

ASA 8.3(x) : 三个内部网络与互联网的连接配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[ASA 8.3 配置](#)

[ASA 8.3 及更高版本的配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

本文提供关于如何设置使用 8.3(1) 版本的思科自适应安全设备 (ASA) 以便用于三个内部网络的信息。为简单起见，在路由器上使用了静态路线。

请参阅 [PIX/ASA : 使用互联网连接三个内部网络的配置示例 \(适用于运行 8.2 及以前版本软件的思科自适应安全设备 \(ASA\) 上的相同配置\)](#)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息以使用 8.3(1) 版本的思科自适应安全设备 (ASA) 为基础。

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。

规则

有关文档规则的详细信息，请参阅[思科技术提示规则](#)。

配置

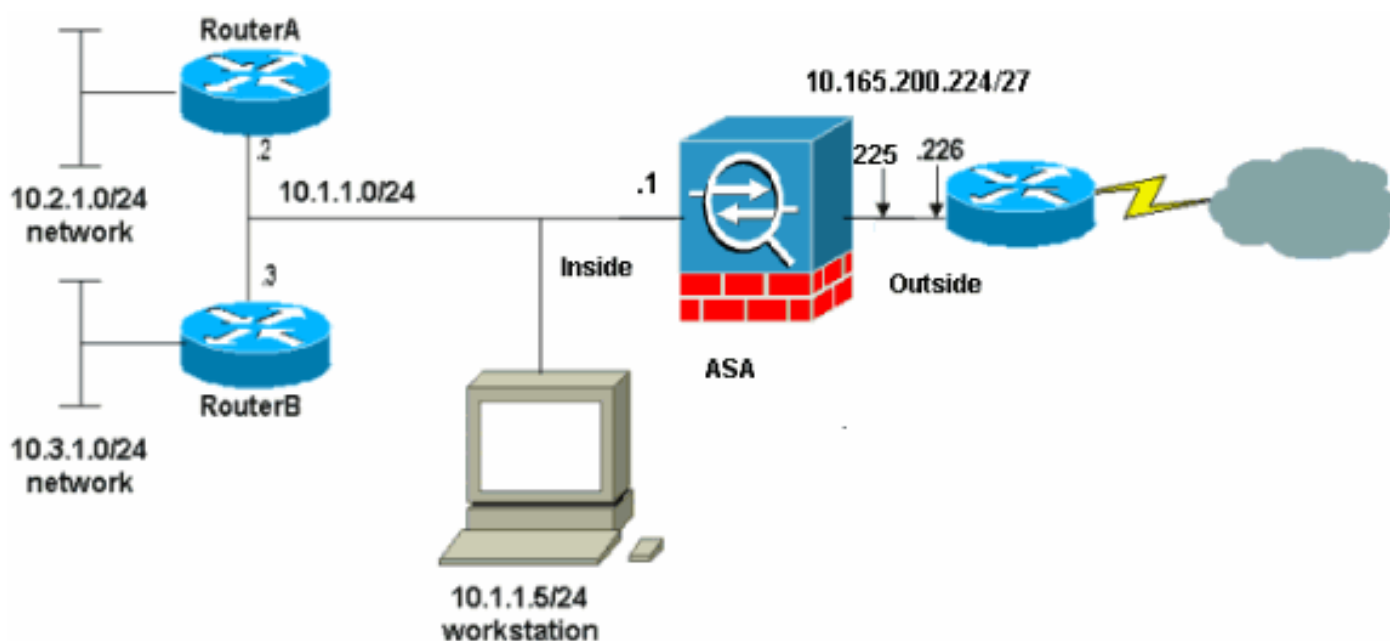
本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用[命令查找工具](#)([仅注册客户](#))。

网络图

本文档使用此网络设置。

注意：10.1.1.0网络上主机的默认网关指向路由器A。在 RouterB 上添加了指向 RouterA 的默认路线。路由器 A 有一个指向 ASA 内部接口的默认路由。



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 8.3 配置

本文档使用以下配置。

如果从 Cisco 设备中获得 `write terminal` 命令的输出，则可使用[命令输出解释程序](#)（[仅限注册用户](#)）显示潜在问题和解决方法。

- [RouterA 配置](#)
- [RouterB 配置](#)
- [ASA 8.3 及更高版本的配置](#)

RouterA 配置

```
RouterA#show running-config
Building configuration...
```

```
Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
```

```
!  
control-plane  
!  
!  
!  
line con 0  
line 33  
no activation-character  
no exec  
transport preferred none  
transport input all  
transport output all  
line aux 0  
line vty 0 4  
password ww  
login  
!  
!  
end  
  
RouterA#
```

RouterB 配置

```
RouterB#show running-config  
Building configuration...  
  
Current configuration : 1132 bytes  
!  
version 12.4  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname RouterB  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no network-clock-participate slot 1  
no network-clock-participate wic 0  
no network-clock-participate wic 1  
no network-clock-participate wic 2  
no network-clock-participate aim 0  
no network-clock-participate aim 1  
no aaa new-model  
ip subnet-zero  
ip cef  
!  
!  
!  
!  
ip audit po max-events 100  
no ip domain lookup  
no ftp-server write-enable  
!  
!  
!  
!  
no crypto isakmp enable
```

```
!  
!  
!  
interface FastEthernet0/0  
ip address 10.1.1.3 255.255.255.0  
duplex auto  
speed auto  
no cdp enable  
!  
interface FastEthernet0/1  
ip address 10.3.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface IDS-Sensor1/0  
no ip address  
shutdown  
hold-queue 60 out  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.1.1.2  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
stopbits 1  
line 33  
no activation-character  
no exec  
transport preferred none  
transport input all  
transport output all  
line aux 0  
line vty 0 4  
password cisco  
login  
!  
!  
end  
  
RouterB#
```

[ASA 8.3 及更高版本的配置](#)

注意：非默认命令以粗体显示。

ASA 8.3(1) 运行配置

```
ASA#show run  
: Saved  
:  
ASA Version 8.3(1)  
!
```

```

hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.165.200.225 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa831-k8.bin

ftp mode passive

!--- Output Suppressed !--- Creates an object called
OBJ_GENERIC_ALL. !--- Any host IP not already matching
another configured !--- object will get 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

!--- Output Suppressed !--- Define a default route to
the ISP router. route outside 0.0.0.0 0.0.0.0
10.165.200.226 1

!--- Define a route to the INTERNAL router with network
10.2.1.0. route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network
10.3.1.0. route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end

```

注：有关在ASA 8.3上配置NAT和PAT的详细信息，请参阅[有关NAT的信息](#)。

有关如何在PIX/ASA上配置访问列表的详细信息，请参阅[PIX/ASA 7.x：使用 nat、global、static 和 access-list 命令进行端口重定向（转发）](#)。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

注：有关如何排除PIX/ASA故障的详细信息，请参阅[排除通过PIX和ASA的连接故障](#)。

[故障排除命令](#)

[命令输出解释程序 \(仅限注册用户 \) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

注意： [在使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。](#)

- **debug icmp trace** — 显示来自主机的 ICMP 请求是否到达 PIX。需要添加 **access-list** 命令，在您的配置中允许 ICMP，以便运行此 debug 命令。
- **logging buffer debugging** - Show connections being being and denied to hosts the the PIX.? 信息存储在 PIX 日志缓冲器中，使用 **show log** 命令可查看输出。

有关如何设置日志记录的详细信息，请参阅 [设置 PIX Syslog。](#)

[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](#)