



# IPsec VPN

## Guida alla risoluzione dei problemi per IPsec VPN con alta latenza



## Registro delle modifiche

Data	Descrizione dei Cambiamenti
16 agosto 2019	Guida alla risoluzione dei problemi per IPsec VPN con alta latenza

# CONTENUTO

1.	Descrizione del documento.....	1
2.	Versione applicabile .....	1
3.	Scenario di problema .....	1
4.	Guida alla risoluzione dei problemi .....	1
4.2	Collo di bottiglia delle prestazioni .....	2
4.3	Gestione della larghezza di banda .....	2
4.4	Rete instabile .....	2
4.5	Risoluzione dei problemi avanzato .....	2
5.	Raccolta informazioni.....	4
6.	Richiedi Articoli .....	4



# 1. Descrizione del documento

Lo scopo di questo documento è fornire indicazioni per la risoluzione dei problemi sulla latenza elevata con IPsec VPN.

## 2. Versione applicabile

Questo documento è applicabile per l'alta latenza con VPN IPsec su tutti i prodotti Sangfor.

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

## 3. Scenario di problema

L'elevata latenza con IPsec VPN in questo documento si riferisce allo scenario in cui il dispositivo Sangfor crea IPsec VPN con un altro dispositivo di terze parti ma la latenza è elevata.

La latenza elevata con VPN IPsec viene principalmente suddivisa nei seguenti scenari:

- Collo di bottiglia delle prestazioni
- Gestione della larghezza di banda
- Rete instabile

## 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 per l'elevata latenza con IPsec VPN:

1. Assicurati che sia il lato Sangfor che il lato client siano in grado di eseguire il ping l'uno all'altro.
  - i. andare 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.

## 4.2 Collo di bottiglia delle prestazioni

Verificare se è causato da un collo di bottiglia delle prestazioni

Controlla l'I/O del disco con il comando: **iotstat -mx 1**

Device:	rrqm/s	wrqm/s	r/s	w/s	rMB/s	wMB/s	avgrq-sz	avgqu-sz	await	r_await	w_await	svctm	%util
sda	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dm-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dm-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dm-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dm-3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dm-4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dm-5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Controllare e assicurarsi che **%util** non sia troppo alto. Se **%util** mostra più di **80** per la maggior parte del tempo, significa che l'I/O del dispositivo è insufficiente.

Controlla l'utilizzo della CPU con il comando: **mpstat -P ALL 1**

02:44:57 PM	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%idle
02:44:58 PM	all	1.02	0.00	3.06	0.00	0.00	0.00	0.00	0.00	95.92
02:44:58 PM	0	1.01	0.00	4.04	0.00	0.00	1.01	0.00	0.00	93.94
02:44:58 PM	1	0.00	0.00	1.03	0.00	0.00	0.00	0.00	0.00	98.97

Controllare e assicurarsi che **%idle** non sia troppo basso. Se **%idle** mostra meno di **20** per la maggior parte del tempo, significa che la CPU del dispositivo inattiva è molto bassa.

## 4.3 Gestione della larghezza di banda

1. Controlla se c'è qualche funzione di gestione della larghezza di banda o QoS nel mezzo o su entrambi i dispositivi che costruiscono IPsec VPN.
2. Disabilita la gestione della larghezza di banda
3. Abilitare la modalità di bypass su entrambi i dispositivi per evitare che venga influenzato da qualsiasi funzione.

## 4.4 Rete instabile

1. Ping dal dispositivo Sangfor all'IP pubblico lato peer e viceversa. Assicurarsi che il Ping a IP Pubblico abbia una bassa latenza. Se la latenza è elevata, influenzerà anche il traffico VPN.
2. Eseguire il ping da un PC di test al gateway o al dispositivo che gestisce la VPN. Assicurarsi che il ping abbia una bassa latenza. Se la latenza è elevata, è più probabile che il problema di latenza elevata sia causato dalla rete interna instabile.

## 4.5 Risoluzione dei problemi avanzato

Comando utilizzato per catturare i pacchetti:

tcpdump -i any -nnv \(\host 119.36.128.43 o host 10.60.242.3\) e \(\ip[2:2]=138 o ip[2:2]=192\) -w /tmp/ping.pcap

Quindi, eseguire Ping test su un PC con il comando: ping 10.59.1.142 -l 110 -c 200

Di seguito è riportato un esempio di latenza elevata con IPsec VPN.

119.36.128.43	10.60.164.33	ESP	208	ESP (SPI=0xc7a95cf7)	
10.60.242.3	10.59.1.142	ICMP	154	Echo (ping) request	id=
10.60.242.3	10.59.1.142	ICMP	154	Echo (ping) request	id=
10.59.1.142	10.60.242.3	ICMP	154 0.257	Echo (ping) reply	id=
10.59.1.142	10.60.242.3	ICMP	154	Echo (ping) reply	id=
10.60.164.33	119.36.128.43	ESP	208	ESP (SPI=0xc3aeb1b5)	
119.36.128.43	10.60.164.33	ESP	208	ESP (SPI=0xc7a95cf7)	
10.60.242.3	10.59.1.142	ICMP	154	Echo (ping) request	id=

Sopra il processo completo del ping e dei pacchetti scambiati da un sito all'altro che consiste di 6 pacchetti in totale.

1. Il 1° pacchetto 119.36.128.43 > 10.60.164.33 è il pacchetto ESP corrispondente al pacchetto PING inviato dal sito peer e ricevuto alla porta AF WAN
2. Il 2° pacchetto 10.60.242.3 > 10.59.1.142 è la richiesta ICMP inviata dal peer e ricevuta dal VPNTUN
3. Il 3° pacchetto 10.60.242.3 > 10.59.1.142 2 è la richiesta ICMP inviata dal peer e ricevuta alla porta AF LAN
4. Il 4° pacchetto 10.59.1.142 > 10.60.242.3 è il pacchetto di risposta ICMP dal lato locale e ricevuto dalla porta LAN AF
5. Il 5° pacchetto 10.59.1.142 > 10.60.242.3 è il pacchetto di risposta ICMP dal lato locale e ricevuto dal VPNTUN
6. Il 6° pacchetto 10.60.164.33 > 119.36.128.43 è l'AF incapsulato nel pacchetto PING dentro il pacchetto ESP e inviato fuori

Dopo aver compreso tutti e 6 i pacchetti, è più facile sapere quale parte causa il picco di latenza.

2017-08-31 16:47:55.008577
2017-08-31 16:47:55.008631
2017-08-31 16:47:55.008638
2017-08-31 16:47:55.008862
2017-08-31 16:47:55.008909
2017-08-31 16:47:55.008911

2° - 1° = Tempo impiegato per il decapsulamento da WAN a VPNTUN

3° - 2° = Tempo impiegato per la trasmissione della richiesta da VPNTUN a LAN

5° - 4° = Tempo impiegato per la trasmissione della risposta da LAN a VPNTUN

6° - 5° = Tempo impiegato per l'incapsulamento da VPNTUN a WAN

Da qui partiamo per determinare quale parte causa il problema di latenza.

## 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 Sangfor Server e versione firmware.
- ii. Screenshot dei log di sistema per entrambe le parti.
- iii. Quale passaggio 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>





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