配置私有网络到私有网络的 IPSec 路由器隧道，以实现 NAT 和静态

目录

简介

此示例配置向您说明如何：

- 加密两个专用网络（10.1.1.x 和 172.16.1.x）之间的流量。
- 将静态 IP 地址（外部地址 200.1.1.25）分配给位于 10.1.1.3 的网络设备。

可以使用访问控制列表 (ACL) 指示路由器不对专用网络到专用网络的流量执行网络地址转换 (NAT)，在该流量离开路由器时随后会对其进行加密并置于隧道上。在此示例配置中，10.1.1.x 网络上的内部服务器还有一个静态 NAT。此示例配置使用 NAT 命令的 route-map 选项，从而在通过加密隧道发送 NAT 流量时阻止其成为 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 IOS® 软件版本 12.3(14)T
- 两个 Cisco 路由器

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。

为什么 ACL 中的 deny 语句指定 NAT 流量？

在使用 Cisco IOS IPsec 或 VPN 时，您可从概念上将网络替换为隧道。在此图中，您可将 Internet 网云替换为范围从 200.1.1.1 到 100.1.1.1 的 Cisco IOS IPsec 隧道。使此网络从通过隧道链接在一起的两个专用 LAN 的角度来看是透明的。因此，通常您不希望对一个从专用 LAN 进入远程专用 LAN 的流量使用 NAT。在数据包到达内部路由器 3 网络时，您希望看到来自路由器 2 网络的数据包，这些数据包具有来自 10.1.1.0/24 网络（而不是 200.1.1.1）的源 IP 地址。

有关如何配置 NAT 的详细信息，请参阅 NAT 运行顺序。本文档说明数据包从内部进入外部时在加密检查之前会进行 NAT。这就是您必须在配置中指定此信息的原因。

<#root>

```
ip nat inside source list 122 interface Ethernet0/1 overload
```

<#root>

```
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

注意：也可以构建隧道并仍然使用NAT。在此情况下，您可以将 NAT 流量指定为“用于 IPsec 的相关流量”（在本文档的其他部分中称为 ACL 101）。有关在 NAT 处于活动状态时如何建立隧道的详细信息，请参阅在拥有重复 LAN 子网的路由器之间配置 IPSec 隧道。

静态 NAT 的情况如何，为什么我不能通过 IPsec 隧道到达该地址？

对于位于 10.1.1.3 的服务器，此设置还包括静态一对一 NAT。此情况是 NAT'd 至 200.1.1.25，以便 Internet 用户可对其进行访问。发出以下命令：

<#root>

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

此静态 NAT 通过加密隧道阻止 172.16.1.x 网络上的用户到达 10.1.1.3。这是因为您需要通过 ACL 122 拒绝加密流量成为 NAT'd。不过，对于到达 10.1.1.3 以及从 10.1.1.3 发出的所有连接，静态 NAT 命令的优先级高于常规 NAT 语句。静态 NAT 语句不专门拒绝加密流量也成为 NAT'd。172.16.1.x 网络上的用户连接到 10.1.1.3 时，来自 10.1.1.3 的回复为 NAT'd 至 200.1.1.25，因此回复不会通过加密隧道返回（在加密前发生 NAT）。

您必须通过静态 NAT 语句的 route-map 命令拒绝加密流量成为 NAT'd（甚至静态一对一 NAT'd）。

注意：仅在Cisco IOS软件版本12.2(4)T及更高版本中支持静态NAT上的route-map选项。有关其他信息，请参阅 NAT — 能够将路由映射用于静态转换。

您必须发出以下附加命令，才能允许加密访问 10.1.1.3（静态 NAT'd 主机）：

<#root>

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

这些语句指示路由器仅将静态 NAT 应用于与 ACL 150 匹配的流量。ACL 150 表明不将 NAT 应用于源自 10.1.1.3 并通过加密隧道发往 172.16.1.x 的流量。但是，将 NAT 应用于源自 10.1.1.3 的所有其他流量（基于 Internet 的流量）。

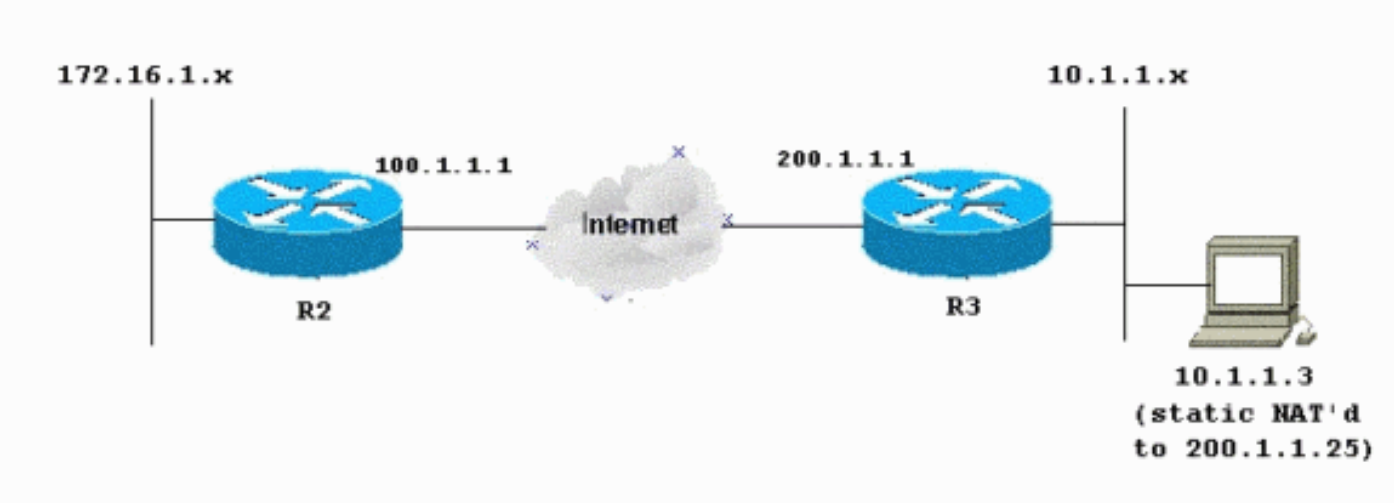
配置

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(仅限注册客户)查找有关本文档中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- 路由器 2
- 路由器 3

R2 - 路由器配置

```
<#root>

R2#

write terminal

Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!

hostname R2

!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
```

```
crypto isakmp policy 10
 authentication pre-share

!

crypto isakmp key ciscokey address 200.1.1.1

!
!

crypto ipsec transform-set myset esp-3des esp-md5-hmac


!

crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset


!--- Include the private-network-to-private-network traffic !--- in the encryption process:


match address 101

!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0


ip nat inside

 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0


ip nat outside

 ip virtual-reassembly


crypto map myvpn

!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!

!--- Except the private network from the NAT process:


ip nat inside source list 175 interface Ethernet1/0 overload

!

!--- Include the private-network-to-private-network traffic !--- in the encryption process:


access-list 101 permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
```

```
!--- Except the private network from the NAT process:

access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any

!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

R3 - 路由器配置

<#root>

```
R3#

write terminal

Building configuration...
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!

crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1

!
!
```

```
crypto ipsec transform-set myset esp-3des esp-md5-hmac

!

crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset


!--- Include the private-network-to-private-network traffic !--- in the encryption process:



match address 101

!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0


ip nat inside

 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0


ip nat outside

 ip virtual-reassembly


crypto map myvpn

!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!

!--- Except the private network from the NAT process:


ip nat inside source list 122 interface Ethernet1/0 overload


!--- Except the static-NAT traffic from the NAT process if destined !--- over the encrypted tunnel:


ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat

!

access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255


!--- Except the private network from the NAT process:


access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
access-list 122 permit ip 10.1.1.0 0.0.0.255 any


!--- Except the static-NAT traffic from the NAT process if destined !--- over the encrypted tunnel:


access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any

!

route-map nonat permit 10
 match ip address 150

!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

验证

当前没有可用于此配置的验证过程。

故障排除

使用本部分可排除配置故障。

有关其他信息，请参阅 IP 安全故障排除 - 了解和使用 debug 命令。

故障排除命令

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。

注意：使用debug命令之前，请参阅有关Debug命令的重要信息。

- debug crypto ipsec sa — 显示阶段 2 的 IPSec 协商。
- debug crypto isakmp sa — 查看阶段 1 的 ISAKMP 协商。
- debug crypto engine — 显示加密会话。

相关信息

- IPsec 协商/IKE 协议 - Cisco Systems
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。