

#Troubleshooting# How to Perform Health Check on Security Appliance

***Product:** NSF

***Version:** 8.0.85

*1. Introduction

1.1 User Scenario

Nowadays, the importance of having an efficient firewall is fundamental because it ensures a security perimeter for the corporate network. Being a network device in operation 24 hours a day, it is essential to monitor it and perform routine operations to keep it in optimal condition.

Firewalls play a crucial role in safeguarding networks from cyber threats, and regular maintenance ensures their effectiveness.

1.2 Requirements

1. The user's network has NSF device as firewall.

*2. Health check steps

In this guide, we will see the main checks and maintenance tasks performed to keep the firewall in optimal condition. This guide is not specific to any model of Sangfor NSF.

2.1 Check Hardware Status

- Verify the power supply, fans, and other physical components.
- Inspect the LEDs on the device to ensure they indicate normal operation.

2.2 Review System Logs

- Navigate to the system logs section and review any error messages or warnings.
- Look for anomalies related to CPU usage, memory, or network interfaces.

2.3 Check Network Interfaces

- Verify that all network interfaces (WAN, LAN, DMZ, etc.) are up and operational.
- Ensure that IP addresses, subnet masks, and gateway settings are configured correctly.

2.4 Security Policy Inspection

- Review the security policies configured on the appliance.
- Ensure that rules are correctly defined and match the desired security posture.

2.5 Update Signatures and Threat Intelligence

- Sangfor Network Secure relies on threat intelligence feeds to detect and prevent attacks.
- Regularly check that all databases in the Security Capability Update are updated.

2.6 Test Connectivity and Traffic Flow

- Perform connectivity tests by sending traffic through the appliance.
- Verify that traffic correctly passes through the firewall rules and policies (both inbound and outbound) by looking the hits on policy page. It's also a good idea to do a precise traffic test through the troubleshooting section of NSF to ensure that the policy is working as expected.

*3. Precaution

1. Keep in mind that it's recommended to monitor firewall metrics with tools like PRTG or Zabbix through SNMP to have historical data about traffic, interface uptime and so on (with alerts and triggers configured).

It's also a good idea to set email alerts on Sangfor NSF about login failure and other user driven events.