配置双重内部网络的ASA

目录

简介

本文描述如何配置Cisco可适应安全工具(ASA)该运行软件版本9.x为使用两个内部网络。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

运行软件版本9.x的本文档中的信息根据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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

当您添加在ASA防火墙后时的第二个内部网络，请考虑此重要信息：

- ASA 不支持附属寻址。
- 必须在ASA后用于路由器为了达到在当前网络和新加的网络之间的路由。
- 所有的默认网关主机必须指向内部路由器。
- 您必须添加在内部路由器的一个默认路由对ASA的该点。
- 您必须清除内部路由器的地址解析服务(ARP)缓存。

配置

请使用在此部分描述为了配置ASA的信息。

网络图

这是使用示例在本文中的拓扑：

> **Note**:在此配置方面使用的IP寻址机制不是合法可路由的在互联网。他们是在实验室环境使用的RFC 1918地址。

ASA 9.x配置

如果有输出**write terminal命令**从您的Cisco设备，您能使用Output Interpreter Tool (仅限注册用户)为了显示潜在问题和修正。

这是运行软件版本9.x 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
```

允许内部主机对外部网络的访问与PAT

如果打算让内部主机共享转换的单个公共地址，使用端口地址转换(PAT)。其中一最简单的PAT配置介入所有内部主机的转换，以便他们看来是外部接口IP。这是使用的典型PAT配置，当从ISP时是可得到可路由IP地址的数量对仅一些被限制，或者一个。

完成这些步骤为了允许内部主机对外部网络的访问与PAT ：

1. 导航对**Configuration>防火墙> NAT规则**，单击**添加**，并且选择**网络对象**为了配置一个动态NAT规则：

2. 配置网络/host/动态PAT要求的范围。在本例中，所有里面子网选择。应该为特定子网重复此进程您希望如此翻译：

3. 点击**NAT**，检查**添加自动地址转换规则**复选框，输入**动态，**并且设置**翻译的地址**选项，以便反射外部接口。如果点击省略号按钮，协助解决您选择一个预先配置的对象，例如外部接口：

4. 单击**先进**为了选择源和目的接口：

5. 点击OK键，然后单击**应用**为了应用更改。一旦完整，可适应安全设备管理器(ASDM)显示NAT规则：

路由器 B 配置

这是路由器的B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HTTP访问网站通过Web浏览器为了验证您的配置适当地工作。

此示例使用主机在IP地址198.51.100.100的一个站点。如果连接是成功的，在部分提供跟随的输出

在ASA CLI能被看到。

连接

输入**address命令的显示连接**为了验证连接：

```
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，不用阻塞由接口访问控制表(ACL)。

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。

> **Note**:参考ASA TCP连接标志(连接积累和卸载) Cisco文档关于连接标志的更多信息。

故障排除

请使用在此部分描述为了排除故障配置问题的信息。

系统日志

输入**show log命令**为了查看Syslog ：

```
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)
```

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*与信息有关的级别*。

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)。因为流量从里面横断到外部接口，它指示源IP地址和端口、以及转换后的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，防火墙不生成日志表明连接被建立了。反而，它记录连接的一个原因能拒绝或征兆关于从创建禁止连接的要素。

数据包跟踪程序

输入此命令为了启用数据包跟踪程序功能：

```
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
```

在ASA的数据包跟踪程序功能允许您指定一*被模拟的*数据包和查看所有多种步骤，检查，并且作用防火墙完成，当处理流量。使用此工具，识别您相信*应该*允许穿过防火墙，并且使用5-tupple为了模拟流量流量的示例是有用的。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：

- 被模拟的数据包在内部接口到达。
- 使用的协议是TCP。
- 被模拟的客户端IP地址是192.168.1.5。
- 客户端发送从端口1234被发出的流量。
- 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。

注意没有外部接口的提及在命令的。这归结于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。

> **提示**：*使用CLI，8.4和8.6*，关于数据包跟踪程序功能的更多信息，参考有数据包*Cisco ASA 5500系列配置指南的*跟踪程序部分的跟踪数据包。

捕获

输入这些命令为了应用捕获：

```
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**两个捕获的配置在内部和外部接口，分别。**捕获**命令使用**匹配**关键字，允许您指定流量您要捕获。

对于*capin*捕获示例，指示您要匹配在内部接口被看到的流量(入口或出口)该匹配*TCP主机192.168.1.5主机198.51.100.100*。换句话说，从主机*192.168.1.5*发送主机*198.51.100.100的*您要捕获所有TCP数据流，或者反之亦然。使用**匹配**关键字允许防火墙捕获该流量双向。**capture命令**为外部接口定义不参考内部客户端IP地址，因为防火墙执行在该客户端IP地址的PAT。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，您能然后尝试再建立连接，并且继续查看与**显示捕获*<capture_name>的***捕获请发出命令。在本例中，您能看到客户端能连接到服务器，如明显由在捕获被看到的TCP三通的握手。

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
- RFC (RFC)
- 思科ASA系列CLI配置指南， 9.0 âÂ Â 配置静态和默认路由
- 技术支持&文档âÂ Â Cisco系统