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

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

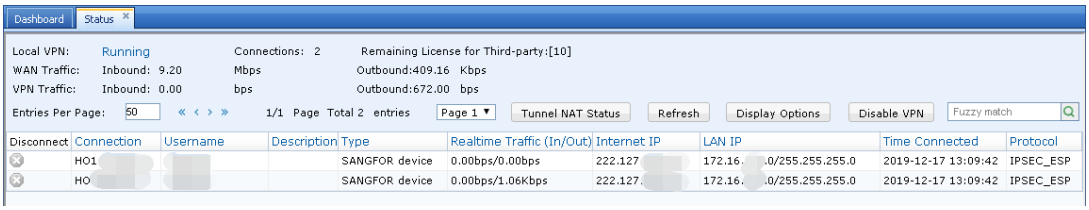
4.1 General Scenario Troubleshooting Step

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.

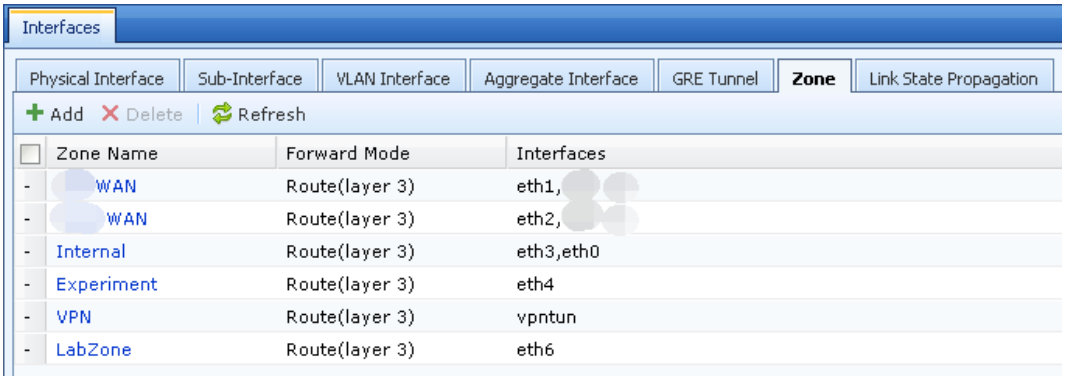


Each entry that created in Phase 2 will generate a VPN connection entry in VPN Status page.

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

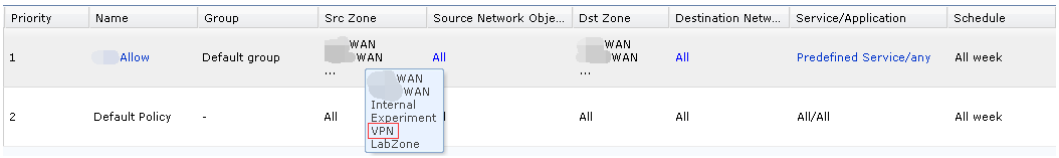
For certain Sangfor device such as Sangfor NGAF, it will auto generate a "VPNTUN" zone when the Sangfor NGAF is used to build VPN.



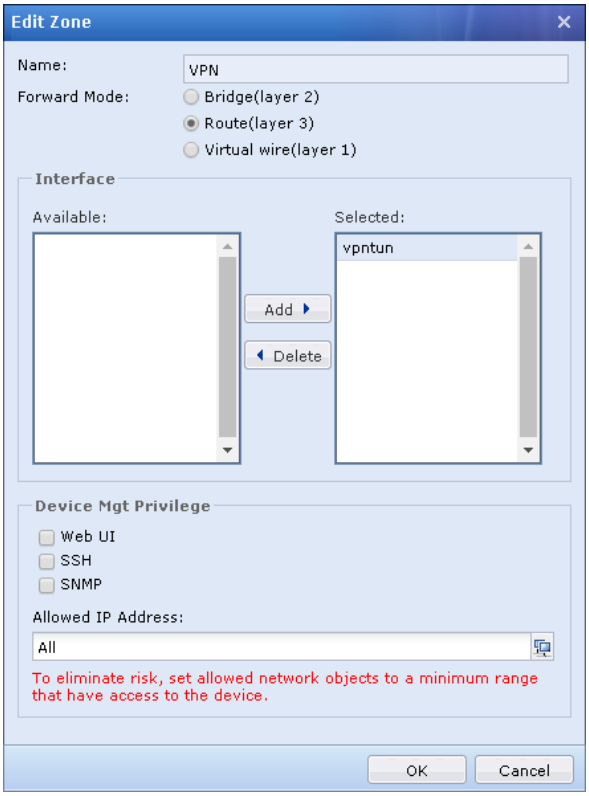
By default, Sangfor NGAF Application Control policy has a “Deny All” policy. Therefore, if VPNTUN zone did not include in any allow policy, the traffic will drops into “Deny All” policy.

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.



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