



**SANGFOR**

## **IPsec VPN**

**Troubleshooting guide for unable to access peer side  
with IPsec VPN built-up**



---

## Change Log

Date	Change Description
Dec 17, 2019	Troubleshooting guide for unable to access peer side with IPsec VPN built-up

---

# CONTENT

<b>1. Document Description</b> .....	<b>4</b>
<b>2. Applicable Version</b> .....	<b>4</b>
<b>3. Problem Scenario</b> .....	<b>4</b>
<b>4. Troubleshooting Guide</b> .....	<b>5</b>
4.1 General Scenario Troubleshooting Step .....	5
4.2 Configuration error in Phase 2 .....	5
4.3 Application Control configuration error .....	5
4.4 Unreplied ESP .....	<b>Error! Bookmark not defined.</b>
<b>5. Collect Information</b> .....	<b>7</b>
<b>6. Request Articles</b> .....	<b>7</b>

---

## 1. Document Description

The purpose of this document is to provide guidance for troubleshooting on the unable to access peer side with IPsec VPN built-up.

## 2. Applicable Version

This document is applicable for the failure of building up IPsec VPN on all Sangfor product.

The version included VPN/DLAN version 5.0 onwards.

## 3. Problem Scenario

Unable to access peer side with IPsec VPN built-up in this document is referring to the scenario that Sangfor devices has built-up IPsec VPN with third-party device, but unable to access each other.

For unable to access peer side with IPsec VPN built-up, mainly divided into the following scenarios:

- Configuration error in Phase 2
- Application Control configuration error

## 4. Troubleshooting Guide

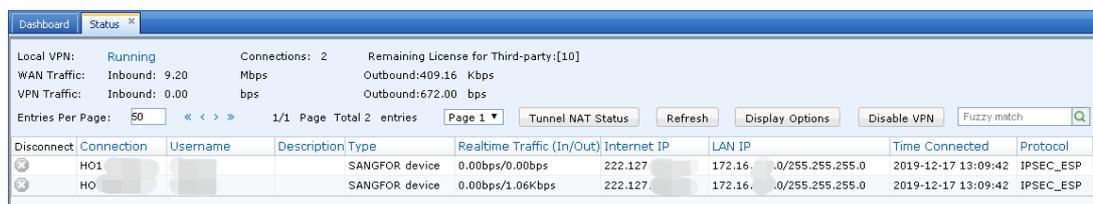
### 4.1 General Scenario Troubleshooting Step

The following basic information need to be confirmed when unable to access peer side with IPsec VPN built-up:

1. Make sure both Sangfor side and Third-party are able to ping to each other.
  - i. Navigate to [Maintenance] > [Web Console]
  - ii. Ping to peer side device IP
  - iii. Ensure it is able to Ping to each other
2. Make sure the IPsec VPN Service port – 500 and 4500 is allowed in both sides.
3. Sangfor device do not support IKEv2 yet, therefore must use IKEv1 to build the IPsec VPN with third party device.
4. For NAT scenario, recommend to use Aggressive mode.
5. Make sure the IPsec VPN tunnel has been built-up

### 4.2 Configuration error in Phase 2

Check if all segment that allows to communicate with peer side are configured correctly and the VPN connection status is displayed in the VPN Status page.



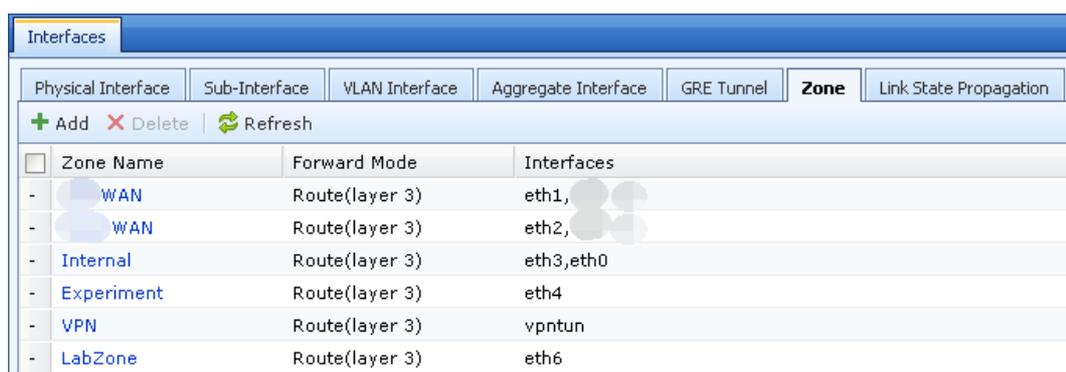
Disconnect	Connection	Username	Description	Type	Realtime Traffic (In/Out)	Internet IP	LAN IP	Time Connected	Protocol
	HO1			SANGFOR device	0.00bps/0.00bps	222.127.	172.16.0/255.255.255.0	2019-12-17 13:09:42	IPSEC_ESP
	HO			SANGFOR device	0.00bps/1.06Kbps	222.127.	172.16.0/255.255.255.0	2019-12-17 13:09:42	IPSEC_ESP

Each entry that created in Phase 2 will generate a VPN connection entry in VPN Status page.

If the respective network segment did not show on the VPN Status page, check on Phase 2 Inbound and Outbound policy for both sides.

### 4.3 Application Control configuration error

For certain Sangfor device such as Sangfor NGAF, it will auto generate a “VPNTUN” zone when the Sangfor NGAF is used to build VPN.



Zone Name	Forward Mode	Interfaces
- WAN	Route(layer 3)	eth1,
- WAN	Route(layer 3)	eth2,
- Internal	Route(layer 3)	eth3,eth0
- Experiment	Route(layer 3)	eth4
- VPN	Route(layer 3)	vpntun
- LabZone	Route(layer 3)	eth6

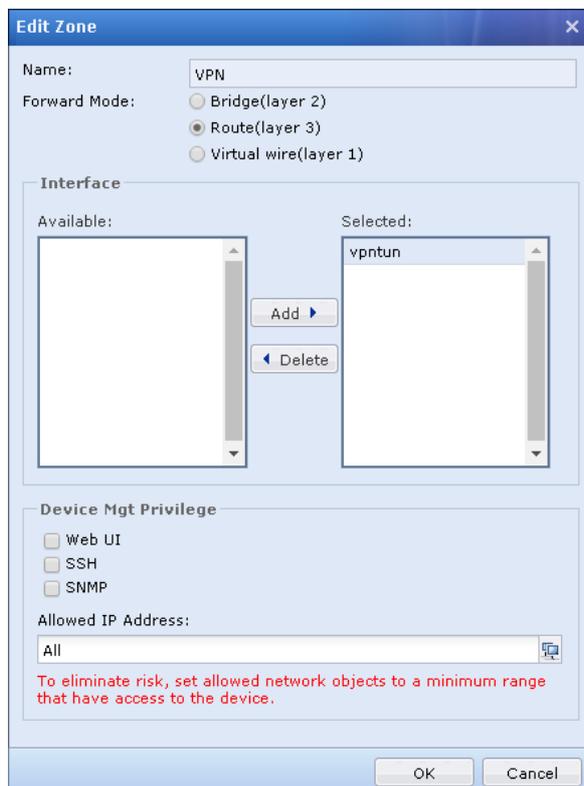
By default, Sangfor NGAF Application Control policy has a “Deny All” policy. Therefore, if VPNTUN zone did not include in any allow policy, the traffic will drops into “Deny All” policy.

In order to prevent and solve the problem, below are the solutions:

1. Create an Allow policy, select all available zone, or LAN and VPN for both Source and Destination zone. So that traffic from LAN to VPN will not be denied by the default “Deny All” policy.

Priority	Name	Group	Src Zone	Source Network Obj...	Dst Zone	Destination Netw...	Service/Application	Schedule
1	Allow	Default group	WAN WAN	All	WAN WAN	All	Predefined Service/any	All week
2	Default Policy	-	All	WAN WAN Internal Experiment VPN LabZone	All	All	All/All	All week

2. Remove the “vpntun” from zone. Navigate to [Network] > [Interfaces] > [Zone], then click on VPN zone, and “Delete” vpntun from the “Selected”.



**Note: Removing VPNTUN from zone will result in unable to control VPN traffic with Application Control Policy as well as Bandwidth Management.**

---

## 5. Collect Information

If the problem still unable to be resolve through the troubleshooting steps above, you can collect the below information and escalate the problem to Sangfor Technical Support with the Community Open a Case feature. Technical Engineer will contact you to provide assistance on resolving the issue.

Information need to be collect:

- i. Server Model and both sides firmware version.
- ii. Screenshot of the System Logs for both sides.
- iii. What troubleshooting step you had gone through.

Open a support case access link:

<http://community.sangfor.com/plugin.php?id=service:case>

## 6. Request Articles

If you have new document requirement, you can feedback to us with the feedback link below. We will provide the troubleshooting guide document based on the feedback.

Feedback Link

CMS: <http://192.200.19.22/request-articles/>

Sangfor Community: <http://community.sangfor.com/plugin.php?id=service:feedback>



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

