SANGFOR

VPN 常见多总部部署方案

作者:李圣悦

版本: V1

2017 年 7 月 24 日

1. 第三方对接，作为分支，双总部双活数据中心

1.1. 场景描述

第三方对接，我方作为分支只有一条线路，两台第三方设备作为总部，两个数据中心双活主备，两总部内网网段一致，业务做主备，双数据中心内网专线做数据同步。需要我方设备同时跟两个总部建立标准 ipsec 连接，在主数据中心连接断开之后，数据能够走到被数据中心。

1.2. 实现方案

可以使用永安保险定制 GPLAT-2016032301 定制方案

具体配置如下

1> 第一阶段

每一个总部配置一条第一阶段，其中备份数据中心的连接，比如这里总部 2 是备用的总部。(不同的分支可以选用不同的备用总部)

2> 第二阶段

第二阶段配置根据实际情况配置，主备两个总部出入站可以配置成一样，也可以配置成不一样

3> 运行结果

两个总部建立成功

当总部 1 断开之后，数据会自动切换到总部 2

当总部 1 恢复之后，会自动恢复会总部 2

1.3. 支持情况

当前定制支持 AF6.8，改动代码可以通用，其他产品线可以定制迁移支持。

下一个正式版本会合入，预计是 DLAN5.3 会合入。

1.4. 场景发散

该方案支持同时跟两个总部对接，所以也支持对端两条线路做主备，需要我方支持同时跟两条线路建立标准 ipsec。

1.5. 已知缺陷

1.5.1 主数据中心断开后，触发感兴趣流不会发起协商。

原因: 主数据中心虽然断了，但被数据中心还在，所以没有触发

解决方案: 永安保险定制中支持长连接 ping 机制，可以保证断开后发起协商。另外触发感兴趣流问题会在正式版本中优化。

1.5.2 野蛮模式下主备连接的身份 ID 不能完全一样

原因: 野蛮模式下使用身份 ID 作为一个连接的标识，如果一样，没法区分协商的连接是主还是备。就像主模式下对端的 IP 不能一样是同一个道理。

解决方案: 使用主模式，或者将身份 ID 配置成不一样。正式版本会做优化，预计优化成: 对端固定 IP 时除了使用身份 ID 还使用 IP 来区分，这样适用场景会更广。

2. 第三方对接，我方两条线路，实现分支选择指定线路接入

2.1. 场景描述

第三方对接，我方作为总部有两条线路，一条联通线路，一条电信线路。第三方设备作为分支只有一条线路(联通或者电信)，需要联通的分支接入联通线路，电信的分支接入电信。

2.2. 实现方案

方案一. 使用前置设备做选路

当前是厦门国贸 AF 使用了这个方案。

1> 使用一台前置设备，支持多线路

2> 前置设备的多条线路都映射给下联的 VPN 设备，使得 VPN 只是用一条线路。

缺陷:

1> 需要增加一台设备

2> 存在 nat 只能使用野蛮模式对接

3> 我方主动协商时，需要前置设备支持策略路由或者 ips，使得电信 IP 走电信线路，联通 IP 走联通线路。

方案二. 设备自身做 NAT

主要是替代方案一的前置做 nat

1> 设备支持多条线路，配置多线路

2> 选择主要运营商线路作为第三方出口，比如线路 1

3> 对端主动跟线路 2 建立连接

i. 配置 dnat，目的地址是线路 2 的 IP，目的端口是 500 和 4500，目的地址变成线路 1 的 IP

ii. 回包，需要做路由保证数据从线路 2 出去

4> 主动连接对端

i. 做路由，使得需要走线路 2 的数据走线路 2

ii. 做 snat，源是线路 1，走线路 2 的数据将源 IP 改成线路 2 的 IP

5> 第三方连接需要启用 natt

缺陷:

1> 由于方案中的 snat 和 dnat 需要能够方向 nat，所以需要设备支持反向 nat，其中 AF 不支持。

2> 如果分支比较多，需要大量路由和 nat。

2.3. 后续正式版本改进方案

后续版本如果要真正完美支持这种场景，需要重新设计

预计实现

1> 标准 ipsec 支持监听多条线路，使得能够处理多条线路过来的数据包

2> 第三方第一阶段配置支持指定线路，使得能够跟对端使用指定的线路协商和走数据

3. 第三方对接，我方两条线路做线路主备

3.1. 场景描述

第三方对接，我方有两条线路，做线路灾备。在主线路故障之后能够使用备用线路进行第三方协商，在主线路恢复之后，为避免 ipsec 不稳定，不需要切换回去。

3.2. 实现方案

使用光大证券 GPLAT-2016032302 定制方案

方案描述: 利用 vpn 多线路检测的功能，在发现 ipsec 选择的出口线路故障之后，切换成其他出口线路，ipsec 走出口 IP 改变的流程重建所有标准 ipsec。

配置方法:

1> 启用多线路探测，并配置好相关的参数

2> 配置第三方配置，跟之前一样。选择出口线路作为初始选择的线路

效果描述:

1> 初始时选择指定出口跟对端建立连接。

2> 多线路检测发现线路故障之后。(可以拔线测试)

3> 会重现选择一条激活的线路跟对端建立连接

3.3. 支持情况

当前仅 AC+DLAN4.32 定制支持，其他产品线可以定制迁移支持。

该方案适用场景比较少，只支持在我方多条线路需要做线路灾备的场景下适用。当一条线路故障之后，会断开所有的 ipsec 连接，同时都切换到另外一条线路上，也就是说同时也只能使用一条线路，如果要不同的分支使用不同线路，那属于第 2 节的场景。

4. 第三方对接，对端两条线路，实现线路灾备

4.1. 场景描述

对端有两条线路做主备，需要我方跟对端同时建立两条 ipsec 连接，在主线路故障之后，数据能够切换到另外一条连接上。

4.2. 实现方案

方案一. 使用跟第 1 节相同的方案。

方案二. 使用对端动态 IP 的方式跟对端建立野蛮模式对接

1> 配置野蛮模式跟对端建立 ipsec 连接

2> 对端地址类型选择”对端是动态 IP”

3> 在对端线路切换时自动选择一个 IP 跟我方建立连接

缺陷:

1> 只能对端发起连接

2> 只能使用野蛮模式

5. Sangfor vpn，双总部一主一备

5.1. 场景描述

总部 sangfor vpn 设备，双总部，内网相同，提供相同的服务，一主一备，分支可以随意指定主总部和备总部。

5.2. 方案

5.2.1 配置方案

由于两个总部内网一样，比如 LAN 口都是 192.168.1.0/24，使用常规的方法建立 sangfor vpn 会报冲突，可以采用如下方案建立 vpn:

1> 假设两总部 DMZ 口不同网段，可以使用 DMZ 口建立 VPN。确保不会因为冲突导致无法建立 vpn。

2> 建立隧道间路由

配置两条隧道间路由，源地址是分支内网网段，目的地址是 192.168.1.0/24，目的路由用户分别是两个总部。如下图

隧道间路由顺序有优先级，数据最终会先走上面的，如果上面的连接不在会走下面的，达到主备总部的效果，如上图，总部 2 就是总部 1 的备份。

5.2.1 适用场景和特点描述

这里说是特点是因为下面的描述在某些场景中可能会被考虑而成为缺陷

- **在某些场景中，两个总部的 dmz 口和 lan 口可能都一样，内网划分到 dmz 口和 lan 口仅仅是为了方便隔离。**

对于这种场景可以配置如下

i. 总部 1 使用 lan 口作为 vpn 内网口。总部 2 使用 dmz 口作为 vpn 内网口。保证 vpn 能够对接成功。

ii. 由于隧道间路由优先级高于 vpn 学习到的路由，并且配置的时候不会去判断是否跟学习到的路由冲突，也就意味着可以在隧道间路由中配置跟学习到的路由冲突的路由，也就是可以通过隧道间路由来控制所有路由的顺序。详细配置如下

>> 配置到总部 lan 和 dmz 内网的路由下一跳走到总部 1

>> 配置到总部 lan 和 dmz 内网的路由下一跳走到总部 2

>> 总部 1 的优先级高于总部 2

优点:

1. 通过不冲突的方法建立起 vpn。使用大多场景，总会找到不冲突的方法
2. 使用隧道间路由的优先级，比较直观，比较灵活

缺点:

1. 不能自动学习总部的路由，如果总部新增网段，需要每一个分支都增加隧道间路由

适用场景: 总部网段比较固定，后续变动小

- **整个协商和数据流程跟之前一样，可以在多线路场景中使用**

总部和分支都具备多条线路，建立起 n*m 条隧道，当总部 1 建立的所有隧道都断开之后，才会走总部 2。

所以在某种特殊的多线路场景中很局限。比如总部和分支建立的多条隧道中有部分隧道质量很差，客户不希望走这些隧道，希望在质量好的隧道异常之后直接走总部 2。

6. Sangfor vpn，双总部互为主备

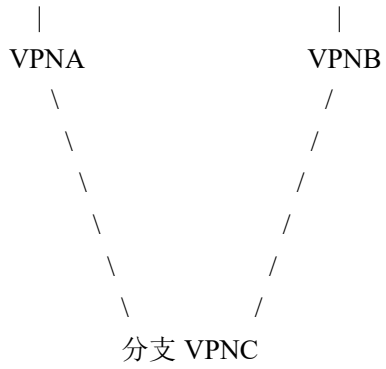
6.1. 场景描述

总部 sangfor vpn 设备，双总部，双数据中心内网不同，互为主备，中间有专线互联。需要实现分支跟总部 A 断开之后能够通过总部 B 的连接访问到总部 A 的数据中心。

NetA　　NetB

　|　　|

核心 A　----专线----　核心 B



6.2. 实现方案

6.2.1 方案一. 双连接方案

顾名思义，就是同时跟 VPNA 和 VPNB 建立连接。认为 VPNA 和 VPNB 都具备了 NetA 和 NetB。

6.2.1.1 配置方法

1> 分支配置两条连接同时跟两个总部建立连接。

2> 配置四条隧道间路由，分别是

路由 A. 访问 NetA 走 VPNA

路由 B. 访问 NetB 走 VPNA

路由 C. 访问 NetA 走 VPNB

路由 D. 访问 BetB 走 VPNB

可以根据策略调整优先级，比如如果需要访问 NetA 优先走 VPNA，那路由 A 在路由 C 上面，如果需要访问 NetB 优先走 VPNB 则路由 D 在路由 B 上面。

3> 比较重要的是 NetA 和 NetB 回包路由

这里有两种做法

做法 A: 启用核心交换机和 VPNA、VPNB 的 RIP 功能

VPNA 启用 RIP，在 VPNA 建立起 VPN 后学习到 VPNC 的路由后，使用 rip 协议通知核心 A，核心 A 会将学习到的路由通知核心 B，由于多走了一步，所以路由度量值会+1。核心 A 学习到 C 的路由有两条，一条从 VPNA 到 VPNC，另外一条从 VPNB 到 VPNC，并且 VPNA 度量值比 VPNB 小，优先级高，优先走 VPNA。当 VPNA 跟 VPNC 的 vpn 断开之后，只剩下一条路由，数据走 VPNB 到 VPNC

缺陷: 需要依赖核心交换机路由交换的功能。

做法 B: 做 NAT

在 VPNA 上将 VPNC 过来的数据做 snat，将源地址转换成 IPA，在 VPNB 上将 VPNC 过来的数据做 snat 将源地址转换成 IPB。NetA 和 NetB 上根据回包的目的地址是 IPA 还是 IPB 做路由，则可以准确不误回包。

缺陷: 只能分支去访问总部

6.2.1.2 优缺点

优点:

1. 可以实现访问 NetA 优先走 VPNA，访问 NetB 优先走 B
2. 同时跟两个总部建立连接，在切换时省去一个连接过程，切换速度更快

缺点:

1. 总部 NetA 和 NetB 网络需要比较固定，不适合经常调整网络的场景。因为没调整一次就需要在每一个分支修改隧道间路由。
2.

6.2.2 方案二. 单连接方案

也就是一个时间只跟一个总部建立 vpn。

6.2.2.1 配置方法

1> 分支使用主备 webagent 的方式跟两个总部建立一条连接。
当主 webagent 的连接断开之后会连接到备 webagent

2> 总部启用 rip，让两个核心能够学习到路由，回包没有问题。

6.2.2.2 优缺点

优点:

1> 路由比较简单，总部新增网络只需要添加到本地子网，各个分支会自动学习到

缺点:

1> 同时只建立一条连接，一个分支所有数据都走一个总部。只能不同分支选择不同的总部来均衡。

2> 故障切换时间比方案一慢，需要考虑重连的时间。

7. Sangfor vpn，多总部集群方案

7.1. 场景描述

有上万个分支，一个总部设备并发性能不够，需要总部集群。

7.2. 方案

1> 多台具备 vpn 功能的设备集群，前置使用 AD 做负载均衡

2> 多台设备之间 vpn 配置同步，有两个方案

A. Ipsec 前段时间实现了使用工具去同步配置 -- 已经完成

>> 选用一台设备作为配置主机

>> 设置好配置主机的配置同步的端口

>> 设置好配置备机的配置同步参数后，备机能够定时获取配置主机的配置，然后生效

B. 使用集中管理平台，定制 VPN 配置模板，使得各个集群主机使用相同的配置模板进行配置。

3> 集群的 vpn 设备启用 rip 功能，核心交换机自动学习到分支的路由，回包没有问题。