配置SD-WAN基于区域的防火墙(ZBFW)和路由泄 漏

目录

简介 <u>先决条件</u> <u>要求</u> 使用的组件 <u>背景信息</u> 配置 <u>网络图</u> 路由泄漏配置 <u>ZBFW配置</u> <u>这证</u> <u>故障排除</u> <u>方法1.从OMP表查找目的VPN</u> <u>方法2.借助平台命令查找目的VPN</u> <u>方法3.借助数据包跟踪工具查找目的VPN</u> <u>故障切换可能导致的问题</u>

简介

本文档介绍如何配置、验证基于区域的防火墙(ZBFW)并排除虚拟专用网络(VPN)之间的路由泄漏故障。

先决条件

要求

Cisco 建议您了解以下主题:

- 思科SD-WAN重叠提供初始配置
- vManage用户界面(UI)中的ZBFW配置
- •从vManage UI进行路由泄漏控制策略配置

使用的组件

为进行演示,使用了以下软件:

- 带20.6.2软件版本的思科SD-WAN vSmart控制器
- 带20.6.2软件版本的思科SD-WAN vManage控制器
- 两台Cisco IOS®-XE Catalyst 8000V虚拟边缘平台路由器,带17.6.2软件版本,在控制器模式

下运行

• 三台Cisco IOS-XE Catalyst 8000V虚拟边缘平台路由器,带17.6.2软件版本,在自治模式下运行

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

本文档说明路由器如何确定SD-WAN重叠中的目的VPN映射,以及如何验证和排除VPN之间的路由 泄漏故障。它还描述了当从不同VPN通告同一子网时路径选择的特性,以及由此可能产生哪些问题 。

配置

网络图



两台SD-WAN路由器都配置了基本参数,以便与SD-WAN控制器建立控制连接,并在它们之间建立数据平面连接。本文档不涉及此配置的详细信息。此表汇总了VPN、站点ID和区域分配。

	cE1	cE2
站点ID	11	12
VPN	30	10,20
系统IP	169.254.206.11	169.254.206.12

服务端的路由器在每个虚拟路由和转发(VRF)中配置了静态默认路由,这些路由指向对应的SD-WAN路由器。同样,SD-WAN边缘路由器配置了指向相应子网的静态路由。请注意,为了演示路由 泄漏和ZBFW的潜在问题,cE2服务端后面的路由器具有相同的子网192.168.12.0/24。在cE2后面的 两台路由器上,都有一个环回接口,配置为模拟具有相同IP地址192.168.12.12的主机。

请注意,Cisco IOS-XE路由器R10、R20和R30在SD-WAN边缘路由的服务端以自主模式运行,这 些路由器主要用于在本演示中模拟终端主机。SD-WAN边缘路由上的环回接口不能用于此目的,而 不能用于实际主机(如服务端路由器),因为源自SD-WAN边缘路由器VRF中的接口的流量不被视 为源自ZBFW区域的流量,而是属于边缘路由器的特殊自身区域。因此,不能将ZBFW区域视为与 VRF相同。对自身区域的详细讨论不属于本文的讨论范围。

路由泄漏配置

主要控制策略配置目标是允许所有路由从VPN 10和20泄漏到VPN 30。VRF 30仅存在于路由器 cE1上,VRF 10和20仅在路由器cE2上配置。为此,配置了两个拓扑(自定义控制)策略。以下是

将所有路由从VPN 10和20导出到VPN 30的拓扑。

\equiv Cisco v	Manage 🔗 S	elect Resource Group+	Configuration · Policies			୭ 🗘
View Custom Cont	rol Policy					
Name	LEAK_VPN10_20_t	to_30				
Description	Route leaking form	VPN 10,20 to 30				
Route	1	Route		Actions		Route
Default Action		VPN List: VPN Id	VPN_10_20	Accept Export To: VP	1_30	
		~				

请注意,Default Action(默认操作)设**置为Allow**(允许),以避免意外阻止TLOC通告或正常 VPN内路由通告。

≡ Cisco vM	anage 😯 Select Resource Group - Configuration - Policies	
View Custom Control	Policy	
Name	LEAK_VPN10_20_to_30	
Description	Route leaking form VPN 10,20 to 30	
E Route	Default Action Accept Enabled	

同样,拓扑策略也配置为允许从VPN 30向VPN 10和20反向通告路由信息。

≡ Cisco vMa	anage 🔿 🤅	Select Resource Group-	Configuration · Policies		$\bigcirc \equiv \bigcirc$	4
View Custom Control P	Policy					
Name	LEAK_VPN30_to_	io_10_20				
Description	Allow route leaking	king from VPN 30 to 10 and 20				
	.	Route				Route
	1	Match Conditions		Actions		
Default Action		VPN List:	VPN_30	Accept		
		VPN Id		Export To: V	PN_10_20	

■ Cisco vManage ⑦ Select Resource Group Configuration · Policies

View Custom Control P	View Custom Control Policy						
Name	EAK_VPN30_to_10_20						
Description	w route leaking from VPN 30 to 10 and 20						
Route	Default Action						
	Accept Enabled						
Default Action							

然后,两个拓扑策略都分配给在入口(传入)方向对应的站点列表。当从cE1(站点ID 11)收到来 自VPN 30的路由时,vSmart控制器会将其导出到VPN 10和20的重叠管理协议(OMP)表。

≡ Cisco vMa	nage 🕜 Select Re	source Group-	Configuration · Policies		
Centralized Policy > E	dit Policy	_			
		Policy A	Application Topology Traffic R	ules	
Add policies to sites	and VPNs				
Policy Name	ROUTE_LEAKING				
Policy Description	Route Leaking Policy				
New Site List Direction		Site List		Action	
in		SITE_11		/ 1	
		Preview	Save Policy Changes	Cancel	

同样,在收到来自cE2的VPN 10和20路由(站点ID 12)时,vSmart会将来自VPN 10和20的路由导 出到VPN 30路由表中。

entralized Policy > E	dit Policy				
		Policy	Application Topology Traffic Rules		
Add policies to sites	and VPNs				
Policy Name	ROUTE_LEAKING				
Policy Description	Route Leaking Policy				
opology Appli	cation-Aware Routing	Traffic Data	Cflowd		
AK VDN10 20	to 20				CUSTOM CONT
EAK_VPINTU_20	_10_30				COSTOM CONT
_					
New Site List					
New Site List					
New Site List Direction		Site List		Action	
+ New Site List		Site List		Action	
(+) New Site List		Site List SITE_12		Action	
New Site List irection		Site List SITE_12		Action	
New Site List		Site List SITE_12		Action	
New Site List		Site List SITE_12		Action	
New Site List		Site List		Action	

此外,还提供完整的控制策略配置预览以供参考。

viptela-policy:policy control-policy LEAK_VPN10_20_to_30 sequence 1 match route vpn-list VPN_10_20 prefix-list _AnyIpv4PrefixList ! action accept export-to vpn-list VPN_30 ! ! defaultaction accept ! control-policy LEAK_VPN30_to_10_20 sequence 1 match route vpn-list VPN_30 prefix-list _AnyIpv4PrefixList ! action accept export-to vpn-list VPN_10_20 ! ! default-action accept ! lists site-list SITE_11 site-id 11 ! site-list SITE_12 site-id 12 ! vpn-list VPN_10_20 vpn 10 vpn 20 ! vpn-list VPN_30 vpn 30 ! prefix-list _AnyIpv4PrefixList ip-prefix 0.0.0.0/0 le 32 ! ! apply-policy site-list SITE_12 control-policy LEAK_VPN10_20_to_30 in ! site-list SITE_11 control-policy LEAK_VPN30_to_10_20 in ! !

必须从vManage控制器配置(vManage controller Configuration)>**策略(Policies)部**分激活策略,才能 在vSmart控制器上生效。

ZBFW配置

日标区域

下表总结了ZBFW,以便过滤本文演示的需求。

百尔区域 源区域	VPN_10	VPN_20	VPN_30
VPN_10	区域内允许	拒绝	拒绝
VPN_20	拒绝	区域内允许	允许
VPN_30	允许	拒绝	区域内允许

主要目标是允许从路由器cE1 VPN 30的服务端发往VPN 10但不发往VPN 20的任何Internet控制消息协议(ICMP)流量。必须自动允许返回流量。



此外,必须允许来自路由器cE2服务端VPN 20的任何ICMP流量传输到cE1的VPN 30服务端,但不 允许从VPN 10。必须自动允许从VPN 30到VPN 20的返回流量。

≡ Cisco	vManage 🛛 🖓 🤅	Select Resource G	iroup -		Configura	ation · Security				\bigcirc	04
Edit Firewall Polie	cy	Sour	rces VPN_20		Apply Zond	e-Pairs		Destinations VPN_30		×	
Name	VPN_20_to_30					Description	Allow to initiate ICMP fro	m VPN 20 to 30			
Q Search											∇
Add Rule/Rule	e Set Rule ∽										
Default Action D	rop ¢									Tota	al Rows: 0 🔅
Order	Name	Rule Sets	Action	Log	Source Data Prefix	Source Port	Destination Data Pref	ix Destination Port	Protocol	Application L	ist To Drc
Θ 1	Rule 1	N/A	Inspect	N/A	192.168.20.0/24	Any	192.168.30.0/24	Any	1	Any	
Θ 2	Rule 2	N/A	Inspect	N/A	192.168.12.0/24	Any	192.168.30.0/24	Any	1	Any	•••
					Save Firewall Policy	Cane	el				

≡ Cisco	v Manage	⑦ Select Resource Group ▼	Configur	ration · Secur	ity		\bigcirc	Ξ	04	2
Security > A Firewall	dd Security Policy	evention URL Filtering	- Advanced Malwa			TLS/SSL Decryption		Pol		
Q Search										7
Add Firewall Po	licy 🗸 (Add a Firev	vall configuration)					Total R	lows: 2	Q	曫
Name	Туре	Description	Reference Count	Updated By	Last Updated 🔺					
VPN_30_to_10	🖪 zoneBasedFW	Allow to initiate ICMP from VPN 30 to 10	0	enk	25 Feb 2022 5:05:25 PM CET					
VPN_20_to_30	C zoneBasedFW	Allow to initiate ICMP from VPN 20 to 30	0	enk	25 Feb 2022 5:06:23 PM CET					

在此,您可以找到ZBFW策略预览以供参考。

policy zone-based-policy VPN_20_to_30 sequence 1 seq-name Rule_1 match source-ip 192.168.20.0/24 destination-ip 192.168.30.0/24 protocol 1 ! action inspect ! ! sequence 11 seq-name Rule_2 match source-ip 192.168.12.0/24 destination-ip 192.168.30.0/24 protocol 1 ! action inspect ! ! default-action drop ! zone-based-policy VPN_30_to_10 sequence 1 seq-name Rule_1 match source-ip 192.168.30.0/24 destination-ip 192.168.10.0/24 protocol 1 ! action inspect ! ! sequence 11 seq-name Rule_2 match protocol 1 source-ip 192.168.30.0/24 destination-ip 192.168.10.0/24 protocol 1 ! action inspect ! ! sequence 11 seq-name Rule_2 match protocol 1 source-ip 192.168.30.0/24 destination-ip 192.168.12.0/24 ! action inspect ! ! default-action drop ! zone VPN_10 vpn 10 ! zone VPN_20 vpn 20 ! zone VPN_30 vpn 30 ! zone-pair ZP_VPN_20_VPN_30_VPN_20_to_30 source-zone VPN_20 destination-zone VPN_30 zone-policy VPN_20_to_30 ! zone-pair ZP_VPN_30_VPN_10_VPN_30_to_10 source-zone VPN_30 destination-zone VPN_10 zone-policy VPN_30_to_10 ! zone-to-nozone-internet deny !

Cancel

要应用安全策略,必须在设备模板的"其**他模**板"部分的"安全策略"下**拉菜单**部分下分配该策略。

■ Cisco vManage	e 🕜 Select Resource Grou	p▼ Config	juration · Templates	3		\bigcirc	≡ 0	
		Devi	ce Feature					
Basic Information T	ransport & Management VPN	Service VPN	Cellular Ac	dditional Templates	Switchport			
Additional Templates								
AppQoE	Choose	¥						
Global Template *	Factory_Default_Global_CISCO	D_Templ 🔻 🤅)					
Cisco Banner	Choose	•						
Cisco SNMP	Choose	•						
TrustSec	Choose	•						
CLI Add-On Template	Choose	¥						
Policy	Choose	¥						
Probes	Choose	¥						
Security Policy	TEST_SECURITY_POLICY	•						
	None		Empty template selection.					
Switch Port + Switch Port	~							
		Update	Cancel					

更新设备模板后,安全策略将在应用安全策略的设备上变为活动状态。为了在本文档中进行演示 ,仅在cE1路由器上启用安全策略已足够。

验证

现在,您需要验证所需的安全策略(ZBFW)目标是否已实现。

使用ping测试可确认从区域VPN 10到VPN 30的流量会按预期被拒绝,因为没有为从VPN 10到VPN 30的流量配置区域对。

R10#ping 192.168.30.30 source 192.168.10.10 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of 192.168.10.10 Success rate is 0 percent (0/5) R10#ping 192.168.30.30 source 192.168.12.12 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of 192.168.12.12 Success rate is 0 percent (0/5)

同样,安全策略配置允许来自VPN 20的流量按照预期到达VPN 30。

R20#ping 192.168.30.30 source 192.168.20.20 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of

192.168.20.20 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms R20#ping 192.168.30.30 source 192.168.12.12 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of 192.168.12.12 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms 策略配置允许从VPN 30到区域VPN 10中子网192.168.10.0/24的流量按预期。

R30#ping 192.168.10.10 source 192.168.30.30 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds: Packet sent with a source address of 192.168.30.30 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms 拒绝从VPN 30到区域VPN 20中子网192.168.20.0/24的流量,因为没有为此流量配置区域对(预期)。

R30#ping 192.168.20.20 source 192.168.30.30 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds: Packet sent with a source address of 192.168.30.30 Success rate is 0 percent (0/5)

当您尝试ping IP地址192.168.12.12时,可以观察到其他您感兴趣的结果,因为该地址可能位于区域 VPN 10或VPN 20中,并且从位于SD-WAN边缘路由器cS服务端的路由器R30的角度无法确定目的 VPNe1。

R30#ping 192.168.12.12 source 192.168.30.30 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds: Packet sent with a source address of 192.168.30.30 Success rate is 0 percent (0/5)

VRF 30中所有源的结果相同。这确认了它不依赖于等价多路径(ECMP)哈希函数结果:

R30#ping 192.168.12.12 source 192.168.30.31 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds: Packet sent with a source address of 192.168.30.31 Success rate is 0 percent (0/5) R30#ping 192.168.12.12 source 192.168.30.32 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds: Packet sent with a source address of 192.168.30.32 Success rate is 0 percent (0/5)

根据目标IP 192.168.12.12的测试结果,您只能猜测它位于VPN 20中,因为它不响应ICMP回应请求 ,而且很可能会被阻止,因为没有配置区域对来允许从VPN 30到VPN 20(根据需要)的流量。 如 果IP地址相同的目标192.168.12.12位于VPN 10中,并假设该目标响应ICMP回应请求,则根据VPN 30到VPN 20的ICMP流量的ZBFW安全策略,必须允许流量。您必须确认目标VPN。

故障排除

方法1.从OMP表查找目的VPN

简单检查cE1上的路由表并不有助于了解实际目的VPN。从输出中可以获得的最有用信息是目标的 系统IP(169.254.206.12),并且没有发生ECMP。

cE1# show ip route vrf 30 192.168.12.0 255.255.255.0 Routing Table: 30 Routing entry for 192.168.12.0/24 Known via "omp", distance 251, metric 0, type omp Last update from 169.254.206.12 on Sdwan-system-intf, 01:34:24 ago Routing Descriptor Blocks: * 169.254.206.12 (default), from 169.254.206.12, 01:34:24 ago, via Sdwan-system-intf Route metric is 0, traffic share count is 1

要查找目的VPN,首先需要从cE1上的OMP表中查找目的前缀的服务标签。

cE1#show sdwan omp routes vpn 30 192.168.12.0/24 Generating output, this might take time, please wait ... Code: C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Inv -> invalid Stg -> staged IA -> On-demand inactive U -> TLOC unresolved PATH ATTRIBUTE FROM PEER ID LABEL STATUS TYPE TLOC IP COLOR ENCAP PREFERENCE ---

------ 169.254.206.4 12 1007 C,I,R installed 169.254.206.12 private2 ipsec - 我们可以看到标签值为1007。最后,如果在vSmart控制器上检查了来自具有系统IP 169.254.206.12的路由器的所有服务,则可以找到目的VPN。

方法2.借助平台命令查找目的VPN

要借助平台命令查找目标VPN,首先需要借助show ip vrf detail 30或show platform software ip f0 cef table * summary 命令在cE1路由器上获取VPN 30的内部VRF ID。

cE1#show ip vrf detail 30 | i Id VRF 30 (VRF Id = 1); default RD 1:30; default VPNID 在这种情况下, VRF ID 1被分配给名为30的VRF。平台命令显示SD-WAN软件中对象的输出链元素 (OCE)链,这些对象代表在Cisco IOS-XE软件中确定数据包路径的内部转发逻辑:

cE1#show platform software ip F0 cef table index 1 prefix 192.168.12.0/24 oce === Prefix OCE === Prefix/Len: 192.168.12.0/24 Next Obj Type: OBJ_SDWAN_NH_SLA_CLASS Next Obj Handle: 0xf800045f, urpf: 0 Prefix Flags: unknown aom id: 1717, HW handle: 0x561b60eeba20 (created) 感兴趣的前缀指向ID为0xf800045f的服务级别协议(SLA)类类型(OBJ_SDWAN_NH_SLA_CLASS)的下一跳对象,可进一步验证,如下所示:

cE1#show platform software sdwan F0 next-hop sla id 0xf800045f SDWAN Nexthop OCE SLA: num_class 16, client_handle 0x561b610c3f10, ppe addr 0xdbce6c10 SLA_0: num_nhops 1, Fallback_sla_flag TDL_FALSE, nhobj_type SDWAN_NH_INDIRECT ECMP: 0xf800044f SLA_1: num_nhops 0, Fallback_sla_flag TDL_FALSE, nhobj_type ADJ_DROP ECMP: 0xf800000f 0xf800000f

这是长输出,因此跳过了2到15的SLA类,因为没有配置回退SLA类,并且所有类指向与SLA 1相同 的特殊DROP邻接。主要关注来自SLA 0的间接类型(SDWAN_NH_INDIRECT)的下一跳对象。我们 还可以注意,没有ECMP和所有ID相同(0xf800044f)。 可以进一步验证是否找到最终目标VPN和服 务标签。

cE1#show platform software sdwan F0 next-hop indirect id 0xf800044f SDWAN Nexthop OCE Indirect: client_handle 0x561b610f8140, ppe addr 0xd86b4cf0 nhobj_type: SDWAN_NH_LOCAL_SLA_CLASS, nhobj_handle: 0xf808037f label: 1007, vpn: 20, sys-ip: 169.254.206.12, vrf_id: 1, sla_class: 1

方法3.借助数据包跟踪工具查找目的VPN

查找目的VPN的另一种方法是**数据包跟踪**工具,它可以实时分析通过路由器传输的实际数据包。调 试条件设置为仅与IP地址192.168.12.12的流量匹配/匹配。

cE1#debug platform condition ipv4 192.168.12.12/32 both cE1#debug platform packet-trace packet 10 Please remember to turn on 'debug platform condition start' for packet-trace to work cE1#debug platform condition start

接下来,如果流量是在**ping**的帮助下从R30发起的,则您可以在cE1上看到匹配的数据包并检查每个 数据包的详细信息。在本例中,它是第一个数据包编号0。最重要的一行用<<<**<<符号突**出显示。

cE1#show platform packet-trace summary Pkt Input Output State Reason 0 Gi6 Tu3 DROP 52 (FirewallL4Insp) 1 Gi6 Tu3 DROP 52 (FirewallL4Insp) 2 Gi6 Tu3 DROP 52 (FirewallL4Insp) 3 Gi6 Tu3 DROP 52 (FirewallL4Insp) 4 Gi6 Tu3 DROP 52 (FirewallL4Insp) 5 Gi6 Tu3 DROP 52 (FirewallL4Insp) cE1#show platform packet-trace packet 0 Packet: 0 CBUG ID: 0 Summary Input : GigabitEthernet6 Output : Tunnel3 State : DROP 52 (FirewallL4Insp) <<<<<<<<<<<><><<<<<<<>>Timestamp Start : 161062920614751 ns (03/24/2022 16:19:31.754050 UTC) Stop : 161062920679374 ns (03/24/2022 16:19:31.754114 UTC) Path Trace Feature: IPV4(Input) Input : GigabitEthernet6 Output : packet-trace告诉,ping发送的所有五个ICMP回应数据包已丢弃丢弃代码52(FirewallL4Insp)。 部分 功能:SDWAN转发告知目的VPN为20, 而隧道数据包的内部报头中的服务标签1007用于转发以在 cE2上指定目的VPN。部分功能:ZBFW进一步确认数据包已丢弃,因为区域对未配置为从输入 VPN 20发往VPN 30区域的流量。

故障切换可能导致的问题

如果路由192.168.12.0/24被R20撤回或无法从VRF 20中的cE2到达,会发生什么情况?虽然从VRF 30的角度来看,子网是相同的,但是,由于ZBFW安全策略对从区域VPN 30到区域VPN 20和区域 VPN 10的流量的处理方式不同,它可能会导致不理想的结果,如允许的流量,但不能相反。

例如,如果模拟cE2和R20路由器之间的链路故障。这会导致192.168.12.0/24路由从vSmart控制器 上的VPN 20路由表中退出,而VPN 10路由会泄露到VPN 30路由表中。根据在cE1上应用的安全策 略,允许从VPN 30到VPN 10的连接(从安全策略的角度来看是预期的,但对于两个VPN中显示的 特定子网而言,这是不可取的)。

cE1#show platform packet-trace packet 0 Packet: 0 CBUG ID: 644 Summary Input : GigabitEthernet6 Output : GigabitEthernet3 State : FWD Timestamp Start : 160658983624344 ns (03/24/2022 16:12:47.817059 UTC) Stop : 160658983677282 ns (03/24/2022 16:12:47.817112 UTC) Path Trace Feature: IPV4(Input) Input : GigabitEthernet6 Output :

请注意,标签1006已用于代替1007,输出VPN ID为10而不是20。此外,根据ZBFW安全策略允许 数据包,并给出了相应的区域对、类映射和策略名称。

由于最早的路由保留在VPN 30的路由表中,而在本例中,在初始控制策略应用程序VPN 20路由泄 露到vSmart的VPN 30 OMP表中后,VPN 10路由会出现更大的问题。想象一下,当最初的想法与 本文中描述的ZBFW安全策略逻辑完全相反时的情景。例如,目标是允许从VPN 30到VPN 20的流 量,而不允许到VPN 10的流量。如果在初始策略配置后允许流量,那么在故障或

192.168.12.0/24路由从VPN 20退出后,即使在恢复后,流量仍会被阻止到192.168.12.0/24子网 ,因为192.168.12.0/24路由仍然会从VPN 1泄露0。