面向集成的VPN解决方案

陶志勇, 阳王东

引用本文

陶志勇, 阳王东. 面向集成的VPN解决方案[J]. 计算机科学, 2024, 51(9): 357-364.

TAO Zhiyong, YANG Wangdong. Integrated VPN Solution [J]. Computer Science, 2024, 51(9): 357-364.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240200062

面向集成的 VPN 解决方案

陶志勇[1,2]　阳王东[2]
1 长沙民政职业技术学院软件学院　长沙 410004
2 湖南大学信息科学与工程学院　长沙 410082
(27537406@qq.com)

摘　要　针对传统方式构建的 VPN 不支持承载多种数据类型、承载数据缺乏安全性、标签边缘设备负载过重等问题,提出了集成的 VPN 解决方案。该方案设计包含 GRE VPN 的建立、IPSEC VPN 的建立、网络设备虚拟化、MPLS VPN 的建立、私网数据的识别与隔离 5 个关键步骤,实现了各 VPN 技术数据的嵌套与各 VPN 技术的相互融合,融合后的 VPN 既支持承载多种数据类型,又支持数据交互的安全,且能实现私网数据访问控制与地址复用,还能实现数据的负载分担。为验证方案的可行性,对方案建立的隧道、网络资源池、标签转发路径等方面进行了测试与验证,达到了预期设定的目标。为凸显方案的优势,与传统方式在背板带宽、端口速率等方面进行了对比分析。分析结果表明,该方案的背板带宽与端口速率随着资源池中设备数的增加而增长,其数据传输能力相比传统方式成倍增长,且在数据的负载分担、数据安全、可管理性与可维护性等方面优于传统方案,为构建实用、可靠、安全的 VPN 提供了思路。

关键词:虚拟私有网;多协议标签交换;边界网络路由协议;虚拟化;标签边缘设备
中图分类号　TP393

Integrated VPN Solution

TAO Zhiyong[1,2] and YANG Wangdong[2]
1 Software School,Changsha Social Work College,Changsha 410004,China
2 College of Computer Science and Electronic Engineering,Changsha 410082,China

Abstract　Aimed at the problems that the traditional VPN does not support the carrying of multiple data types,lack of security of data,and overweight label edge devices,an integrated VPN solution is proposed.. The design includes the establishment of GRE VPN,the establishment of IPSEC VPN,the virtualization of network equipment,the establishment of MPLS VPN,the recognition and isolation of private network data,to realize the nesting of each VPN technology data and the mutual integration of each VPN technology. The integrated VPN supports multiple data types,also supports the security of data interaction,and can achieve private network data access control and address reuse,and can also realize the load sharing of data. In order to verify the feasibility of the scheme,tunnels,network resource pools,and label forwarding paths established by the scheme have been tested and verified,and expected goal is achieved. In order to highlight the advantages of the scheme,it is compared with traditional methods in terms of backplane bandwidth and port rate. The analysis results show that the backplane bandwidth and port rate of the scheme increase with the increase of the device number in the resource pool,and its data transmission capability is multiplied compared with the traditional mode,and the data load is reduced. It is superior to the traditional scheme in load sharing,data security,manageability and maintainability,and provides an new ideal for building a practical,reliable and secure VPN.

Keywords　Virtual private network,Multi-protocol label exchange,Boundary network routing protocol,Virtualization,Label edge equipment

1　引言

IETF(Internet Engineering Task Force,因特网工程组)发布的 RFC(Request for Comments,请求注解)-2764,撰述的 VPN(Virtual Private Network,虚拟私有网)技术为私网数据穿越公网提供了路径,为企业与出差员工、分支机构、合作伙伴等

到稿日期:2024-02-09　返修日期:2024-04-24
基金项目:国家自然科学基金(61872127);湖南省教育厅资助科研项目(22C1433);湖南省普通高等学校教学改革研究项目(ZJGB2022159)
This work was supported by the National Natural Science Foundation of China(61872127),Research Foundation of the Education Department of Hunan Province (22C1433) and Research Project on Teaching Reform in Ordinary Higher Education Institutions in Hunan Province (ZJGB2022159).
通信作者:阳王东(342681652 @qq.com)

异地协同办公提供了通道[1-2]。随后发布的 RFC-2784 阐释的 GRE(Generic Routing Encapsulation,通过路由封装) VPN 不但能承载私网的单播数据穿越公网,且能承载组播数据,但该技术不能保障私网数据交互的安全。为此,IETF 发布了 RFC-4302 与 RFC-4303,阐述的 IPSEC(Internet Protocol Security,互联网安全协议)能对交互的私网数据进行加密、完整性校验等,保障了数据交互的安全,但该技术不支持组播[3]。

因在运营商的网络中 GRE 与 IPSEC 技术不能对用户私网数据进行有效控制与隔离以及地址复用等问题,IETF 发布了 RFC-4364,描述了 MPLS(Multi-protocol Label Switching,多协议标签交换)与 BGP(Border Gateway Protocol,BGP)技术构建的 VPN,提出了在运营商的网络中对不同用户私网数据进行访问控制及地址复用的方法,进而使上述技术构建的 VPN 被用户广泛应用[4-5]。

然而,随着运营商网络承载的用户数据呈爆炸式增长,原本处于层次化模型中性能最弱的标签边缘设备需处理上万甚至上十万用户的数据,标签边缘设备不勘重负,而如何给标签边缘设备减负,以及使构建的 VPN 同时支持组播、支持数据交互安全、支持访问控制与地址复用,是目前构建的 VPN 亟待解决的问题。

智能弹性架构(Intelligent Resilient Framework,IRF)是一种针对网络设备的虚拟化技术,该技术能将多台物理设备虚拟成一台逻辑设备,由虚拟化后的多台物理设备共同分担数据的处理[6-7]。而本文针对 GRE 技术不支持数据交互安全、IPSEC 不支持组播、MPLS 与 BGP 无法实现数据的负载分担的问题,提出了一种集成的 VPN 解决方案。集成的 VPN 解决方案采用嵌套的方式封装数据,使各 VPN 技术相互融合,聚合各传统 VPN 技术的优点,进而使构建的 VPN 既支持组播,又支持数据交互的安全,且能实现私网数据访问控制与地址复用,还能实现数据的负载分担。同时,将集成的 VPN 解决方案与单独采用 GRE,IPSEC,MPLS 技术构建的 VPN 在背板带宽、扩展性、安全性等维度进行对比分析,验证了该方案的优势[8-9]。

2 相关工作

自 IETF 在 2000 年发布 RFC-2764,在全球掀起了 VPN 研究的热潮,先后涌现了 GRE,IPSEC,MPLS 等 VPN 技术。而对于 GRE,IPSEC,MPLS 的研究主要聚焦于以下维度。1)GRE 技术在组播业务中的研究,如 Lin 等[10]针对疫情线上直播教学的需要,提出了“VPN+组播”组网技术,为直播教学提供了关键技术支撑,但构建的 VPN 不能提供数据的安全保护,未实现数据访问控制与负载分担。2)IPSEC 在数据安全中的研究,如 Amaldeep 等、He 等提出了在数据通信中如何识别数据,实现对数据进行加密、完整性的保护,为数据交互提供了安全保障[11-13],但构建的 VPN 未解决不同用户数据访问控制、隔离、负载分担。3)MPLS 在企业网络中的应用研究,如 Komala 等、Li 等将该技术应用于交通、电力等行业,保障企业不同业务数据的访问控制与隔离[14-16],但构建的 VPN 未对交互的数据进行安全保护,且未实现数据的负载分担。

然而,随着企业规模的不断扩大,VPN 需处理的数据量会不断增多,尤其是运营商网络需承载的用户数据呈几何增长,亟需在 VPN 网络中实现数据负载分担,以保障企业业务数据的正常交互。为此,网络设备虚拟化技术应运而生。国外厂商 3com 在 2001 年率先提出了可扩展弹性网络(Expandable Resilient Networking, XRN)的概念,并且在其 S4400 系统网络设备上实现了 XRN 技术,但该虚拟化技术只支持集中式虚拟方式,且稳定性不高。随后美国著名网络设备厂商思科公司在 2007 年提出了虚拟交换系统(Virtual Switch System, VSS)的概念,并将两台物理 Cisco Catalyst 6500 系列交换机作为单一逻辑虚拟交换机运行,从而提高了运营效率,增强了不间断通信,且 VSS 同时支持集中式与分布式虚拟化方式。

而国内网络设备厂商对该技术的研究也紧随其后,华为提出了自己的虚拟化技术集群交换系统 CSS(Cluster Switch System,集群交换系统),锐捷厂商也不甘落后,提出了虚拟化技术 VSU(Virtual Switch Unit,虚拟交换单元),新华三技术有限公司也一直致力于虚拟化技术的研究和优化,继推出 IRF(Intelligent Resilient Framework,智能弹性架构)版本 1 之后,又推出了功能更加完善的虚拟化技术 IRF2 与 IRF3。目前国内网络设备厂商对该技术的研究主要聚焦于利用该技术构建数据中心网络、大二层网络、超融合网络,支持大容量的虚拟机数据的迁移。而国内科研所与院校科研人员对于该技术的研究,以网络设备虚拟化为关键字在知网进行检索(截止检索日期为 2023 年 12 月 22 日),检索到期刊论文 50 篇,学位论文 10 篇,会议论文 7 篇。上述文献对于该技术的研究主要聚焦在 3 个维度:1)移动通信网络,如 Qureshi 等阐述了将该技术应用于移动通信网络[17];2)企业网络,如 Jaff 和 Emmanuel 等阐释了在企业网中如何应用该技术[18-19];3)数据中心,如 Salagrama 等论述了在数据中心建设中如何运用该技术[20]。

由上述研究现状可知,网络设备虚拟化技术主要体现在数据中心、移动通信、企业网络 3 个方面。而将该技术与 GRE,IPSEC,MPLS 以及 BGP 相融合,构建同时支持组播、保障数据交互安全、实现数据访问控制与地址复用、负载分担私网数据的 VPN 尚未查阅到相关文献资料,由此可见该领域的研究处于起步的阶段。本文试图将 GRE,IPSEC,MPLS 与 BGP,IRF 相互融合,构建实用性好、可靠强、安全性高的 VPN。本文的贡献主要体现在以下几个方面:1)面向集成的 VPN 解决方案,使多种技术相互融合,融合后构建的 VPN 取其各 VPN 技术的优点,使构建的 VPN 安全、可靠、实用性更强;2)面向集成的 VPN 解决方案,提供了设计思路、设计网络模型、方案的设计与实现,为后续研究夯实了基础;3)该解决方案在资源利用率、可靠性、背板带宽等方面优于单独采用 GRE,IPSEC,MPLS,BGP 构建的 VPN 解决方案。

3 集成 VPN 的方案设计

3.1 设计思路

集成 VPN 采用 5 层虚拟的设计理念,第一层虚拟采用 GRE 建立 VPN,使其能承载用户不同类型的私网数据;第二

层虚拟由 IPSEC 建立 VPN，对承载的数据进行安全保护；第三层虚拟由 IRF 将多台物理设备虚拟成一个资源池，由资源池中的物理设备共同承载用户的数据；第四层虚拟采用 MPLS 在公网建立 VPN，为不同用户私网数据在公网中传输提供路径；第五层虚拟采用 BGP，给不同用户分配不同的标签，构建每个用户单独的 VPN。上述策略构建的集成 VPN 能承载丰富的数据类型，对承载的数据提供机密性、完整性保护，为不同用户构建其独立 VPN，隔离不同用户的数据，实现地址的复用，并能负载分担不同用户的私网数据，融合了 GRE，IPSEC，MPLS，BGP，IRF 技术的优点。

3.2 网络模型

为了验证该设计思路的可用性与可操作性，构建所需的网络模型，如图 1 所示。实验的目的是实现图 1 中 X 与 Y 用户总部与分部私网数据的交互，对不同用户的私网数据进行访问控制与隔离，实现不同用户私网数据的负载分担，并保障数据交互的安全。

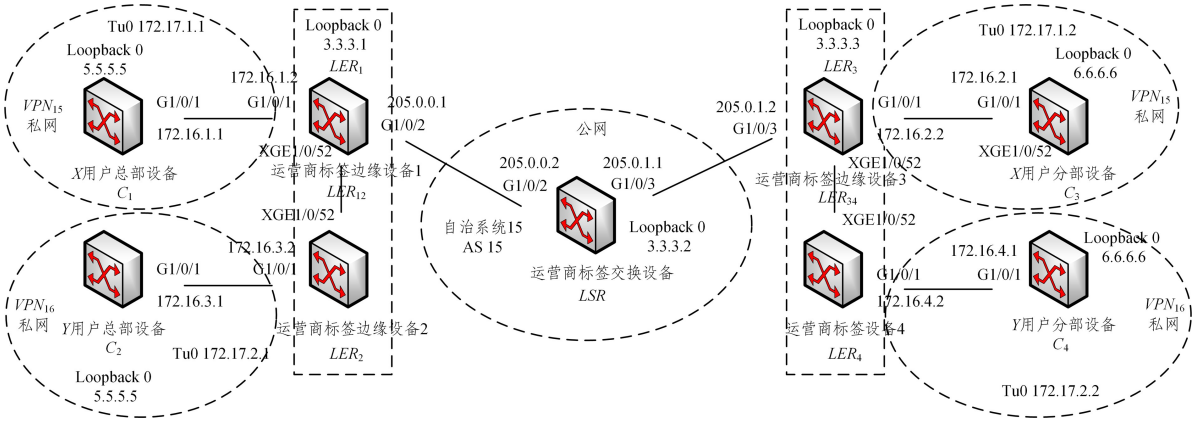

图 1 方案设计的网络模型

Fig. 1 Network model of the designed scheme

为使后续阐释简明扼要，对网络模型中的名称进行定义。X 用户总部与 Y 用户总部中的 loopback 地址模拟需要承载的总部私网数据，分别用 D_1 与 D_2 表示。X 用户分部与 Y 用户分部中的 loopback 地址模拟需要承载的分部私网数据，分别用 D_3 与 D_4 表示；X 用户总部设备与 Y 用户总部设备分别用 C_1 与 C_2 表示；X 用户分部设备与 Y 用户分部设备分别用 C_3 与 C_4 表示；连接 X 用户总部设备的运营商标签边缘设备 1 表示为 LER_1；连接 Y 用户总部设备的运营商标签边缘设备 2 表示为 LER_2；运营商标签边缘设备 1 与运营商标签边缘设备 2 虚拟化后的设备表示为 LER_{12}；连接 Y 用户分部设备的运营商标签边缘设备 3 表示为 LER_3；连接 Y 用户分部设备的运营商标签边缘设备 4 表示为 LER_4；运营商标签边缘设备 3 与运营商标签边缘设备 4 虚拟化后的设备表示为 LER_{34}；运营商标签交换设备用 LSR 表示；X 用户总部与分部构建的 VPN 表示为 VPN_{15}；Y 用户总部与分部构建的 VPN 表示为 VPN_{16}；自治系统 15 表示为 $AS15$。

3.3 方案设计

实现图 1 所示网络模型中各总部与分部私网数据的交互，同时保障交互时数据的安全性，且负载分担、识别与隔离不同用户的数据，需在网络模型部署与融合 GRE，IPSEC，IRF，MPLS 以及 BGP 技术。首先采用 GRE 封装需承载的私网数据，其次采用 IPSEC 对 GRE 承载的数据进行安全保护，再次采用 IRF 实现不同用户数据的负载分担，最后采用 BGP 识别与隔离不同用户数据，并通过 MPLS 在公网中建立承载私网用户数据的路径。上述技术承载私网数据的数据封装过程及承载路径，如图 2 所示。

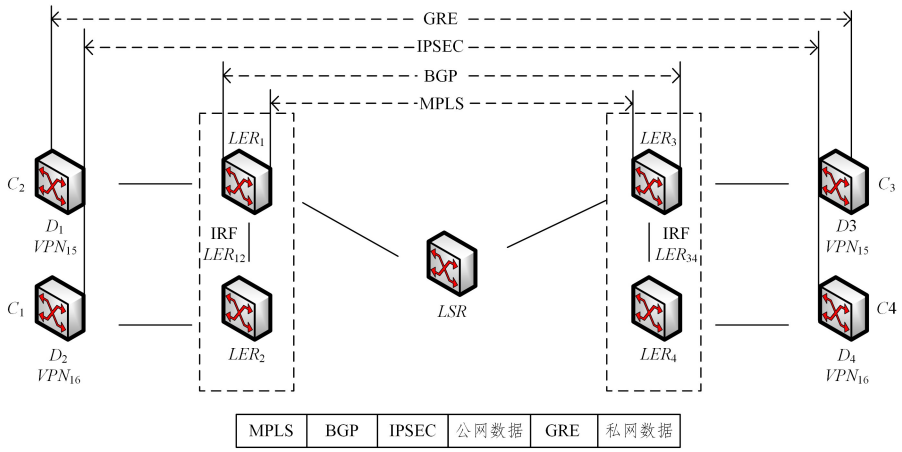

图 2 集成 VPN 的各技术的隧道路径与数据封装

Fig. 2 Tunnel path and data packaging of each technology of integrated VPN

实现图 2 中各总部与分部私网数据的交互，识别与隔离、负载分担、安全保护不同用户的私网数据，需要在网络模型中

完成 GRE VPN 的建立、IPSEC VPN 的建立、网络设备虚拟化、MPLS VPN 的建立、私网数据的识别与隔离 5 个关键步骤。

1)GRE VPN 的建立

因公网无法识别私网数据,故需要将私网数据进行封装。考虑到私网数据存在单播、组播、广播数据类型,方案采用能同时支持承载 3 种数据类型的 GRE 技术。使用 GRE 技术承载私网数据,需在 C_1 与 C_3、C_2 与 C_4 设备上完成 3 个主要部署:(1)在 C_1 与 C_3、C_2 与 C_4 上采用 interface tunnel 指令创建承载私网数据的逻辑接口;(2)在逻辑接口下指定封装 GRE 报文头的源与目的公网地址;(3)在 C_1 与 C_3、C_2 与 C_4 上部署到目的私网的路由。

2)IPSEC VPN 的建立

因需要确保私网数据的机密性与完整性,故采用 IPSEC 技术承载 GRE 封装的私网数据。由于私网数据已被 GRE 封装,且 GRE 被其逻辑接口下部署的源与目的公网地址封装,因此 IPSEC 只需对 GRE 外层的源与目的公网地址进行安全保护,即可以确保 GRE 内层私网数据的机密性与完整性。采用 IPSEC 技术确保数据的安全,首先需在 C_1 与 C_3、C_2 与 C_4 上采用访问控制列表,以匹配需要保护的数据;继而在 C_1 与 C_3、C_2 与 C_4 上执行 ipsec transform-set 指令进入安全提议视图,在视图下完成安全协议工作模式、安全协议加密算法、验证算法的选择;接着运行 ike keychain 与 ike profile 指令,协商双方的预共享密钥;然后执行 ipsec policy 指令,在安全策略视图下引用访问控制列表保护的数据、引用安全提议、引用 ike;最后将安全策略应用于 C_1,C_2,C_3,C_4 设备的 G1/0/0 接口,保障承载数据的机密性与完整性。

3)网络设备虚拟化

GRE 与 IPSEC 技术融合构建的 VPN,能承载单播、组播、广播的数据类型,且能加强数据的安全,但上述技术的融合未能解决数据的负载分担问题。而 IRF 技术将多台物理设备虚拟成一个资源池,由资源池中多台物理设备共同承载数据的转发。实现 LER_1 与 LER_2、LER_3 与 LER_4 负载分担用户私网数据,先需采用 irf member member-id renumber new-member-id 给 4 台设备分配不同的成员编号,进而标识设备在资源池中的身份;然后执行 irf-port member-id/port-number 指令进入 IRF 端口视图,将图 1 中的 LER_1 与 LER_2、LER_3 与 LER_4 相连的物理端口加入 IRF 端口下进行管理;最后执行 irf-port-configuration active 指令,激活网络设备虚拟化的配置,则将 LER_1 与 LER_2 虚拟成 LER_{12},LER_3 与 LER_4 虚拟成 LER_{34},由两台物理设备共同承载私网数据的转发。

4)MPLS VPN 的建立

GRE,IPSEC,IRF 技术融合构建的 VPN 支持能承载多种数据类型,保障了数据的安全,并实现了数据的负载分担,但实现用户总部与分部私网数据的交互,还需在运营商的网络中采用 MPLS 技术建立逻辑通道。逻辑通道的建立需在运营商的网络中执行 mpls lsr-id 指令,给不同的设备标识其身份,并运行 mpls ldp 指令给图 1 拓扑中的 LER_{12},LSR,LER_{34} 指定分配标签的协议。同时在 LER_1,LSR,LER_3 相连的接口下执行 mplsenable 与 mpls ldp 指令,启用接口 mpls 功能,并给 LER_1,LSR,LER_3 设备的 loopback 地址分配标签,进而构建承载私网数据的标签转发路径。

5)私网数据的隔离与识别

因 C_1 与 C_2、C_3 与 C_4 采用了相同的 loopback 地址,导致标签边缘设备 LER_{12} 与 LER_{34} 的路由表学习到相同的 loopback 地址的路由,产生了冲突。而多进程技术与虚拟路由技术的多实例的每个进程与每个实例有独立的路由表,且路由表间相互隔离,为解决路由冲突提供了思路。以 LER_{12} 为例,阐释如何解决路由冲突问题。具体的实现需在 LER_{12} 上创建 2 个进程与 2 个实例,如进程与实例名都为 15 和 16,名称相同的进程与实例绑定。进程 15 与进程 16 路由表分别用于接收 C_1 和 C_2 发送过来的路由,且接收后将路由导入各自绑定的实例路由表中,实现路由的隔离,解决了路由冲突,且实现了地址的复用。LER_{34} 设备上学习 C_3 与 C_4 相同的 loopback 地址的路由,解决冲突的方法与 LER_{12} 相同,在此不重复赘述。

上述方法解决了 LER_{12} 收到 C_1 与 C_2、LER_{34} 收到 C_3 与 C_4 发送相同 loopback 地址的路由,并产生冲突的问题。而 LER_{12} 通过 MPLS 建立的路径收到 LER_{34} 发送过来的 loopback 地址的路由,识别不了 loopback 地址是属于 C_3 还是 C_4。同样,LER_{34} 收到 LER_{12} 发送过来的 loopback 地址的路由,也不清楚是属于 C_1 还是 C_2。为了识别路由的来源,在 LER_{12} 与 LER_{34} 上,分别执行 ip vpn-instance vpn-instance-name 指令,创建 2 个实例 15 和 16,给两台设备相同的实例分配同样的 BGP 的 RT(Route Target)属性值,不同的实例 RT 值不同。进而使 LER_{12} 与 LER_{34} 实例 15、实例 16 路由表下的路由有相同的 RT 值。LER_{12} 与 LER_{34} 通过 BGP 技术交互总部与分部的 loopback 地址的路由,根据路由携带的 RT 值识别其来源,与自身实例相同的 RT 值的路由则接收,否则丢弃。进而使 LER_{12} 与 LER_{34} 交互 loopback 地址的路由时,能识别路由的来源,并将 loopback 地址的路由接收到对应的实例路由表中,为后续各总部与分部私网数据的访问夯实了基础。

当 C_1 设备访问 C_3 的 loopback 地址,访问数据到达 LER_{34},LER_{34} 查询实例路由表,发现实例 15 路由表与实例 16 路由表都有匹配该访问数据的路由,导致 LER_{34} 无法判断选哪一个实例路由表转发该数据。针对上述问题,采用 BGP 的 Lable 属性来解决。通过 BGP 的 Lable 属性,在 LER_{34} 给 C_3 与 C_4 的 loopback 地址的路由分配不同的 Lable 属性值,将 C_3 与 C_4 的 loopback 地址的路由携带的 Lable 属性值发送给 LER_{12}。当 C_1 设备访问 C_3 的 loopback 地址的数据到达 LER_{12},LER_{12} 使用 LER_{34} 给 C_3 分配的 Lable 属性值封装该访问数据,LER_{12} 通过 MPLS 建立的路径将访问数据发送给 LER_{34},LER_{34} 根据封装的 Lable 属性值选择存放 C_3 的 loopback 地址路由的实例路由表转发该数据,进而实现 C_1 设备能访问 C_3 的 loopback 地址。针对 C_3 访问 C_1 的 loopback 地址,以及 C_2 与 C_4 设备 loopback 地址的相互访问,采用上述方法即可解决,在此不重复撰述。

4 性能分析与评估

4.1 方案测试与验证

为验证上述方案设计是否完成预定的目标,依托新华三

技术有限公司开发的 H3C Cloud Lab 仿真平台（该仿真平台将真实设备的操作系统导入，能完全模拟真实设备所有功能特性），对方案的隧道建立、资源池的建立、MPLS 标签路径的构建、数据的隔离与识别进行验证。

1）GRE 与 IPSEC 隧道验证

方案的设计能承载多种类型的数据，并能保障承载数据的机密性与完整性。上述功能实现的关键是，需在 C_1 与 C_3、C_2 与 C_4 上建立承载私网数据的 GRE VPN 的隧道，以及 IPSEC VPN 的隧道。再分别在 C_1 与 C_2 上执行 display interface Tunnel 0 brief 与 display ike sa，结果如图 3 所示。

```
[C1]display interface Tunnel 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Tun0                 UP   UP       172.17.1.1
[C1]display ike sa
   Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
   1               172.16.2.1            RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
[C2]display interface Tunnel 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Tun0                 UP   UP       172.17.2.1
[C2]display ike sa
   Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
   1               172.16.4.1            RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

图 3　GRE VPN，IPSEC VPN 隧道建立

Fig. 3　Tunnel establishment of GRE VPN and IPSEC VPN

图 3 中 C_1 与 C_2 承载私网数据的 Tun 0 接口物理状态与协议状态显示为 up，说明承载私网数据的 GRE VPN 隧道已建立；而 Flag 的 RD 状态则表明 IPSEC VPN 已保护私网数据安全。

2）网络资源池验证

上文已验证 GRE VPN 与 IPSEC VPN 隧道工作正常，意味着方案设计已支持承载多种数据类型，并能确保数据交互时的机密性与完整性。而能否实现数据负载分担，分别在 LER_{12} 与 LER_{34} 上运行 display irf，查看网络资源池建立状态，结果如图 4 所示。图 4 中 Role 的状态结果为 Master 与 Standby，有力证实了 LER_1 与 LER_2、LER_3 与 LER_4 的资源池已建立，由 2 台设备共同分担数据的传输，解决单台设备承载数据负载过重所导致的数据传输异常问题。

```
<LER12>display irf
MemberID    Role     Priority  CPU-Mac         Description
 *+1        Master   1         6a60-1aaf-0104  ---
  10        Standby  1         6a60-1f61-0204  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 6a60-1aaf-0100
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 5
<LER34>display irf
MemberID    Role     Priority  CPU-Mac         Description
 *+1        Master   1         6a60-2d1e-0404  ---
  10        Standby  1         6a60-32d9-0504  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 6a60-2d1e-0400
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 5
```

图 4　网络资源池状态结果

Fig. 4　Status of network resource pool

3）MPLS 标签路径验证

实现不同用户总部与分部私网数据的交互，需要在运营商的网络中运用 MPLS 建立标签路径，提供承载私网数据的通道。在运营商的 *LSR* 设备执行 display mpls ldp lsp 指令，结果如图 5 所示。图 5 显示 LER_1、*LSR*、LER_3 的 loopback 接口，MPLS 已分配标签，生成了承载私网数据的标签转发路径。

```
<LSR>display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 3          Ingress: 2          Transit: 2          Egress: 1

FEC              In/Out Label        Nexthop         OutInterface
3.3.3.1/32       -/1279(L)
                 -/3                 205.0.0.1       GE1/0/2
                 1151/3              205.0.0.1       GE1/0/2
3.3.3.2/32       3/-
                 -/1278(L)
                 -/1151(L)
3.3.3.3/32       -/1150(L)
                 -/3                 205.0.1.2       GE1/0/3
                 1150/3              205.0.1.2       GE1/0/3
```

图 5　MPLS 标签转发表

Fig. 5　MPLS label repost

4）数据隔离与识别验证

两个总部与分部采用相同的地址，导致运营商的 LER_{12} 与 LER_{34} 学习到相同的地址，产生冲突。方案采用多进程与虚拟路由技术多实例相融合，解决了上述问题。在 LER_{12} 与 LER_{34} 分别执行 dis ip ro vpn-instance vpn15 5.5.5.5 to 6.6.6.6 | begin Destination 与 dis ip ro vpn-instance vpn16 5.5.5.5 to 6.6.6.6 | begin Destination 指令，结果如图 6 所示。

```
[LER12]dis ip ro vpn-instance vpn15 5.5.5.5 to 6.6.6.6 | begin Destination
Destination/Mask    Proto   Pre Cost      NextHop         Interface
5.5.5.5/32          O_INTRA 10  1         172.16.1.1      GE1/0/1
6.6.6.6/32          BGP     255 2         3.3.3.3         GE1/0/2
[LER12]dis ip ro vpn-instance vpn16 5.5.5.5 to 6.6.6.6 | begin Destination
Destination/Mask    Proto   Pre Cost      NextHop         Interface
5.5.5.5/32          O_INTRA 10  1         172.16.3.1      GE10/0/1
6.6.6.6/32          BGP     255 2         3.3.3.3         GE1/0/2
[LER34]dis ip ro vpn-instance vpn15 5.5.5.5 to 6.6.6.6 | begin Destination
Destination/Mask    Proto   Pre Cost      NextHop         Interface
5.5.5.5/32          BGP     255 2         3.3.3.1         GE1/0/3
6.6.6.6/32          O_INTRA 10  1         172.16.2.1      GE1/0/1
[LER34]dis ip ro vpn-instance vpn16 5.5.5.5 to 6.6.6.6 | begin Destination
Destination/Mask    Proto   Pre Cost      NextHop         Interface
5.5.5.5/32          BGP     255 2         3.3.3.1         GE1/0/3
6.6.6.6/32          O_INTRA 10  1         172.16.4.1      GE10/0/1
```

图 6　LER_{12} 与 LER_{34} 的实例路由表

Fig. 6　Example routing table of LER_{12} and LER_{34}

图 6 中的结果表明，LER_{12} 与 LER_{34} 分别将 C_1 与 C_2、C_3 与 C_4 发送过来的路由存入对应的实例路由表，且 LER_{12} 与 LER_{34} 通过 BGP 技术完成了各总部与分部私网路由的交互，实现了不同用户路由的隔离及地址的复用。

C_1 设备访问 C_3 的 loopback 地址，访问数据到达 LER_{34}，LER_{34} 需根据 BGP 的 Lable 属性分配的标签值决定选用哪一个实例路由表来转发数据，在 LER_{34} 与 LER_{12} 分别运行 display bgp routing-table vpnv4 inlabel | begin Network 与 display bgp routing-table vpnv4 outlable | begin Network，结果如图 7 所示。

```
<LER34>display bgp routing-table vpnv4 inlabel | begin Route
 Route distinguisher: 15:1
 Total number of routes: 2

     Network            NextHop         OutLabel        InLabel
* >  6.6.6.6/32         172.16.2.1      NULL            1149
* >  172.16.2.0/24      172.16.2.2      NULL            1151

 Route distinguisher: 16:1
 Total number of routes: 2

     Network            NextHop         OutLabel        InLabel
* >  6.6.6.6/32         172.16.4.1      NULL            1148
* >  172.16.4.0/24      172.16.4.2      NULL            1150
<LER12>display bgp routing-table vpnv4 outlabel | begin Route
 Route distinguisher: 15:1(vpn15)
 Total number of routes: 2

     Network            NextHop         OutLabel
* >i 6.6.6.6/32         3.3.3.3         1149
* >i 172.16.2.0/24      3.3.3.3         1151

 Route distinguisher: 16:1(vpn16)
 Total number of routes: 2

     Network            NextHop         OutLabel
* >i 6.6.6.6/32         3.3.3.3         1148
* >i 172.16.4.0/24      3.3.3.3         1150
```

图 7　BGP 的 Lable 属性给路由分配的标签

Fig. 7　Label assigned to a route by BGP's Lable attibute

图 7 中，LER_{34} 的 InLable 的 1 149 标签是 LER_{34} 给 LER_{12}

发布 6.6.6.6 路由时分配的标签，而 LER_{12} 中显示的 OutLable 的 1149 即为 LER_{34} 分配的标签。C_1 设备访问 C_3 的 loopback 地址的数据到达 LER_{12} 时，LER_{12} 则用 OutLable 的 1149 封装数据，封装好后通过 MPLS 建立的隧道转发给 LER_{34}，LER_{34} 根据标签 1149 则会选择 InLable 为 1149 的实例路由表转发该数据。

4.2 性能对比

为了评估方案的有效性与优越性，对集成 VPN 方案与传统方式采用独立技术构建的 VPN 进行定性与定量的对比分析。

1)定性对比

定性对比主要包括负载分担、机密性、数据隔离等 8 个维度，将集成 VPN 解决方案与文献[10]采用的 GRE VPN、文献[13]采用的 IPSEC VPN、文献[14]采用的 MPLS VPN 进行了对比。表 1 所列的对比情况充分说明采用集成 VPN 相比传统的 VPN 解决方案，支持的特性与功能更强、兼容性更好，优势突出。

表 1 集成 VPN 的优势

Table 1 Advantages of integrated VPN

特性	GRE	IPSEC	MPLS	集成 VPN
支持组播	支持	不支持	支持	支持
支持多协议	支持	不支持	支持	支持
支持负载分担	不支持	不支持	不支持	支持
支持机密性	不支持	支持	不支持	支持
支持完整性	不支持	支持	不支持	支持
支持数据隔离	不支持	实现复杂	支持	支持
支持数据识别	不支持	不支持	支持	支持
地址复用	不支持	不支持	支持	支持

2)定量对比

为凸显方案的优势，采集了方案 LER_{12} 设备的背板带宽、地址条目、维护表项(邻居表、进程与 IP 路由表、标签转发表)、端口速率与传统方案进行对比，并借助 EXCEL，导入采集的数据，利用带数据标记的折线图生成了相应的图表，如图 8—图 11 所示。

(1)背板带宽

背板带宽是衡量设备数据处理能力重要的指标之一。方案采用虚拟化技术将 2 台运营商的标签边缘设备构建为一个资源池，由 2 台设备共同分担数据的处理，有效增强了数据处理能力。目前新华三技术有限公司在运营商的网络中部署 VPN 时采用主流的 S6850 设备，图 8 给出了本文方案与文献[15]中的传统方案采用同样的 S6850 设备在背板带宽维度的对比。文献[15]中的传统方式未采用虚拟化，单台设备的背板带宽为 76.8 Tbps，而本文方案采用 H3C S6850 设备最大支持 10 台设备虚拟化，背板带宽达到 768 Tbps，方案的数据处理能力有明显的提升。

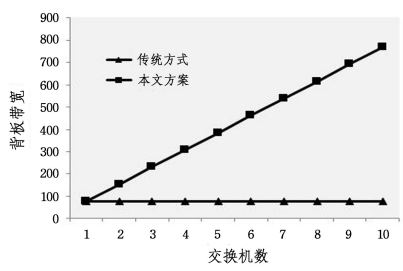

图 8 两种方案背板带宽的对比

Fig. 8 Comparison of backplane bandwidth of two schemes

(2)地址条目

文献[15]采用传统方式构建的 VPN 需每台标签边缘设备与标签交换设备相连，则需要分配 2 个地址给相连的设备接口，用于标识设备身份及完成路由信息的交互；传统方式每台标签边缘设备需给部署的 loopback 接口分配地址，用于在 MPLS 中标识其身份及完成标签的生成。而该方案采用网络设备虚拟化技术，最大支持 10 台物理设备虚拟成一台逻辑设备并与标签交换设备相连，10 台设备可以共用一个地址与相连的标签交换设备通信，共用一个 loopback 接口地址在 MPLS 中标识身份及完成标签的生成。随着运营商网络标签边缘设备的递增，该方案节省的地址优势更加明显，图 9 显示当运营商网络采用的标签边缘设备达到 350 台时，文献[15]中采用传统方式构建的 VPN 标签边缘设备与标签交换设备相连的地址需 700 个，用于在 MPLS 中标签设备身份的 loopback 地址需 350 个，共计 1050 个。而采用本方案相连的接口地址只需 70 个，loopback 地址只需 35 个，共计 105 个，大大节省了地址资源，减少了网络部署与维护的工作量。

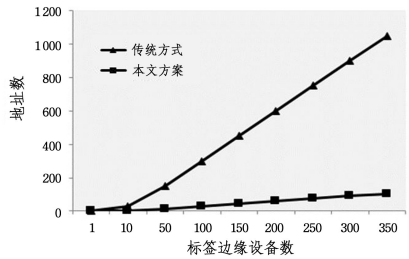

图 9 两种方案地址数的对比

Fig. 9 Comparison of the address number of two solutions

(3)维护表项

文献[15]采用传统方式构建的 VPN 每台标签边缘设备与标签交换设备交互路由时需维护 3 个表(邻居表、路由协议的路由表、IP 路由表)。为在运营商的网络中实现私网数据的交互，每台标签边缘设备还需建立标签的邻居表与标签转发表。而该方案支持设备虚拟化，可以让 10 台物理设备共享上述 5 个表，减轻了设备的负担，且方便管理。传统方式与本文方案维护表项的计算式如下。

传统方案维护表数的计算方式如下：

$$W=P\times J \tag{1}$$

其中，W 为维护表数，J 为网络中标签边缘设备数，P 为一台设备需要的维护表数。

本文方案维护表数的计算方式如下：

$$W=P\times J/10 \tag{2}$$

图 10 给出了文献[15]采用传统方式与本文方案维护表项的数据对比，网络中标签边缘设备为 300 台时，传统方式 1 台设备需维护 5 个表项，共计 1500 个。而该方案可以实现 10 个设备共享 1 个邻居表、路由协议的路由表、IP 路由表、标签邻居表、标签转发表，只需维护 150 个，减轻设备负载的优势凸显。

(4)端口速率

端口速率是衡量设备数据传输能力的关键指标之一，该

方案通过 IRF 虚拟化技术将多台标签边缘设备虚拟成一台逻辑设备，由多台标签边缘设备端口分担其数据传输，大大提升了数据的传输能力。该方案的端口速率的计算式如下：

$$V=\sum_{i=1}^{m}(10\times n_i+100\times q_i) \tag{3}$$

其中，V 表示该方案虚拟化后资源池中所有标签边缘设备所能提供的端口速率；m 为资源池中交换机的数量；n_i 表示第 i 个交换机端口速率为 10 Gbps 的数量；q_i 表示第 i 个交换机端口速率为 100 Gbps 的数量。

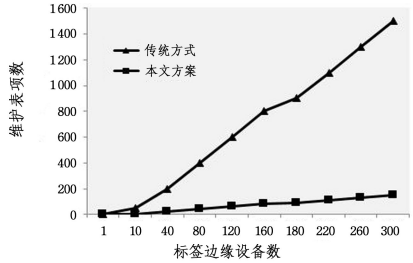

图 10 两种方案维护表项数对比

Fig. 10 Comparison of the number of maintenance table item of two schemes

本文方案采用的新华三通信有限公司的 S6850 设备最多能支持将 10 台物理设备虚拟化，1 台 S6850 设备主控板与业务板所有端口的端口速率为 1 280 Gbps，10 设备虚拟化后的端口速率为 12800Gbps。而文献[15]中的传统方式因各交换机独立运行，增加交换机并不能提升端口的数据传输能力。图 11 给出了两种方案在端口速率维度的对比，对比结果显示，在数据传输能力上，该方案明显优于传统方式。

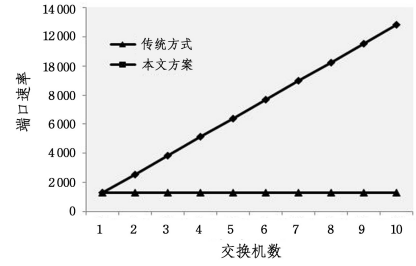

图 11 两种方案端口速率的对比

Fig. 11 Comparison of port rates of two schemes

结束语 为使构建的 VPN 能承载多种数据类型、保障传输数据的安全、识别与隔离不同用户的私网数据，本文提出了集成的 VPN 解决方案，构建方案所需的网络模型，在网络模型中部署与实施该设计理念。为验证方案的可用性与优越性，对 GRE 与 IPSEC 隧道、网络资源池、MPLS 标签路径、数据隔离与识别进行了测试与验证，测试与验证结果表明方案达到了预期目标。同时，将本文方案与传统方式构建的 VPN 在背板带宽、端口速率、地址条目、维护表项以及表 1 所列的 8 个维度进行了对比分析，分析结果表明该方案在数据处理能力、数据传输安全、可管理性与可维护性等方面优势突出。目前未购买测试方案的丢包数、收敛比的设备，后续购买设备后将完成上述指标的测试。另外，后续将研究集成 VPN 在跨域 VPN 中的应用。

参 考 文 献

[1] HAI P N P, HONG H N, QUOC B B, et al. A Comparative Research on VPN Technologies on Operating System for Routers [C]// 2021 International Conference on Advanced Technologies for Communications (ATC). IEEE, 2021: 89-93.

[2] JUMA M, MONEM A A, SHAALAN K. Hybrid end-to-end VPN security approach for smart IoT objects [J]. Journal of Network and Computer Applications, 2020, 158: 102598.

[3] ESPER D A, DATTA S, ROY M. Implementing Protection on Internal Networks using IPSec Protocol [C]// 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2022, 1: 378-383.

[4] OJHA P D, HANSDAH R C. A Heuristic Approach to Detect MPLS L3 VPN Misconfiguration in Multi-Homed Multi-VRF Site-Redundant CE Environments [J]. IEEE Transactions on Network and Service Management, 2020, 18(2): 2294-2307.

[5] SLLAME A M. Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks [C]// 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA). IEEE, 2022: 32-37.

[6] YAN J, LI F. Application of Network Security in Data Center Based on Private Cloud [C]// 2023 5th International Conference on Decision Science & Management (ICDSM). IEEE, 2023: 178-183.

[7] GAO Y. Newenergy vehicle engine speed control method based on vehicle networking technology [J]. Journal of Computational Methods in Sciences and Engineering, 2022, 22(6): 2201-2215.

[8] VARVELLO M, AZURMENDI I Q, NAPPA A, et al. VPN-zero: a privacy-preserving decentralized virtual private network [C]// 2021 IFIP Networking Conference (IFIP Networking). IEEE, 2021: 1-6.

[9] XIE Y, ZHANG C, HE X, et al. Application research of meteorological virtual private network security remote access technology [C]// 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2023, 6: 423-426.

[10] LIN Q L, HU X M, LI P. Under the epidemic situation, we networking technology research on large-scale live broadcast teaching [J]. Computer Technology and Development, 2021, 31(6): 140-145.

[11] AMALDEEP S, SANKARAN S. Cross Protocol Attack on IPSec-based VPN [C]// 2023 11th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2023: 1-6.

[12] HE W, ZHAO Y, LIU Z, et al. Design of Dual-link Shared GRE over IPSec VPN on P2MP Networks [C]// 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA). IEEE, 2023: 1781-1783.

[13] AMALDEEP S, SANKARAN S. Cross Protocol Attack on IPSec-based VPN [C]// 2023 11th International Symposium on

Digital Forensics and Security(ISDFS). IEEE, 2023: 1-6.
[14] KOMALA C R, HEMA M, GOYAL H R, et al. Performance Evaluation of VPNS over MPLS-Linux Networks[C]// 2023 International Conference on Advances in Computing, Communication and Applied Informatics(ACCAI). IEEE, 2023: 1-7.
[15] LI Y F. Based on BGP MPLS VPN Cross-the-domain Group Simulation Design [J]. Laboratory Research and Exploration, 2021, 40(3): 121-128.
[16] LI F, SHEN H T, SHI L, et al. A mpls-based power line carrier communication can distinguish the fault recovery mechanism [J]. The Journal of Tailhrtz Science and Electronic Information, 2023, 21(8): 997-1001.
[17] QURESHI K N, AHMAD E, ANWAR M, et al. Network functions virtualization for mobile core and heterogeneous cellular networks[J]. Wireless Personal Communications, 2022, 122(3): 2543-2559.
[18] JAFF A. Software Defined Networking Automation Using OpenDaylight and Network Virtualization for security and scalability: A network enterprise case[C]// ITM Web of Conferences. EDP Sciences, 2022, 42: 01014.
[19] EMMANUEL T, MICHEL D D E, AGBOR E O B. Virtualization of a 4G Evolved Packet Core Network Using Network Function Virtualization(NFV) Technology with NS3 for Enterprise and Educational Purpose[J]. American Journal of Networks and Communications, 2024, 13(1): 1-18.
[20] SALAGRAMA S, BIBHU V. Study of it and data center virtualization[C]// 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM). IEEE, 2022, 2: 274-278.

TAO Zhiyong, born in 1980, postgraduate, associate professor, is a member of CCF (No. C3683M). His main research interests include network communication and cloud computing.

YANG Wangdong, born in 1974, Ph.D, professor, Ph.D supervisor, is a member of CCF (No. 34909M). His main research interests include network communication, cloud computing, software engineering.

(责任编辑:喻藜)