ASA三个内部网络的版本9.(x)连接与互联网配置示例的

目录

简介

本文提供信息关于怎样设置Cisco可适应安全工具(ASA)版本9.1(5)为了用在三个内部网络上。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

本文档中的信息根据Cisco可适应安全工具(ASA)版本9.1(5)。

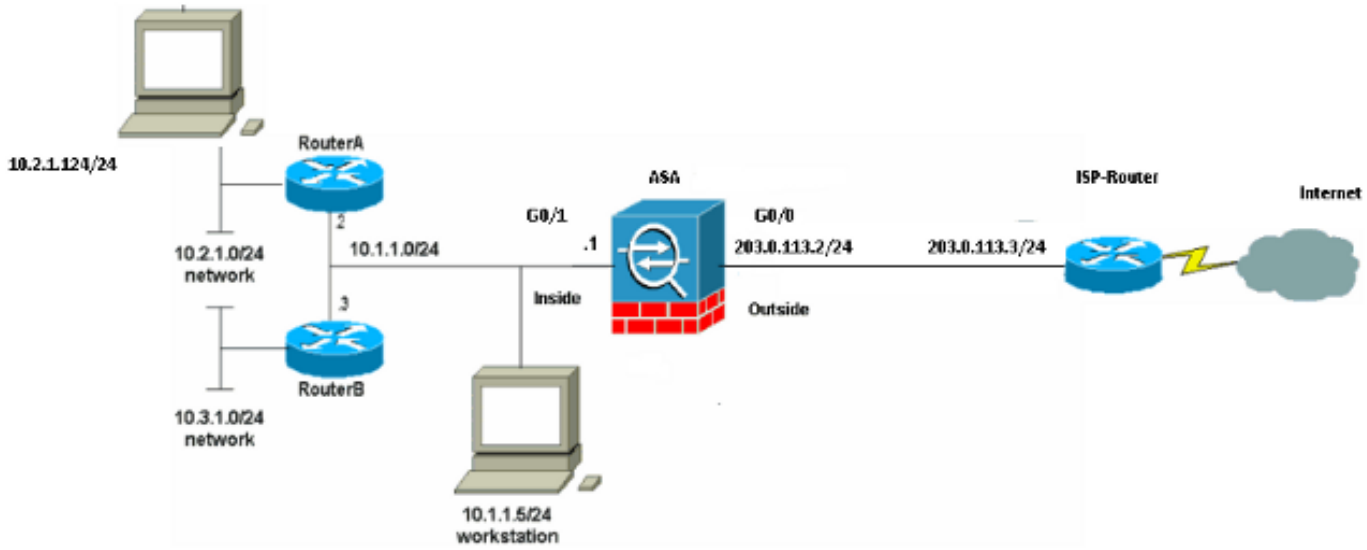
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

本部分提供有关如何配置本文档所述功能的信息。

Note: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



Note: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版本9.1和新配置

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版本9.1和新配置

```
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。请使用Output Interpreter Tool为了查看show命令输出分析。

设法通过与浏览器的HTTP访问网站。此示例使用主机在198.51.100.100的一个站点。如果连接是成功的，此输出在ASA CLI能被看到。

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是状态防火墙，并且从Web服务器的回程数据流允许上一步通过防火墙，因为在防火墙连接表里匹配一***连接***。匹配连接事先存在的流量通过防火墙允许和没有由接口ACL阻塞。

在上一个输出中，内部接口的客户端建立了对198.51.100.100主机的连接外部接口。此联系用TCP协议建立和是空闲在六秒。连接标志指示此连接的当前状态。关于连接标志的更多信息可以在ASA TCP连接标志找到。

Syslog

```
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)
```

ASA防火墙在正常操作时生成Syslog。Syslog在根据操作日志配置的冗余排列。输出显示被看到在级别六的两Syslog，或者'信息性'级别。

在本例中，有生成的两Syslog。第一是表明的日志消息防火墙建立了转换，特别地一个动态TCP转换(PAT)。当流量从里面横断到外部接口，它指示源IP地址和端口和转换后的IP地址和端口。

第二Syslog表明防火墙在其此特定的流量的连接表里建立了连接在客户端和服务器之间。如果防火墙配置为了阻塞此连接尝试，或者某个其他要素禁止了此连接(资源约束或一可能的误配置)的创建，防火墙不会生成表明的日志连接被建立了。反而它将记录连接的一个原因能拒绝或关于什么要素的一个征兆从创建禁止了连接。

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
```

作为此配置一部分， PAT配置为了翻译内部主机IP地址到是可路由的在互联网的地址。为了确认这些转换创建，您能检查NAT转换(xlate)表。show xlate命令，当与**本地关键字**和内部主机的IP地址结合，显示所有条目现在转换表里为该主机。上一个输出显示有为在内部和外部接口之间的此主机当前建立的转换。内部主机IP和端口翻译对203.0.113.2地址每我们的配置。标志列出了， r我，表明转换是**动态**和**portmap**。关于不同的NAT配置的更多信息可以在关于NAT的信息找到。

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提供排除故障连接的多个工具。如果问题仍然存在，在您验证配置并且检查以前后列出的输出，这些工具和技术也许帮助确定您的连通性故障的原因。

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
```

在ASA的数据包跟踪程序功能允许您指定一被模拟的数据包和发现所有多种步骤，检查，并且作用防火墙审阅，当处理流量时。使用此工具，识别您相信应该允许穿过防火墙流量的示例是有用的，并且使用5-tupple为了模拟流量。在前一个示例中，数据包跟踪程序用于为了模拟满足这些标准的连接尝试：

- 被模拟的数据包在**里面**到达。
- 使用的协议是**TCP**。
- 被模拟的客户端IP地址是**10.2.1.124**。
- 客户端发送从端口发出的流量**1234**。
- 流量被注定到在IP地址**198.51.100.100的**一个服务器。
- 流量被注定到端口**80**。

注意没有接口的提及**从外部**在命令。这是由数据包跟踪程序设计。工具如何告诉您防火墙处理那种连接尝试，包括如何将路由它，并且在哪个接口外面。关于数据包跟踪程序的更多信息可以在有数据包跟踪程序。的跟踪数据包找到

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防火墙能捕获进入或离开其接口的流量。此捕获功能是意想不到的，因为能明确证明流量是否到达在，或者分支从，防火墙。前一个示例显示名为**capin**和**capout的**两个捕获的配置在各自内部和外部接口。捕获命令使用了**匹配**关键字，允许您是特定关于什么流量您要捕获。

对于捕获**capin，**指示您在该的内部接口要匹配流量被看到(入口或出口)匹配**TCP主机10.2.1.124主机198.51.100.100**。换句话说，从**主机10.2.1.124**发送**主机198.51.100.100**或**反之亦然的**您要捕获所有TCP数据流。使用**匹配**关键字允许防火墙捕获该流量双向。因为防火墙执行在该客户端IP地址

的PAT capture命令定义外部接口的不参考内部客户端IP地址。结果，您不能**配比**与该客户端IP地址。反而，此示例使用其中**任一**为了表明所有可能的IP地址将匹配该情况。

在您配置捕获后，您然后会尝试再建立连接，并且继续查看捕获用**显示捕获** *<capture_name>*命令。在本例中，您能看到客户端能连接到服务器如明显由在捕获看到的TCP三通的握手。