

# #Risoluzione dei problemi# Risoluzione dei problemi relativi alla rete sul firewall passivo di un cluster firewall

**\* Prodotto:** NSF

**\* Versione:** 8.0.85

## \*1. Introduzione

### 1.1 Scenario utente

Avere un cluster di firewall in alta affidabilità (High Availability) offre ridondanza in caso di guasto (hardware o software) su uno dei membri del cluster.

In questo caso, è importante avere un collegamento ridondante per le connessioni WAN e LAN al fine di mantenere connessi entrambi i membri del cluster che sono in alta affidabilità (High Availability).

### 1.2 Requisiti

1. La rete dell'utente dispone di due firewall Sangfor NGAF configurati in alta affidabilità.

## \*2. Passaggi per la risoluzione dei problemi

In questa guida, vedremo i principali controlli da effettuare quando si verifica un problema con la connessione dalla rete interna alla rete esterna dopo aver collegato il link ISP (WAN) al membro passivo Sangfor NSF del cluster firewall (alta affidabilità).

### 2.1 Verifica della configurazione

- Confermare che i firewall Sangfor NSF siano correttamente configurati in alta affidabilità e che vi è heartbeat tra i due membri del cluster.
- Assicurarsi che il firewall passivo sia sincronizzato con quello attivo (ad eccezione dell'interfaccia di heartbeat).

### 2.2 Verifica delle interfacce e delle zone

- Verificare la configurazione delle interfacce di rete esterne (WAN) e interne (LAN) su entrambi i firewall.
- Assegnare le zone corrette a ciascuna interfaccia.

## 2.3 Routing e gateway predefinito

- Configurare una rotta predefinita (0.0.0.0/0) che punti al router del provider (gateway ISP).
- Confermare che l'indirizzo next-hop per la rotta predefinita sia impostato correttamente (solitamente è l'ip dell'apparato del provider).

## 2.4 NAT Policies

- Esaminare le policies NAT:
  - Assicurarsi che la traduzione NAT sia configurata correttamente per il traffico che va dalla rete interna alla rete esterna (Internet)

## 2.5 Policy di controllo degli accessi

- Verificare le policy di controllo degli accessi:
  - Accertarsi che il traffico dalla rete interna alla rete esterna sia consentito.
  - Assicurarsi che le policy di controllo delle applicazioni non blocchino il traffico.

## 2.6 Monitoraggio dei log e degli avvisi

- Monitorare regolarmente i log per eventuali messaggi di errore o pacchetti persi.
- Configurare gli avvisi per essere informati di eventuali problemi (ad esempio, guasto del collegamento, failover HA).

## \*3. Precauzione

1. Tenere a mente che una corretta configurazione, il routing e le policy di sicurezza sono essenziali per una comunicazione efficace tra la rete interne e la rete esterna.