

# 在ASA防火墙上配置网络地址转换和ACL

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [背景信息](#)

### [概述](#)

#### [目标](#)

#### [访问控制列表概述](#)

#### [NAT 概述](#)

### [配置](#)

#### [使用入门](#)

#### [拓扑](#)

#### [步骤1:将NAT配置为允许主机访问Internet](#)

#### [第二步：配置NAT以从Internet访问Web服务器](#)

#### [第三步：配置 ACL](#)

#### [第四步：使用Packet Tracer功能测试配置](#)

### [验证](#)

### [故障排除](#)

### [结论](#)

---

## 简介

本文档介绍如何在ASA防火墙上配置网络地址转换(NAT)和访问控制列表(ACL)。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于运行 ASA 代码版本 9.1 (1) 的 ASA 5510 防火墙。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 背景信息

本文档介绍如何在ASA防火墙上配置NAT和ACL以允许出站和入站连接的简单明了的示例。它使用 Adaptive Security Appliance(ASA)5510防火墙编写，而不是运行ASA代码版本9.1(1)，但这可以轻松应用于任何其他ASA防火墙平台。如果您使用 ASA 5505 等用 VLAN 代替物理接口的平台，则需要相应地更改接口类型。

## 概述

### 目标

在此示例配置中，您可以查看需要哪些NAT和ACL配置才能允许对ASA防火墙DMZ中Web服务器的入站访问，并允许来自内部和DMZ主机的出站连接。这可以概括为以下两个目标：

1. 允许内部和 DMZ 上的主机到互联网的出站连接。
2. 允许互联网上的主机使用 IP 地址 192.168.1.100 访问 DMZ 上的 Web 服务器。

在执行完成这两个目标所必须完成的步骤之前，本文档简要介绍了ACL和NAT在较新版本ASA代码（版本8.3及更高版本）上的工作方式。

### 访问控制列表概述

访问控制列表（简称访问列表或 ACL）是 ASA 防火墙在确定是允许还是拒绝流量时所用的方法。默认情况下，防火墙会拒绝从较低安全级别流向较高安全级别的流量。这可由应用于较低安全性接口的 ACL 改写。此外，ASA 默认允许从较高安全性接口到较低安全性接口的流量。此行为也可以使用 ACL 改写。

在较早版本（8.2 版和更低版本）的 ASA 代码中，ASA 会在先没有首先反向转换数据包的情况下，并将传入连接或数据包与接口上的 ACL 进行比较。换句话说，ACL 必须允许该数据包，就像要在接口上捕获该数据包一样。在 8.3 版和更高版本的代码中，ASA 在检查接口 ACL 之前不会反向转换该数据包。这意味着，对于 8.3 版和更高版本的代码以及本文档来说，允许到主机的实际 IP 的流量，而不是到主机的已转换 IP 的流量。

有关ACL的详细信息，请参阅[手册2: Cisco ASA系列防火墙CLI配置指南9.1](#)的[配置访问规则](#)部分。

### NAT 概述

8.3 版和更高版本 ASA 中的 NAT 分成两种类型：自动 NAT（对象 NAT）和手动 NAT（两次 NAT）。前者（即对象 NAT）在网络对象的定义中进行配置。本文档后面会提供相关示例。此 NAT 方法的一个主要优点是 ASA 会自动对处理规则进行排序，以避免冲突。这是最简单的 NAT 形式，但这种简单的特点使得配置粒度方面存在限制。例如，无法根据数据包中的目标做出转换决定，而第二种 NAT 类型（即手动 NAT）可以。手动 NAT 的粒度更稳定，但需要按正确的顺序配置行，才能实现正确的行为。这会使此NAT类型复杂化，因此不能在此配置示例中使用它。

有关NAT的详细信息，请参阅[第2册：Cisco ASA系列防火墙CLI配置指南9.1](#)的[有关NAT的信息](#)部分。

。

# 配置

## 使用入门

基本的 ASA 配置设置是将三个接口连接到三个网段。ISP 网段连接到 Ethernet0/0 接口，标记为外部，安全级别为 0。内部网络连接到 Ethernet0/1，标记为内部，安全级别为 100。Web 服务器驻留的 DMZ 段连接到 Ethernet0/2，标记为 DMZ，安全级别为 50。

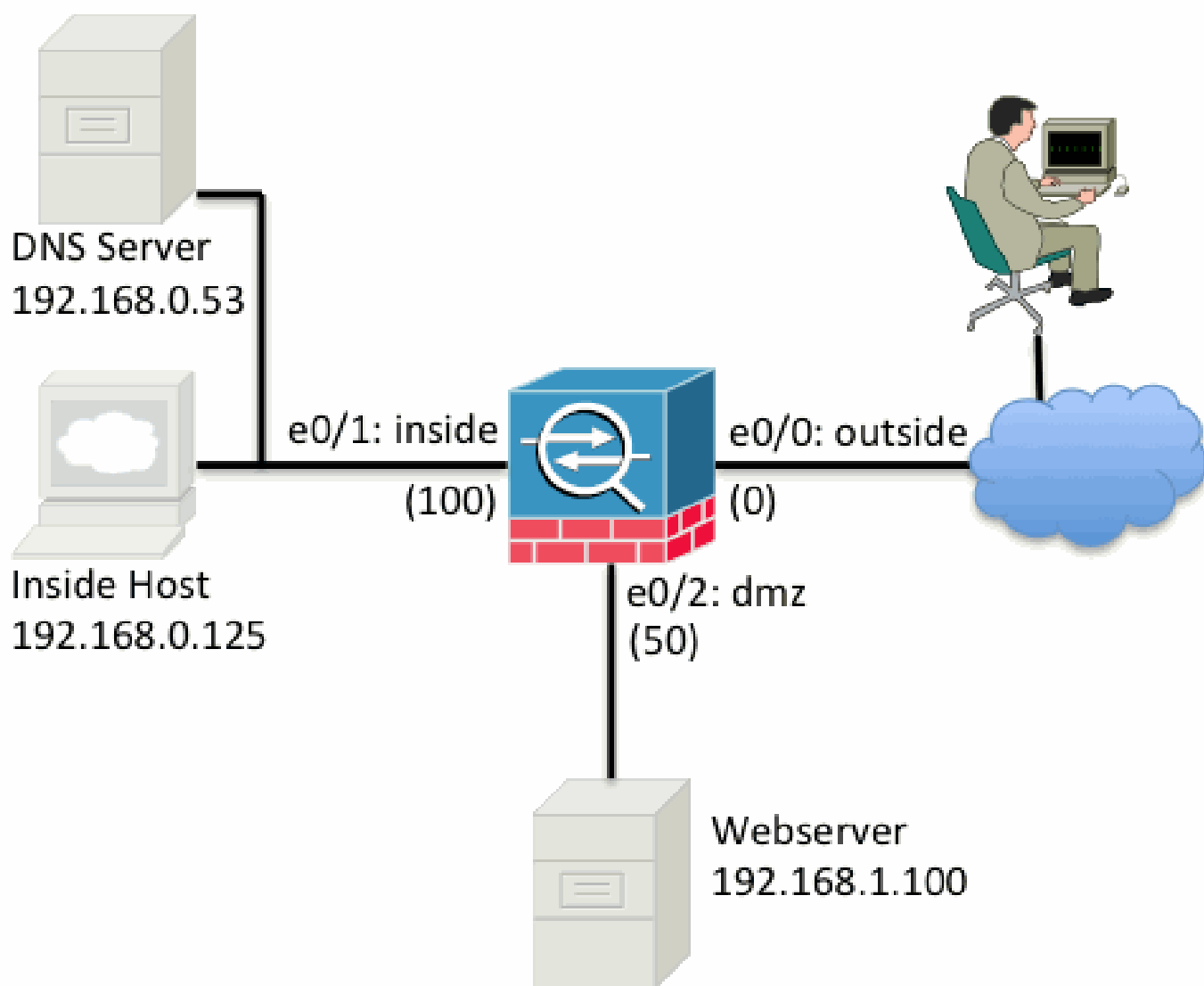
该示例中的接口配置和 IP 地址如下所示：

```
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
```

在此，您可以看到，ASA 内部接口的 IP 地址设为 192.168.0.1，这是内部主机的默认网关。ASA 外部接口配置的 IP 地址获取自 ISP。存在一个默认路由，它将下一跳设置为 ISP 网关。如果使用 DHCP，系统会自动提供。DMZ 接口配置的 IP 地址为 192.168.1.1，这是 DMZ 网段上主机的默认网关。

## 拓扑

下图以直观的方式显示了具体的连接和配置：



## 步骤1:将NAT配置为允许主机访问Internet

在本示例中，使用对象NAT（也称为AutoNAT）。首先，配置 NAT 规则，以便允许内部和 DMZ 段上的主机连接到互联网。因为这些主机使用专用 IP 地址，所以您需要将其转换为可在互联网上路由的内容。在本例中，转换这些地址，使之看起来像 ASA 外部接口的 IP 地址。如果外部 IP 经常更改（可能是由于使用 DHCP），这是设置此项的最简单方法。

要配置此 NAT，需要创建一个表示内部子网的网络对象和一个表示 DMZ 子网的网络对象。在这些对象中的每个对象中，配置一个动态nat规则，这些客户端从各自的接口传递到外部接口时，该规则可以对这些客户端进行端口地址转换(PAT)。

此配置如下所示：

```
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
```

如果您查看此时的运行配置（使用show run命令的输出），可以看到对象定义被拆分为输出的两个部分。第一部分仅指示对象中的内容（主机/子网、IP 地址等），而第二部分则显示与该对象关联的 NAT 规则。如果获取采纳之前输出中的第一个条目：

当与 192.168.0.0/24 子网匹配的主机从内部接口遍历到外部接口时，您需要将其动态转换为外部接口。

## 第二步：配置 NAT 以从 Internet 访问 Web 服务器

既然内部和 DMZ 接口上的主机可以连接到互联网，您就需要修改配置，以便互联网用户可以访问 TCP 端口 80 上的 Web 服务器。在本例中，设置的目的是为了让互联网用户可以连接到 ISP 提供的另一个 IP 地址，也就是我们拥有的另一个 IP 地址。本例使用 198.51.100.101。使用此配置，互联网上的用户可以通过访问 TCP 端口 80 上的 198.51.100.101 来访问 DMZ Web 服务器。此任务使用对象 NAT，ASA 可以将 Web 服务器 (192.168.1.100) 上的 TCP 端口 80 转换为类似于外部 TCP 端口 80 上的 198.51.100.101。具体操作与以前类似：定义对象并为该对象定义转换规则。此外，定义第二个对象来表示可将此主机转换到的 IP。

此配置如下所示：

```
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
```

下面总结一下此 NAT 规则在本例中的含义：

如果与 DMZ 段上的 IP 地址 192.168.1.100 匹配的主机从 TCP 端口 80 (www) 建立连接，但该连接要扩展到外部接口，则您需要将其转换为外部接口上的 TCP 端口 80 (www)，并将该 IP 地址转换为 198.51.100.101。

这似乎有点奇怪……“源自 TCP 端口 80 (www)”，但 Web 流量发往端口 80。务必要了解这些 NAT 规则在本质上是双向的。因此，为了对这句话重新措辞，可以反向来表达。这样意思会更明确：

当外部主机在目标 TCP 端口 80 (www) 上建立到 198.51.100.101 的连接时，您可以将目标 IP 地址转换为 192.168.1.100，目标端口可以转换为 TCP 端口 80 (www)，并将其发送到 DMZ。

这样措辞会更容易理解。接下来，您需要设置 ACL。

## 第三步：配置 ACL

NAT 已完成配置，本次配置接近尾声。请记住，ASA 上的 ACL 可用于改写默认的安全行为，具体如下所述：

- 如果流量从较低安全性接口流向较高安全性接口，该流量将遭到拒绝。

- 如果流量从较高安全性接口流向较低安全性接口，该流量将得到允许。

因此，如果配置中未添加任何 ACL，则示例中的以下流量会正常工作：

- 内部（安全级别为 100）主机可以连接到 DMZ（安全级别为 50）主机。
- 内部（安全级别为 100）主机可以连接到外部（安全级别为 0）主机。
- DMZ（安全级别为 50）主机可以连接到外部（安全级别为 0）主机。

但是，以下流量会遭到拒绝：

- 外部（安全级别为 0）主机无法连接到内部（安全级别为 100）主机。
- 外部（安全级别为 0）主机无法连接到 DMZ（安全级别为 50）主机。
- DMZ（安全级别为 50）主机无法连接到内部（安全级别为 100）主机。

ASA 会因其当前配置而拒绝从外部到 DMZ 网络的流量，因此，尽管在第 2 步中配置了 NAT，互联网用户也无法访问 Web 服务器。您需要明确允许此流量。在 8.3 版和更高版本的代码中，必须使用 ACL 中主机的实际 IP 而不是转换后的 IP。这意味着，配置必须允许流向 192.168.1.100 的流量，并且不允许流向端口 80 上的 198.51.100.101 的流量。为简单起见，步骤 2 中定义的对象也可以用于此 ACL。创建 ACL 后，需要将其应用到外部接口上的入站。

具体配置命令如下所示：

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

访问列表行表明：

允许流量从任何（地方）流向端口 80 上的 Web 服务器 (192.168.1.100) 对象所表示的主机。

值得注意的是，此处的配置使用了 any（任何）这个关键字。由于客户端的源 IP 地址到达您的网站时并不知道，因此请指定 any 含义，Any IP address。

从 DMZ 段到内部网络段的主机的流量如何会怎样呢？例如，DMZ 主机需要连接到的内部网络中的服务器。ASA 如何才能只允许特定流量到达内部服务器，同时阻止所有其他从 DMZ 到内部网段的流量？

在本例中，假定内部网络上有一个 IP 地址为 192.168.0.53 的 DNS 服务器，DMZ 上的主机需要访问该服务器以进行 DNS 解析。您创建所需的 ACL 并将其应用于 DMZ 接口，以便 ASA 可以为进入该接口的流量改写前述的默认安全行为。

具体配置命令如下所示：

```
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
```

与仅允许该流量到达 UDP 端口 53 上的 DNS 服务器相比，ACL 要更复杂。如果我们所做的只是第一条允许线路，则所有流量都会被阻止从DMZ传输到互联网上的主机。ACL末尾有一个隐式deny IP any any。因此，DMZ 主机将无法访问互联网。尽管默认情况下允许从 DMZ 到外部的流量，但如果将 ACL 应用到 DMZ 接口，则 DMZ 接口的默认安全行为将不再有效，必须显式允许接口 ACL 中的流量。

#### 第四步：使用Packet Tracer功能测试配置

现在配置已完成，您需要对其进行测试以确保其有效。最简单的方法是使用实际主机（前提是这是您的网络）。但是，为了从CLI测试此情况并进一步探索ASA的一些工具，请使用packet tracer测试遇到的任何问题并对其进行可能的调试。

Packet Tracer 的工作原理是，根据一系列参数模拟数据包，并将该数据包注入到接口数据路径中，此方法类似于离线获取真实的数据包。此数据包在通过防火墙时会经历无数项检查和流程，Packet Tracer 会记录最终结果。模拟内部主机连接互联网上的主机。此命令指示防火墙：

模拟进入内部接口的 TCP 数据包从源端口 12345 上的 IP 地址 192.168.0.125 到达端口 80 上的 IP 地址 203.0.113.1。

```
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

最终结果是该流量得到了允许，这意味着，该数据包通过了配置中的所有 NAT 和 ACL 检查并且已发送到外部的出口接口。请注意，数据包是在第 3 阶段进行转换的，该阶段的详细信息显示了所符合的规则。主机 192.168.0.125 根据配置动态转换为 198.51.100.100。

现在，运行它以便从互联网连接到 Web 服务器。请记住，Internet 上的主机可以通过连接到外部接口上的 198.51.100.101 来访问 Web 服务器。此外，以下命令意味着：

模拟进入外部接口的 TCP 数据包从源端口 12345 上的 IP 地址 192.0.2.123 到达端口 80 上的 IP 地址 198.51.100.101。

```
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
```

结果同样是数据包获得了允许。ACL检查后，配置看起来正常，Internet（外部）的用户可以使用外部IP访问该Web服务器。

## 验证

“第 4 步 - 使用 Packet Tracer 功能测试配置”中包括验证过程。

## 故障排除

目前没有关于如何对此配置进行故障排除的具体信息。

## 结论

配置ASA执行基本NAT并不是一项很困难的任務。如果您使用的 IP 地址和端口与配置示例中的不同，可以根据您的具体场景调整本文档中的示例。经过组合，最终的 ASA 配置类似于 ASA 5510 的配置：

```
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

```

例如，在 ASA 5505 上，接口的连接如前所述（外部网络连接到 Ethernet0/0、内部网络连接到 Ethernet0/1、DMZ 连接到 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
```

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。