ASA版本9.(x)使用Internet连接三个内部网络的配置示例

目录

简介

本文档提供有关如何设置思科自适应安全设备(ASA)版本9.1(5)以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。

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思科自适应安全设备(ASA)版本9.1(5)。

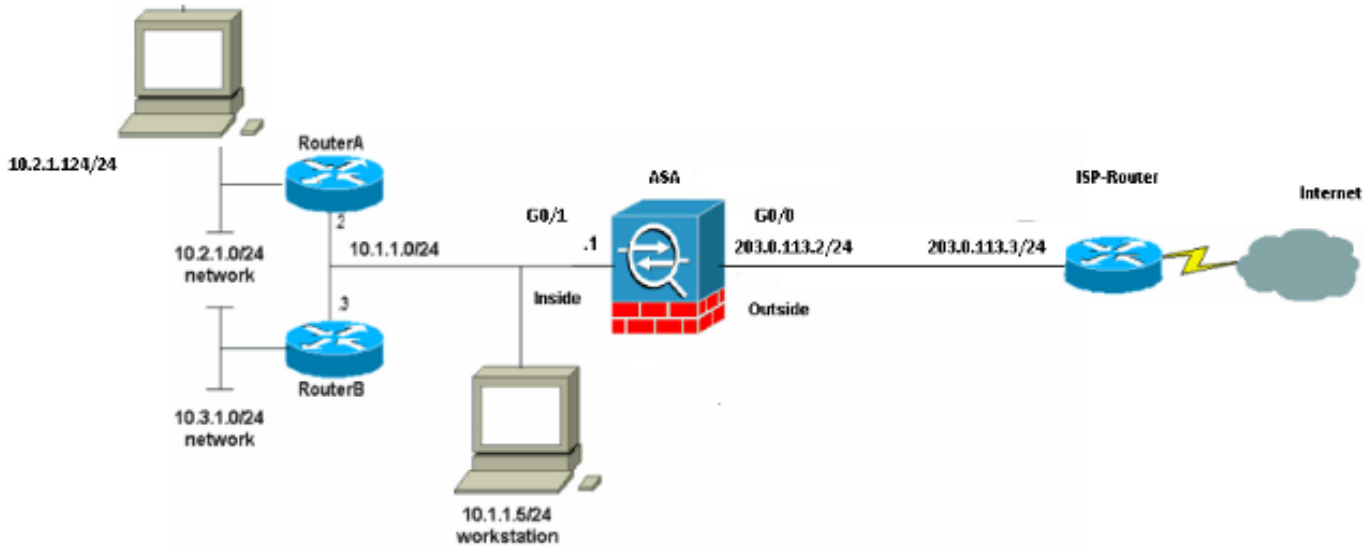
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

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：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



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 9.1 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。

配置

- 路由器 A 配置
- 路由器 B 配置
- ASA 9.1及更高版本配置

路由器 A 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#
```

路由器 B 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 9.1及更高版本配置

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive
```

```
!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- 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 0.0.0.0 203.0.113.3 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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

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

连接

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
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。***与预先存在的连接匹配的流量允许通过防火墙，且不被接口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。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 | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

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:10.2.1.124/18711 (203.0.113.2/18711)
```

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

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 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:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 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。要确认已创建这些转换，可以检查NAT转换(xlate)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203.0.113.2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

本部分提供的信息可用于对配置进行故障排除。

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 10.2.1.124 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，可以确定您认为应该允许通过防火墙的流量示例，并使用该5-tupple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 10.2.1.124。
- 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 10.2.1.124 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       10.2.1.124.18711 > 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 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 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 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 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。

对于捕获捕获功能，指示您要匹配内部接口（入口或出口）上发现的与**tcp主机10.2.1.124主机198.51.100.100匹配的流量**。换句话说，您要捕获从**host 10.2发送的任何TCP流量。1.124**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，我们应尝试再次建立连接，然后使用 show capture<capture_name> 命令查看捕获结果。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。