#Risoluzione Problemi# Come eseguire un check sullo stato di salute del firewall

***Product:** NSF

***Version:** 8.0.85

*1. Introduzione

1.1 Scenario

Oggigiorno l'importanza di avere un firewall efficiente è fondamentale dato che esso garantisce un perimetro di sicurezza riguardo la rete aziendale. Essendo un dispositivo di rete in funzione ogni giorno 24 ore su 24, è importante tenerlo monitorato ed eseguire operazioni di routine al fine di mantenerlo in stato ottimale.

I firewall svolgono un ruolo cruciale nel proteggere le reti dalle minacce informatiche, e la manutenzione regolare ne garantisce l'efficacia.

1.2 Requisiti

1. La rete dell'utente deve avere Sangfor NSF come firewall.

*2. Health check steps

In questa guida, vedremo i principali controlli e le attività di manutenzione da eseguire per mantenere il firewall in condizioni ottimali. Questa guida non è specifica per un modello particolare di Sangfor NSF.

Ecco una breve descrizione delle attività da svolgere:

2.1 Verifica dello stato hardware

- Assicurarsi che tutti i componenti hardware funzionino correttamente.
- Verificare l'alimentazione, le ventole e gli altri componenti fisici.
- Ispezionare i LED del dispositivo per garantire che indichino un funzionamento normale.

2.2 Revisione dei log di sistema

- Accedere all'interfaccia di gestione del dispositivo tramite l'interfaccia web.
- Navigare nella sezione dei log di sistema e verificare eventuali messaggi di errore o avvisi.

- Rilevare anomalie legate all'utilizzo della CPU, alla memoria o alle interfacce di rete.

2.3 Verifica delle interfacce di rete

- Verificare che tutte le interfacce di rete (WAN, LAN, DMZ, ecc.) siano operative.
- Controllare eventuali errori o collisioni sulle interfacce.
- Assicurarsi che gli indirizzi IP, le maschere di sottorete e le impostazioni del gateway siano configurati correttamente.

2.4 Ispezione delle politiche di sicurezza

- Rivedere le politiche di sicurezza configurate sull'appliance.
- Verificare che le regole siano correttamente definite e corrispondano alla postura di sicurezza desiderata.
- Controllare la presenza di regole obsolete o non necessarie.

2.5 Aggiornamento delle firme e dell'intelligence sulle minacce

- Sangfor Network Secure si basa su feed di intelligence sulle minacce per rilevare e prevenire gli attacchi.
- Verificare regolarmente che le firme delle minacce siano aggiornate.

2.6 Test di connettività e flusso di traffico

- Eseguire test di connettività inviando traffico attraverso l'appliance.
- Verificare che il traffico passi correttamente attraverso le regole e le politiche del firewall (sia in ingresso che in uscita).
- È anche consigliabile effettuare test di traffico precisi attraverso la sezione di risoluzione dei problemi di NSF per garantire che le politiche funzionino come previsto.

2.7 Revisione delle metriche di performance

- Monitorare la larghezza di banda, la latenza e l'utilizzo delle risorse.
- Assicurarsi che l'appliance operi nei limiti specificati.
- Consultare la documentazione del modello Sangfor NSF per specifiche dettagliate sull'appliance che si sta utilizzando.

*3. Precauzioni

1. Si consiglia di monitorare le metriche del firewall con strumenti come PRTG o Zabbix tramite SNMP per avere dati storici sul traffico, l'uptime delle interfacce e altro (con allarmi e trigger configurati).

È anche una buona idea impostare avvisi via e-mail su Sangfor NSF per eventi come i tentativi di accesso falliti e altre attività degli utenti.