使用Firepower管理中心配置发夹

目录

简介

本文档介绍使用Firepower管理中心(FMC)在Firepower威胁防御(FTD)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：

- Firepower Management Center (FMC)
- 防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower管理中心虚拟7.2.4。
- Firepower威胁防御虚拟7.2.4。

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。

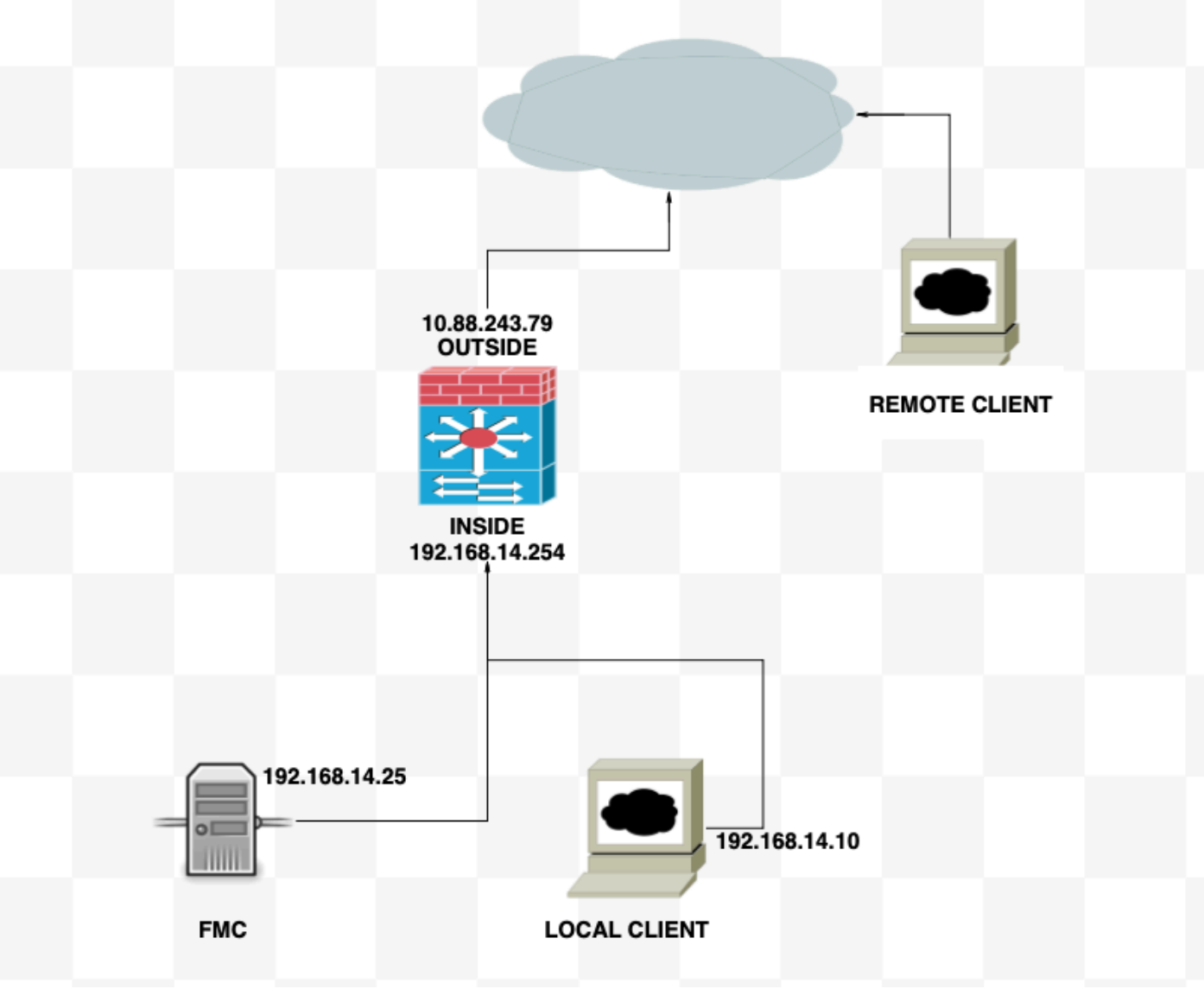
配置

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。

此功能对于本地网络中的Web托管等网络服务非常有用，因为本地网络上的用户需要使用与外部用户相同的URL或IP地址访问内部服务器。无论请求是从本地网络内部还是外部发出，它都可以确保资源的统一访问。

在本示例中，必须通过FTD的外部接口的IP访问FMC

图解

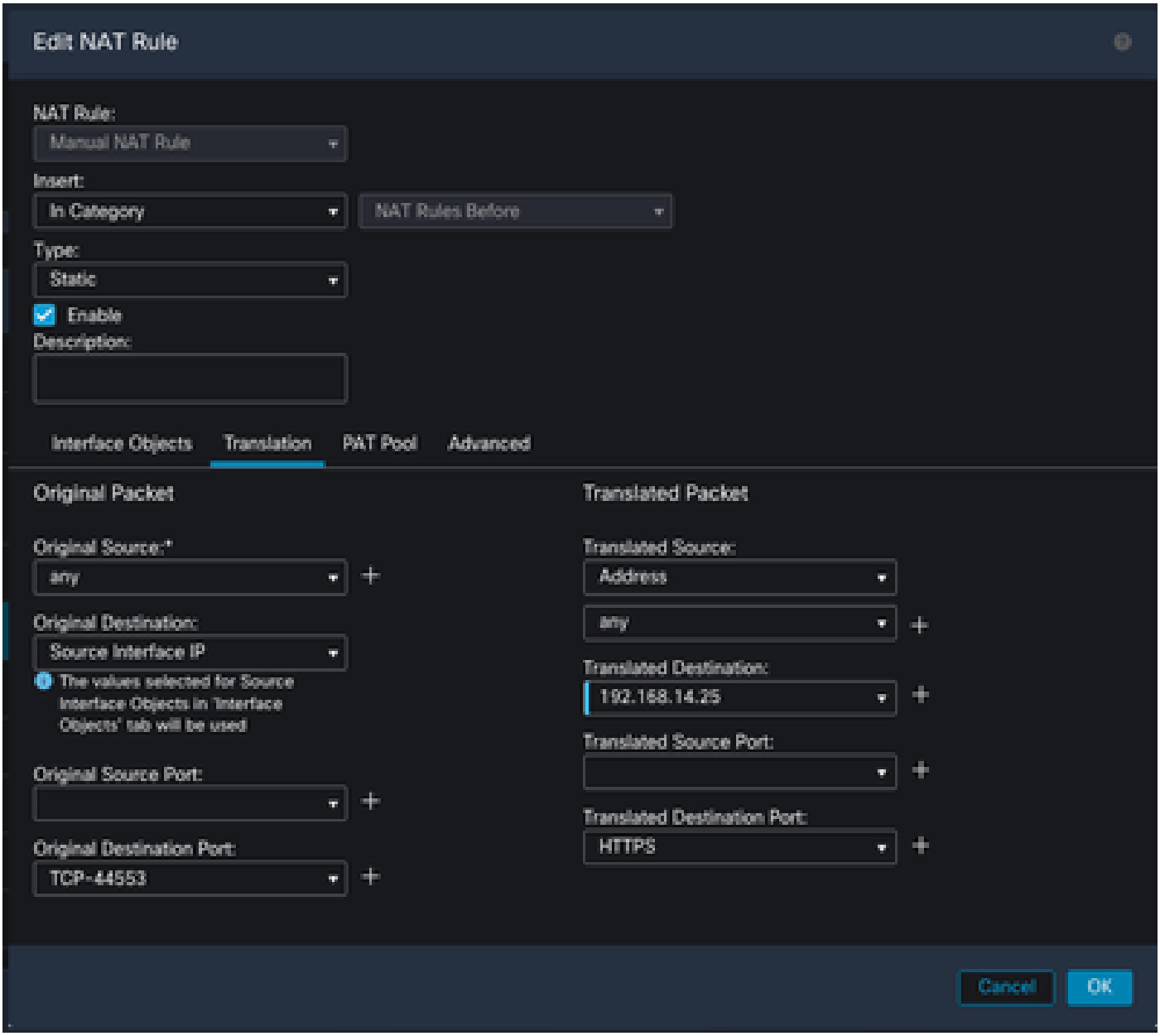


步骤1:配置外部内部Nat

首先，必须配置静态NAT；在本示例中，使用外部接口的IP转换目标IP和目标端口，44553换端口目标。

在FMC中，导航到设备> NAT以创建或编辑现有策略，然后点击添加规则框。

- NAT规则：手动Nat规则
- 原始来源：任意
- 原始目标：源接口IP
- 原始目标端口：44553
- 转换后的目的地： 192.168.14.25
- 转换后的目标端口：443



配置策略。导航到策略>访问控制以创建或编辑现有策略，然后点击添加规则框。

源区域：外部

目标区域：内部

源网络：任意

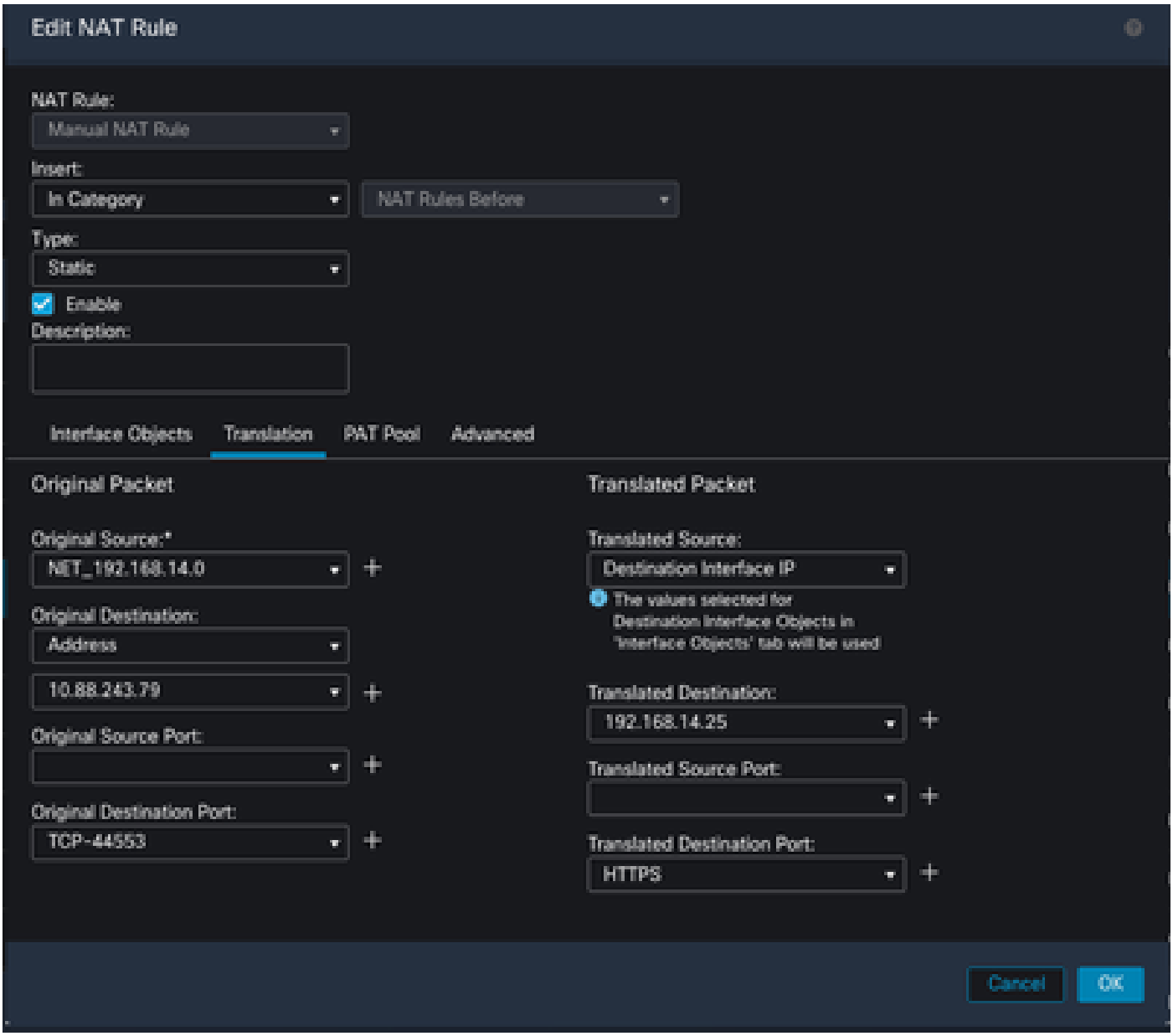
目的网络：10.88.243.79

第二步：配置内部到内部Nat（发夹）

第二步，必须从内部配置静态NAT；在本示例中，目标IP和目标端口使用对象与外部接口的IP进行转换，目标端口为44553。

从FMC导航到设备> NAT以编辑现有策略，然后点击添加规则框。

- NAT规则：手动Nat规则
- 原始来源：192.168.14.0/24
- 原始目的地：地址10.88.243.79
- 原始目标端口：44553
- 转换后的源：目标接口IP
- 转换后的目的地： 192.168.14.25
- 转换后的目标端口：443



配置策略。导航到策略>访问控制以编辑现有策略，然后点击添加规则框。

源区域：任意

目标区域：任意

源网络：192.168.14.0/24

目的网络：10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	Any
2	Hairpin	Any	Any	NET_192.168.14	10.88.243.79

验证

从本地客户端对目的IP和目标端口执行telnet：

如果此错误消息“telnet unable to connect to remote host： Connection timed out”提示，则在配置期间的某一时刻出现了问题。

```
┌──(root💀kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

但如果它显示Connected，则配置成功。

```
┌──(root💀kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

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规则都在FMC中正确配置。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规则是否位于可匹配相同流量的任何其他规则的顶部。FMC中的规则按顺序处理，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FMC中提供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。

从LINA：

```
<#root>

firepower#

 clear xlate
```

- 验证转换：如果使用FTD设备验证NAT转换是否按预期执行，请在命令行中使用show xlate和show nat等命令。

从LINA：

```
<#root>

firepower#

 show nat
```

```
<#root>

firepower#

 show xlate
```

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）。