IPsec VPN

Guida alla risoluzione dei problemi per l'errore di creazione di VPN IPsec

Registro delle modifiche

Data	Descrizione dei Cambiamenti
Aprile 4, 2019	Guida alla risoluzione dei problemi per l'errore di creazione di VPN IPsec

CONTENUTO

1. Descrizione del documento....1
2. Versione applicabile....1
3. Scenario di problema....1
4. Guida alla risoluzione dei problemi....1
   4.1 Step per la risoluzione dei problemi relativi ad uno scenario generale...1
   4.2 Creazione di IPsec VPN, errore e soluzione....2
      4.2.1 Negoziazione dell'associazione di sicurezza della Fase 1 non riuscita .2
      4.2.2 Negoziazione dell'associazione di sicurezza di Fase 2 non riuscita 2
   4.3 Risoluzione dei Problemi Avanzata....2
5. Raccolta informazioni....4
6. Richiedi Articoli....5

1. Descrizione del documento

Lo scopo di questo documento è fornire indicazioni per la risoluzione dei problemi relativi all'errore di creazione di IPsec VPN.

2. Versione applicabile

Questo documento è applicabile in caso di fallimento della creazione di IPsec VPN su tutti i prodotti Sangfor.

La versione include VPN/DLAN dalla versione 5.0 in poi.

3. Scenario di problema

L'errore di creazione di IPsec VPN in questo documento si riferisce allo scenario in cui il dispositivo Sangfor sta tentando di creare IPsec VPN con un altro dispositivo di terze parti.

Il fallimento della creazione di Sangfor VPN viene principalmente suddiviso nei seguenti scenari:

- Errore di configurazione nella fase 1 o nella fase 2
- La porta del servizio VPN IPsec non è consentita
- Protocollo non supportato

4. Guida alla risoluzione dei problemi

4.1 Step per la risoluzione dei problemi relativi ad uno scenario generale

Le seguenti informazioni di base devono essere confermate quando la VPN IPsec genera un errore:

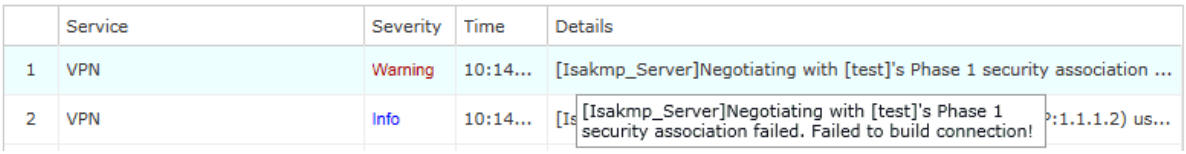
1. Assicurati che sia il lato Sangfor che il lato client siano in grado di eseguire il ping l'uno all'altro.
    i. Passare a [**Maintenance**] > [**Web Console**]
    ii. Ping all'IP del dispositivo lato peer
    iii. Assicurarsi che sia in grado di eseguire il ping l'uno all'altro
2. Assicurati che la porta del servizio VPN Ipsec - 500 e 4500 sia consentita su entrambi i lati.
3. Il dispositivo Sangfor non supporta ancora IKEv2, quindi deve utilizzare IKEv1 per creare la VPN IPsec con un dispositivo di terze parti.

4. Per lo scenario NAT, è consigliato di utilizzare la modalità Aggressive Mode.

4.2 Creazione di IPsec VPN, errore e soluzione

4.2.1 Negoziazione dell'associazione di sicurezza della Fase 1 non riuscita

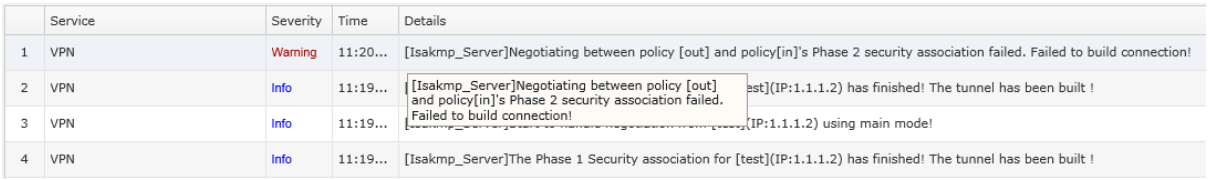
1. System Logs:



2. Causa Possibile:
   i. La configurazione della fase 1 su entrambi i lati è diversa
   ii. La porta del servizio VPN IPsec è bloccata o non raggiungibile
   iii. Il lato peer è irraggiungibile
3. Soluzione:
   i. Controllare e assicurarsi che la configurazione di fase 1 sia la stessa e che entrambe le configurazioni siano uguali
   ii. Assicurarsi che la porta del servizio VPN IPsec – 500 e 4500 sia consentita
   iii. Assicurarsi che l'IP pubblico lato peer sia corretto e raggiungibile.

4.2.2 Negoziazione dell'associazione di sicurezza di Fase 2 non riuscita

1. System Logs:



2. Causa Possibile:
   i. La configurazione della fase 2 su entrambi i lati è diversa
3. Soluzione:
   i. Controllare e assicurarsi che la configurazione di fase 2 sia la stessa e che entrambe le configurazioni siano uguali

4.3 Risoluzione dei Problemi Avanzata

1. Prerequisito:

Prima di acquisire il pacchetto, il servizio VPN deve prima essere disabilitato per acquisire il pacchetto completo dall'avvio

2. Cattura pacchetti:

Cattura il pacchetto di fase 1 dal dispositivo Sangfor tramite back-end.

Comando: tcpdump –i wanport port 500 o port 4500 –s0 –w /tmp/phase1.pcap

Nota: wanport nel comando precedente si riferisce alla porta WAN del dispositivo Sangfor. Di solito sarà ETH2.

3. Analisi dal pacchetto:

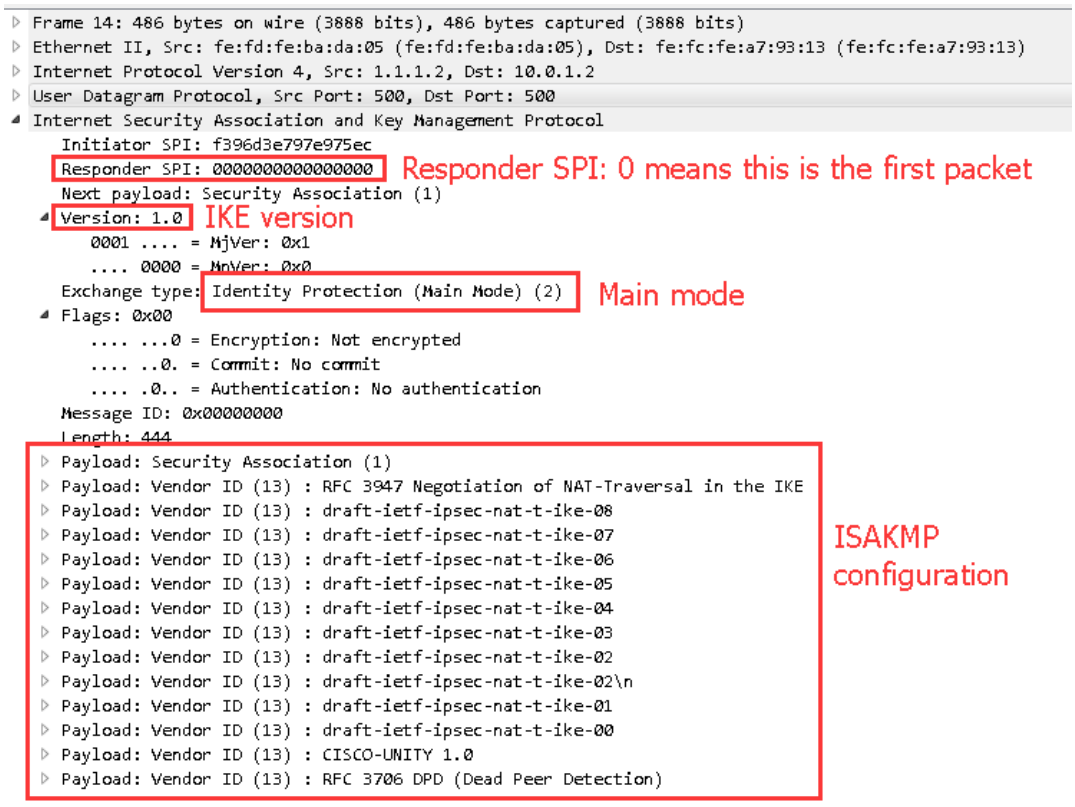
Aggressive:

	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

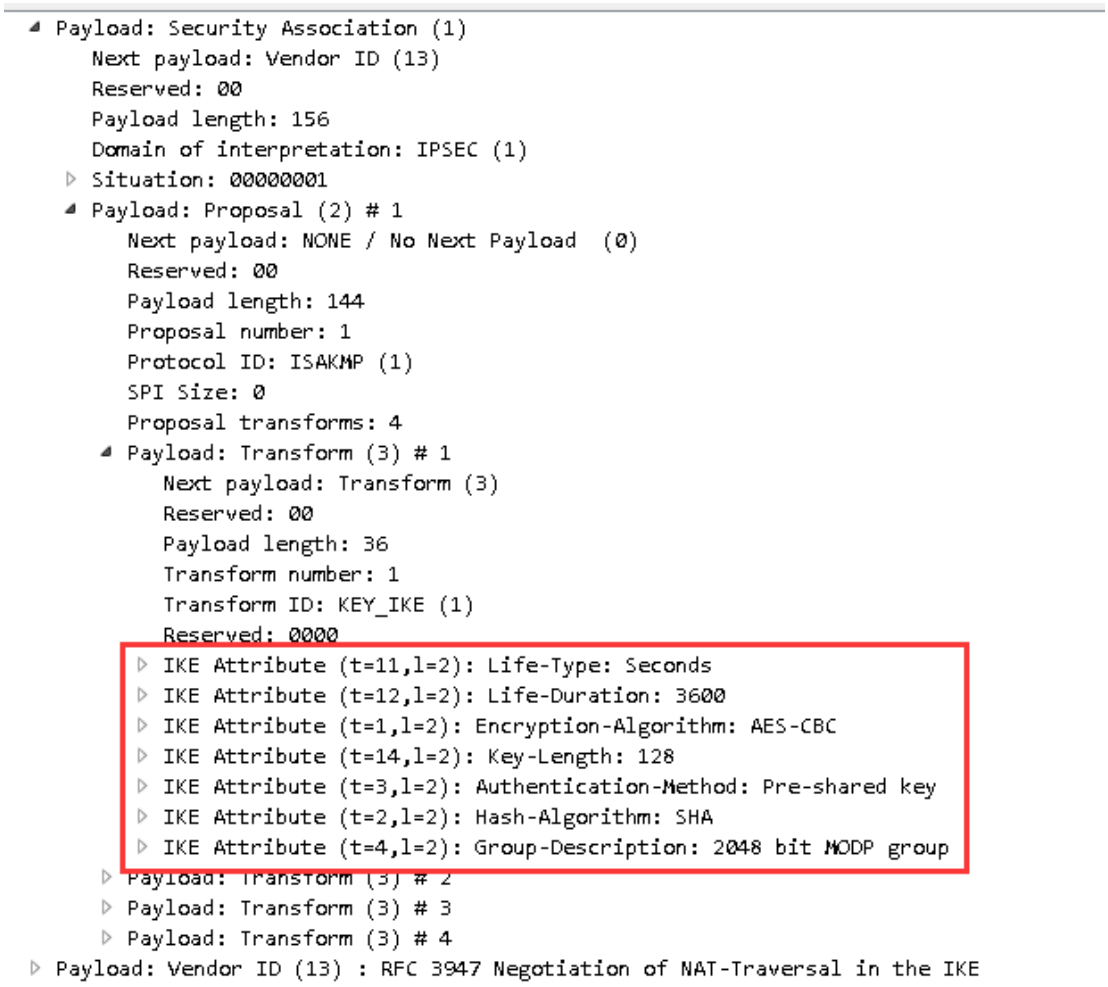
Modalità principale:

	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)

- I primi pacchetti mostreranno la modalità utilizzata per creare IPsec VPN. 6 pacchetti per la modalità principale, mentre 3 pacchetti per la modalità aggressiva
- Per la modalità principale, i primi 2 pacchetti sono la negoziazione dell'associazione di sicurezza tra entrambe le parti che include algoritmo di autenticazione, algoritmo di crittografia, versione IKE e così via
- Il terzo e il quarto pacchetto sono la negoziazione del gruppo D-H e della chiave precondivisa
- Il quinto e il sesto pacchetto sono la negoziazione dell'identità

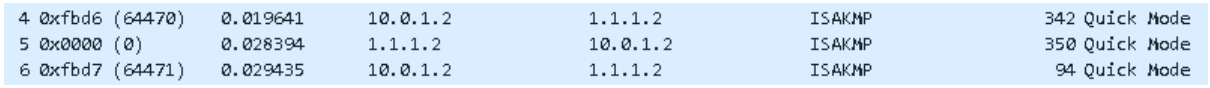


- Dall'acquisizione del pacchetto, la configurazione della Security Association lato peer verrà mostrata qui. Quindi, lato Sangfor deve solo seguire ciò che il lato peer ha configurato e la VPN sarà in grado di crearsi facilmente



- Dopo aver espanso il payload dal pacchetto, verrà mostrata tutta la Security Association

Fase 2



- A differenza della Fase 1, la Fase 2 contiene solo 3 pacchetti solo con modalità Aggressiva o Modalità Principale.

5. Raccolta informazioni

Se il problema non può ancora essere risolto attraverso i passaggi di risoluzione dei problemi di cui sopra, è possibile raccogliere le informazioni riportate di seguito e inoltrare il problema al supporto tecnico Sangfor con la funzione Community Open a Case. L'ingegnere tecnico ti contatterà per fornirti assistenza sulla risoluzione del problema.

Queste le informazioni che devono essere raccolte:

i. Modello server e versione firmware di entrambi i lati.

ii. Screenshot dei log di sistema per entrambe le parti.

iii. Quali passaggi di risoluzione dei problemi hai già effettuato.

Link per accedere e aprire un ticket al supporto:

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

6. Richiedi Articoli

Se hai necessità di avere nuova documentazione o risoluzione a problemi, puoi inviarci un feedback al link di feedback qui sotto. Forniremo il documento guida alla risoluzione dei problemi in base al feedback.

Feedback Link

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

Comunità Sangfor: http://community.sangfor.com/plugin.php?id=service:feedback