在CSPC NAT路由器中禁用PING (ICMP)

目录

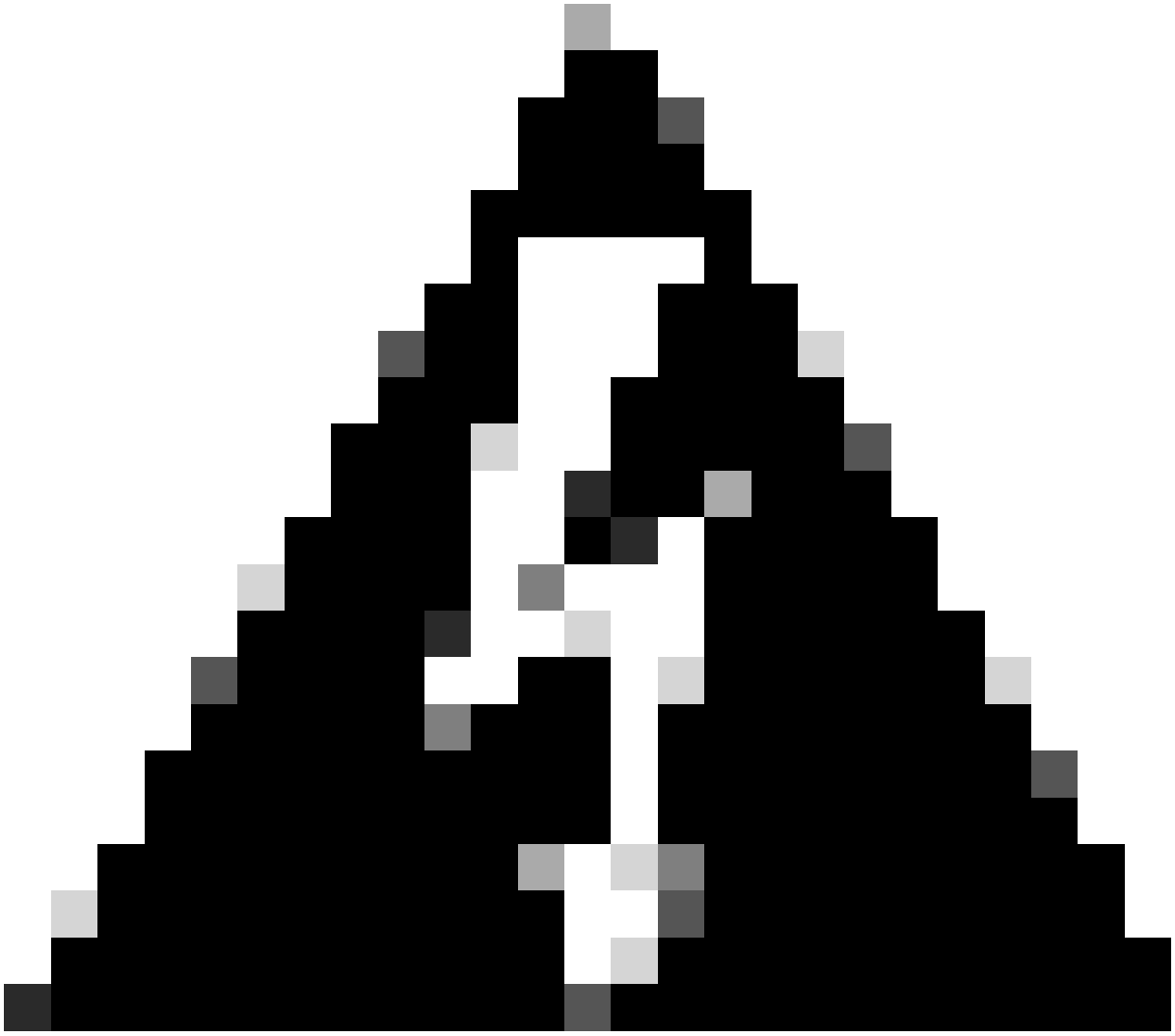
简介

本文档介绍如何阻止来自Cent7_NAT路由器的ICMP (ping)响应。

先决条件

要求

对NAT路由器的根访问



警告：请记住，禁用ICMP会导致traceroute（从Linux）和tracert（从windows）不可用。

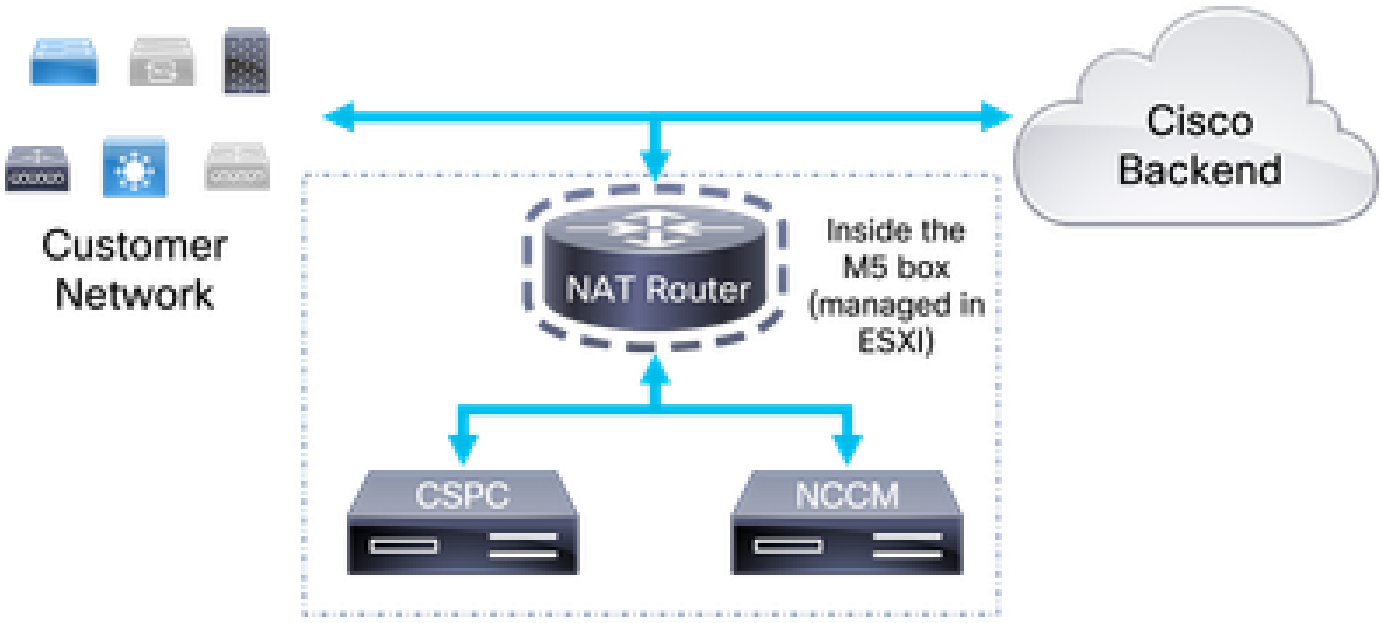
使用的组件

- CSPC（测试版本：Cent7_NAT_V3.ova）
- （可选）访问ESXI（以防与VM的连接丢失）

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

网络图



配置

1. 使用收集器的IP地址和SSH客户端上的端口1022登录NAT路由器。
2. 将用户更改为根用户。

```
su -
```

3. 备份/etc/sysctl.conf文件：

```
cp /etc/sysctl.conf /etc/sysctl.conf.bkup<date>
```

```
[root@localhost sysconfig]# ls -ltr /etc/sysctl.conf
-rw-r--r--. 1 root root 1449 Aug 10  2021 /etc/sysctl.conf
[root@localhost sysconfig]# cp /etc/sysctl.conf /etc/sysctl.conf.bkup29March2022
[root@localhost sysconfig]#
```

4. 备份后，修改/etc/sysctl.conf文件并添加以下行：

```
net.ipv4.icmp_echo_ignore_all = 1
```

5. 注释掉所有匹配net.ipv4.icmp的行。
6. 保存更改。

```
net.ipv4.conf.default.log_martians=1
#
##deny icmp (ping)
net.ipv4.icmp_echo_ignore_all =1
##deny icmp (ping)
#
##net.ipv4.icmp_echo_ignore_broadcasts=1
##net.ipv4.icmp_ignore_bogus_error_responses=1
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

⚠ 警告：在步骤7之后，对CSPC、NCCM和AFM的SSH访问丢失

7. 使用命令加载新变量。

```
sysctl -p
```

⚠ 警告：在步骤8之后，与CSPC、NCCM和AFM的连接中断。这可能会影响从NCCM应用到设备的持续收集和更改。

8. 重新启动NAT路由器。

9. 通过打开SSH会话验证与CSPC、NCCM和AFM的连接（如果适用）。

验证

步骤7完成后，对Cent7_NAT路由器的IP地址执行ping操作会停止响应。
攻击前：

```
C:\Users\Gabriel.Milenko>ping 10.79.245.174

Pinging 10.79.245.174 with 32 bytes of data:
Reply from 10.79.245.174: bytes=32 time<1ms TTL=62
Reply from 10.79.245.174: bytes=32 time<1ms TTL=62
Reply from 10.79.245.174: bytes=32 time<1ms TTL=62
Reply from 10.79.245.174: bytes=32 time<1ms TTL=62

Ping statistics for 10.79.245.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

在:

```
C:\Users\Gabriel.Milenko>ping 10.79.245.174

Pinging 10.79.245.174 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.79.245.174:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

故障排除

如果在Cent7_NAT路由器重新启动后无法恢复与CSPC、NCCM或AFM盒的连接，请登录Cent7_NAT路由器，并使用步骤3中的备份恢复更改。

```
cp /etc/sysctl.conf.bkup<date> /etc/sysctl.conf
```

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）。