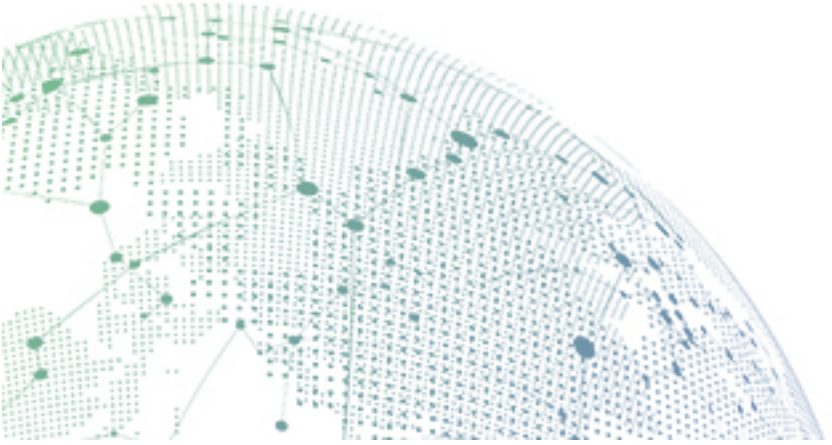
SANGFOR

NGAF

Route Mode Deployment with GRE Configuration

Version 8.0.5



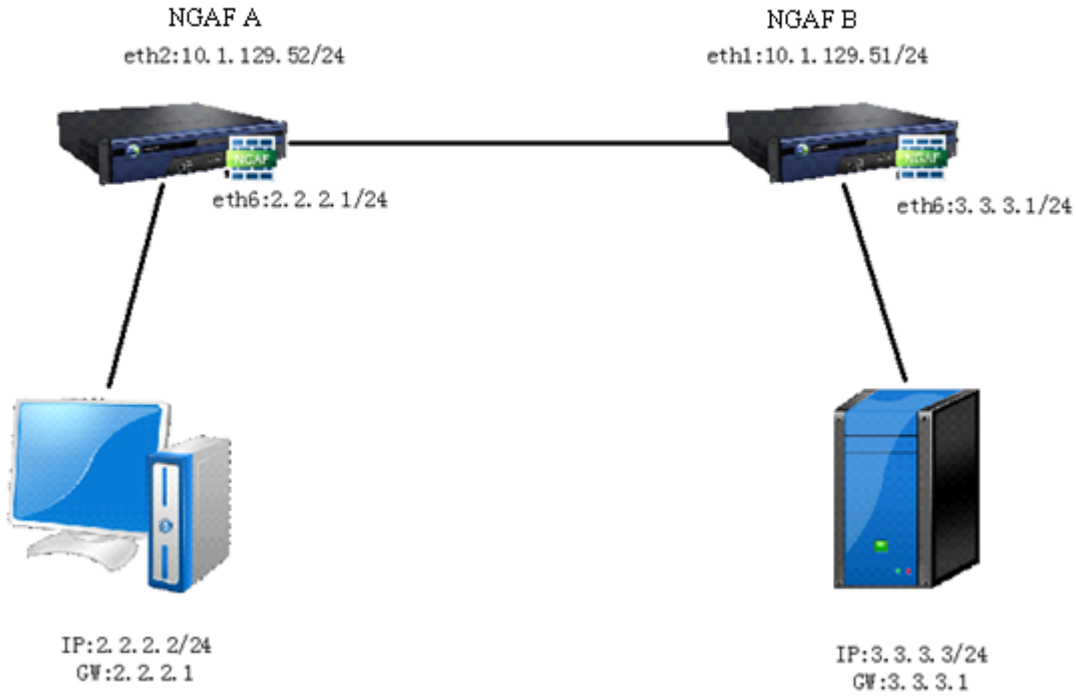
Change Log

Date	Change Description
Oct 22, 2018	Version 8.0.5 document release.

CONTENT

Chapter 1 Network Topology

Route mode deployment GRE environment as below:



Note that the NGAF must be able to communicate with each other.

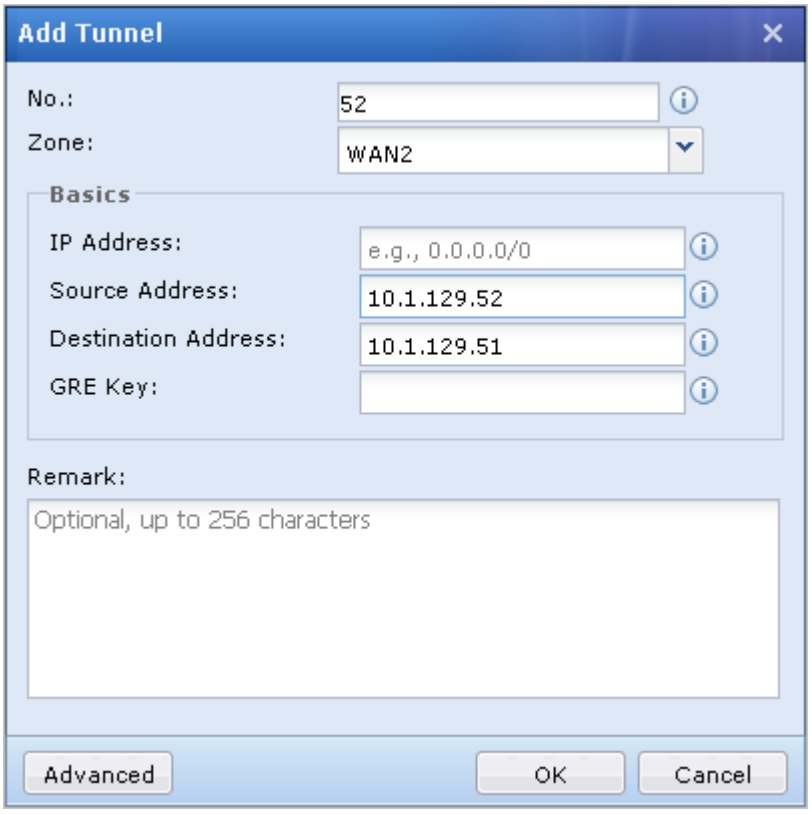
Chapter 2 NGAF Configuration

1. Basic network configuration: Make sure that the interfaces, default route and domain is configured correctly. Content security policies must be allow. Refer to the following link for route deployment:

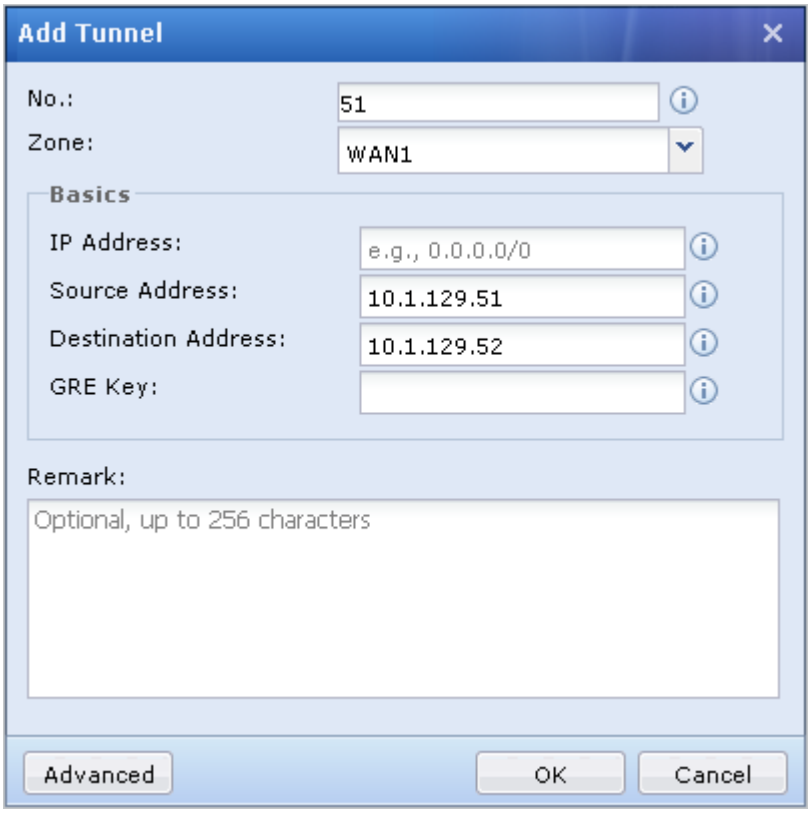
   http://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=354&highlight=

2. After completing the basic network configuration, the second step is configuring the GRE tunnel. Navigate to [Network] > [Interface] > [GRE Tunnel] to configure the GRE tunnel.

Firewall A:



Firewall B:



Note:

IP Address: GRE tunnel IP address, this IP must be a new IP and cannot conflict with the local or peer interface. Can be ignored in route mode deployment.

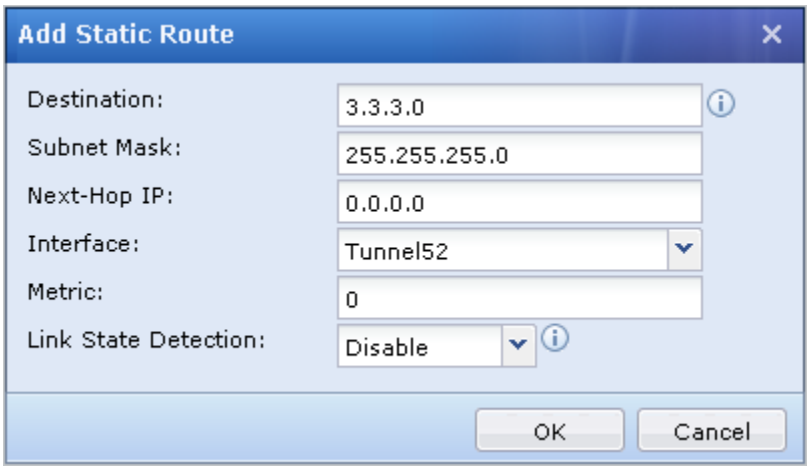
Source Address: Local egress WAN IP address

Destination Address: Opposite egree WAN IP address

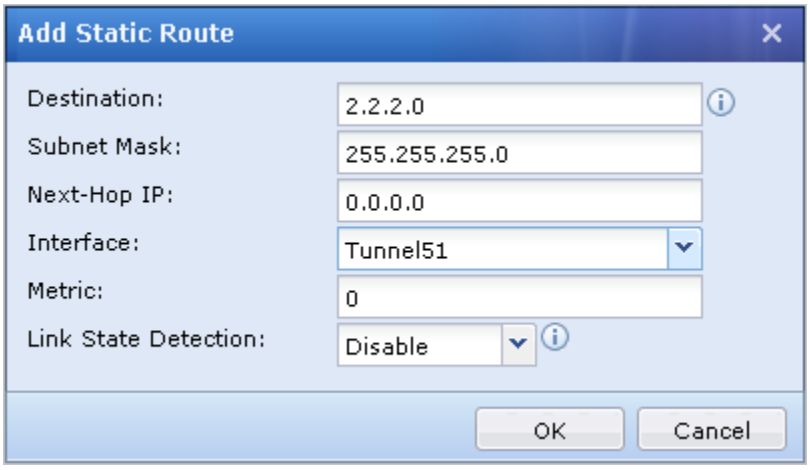
GRE Key: Both ends must be the same, can be ignored

3. Third step is to build a static route

Firewall A:



Firewall B:



Note:

Destination: Peer IP address accessed through tunnel

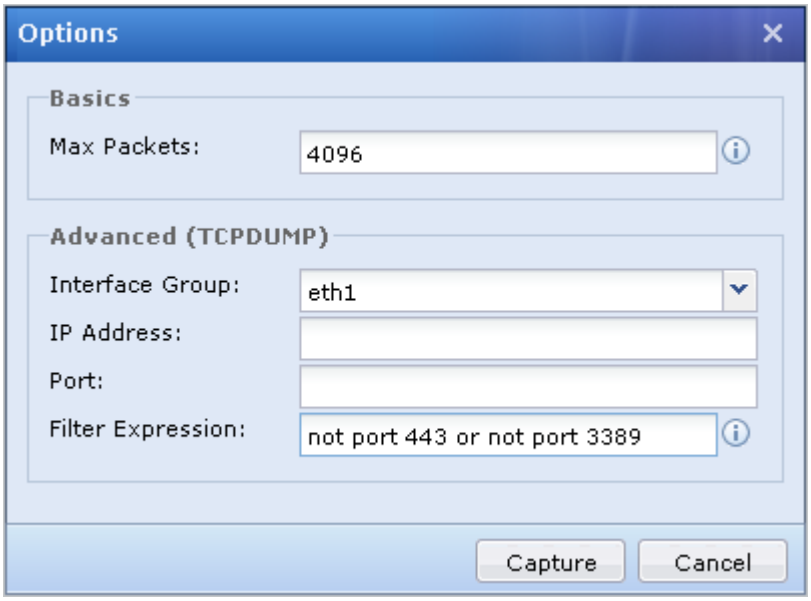
Subnet Mask: Subnet mask of the IP address

Next-Hop IP: 0.0.0.0

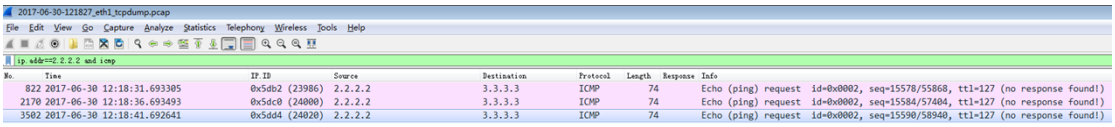
Interface: Select GRE tunnel interface

4. Testing:

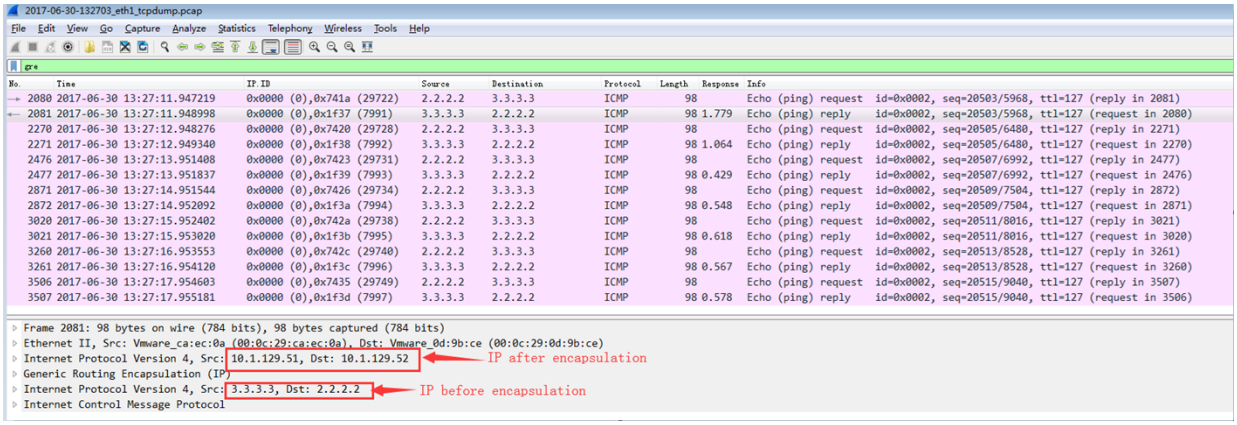
   1. Under the circumstances where GRE tunnel is not built and PC is unable to ping to server ip 3.3.3.3. First, under [System] > [Troubleshooting] > [Capture Packets], setup the parameters to capture packet, then ping 3.3.3.3 using the PC, as shown below:



   2. In the data packet, we can see that the eth1 source ip 2.2.2.2 has not go through address translation. The request packet is sent to 3.3.3.3 without returning the packet, as shown below:



   3. Under the circumstances where GRE tunnel is built and PC is able to ping to server ip 3.3.3.3. Capture packet according to the parameters on top, then in the data packet, we can see that the original source ip is encapsulated with the ip address of the external network interface, as shown below:



Chapter 3 Precaution

1) Security functionality checking must configure with zone, zone of the egress port; for those who does not requires seucurity functionalities, there is no needs to
2) It is not necessary to configure IP address for GRE tunnel.
3) The source address and destination address correspond to the egress interface IP address.
4) The GRE keys on both ends of the GRE tunnel must be the same, not necessary to configure.
5) Configure static route to import data into the GRE tunnel. Select the GRE tunnel interface as static route interface, next hop IP address is 0.0.0.0.