#Risoluzione# Risolvere problematiche inerenti l'accesso internet con NGAF come firewall

***Prodotto:** NGAF

***Versione:** 8.0.85

*1. Introduzione

1.1 Scenario

Sostituire un firewall su una rete esistente può comportare delle difficoltà. In questa guida vedremo quali sono le possibili soluzioni nel caso non vi sia connettività internet dopo aver configurato il firewall Sangfor NGAF

1.2 Requisiti

1. Firewall Sangfor NGAF aggiornato all'ultima release

*2. Guida per la risoluzione dei problemi

In questa guida, vedremo cosa controllare nel caso gli utenti serviti dal firewall Sangfor NGAF non riescano a navigare (a prescindere dalla modalità di configurazione del firewall).

2.1 Sangfor NGAF configurato in modalità Route

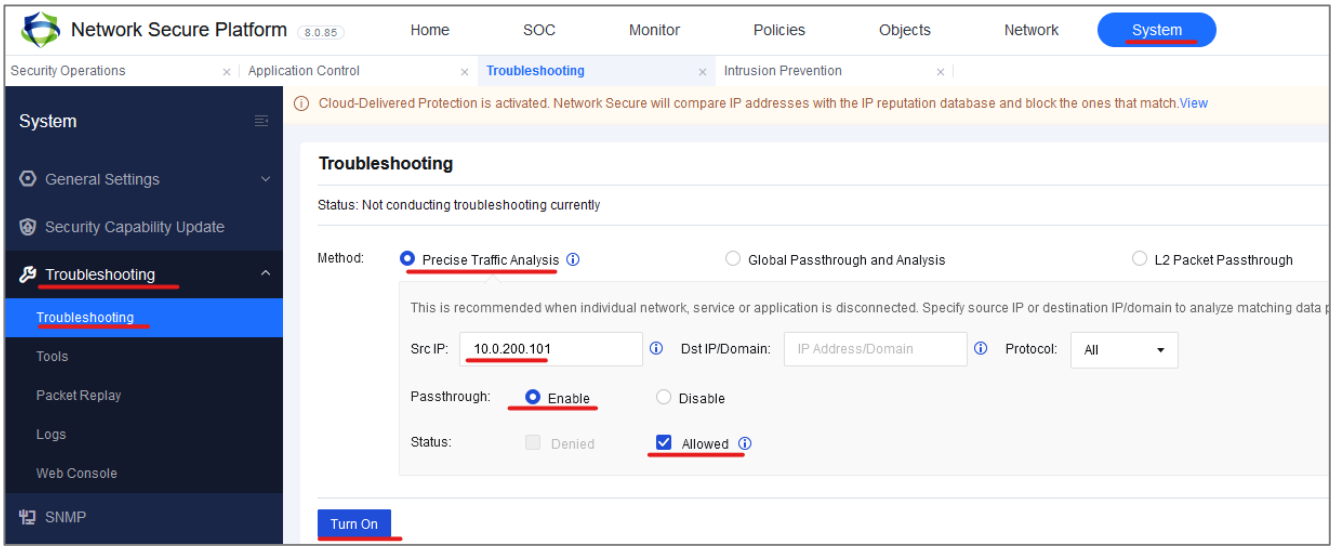
Se il firewall Sangfor NGAF è configurato in modalità route e la tua rete locale è layer L2, il gateway dei PC deve essere l'ip assegnato all'interfaccia LAN del firewall NGAF. Controllare se l'p sorgente dei client riesce a raggiungere l'p dell'interfaccia LAN del firewall o se viene bloccato da una policy.

Se non riuscite a pingare l'interfaccia LAN del firewall, verificare se vi sono restrizioni configurate nello switch inerente l'ip del PC o se vi è una configurazione errata della VLAN ove il PC risiede. Inoltre, controllare se vi sono Access Control List (ACL) impostate nello switch che impediscono l'accesso alla rete esterna dal PC.

Invece, se la vostra rete locale LAN è configurata come Layer 3 su NGAF ed un utente non riesce a navigare su internet su una rete Layer 3, potete effettuare un test pingando l'ip dello switch. Se il ping fallisce, controllare se vi sono problemi con lo switch core cui il PC è connesso. Se l'ip dello switch è pingabile, provate a pingare l'interfaccia LAN del firewall NGAF.

Nel caso non riuscite a pingare l'interfaccia LAN del firewall, provate ad effettuare un login sul

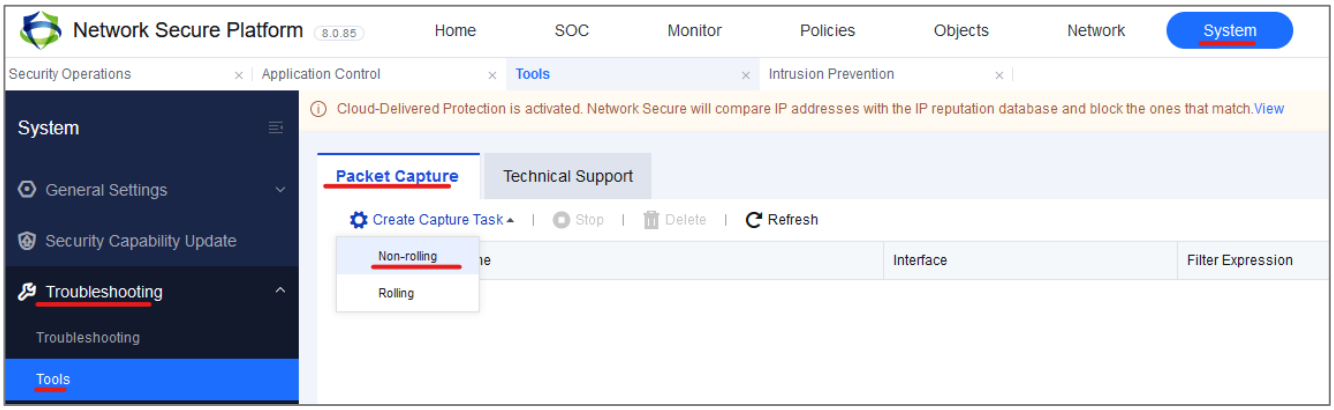
firewall NGAF. Se il login va a buon fine, potete abilitare il pass-through per quell'ip che non riesce ad accedere ad internet. Questo vi è d'aiuto nel verificare se vi è una policy che effettivamente blocca l'accesso ad internet da quel pc. Per far ciò, recarsi su: **System > Troubleshooting > Troubleshooting > Precise Traffic Analysis** e configurare l'ip del pc nel campo IP address. Fare attenzione a non configurare l'ip del pc sul campo excluded IP. Per esempio, se noi abbiamo un PC avente IP 10.0.200.101 è possibile abilitare l'analisi del traffico come segue:



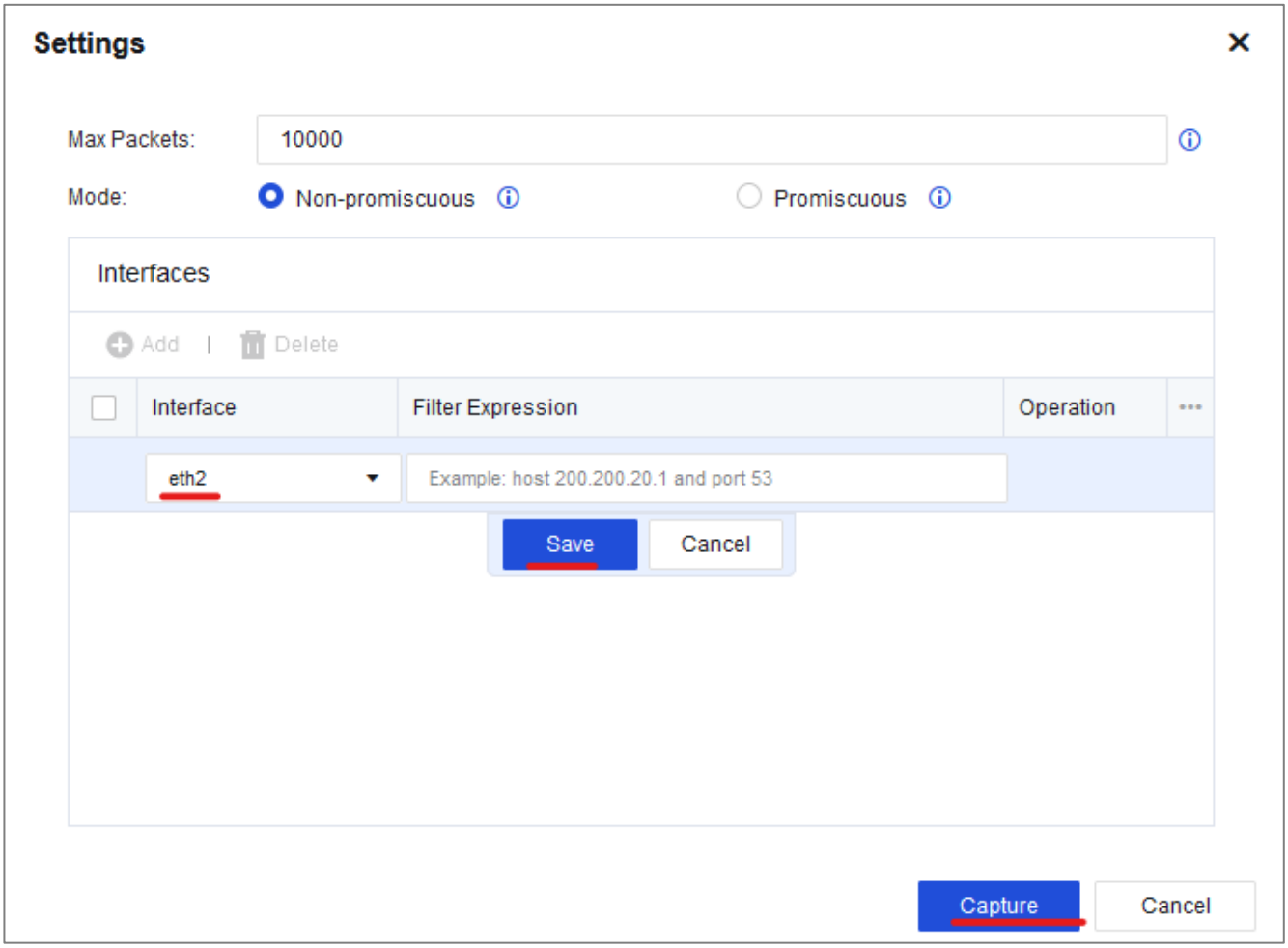
Se ancora la navigazione non dovesse funzionare dopo aver attivato il pass-through, è possibile catturare i pacchetti recandosi su **System > Troubleshooting > Tools > Packet Capture** al fine di catturare il traffico generato dal PC. Analizzando il file contenente il dump della cattura del traffico è possibile capire se i pacchetti del traffico generato dal PC effettivamente raggiungono l'interfaccia LAN del firewall o se vi sono altri dispositivi in rete che eseguono un NAT dell'ip sorgente del PC che non riesce a navigare in internet.

Per catturare i pacchetti che arrivano all'interfaccia lan del firewall (eth2 nel nostro NGAF) riporto di seguito i passaggi:

1) Avviare una cattura di pacchetti non rolling

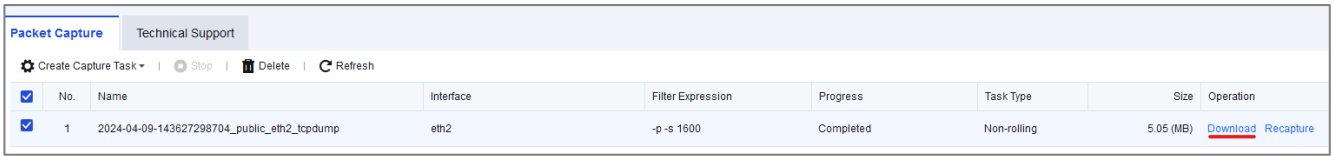


2) Specificare l'interfaccia LAN del firewall e confermare cliccando salva. Avviare la cattura dei pacchetti.



3) Effettuare dei test di accesso internet da parte del PC che non naviga e al termine cliccare su stop capture.

4) In seguito, cliccare su download per caricare il file contenente il traffico pervenuto al firewall nell'interfaccia LAN



5) Usare uno strumento esterno come Wireshark per analizzare il file dump del traffico contenente tutti i dettagli del traffico che è pervenuto dalla rete locale verso il firewall.

Se nell'interfaccia LAN del firewall non è pervenuto alcun pacchetto da parte del PC coinvolto, controllare se vi sono restrizioni Access Control List (ACL) sulla porta cui è collegato il PC sul switch core.

Se l'interfaccia LAN del firewall è riuscita a catturare del traffico proveniente dal PC, dovreste effettuare una nuova cattura di pacchetti nell'interfaccia WAN ed avviare un ping dal PC verso l'ip della risorsa esterna che si vuole raggiungere.

Questo per verificare se l'indirizzo IP del PC viene tradotto correttamente. Fare riferimento ai passi precedenti su come effettuare la cattura dei pacchetti.

Nel seguente documento, l'interfaccia WAN del firewall è Eth1 e l'interfaccia LAN del firewall è Eth2. L'indirizzo del PC è 10.0.200.101 .

Si deve verificare se l'IP sorgente nel pacchetto viene convertito o meno in un ip pubblico.

Controllare se l'ip del PC è stato aggiunto al Source Network Address Translation (SNAT) del Network Address Translation (NAT).

2.2 Sangfor NGAF configurato in modalità Bridge mode

Se il firewall Sangfor NGAF è stato configurato in modalità Bridge e gli utenti non riescono ad accedere ad internet, suggerisco di abilitare il pass-through come descritto nei passaggi precedenti per verificare se vi sono policy che bloccano l'IP sorgente nella navigazione internet.

Se la rete locale ancora non riesce a navigare su internet dopo aver abilitato il pass-through, potete usare il metodo descritto prima per la cattura dei pacchetti per capire se arrivano i pacchetti del traffico al firewall NGAF. Se nell'interfaccia LAN del firewall non è pervenuto alcun pacchetto da parte del PC coinvolto, controllare se vi sono restrizioni Access Control List (ACL) sulla porta cui è collegato il PC sul switch core.

Se non riuscite a bypassare il firewall NGAF, controllare se non vi siano anomalie nel PC o nella rete locale.

*3. Attenzione

Tenere a mente che una volta abilitato il pass-through Layer 2 , il firewall lascia passare qualsiasi traffico venga effettuato.