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

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

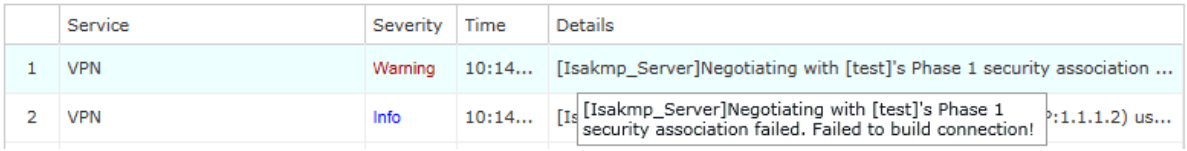
The following basic information need to be confirmed when the IPsec VPN build up failure:

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:



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. Failed to build connection!
3	VPN	Info	11:19...	[redacted](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:

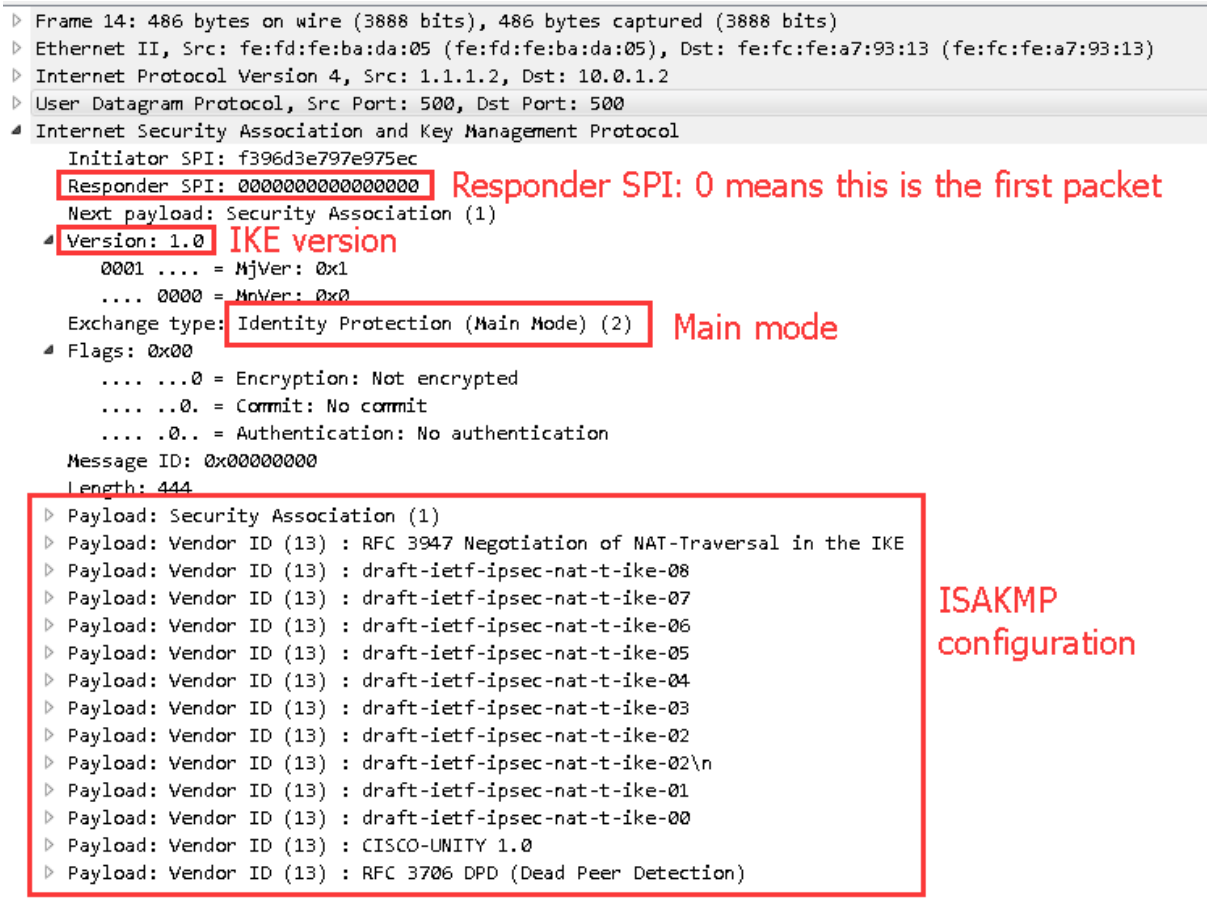
   Aggressive:

	ip.id	Time	Source	Destination	Protocol	Length	Info
1	0xfbd4 (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	0xfbd5 (64469)	0.018913	10.0.1.2	1.1.1.2	ISAKMP	94	Aggressive

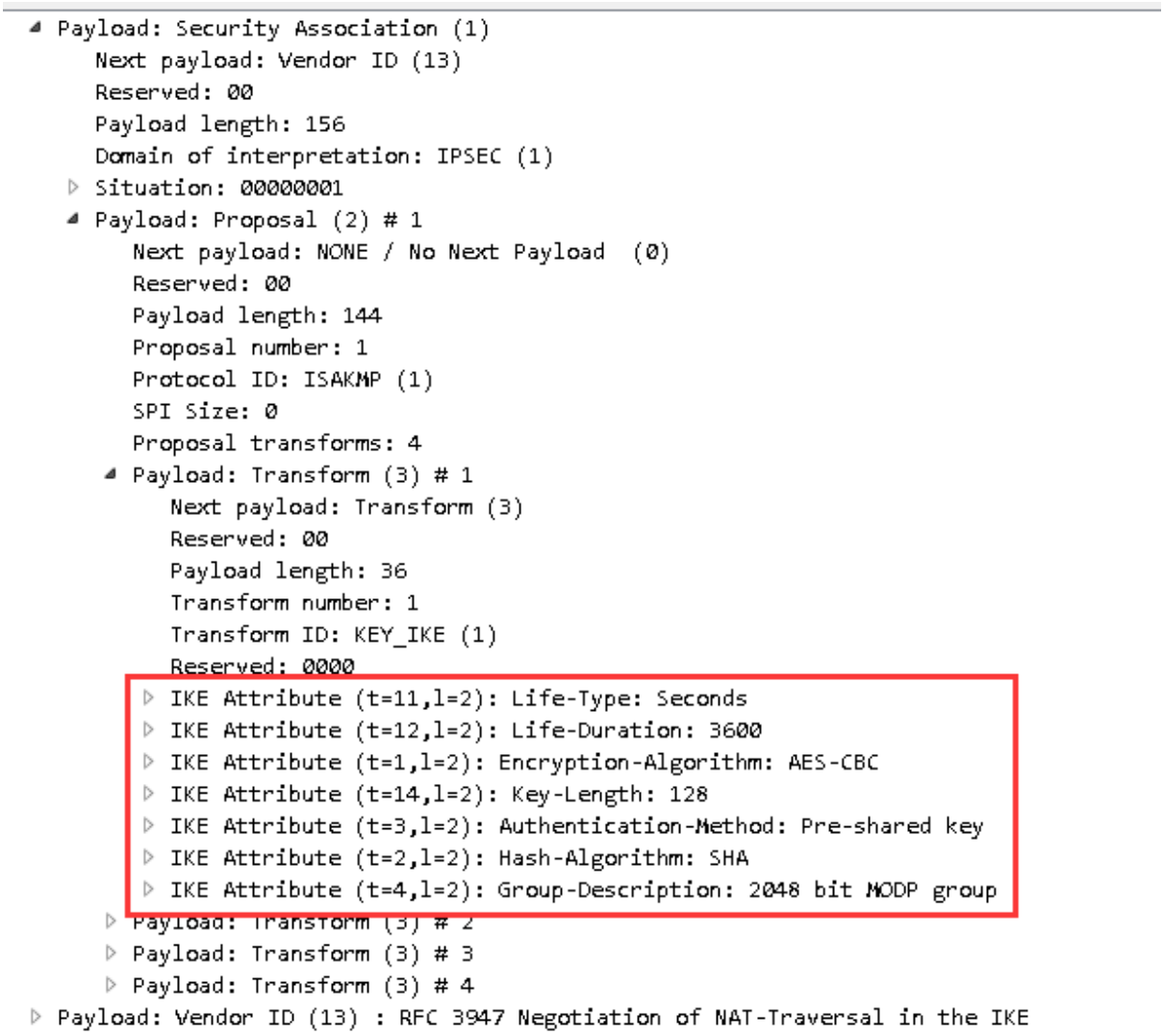
   Main Mode:

	ip.id	Time	Source	Destination	Protocol	Length	Info
1	0xfbd4 (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	0xfbd5 (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	0xfbd6 (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



- 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



- 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