SANGFOR

NGAF
GRE over IPsec VPN Configuration Guide

Version 8.0.8

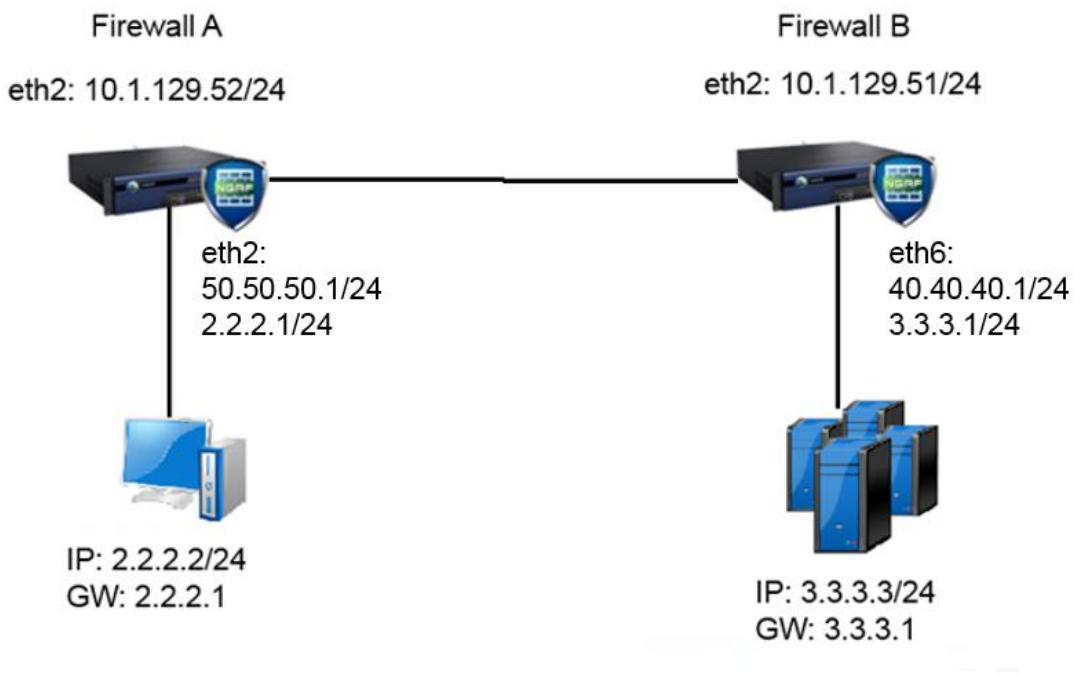
Change Log

Date	Change Description
Nov 27,2019	GRE over IPsec VPN Configuration Guide

CONTENT

Chapter 1 Application Scenario

GRE over IPsec VPN, as shown in below:



Requirement:

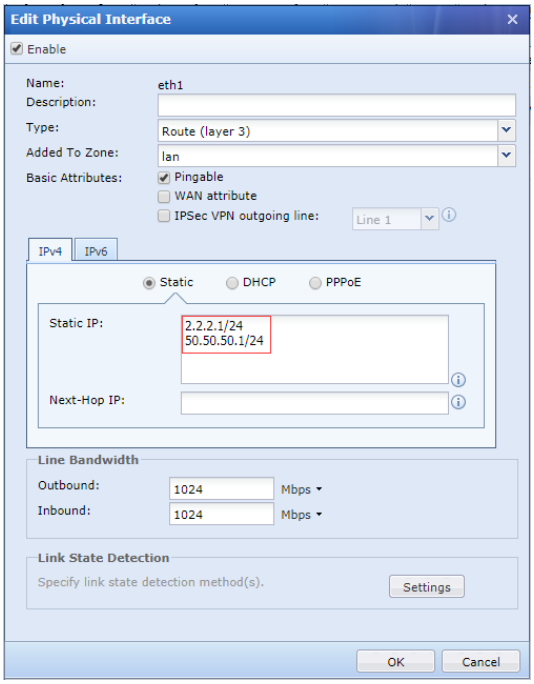
1. The version of NGAF must at least 7.1.
2. NGAF is able to communicate with peer.
3. Both end need to use IPsec VPN to establish connection.
4. In VPN LAN interface a different network segment IP should be added on top of the existing gateway IP. The new IP is used to troubleshoot the effect of VPN inbound policy and outbound policy which directly allow LAN IP communicate via VPN tunnel.

Chapter 2 Configuration Method

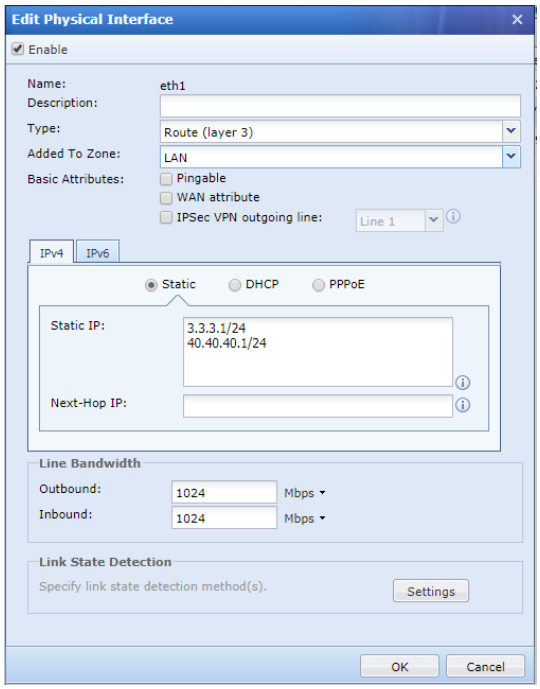
1. The basic network configuration needs to ensure that the interface, default route and zone is configured correctly. The content security policy should be allow all. The details may refer to "SANGFOR_NGAF_V8.0.5_Route Mode Deployment Guide", as shown in below: http://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=975

   An additional network segment was added in NGAF LAN interface, Firewall A add 50.50.50.1, Firewall B add 40.40.40.1

   Firewall A



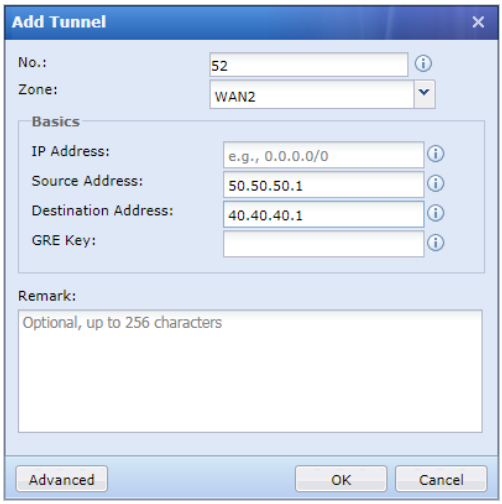
Firewall B



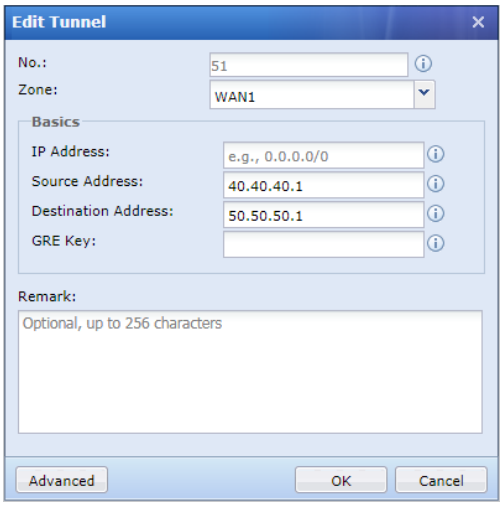
Note: Except NAT does not need to configure, other configuration may refer to the file provided.

2. After the basic network configuration has been done, then in Network > Interface > GRE Tunnel to configure GRE interface, as shown:

Firewall A



Firewall B



Note:

IP address: GRE interface IP address, this IP is a new IP address, the local PC and peer interface IP should not have IP conflict. The configuration of OSPF scenario must be configure.

Source IP address: Local WAN interface IP address

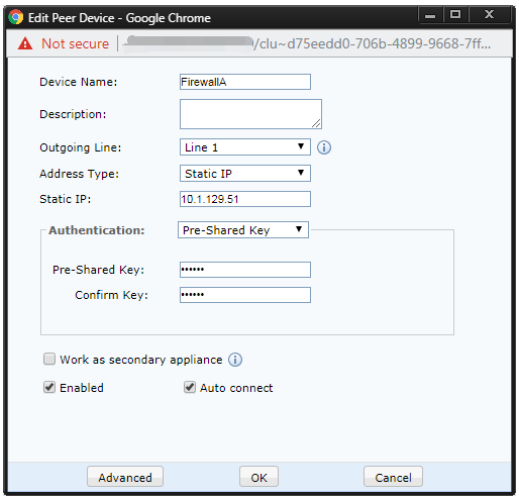
Destination IP address: Peer WAN interface IP address

GRE Key: Must be same on both side, it can be not configured.

3. Configure IPsec VPN, by using the interface newly add IP address to build the CPN connection, the detail of the configuration as shown:

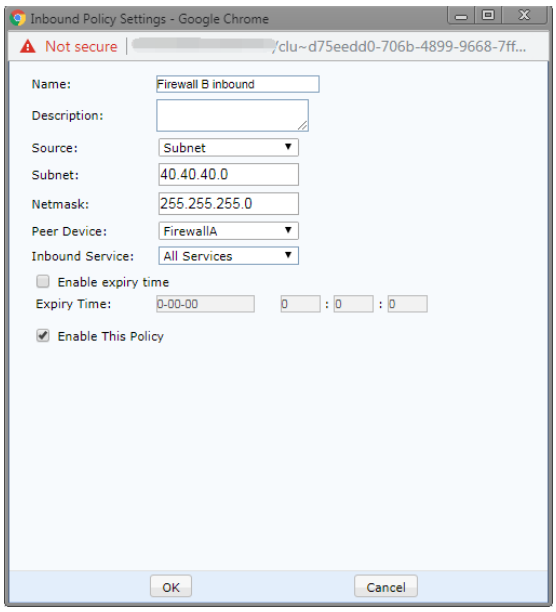
   Firewall A

   Phase 1 configuration:

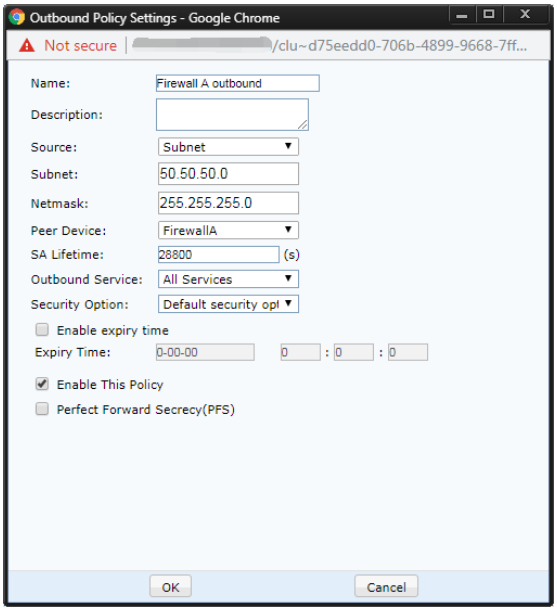


Phase 2 configuration:

Inbound Policy:

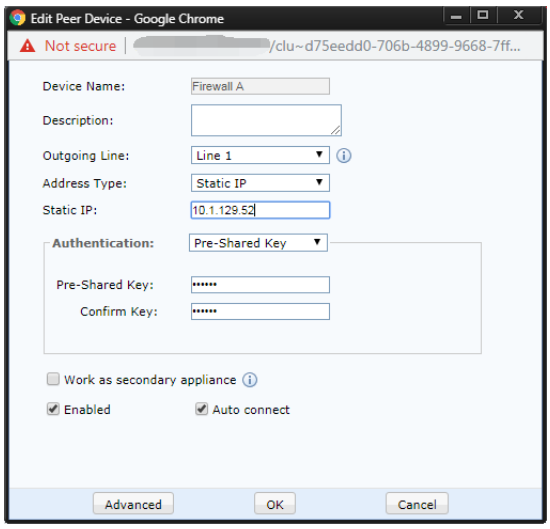


Outbound Policy:



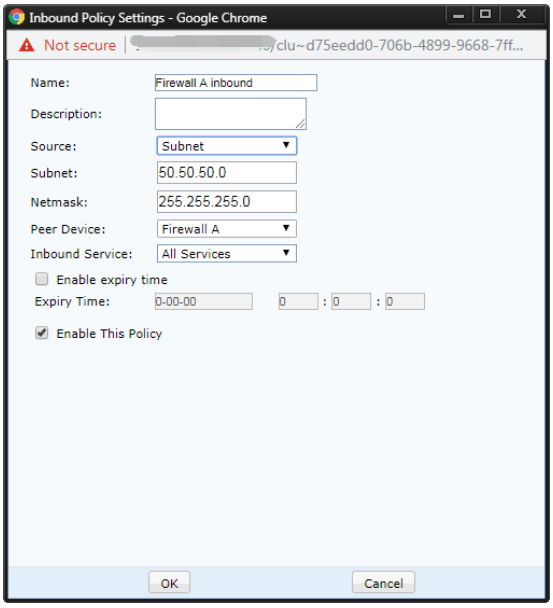
Firewall B

Phase 1 configuration:

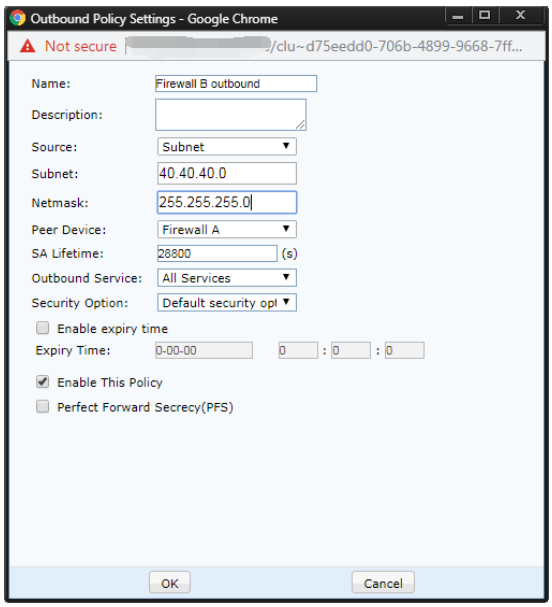


Phase 2 configuration:

Inbound policy:

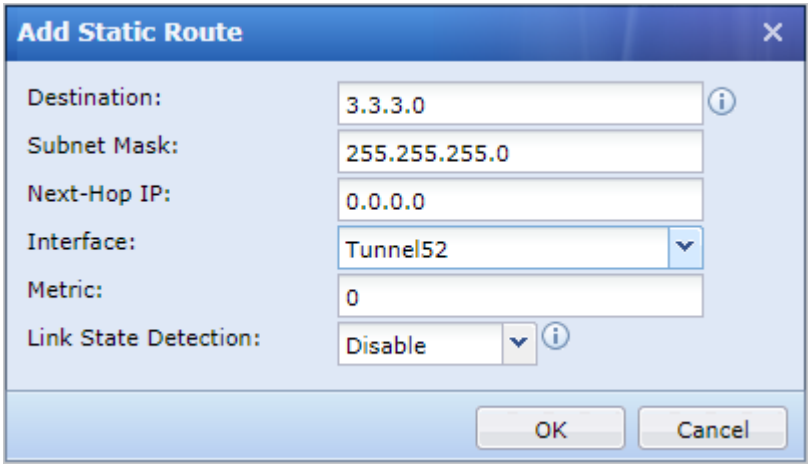


Outbound policy:

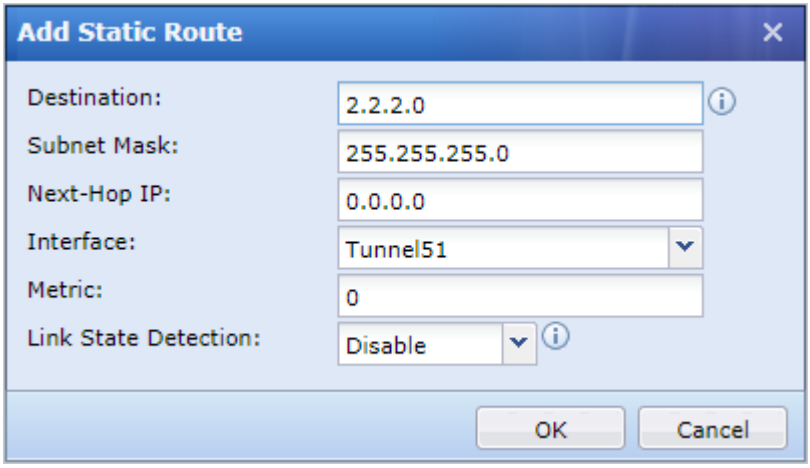


4. Configure a static route that will route the packet into GRE tunnel, as shown in below:

Firewall A:



Firewall B:



As the VPN tunnel has been encrypted, therefore if the packet is capture from WAN interface is not able to capture GRE encapsulated packet. But the GRE tunnel in this testing environment must be build up, then LAN PC and server IP is able to ping each other. This is because VPN inbound and outbound policy does not contain LAN PC and server IP, PC's ping packet is unable to enter VPN tunnel. Therefore, if there is any misconfigured, the packet will not enter GRE tunnel, PC is not able to ping server.

Chapter 3 Precautions

1. In VPN LAN interface a different network segment IP should be added on top of the existing gateway IP. The newly added IP will act as the VPN route address.
2. Need to configure a static route to let the packet go through GRE tunnel. GRE tunnel interface will be choose as the static route interface, next-hop IP will be 0.0.0.0
3. The VPN service need to be enabled in **Network** > **IPsec VPN** > **Status**.

SANGFOR