



SANGFOR



NGAF

GRE over IPsec VPN Configuration Guide

Version 8.0.8



Change Log

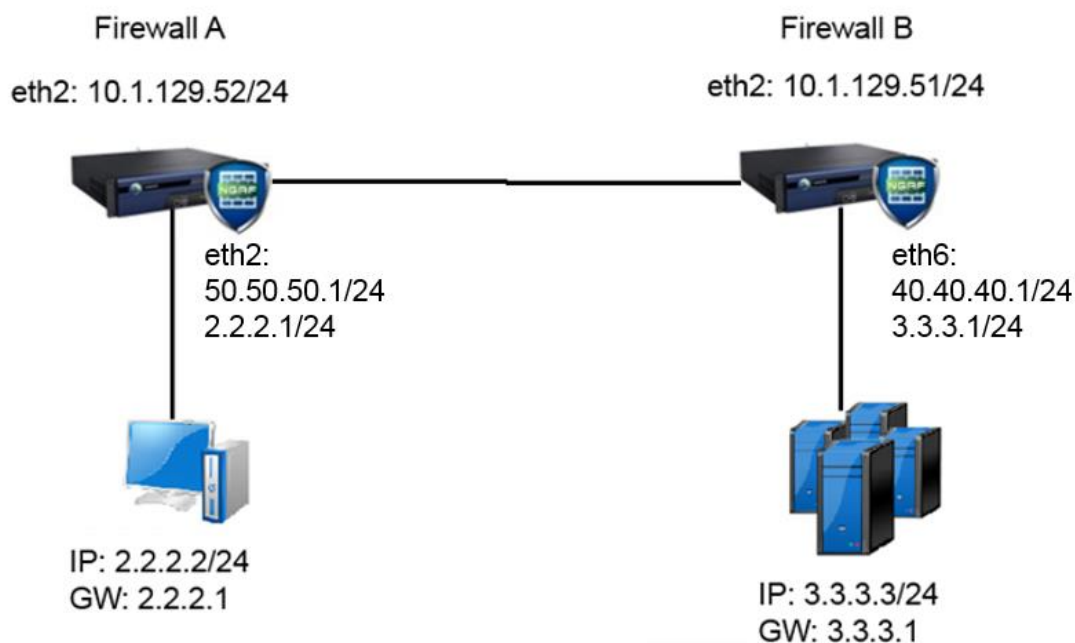
Date	Change Description
Nov 27,2019	GRE over IPsec VPN Configuration Guide

CONTENT

Chapter 1 Application Scenario	1
Chapter 2 Configuration Method.....	2
Chapter 3 Precautions	8

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

The screenshot shows the 'Edit Physical Interface' configuration window for Firewall A. The interface is named 'eth1' and is configured as a 'Route (layer 3)' type, added to the 'lan' zone. Basic attributes include 'Pingable' checked, 'WAN attribute' unchecked, and 'IPSec VPN outgoing line' set to 'Line 1'. The 'IPv4' tab is selected, showing 'Static' IP configuration with two addresses: '2.2.2.1/24' and '50.50.50.1/24'. The 'Line Bandwidth' section shows 'Outbound' and 'Inbound' both set to '1024' Mbps. The 'Link State Detection' section is at the bottom with a 'Settings' button. The window has 'OK' and 'Cancel' buttons at the bottom right.

Firewall B

The 'Edit Physical Interface' window shows the configuration for interface 'eth1'. The 'Enable' checkbox is checked. The 'Name' is 'eth1'. The 'Type' is set to 'Route (layer 3)'. The 'Added To Zone' is 'LAN'. Under 'Basic Attributes', 'Pingable' is checked, while 'WAN attribute' and 'IPSec VPN outgoing line' are unchecked. The 'IPSec VPN outgoing line' dropdown is set to 'Line 1'. The 'IPv4' tab is selected, showing 'Static' as the IP configuration mode. The 'Static IP' field contains '3.3.3.1/24' and '40.40.40.1/24'. The 'Next-Hop IP' field is empty. The 'Line Bandwidth' section shows 'Outbound' and 'Inbound' both set to '1024' Mbps. The 'Link State Detection' section has a 'Settings' button. At the bottom are 'OK' and 'Cancel' buttons.

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

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

Firewall A

The 'Add Tunnel' window shows the configuration for a new tunnel. The 'No.' is '52'. The 'Zone' is 'WAN2'. Under the 'Basics' section, 'IP Address' is 'e.g., 0.0.0.0/0', 'Source Address' is '50.50.50.1', 'Destination Address' is '40.40.40.1', and 'GRE Key' is empty. The 'Remark' field contains the text 'Optional, up to 256 characters'. At the bottom are 'Advanced', 'OK', and 'Cancel' buttons.

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:

Inbound Policy Settings - Google Chrome

Not secure | /clu~d75eadd0-706b-4899-9668-7ff...

Name: Firewall B inbound

Description:

Source: Subnet

Subnet: 40.40.40.0

Netmask: 255.255.255.0

Peer Device: FirewallA

Inbound Service: All Services

☐ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☒ Enable This Policy

OK Cancel

Outbound Policy:

Outbound Policy Settings - Google Chrome

Not secure | /clu~d75eadd0-706b-4899-9668-7ff...

Name: Firewall A outbound

Description:

Source: Subnet

Subnet: 50.50.50.0

Netmask: 255.255.255.0

Peer Device: FirewallA

SA Lifetime: 28800 (s)

Outbound Service: All Services

Security Option: Default security opt

☐ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☒ Enable This Policy

☐ Perfect Forward Secrecy(PFS)

OK Cancel

Firewall B

Phase 1 configuration:

Edit Peer Device - Google Chrome

Not secure | /clu~d75eedd0-706b-4899-9668-7ff...

Device Name: Firewall A

Description:

Outgoing Line: Line 1

Address Type: Static IP

Static IP: 10.1.129.52

Authentication: Pre-Shared Key

Pre-Shared Key: *****

Confirm Key: *****

☐ Work as secondary appliance

☒ Enabled ☒ Auto connect

Advanced OK Cancel

Phase 2 configuration:

Inbound policy:

Inbound Policy Settings - Google Chrome

Not secure | /clu~d75eedd0-706b-4899-9668-7ff...

Name: Firewall A inbound

Description:

Source: Subnet

Subnet: 50.50.50.0

Netmask: 255.255.255.0

Peer Device: Firewall A

Inbound Service: All Services

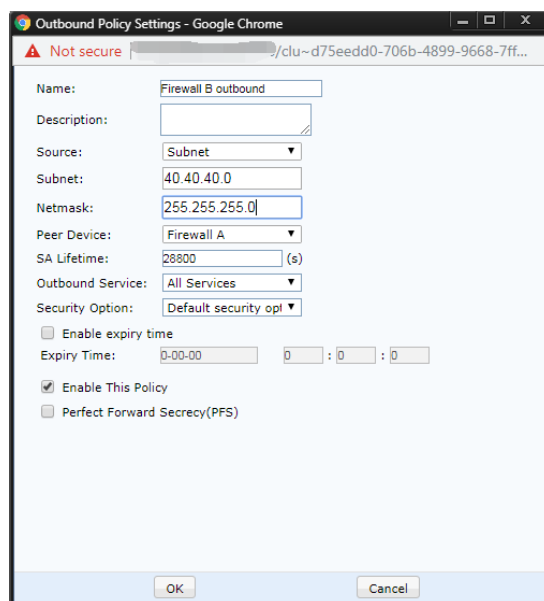
☐ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☒ Enable This Policy

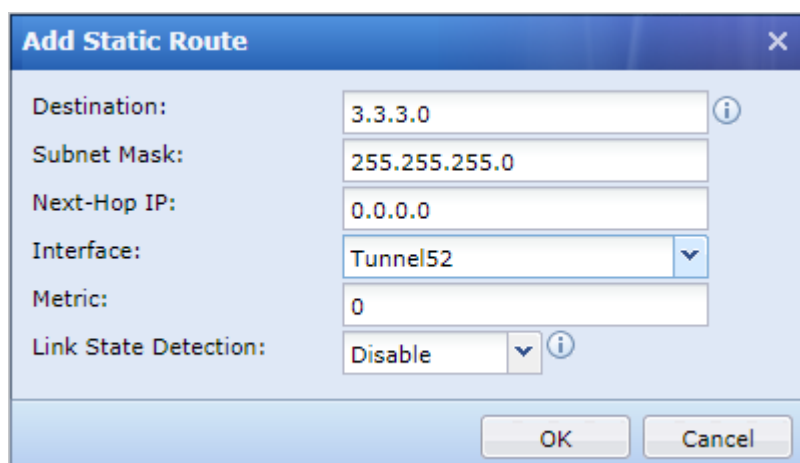
OK Cancel

Outbound policy:

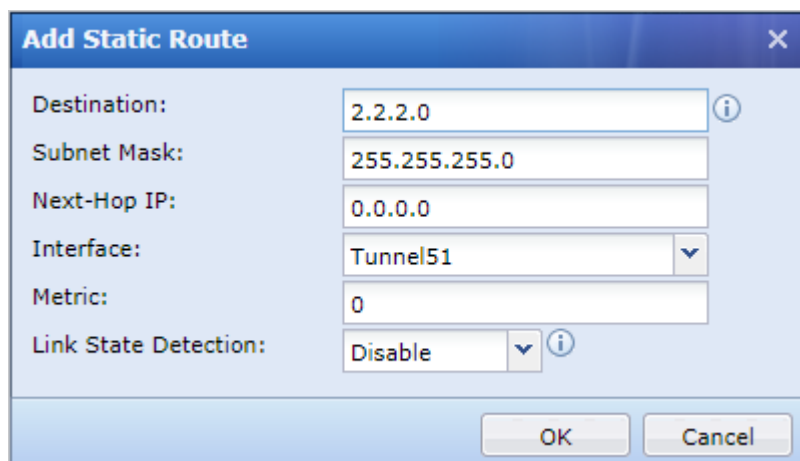


4. Configure a static route that will route the packet into GRE tunnel, as shown in below:

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

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc