ASA 8.3 (x)与两个内部网络以及互联网动态PAT的配置示例

目录

简介

本文档提供在运行软件版本 8.3(1) 的 Cisco 自适应安全设备上 (ASA) 进行动态 PAT 配置的示例。通过将实际源地址和源端口转换为映射地址和唯一映射端口，动态 PAT 可将多个实际地址转换为单一映射地址。每个连接都需要独立的转换会话，因为每个连接都有不同的源端口。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 确保内部网络中具备两个位于 ASA 内部的网络：192.168.0.0/24 — 直接连接至 ASA 的网络。192.168.1.0/24 — 位于 ASA 内部，但在另一个设备之后（例如，路由器）的网络。
- 确保内部用户按以下方式进行 PAT：192.168.1.0/24 子网上的主机进行 PAT，获得由 ISP 提供的备用 IP 地址 (10.1.5.5)。其他位于 ASA 内部之后的主机进行 PAT，获得 ASA 外部接口的 IP 地址 (10.1.5.1)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 自适应安全设备 (ASA) 版本 8.3(1)
- ASDM 版本 6.3(1)

注意： 要使 ASDM 可配置 ASA，请参阅允许 ASDM 进行 HTTPS 访问。

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

关于文件规则的信息，请参见Cisco技术提示规则。

配置

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 CLI 配置
- ASDM 配置

ASA CLI 配置

本文档使用如下所示的配置。

ASA 动态 PAT 配置

```
ASA#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.

!--- 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 10.1.5.1), for internet bound traffic.
ASA(config)#object network OBJ_GENERIC_ALL
ASA(config-obj)#subnet 0.0.0.0 0.0.0.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_GENERIC_ALL interface

!--- The above statements are the equivalent of the !---
nat/global combination (as shown below) in v7.0(x), !---
v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code:
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 interface


!--- Creates an object called OBJ_SPECIFIC_192-168-1-0.
!--- Any host IP facing the the 'inside' interface of
the ASA !--- with an address in the 192.168.1.0/24
subnet will get PAT !--- to the 10.1.5.5 address, for
```

```
internet bound traffic. ASA(config)#object network
OBJ_SPECIFIC_192-168-1-0
ASA(config-obj)#subnet 192.168.1.0 255.255.255.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_SPECIFIC_192-168-1-0 10.1.5.5

!--- The above statements are the equivalent of the
nat/global !--- combination (as shown below) in v7.0(x),
v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA
code: nat (inside) 2 192.168.1.0 255.255.255.0
global (outside) 2 10.1.5.5
```

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
!
!--- Configure the outside interface. ! interface
GigabitEthernet0/0 nameif outside security-level 0 ip
address 10.1.5.1 255.255.255.0 !--- Configure the inside
interface. ! interface GigabitEthernet0/1 nameif inside
security-level 100 ip address 192.168.0.1 255.255.255.0
! 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:/asa831-k8.bin ftp mode passive object
network OBJ_SPECIFIC_192-168-1-0
 subnet 192.168.1.0 255.255.255.0
object network OBJ_GENERIC_ALL
 subnet 0.0.0.0 0.0.0.0

pager lines 24
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source dynamic OBJ_GENERIC_ALL
interface
nat (inside,outside) source dynamic OBJ_SPECIFIC_192-
168-1-0 10.1.5.5

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 10.1.5.2
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
```

ASDM 配置

要通过 ASDM 接口完成此配置，必须：

1. 添加三个网络对象；本示例添加了以下网络对象：OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. 创建两个 NAT/PAT 规则；本示例为以下网络对象创建了 NAT 规则：OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

添加网络对象

完成以下步骤以添加网络对象：

1. 登录 ASDM，选择 **Configuration > Firewall > Objects > Network Objects/Groups**。
2. 选择 **Add > Network Object** 添加网络对象。此时将出现 Add Network Object 对话框。
3. 在 Add Network Object 对话框中输入以下信息：网络对象的名称。（本示例使用 *OBJ_GENERIC_ALL*。）网络对象的类型。（本示例使用 *Network*。）网络对象的 IP 地址。（本示例使用 *0.0.0.0*。）网络对象的网络掩码。（本示例使用 *0.0.0.0*。）
4. 单击 **Ok**。这样就创建了网络对象，并显示在 Network Objects/Groups 列表中，如下图所示：
5. 重复以上步骤添加第二个网络对象，然后单击 **OK**。本示例使用这些值：名称：*OBJ_SPECIFIC_192-168-1-0*类型：网络IP 地址：*192.168.1.0*网络屏蔽：*255.255.255.0*这样就创建了第二个网络对象，并显示在 Network Objects/Groups 列表中，如下图所示：
6. 重复以上步骤添加第三个网络对象，然后单击 **OK**。本示例使用这些值：名称：*10.1.5.5*类型：*主机*IP 地址：*10.1.5.5*这样就创建了第三个网络对象，并显示在 Network Objects/Groups 列表中。Network Objects/Groups 列表当前应包括要参考的 NAT 规则的三个所需对象。

创建 NAT/PAT 规则

完成以下步骤以创建新的 NAT/PAT 规则：

1. 创建第一个 NAT/PAT 规则：在 ASDM 中，选择 **Configuration > Firewall > NAT Rules**，并单击 **Add**。此时将出现 Add NAT Rule 对话框。在 Add NAT Rule 对话框的 Match Criteria:Original Packet 区域中，在 Source Interface 下拉列表中选择 **inside**。单击位于 Source Address 文本字段右侧的浏览 (...) 按钮。此时将出现 Browse Original Source Address 对话框。在 Browse Original Source Address 对话框中，选择创建的第一个网络对象。（本示例中，选择 **OBJ_GENERIC_ALL**。）单击 **Original Source Address**，然后单击 **OK**。*OBJ_GENERIC_ALL* 网络对象将显示在 Add NAT Rule 对话框的 Match Criteria:Original Packet 区域的 Source Address 字段中。在 Add NAT Rule 对话框的 Action:Translated Packet 区域中，在 Source NAT Type 对话框中选择 **Dynamic PAT (Hide)**。单击位于 Source Address 文本字段右侧的浏览 (...) 按钮。此时将出现 Browse Translated Source Address 对话框。在 Browse Translated Source Address 对话框中，选择 **outside** 接口对象。（此接口已经创建，属于原始配置的一部分。）单击 **Translated Source Address**，然后单击 **OK**。此时外部接口将显示在 Add NAT Rule 对话框的 Action:Translated Packet 区域的 Source Address 字段中。**注意：** *Destination Interface* 字段也变为外部接口。确认完成的第一个 PAT 规则显示如下：在 Add NAT Rule 对话框的 Match Criteria:Original Packet 区域中，确认以下值：Source Interface = insideSource Address = OBJ_GENERIC_ALLDestination Address = anyService = any在 Add NAT Rule 对话框的 Action:Translated Packet 区域中，确认以下值：Source NAT Type = Dynamic PAT (Hide)Source Address = outsideDestination Address = OriginalService = Original单击 **Ok**。第一个 NAT 规则显示在 ASDM 中，如下图所示：
2. 创建第二个 NAT/PAT 规则：在 ASDM 中，选择 **Configuration > Firewall > NAT Rules**，并单击 **Add**。在 Add NAT Rule 对话框的 Match Criteria:Original Packet 区域中，在 Source Interface 下拉列表中选择 **inside**。点击浏览(...)按钮。此时将出现 Browse Original Source Address 对话框。在 Browse Original Source Address 对话框中，选择创建的第二个对象。（本示例中，选择 **OBJ_SPECIFIC_192-168-1-0**。）单击 **Original Source Address**，然后单击 **OK**。*OBJ_SPECIFIC_192-168-1-0* 网络对象将显示在 Add NAT Rule 对话框的 Match Criteria:Original Packet 区域的 Source Address 字段中。在 Add NAT Rule 对话框的 Action:Translated Packet 区域中，在 Source NAT Type 对话框中选择 **Dynamic PAT (Hide)**。单击位于 Source Address 字段右侧的 **...** 按钮。此时将出现 Browse Translated Source Address 对话框。在 Browse Translated Source Address 对话框中，选择 **10.1.5.5** 对象。（此接口已经创建，属于原始配置的一部分。）单击 **Translated Source Address**，然后

单击 **OK**。**10.1.5.5** 网络对象将显示在 Add NAT Rule 对话框的 Action:Translated Packet 区域的 Source Address 字段中。在 Add NAT Rule 对话框的 Match Criteria:Original Packet 区域中，在 Destination Interface 下拉列表中选择 **outside**。**注意：** 如果此选项未选择 *outside*，则目标接口将参考 *Any*。确认完成的第二个 NAT/PAT 规则显示如下：在 Add NAT Rule 对话框的 Match Criteria:Original Packet 区域中，确认以下值：Source Interface = insideSource Address = OBJ_SPECIFIC_192-168-1-0Destination Address = outsideService = any在 Add NAT Rule 对话框的 Action:Translated Packet 区域中，确认以下值：Source NAT Type = Dynamic PAT (Hide)Source Address = 10.1.5.5Destination Address = OriginalService = Original单击 **Ok**。完成的 NAT 配置将显示在 ASDM 中，如下图所示：

3. 单击 **Apply** 按钮更改运行的配置。

这样就完成了在 Cisco 自适应安全设备 (ASA) 上配置动态 PAT。

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（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。

验证通用 PAT 规则

- show local-host — 显示本地主机的网络状态。

```
ASA#show local-host

   Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
 !--- The TCP connection outside address corresponds !--- to the actual destination of
125.255.196.170:80 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051,
          idle 0:00:03, bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
          bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

 !--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA –
10.1.5.1. Xlate: TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
          ri idle 0:00:17 timeout 0:00:30
    TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
          ri idle 0:00:17 timeout 0:00:30

  Conn:
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03,
          bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
          bytes 11896, flags UIO
```

- show conn — 显示指定连接类型的连接状态。

```
ASA#show conn
```

```
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06,
          bytes 13758, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01,
          bytes 13526, flags UIO
```

- show xlate — 显示有关转换插槽的信息。

```
ASA#show xlate
4 in use, 7 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
          T - twice
TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
          ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
          ri idle 0:00:23 timeout 0:00:30
```

验证特定 PAT 规则

- show local-host — 显示本地主机的网络状态。

```
ASA#show local-host
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
 !--- The TCP connection outside address corresponds to !--- the actual destination of
125.255.196.170:80. Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067,
          idle 0:00:07, bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1066,
          idle 0:00:03, bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited


 !--- The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5.
Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
          ri idle 0:00:17 timeout 0:00:30
    TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags
          ri idle 0:00:17 timeout 0:00:30

  Conn:
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
          bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
          bytes 11896, flags UIO
```

- show conn — 显示指定连接类型的连接状态。

```
ASA#show conn
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
          bytes 13653, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
          bytes 13349, flags UIO
```

- show xlate — 显示有关转换插槽的信息。

```
ASA#show xlate
3 in use, 9 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
          T - twice
```

```
TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
          ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags
          ri idle 0:00:23 timeout 0:00:30
```

故障排除

目前没有针对此配置的故障排除信息。

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