基于华为DSVPN技术的高安全性企业专网设计与仿真

程铋峪[1],王　飞[1],李　涛[2]

(1.安徽邮电职业技术学院,安徽合肥 230031;
2.中国电信股份有限公司南京江宁区分公司,江苏南京 211106)

【摘要】随着技术不断发展、进步,越来越多的企业在各地建立起自己的分支机构,并构建企业专用的Hub-Spoke网络,虽然传统IPSec VPN、GRE over IPSec等技术能够构建安全可靠的企业专网,但其技术本身多用于固定IP场景,因此较难满足Hub-Spoke场景下,分支机构动态IP全互联业务接入与互访。以华为动态智能VPN技术为基础,提出一种高安全性Hub-Spoke企业专网设计方案,在IPSec保护下各分支Spoke站点可实现全互联通信。

【关键词】动态智能VPN;mGRE隧道;NHRP映射;动态路由学习;IPSec保护
【doi:10.3969/j.issn.2095-7661.2022.04.007】
【中图分类号】TP393.18　　【文献标识码】A　　【文章编号】2095-7661(2022)04-0021-05

Design and Simulation of High Security Enterprise Private Network Based on Huawei DSVPN Technology

CHENG Bi-yu[1], WANG Fei[1], LI Tao[2]

(1. Anhui Post and Telecommunication College, Hefei, Anhui, China 230031;
2. Nanjing Jiangning District Branch of China Telecom Co. Ltd., Nanjing, Jiangsu, China 211106)

Abstract: With the continuous development of technology, more and more enterprises have established their own branches in various places and built enterprise-specific Hub-Spoke networks. Traditional IPSec VPN and GRE over IPSec technologies can construct secure and reliable enterprise networks. However, these technologies are mainly used in fixed IP address scenarios. Therefore, they cannot meet the requirements for dynamic IP interconnection service access and mutual access in hub-Spoke scenarios. This paper proposes a hub-Spoke enterprise private network with high security based on Huawei dynamic smart VPN technology. All branches of Spoke sites can communicate with each other under the protection of IPSec.

Keywords: DSVPN; mGRE tunnel; NHRP mapping; dynamic route learning; IPSec protection

随着企业规模不断扩大,中大型企业其分支机构往往不只一处,企业网络愈发变得复杂[1],最终形成以总部为Hub,各分支机构为Spoke的Hub-Spoke网络架构[2]。由于分支机构Spoke站点与公网互联地址常为浮动IP地址,为实现各Spoke站点之间安全可靠的通信,常规解决方案往往在总部Hub与各分支之间构建IPSec隧道[3],此种方式既增加了总部Hub设备其CPU处理负担,设备对数据包解封装与再封装也极大增加了数据传输时延,业务实时性无法得到保障;此外各Spoke站点之间以固定域名方式构建全互联IPSec隧道,亦可实现互访通信,随着分支Spoke站点不断新增,对于网络管理人员来说其配置量将会呈指数增加。综上,传统IPSec技术在中大型企业Hub-Spoke网络实施中并不灵活。

为解决企业分支各Spoke站点公网地址浮动,站点之间无法灵活构建VPN专网隧道的问题,本文以华为DSVPN技术为基础[4],提出Hub-Spoke架构下的VPN构建方案,并结合IPSec技术,进一步对业务数据进行加密,以提高网络安全性。

[收稿日期] 2022-09-22

[作者简介] 程铋峪(1989—),男,安徽滁州人,安徽邮电职业技术学院讲师,工程师,硕士,研究方向:通信与网络技术。

[基金项目] 2021年度高等学校省级质量工程项目"'IP+全光网'背景下高职院校光纤通信技术课程建设研究"(项目编号:2021jyxm0775)。

1 DSVPN技术

1.1 构建总部与分支站点间mGRE隧道

如图1所示，企业专网由总部Hub和位于异地的两个Spoke站点构成。其中，分支Spoke站点设备配置Hub网关设备的公网IP地址与其Tunnel隧道IP地址的映射关系，即手工配置总部NHRP映射表项。若要Hub与各Spoke站点间的静态mGRE隧道能建立成功，总部Hub设备也应获得Spoke站点的公网IP地址与其Tunnel隧道IP地址映射表项。

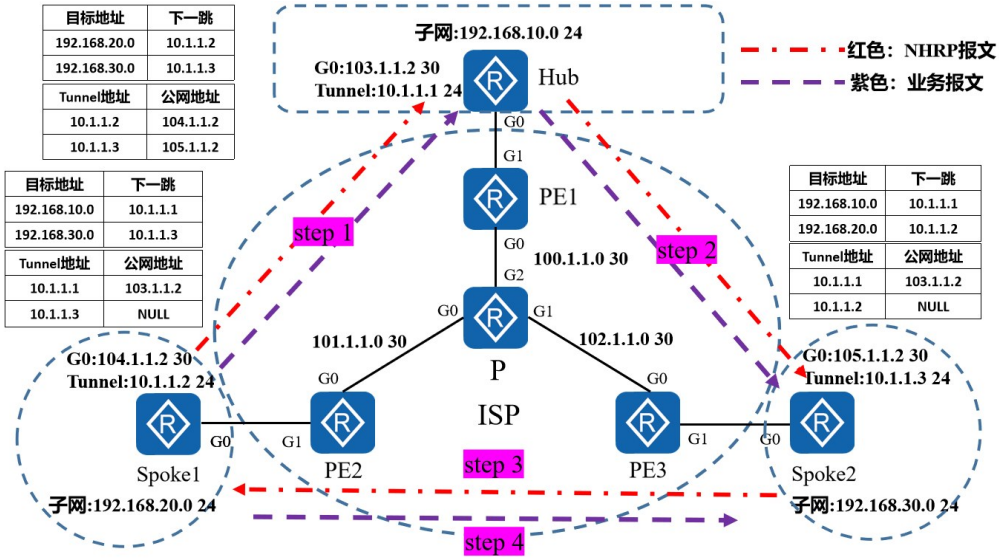

图1 Hub-Spoke企业专网架构图

由于公网运营商的路由可达，两个分支Spoke站点将向总部Hub发送NHRP注册请求报文，该报文中包含分支Spoke站点公网IP与Tunnel隧道IP之间的映射关系，总部收到报文后提取映射关系，形成Spoke站点的NHRP映射表，并向分支机构回复NHRP应答报文，进而建立起Hub与Spoke站点间的静态mGRE隧道。此外，当Spoke站点公网IP地址变化以及计时器到期时，均会重新触发Spoke向Hub发送NHRP注册请求报文，使得总部Hub刷新NHRP表项，也使该表项不被老化，始终在总部与分部间建立的静态mGRE隧道。

1.2 获取总部与分支站点内网路由

在分支机构Spoke为数不多的场景下，为使得总部以及各分支机构设备能获取本企业目标网段的内网路由，可直接在总部Hub设备、Spoke1和Spoke2设备上配置静态路由[5]，从而将企业内网流量引入隧道，封装上公网IP并在公网传递。如图1所示，在Hub设备上分别配置到Spoke站点192.168.20.0及192.168.30.0网段路由，其下一跳指向站点Tunnel隧道地址10.1.1.2以及10.1.1.3；在Spoke1上分别配置到Hub及Spoke2的192.168.10.0及192.168.30.0网段路由，其下一跳指向Tunnel隧道地址10.1.1.1以及10.1.1.3；在Spoke2上分别配置到Hub及Spoke1的192.168.10.0及192.168.20.0网段路由，其下一跳指向Tunnel隧道地址10.1.1.1以及10.1.1.2。

上述获取内网路由方式，配置简单但灵活性较差，随着企业规模扩大，Spoke站点数量不断增加，维护人员需要随着网络架构的变化而去调整静态路由，这与现代企业自动化网络运维的初衷相背离。

由于总部Hub与分支机构Spoke之间的静态mGRE隧道已经建立，为自适应网络拓扑变化，网络设备能够动态学习各目标网段的内网路由，简化网络运维工作量，可直接在Hub与Spoke设备上运行OSPF协议[6]，并将企业内网网段及互联Tunnel隧道网段宣告至OSPF中。需要注意，在Hub-Spoke架构下，总部Hub设备作为中心节点，应使其成为本区域中的DR，OSPF网络中的1类LSA及2类LSA通过LS Update报文携带，并利用已经建立的mGRE隧道进行封装。

如图2所示，总部Hub作为OSPF网络中的DR，向对等体同步LSA，报文封装前的源目IP分别是10.1.1.1、10.1.1.2，经隧道封装后源目IP分别是103.1.1.2、104.1.1.2。报文中携带了4条LSA，其中三条1类LSA分别由Hub、Spoke1、Spoke2产生用于描述设备自身网络拓扑情况，一条2类LSA由网络中DR设备产生。当OSPF网络中所有设备LSDB完成同步后，各设备以自己为根，算出到目标网段SPF路径树，生成路由信息。

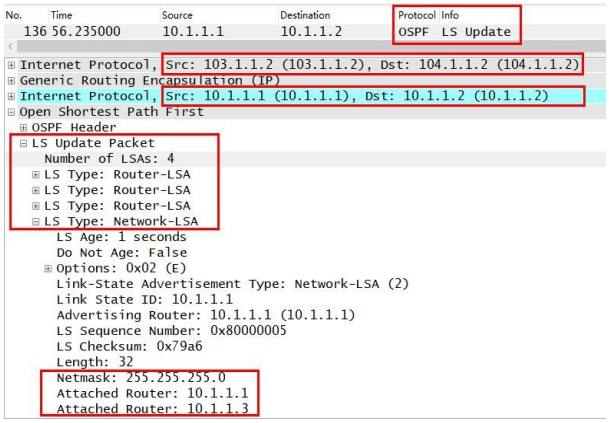

图2　OSPF报文封装

1.3 Normal模式下构建分支站点间mGRE隧道

当Spoke1首次与Spoke2站点进行业务数据传递时，将触发Spoke1与Spoke2之间建立动态mGRE隧道。如图1所示，Spoke1访问Spoke2站点192.168.30.0网段，业务流量到达Spoke1，根据目标网段查路由表，发现下一跳地址是10.1.1.3，并根据下一跳地址查NHRP映射表，由于是首次发起的业务流量，NHRP表项中10.1.1.3对应的公网地址为空。第一步，Spoke1会将业务流量直接转发给总部Hub，同时向总部Hub发送NHRP注册请求报文，请求10.1.1.3对应的公网地址；第二步，当总部Hub收到Spoke1发送的业务报文以及NHRP注册请求报文后，将报文转发给Spoke2，Spoke2收到报文后学习Spoke1站点的NHRP映射关系，并更新至本端设备NHRP表项中；第三步，Spoke2直接向Spoke1发送NHRP应答报文，报文携带Spoke2的Tunnel隧道地址和公网地址的映射；第四步，Spoke1收到Spoke2发来的NHRP应答报文后，学习对应映射关系，并更新至NHRP表项中，完成Spoke之间的动态mGRE隧道的建立。随后业务流量到达Spoke1，直接送入mGRE隧道封装，经公网发送至Spoke2站点，完成流量传递。

2 基于DSVPN的高安全性企业专网设计

2.1 设计目的

基于DSVPN技术，提出中大型企业专网规划、设计解决方案，可灵活实现企业网络各Spoke站点间，Hub与Spoke之间业务互访。为构建安全可靠的数据传输服务，本方案同时采用了IPSec保护框架，以此来保障业务数据的保密性与完整性。

2.2 方案规划

基于DSVPN的高安全性企业专网方案，具体规划如下，网络设备所属区域及其接口地址规则如表1所示。

1）总部Hub设备、分支Spoke1设备、分支Spoke2设备均使用LoopBack接口模拟其所在内部网络。

2）P设备、PE1设备、PE2设备、PE3设备，模拟ISP运营商公网，其中公网运行ISIS动态路由协议[7]。

3）Hub设备、Spoke1设备、Spoke2设备作为企业出口使用ISIS协议与运营商公网对接，并通过建立成功的mGRE隧道封装OSPF报文。

4）为提高专网安全性，Hub设备、Spoke1设备、Spoke2设备使用IPSec框架保护。

5）IPSec安全联盟包括：ESP安全协议、Transport封装模式、SHA-512认证算法、AES-256加密算法。

表1　本方案网络设备所属区域及其接口地址规划表

	所属区域	接口IP	子网掩码	接口名称
P设备	49.0000.0000.0001.00	101.1.1.1	255.255.255.252	GigabitEthernet0/0/0
		102.1.1.1	255.255.255.252	GigabitEthernet0/0/1
		100.1.1.1	255.255.255.252	GigabitEthernet0/0/2
PE1设备	49.0000.0000.0002.00	100.1.1.2	255.255.255.252	GigabitEthernet0/0/0
		103.1.1.1	255.255.255.252	GigabitEthernet0/0/1
PE2设备	49.0000.0000.0003.00	101.1.1.2	255.255.255.252	GigabitEthernet0/0/0
		104.1.1.1	255.255.255.252	GigabitEthernet0/0/1
PE3设备	49.0000.0000.0004.00	102.1.1.2	255.255.255.252	GigabitEthernet0/0/0
		105.1.1.1	255.255.255.252	GigabitEthernet0/0/1
Hub设备	49.0000.0000.0005.00	103.1.1.2	255.255.255.252	GigabitEthernet0/0/0
		192.168.10.1	255.255.255.0	LoopBack0
		10.1.1.1	255.255.255.0	Tunnel0/0/0
Spoke1设备	49.0000.0000.0006.00	104.1.1.2	255.255.255.252	GigabitEthernet0/0/0
		192.168.20.1	255.255.255.0	LoopBack0
		10.1.1.2	255.255.255.0	Tunnel0/0/0

表1（续）

	所属区域	接口IP	子网掩码	接口名称
Spoke2设备	49.0000.0000.0007.00	105.1.1.2	255.255.255.252	GigabitEthernet0/0/0
		192.168.30.1	255.255.255.0	LoopBack0
		10.1.1.3	255.255.255.0	Tunnel0/0/0

2.3 配置DSVPN

1）P设备配置（ISP网络运行ISIS路由协议，PE1、PE2以及PE3配置类似）：

[P]isis 1

[P-isis-1] network-entity 49.0000.0000.0001.00

[P-GigabitEthernet0/0/0] ip address 101.1.1.1 255.255.255.252

[P-GigabitEthernet0/0/0] isis enable 1

[P-GigabitEthernet0/0/1] ip address 102.1.1.1 255.255.255.252

[P-GigabitEthernet0/0/1] isis enable 1

[P-GigabitEthernet0/0/2] ip address 100.1.1.1 255.255.255.252

[P-GigabitEthernet0/0/2] isis enable 1。

2）总部Hub设备配置（运行ISIS、OSPF、DSVPN以及IPSec协议）：

[Hub]ipsec proposal 1 ///配置IPSec安全提议，包括认证、加密方式等

[Hub-ipsec-proposal-1] encapsulation-mode transport

[Hub-ipsec-proposal-1] esp authentication-algorithm sha2-512

[Hub-ipsec-proposal-1] esp encryption-algorithm aes-256

[Hub]ike proposal 1 使用系统默认IKE安全提议

[Hub]ike peer Hub v1 ///配置IKE对等体

[Hub-ike-peer-Hub]pre-shared-key cipher Security@123

[Hub-ike-peer-Hub]ike-proposal 1

[Hub]ipsec profile 1 ///配置IPSec安全框架

[Hub-ipsec-profile-1]ike-peer Hub

[Hub-ipsec-profile-1] proposal 1

[Hub-isis-1] network-entity 49.0000.0000.0005.00

[Hub-GigabitEthernet0/0/0] ip address 103.1.1.2 255.255.255.252

[Hub-GigabitEthernet0/0/0] isis enable 1

[Hub-LoopBack0] ip address 192.168.10.1 255.255.255.0

[Hub]interface Tunnel0/0/0 ///隧道接口下配置DSVPN

[Hub-Tunnel0/0/0] ip address 10.1.1.1 255.255.255.0

[Hub-Tunnel0/0/0] tunnel-protocol gre p2mp

[Hub-Tunnel0/0/0] source GigabitEthernet0/0/0

[Hub-Tunnel0/0/0] ospf network-type broadcast

[Hub-Tunnel0/0/0] ipsec profile 1 ///隧道接口应用IPSec安全框架

[Hub-Tunnel0/0/0]nhrp entry multicast dynamic ///动态学习NHRP表项

[Hub]ospf 1 router-id 10.1.1.1

[Hub-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0

[Hub-ospf-1-area-0.0.0.0] network 192.168.10.1 0.0.0.0。

3）分支Spoke1、Spoke2通用配置参照Hub，此处仅列出与Hub配置不同之处：

[Spoke1-Tunnel0/0/0]ospf dr-priority 0

[Spoke1-Tunnel0/0/0]nhrp entry 10.1.1.1 103.1.1.2 register ///静态配置总部NHRP映射表

[Spoke2-Tunnel0/0/0]ospf dr-priority 0

[Spoke2-Tunnel0/0/0]nhrp entry 10.1.1.1 103.1.1.2 register ///静态配置总部NHRP映射表。

3 网络连通性测试与安全性验证

规划、设计以及数据配置完成后，对本DSVPN企业专网进行连通性测试以及安全性验证。测试及验证使用华为eNSP仿真软件[8]，测试验证的网络设备选用AR2220，其版本号为V200R003C00。

如图3所示，对总部Hub访问分支Spoke以及分支Spoke1访问分支Spoke2进行连通性测试，经测试表明本网络连通性正常，可以进行业务互访。为了展示DSVPN灵活构建的mGRE隧道，如图4所示，分支机构Spoke1与总部Hub构建了静态mGRE隧道，Spoke1与Spoke2构建了动态mGRE隧道，该动态隧道由业务流量触发。为验证设计方案安全性，通过display ipsec sa brief命令查看总部Hub设备分别与Spoke1、Spoke2建立的双向共计4条IPSec安全联盟。如图5所示，在总部Hub设备公网出口GigabitEthernet0/0/0抓取业务流量，观察发

现数据均以密文形式呈现，进而保障企业内网数据安全可靠传输。为了进一步说明在DSVPN中IPSec安全框架对数据保护的价值，在总部Hub设备、各分支Spoke设备中，取消引入IPSec安全框架，在总部Hub设备进行ICMP报文测试，此时在Hub设备GigabitEthernet0/0/0公网接口上能够抓取到ICMP报文。综上，经网络连通性测试以及安全性验证，本设计方案可以灵活实现Hub-Spoke架构下各分支机构内网互访，业务层面保障了数据传输的安全性。

```
<Hub>ping -a 192.168.10.1 192.168.20.1
  PING 192.168.20.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.20.1: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 192.168.20.1: bytes=56 Sequence=2 ttl=255 time=60 ms
    Reply from 192.168.20.1: bytes=56 Sequence=3 ttl=255 time=60 ms
    Reply from 192.168.20.1: bytes=56 Sequence=4 ttl=255 time=60 ms
    Reply from 192.168.20.1: bytes=56 Sequence=5 ttl=255 time=70 ms

  --- 192.168.20.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/66/80 ms

<Spoke1>ping -a 192.168.20.1 192.168.30.1
  PING 192.168.30.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.30.1: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 192.168.30.1: bytes=56 Sequence=2 ttl=255 time=80 ms
    Reply from 192.168.30.1: bytes=56 Sequence=3 ttl=255 time=60 ms
    Reply from 192.168.30.1: bytes=56 Sequence=4 ttl=255 time=60 ms
    Reply from 192.168.30.1: bytes=56 Sequence=5 ttl=255 time=70 ms

  --- 192.168.30.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/64/80 ms
```

图3　各站点间连通性测试

```
<Spoke1>display  nhrp  peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr      Type          Flag
--------------------------------------------------------------------------------
10.1.1.1        32    103.1.1.2       10.1.1.1          static        hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 02:10:15
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr      Type          Flag
--------------------------------------------------------------------------------
10.1.1.3        32    105.1.1.2       10.1.1.3          dynamic       route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:05:05
Expire time     : 01:54:58

Number of nhrp peers: 2
<Hub>display ipsec sa brief

Number of SAs:4
    Src address     Dst address        SPI    VPN  Protocol     Algorithm
-------------------------------------------------------------------------------
      103.1.1.2       104.1.1.2 3217517986      0    ESP   E:AES-256 A:SHA2_512_
256
      104.1.1.2       103.1.1.2 3019586584      0    ESP   E:AES-256 A:SHA2_512_
256
      103.1.1.2       105.1.1.2 1937043211      0    ESP   E:AES-256 A:SHA2_512_
256
      105.1.1.2       103.1.1.2 1312893180      0    ESP   E:AES-256 A:SHA2_512_
256
```

图4　mGRE隧道及IPSec安全联盟

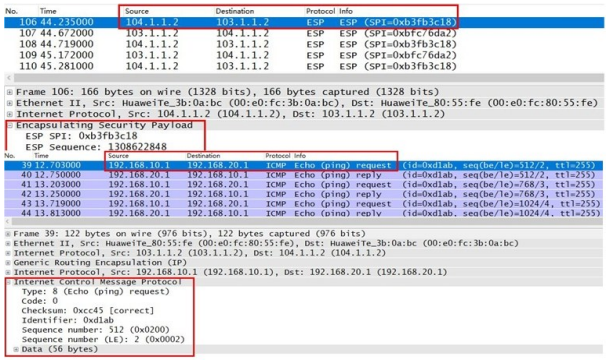

图5　IPSec流量保护

4　结论

相比传统IPSec VPN、GRE over IPSec等技术，动态智能DSVPN能够更灵活地在企业网各站点间部署，即使站点公网地址浮动，也能够动态建立VPN隧道。本文以DSVPN为基础，提出一种Hub-Spoke企业网架构设计方案，该方案协同运用ISIS、OSPF、IPSec等多种技术，能够较好自适应企业网络中的拓扑变化，便于网络维护管理，测试表明该方案中业务数据的安全性能够得到保障，满足中大型企业专网建设需求。

【参考文献】

[1]潘学文.基于HCL的企业网络规划与设计[J].现代工业经济和信息化,2021(6):70-71,78.

[2]李辉,崔建涛.基于OSPF的帧中继Hub-Spoke拓扑多点接口网络的研究[J].郑州轻工业学院学报(自然科学版),2011(3):77-80.

[3]陈彬,杜陈艳,陈建兵.基于IPsec VPN的远程访问服务[J].云南师范大学学报(自然科学版),2021(6):25-27.

[4]徐慧洋,白杰,卢宏旺.华为防火墙技术漫谈[M].北京:人民邮电出版社,2015.

[5]程铋峪,徐弢.基于华为eNSP综合性路由交换网络的设计与实现[J].湖南邮电职业技术学院学报,2021(1):12-15.

[6]李勇,沈秀娟.OSPF协议原理分析及其两种仿真实验设计与实现[J].曲靖师范学院学报,2021(6):43-48.

[7]李俊杰.ISIS路由协议中路由计算研究[J].现代电子技术,2011(19):94-96.

[8]李凤银,禹继国,鞠宏伟,刘晓欢.基于eNSP的网络工程实践教学体系探索[J].实验技术与管理,2018(3):209-212.