NAT 支持使用路由映射的 多个池

目录

简介

本文解释如何使用访问列表(而不是路由映射)，更改网络地址转换(NAT)功能。 关于 NAT 的更多信息，请参阅 Cisco IOS NAT。

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以下软件和硬件版本：

- Cisco 2500 系列路由器。
- Cisco IOS® 软件版本 12.3(3)。

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

需要创建转换条目时，NAT **仅使用访问列表和路由映射。**如果与数据流匹配的转换条目已经存在，则使用该转换条目。**不会查询任何访问列表或路由映射。**使用访问列表或路由映射之间的区别在于：创建的转换条目的类型不同。

路由映射

当 NAT 使用路由映射来决定创建转换条目时，它通常会创建“完全扩展的”的转换条目。此转换项将包含两个里面和超出（本地和全局）地址条目和所有 TCP 或 UDP 端口信息。请参阅 NAT：本地和全局定义以获得有关内部和外部（本地和全局）地址的更多信息。

访问列表（无过载）

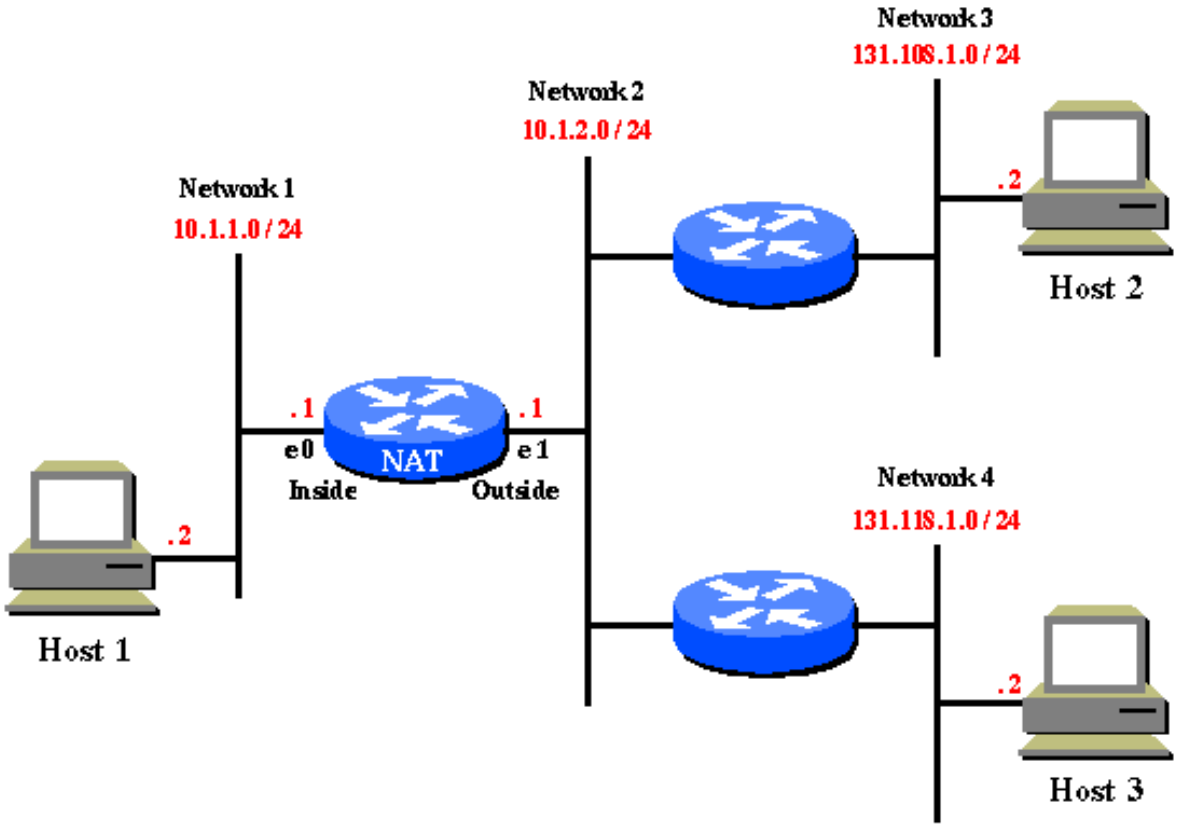
当 NAT 使用访问控制列表来决定创建转换条目时，它会创建“简单的”转换条目。这条“简单”条目将只包含内部和外部的本地和全局的IP地址条目，取决于是否配置了 **ip nat inside 或 ip nat outside 命令。**而且，它不会包括任何 TCP 或 UDP 端口信息。

访问列表（有过载）

当 NAT 使用访问控制列表，并指定超载时，NAT 将创建“完全扩展的”转换条目。(参见附注1)。 该操作类似于路由映射，只不过路由影射具有一些其它功能。有关更多详细信息，请参阅注意 2。通过选择以下链接之一，可以查看简单 NAT 转换条目和完全扩展 NAT 转换条目的示例：

- 简单 NAT 转换条目
- 完全扩展 NAT 转换条目

下面是一个网络图示例，用于说明对 NAT 使用路由映射和使用访问列表之间的区别：



在此网络图示例中，10.1.1.0 上的主机必须转换为：

- 131.108.2.0（去往 131.108.1.0 时）
- 131.118.2.0（去往 131.118.1.0 时）

访问列表方法

使用访问控制列表方法，您可以执行以下操作，转换 10.1.1.0 上的主机：

```
ip nat pool pool108 131.108.2.1 131.108.2.254 prefix-length 24
!--- Defines a pool of global addresses to be allocated as needed. ip nat pool pool118
131.118.2.1 131.118.2.254 prefix-length 24 ip nat inside source list 108 pool pool108 !---
Establishes dynamic source translation, specifying the !--- access list defined below. ip nat
inside source list 118 pool pool118 interface ethernet0 ip address 10.1.1.1 255.255.255.0 ip nat
inside !--- Marks the interface as connected to the inside. interface ethernet1 ip address
10.1.2.1 255.255.255.0 ip nat outside !--- Marks the interface as connected to the outside.
access-list 108 permit ip 10.1.1.0 0.0.0.255 131.108.1.0 0.0.0.255 !--- Defines the access-list
mentioning those addresses !--- that are to be translated. access-list 118 permit ip 10.1.1.0
0.0.0.255 131.118.1.0 0.0.0.255
```

有关这些命令的更多信息，请参阅 IP 编址和服务命令。

主机 1 到主机 2

下面是主机 1 远程登录到主机 2 时发生的情况。

```
Packet on (Network 1) s:10.1.1.2(1024)     d:131.108.1.2(23)
     Packet on (Network 2) s:131.108.2.1(1024)  d:131.108.1.2(23)   (after NAT)
```

NAT 利用访问控制列表与数据流匹配，此时创建简单的转换条目，包括内部转换信息，没有协议或端口信息：

```
inside                          outside
         local        global          global         local
        10.1.1.2     131.108.2.1       ----           ----
```

返回数据包：主机 2 到主机 1：

```
Packet on (Network 2)  s:131.108.1.2(23)  d:131.108.2.1(1024)
     Packet on (Network 1)  s:131.108.1.2(23)  d:10.1.1.2(1024)      (after NAT)
```

主机 1 到主机 3

如果上面的简单转换已经完成，接下来是主机 1 也远程登录主机 3 时会发生的情况。

```
Packet on (Network 1)  s:10.1.1.2(1025)     d:131.118.1.2(23)
     Packet on (Network 2)  s:131.108.2.1(1025)  d:131.118.1.2(23)   (after NAT)
```

可以看到存在问题。从10.1.1.0主机到131.118.1.0主机的数据包应转换为131.118.2.0，而不是131.108.2.0。发生这种情况的原因是，10.1.1.1已经有一个NAT转换条目2 <—> 131.108.2.1，它也与主机1和主机3之间的流量匹配。因此，将使用此转换条目，并且不检查访问列表108和118。

当 NAT 转换表中的简单转换条目就位时，可以由**任何外部用户在任何外部主机上使用该条目以便将数据包发送到主机 1，前提是该外部用户使用主机 1 的内部全局地址 (131.108.2.1)。通常需要使用静态 NAT 转换才能实现上述操作。**

路由映射方法

本文档中示例的正确配置方式是使用路由映射。使用路由映射方法，您需要执行以下操作，在 10.1.1.0 上转换主机：

```
ip nat pool pool-108 131.108.2.1 131.108.2.254 prefix-length 24
     ip nat pool pool-118 131.118.2.1 131.118.2.254 prefix-length 24

     ip nat inside source route-map MAP-108 pool pool-108
     !--- Establishes dynamic source translation, specifying !--- the route-map MAP-108 which is
defined below. ip nat inside source route-map MAP-118 pool pool-118 !--- Establishes dynamic
source translation, specifying the route-map MAP-118. !--- Here, the route-maps are consulted
instead of !--- access-lists (as in the previous case). interface ethernet0 ip address 10.1.1.1
255.255.255.0 ip nat inside interface ethernet1 ip address 10.1.2.1 255.255.255.0 ip nat outside
access-list 108 permit ip 10.1.1.0 0.0.0.255 131.108.1.0 0.0.0.255 access-list 118 permit ip
10.1.1.0 0.0.0.255 131.118.1.0 0.0.0.255 route-map MAP-108 permit 10 !--- Defines the Route-map
MAP-108. match ip address 108 !--- Specifies the criteria for translation. Here, the IP !---
address mentioned in the access-list 108 is translated. !--- The translation is defined in the
!--- ip nat inside source route-map MAP-108 pool pool-108 command.



     route-map MAP-118 permit 10
     !--- Defines the Route-map MAP-108. match ip address 118 !--- The IP address mentioned in
the access-list 118 is translated. !--- The translation is defined in the !--- ip nat inside
source route-map MAP-118 pool pool-118 command.
```

有关这些命令的更多信息，请参阅 IP 编址和服务命令。

主机 1 到主机 2

下面是主机 1 远程登录到主机 2 时发生的情况：

```
Packet on (Network 1) s:10.1.1.2(1024)     d:131.108.1.2(23)
     Packet on (Network 2) s:131.108.2.1(1024)  d:131.108.1.2(23)   (after NAT)
```

在这种情况下，因为 NAT 使用路由映射匹配将要转换的数据流，所以 NAT 会创建一个完全扩展的转换条目，包括内部和外部转换信息：

```
 inside                                outside
         local            global             global             local
     10.1.1.2:1024    131.108.2.1:1024   131.108.1.2:23     131.108.1.2:23
```

返回数据包：主机 2 到主机 1：

```
Packet on (Network 2) s:131.108.1.2(23)  d:131.108.2.1(1024)
     Packet on (Network 1) s:131.108.1.2(23)  d:10.1.1.2(1024)      (after NAT)
```

主机 1 到主机 3

现在，当主机 1 将数据包发送到主机 3 时，将发生以下情况：

```
Packet on (Network 1) s:10.1.1.2(1025)     d:131.118.1.2(23)
     Packet on (Network 2) s:131.118.2.1(1025)  d:131.118.1.2(23)   (after NAT)
```

转换正确完成，因为 (N1) 上的数据包与用于主机 1 到主机 2 的流量的完全扩展转换条目不匹配。由于现有转换不匹配，因此 NAT 为主机 1 到主机 3 的流量创建另一个转换条目。

下面是 NAT 路由器上的完全扩展转换条目：

```
inside                                outside
         local            global             global             local
     10.1.1.2:1024    131.108.2.1:1024   131.108.1.2:23     131.108.1.2:23
     10.1.1.2:1025    131.118.2.1:1025   131.118.1.2:23     131.118.1.2:23
```

由于 NAT 转换表有两个完整的条目，因而它将正确转换来自同一来源、通向两个不同目的地的数据流。

与通过访问列表创建的简单转换条目不同，通过路由映射创建的完全扩展转换条目不能被任何其他外部用户用于向主机1发送数据包。要允许此操作，需要静态NAT转换。

注意 1

在超载的访问列表的情况下，配置类似于没有超载的访问列表。例外的是，您必须将关键字超载添加到ip nat inside source list 108 pool pool108和ip nat inside source list 118 pool pool118命令。

注意 2

使用 route-map 的优点是，在 **match 命令下，您能够有更多选项，而不只是源 IP 地址。**例如，在 route-map 中，可以指定 **match interface 或 match ip next-hop。**利用路由映射，您可以指定 IP 地址以及接口或数据包将转发的下一跳地址。所以，NAT 的 route-map 应用于用户多归属到不同 ISP 的情况下。

相关信息

- NAT — 可使用路由映射进行静态转换
- Cisco IOS 网络地址转换
- 配置网络地址转换
- NAT:本地和全局定义
- 编址和服务的 Cisco IOS IP 命令参考（版本 12.3）
- 技术支持和文档 - Cisco Systems