在ASA上配置发夹

目录

简介

本文档介绍在思科自适应安全设备(ASA)上成功配置发夹的必要步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA上的NAT配置
- ASA上的ACL配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科自适应安全设备软件版本9.18(4)22

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

发夹式网络地址转换(NAT)也称为NAT环回或NAT反射，是网络路由中使用的技术，通过此技术，专用网络上的设备可以通过公有IP地址访问同一专用网络上的其他设备。

当服务器托管在路由器后面，并且您希望与服务器位于同一本地网络中的设备能够像外部设备一样使用公有IP地址（Internet服务提供商分配给路由器的地址）访问该服务器时，就会使用这种方法。

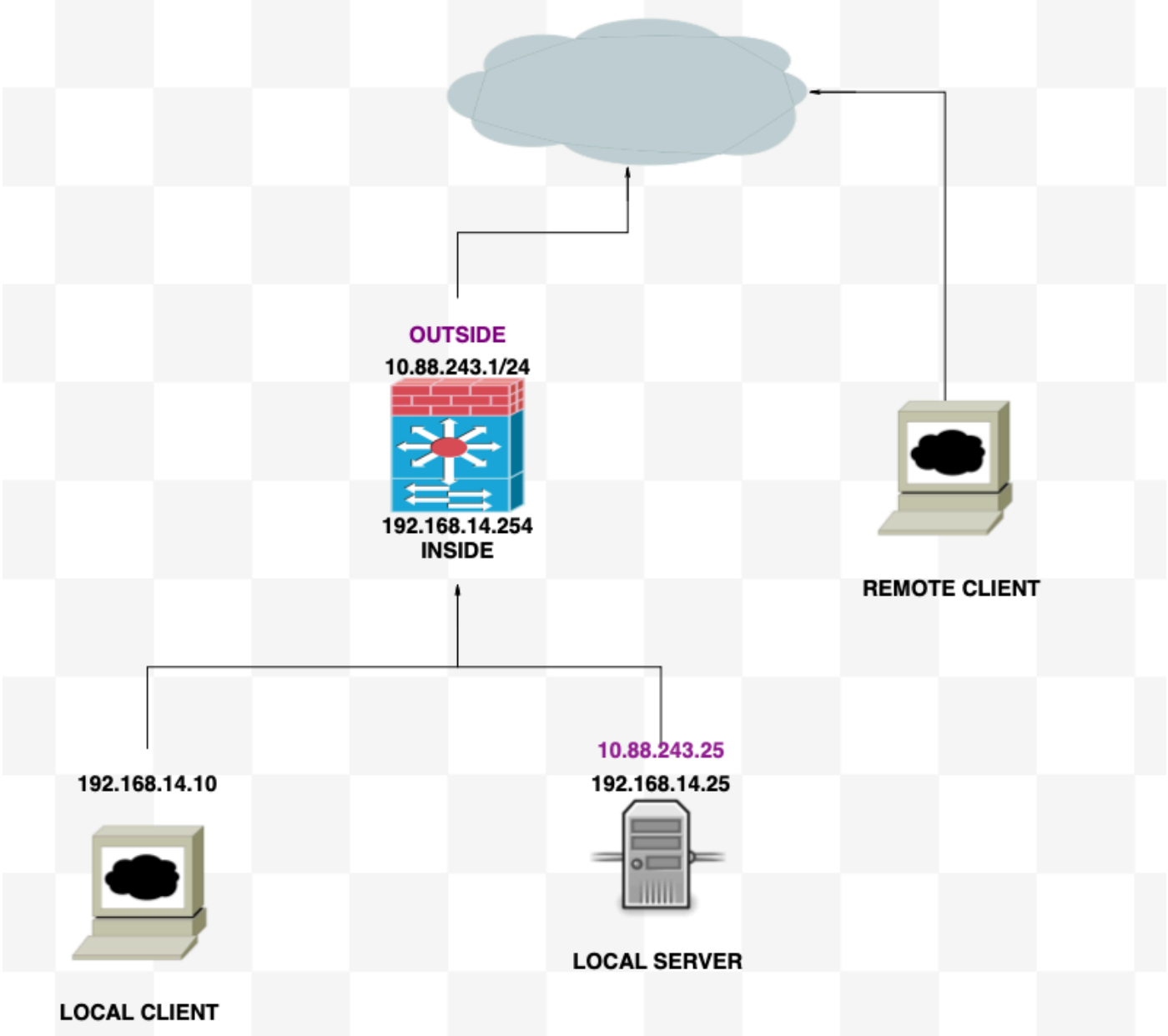
之所以使用发夹这一术语是因为来自客户端的流量进入路由器（或实施NAT的防火墙），然后被转换后像发夹一样返回到内部网络，以访问服务器的专用IP地址。

例如，您的本地网络上有一台具有私有IP地址的Web服务器。您想使用其公有IP地址或解析为公有IP地址的域名访问此服务器，即使您位于同一本地网络上。

如果没有发夹NAT，您的路由器将无法理解此请求，因为它期望对公共IP地址的请求来自网络外部。

发夹NAT允许路由器识别虽然请求发送到公共IP，但需要将其路由到本地网络中的设备，从而解决该问题。

网络图



配置

步骤1:创建对象

- 内部网络：192.168.14.10
- Web服务器：192.168.14.25
- 公共Web服务器：10.88.243.25
- 端口：80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

第二步：创建NAT

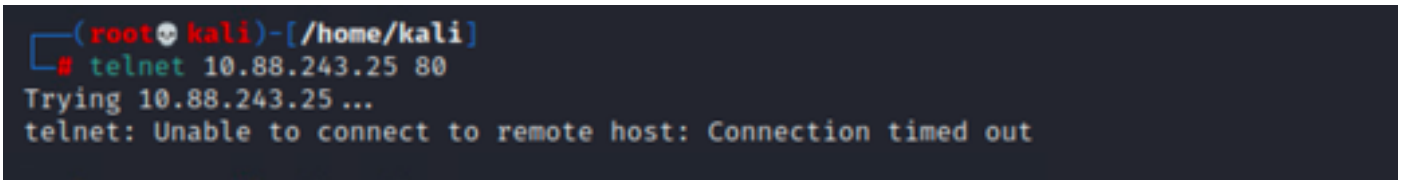
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

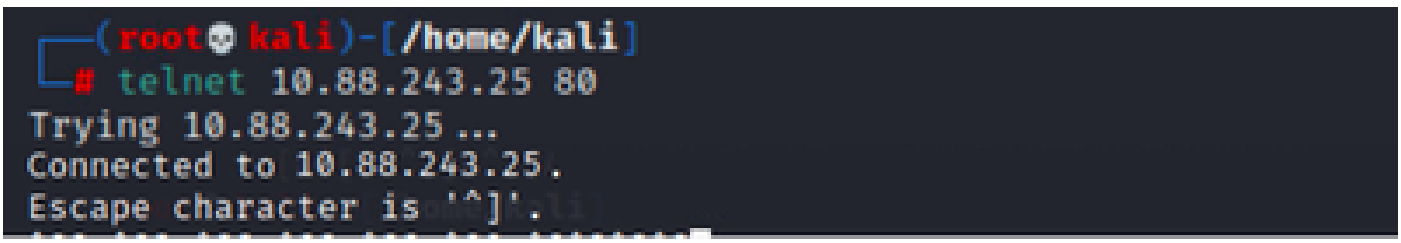
验证

从本地客户端使用目的端口执行telnet目的IP：

如果此消息“telnet unable to connect to remote host： Connection timed out”提示符，则在配置期间的某个时间出现了问题。



但如果它显示“Connected”，它就会成功！



故障排除

如果遇到网络地址转换(NAT)问题，请使用本分步指南排除和解决常见问题。

第1步：NAT规则配置检查

- 检查NAT规则：确保所有NAT规则都配置正确。检查源和目的IP地址以及端口是否准确。
- 接口分配：确认NAT规则中正确分配了源接口和目标接口。不正确的映射可能导致无法正确转换或路由流量。
- NAT规则优先级(NAT Rule Priority)：验证NAT规则的优先级是否高于可能匹配相同流量的任何其他规则。规则按顺序处理，因此放在较高位置的规则具有优先权。

第2步：访问控制规则(ACL)验证

- 检查ACL：检查访问控制列表，确保它们适用于允许NAT流量。必须配置ACL以识别转换后的IP地址。
- 规则顺序：确保访问控制列表的顺序正确。与NAT规则一样，ACL也是自上而下进行处理，并且与流量匹配的第一个规则是应用的规则。
- Traffic Permissions：验证是否存在适当的访问控制列表，以允许从内部网络到转换后目标的流量。如果缺少规则或规则配置不正确，可能会阻止所需的流量。

第3步：其他诊断

- 使用诊断工具：利用可用的诊断工具监控和调试通过设备的流量。这包括查看实时日志和连接事件。
- 重新启动连接：在某些情况下，现有连接无法识别对NAT规则或ACL所做的更改，直到它们重新启动。考虑清除现有连接以强制应用新规则。

<#root>

ciscoasa(config)#

clear xlate

- 验证转换：如果您使用ASA设备来验证是否正在按预期执行NAT转换，请在命令行中使用show xlate和show nat等命令。

<#root>

ciscoasa(config)#

show xlate

<#root>

```
ciscoasa(config)#
 show nat
```

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）。