



## **IPsec VPN**

# **Guida alla risoluzione dei problemi per l'impossibilità di accedere al lato peer con IPsec VPN integrata**



## Registro delle modifiche

| Data              | Descrizione dei Cambiamenti  |
|-------------------|--|
| Dicembre 17, 2019 | Guida alla risoluzione dei problemi per l'impossibilità di accedere al lato peer con IPsec VPN integrata |
|                   |  |

## 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 Errore di configurazione nella fase 2 .....                                | 2 |
| 4.3 Errore di configurazione di Application Control.....                       | 2 |
| 4.4 ESP senza risposta .....   | 3 |
| 5. Raccolta informazioni.....  | 4 |
| 6. Richiesta Documentazione .....  | 5 |

# 1. Descrizione del documento

Lo scopo di questo documento è fornire indicazioni per la risoluzione dei problemi per l'impossibilità di accedere al lato peer con IPsec VPN.

## 2. Versione applicabile

Questo documento è applicabile per il 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'impossibilità per accedere lato peer con VPN IPsec integrata in questo documento si riferisce allo scenario in cui i dispositivi Sangfor hanno costruito IPsec VPN con dispositivo di terze parti, ma non sono in grado di accedervi l'un l'altro.

L'impossibilità di accedere al lato peer con IPsec VPN integrata viene principalmente suddivisa nei seguenti scenari:

- Errore di configurazione nella fase 2
- Errore di configurazione di Application Control
- ESP senza risposta

## 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 non è possibile accedere al lato peer con IPsec VPN integrato:

1. Assicurati che sia il lato Sangfor che la terza parte 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, consigliare di utilizzare la modalità Aggressive mode.
5. Assicurati che il tunnel VPN IPsec sia stato creato

## 4.2 Errore di configurazione nella fase 2

Verificare se tutti i segmenti che consentono di comunicare con il lato peer siano configurati correttamente e lo stato della connessione VPN venga visualizzato nella pagina di Stato della VPN.

| Disconnect | Connection | Username | Description | Type           | Realtime Traffic (In/Out) | Internet IP | LAN IP  | Time Connected      | Protocol  |
|------------|------------|----------|-------------|----------------|---------------------------|-------------|---------|---------------------|-----------|
|            | HO1        |          |             | SANGFOR device | 0.00bps/0.00bps           | 222.127.    | 172.16. | 2019-12-17 13:09:42 | IPSEC_ESP |
|            | HO         |          |             | SANGFOR device | 0.00bps/1.06Kbps          | 222.127.    | 172.16. | 2019-12-17 13:09:42 | IPSEC_ESP |

Ogni voce creata nella fase 2 genererà una voce di connessione VPN nella pagina di Stato VPN.

Se il rispettivo segmento di rete non è visualizzato nella pagina di Stato VPN, controllare i criteri di fase 2 in entrata e in uscita per entrambe le parti.

## 4.3 Errore di configurazione di Application Control

Per alcuni dispositivi Sangfor come Sangfor NGAF, genererà automaticamente una zona "VPNTUN" quando Sangfor NGAF viene utilizzato per costruire VPN.

| Zone Name  | Forward Mode   | Interfaces |
|------------|----------------|------------|
| WAN        | Route(layer 3) | eth1,      |
| WAN        | Route(layer 3) | eth2,      |
| Internal   | Route(layer 3) | eth3,eth0  |
| Experiment | Route(layer 3) | eth4       |
| VPN        | Route(layer 3) | vpntun     |
| LabZone    | Route(layer 3) | eth6       |

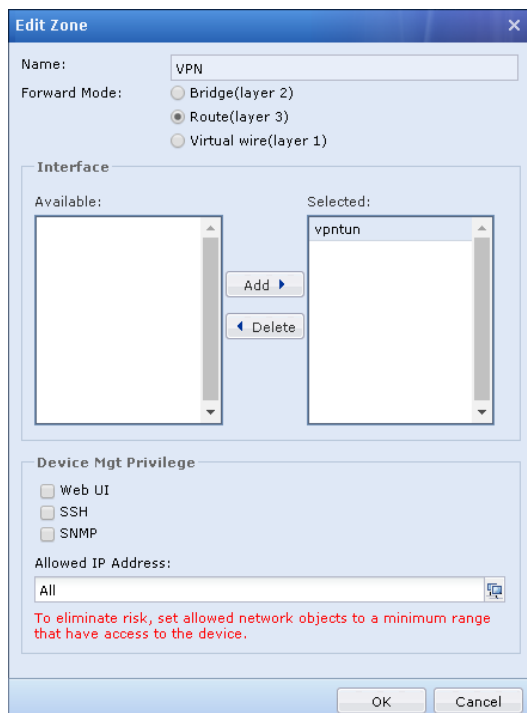
Per impostazione predefinita, il criterio di controllo delle applicazioni sangfor NGAF ha un criterio "Nega tutto (Deny All)". Pertanto, se la zona VPNTUN non è stata inclusa in alcun criterio di autorizzazione, il traffico sarà gestito nella policy "Nega tutto".

Al fine di prevenire e risolvere il problema, di seguito sono riportate le soluzioni:

1. Creare un criterio "Allow" (Consenti) e selezionare tutte le zone disponibili oppure LAN e VPN per l'area di origine e di destinazione., in modo che il traffico da LAN a VPN non venga negato dalla policy predefinita "Nega tutto".

| Priority | Name           | Group         | Src Zone | Source Network | Dst Zone | Destination Network | Service/Application    | Schedule |
|----------|----------------|---------------|----------|----------------|----------|---------------------|------------------------|----------|
| 1        | Allow          | Default group | WAN      | All            | WAN      | All                 | Predefined Service/any | All week |
| 2        | Default Policy | -             | All      | All            | All      | All                 | All/All                | All week |

2. Rimuovere il "vpntun" dalla zona. Passare a [Network] > [Interfaces] > [Zone], quindi fare clic su Zona VPN e "Elimina" vpntun da "Selezionato".



**Nota:** la rimozione di VPNTUN dalla zona comporterà l'impossibilità di controllare il traffico VPN con Application Control Policy e Bandwidth Management.

## 4.4 ESP senza risposta

ESP (Encapsulating Security Payload) è il pacchetto quando il traffico è stato incapsulato dal tunnel VPN e l'uscita dall'interfaccia WAN.

Di seguito è riportato l'esempio di ESP senza risposta:

HQ IP : 222.127.x.x

IP di filiale : 152.32.x.x

Il PC di Filiale è impossibilitato ad eseguire il ping ad un server che si trova presso la sede centrale. Dal pacchetto di acquisizione del Firewall della filiale è stato scoperto che l'ESP è stato inviato.

```
AF8.0.7.197 ~ # tcpdump -i any esp -nn -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
17:25:12.152969 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xcd), length 116
17:25:13.154035 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xce), length 116
17:25:14.156004 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xcf), length 116
17:25:15.166928 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd0), length 116
17:25:16.167953 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd1), length 116
17:25:17.170206 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd2), length 116
17:25:18.170987 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd3), length 116
17:25:19.172960 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd4), length 116
17:25:20.174898 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd5), length 116
17:25:21.176868 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd6), length 116
10 packets captured
10 packets received by filter
0 packets dropped by kernel
AF8.0.7.197 ~ #
```

Quindi, dal pacchetto di acquisizione HQ Firewall è emerso che l'ESP dal lato Filiale è stato ricevuto, ma non ha risposto.

```
2. 222.127. ~ # tcpdump -i any esp -nn -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
17:25:12.154974 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xcd), length 116
17:25:13.156022 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xce), length 116
17:25:14.159272 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xcf), length 116
17:25:15.168736 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd0), length 116
17:25:16.172859 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd1), length 116
17:25:17.172117 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd2), length 116
17:25:18.175769 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd3), length 116
17:25:19.176881 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd4), length 116
17:25:20.176809 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd5), length 116
17:25:21.179169 IP 152.32. > 222.127. : ESP(spi=0x41a86602,seq=0xd6), length 116
10 packets captured
10 packets received by filter
0 packets dropped by kernel
AF8.0.7.197 ~ #
```

Dai risultati di cui sopra, HQ non ha risposto ESP alla filiale. Ciò potrebbe essere causato da qualche dispositivo che ha bloccato il traffico o qualche configurazione errata.

## 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.

Le informazioni devono essere raccolte:

- i. Modello server e versione firmware di entrambi i lati.
- ii. Screenshot dei registri 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. Richiesta Documentazione**

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

