Sangfor VPN

Guida alla risoluzione dei problemi per alta latenza in Sangfor VPN

Registro delle modifiche

Data	Descrizione dei Cambiamenti
Settembre 12, 2019	Guida alla risoluzione dei problemi per alta latenza in Sangfor VPN

CONTENUTO

1. Descrizione del documento

Lo scopo di questo documento è fornire indicazioni per la risoluzione dei problemi su alta latenza con Sangfor VPN.

2. Versione applicabile

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

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

3. Scenario di problema

L'alta latenza con Sangfor VPN in questo documento si riferisce allo scenario in cui i dispositivi Sangfor costruiscono Sangfor VPN ma la latenza è elevata.

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

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

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 c'è una latenza elevata con Sangfor VPN:

1. Traceroute verso l'IP di destinazione, assicurarsi che non ci sia Loop nel mezzo
2. Assicurati che il traffico passi attraverso Sangfor VPN

4.2 Rete instabile

Questo può essere rilevato eseguendo il ping dell'indirizzo IP pubblico del sito peer. Se è presente anche la rete pubblica, il problema è molto probabilmente causato dalla rete pubblica.

4.3 Larghezza di banda insufficiente

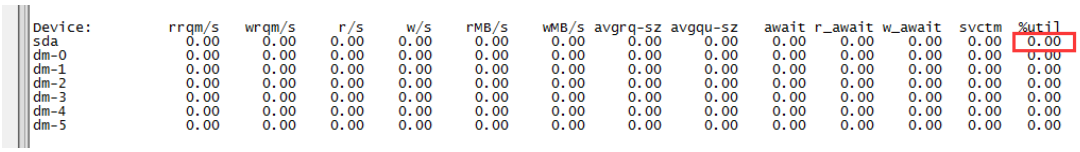
Se tutte le filiali hanno problemi, è necessario verificare se la larghezza di banda della sede centrale è utilizzata al massimo. Se c'è un problema con una sola filiale, allora non c'è modo di verificare se la filiale ha utilizzato appieno la larghezza di banda.

Se il dispositivo Sangfor è direttamente collegato alla rete pubblica, possiamo controllare direttamente il traffico in tempo reale della porta di rete.

4.4 Collo di bottiglia delle prestazioni

Accedere alla Web Console per verificare l'utilizzo della CPU del dispositivo. Se la CPU usage è molto alta, ciò potrebbe comportare un'elevata latenza con VPN.

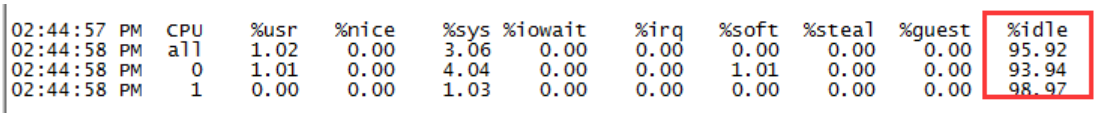
Controlla l'I/O del disco con il comando: **iostat –mx 1**



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**



	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%idle
02:44:57 PM	all	1.02	0.00	3.06	0.00	0.00	0.00	0.00	0.00	95.92
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 inattiva del dispositivo è molto bassa.

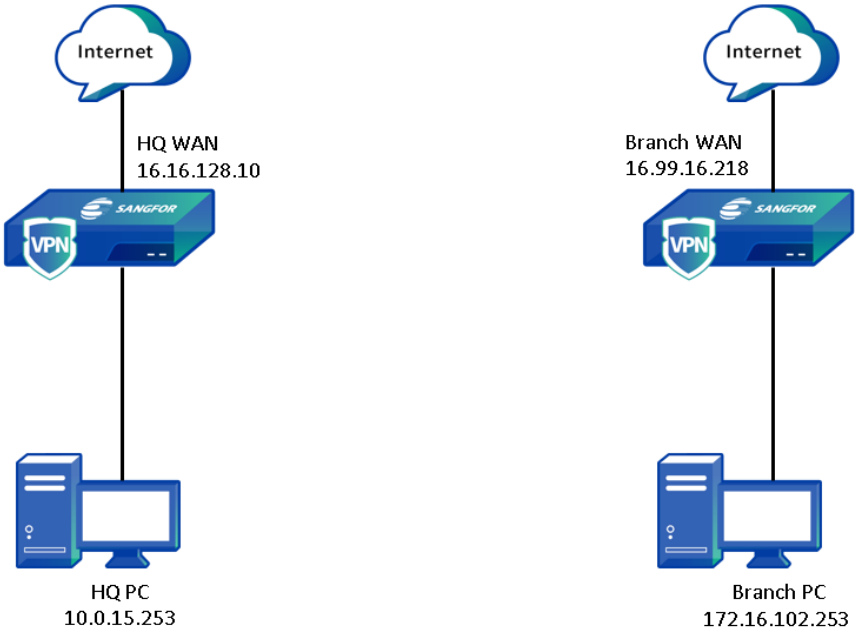
4.5 Gestione della larghezza di banda

Controlla se il dispositivo VPN ha il controllo del flusso o la funzione di gestione della larghezza di banda. Se esiste un criterio di restrizione, disabilitare il controllo del flusso per eliminarne l'impatto.

5. Risoluzione avanzata dei problemi

Acquisisci pacchetti e analizzali per scoprire la possibile causa principale dell'alta latenza.

Scenario di esempio:



Prima di acquisire il pacchetto, eseguire il comando Ping da Branch PC a HQ PC con il seguente comando: **ping 10.0.15.253 -s 400 -I 172.16.102.253**

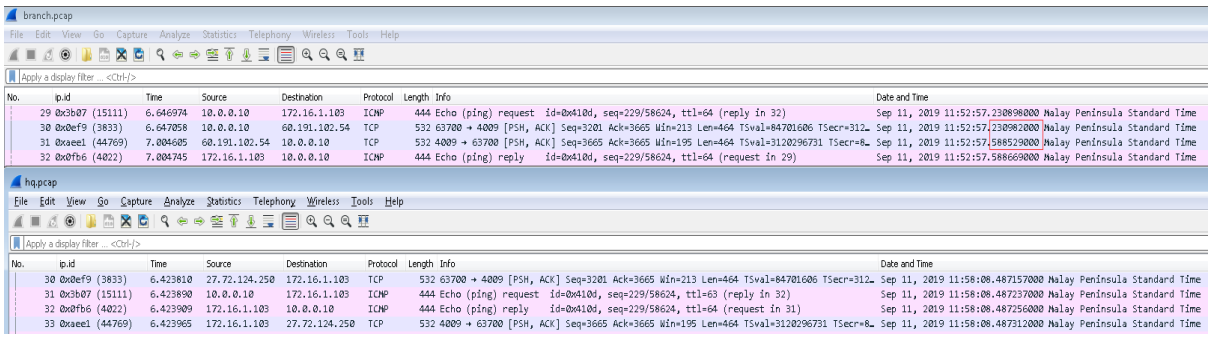
Comando utilizzato per acquisire il pacchetto nel dispositivo HQ:

tcpdump -i any -nnv \(host 10.0.15.253 o host 16.99.16.218) e \(ip[2:2]=428 o ip[2:2]=516 o ip[2:2]=508\) -w /tmp/hq.pcap

Comando utilizzato per acquisire il pacchetto nel dispositivo Branch :

tcpdump -i any -nnv \(host 10.0.15.253 o host 16.16.128.10\) e \(ip[2:2]=428 o ip[2:2]=516 o ip[2:2]=508\) -w /tmp/branch.pcap

Interrompere l'acquisizione dei pacchetti quando si verifica il problema di latenza elevata. Quindi, scarica e raccogli entrambi i pacchetti.



Analizzare i pacchetti facendo riferimento ai pacchetti di esempio come sopra. Come da figura sopra, il pacchetto in alto è da Filiale mentre il pacchetto in basso è da HQ. L'analisi dovrebbe

iniziare dalla Filiale, perché il Ping è stato eseguito dalla Filiale ad HQ. Pertanto la Sorgente è dalla filiale al quartier generale.

Il processo completo è il seguente:

1. Facendo riferimento alla figura precedente, il primo pacchetto dalla filiale è il pacchetto ricevuto dall'interfaccia LAN del dispositivo della filiale
2. Il secondo pacchetto del ramo è il pacchetto che il dispositivo della Filiale ha incapsulato il pacchetto Ping e lo invia tramite il tunnel VPN

Ora, fai riferimento al pacchetto HQ perché il traffico è stato inviato dal lato Filiale.

3. Facendo riferimento alla figura sopra, il primo pacchetto dal quartier generale è il pacchetto incapsulato che ha ricevuto nel tunnel VPN del dispositivo HQ
4. Il secondo pacchetto dal quartier generale è il pacchetto che il dispositivo HQ ha decapsulato e invia alla destinazione dalla porta LAN HQ
5. Il terzo pacchetto dal quartier generale viene ricevuto dalla porta LAN, che è la risposta alla richiesta Ping
6. L'ultimo pacchetto dal quartier generale è il pacchetto che il dispositivo HQ incapsula il pacchetto e restituisce alla filiale

Quindi, fare riferimento al pacchetto Filiale perché il processo lato HQ è stato completato.

7. Il terzo pacchetto dalla filiale è il pacchetto incapsulato che ha ricevuto nel tunnel VPN che risponde dal lato HQ
8. L'ultimo pacchetto è il pacchetto che il dispositivo della Filiale ha inoltrato al pacchetto di risposta all'host

Dalla figura sopra, il problema della latenza può essere facilmente individuato dal secondo e terzo pacchetto Filiale. Prendere il tempo del terzo pacchetto Filiale e dedurre il tempo del secondo pacchetto Filiale, la sottrazione sarà di circa 360ms-370ms di latenza.

Riferendosi alla spiegazione precedente, il terzo pacchetto Filiale è il pacchetto incapsulato ricevuto nel tunnel VPN che risponde dal lato HQ. Pertanto, esiste una sola possibilità, che è causata dalla rete pubblica.

6. 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

7. 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