Risoluzione dei problemi di flap IGP, perdita di pacchetti o rimbalzo del tunnel su un tunnel VPN con EEM e SLA IP

Sommario

Introduzione

In questo documento viene descritta la procedura da seguire quando si verificano flap EIGRP/OSPF/BGP su un tunnel DMVPN/GRE/sVTI/FlexVPN.

Premesse

Per risolvere questo problema, è necessario rispondere alla prima domanda: "Si tratta di un problema di VPN, di protocollo di routing o di ISP?" Per rispondere alla domanda, è necessario eseguire i test di connettività sull'underlay (di solito Internet o una WAN privata) e sull'overlay (di solito il tunnel VPN) durante il flap/l'interruzione. Sfortunatamente questi eventi di flap possono essere transitori e intermittenti e di conseguenza può essere difficile eseguire questi test durante il tempo del problema. In questo documento vengono fornite indicazioni sull'utilizzo del contratto di servizio (SLA, Service Level Agreement) IP, sugli oggetti di rilevamento e su Embedded Event Manager (EEM) per la raccolta automatica di queste informazioni al momento del problema.

Informazioni sulle funzionalità

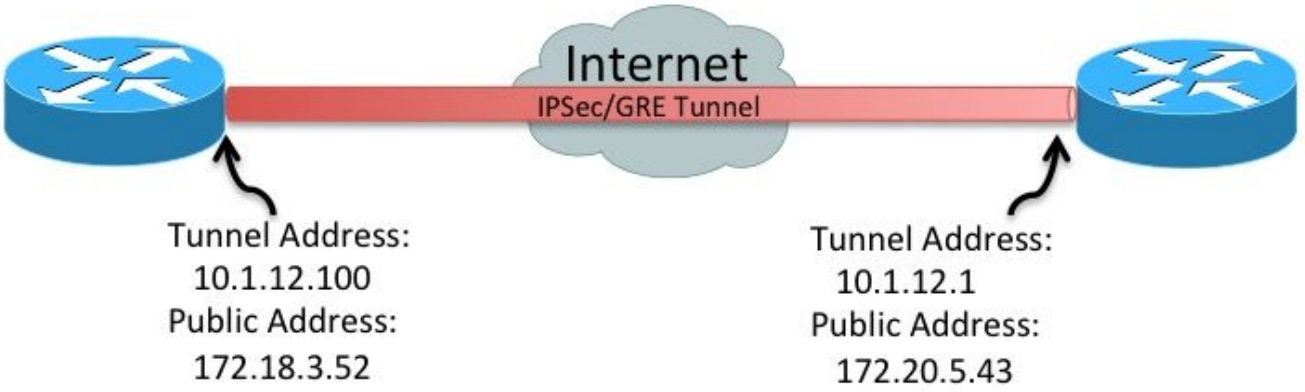
Gli SLA IP sono processi che vengono eseguiti sul router in background e verificano una serie di condizioni di rete. In questo documento, la connettività IP generale viene testata con "icmp-echo" test.

Un oggetto traccia può quindi tenere traccia dello stato del contratto di servizio IP. Quindi, con un'applet EEM, lo stato della rete può essere registrato nel buffer syslog quando l'oggetto track cambia.

Usare lo stato della rete registrato nella cronologia syslogs per comprendere lo stato della rete

durante il flap o l'interruzione e determinare se si è verificato un problema IGP (Interior Gateway Protocol), di crittografia o di trasporto.

Metodologia



Passaggio 1. Definire un contratto di servizio per tenere traccia della connessione sottostante (connettività Internet)

- Opzione A
  Indirizzo IP pubblico su indirizzo IP pubblico (172.18.3.52 > 172.20.5.43). Poiché il peer remoto in genere risponde all'ICMP, questo SLA deve essere definito su un solo dispositivo.

```
ip sla 100
    icmp-echo 172.20.5.43 source-interface FastEthernet4
    frequency 5
ip sla schedule 100 life forever start-time now
```

- Opzione B **Nota:** In alcuni ambienti, i pacchetti ICMP (Internet Control Message Protocol) vengono bloccati nella rete sottostante/di trasporto. In questi ambienti, udp-echo è possibile usare i pacchetti al posto di icmp-echo per SLA IP.
  Iniziatore SLA IP (router sinistro)

```
ip sla 100
 udp-echo 172.20.5.43 1501 source-ip 172.18.3.52 source-port 1501 control disable
 frequency 5
ip sla schedule 100 life forever start-time now
```

  Risponditore SLA IP (router destro)

```
ip sla responder
ip sla responder udp-echo ipaddress 172.20.5.43 port 1501
```

Passaggio 2. Definire un contratto di servizio per tenere traccia della sovrapposizione (connettività tunnel)

- Indirizzo IP del tunnel per l'indirizzo IP del tunnel (10.1.12.100 > 10.1.12.1)

```
ip sla 200
    icmp-echo 10.1.12.1 source-interface Tunnel100
    frequency 5
ip sla schedule 200 life forever start-time now
```

Questi SLA inviano un singolo pacchetto ogni cinque secondi ai peer definiti. Se il peer risponde, il contratto di servizio viene contrassegnato come "OK". Se non risponde, viene contrassegnato "Timeout". Gli oggetti traccia monitorano lo stato del contratto di servizio.

Passaggio 3. Definizione degli oggetti traccia per monitorare gli stati degli SLA

- Sottolinea oggetto traccia connettività

```
track 100 ip sla 100
   delay down 15 up 15
```

- Sovrapponi oggetto traccia connettività

```
track 200 ip sla 200
   delay down 15 up 15
```

Quando l'oggetto di rilevamento cambia, è possibile inserire un messaggio nei syslog.

Passaggio 4. Definire un'applet EEM da registrare quando gli oggetti traccia vengono modificati

- Creare un'applet EEM per quando il trasporto sottostante non riesce e un'altra per quando viene ripristinato

```
event manager applet ipsla100down
    event track 100 state down
    action 1.0 syslog msg "Underlay SLA probe failed!"
event manager applet ipsla100up
   event track 100 state up
   action 1.0 syslog msg "Underlay SLA probe came up!"
```

- Creare un'applet EEM per quando il trasporto di sovrapposizione non riesce e un'altra per quando viene ripristinato

```
event manager applet ipsla200down
    event track 200 state down
    action 1.0 syslog msg "Overlay SLA probe failed!"
event manager applet ipsla200up
   event track 200 state up
   action 1.0 syslog msg "Overlay SLA probe came up!"
```

Analisi dei dati

Quando si verifica un'interruzione, raccogliere l'output del **show log** cercare i messaggi SLA mostrati nella sezione precedente.

Esistono tre possibili scenari:

1. Entrambi gli accordi sui livelli di servizio falliscono. Ciò significa: La connettività di layer 3 tra i due peer nell'alloggiamento (Internet/MPLS) è stata interrotta. Ciò richiede ulteriori indagini.Non ci sono problemi con il tunnel. Ha fallito perché è una vittima dell'interruzione

della base.
2. Lo SLA fisico non ha esito negativo, a differenza dello SLA tunnel. Ciò significa: La connettività di livello 3 tra i due peer su Internet funziona correttamente.C'è un problema con il tunnel. Sono necessarie ulteriori indagini sul tunnel.
3. Nessuno dei due accordi sui livelli di servizio fallisce. Ciò significa: La connettività di livello 3 tra i due peer su Internet funziona correttamente.La connettività unicast di layer 3 tra i due peer nel tunnel funziona correttamente.Connettività multicast di livello 3 attraverso il tunnel sconosciuta. Per verificarlo, eseguire il ping dell'indirizzo multicast utilizzato dall'IGP.Se il test funziona, significa che l'applicazione presenta un problema (EIGRP/OSFP/BGP). Sono necessarie ulteriori indagini sul protocollo.