

# ASA 8.4(x)将单个内部网络连接到Internet配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[ASA 8.4 配置](#)

[路由器配置](#)

[ASA 8.4 及更高版本的配置](#)

[验证](#)

[连接](#)

[系统日志](#)

[NAT 转换 \(Xlate\)](#)

[故障排除](#)

[Packet-Tracer](#)

[捕获](#)

[相关信息](#)

## 简介

本文档介绍如何设置8.4(1)版的思科自适应安全设备(ASA)，以在单个内部网络上使用。

请参阅 [PIX/ASA：使用Internet连接单个内部网络配置示例](#)，用于8.2及更低版本ASA上的相同配置。

## 先决条件

### 要求

本文档没有任何特定的前提条件。

### 使用的组件

本文档中的信息基于版本为8.4(1)的ASA。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

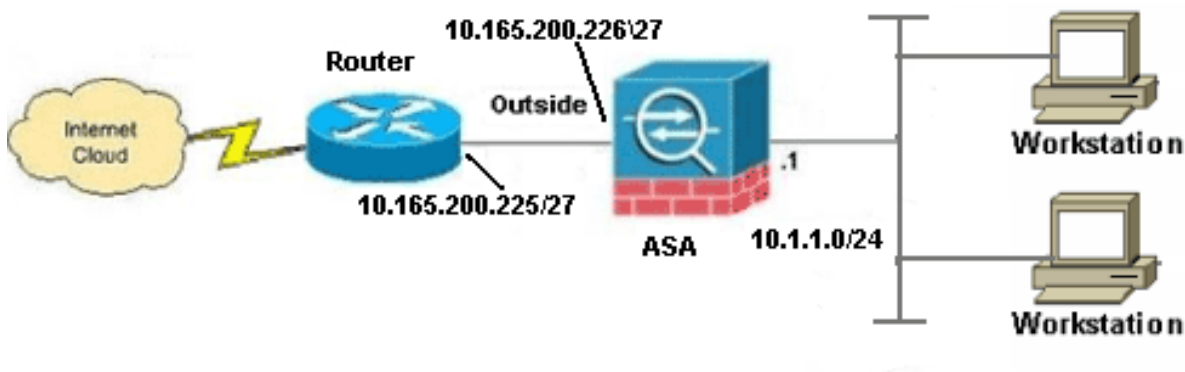
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：**要查找有关本文档中所使用的命令的详细信息，请使用[命令查找工具（仅限注册用户）](#)。

## 网络图

本文档使用以下网络设置：



**注意：**此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 [RFC 1918 地址](#)。

## ASA 8.4 配置

本文档使用以下配置：

- 路由器配置
- ASA 8.4 及更高版本的配置

## 路由器配置

Building configuration...

Current configuration:

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

```

!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
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

```

## ASA 8.4 及更高版本的配置

```

ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1

```

```
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (PAT) to the outside interface IP
!--- on the ASA (or 10.165.200.226) for Internet bound traffic.
!
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
!
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
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:6fffb3dc9cb863fd71c71244a0ecc5f
: end
```

**注意：**有关ASA 8.4版上网络地址转换(NAT)和端口地址转换(PAT)配置的详细信息，请参阅[有关NAT的信息](#)。

有关在 ASA 版本 8.4 上配置访问列表的详细信息，请参阅[有关访问列表的信息](#)。

## 验证

尝试使用Web浏览器通过HTTP访问网站。本示例使用托管于198.51.100.100的站点。如果连接成功，则可在ASA CLI上看到以下输出：

## 连接

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA 是状态化防火墙，来自 Web 服务器的返回流量会因为与防火墙连接表中的**连接匹配，而被允许通过防火墙**。与既有连接匹配的流量不会被接口 ACL 阻止，即可通过防火墙。

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。有关连接标记的更多信息，可参阅 [ASA TCP 连接标记](#)。

## 系统日志

```
ASA(config)# show log | in 10.1.1.154
```

```
Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:  
10.1.1.154/58799 to outside:10.165.200.226/58799
```

```
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:10.1.1.154/58799 (10.165.200.226/58799)
```

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。上面的输入显示了两个第 6 级别（即“信息”级别）的系统日志。

在此示例中，防火墙生成了两个系统日志。第一个系统日志记录的消息表明，防火墙已建立了转换，并明确指出是动态 TCP 转换 (PAT)。从中可以看出流量从内部接口流向外部接口时的源 IP 地址和端口以及转换 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。如果防火墙已配置为阻止此连接尝试，或者有其他因素禁止创建此连接（资源限制或配置错误），防火墙不会生成日志来表明建立了此连接。在这种情况下，防火墙会生成一条日志来说明连接被拒绝的原因，或者指明禁止创建连接的因素。

## NAT 转换 (Xlate)

```
ASA(config)# show xlate local 10.1.1.154
```

```
3 in use, 80 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,  
s - static, T - twice, N - net-to-net
```

```
TCP PAT from inside:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle  
0:02:42 timeout 0:00:30
```

作为此配置的一部分，配置 PAT 是为了将内部主机 IP 地址转换为可在互联网上路由的地址。为了确认是否创建了这些转换，您可以查看 xlate（转换）表。show xlate 命令与 **local** 关键字和内部主机的 IP 地址结合使用时，会显示该主机的转换表中存在的所有条目。前面的输出显示，此主机当前在内部接口和外部接口之间建立了转换。根据我们的配置，内部主机 IP 和端口会转换为 10.165.200.226 地址。列出的标记 ri 表示转换是动态的，并且是端口映射。有关不同 NAT 配置的详细信息，请参阅：[有关 NAT 的信息](#)。

## 故障排除

ASA 提供多种工具来排除连接故障。如果在验证配置并检查之前列出的输出后问题仍然存在，这些工具和技术可能有助于确定连接故障的原因。

## Packet-Tracer

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 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
```

利用 ASA 的 Packet Tracer 功能，您可以指定一个模拟数据包，以便查看防火墙在处理流量时的各种步骤、检查和功能。使用此工具，可以确定您认为应允许流量通过防火墙的示例，并使用该 5-tuple 来模拟流量，这非常有帮助。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：

- 模拟数据包到达网络内部。
- 使用的协议是 TCP。
- 模拟客户端 IP 地址为 10.1.1.154。
- 客户端发送的流量源于端口 1234。
- 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。

需要注意的是，命令中未提及外部接口。这是由于 Packet Tracer 设计上的原因。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。有关 Packet Tracer 的更多信息，请参阅使用 Packet Tracer 跟踪数据包。

## 捕获

```
ASA# capture capin interface inside match tcp host 10.1.1.154 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      10.1.1.154.58799 > 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 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884      10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA# show capture capout
```

```
3 packets captured
```

```
1: 11:31:23.432869      10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914      10.165.200.226.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA 防火墙可以捕获进入或离开接口的流量。这个捕获功能非常有用，因为它可以明确证明流量是否已经到达或离开防火墙。上面提供了两个捕获的配置示例（在内部接口上执行的名为 capin 的捕获和在外部接口上执行的名为 capout 的捕获）。capture 命令中使用了 match 关键字，用于指定需要捕获的流量。

对于捕获捕获，您表示要匹配内部接口（入口或出口）上发现的与 tcp 主机 10.1.1.154 主机 198.51.100.100 匹配的流量。换句话说，您要捕获从主机 10.1.1 发送的任何 TCP 流量 1.154 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 命令未引用内部客户端 IP 地址，因为防火墙会在该客户端 IP 地址上执行 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，您将再次尝试建立连接，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，这一点从捕获中看到的 TCP 三次握手中可以明显看出。

## 相关信息

- [Cisco 自适应安全设备管理器](#)
- [Cisco ASA 5500 系列自适应安全设备](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)