Disable PING (ICMP) in the CSPC NAT Router

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

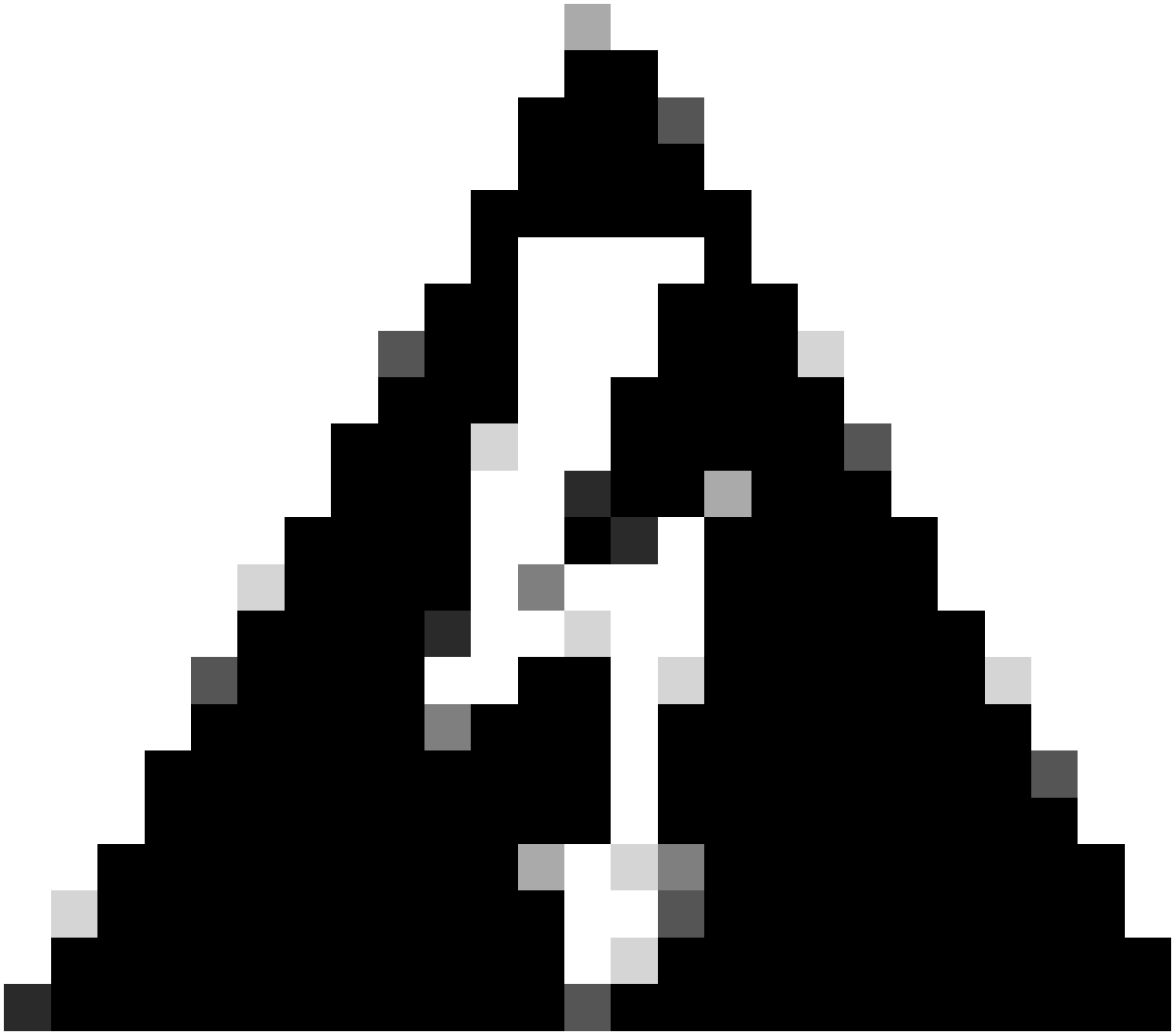
Introduction

This document describes how to block ICMP (ping) responses from Cent7_NAT router.

Prerequisites

Requirements

Root access to the NAT router



Warning: Keep in mind that disabling ICMP renders traceroute (from Linux) and tracert (from windows) unusable.

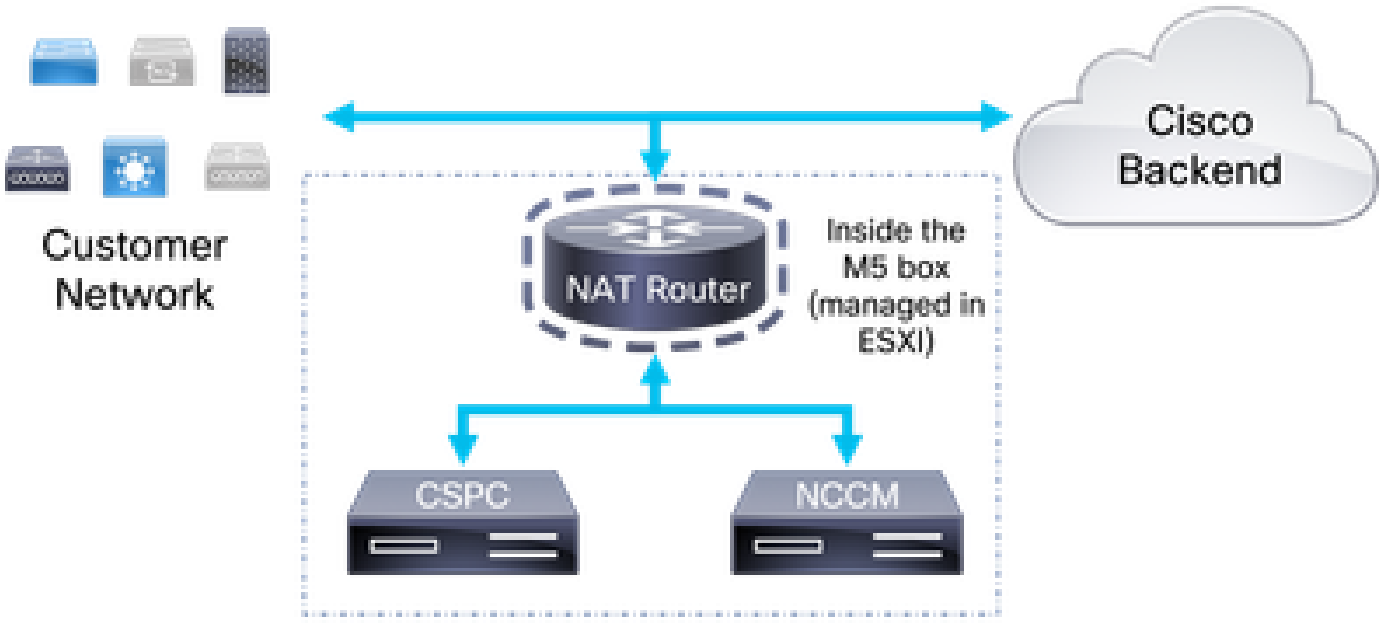
Components Used

- CSPC (tested version: Cent7_NAT_V3.ova)
- (Optional) Access to ESXI (in case connectivity to the VM is lost)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configurations

1. Log in to the NAT router by using the IP of your collector and port 1022 on your SSH client.
2. Change your user to root.

```
su -
```

3. Backup the /etc/sysctl.conf file:

```
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. Once backed up, modify the **/etc/sysctl.conf** file and add the line:

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

5. Comment out all lines matching **net.ipv4.icmp**.
6. Save your changes.

```
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
```

Warning: SSH access to CSPC, NCCM and AFM is lost after step 7

7. Load the new variables with the command.

```
sysctl -p
```

Warning: Connection from CSPC, NCCM, and AFM is interrupted after step 8. This can affect ongoing collections and changes being applied from NCCM to the devices.

8. Reboot the NAT router.

9. Verify connectivity to CSPC, NCCM and AFM (if applicable) by opening a SSH session to them.

Verify

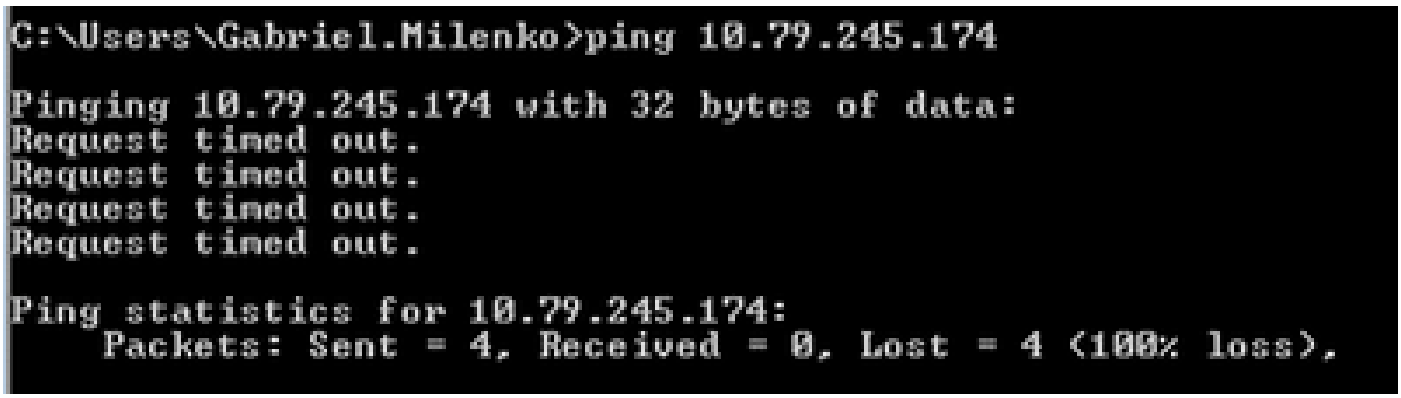
After step 7, ping to the Cent7_NAT router IP address stops responding.
Before:

```
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
```

After:



Troubleshoot

If connectivity to the CSPC, NCCM or AFM boxes is not recovered upon reboot of the Cent7_NAT router, log into the Cent7_NAT router and revert the changes using the backup from step 3.

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