Balanceamento de carga L2TP e failover

Contents

Introduction

Este documento explica os recursos de um concentrador de acesso L2TP (LAC) que executa funções de balanceamento de carga e failover para vários servidores de rede L2TP (LNS).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Balanceamento de carga LNS

Ao usar o RADIUS para fornecer informações de túnel de rede de discagem privada virtual (VPDN) para um LAC, é possível encaminhar usuários do mesmo serviço de identificação de número discado (DNIS) ou domínio para vários LNS. Esse é um requisito quando os túneis e as sessões de entrada precisam ser compartilhados entre vários LNSs para auxiliar na distribuição de carga e oferecer níveis mais altos de redundância. Para habilitar o recurso de balanceamento de carga, os endereços IP para cada LNS que está disponível como um endpoint de túnel devem ser entregues no par atributo/valor do atributo específico do fornecedor (VSA) da Cisco.

```
Cisco:Avpair = "vpdn:ip-addresses=10.51.6.82,10.51.6.59"
```

O ',' é usado como delimitador para indicar que há vários pontos finais disponíveis para o LAC (você também pode usar um espaço como delimitador para indicar a mesma prioridade de pontos finais de túnel). O LAC seleciona qual endpoint usar com base na seleção aleatória do primeiro endereço IP não ativo entregue. Se estiver ocupado (o LAC não pode se conectar ao endereço IP), o próximo endereço IP será selecionado. Se não houver endereços IP não ativos disponíveis, a próxima seleção será baseada em um endereço IP que esteja em 'estado de túnel aberto' e, finalmente, um endereço IP que esteja 'estado de túnel pendente'.

Failover de LNS

O software Cisco IOS® permite um máximo de seis níveis de prioridade ao utilizar vários LNSs. Usando '/' como delimitador, você pode atribuir diferentes grupos de prioridade ao LNS que são baixados para o LAC. Isso permite que determinados LNSs operem como o LNS principal e outros como um backup. Como antes, os endpoints de túnel são entregues no par atributo/valor do Cisco VSA.

```
Cisco:Avpair = "vpdn:ip-addresses=10.51.6.82/10.51.6.59"
```

O delimitador '/' indica que 10.51.6.82 está no Grupo de Prioridade 1 e 10.51.6.59 está no Grupo de Prioridade 2.

Balanceamento de carga e failover de LNS

Épossível usar balanceamento de carga e failover no mesmo perfil. Isso é obtido usando o par de atributos/valores do Cisco VSA `"vpdn:ip-addresses"`, como mostrado aqui:

```
Cisco:Avpair = "vpdn:ip-addresses=
1.1.1.1,2.2.2.2/3.3.3.3,4.4.4.4/5.5.5.5,6.6.6.6"
```

Isto é interpretado como:

- os pontos finais de túnel 1.1.1.1 e 2.2.2.2 estão no grupo de prioridade 1
- os pontos finais de túnel 3.3.3.3 e 4.4.4.4 estão no grupo de prioridade 2
- os pontos finais de túnel 5.5.5.5 e 6.6.6.6 estão no Grupo de prioridade 3

A função de balanceamento de carga é executada no Grupo de prioridade 1 - não ativo/não ocupado, aberto, pendente. Se não houver nenhum disponível nesse nível de prioridade, vá para o próximo nível de prioridade e continue a lógica de seleção.

Teste de laboratório

O teste nesta seção mostra três cenários diferentes para o uso dos recursos de balanceamento de carga e failover:

- Balanceamento de carga de LNS usando pares de atributo/valor específicos do fornecedor da Cisco
- Failover de LNS usando pares de atributo/valor específicos do fornecedor da Cisco
- Balanceamento de carga e failover de LNS usando pares de atributo/valor específicos do fornecedor da Cisco

Balanceamento de carga de LNS usando pares de atributos/valores específicos do fornecedor da Cisco

Perfil RADIUS

Perfis de túnel e usuário RADIUS no Merit RADIUS Server 3.6B:

```
2500-1 Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
Framed-IP-Address = 255.255.255.255

dnis:614629 Password = "cisco"
Service-Type = Outbound,
Cisco:Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Avpair = "vpdn:tunnel-id=hgw",
Cisco:Avpair = "vpdn:ip-addresses=10.51.6.82,10.51.6.59",
Cisco:Avpair = "vpdn:l2tp-tunnel-password=hello"
```

LAC - Configuração

```
aaa new-model
!--- Enables Authentication, Authorization and Accounting functionality. aaa group server radius
NSA_LAB server 10.51.6.3 auth-port 1645 acct-port 0 non-standard ! aaa authentication login
default local aaa authentication ppp default local group NSA_LAB aaa authentication ppp DIAL
group NSA_LAB local aaa authorization network default group NSA_LAB local aaa authorization
network DIAL group NSA_LAB local !--- Authentication and Authorization will be implemented !---
in sequence by the methods configured. vpdn enable !--- Enables the VPDN feature. no vpdn
logging vpdn search-order dnis !--- Once LCP state is open, the dialed number is checked !--- to
see if the remote is a VPDN user. interface Serial0:15 no ip address encapsulation ppp no
logging event link-status dialer rotary-group 1 dialer-group 1 autodetect encapsulation ppp v120
no snmp trap link-status isdn switch-type primary-net5 isdn incoming-voice modem compress stac !
interface Dialer1 ip unnumbered Loopback0 encapsulation ppp no ip mroute-cache dialer-group 1
autodetect encapsulation ppp v120 !--- Allows the encapsulation type to be dynamically set if
the call !--- type is not identified in the ISDN Q.931 Lower Layer Compatibility. peer default
ip address pool default compress stac ppp authentication chap pap DIAL ppp authorization DIAL !-
-- The list-name DIAL is configured, that PPP Authentication and !--- Authorization will use.
ppp chap hostname 5300-1 !--- The name 5300-1 is used for all CHAP challenge and response on !--
- this interface. ppp multilink ! radius-server host 10.51.6.3 auth-port 1645 acct-port 1646
non-standard !--- 'non-standard' indicates that the RADIUS Server will use !--- non standard
RADIUS attributes.
```

LNS - Configuração

```
aaa new-model
!--- Enables Authentication, Authorization and Accounting functionality. aaa authentication
login default local aaa authentication enable default group radius enable aaa authentication ppp
default local aaa authentication ppp vpdn group radius none aaa authorization network default
local none aaa authorization network vpdn group radius local !--- Authentication and
Authorization will be implemented !--- in sequence by the methods configured. vpdn enable !---
Enables the VPDN feature. vpdn-group 1 accept-dialin protocol l2tp virtual-template 1 local name
l2tp-gw l2tp tunnel password 7 1211001B1E04 !--- The LNS will accept connections from the LAC
using L2TP !--- using All Virtual-Access Interfaces that are created will be cloned from !---
Virtual-Template 1. The name 'l2tp-gw' is used to identify the password, !--- that will
authenticate the tunnel, is encrypted. interface Ethernet5/0 ip address 10.51.6.59 255.255.252.0
! interface Virtual-Template1 ip unnumbered Ethernet5/0 no ip route-cache cef peer default ip
address pool default ppp authentication chap vpdn ppp authorization vpdn ! radius-server host
10.51.6.3 auth-port 1645 acct-port 1646 non-standard !--- 'non-standard' identifies the RADIUS
Server will be !--- using nonstandard RADIUS attributes.
```

Depurações retiradas do LAC

```
Jan 1 00:32:54.847: %LINK-3-UPDOWN: Interface Serial0:0, changed state to up
Jan 1 00:32:55.027: Se0:0 PPP: Treating connection as a callin
Jan 1 00:32:55.027: Se0:0 PPP: Phase is ESTABLISHING, Passive Open
Jan 1 00:32:55.027: Se0:0 CHAP: Using alternate hostname 5300-1
Jan 1 00:32:55.027: Se0:0 LCP: State is Listen
Jan 1 00:32:55.027: Se0:0 LCP: I CONFREQ [Listen] id 112 len 10
- snip -
Jan 1 00:32:55.063: Se0:0 LCP: State is Open
Jan 1 00:32:55.063: Se0:0 PPP: Phase is AUTHENTICATING, by this end
Jan 1 00:32:55.063: Se0:0 CHAP: Using alternate hostname 5300-1
Jan 1 00:32:55.063: Se0:0 CHAP: O CHALLENGE id 14 len 27 from "5300-1"
Jan 1 00:32:55.083: Se0:0 CHAP: I RESPONSE id 14 len 27 from "2500-1"
Jan 1 00:32:55.083: Se0:0 PPP: Phase is FORWARDING
Jan 1 00:32:55.083: Se0:0 VPDN: Got DNIS string 614629
Jan 1 00:32:55.083: Se0:0 VPDN: Looking for tunnel -- dnis:614629 --
Jan 1 00:32:55.083: Serial0:0 AAA/AUTHOR/VPDN (480033158):
Port='Serial0:0' list='default' service=NET
Jan 1 00:32:55.083: AAA/AUTHOR/VPDN: Serial0:0 (480033158) user='dnis:614629'
Jan 1 00:32:55.087: Serial0:0 AAA/AUTHOR/VPDN (480033158): send AV service=ppp
Jan 1 00:32:55.087: Serial0:0 AAA/AUTHOR/VPDN (480033158): send AV protocol=vpdn
Jan 1 00:32:55.087: Serial0:0 AAA/AUTHOR/VPDN (480033158): found list "default"
Jan 1 00:32:55.087: Serial0:0 AAA/AUTHOR/VPDN (480033158): Method=NSA_LAB (radius)
Jan 1 00:32:55.087: RADIUS: Initial Transmit Serial0:0 id 50 10.51.6.3:1645,
Access-Request, len 100
Jan 1 00:32:55.087: Attribute 4 6 0A330644
Jan 1 00:32:55.087: Attribute 5 6 00000000
Jan 1 00:32:55.087: Attribute 26 17 00000009020B5365
Jan 1 00:32:55.087: Attribute 61 6 00000002
Jan 1 00:32:55.087: Attribute 1 13 646E6973
Jan 1 00:32:55.087: Attribute 30 8 36313436
Jan 1 00:32:55.087: Attribute 2 18 F0AF3BC4
Jan 1 00:32:55.087: Attribute 6 6 00000005
Jan 1 00:32:55.091: RADIUS: Received from id 50 10.51.6.3:1645,
Access-Accept, len 167
Jan 1 00:32:55.091: Attribute 6 6 00000005
Jan 1 00:32:55.091: Attribute 26 29 0000000901177670
Jan 1 00:32:55.091: Attribute 26 26 0000000901147670
Jan 1 00:32:55.091: Attribute 26 47 0000000901297670
Jan 1 00:32:55.091: Attribute 26 39 0000000901217670
 !--- LAC receives a call, negotiates PPP, LCP is declared Open, !--- the dialed number is
queried to ascertain if this is a VPDN customer. !--- VPDN attempts to find an existing tunnel
for the user, queries RADIUS for !--- the tunnel information. Jan 1 00:32:55.091: RADIUS: saved
authorization data for user 61F40024 at 61F9813C Jan 1 00:32:55.091: RADIUS: cisco AVPair
```

"vpdn:tunnel-type=l2tp" Jan 1 00:32:55.091: RADIUS: cisco AVPair "vpdn:tunnel-id=hgw" Jan 1 00:32:55.091: RADIUS: cisco AVPair "vpdn:ip-addresses=10.51.6.82,10.51.6.59" Jan 1 00:32:55.095: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=hello" Jan 1 00:32:55.095: AAA/AUTHOR (480033158): Post authorization status = PASS_ADD Jan 1 00:32:55.095: AAA/AUTHOR/VPDN: Processing AV service=ppp Jan 1 00:32:55.095: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn Jan 1 00:32:55.095: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp Jan 1 00:32:55.095: AAA/AUTHOR/VPDN: Processing AV tunnel-id=hgw **Jan 1 00:32:55.095: AAA/AUTHOR/VPDN: Processing AV ip-addresses=**
10.51.6.82,10.51.6.59
Jan 1 00:32:55.095: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=hello
Jan 1 00:32:55.095: Se0:0 VPDN/RPMS/: Got tunnel info for dnis:614629
Jan 1 00:32:55.095: Se0:0 VPDN/RPMS/: LAC hgw
Jan 1 00:32:55.095: Se0:0 VPDN/RPMS/: l2tp-busy-disconnect yes
Jan 1 00:32:55.095: Se0:0 VPDN/RPMS/: l2tp-tunnel-password xxxxxx
Jan 1 00:32:55.095: Se0:0 VPDN/RPMS/: 2 IP addresses
Jan 1 00:32:55.095: Se0:0 VPDN/RPMS/: IP 10.51.6.82 Priority 1
Jan 1 00:32:55.095: Se0:0 VPDN/RPMS/: IP 10.51.6.59 Priority 1
Jan 1 00:32:55.095: Se0:0 VPDN/: curlvl 1 Address 0: 10.51.6.82, priority 1
Jan 1 00:32:55.095: Se0:0 VPDN/: Select non-active address 10.51.6.82, priority 1
!--- The tunnel information is downloaded, using Cisco VSA. Two LNS IP !--- Addresses are used with a ',' as the delimiter, indicating that both !--- have equal priority. In this case 10.51.6.82 is selected as the tunnel !--- endpoint. Jan 1 00:32:55.095: Se0:0 VPDN: Find LNS process created Jan 1 00:32:55.095: Tnl 49467 L2TP: SM State idle Jan 1 00:32:55.095: Tnl 49467 L2TP: O SCCRQ Jan 1 00:32:55.099: Tnl 49467 L2TP: Tunnel state change from idle to wait-ctl-reply Jan 1 00:32:55.099: Tnl 49467 L2TP: SM State wait-ctl-reply **Jan 1 00:32:55.099: Se0:0 VPDN: Forward to address 10.51.6.82**
Jan 1 00:32:55.099: Se0:0 VPDN: Pending
Jan 1 00:32:55.099: Se0:0 VPDN: Process created
Jan 1 00:32:55.191: Tnl 49467 L2TP: I SCCRP from l2tp-gw
Jan 1 00:32:55.191: Tnl 49467 L2TP: Got a challenge from remote peer, l2tp-gw
Jan 1 00:32:55.191: Tnl 49467 L2TP: Got a response from remote peer, l2tp-gw
Jan 1 00:32:55.191: Tnl 49467 L2TP: Tunnel Authentication success
Jan 1 00:32:55.191: Tnl 49467 L2TP: Tunnel state change from wait-ctl-reply to established
Jan 1 00:32:55.191: Tnl 49467 L2TP: O SCCCN to l2tp-gw tnlid 62193
Jan 1 00:32:55.195: Tnl 49467 L2TP: SM State established
Jan 1 00:32:55.195: Tnl/Cl 49467/16 L2TP: Session FS enabled
Jan 1 00:32:55.195: Tnl/Cl 49467/16 L2TP: Session state change from idle to wait-for-tunnel
Jan 1 00:32:55.195: Se0:0 Tnl/Cl 49467/16 L2TP: Create session
Jan 1 00:32:55.195: Tnl 49467 L2TP: SM State established
Jan 1 00:32:55.195: Se0:0 Tnl/Cl 49467/16 L2TP: O ICRQ to l2tp-gw 62193/0
Jan 1 00:32:55.195: Se0:0 Tnl/Cl 49467/16 L2TP: Session state change from wait-for-tunnel to wait-reply
Jan 1 00:32:55.195: Se0:0 VPDN: 2500-1 is forwarded
Jan 1 00:32:55.327: Se0:0 Tnl/Cl 49467/16 L2TP: O ICCN to l2tp-gw 62193/17
Jan 1 00:32:55.327: Se0:0 Tnl/Cl 49467/16 L2TP: Session state change from wait-reply to established
Jan 1 00:32:56.195: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0:0, changed state to up
Jan 1 00:33:00.851: %ISDN-6-CONNECT:Interface Serial0:0 is now connected to 2500-1
Jan 1 00:33:06.111: %ISDN-6-CONNECT: Interface Serial0:1 is now connected to N/A N/A
!--- Second call is received by the LAC, !--- the dialed number is a VPDN customer. Jan 1 00:33:35.027: As1 LCP: I CONFREQ [Closed] id 1 len 23 - snip - **Jan 1 00:33:39.275: As1 LCP: State is Open**
Jan 1 00:33:39.275: As1 PPP: Phase is AUTHENTICATING, by this end
Jan 1 00:33:39.275: As1 CHAP: Using alternate hostname 5300-1
Jan 1 00:33:39.275: As1 CHAP: O CHALLENGE id 2 len 27 from "5300-1"
Jan 1 00:33:39.383: As1 CHAP: I RESPONSE id 2 len 25 from "paul"
Jan 1 00:33:39.383: As1 PPP: Phase is FORWARDING
Jan 1 00:33:39.383: As1 VPDN: Got DNIS string 614629
Jan 1 00:33:39.383: As1 VPDN: Looking for tunnel -- dnis:614629 --
Jan 1 00:33:39.387: Async1 AAA/AUTHOR/VPDN (3019717950):

```
Port='Async1' list='default' service=NET
Jan 1 00:33:39.387: AAA/AUTHOR/VPDN: Async1 (3019717950) user='dnis:614629'
Jan 1 00:33:39.387: Async1 AAA/AUTHOR/VPDN (3019717950): send AV service=ppp
Jan 1 00:33:39.387: Async1 AAA/AUTHOR/VPDN (3019717950): send AV protocol=vpdn
Jan 1 00:33:39.387: Async1 AAA/AUTHOR/VPDN (3019717950): found list "default"
Jan 1 00:33:39.387: Async1 AAA/AUTHOR/VPDN (3019717950): Method=NSA_LAB (radius)
Jan 1 00:33:39.387: RADIUS: Initial Transmit Async1 id 52 10.51.6.3:1645,
Access-Request, len 97
Jan 1 00:33:39.387: Attribute 4 6 0A330644
Jan 1 00:33:39.387: Attribute 5 6 00000001
Jan 1 00:33:39.387: Attribute 26 14 0000000902084173
Jan 1 00:33:39.387: Attribute 61 6 00000000
Jan 1 00:33:39.387: Attribute 1 13 646E6973
Jan 1 00:33:39.387: Attribute 30 8 36313436
Jan 1 00:33:39.387: Attribute 2 18 E9164E4C
Jan 1 00:33:39.387: Attribute 6 6 00000005
Jan 1 00:33:39.391: RADIUS: Received from id 52 10.51.6.3:1645,
Access-Accept, len 167
Jan 1 00:33:39.391: Attribute 6 6 00000005
Jan 1 00:33:39.391: Attribute 26 29 0000000901177670
Jan 1 00:33:39.391: Attribute 26 26 0000000901147670
Jan 1 00:33:39.391: Attribute 26 47 0000000901297670
Jan 1 00:33:39.391: Attribute 26 39 0000000901217670
Jan 1 00:33:39.391: RADIUS: saved authorization data for user
621904CC at 61FAB9EC
Jan 1 00:33:39.391: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp"
Jan 1 00:33:39.391: RADIUS: cisco AVPair "vpdn:tunnel-id=hgw"
Jan 1 00:33:39.391: RADIUS: cisco AVPair "vpdn:ip-addresses=10.51.6.82,10.51.6.59"
Jan 1 00:33:39.391: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=hello"
Jan 1 00:33:39.395: AAA/AUTHOR (3019717950): Post authorization status = PASS_ADD
Jan 1 00:33:39.395: AAA/AUTHOR/VPDN: Processing AV service=ppp
Jan 1 00:33:39.395: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn
Jan 1 00:33:39.395: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
Jan 1 00:33:39.395: AAA/AUTHOR/VPDN: Processing AV tunnel-id=hgw
Jan 1 00:33:39.395: AAA/AUTHOR/VPDN:
Processing AV ip-addresses=10.51.6.82,10.51.6.59
Jan 1 00:33:39.395: AAA/AUTHOR/VPDN:
Processing AV l2tp-tunnel-password=hello
Jan 1 00:33:39.395: As1 VPDN/RPMS/: Got tunnel info for dnis:614629
Jan 1 00:33:39.395: As1 VPDN/RPMS/: LAC hgw
Jan 1 00:33:39.395: As1 VPDN/RPMS/: l2tp-busy-disconnect yes
Jan 1 00:33:39.395: As1 VPDN/RPMS/: l2tp-tunnel-password xxxxxx
Jan 1 00:33:39.395: As1 VPDN/RPMS/: 2 IP addresses
Jan 1 00:33:39.395: As1 VPDN/RPMS/: IP 10.51.6.82 Priority 1
Jan 1 00:33:39.395: As1 VPDN/RPMS/: IP 10.51.6.59 Priority 1
Jan 1 00:33:39.395: As1 VPDN/: curlvl 1 Address 1: 10.51.6.59, priority 1
Jan 1 00:33:39.395: As1 VPDN/: Select non-active address 10.51.6.59, priority 1
!--- The second non-active endpoint is selected 10.51.6.59 !--- and the control connection is
established. Jan 1 00:33:39.395: As1 VPDN: Find LNS process created Jan 1 00:33:39.395: Tnl
20770 L2TP: SM State idle Jan 1 00:33:39.395: Tnl 20770 L2TP: O SCCRQ Jan 1 00:33:39.399: Tnl
20770 L2TP: Tunnel state change from idle to wait-ctl-reply Jan 1 00:33:39.399: Tnl 20770 L2TP:
SM State wait-ctl-reply Jan 1 00:33:39.399: As1 VPDN: Forward to address 10.51.6.59
Jan 1 00:33:39.399: As1 VPDN: Pending
Jan 1 00:33:39.399: As1 VPDN: Process created
Jan 1 00:33:39.399: Tnl 20770 L2TP: I SCCRP from l2tp-gw
Jan 1 00:33:39.399: Tnl 20770 L2TP: Got a challenge from remote peer, l2tp-gw
Jan 1 00:33:39.399: Tnl 20770 L2TP: Got a response from remote peer, l2tp-gw
Jan 1 00:33:39.399: Tnl 20770 L2TP: Tunnel Authentication success
Jan 1 00:33:39.399: Tnl 20770 L2TP: Tunnel state change from
wait-ctl-reply to established
Jan 1 00:33:39.403: Tnl 20770 L2TP: O SCCCN to l2tp-gw tnlid 42921
Jan 1 00:33:39.403: Tnl 20770 L2TP: SM State established
Jan 1 00:33:39.403: As1 VPDN: Forwarding...
Jan 1 00:33:39.403: Tnl/Cl 20770/17 L2TP: Session FS enabled
```

```
Jan 1 00:33:39.403: Tnl/Cl 20770/17 L2TP: Session state change from
idle to wait-for-tunnel
Jan 1 00:33:39.403: As1 Tnl/Cl 20770/17 L2TP: Create session
Jan 1 00:33:39.403: Tnl 20770 L2TP: SM State established
Jan 1 00:33:39.403: As1 Tnl/Cl 20770/17 L2TP: O ICRQ to l2tp-gw 42921/0
Jan 1 00:33:39.403: As1 Tnl/Cl 20770/17 L2TP: Session state change from
wait-for-tunnel to wait-reply
Jan 1 00:33:39.403: As1 VPDN: paul is forwarded
Jan 1 00:33:39.407: As1 Tnl/Cl 20770/17 L2TP: O ICCN to l2tp-gw 42921/16
Jan 1 00:33:39.407: As1 Tnl/Cl 20770/17 L2TP: Session state change from
wait-reply to established
```