#Troubleshooting# Troubleshooting network issues on HA cluster's passive firewall

*Product: NSF

*Version: 8.0.85

***1. Introduction**

1.1 User Scenario

Two NGAF devices deployed as High Availability deployment can give redundancy when device failure (hardware or software) happens on the environment.

On this case, it's important to have redundancy link for WAN and LAN connections to keep connected both cluster members that are in High Availability mode.

1.2 Requirements

1. The user's network has two NSF devices as firewalls in HA mode.

***2. Troubleshooting steps**

In this guide, we will see the main checklist to perform when there's an issue with the connection from the internal network to the external network after connecting the ISP link to the passive Sangfor NSF firewall in HA mode (High Availability).

2.1 Verify Configuration

- Confirm that Sangfor NSF firewalls are correctly configured in HA mode and the heartbeat connection is normal between two devices.
- HA Status is normal on both devices.
- Ensure all the production interface are added to member interface.

2.2 Check Interfaces and Zones

- Verify the configuration of the external (WAN) and internal (LAN) network interfaces on both firewalls.
- Assign the correct zones to each interface. ⌗

2.3 Check Routing

Check if routing is normal, verify the next-hop address is normal and the route status is "valid".

2.4 NAT Policies

- Examine the NAT policies:
    - Ensure that NAT translation is correctly configured for traffic going from the internal network to the external network (Internet)

2.5 Access Control Policies

- Check the access control policies:
    - Verify that traffic from the internal network to the external network is allowed.
    - Confirm that application control policies do not block necessary traffic.

2.6 Monitor Logs and Alerts

- Regularly monitor logs for error messages or dropped packets.
- Set up alerts to notify you of any issues (e.g., link failure, HA failover).

*3. Precaution

Remember that proper configuration of routing, and security policies are essential for successful communication between the internal and external networks.