SANGFOR

NGAF

IPsec VPN Build Up Failed Troubleshooting

Version 8.0.8

Change Log

Date	Change Description
Nov 28, 2019	IPsec VPN Build Up Failed Troubleshooting.

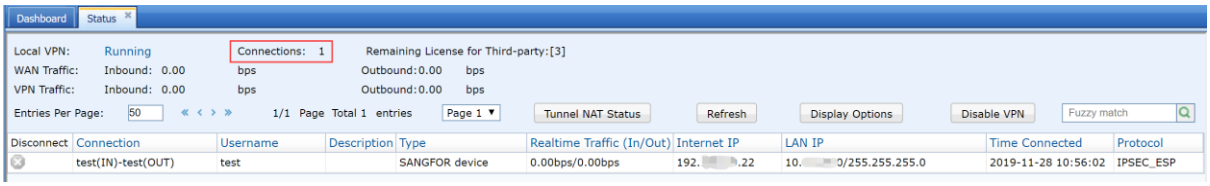
CONTENT

Chapter 1 Application Scenario

NGAF failed to establish IPsec VPN.

Chapter 2 Troubleshooting Methods

1. Go to **Network > IPsec VPN > Status** check whether the standard IPSEC connection is successful. As shown below we can see a normal VPN connection.



We need to pay attention to the following information.

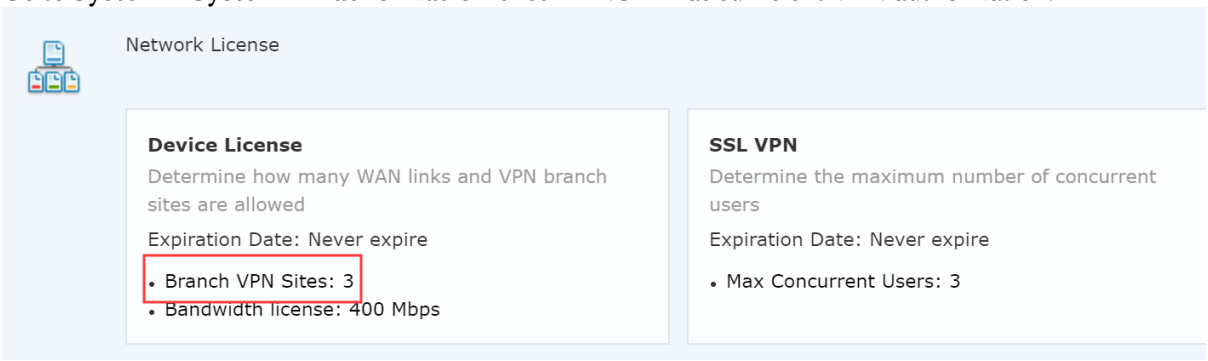
[Internet IP]: The public IP of the peer device connected to this device is displayed here.

[LAN IP]: Internal network segment of the peer device.

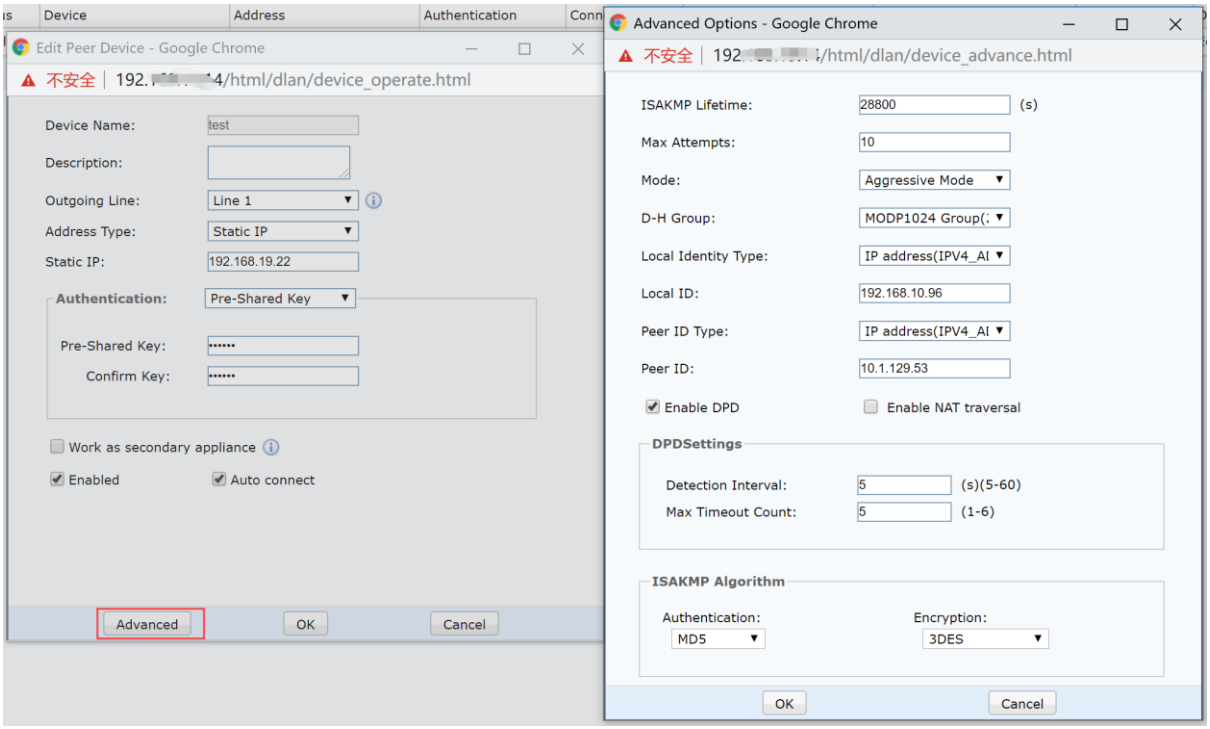
[Time Connected]: VPN connection success time.

[Protocol]: The transfer mode used by the VPN connection.

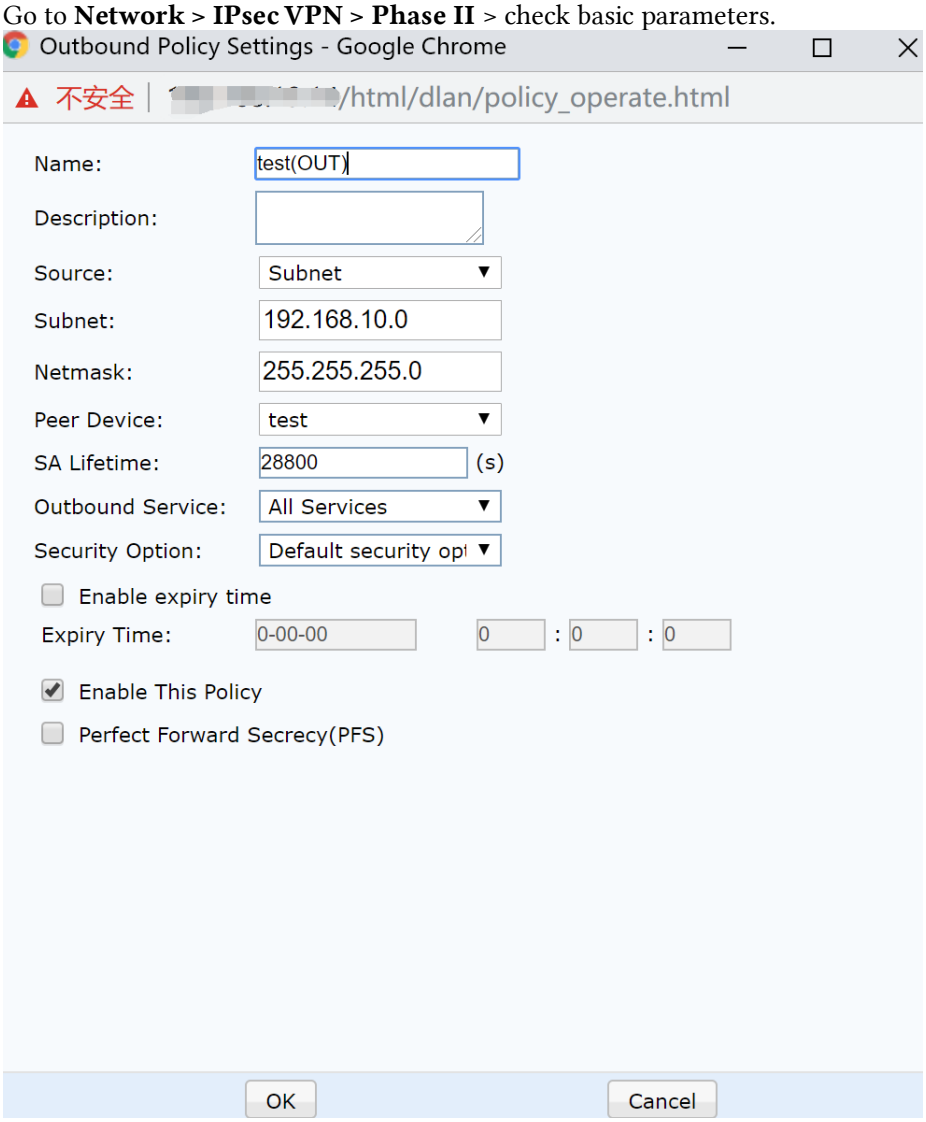
2. Confirm that the network environment of the devices at both ends includes: device deployment mode, NGAF version information, network topology, whether the exit is a dial-up or fixed IP address, and whether a dynamic domain name exists.
   (1) If the VPN devices on both sides have a NAT environment, they must use the aggressive mode, and the UDP 500 and 4500 port mapping must be done on the front device.
   (2) If both parties have fixed IP and no NAT environment, then they can be in aggressive or main mode.
3. Go to **System > System > Authorization** check if NGAF has sufficient VPN authorization.



4. Check whether the basic parameters of the devices at both ends of the VPN are configured correctly.
   (1) Go to **Network > IPsec VPN > Phase I** check basic parameters.



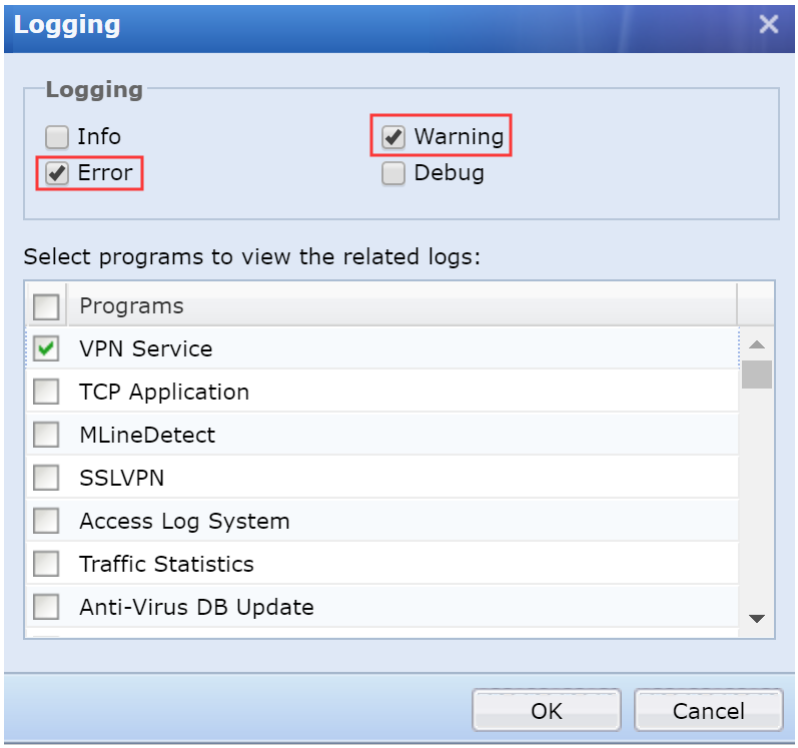
(2) Go to **Network** > **IPsec VPN** > **Phase II** > check basic parameters.



(3) The specific parameters that need to be compared at both ends of the VPN are as follows.

Phase	Auto connect	Whether need to Consistent	Sangfor Device Options	Third-party Decive	Compare Results
Phase I	WAN IP	No Related			
	Auto connect	No Need			
	IKE Version	Must be consistent	Only V1 in NGAF8.0.13		
	Pre-shared Key	Must be consistent			
	ISAKMP Lifetime	Must be consistent			
	Mode	Must be consistent			
	D-H Group	Must be consistent			
	Local Identity Type	aggressive need to compare			
	Local ID	aggressive need to compare			
	Peer ID Type	aggressive need to compare			
	Peer ID	aggressive need to compare			
	Enable DPD	Must be consistent			
	Enable NAT traversal	Must be consistent			
	ISAKMP Authentication Algorithm	Must be consistent			
	ISAKMP Encryption Algorithm	Must be consistent			
Phase II	IPsec Protocol	Must be consistent			
	D-H Group	Must be consistent			
	SA Lifetime	Must be consistent			
	Seurity Option	Must be consistent			
	Authentication Algorithm	Must be consistent			
	Encryption Algorithm	Must be consistent			
	Perfect Forward Secrecy(PFS)	Must be consistent			
	Inbound Policy	Peer intranet network segment			
	Outbound Policy	Local intranet network segment			

5. After checking all configurations, there is no problem, but the VPN still cannot be established. Go to **System** > **Troubleshooting** > **Logs** check VPN service Error or Warning log. If the error log cannot analyze the cause, you can also try to analyze info and debug info. For more common log cause analysis, you can refer to Chapter 4.



6. If the above troubleshooting does not solve your problem, you can try go to **System** > **Troubleshooting** > **Capture Packets** capture the packet to analyze the VPN interactive process.

Chapter 3 Guide for VPN packet analysis

1. The three packets in **Phase I** of Aggressive Mode, as shown below.

12	10.003195	192.168.19.22	192.168.19.14	ISAKMP	346 Aggressive
13	10.010702	192.168.19.14	192.168.19.22	ISAKMP	366 Aggressive
14	10.012927	192.168.19.22	192.168.19.14	ISAKMP	94 Aggressive

2. The six packets in **Phase I** of Main Mode, as shown below.

7	10.353395	192.168.19.14	192.168.19.22	ISAKMP	182 Identity Protection (Main Mode)
8	10.355530	192.168.19.22	192.168.19.14	ISAKMP	182 Identity Protection (Main Mode)
9	10.372499	192.168.19.14	192.168.19.22	ISAKMP	222 Identity Protection (Main Mode)
10	10.386788	192.168.19.22	192.168.19.14	ISAKMP	222 Identity Protection (Main Mode)
11	10.391100	192.168.19.14	192.168.19.22	ISAKMP	102 Identity Protection (Main Mode)
12	10.405654	192.168.19.22	192.168.19.14	ISAKMP	102 Identity Protection (Main Mode)

3. According to the parameter information of the data packet, we can check the parameters and locate the problem. By analyzing the data packet, we can know whether the basic parameters at both ends are consistent. The **Phase I** of the data packet, as shown below:

```
> User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
v Internet Security Association and Key Management Protocol
    Initiator SPI: 0c7e7fd8ff4aec29
    Responder SPI: 0000000000000000          <-- all is 0 mean this is the first packet
    Next payload: Security Association (1)
  > Version: 1.0                             <-- IKE Version
    Exchange type: Identity Protection (Main Mode) (2)   <-- Main Mode
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 140
  v Type Payload: Security Association (1)
      Next payload: Vendor ID (13)
      Payload length: 52
      Domain of interpretation: IPSEC (1)
    > Situation: 00000001
    v Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload  (0)
        Payload length: 40
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
      v Type Payload: Transform (3) # 1                 <-- Other basic parameter
          Next payload: NONE / No Next Payload  (0)
          Payload length: 32
          Transform number: 1
          Transform ID: KEY IKE (1)
        > Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
        > Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
        > Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
        > Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
        > Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
        > Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
```

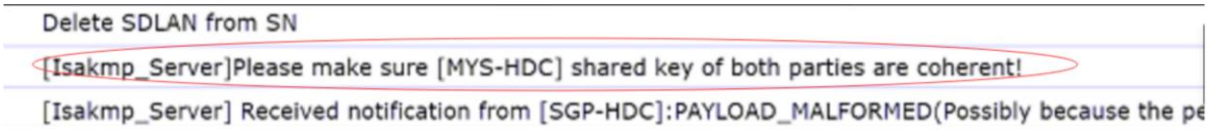
4. If it is stuck in the **Phase II** and the configuration cannot be checked, you can let the peer initiate a connection. We capture the data packet to decrypt and decrypt the second-phase parameters of the peer and then analyze and compare.

13	10.407118	192.168.19.14	192.168.19.22	ISAKMP	198 Quick Mode
14	10.419404	192.168.19.22	192.168.19.14	ISAKMP	198 Quick Mode
15	10.419416	192.168.19.14	192.168.19.22	ISAKMP	94 Quick Mode

Chapter 4 Common Log Cause Analysis

Scenario 1: Shared keys are inconsistent

Warning Logs: Please make sure [MYS-HDC] shared key of both parties are coherent!



Root Cause: Pre-Shared Key of both parties are different.

Solution:

Go to **Network** > **IPsec VPN** > **Phase I** change Pre-Shared Key Configuration.

Scenario 2: It contains too many payloads

Warning Logs: Received an invalid IKE packet, for it contains too many payloads

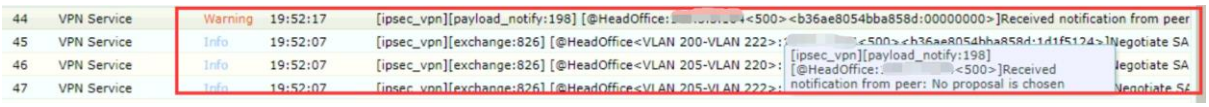
Root cause: There is limitation in payload number in DLAN version 6.2.0 and above.

Solution:

Contact Sangfor support.

Scenario 3: No proposal is chosen

Warning Logs: Received notification from peer: No proposal is chosen.

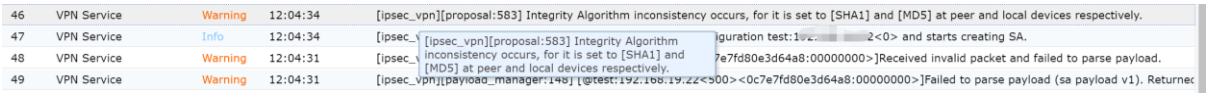


Root Cause: Local did not receive peer ISAKMP Algorithm in **Phase II**.

Solution: Try to use other authentication Algorithm and encryption Algorithm.

Scenario 4: Integrity Algorithm inconsistency

Warning Logs: Integrity Algorithm inconsistency occurs, for it set to [SHA1] and [MD5] at peer and local devices respectively.

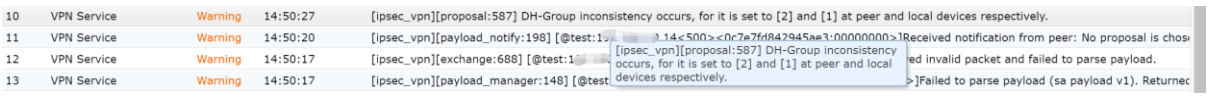


Root Cause: Integrity Algorithm inconsistency

Solution: Modify **Phase I** the ISAKMP Algorithm configuration to be consistent.

Scenario 5: DH-Group inconsistency occurs

Warning Logs: DH-Group inconsistency occurs, for it is set [2] and [1] at peer and local devices respectively.



Root Cause: DH-Group inconsistency.

Solution: Modify the DH-Groups at both ends to be consistent.

Scenario 6: Does not support IKE v2

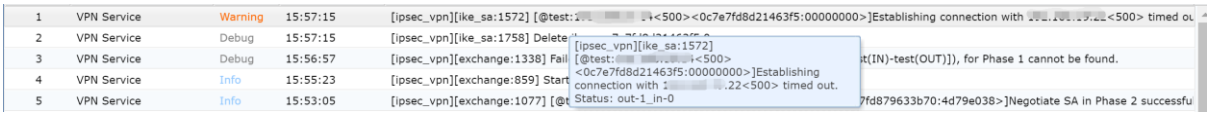
Warning Logs: Message for ip with a uncorrect ISAKMP_MAJOR_VERSION value!

Root Cause: Third-party devices initiate negotiation using IKE v2.

Solution: Setting up third-party devices to use IKE V1.

Scenario 7: Establishing connection timed out

Warning Logs: Establishing connection with ip <500> timed out.



Root Cause: Port 500 on both devices cannot communicate normally.

Probable Cause:

(1) The network of the two devices is unreachable.

(2) A device in the middle intercepted the VPN negotiation packets.

(3) NGAF is not deployed on the public network, and the export device does not map port 500 normally.

(4) The connected packets are intercepted by the DOS or security policy of NGAF itself. It is recommended to enable BYPASS for debugging on a specific IP

Chapter 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 collected:

(1) Network Topology.

(2) VPN negotiated packets.

(3) Screenshot of the System Logs for both sides.

(4) Specific parameter comparison table.

(5) What troubleshooting step you had gone through.

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