



SANGFOR

IPsec VPN

Troubleshooting guide for IPsec VPN build up failure



Change Log

Date	Change Description
April 4, 2019	Troubleshooting guide for IPsec VPN build up failure

CONTENT

1. Document Description	4
2. Applicable Version	4
3. Problem Scenario	4
4. Troubleshooting Guide	5
4.1 General Scenario Troubleshooting Step	5
4.2 IPsec VPN build up Error and Solution	5
4.2.1 Negotiating Phase 1 security association failed	5
4.2.2 Negotiating Phase 2 security association failed	6
4.3 Advanced Troubleshooting	6
5. Collect Information	9
6. Request Articles	9

1. Document Description

The purpose of this document is to provide guidance for troubleshooting on the failure of building up IPsec VPN.

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

The failure of building up IPsec VPN in this document is referring to the scenario that Sangfor device is trying to build IPsec VPN with another third party device.

For failure of building up Sangfor VPN, mainly divided into the following scenarios:

- Configuration error in either Phase 1 or Phase 2
- IPsec VPN Service port did not allowed
- Unsupported protocol

4. Troubleshooting Guide

4.1 General Scenario Troubleshooting Step

The following basic information need to be confirmed when the IPsec VPN build up failure:

1. Make sure both Sangfor side and Client side 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.

4.2 IPsec VPN build up Error and Solution

4.2.1 Negotiating Phase 1 security association failed

1. System Logs:

	Service	Severity	Time	Details
1	VPN	Warning	10:14...	[Isakmp_Server]Negotiating with [test]'s Phase 1 security association ...
2	VPN	Info	10:14...	[Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! :1.1.1.2) us...

2. Possible cause:

- i. Phase 1 configuration on both sides are different
- ii. IPsec VPN Service port is blocked or unreachable
- iii. Peer side is unreachable

3. Solution:

- i. Check and ensure both side Phase 1 configuration is same and both side configuration must be same
- ii. Ensure the IPsec VPN Service port – 500 and 4500 is allowed
- iii. Ensure the peer side Public IP is correct and reachable.

4.2.2 Negotiating Phase 2 security association failed

1. System Logs:

	Service	Severity	Time	Details
1	VPN	Warning	11:20...	[Isakmp_Server]Negotiating between policy [out] and policy[in]'s Phase 2 security association failed. Failed to build connection!
2	VPN	Info	11:19...	[Isakmp_Server]Negotiating between policy [out] and policy[in]'s Phase 2 security association failed. [IP:1.1.1.2] has finished! The tunnel has been built !
3	VPN	Info	11:19...	[Isakmp_Server]Negotiating between policy [out] and policy[in]'s Phase 2 security association failed. Failed to build connection! [IP:1.1.1.2] using main mode!
4	VPN	Info	11:19...	[Isakmp_Server]The Phase 1 Security association for [test](IP:1.1.1.2) has finished! The tunnel has been built !

2. Possible cause:

- i. Phase 2 configuration on both sides are different

3. Solution:

- i. Check and ensure both side Phase 2 configuration is same and both side configuration must be same

4.3 Advanced Troubleshooting

1. Prerequisite:

Before capture packet, the VPN service must first disable in order to capture the complete packet from the starts

2. Packet Capture:

Capture Phase 1 packet from Sangfor device via backend.

Command: `tcpdump -i wanport port 500 or port 4500 -s0 -w /tmp/phase1.pcap`

Note: *wanport* in the command above refers to the WAN port of Sangfor device. Usually will be ETH2.

3. Analyze from the packet:

Aggressive:

	ip.id	Time	Source	Destination	Protocol	Length	Info
1	0xfb4 (64468)	0.000000	10.0.1.2	1.1.1.2	ISAKMP	330	Aggressive
2	0x0000 (0)	0.017393	1.1.1.2	10.0.1.2	ISAKMP	342	Aggressive
3	0xfb5 (64469)	0.018913	10.0.1.2	1.1.1.2	ISAKMP	94	Aggressive

Main Mode:

	ip.id	Time	Source	Destination	Protocol	Length	Info
1	0xfb4 (64468)	0.000000	10.0.1.2	1.1.1.2	ISAKMP	166	Identity Protection (Main Mode)
2	0x0000 (0)	0.000682	1.1.1.2	10.0.1.2	ISAKMP	146	Identity Protection (Main Mode)
3	0xfb5 (64469)	0.001083	10.0.1.2	1.1.1.2	ISAKMP	222	Identity Protection (Main Mode)
4	0x0000 (0)	0.010019	1.1.1.2	10.0.1.2	ISAKMP	230	Identity Protection (Main Mode)
5	0xfb6 (64470)	0.010399	10.0.1.2	1.1.1.2	ISAKMP	110	Identity Protection (Main Mode)
6	0x0000 (0)	0.018310	1.1.1.2	10.0.1.2	ISAKMP	110	Identity Protection (Main Mode)

- The first few packets will show the mode that used to build IPsec VPN. 6 packets for Main mode, while 3 packets for Aggressive mode
- For Main mode, the first 2 packets is negotiation of Security Association between both sides that includes Authentication Algorithm, Encryption Algorithm, IKE version and so on
- The third and the forth packets is negotiation of D-H group and Preshared key
- The fifth and sixth packets is negotiation of identity

```

> Frame 14: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits)
> Ethernet II, Src: fe:fd:fe:ba:da:05 (fe:fd:fe:ba:da:05), Dst: fe:fc:fe:a7:93:13 (fe:fc:fe:a7:93:13)
> Internet Protocol Version 4, Src: 1.1.1.2, Dst: 10.0.1.2
> User Datagram Protocol, Src Port: 500, Dst Port: 500
< Internet Security Association and Key Management Protocol
  Initiator SPI: f396d3e797e975ec
  Responder SPI: 0000000000000000 Responder SPI: 0 means this is the first packet
  Next payload: Security Association (1)
  < Version: 1.0 IKE version
    0001 .... = MjVer: 0x1
    .... 0000 = MnVer: 0x0
  Exchange type: Identity Protection (Main Mode) (2) Main mode
  < Flags: 0x00
    .... 0 = Encryption: Not encrypted
    .... 0 = Commit: No commit
    .... 0 = Authentication: No authentication
  Message ID: 0x00000000
  Length: 444
  > Payload: Security Association (1)
  > Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-08
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-06
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-05
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-04
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-01
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-00
  > Payload: Vendor ID (13) : CISCO-UNITY 1.0
  > Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  
```

ISAKMP configuration

- From the packet capture, peer side Security Association configuration will be shown here. Then, Sangfor side just need to follow what the peer side has configured and the VPN will be able to build up easily

```

  ▲ Payload: Security Association (1)
    Next payload: Vendor ID (13)
    Reserved: 00
    Payload length: 156
    Domain of interpretation: IPSEC (1)
  ▶ Situation: 00000001
  ▲ Payload: Proposal (2) # 1
    Next payload: NONE / No Next Payload (0)
    Reserved: 00
    Payload length: 144
    Proposal number: 1
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Proposal transforms: 4
  ▲ Payload: Transform (3) # 1
    Next payload: Transform (3)
    Reserved: 00
    Payload length: 36
    Transform number: 1
    Transform ID: KEY_IKE (1)
    Reserved: 0000
    ▶ IKE Attribute (t=11,l=2): Life-Type: Seconds
    ▶ IKE Attribute (t=12,l=2): Life-Duration: 3600
    ▶ IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
    ▶ IKE Attribute (t=14,l=2): Key-Length: 128
    ▶ IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
    ▶ IKE Attribute (t=2,l=2): Hash-Algorithm: SHA
    ▶ IKE Attribute (t=4,l=2): Group-Description: 2048 bit MODP group
  ▶ Payload: Transform (3) # 2
  ▶ Payload: Transform (3) # 3
  ▶ Payload: Transform (3) # 4
  ▶ Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE

```

- After expand the Payload from the packet, all the Security Association will be shown

Phase 2

4	0xfbd6 (64470)	0.019641	10.0.1.2	1.1.1.2	ISAKMP	342 Quick Mode
5	0x0000 (0)	0.028394	1.1.1.2	10.0.1.2	ISAKMP	350 Quick Mode
6	0xfbd7 (64471)	0.029435	10.0.1.2	1.1.1.2	ISAKMP	94 Quick Mode

- Unlike Phase 1, Phase 2 only contain 3 packets only with Aggressive mode or Main mode.

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

