a seguinte aparência:

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

Os estados de linha da lista de acesso:

Permitir o tráfego de any (qualquer lugar) para o host representado pelo objeto webserver (192.168.1.100) na porta 80.

Éimportante que a configuração use a palavra any aqui. Como o endereço IP de origem dos clientes não é conhecido quando chega ao site, especifique any significando “Qualquer endereço IP”.

E o tráfego do segmento do DMZ destinado aos hosts no segmento dentro da rede? Por exemplo, um servidor na rede interna ao qual os hosts no DMZ precisam se conectar. Como pode o ASA permitir somente o tráfego específico destinado ao servidor interno e bloquear o resto destinado ao segmento interno do DMZ?

Este exemplo presume que existe um servidor DNS na rede interna no endereço IP 192.168.0.53 que os hosts no DMZ precisam acessar para a resolução de DNS. Você cria a ACL necessária e a aplica à interface do DMZ para que o ASA possa substituir esse comportamento padrão de

segurança, mencionado anteriormente, para o tráfego que entra nessa interface.

Os comandos de configuração têm a seguinte aparência:

```
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
```

A ACL é mais complexa do que simplesmente permitir o tráfego para o servidor DNS na porta UDP 53. Se tudo o que fizéssemos fosse essa primeira linha de permissão, todo o tráfego seria bloqueado da DMZ para os hosts na Internet. As ACLs têm um “deny ip any any” implícito ao final da ACL. Como resultado, os hosts DMZ não seriam capazes de sair para a Internet. Mesmo que o tráfego do DMZ para o exterior fosse permitido por padrão, com a aplicação de uma ACL para a interface do DMZ, os comportamentos padrão de segurança para a interface do DMZ já não estariam em vigor e você deveria permitir explicitamente o tráfego na interface da ACL.

## Etapa 4. Testar a configuração com o recurso Packet Tracer

Agora que a configuração foi concluída, você precisa testá-lo para verificar o funcionamento. O método mais fácil é usar hosts reais (se esta for sua rede). No entanto, com o interesse de testar isso a partir da CLI e explorar ainda mais algumas das ferramentas do ASA, use o packet tracer para testar e possivelmente depurar quaisquer problemas encontrados.

O Packet Tracer funciona simulando um pacote com base em uma série de parâmetros e injetando esse pacote para o caminho de dados da interface, semelhante à maneira como um pacote seria se fosse apanhado fora de conexão. Esse pacote é acompanhado através de várias verificações e processos que são feitos enquanto ele passa pelo firewall, e o Packet Tracer observa o resultado. Simule o host interno saindo para um host na Internet. Esse comando instrui o firewall a:

Simule um pacote de TCP que chega à interface interna do endereço IP 192.168.0.125 na porta de origem 12345 destinada a um endereço IP 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 é permitido, ou seja, passou todas as verificações de NAT e ACL na configuração e foi enviado para interface de saída, externa. Observe que o pacote foi convertido na fase 3, e os detalhes da fase mostram qual regra é atingida. O host 192.168.0.125 é convertido de forma dinâmica para 198.51.100.100, conforme a configuração.

Agora, execute-o para uma conexão da Internet para o servidor Web. Lembre-se de que os hosts na Internet podem acessar o servidor Web conectando-se a 198.51.100.101 na interface externa. Mais uma vez, este próximo comando é convertido em:

Simule um pacote de TCP que chega à interface externa do endereço IP 192.0.2.123 na porta de

origem 12345 destinada a um endereço IP 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
```

Novamente, o resultado é que o pacote é permitido. As ACLs fazem check-out, a configuração parece boa e os usuários na Internet (externa) podem acessar esse servidor Web com o IP externo.

# Verificar

Os procedimentos de verificação estão incluídos na Etapa 4 - Teste de configuração com o recurso Packet Tracer.

# Troubleshoot

No momento, não há informações específicas disponíveis sobre como solucionar problemas dessa configuração.

# Conclusão

A configuração de um ASA para fazer NAT básico não é tão difícil de uma tarefa. O exemplo neste documento pode ser adaptado para seu cenário específico se você alterar os endereços IP e as portas usadas nas configurações de exemplo. A configuração final do ASA, quando combinada, é semelhante a esta 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 interfaces conectadas conforme mostrado anteriormente (externa conectada à Ethernet0/0, interna conectada à Ethernet0/1 e o DMZ conectado à 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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.