SANGFOR

# NGAF

## IPSec VPN Configuration in Mixed Mode

Version 8.0.10

# Contents

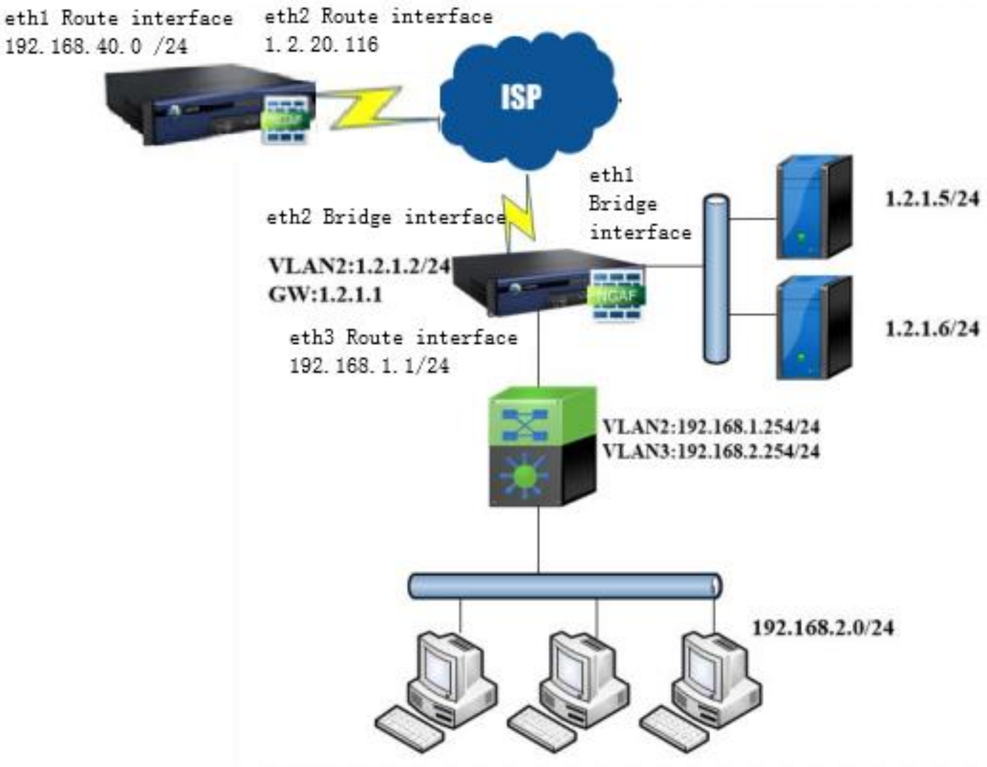
# 1. Function Introduction

As a router, it implements functions such as route forwarding and proxy internet access. In addition, some data is transparently passed through the device.

The full name of VPN is Virtual Private Network. VPN is defined as establishing a temporary and secure connection over a public network (normally through Internet), a secure and stable tunnel through a chaotic public network. By using this tunnel, you can encrypt data several times to achieve the purpose of using Internet safely. A virtual private network is an extension of an intranet. Virtual private networks help to remote users, corporate branches, business partners, and suppliers establish trusted and secure connections to the company's intranet for secure extranet virtual private networks that connect to business partners and users. VPN mainly uses tunnel technology, encryption technology, decryption technology, key management technology and user and device identity authentication technology.

# 2. Application Scenarios

The Sangfor NGAF device is deployed in the mixed mode on the public network egress, as an agent to bring intranet to Internet. In addition, the intranet needs to provide users to access through public network, and each server is assigned a public IP. Users can access the server group directly through the public IP without configure NAT. Users want to build a VPN to Branch LAN users able to access to our server.



# 3. Description of necessary conditions

1 NGAF device, PC and Server that configured public IP.

# 4. Configuration Ideas

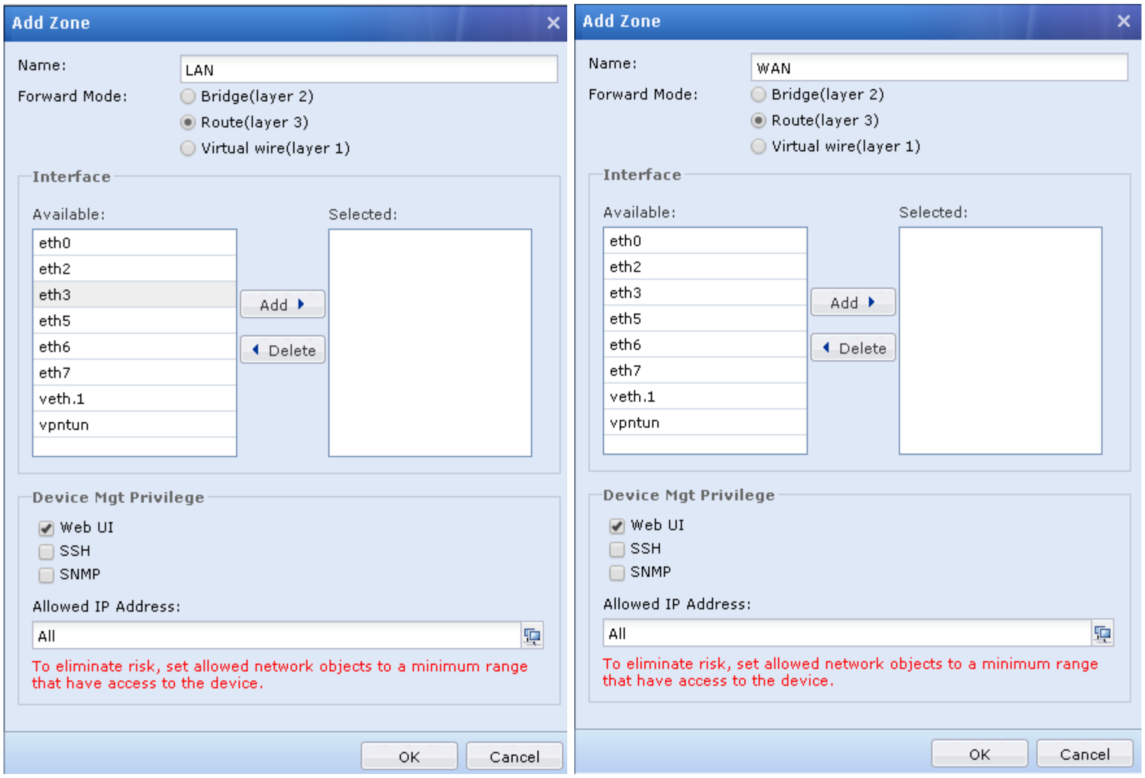
1. Interface/zone configuration.
2. Routing configuration.
3. SNAT configuration.
4. Application Control configuration.
5. VPN configuration

# 5. Configuration and screenshot

## 5.1 Interface/zone configuration

### 5.1.1 Zone configuration:

1. Go to **Network** > **Interfaces** > **Zone** > **Add**, add zone as figure below:



Add Zone

Name: LAN

Forward Mode: ○ Bridge(layer 2) ● Route(layer 3) ○ Virtual wire(layer 1)

Interface

Available: eth0, eth2, eth3, eth5, eth6, eth7, veth.1, vpntun

Selected:

Device Mgt Privilege

☑ Web UI
□ SSH
□ SNMP

Allowed IP Address: All

To eliminate risk, set allowed network objects to a minimum range that have access to the device.

Add Zone

Name: WAN

Forward Mode: ○ Bridge(layer 2) ● Route(layer 3) ○ Virtual wire(layer 1)

Interface

Available: eth0, eth2, eth3, eth5, eth6, eth7, veth.1, vpntun

Selected:

Device Mgt Privilege

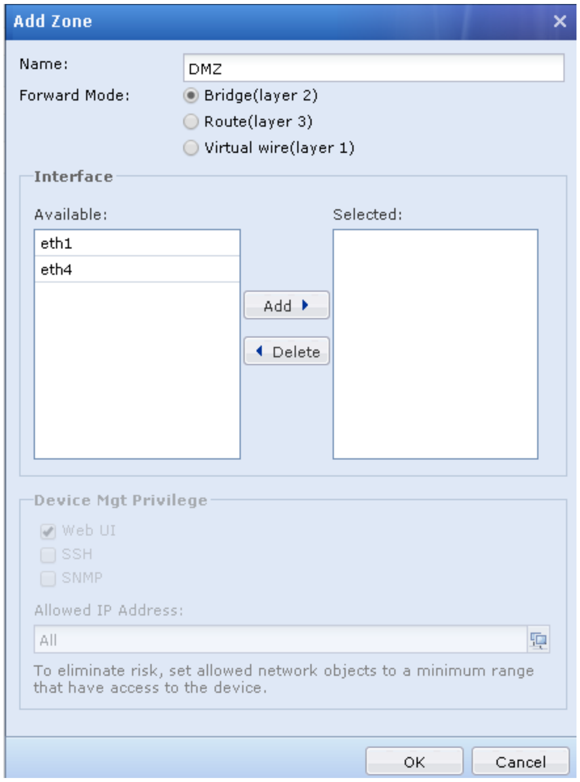
☑ Web UI
□ SSH
□ SNMP

Allowed IP Address: All

To eliminate risk, set allowed network objects to a minimum range that have access to the device.

**Zone name**: LAN/WAN

**Forward mode**: Route (layer3)



Add Zone

Name: DMZ

Forward Mode: ● Bridge(layer 2) ○ Route(layer 3) ○ Virtual wire(layer 1)

Interface

Available: eth1, eth4

Selected:

Device Mgt Privilege

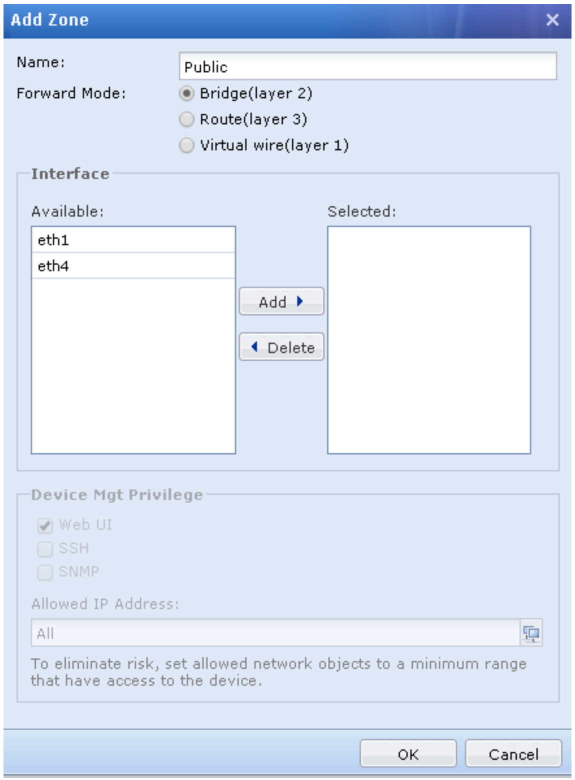
☑ Web UI

□ SSH

□ SNMP

Allowed IP Address: All

To eliminate risk, set allowed network objects to a minimum range that have access to the device.



Add Zone

Name: Public

Forward Mode: ● Bridge(layer 2) ○ Route(layer 3) ○ Virtual wire(layer 1)

Interface

Available: eth1, eth4

Selected:

Device Mgt Privilege

☑ Web UI

□ SSH

□ SNMP

Allowed IP Address: All

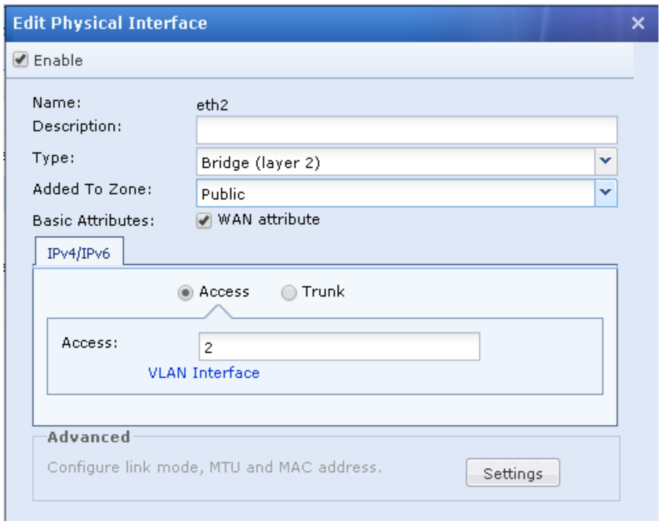
To eliminate risk, set allowed network objects to a minimum range that have access to the device.

**Zone name**: DMZ / Public

**Forward mode**: Bridge (layer 2)

## 5.1.2 Interface configuration

1. Go to **Network** > **Interfaces** > **Physical Interface,** choose the interface that need to configure as Public interface:



Edit Physical Interface

☑ Enable

Name: eth2

Description:

Type: Bridge (layer 2)

Added To Zone: Public

Basic Attributes: ☑ WAN attribute

IPv4/IPv6

● Access ○ Trunk

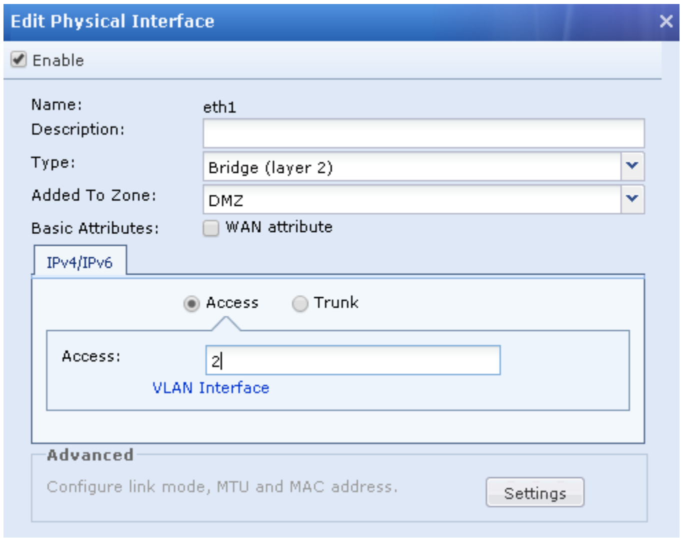
Access: 2

VLAN Interface

Advanced

Configure link mode, MTU and MAC address.

2. Go to **Network** > **Interfaces** > **Physical interface**, choose the interface that need to configure as **DMZ interface**:



Edit Physical Interface

☑ Enable

Name: eth1

Description:

Type: Bridge (layer 2)

Added To Zone: DMZ

Basic Attributes: □ WAN attribute

IPv4/IPv6

● Access ○ Trunk

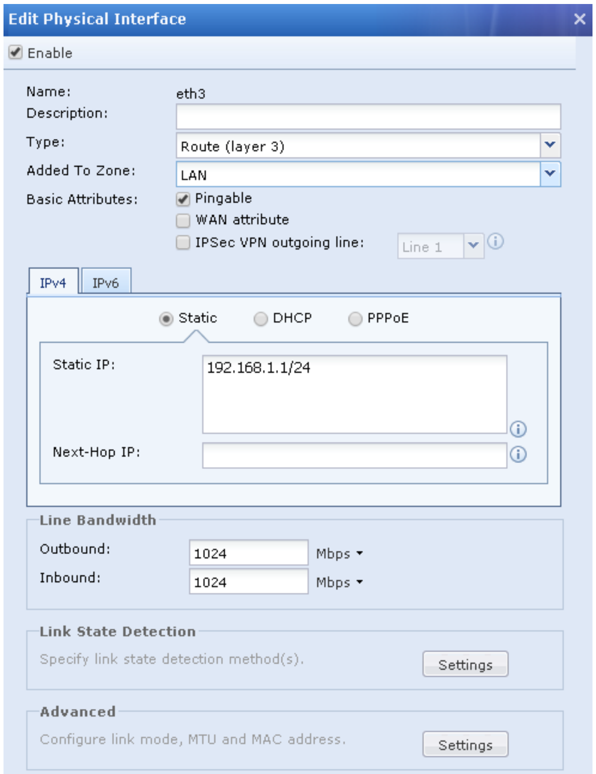
Access: 2

VLAN Interface

Advanced

Configure link mode, MTU and MAC address.

3. Go to **Network** > **Interfaces** > **Physical Interface**, choose the inter face that need to configure as LAN interface:



Edit Physical Interface

☑ Enable

Name: eth3

Description:

Type: Route (layer 3)

Added To Zone: LAN

Basic Attributes: ☑ Pingable

□ WAN attribute

□ IPSec VPN outgoing line: Line 1

IPv4 IPv6

● Static ○ DHCP ○ PPPoE

Static IP: 192.168.1.1/24

Next-Hop IP:

Line Bandwidth

Outbound: 1024 Mbps

Inbound: 1024 Mbps

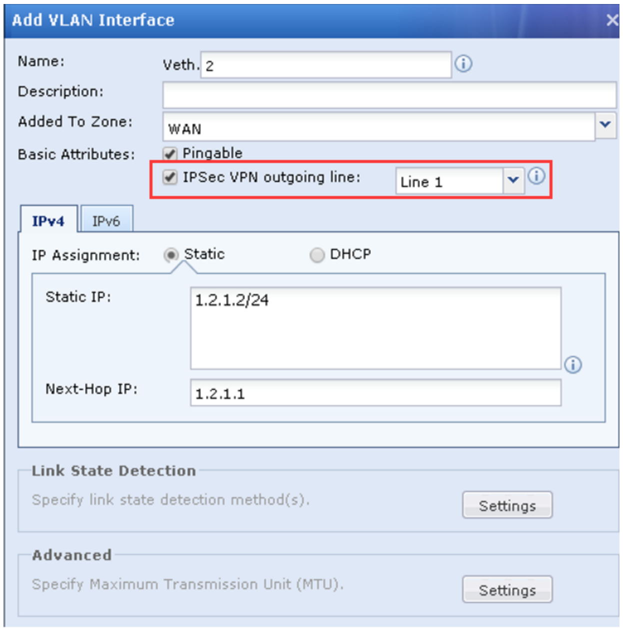
Link State Detection

Specify link state detection method(s).

Advanced

Configure link mode, MTU and MAC address.

4. Go to **Network** > **Interfaces** > **VLAN Interface**, add a new vlan2 and configure as WAN interface as figure below:



Add VLAN Interface

Name: Veth. 2

Description:

Added To Zone: WAN

Basic Attributes: ☑ Pingable

☑ IPSec VPN outgoing line: Line 1

IP Assignment: ● Static ○ DHCP

Static IP: 1.2.1.2/24

Next-Hop IP: 1.2.1.1

Link State Detection

Specify link state detection method(s). Settings

Advanced

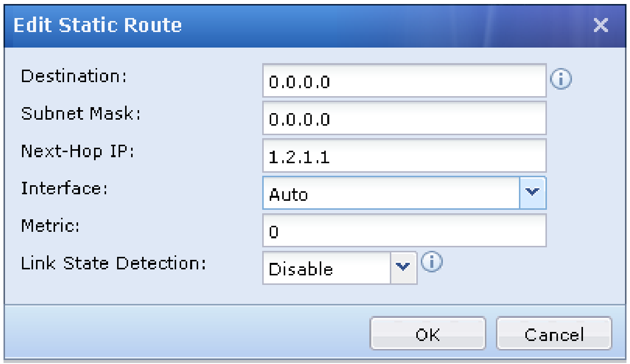
Specify Maximum Transmission Unit (MTU). Settings

**Link State Detection:** Used to detect the quality of the link. The link detection method includes DNS resolve and PING. If you select DNS resolve, you need to configure the DNS server and resolve the domain name. If PING detection is enabled, fill in the PING detection IP address.

## 5.2 Routing Configuration

1. Go to **Network** > **Routing** > **Static route** > **Add** > **Static Route**, as figure below:

**Default route**



Edit Static Route

Destination: 0.0.0.0

Subnet Mask: 0.0.0.0

Next-Hop IP: 1.2.1.1

Interface: Auto

Metric: 0

Link State Detection: Disable

**Destination:** 0.0.0.0, default route should fill 0.0.0.0.

**Subnet mask:** 0.0.0.0, default route should fill 0.0.0.0.

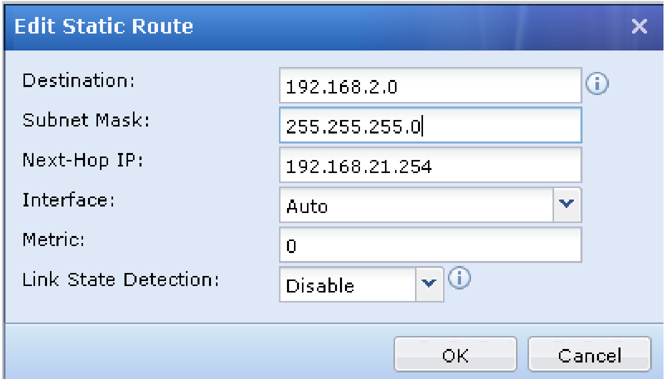
**Next-Hop IP:** Device’s gateway IP, example 1.2.1.1.

**Interface:** Can choose **Auto**, or specific an interface.

**Metric:** Default is 0, the smallest value the highest priority

**Note**: If the device have few WAN, it is required to configure **Policy-Based Route.**

**Return route**



Edit Static Route

Destination: 192.168.2.0

Subnet Mask: 255.255.255.0

Next-Hop IP: 192.168.21.254

Interface: Auto

Metric: 0

Link State Detection: Disable

**Destination:** 192.168.2.0, return route for LAN.

**Subnet mask:** 255.255.255.0, LAN subnet mask.

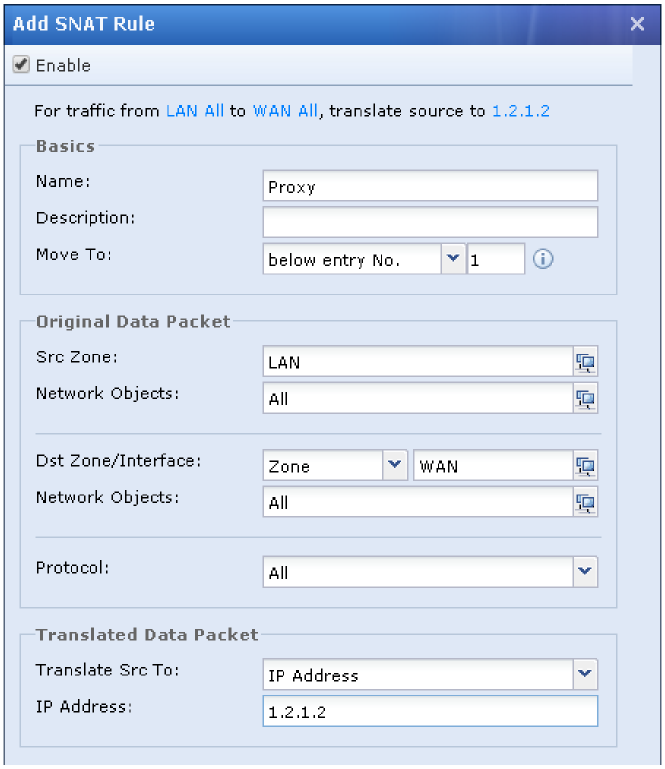
**Next-Hop IP:** Device's gateway, example 192.168.1.254.

**Interface:** Can choose **Auto**, or specific an interface.

**Metric:** Default is 0, the smallest value the highest priority.

## 5.3 SNAT configuration

1. Go to **Policies** > **NAT** > **Add** > **Source NAT**, add the SNAT as figure below:



Add SNAT Rule

☑ Enable

For traffic from LAN All to WAN All, translate source to 1.2.1.2

Basics

Name: Proxy

Description:

Move To: below entry No. 1

Original Data Packet

Src Zone: LAN

Network Objects: All

Dst Zone/Interface: Zone WAN

Network Objects: All

Protocol: All

Translated Data Packet

Translate Src To: IP Address

IP Address: 1.2.1.2

**Name:** Proxy (Define rule name).

**Src Zone:** LAN (Layer 3 zone).

**Network Objects**: All, or specific private network.

**Dst Zone/Interface**: WAN (Layer 3 zone).

**Network Objects**: All.

**Protocol:** If you want to configure SNAT for specific protocol, source port destination port, then you can change this options. In this case we don't need, so we choose **All** for protocol.

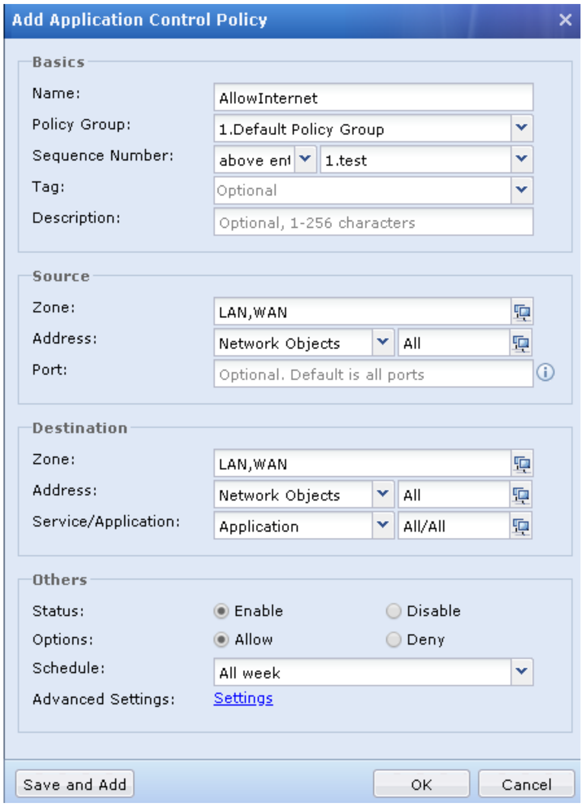
**Translate Src To:** IP Address, specific IP.

IP Address: 1.2.1.2

## 5.4 Application Control configuration

1. Go to **Policies** > **Access Control** > **Application Control** > **Add,** add the application control as figure below:

Allow LAN users access Internet:



Add Application Control Policy

Basics

Name: AllowInternet

Policy Group: 1.Default Policy Group

Sequence Number: above ent 1.test

Tag: Optional

Description: Optional, 1-256 characters

Source

Zone: LAN,WAN

Address: Network Objects All

Port: Optional. Default is all ports

Destination

Zone: LAN,WAN

Address: Network Objects All

Service/Application: Application All/All

Others

Status: ● Enable ○ Disable

Options: ● Allow ○ Deny

Schedule: All week

Advanced Settings: Settings

**Name:** AllowInternet (Define rule name)

**Address:** In **Network Objects** choose **All.** Choose source users or IP that need application control.

**Zone (Source):** LAN and WAN (Layer 3 zone). Choose the source zone that need to do application control.

**Port:** All. Enter port number if need to specific a source port.

**Zone (Destination):** LAN and WAN (Layer 3 zone). Choose the destination zone that need to do application control.

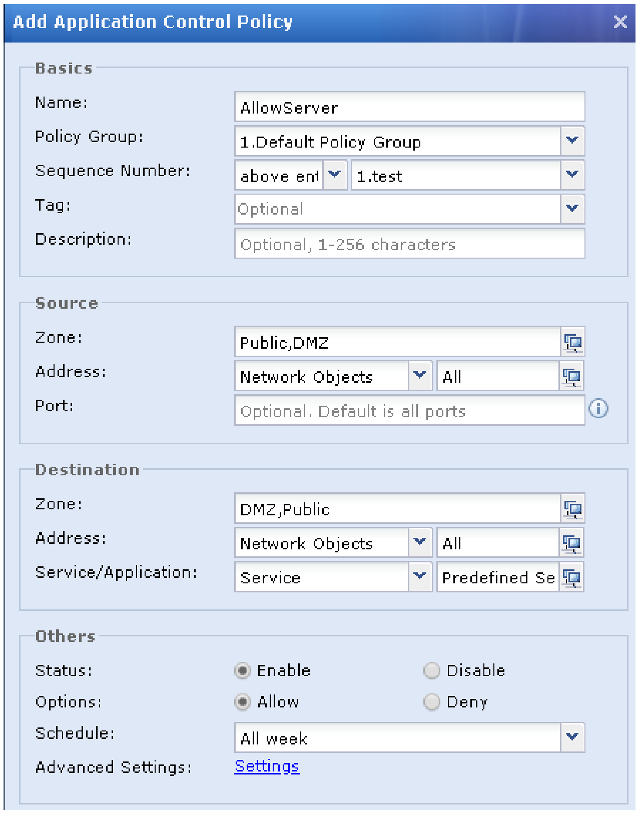
**Address:** In **Network Objects** choose **All.** Choose destination users or IP that need application control.

**Service/Application:** Application. Choose the application that need to do application control.

**Schedule:** All week. Filter rules take effect within the specified time.

**Options**: Allow.

**Allow WAN users access Servers:**



Add Application Control Policy

Basics

Name: AllowServer

Policy Group: 1.Default Policy Group

Sequence Number: above enl 1.test

Tag: Optional

Description: Optional, 1-256 characters

Source

Zone: Public,DMZ

Address: Network Objects All

Port: Optional. Default is all ports

Destination

Zone: DMZ,Public

Address: Network Objects All

Service/Application: Service Predefined Se

Others

Status: ● Enable ○ Disable

Options: ● Allow ○ Deny

Schedule: All week

Advanced Settings: Settings

**Name:** AllowServer (Define rule name)

**Zone (Source):** Public and DMZ (Layer 2 zone). Choose the source zone that need to do application control.

**Address:** In **Network Objects**, choose **All**. Choose source users or IP that need to do application control.

**Port:** All. Enter port number if need to specific a source port.

**Zone (Destination):** Public and DMZ (Layer 2 zone). Choose the destination zone that need to do application control.

**Address:** In **Network Objects,** choose **All**. Choose destination users or IP that need to do application control.

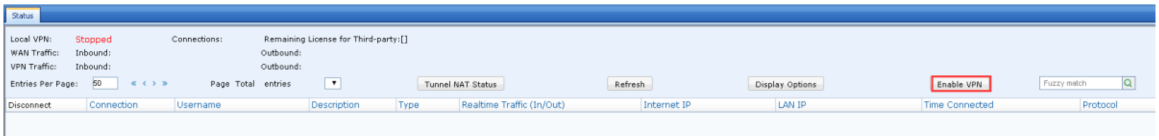
**Service/Application:** In **Service**, choose **any**. Choose the service that needs to be controlled

**Options**: Allow.

**Schedule:** All week. Filter rules take effect within the specified time

# 5.5 VPN configuration

1. Go to **Network** > **IPSecVPN** > **Status,** enable the VPN service as figure below:



Local VPN: Stopped

Connections:

Remaining License for Third-party:[]

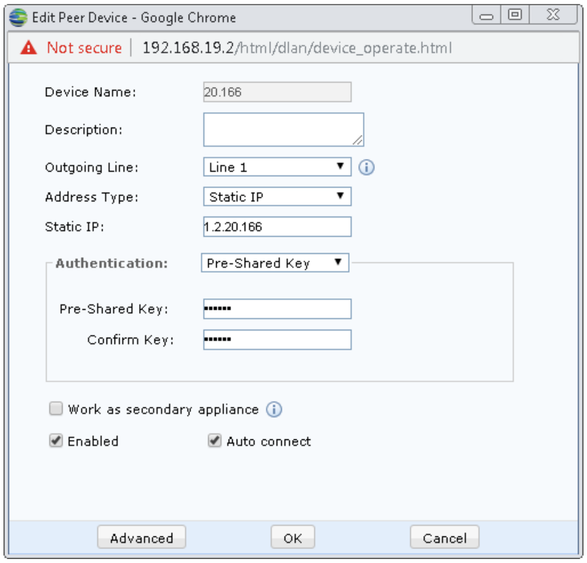
WAN Traffic: Inbound: Outbound:

VPN Traffic: Inbound: Outbound:

Entries Per Page: 50 Page Total entries

| Disconnect | Connection | Username | Description | Type | Realtime Traffic (In/Out) | Internet IP | LAN IP | Time Connected | Protocol |
|---|---|---|---|---|---|---|---|---|---|

2. Go to **Network** > **IPSecVPN** > **IPSec VPN**> **Phase I,** you can refer to figures below:



Edit Peer Device - Google Chrome
Not secure | 192.168.19.2/html/dlan/device_operate.html
Advanced
OK
Cancel

Device Name: 20.166

Description:

Outgoing Line: Line 1

Address Type: Static IP

Static IP: 1.2.20.166

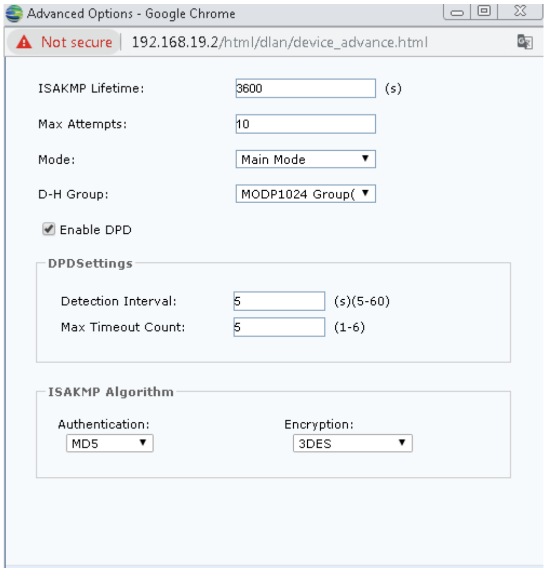
Authentication: Pre-Shared Key

Pre-Shared Key: ••••••

Confirm Key: ••••••

□ Work as secondary appliance

☑ Enabled ☑ Auto connect



Advanced Options - Google Chrome
Not secure | 192.168.19.2/html/dlan/device_advance.html

ISAKMP Lifetime: 3600 (s)

Max Attempts: 10

Mode: Main Mode

D-H Group: MODP1024 Group(

☑ Enable DPD

DPDSettings

Detection Interval: 5 (s)(5-60)

Max Timeout Count: 5 (1-6)

ISAKMP Algorithm

Authentication: MD5

Encryption: 3DES

**Device Name:** Peer device's name.

**Outgoing Line:** Choose the outgoing line that selected on WAN interface.

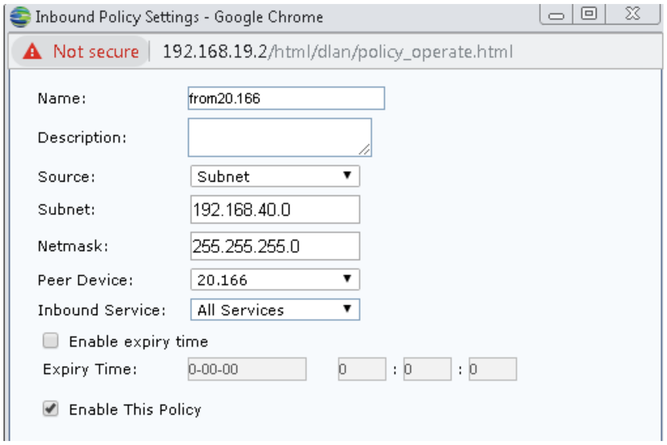
**Address Type:** Choose Static IP.

**Static IP:** Fill the public IP of peer device

**Pre-Shared Key:** Fill a shared key, must make sure noth device is use the same share key.

**Note:** In this scenario, we use the default parameters on **Advanced** options. You can change the parameter due to your requirement, but need to make sure both device is using the same value.

2. Go to **Network** > **IPSecVPN** > **IPSec VPN**> **Phase II,** add the Inbound and Outbound policy as figures below:



Inbound Policy Settings - Google Chrome

Not secure | 192.168.19.2/html/dlan/policy_operate.html

Name: from20.166

Description:

Source: Subnet

Subnet: 192.168.40.0

Netmask: 255.255.255.0

Peer Device: 20.166

Inbound Service: All Services

□ Enable expiry time

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

☑ Enable This Policy

**Name:** Policy name.

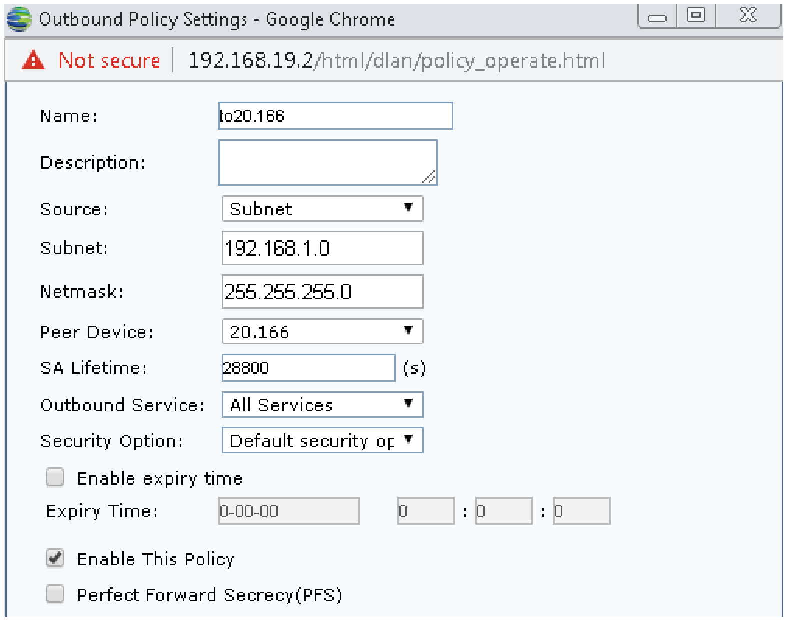
**Source:** In this scenario we choose subnet, you can choose Single IP if only ant to allow 1 IP to access.

**Subnet:** Fill in the peer LAN segment.

**Netmask:** Fill in the subnet mask of the peer LAN segment.

**Peer Device:** Choose the peer device that configured on phase 1.

**Inbound Service:** In this scenario, we choose All Services. You can change this options due to user's requirement.



Outbound Policy Settings - Google Chrome

Not secure | 192.168.19.2/html/dlan/policy_operate.html

Name: to20.166

Description:

Source: Subnet

Subnet: 192.168.1.0

Netmask: 255.255.255.0

Peer Device: 20.166

SA Lifetime: 28800 (s)

Outbound Service: All Services

Security Option: Default security op

□ Enable expiry time

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

☑ Enable This Policy

□ Perfect Forward Secrecy(PFS)

**Name:** Policy name.

**Source:** In this scenario, we choose Subnet because we want to allow all LAN segment to access peer network.

**Subnet:** Fill in the LAN network segment.

**Netmask:** Fill in the subnet mask of the peer LAN segment.

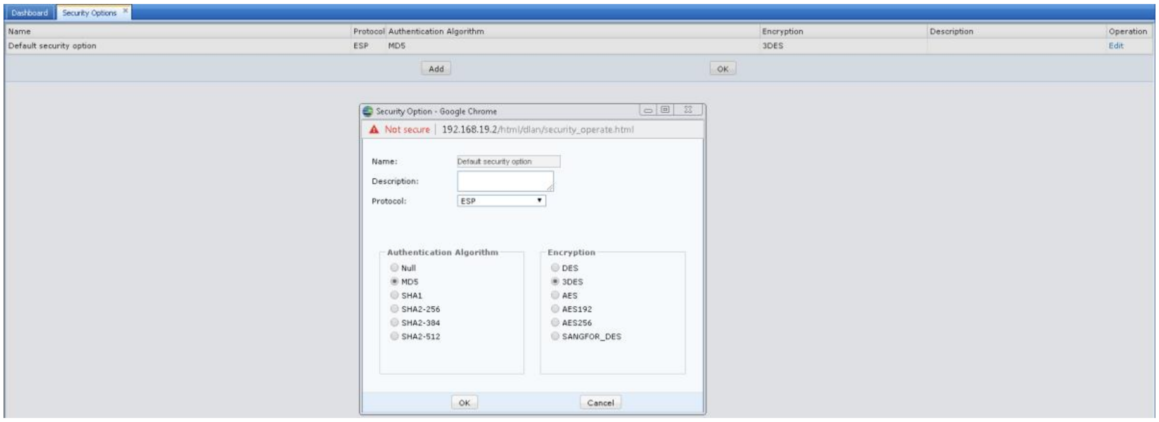
**Peer Device:** Choose the peer device that configured on phase 1.

**SA Lifetime:** In this scenario, we use the default lifetime. You can change it due to user's requirement.

**Outbound Services:** In this scenario, we choose All Services. You can change it due to user's requirement.

**Security Options:** In this case we use the Default security option. You can add a new security option if you don't want to use the default security option.

3. Go to **Network** > **IPSecVPN**> **IPSec VPN** > **Security Options,** to check the default security option or create a new security option as figure below:


Dashboard
Security Options
Add
OK
Security Option - Google Chrome
Not secure | 192.168.19.2/html/dlan/security_operate.html
OK
Cancel

| Name | Protocol | Authentication Algorithm | Encryption | Description | Operation |
|---|---|---|---|---|---|
| Default security option | ESP | MD5 | 3DES | | Edit |

Name: Default security option

Description:

Protocol: ESP

Authentication Algorithm

○ Null
● MD5
○ SHA1
○ SHA2-256
○ SHA2-384
○ SHA2-512

Encryption

○ DES
● 3DES
○ AES
○ AES192
○ AES256
○ SANGFOR_DES

4. On peer device, follow the Step 1 to 3. You need to make sure the parameter of both device is consistent if order to build up the VPN.

# 6. Precautions

In mix mode, device will have Layer 2 and Layer 3 zone at a same time. When adding a new policy, it can only allow to configure policy between Layer 3 to Layer 3 zone or Layer 2 to Layer 2 zone. If the policy add both Layer 2 and Layer 3zone, the policy will not take effect.

SANGFOR

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