为双内网配置 ASA

目录

简介

本文档介绍如何配置运行软件版本 9.x 的 Cisco Adaptive Security Appliance (ASA) 以使用两个内部网络。

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软件版本9.x的Cisco ASA。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

在ASA防火墙后添加第二个内部网络时，请考虑以下重要信息：

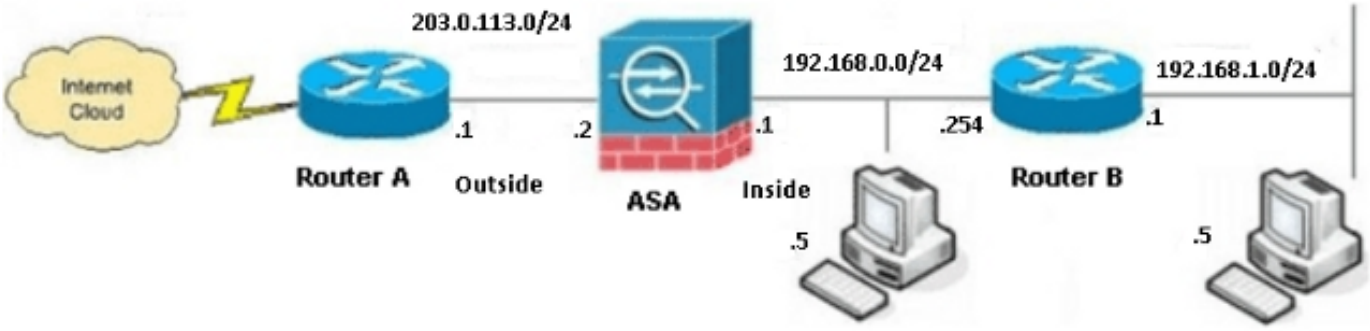
- ASA 不支持附属寻址。
- 必须在ASA后面使用路由器，才能在当前网络和新添加的网络之间实现路由。
- 所有主机的默认网关必须指向内部路由器。
- 您必须在指向ASA的内部路由器上添加默认路由。
- 您必须清除内部路由器上的地址解析协议(ARP)缓存。

配置

使用本节中介绍的信息配置ASA。

网络图

以下是本文档中示例所使用的拓扑：



> **注意**：此配置中使用的IP编址方案在Internet上不可合法路由。它们是实验室环境中使用的RFC 1918地址。

ASA 9.x配置

如果您有来自Cisco设备的**write terminal**命令的输出，则可以使用Output Interpreter工具（仅限注册

客户）来显示潜在问题和解决方法。

以下是运行软件版本9.x的ASA的配置：

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
```

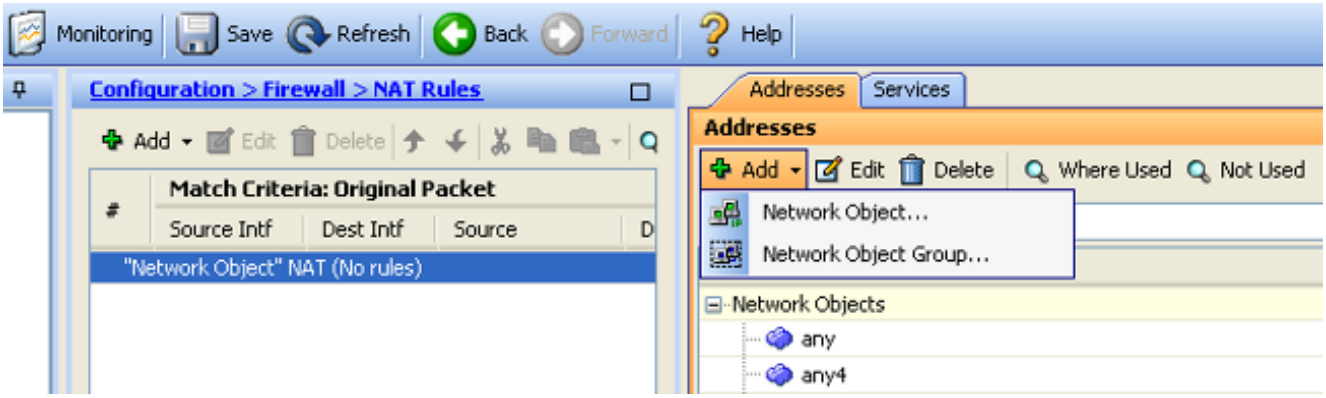
```
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

允许内部主机使用 PAT 访问外部网络

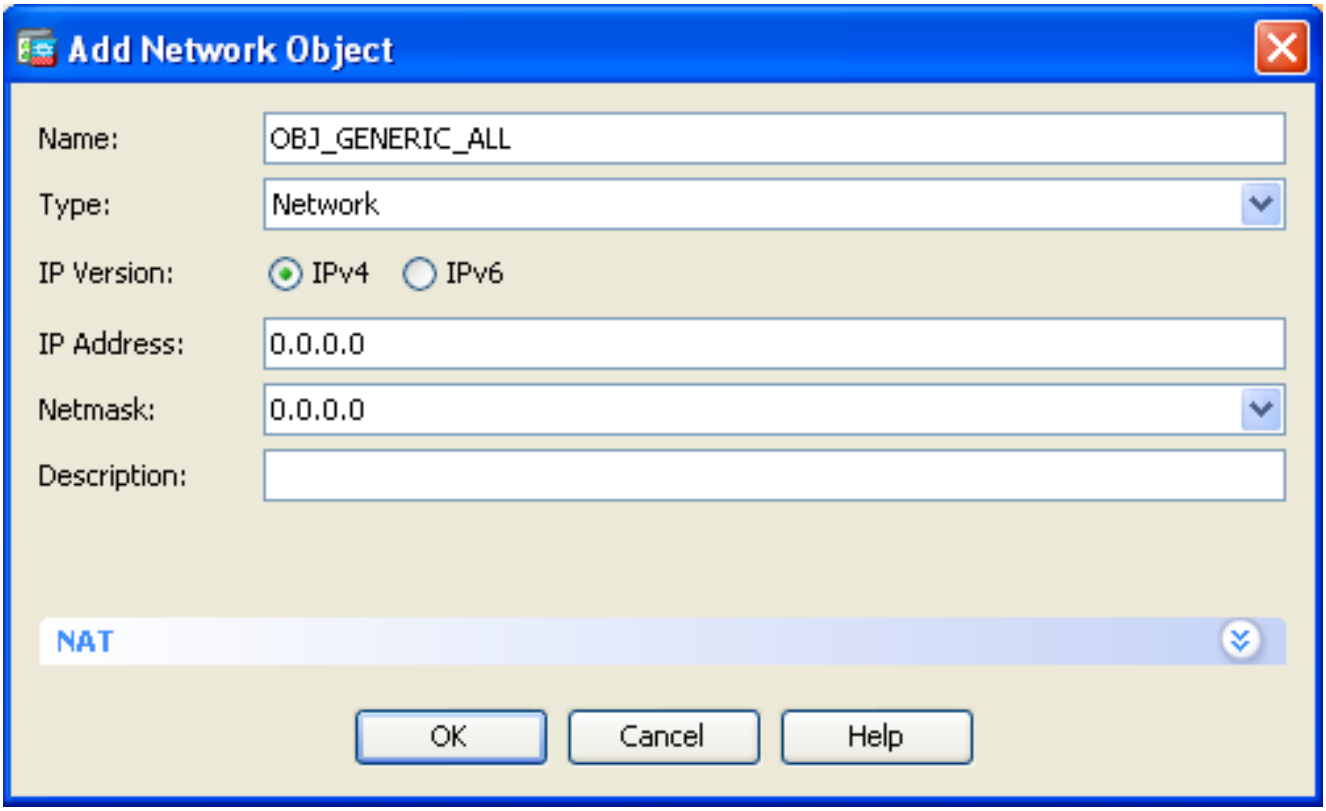
如果希望内部主机共享一个公共地址进行转换，请使用端口地址转换(PAT)。 最简单的PAT配置之一包括转换所有内部主机，使其看起来是外部接口IP。这是ISP提供的可路由IP地址数量限制为少数（或仅限一个）时使用的典型PAT配置。

要允许内部主机通过PAT访问外部网络，请完成以下步骤：

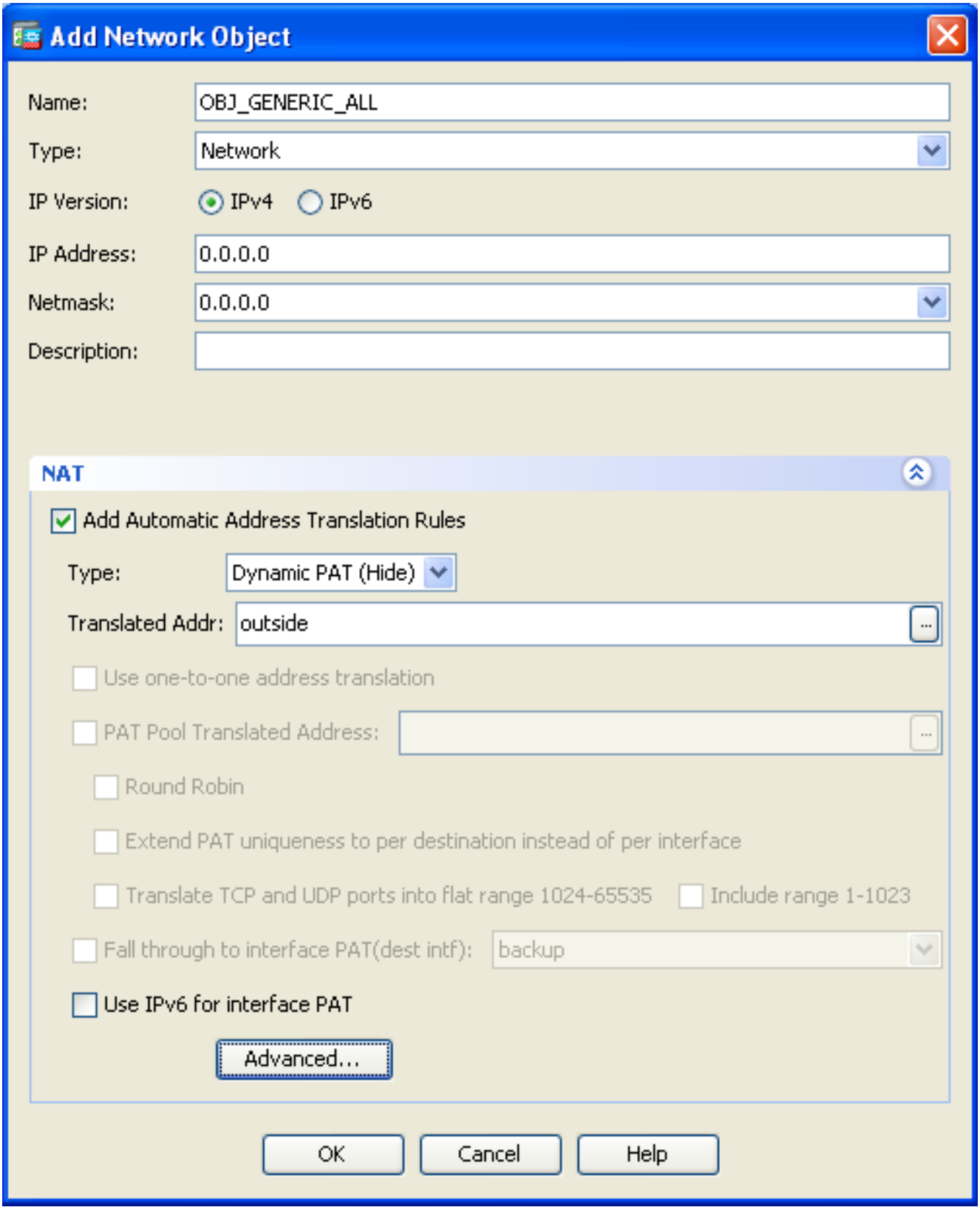
1. 导航至Configuration > **Firewall** > NAT Rules，单击**Add**，然后选择**Network Object**以配置动态NAT规则：



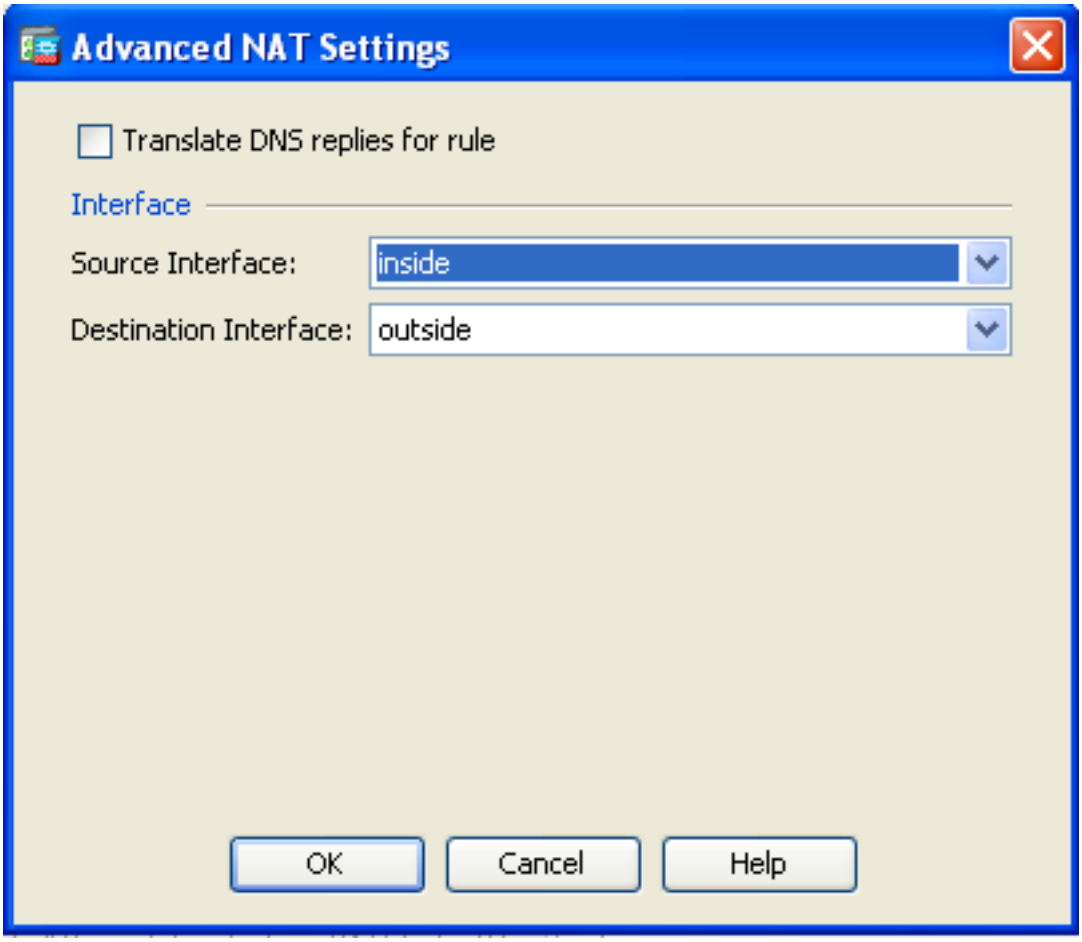
2. 配置需要动态PAT的网络/主机/范围。在本例中，已选择所有内部子网。对于要以这种方式转换的特定子网，应重复此过程：



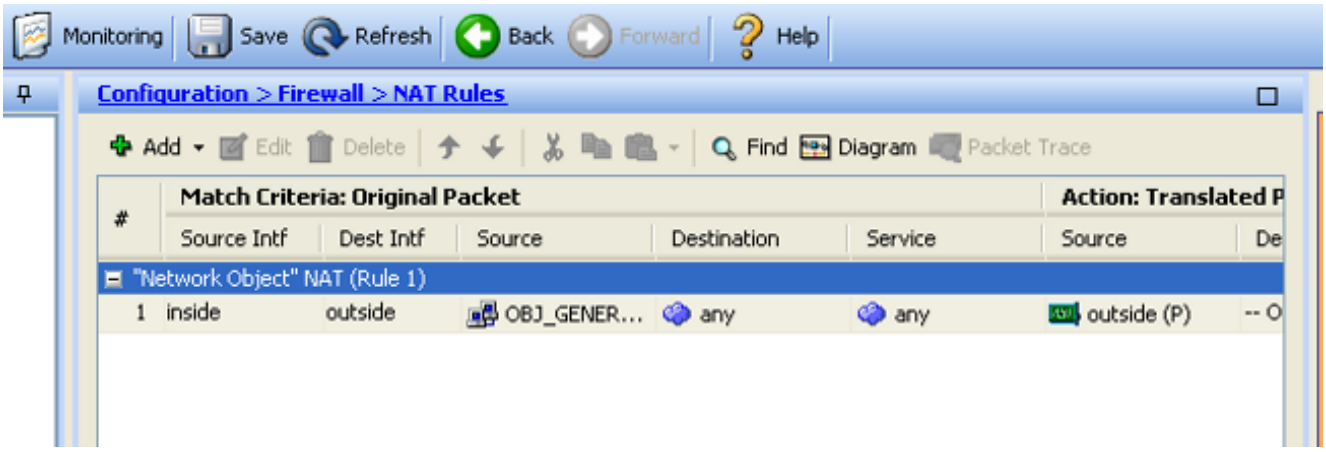
3. 单击**NAT**，选中**添加自动地址转换规则**复选框，输入**动态，并设置"已转换的地址"**选项，以便它能够反映外部接口。如果单击省略号按钮，它将帮助您选择预配置的对象，例如外部接口：



4. 单击**Advanced**以选择源接口和目标接口：



5. 单击**OK**，然后单击**Apply**以应用更改。完成后，自适应安全设备管理器(ASDM)显示NAT规则：



路由器 B 配置

以下是路由器B的配置：

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

验证

通过Web浏览器通过HTTP访问网站，以验证配置是否正常工作。

此示例使用托管于IP地址*198.51.100.100*的站点。如果连接成功，ASA CLI上可以看到以下各节中提供的输出。

连接

输入**show connection address**命令以验证连接：

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA是状态防火墙，并且允许来自Web服务器的返回流量通过防火墙，因为它与防火墙连接表*中的*连接匹配。匹配现有连接的流量可通过防火墙，而不会被接口访问控制列表(ACL)阻止。

在上面的输出中，内部接口上的客户端已经与外部接口上的主机 198.51.100.100 建立了连接。此连接是通过 TCP 协议建立的，而且已空闲 6 秒。连接标记表明此连接的当前状态。

注意：有关连接标志的详细信息，请参阅ASA TCP连接标志(连接建立和拆卸)Cisco文档。

故障排除

使用本节中介绍的信息排除配置问题。

系统日志

输入**show log**命令以查看系统日志：

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:192.168.1.5/58799 (203.0.113.2/58799)
```

在正常运行期间，ASA 防火墙会生成系统日志。根据日志记录配置，系统日志的内容十分丰富。输出显示了在第6级或信息级看到的两个系*统日*志。

在此示例中，防火墙生成了两个系统日志。第一个是指示防火墙已建立转换的日志消息；具体而言，是动态TCP转换(PAT)。 它指示流量从内部接口传输到外部接口时的源IP地址和端口，以及转换后的IP地址和端口。

第二个日志记录表明，防火墙已在其连接表中为该客户端与服务器之间的特定流量创建了一条连接。如果防火墙配置为阻止此连接尝试，或某些其他因素阻止了此连接的创建（资源限制或可能的配置错误），则防火墙不会生成指示已建立连接的日志。相反，它会记录连接被拒绝的原因或与阻止创建连接的因素有关的指示。

数据包跟踪器

输入以下命令以启用Packet Tracer功能：

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80

--Omitted--
```

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

ASA上的Packet Tracer功能允许您指定模拟数据包，并查看防火墙在处理流量时完成的所有步骤、检查和功能。使用此工具，可以确定您认为应允许通过防火墙的*流量*示例，并使用该5管来模拟流量。在上面的示例中，我们使用 Packet Tracer 来模拟符合下列条件的连接尝试：

- 模拟数据包到达内部接口。
- 使用的协议是TCP。
- 模拟客户端 IP 地址为 192.168.1.5。
- 客户端发送来自端口1234的流量。
- 流量的目的位置是 IP 地址为 198.51.100.100 的服务器。
- 流量抵达于端口 80。

请注意，命令中未提及外部接口。这是由Packet Tracer设计造成的。该工具会帮助您了解防火墙如何处理这类连接尝试，包括如何执行路由、从哪个接口离开等等。

> **提示：**有关Packet Tracer功能的详细信息，请参阅*Cisco ASA 5500系列配置指南（使用CLI、8.4和8.6）的*Packet Tracer跟踪数据包部分。

捕获

输入以下命令以应用捕获：

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured
```

```
1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA防火墙可以捕获进入或离开其接口的流量。此捕获功能非常出色，因为它可以明确证明流量是到达还是离开防火墙。上一个示例显示了在内部和外部接口上分别配置名为**capin**和**capout**的两个捕获。**capture**命令使用**match**关键字，该关键字允许您指定要捕获的流量。

对于*capin* 捕获示例，表示要匹配在与*tcp主机192.168.1.5主机198.51.100.100*匹配的内部接口（入口或出口）上看到的流量。换句话说，要捕获发送的任何TCP流量从主机*192.168.1.5*到主机*198.51.100.100*，反之亦然。使用 match 关键字可以使防火墙双向捕捉流量。为外部接口定义的**capture**命令不引用内部客户端IP地址，因为防火墙对该客户端IP地址执行PAT。所以我们无法对该客户端 IP 地址进行匹配操作。因此，示例中使用 any 关键字来指代所有可能与该条件匹配的 IP 地址。

配置捕获后，您可以尝试再次建立连接，然后使用show capture<capture_name>命***令继续查看捕***获。在本例中，您可以看到客户端能够连接到服务器，这一点在捕获中看到的TCP三次握手中可见。

相关信息

- Cisco 自适应安全设备管理器
- Cisco ASA 5500-X系列下一代防火墙
- 请求注解(RFC)
- Cisco ASA系列CLI配置指南， 9.0 - Configuring Static和Default Routes
- 技术支持和文档 阿阿 Cisco Systems