NSCA Server - Inbound TCP Traffic

Article Number: 84 | Rating: Unrated | Last Updated: Wed, Jan 9, 2019 at 9:11 PM

Inbound TCP Traffic

These steps explain how to confirm that the NSCA server is receiving traffic destined for it on the port 5667.

In this example, the following applies:

- Remote computer sending NSCA checks
  - 10.25.14.2
- Nagios server receiving NSCA checks
  - 10.25.5.57

The purpose of this test is to confirm that the network traffic is hitting the Nagios XI server. TCP dump displays the lower level of network traffic before it is intercepted by the Operati

The OS firewall rules are not evaluated yet and hence this test allow you to clearly determine if this traffic is hitting the Nagios XI server.

If your tests show that no traffic is being received then there must be other firewall(s) between the sending device and the Nagios XI server that are blocking the traffic.

Install / Update tcpdump

Establish an SSH session to the Nagios server that has NSCA installed. Execute the following command to install the `tcpdump` program, depending on your OS:

RHEL | CentOS | Oracle Linux

```
yum -y install tcpdump
```

Debian | Ubuntu

```
apt-get install -y tcpdump
```

Wait while tcpdump is installed/updated.

Watch TCP Traffic - Reverse DNS Lookup

Execute the following command:

```
tcpdump src host 10.25.14.2 and tcp dst port 5667 and dst host 10.25.5.57
```

Which should product output like:

```
16:31:30.953780 IP server01.domain.local.49173 > nagioscore01.domain.local.nsca: Flags [S], seq 2930403808, win 8192, options [mss 1460
16:31:30.954118 IP server01.domain.local.49173 > nagioscore01.domain.local.nsca: Flags [.], ack 529817198, win 256, length 0
16:31:30.957628 IP server01.domain.local.49173 > nagioscore01.domain.local.nsca: Flags [P.], seq 0:720, ack 133, win 256, length 720
16:31:30.957647 IP server01.domain.local.49173 > nagioscore01.domain.local.nsca: Flags [F.], seq 720, ack 133, win 256, length 0

16:31:31.958270 IP server01.domain.local.49173 > nagioscore01.domain.local.nsca: Flags [.], ack 134, win 256, length 0
```

When you have finished watching the network traffic press **CTRL + C** to kill `tcpdump`.

Watch TCP Traffic - NO Reverse DNS Lookup

Execute the following command:

```
tcpdump -n src host 10.25.14.2 and tcp dst port 5667 and dst host 10.25.5.57
```

Which should product output like:

```
16:34:31.006031 IP 10.25.14.2.49177 > 10.25.5.57.nsca: Flags [S], seq 2888165083, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sack
16:34:31.006414 IP 10.25.14.2.49177 > 10.25.5.57.nsca: Flags [.], ack 1878217608, win 256, length 0
16:34:31.008941 IP 10.25.14.2.49177 > 10.25.5.57.nsca: Flags [P.], seq 0:720, ack 133, win 256, length 720
16:34:31.008978 IP 10.25.14.2.49177 > 10.25.5.57.nsca: Flags [F.], seq 720, ack 133, win 256, length 0
16:34:32.009828 IP 10.25.14.2.49177 > 10.25.5.57.nsca: Flags [.], ack 134, win 256, length 0
```

When you have finished watching the network traffic press **CTRL + C** to kill `tcpdump`.

Troubleshooting

If you receive this message when trying to execute `tcpdump`:

```
tcpdump: NFLOG link-layer type filtering not implemented
```

Then you will need to define the interface name with the **`-i xxx`** argument, for example:

```
tcpdump -i ens32 src host 10.25.14.2 and tcp dst port 5667 and dst host 10.25.5.57
```

Conclusion

With these steps you will be able to confirm that the NSCA server is correctly receiving TCP traffic on port 5667 from the remote server.

Your next troubleshooting step would be to confirm the firewall rules are in place.

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/

Posted by: **tlea** - Tue, Mar 24, 2015 at 1:22 AM. This article has been viewed 20168 times.

Online URL: https://support.nagios.com/kb/article/nsca-server-inbound-tcp-traffic-84.html