文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

在云计算中 VPN 网络安全技术的应用

卢月静　靳守业　高思宇　杨莹莹
北京市数字农业农村促进中心
DOI:10.12238/acair.v2i3.8655

[摘　要] 在当前的云计算安全防护中,VPN技术是最为典型且常用的一种技术。因此,随着云计算技术和相关服务的不断发展,VPN技术在网络安全中的应用也开始备受关注。基于此,本文便对其在云计算中的应用进行分析。包括VPN技术模式下的隧道技术、访问控制技术、加密认证技术以及密码交换技术的应用。希望此次分析可以为VPN技术的应用与云计算网络安全质量的提升提供科学指导。
[关键词] VPN技术；云计算；网络安全；访问控制；加密认证
中图分类号：TN915.08　文献标识码：A

The Application of VPN Network Security Technology in Cloud Computing

Yuejing Lu　Shouye Jin　Siyu Gao　Yingying Yang
Beijing Digital Agriculture and Rural Promotion Center

[Abstract] VPN technology is the most typical and commonly used technology in current cloud computing security protection. Therefore, with the continuous development of cloud computing technology and related services, the application of VPN technology in its network security has also begun to receive much attention. Based on this, this article analyzes its application in cloud computing. Including the application of tunneling technology, access control technology, encryption and authentication technology, and password exchange technology in VPN technology mode. I hope this analysis can provide scientific guidance for the application of VPN technology and the improvement of cloud computing network security quality.
[Key words] VPN technology; Cloud computing; Network security; Access control; Encryption authentication

前言

在通过VPN技术对云计算条件下的网络安全进行防护时,研究者首先应明确此项技术及其在云计算网络安全防护中的应用优势,然后再以此为依据,结合当前的云计算技术及其服务现状,将VPN技术合理应用其中,以此来有效确保云计算条件下的网络安全。这对于VPN技术的合理应用与云计算网络安全性的提升都将十分有利,从而可促进云计算技术及其相关服务的绿色化发展。

1 VPN技术及其在云计算网络安全防护中的应用优势

VPN技术又叫做虚拟专用网络技术,它是针对互联网类公共网络所设计的一种临时性虚拟化网络,其中涉及到的主要技术包括隧道技术、访问控制技术、加密认证技术以及密码交换技术等。在上述各项先进技术的支持下,VPN网络具备了良好的安全性、加密性以及可认证性特征。

在云计算条件下,VPN技术的主要应用优势是可借助其中的各项安全技术对既有云计算网络进行合理的规划设计,从而为其建设一个可信度足够高、安全性足够强的虚拟化云计算网络。凭借此项优势,VPN技术在现代云计算领域中备受关注,而其应用策略也成为众多云计算研究者和技术人员的重点研究内容。

2 VPN网络安全技术在云计算中的应用分析

2.1隧道技术在云计算中的应用

隧道技术是VPN技术中的关键组成部分,同时也是云计算中最重要的一项VPN技术。就当前的云计算网络安全防护来看,基于VPN安全防护的隧道技术及其应用策略如下：

首先是IP安全标准(IPSee)。在云计算环境中,此项技术可确保用户IP的安全性,其实现方法是采用身份验证、完整性校验以及保密性检验等方法来保护云计算环境中的各类数据资源。其安全协议中封装着可保护数据安全的认证头(AH)以及安全荷载(ESP),前者可保护数据完整性,后者可保护数据完整性与机密性。针对云计算中的安全参数,IPSee主要通过互联网密钥交换技术(IKE)完成协商。将安全联盟(SA)建立在两节点之间,规定数据传输中的协议保障、策略保障和有效管理期内的各类重要因素保障。云计算数据一旦在传输时发生重新阐述情况,全新的附加报头或AH、ESP便会随之生成,该报头也将会得到密

封处理,且加密处理后的用户数据会包含在新的原始IP数据包里。传输中,附加报发只根据传输功率控制(TPC)和用户数据协议(UDP)等原始传输层数据计算,已经过加密处理的附加报发和原始传输层数据计算则在原始IP报头里执行。

其次是网络之间数据包封装隧道协议(GRE),该协议可实现某一协议在另一协议中的封装,以及某一路由与另一路由的通信,从而可实现某一端路由与其他多端路由的数据传输。在云计算环境下的VPN结构里,常规主机网络可以地址形式与路由之间实现物理连接,从而为云计算中的众多数据建立传输通道。在此过程中,我们可将VPN与主机网络之间的交互节点用作GCR通道中的起讫点,如此便可将VPN与网络主机中的路由数据隔开,使同一空间地址在众多VPN中得到同时应用,从而进一步确保云计算中的数据安全。

最后是点对点隧道协议(PPTP),该协议是在传统点对点协议(PPP)基础上诞生的一种新型云计算安全隧道协议。在云计算环境中,该协议的主要实现流程是先采用PPP协议实施数据封装,再采用PPTP协议封装PPP协议中的信息,最后将其集成到IP消息、帧中继以及异步传输模式(ATM)里。在云计算VPN的创建过程中,PPTP需要连接网络附属存储(NAS),并由后者控制。在此过程中,如果采用VPN协议中跨越第二层点对点连接协议封装机制(L2PT)与服务器连接,该协议便可对用户地址做出准确识别,其安全性较PPTP更强。基于此,若云计算环境下的用户较为集中且稳定,我们可通过L2TP与服务器连接;若云计算环境中的用户具有较强流动性,则需要通过PPTP与服务器连接。表1为云计算条件下的VPN隧道技术PPTP与L2TP对比情况：

表1-云计算条件下的VPN隧道技术PPTP与L2TP对比情况

序号	项目	PPTP	L2TP
1	适用环境	大部分	特殊网络、较高安全性要求
2	连接速度	非常快	较快
3	安全性	较高	非常高
4	使用要求	必须为 IP 网络	不同类型网络
5	隧道数	单一隧道	多隧道
6	字节数	6 字节	4 字节
7	是否支持隧道验证	不支持	支持

2.2访问控制技术在云计算中的应用

就目前的云计算网络安全防护工作来看,访问控制技术也是一项典型且常用的VPN技术。作为云计算环境条件下的一款常用虚拟化网络传输技术,VPN技术的一个重要安全防护作用就是控制用户访问。在此项技术的支持下,每一名云计算用户都将拥有一个独属于自己的云计算网络空间和数据访问权限,其权限程度需通过基于云计算的VPN服务商以及云计算网络数据供应商之间的共同协商来确定,以此来实现云计算数据资源安全的最佳保护。

在当前的云计算网络环境中,基于VPN技术的用户访问控制主要有两种策略,第一是通过设定个人身份或团队身份的方式来实施选择性访问控制；第二是根据云计算网络信息的敏感程度来实施访问控制。对于第一种访问控制策略,我们可直接将VPN技术嵌入到云计算网络平台中,以此来实现此项访问控制策略;对于第二种访问控制策略,我们可将云计算平台中的信息敏感程度作为依据,结合实际情况,在VPN技术支持下设置相应的用户访问权限,以此来实现此项访问控制策略。

2.3加密认证技术在云计算中的应用

在通过VPN技术对云计算条件下的网络安全实施防护的过程中,加密认证技术也是一项典型且关键的安全防护技术。其基本实现方法是在通过VPN进行云计算数据传输时,我们需要在隧道起点位置做好待传输数据的加密处理,在隧道终点对其实施解密处理,以免非法用户入侵云计算平台,获取云计算网络中传输的数据,从而使云计算环境下的网络数据安全得到良好防护。

首先是加密技术,在以往的云计算环境下,VPN网络中的常用加密与解密算法需通过数据加密标准(DES)以及三重数据加密算法(3DES)来执行。但是此种执行方法存在较多不足,比如密钥数量众多,管理难度大;密钥传输过程中有很多潜在风险存在等。针对上述情况,具体应用时,我们可通过混合加密体系对需要在云计算网络环境中传输的数据进行加密处理,即通过单钥密码对数据进行加密和解密处理,通过双钥密码对密钥进行传输处理。如此既可以提升云计算网络中的密钥传输速度,也可以对云计算环境下的数据信息做到有效保密。

其次是认证技术,该技术是避免云计算网络数据信息受到恶意攻击的关键,因此也是VPN技术实际应用中的一项重要安全防护技术措施。因此,在对云计算环境中的数据信息进行传输和交换之前,通信双方有必要先实施相应的安全认证,在确定数字证书与认证条件相符之后,通信双方才可以开始网络数据传输和交换。就目前的云计算环境来看,在VPN技术的实际应用中,最常用的一种身份认证方式是口令认证,即通过密码输入的方式进行认证,若系统确定用户输入的密码与其内部储存的密码一致,则表示认证成功,用户可通过VPN技术在云计算网络中进行数据传输与交换,否则,VPN技术将不为其提供数据传输与交换服务。除此之外,用户还可以根据实际情况选择其他的安全认证方法,比如动态令牌认证、质询握手验证协议认证以及数字证书认证等。如此便可对云计算环境中的网络数据做出良好的安全防护,防止数据在VPN传输过程中出现被盗、篡改或丢失等情况。

2.4密钥交换技术在云计算中的应用

密钥交换技术(IKE)是通过VPN技术对云计算网络实施安全防护时的一项关键技术,此项技术主要基于IPSee定义所设置的特殊交换方式来实施密钥交换。在此项技术中,因特网安全联盟和密钥协议(ISAKMP)、密钥确定协议(OAKLEY)以及安全密钥交

换机制(SKEME)实现了有机结合。在这些协议与机制的共同支持下,此项技术在商讨协议共享策略和生成数据验证加密等各种技术方面都独具个性。同时,在IKE技术中,也集成了当前先进的对称加密模型、非对称加密模型以及哈希函数等,从而能够为云计算环境下的网络安全防护提供多种密钥交换模式,以及不同密钥交换模式下的不同选项。就目前的云计算环境来看,在具体的网络安全防护中,常用的IKE密钥交换模式主要包括主动密钥交换模式、积极密钥交换模式以及快速密钥交换模式。而其主要的层次架构有两个,第一个层次叫做IKE SA,该层次是由主动密钥交换模式以及积极密钥交换模式共同组成；第二个层次叫做IPSEC SA,该层次是由快速密钥交换模式构成。

具体应用时,根据ISE技术规则,对于云计算环境中各种数据信息,我们应采取身份验证、共有绘画密钥处理以及协定加密算法等方式来进行安全防护。密钥交换时,我们不可以直接在非安全状态下的网络环境中传递密钥,而是应采取一系列安全数据的形式来完成密钥交换。以此来实现通信双方密钥的及时、有效确定和共享,这也是IKE技术在云计算环境中的一大应用特色。为满足上述密钥交换与共享需求,在基于VPN技术的云计算网络安全防护工作中,我们可将Diffie-Hellman协议引入其密钥交换里。该协议是OAKLEY技术中的一个关键组成部分,也是一种具有很多奇妙特征的密钥交换协议和算法。具体应用时,其奇妙之处在于云计算环境下的通信双方需在该协议的支持下确定一个对称密钥,采用该密钥对需要在云计算网络中传输的数据进行加密处理以及解密处理。但是在此过程中,该协议只用来实现密钥交换,并不能用来对云计算环境中需通过VPN传输的网络数据进行加密与解密处理。在通信双方确定了所需密钥并完成交换后,需根据密钥中的实际操作算法来完成数据加密以及数据解密。因Diffie-Hellman 协议计算具有非常高的复杂度,所以在密钥交换中也就具备了非常高的安全级别,从而可为云计算环境中的密钥交换提供有力的技术支持,尽最大限度确保云计算网络安全性。另外,在具体的密钥交换过程中,IKE技术还可以通过短信验证码发送、电子签名以及非对称加密等技术方法对用户实施身份验证,从而进一步提升密钥交换的安全性,对整体云计算网络安全防护做出合理优化。

3 结束语

综上所述,VPN是当前云计算网络环境中的一种主要传输技术。在云计算平台与相关服务的实际应用中,通过VPN虚拟专用网络的合理构建与应用,可以为用户的网络数据传输、获取与共享等提供有力支持。考虑到此项技术传输的安全性,我们需要结合当前的云计算网络通信情况,对基于VPN的网络安全防护技术进行深入研究,并结合实际需求,将其合理应用到云计算网络环境中,以此来为VPN数据传输提供良好的安全保障,进一步确保整体云计算网络环境中的数据安全。这对于VPN技术应用质量的提升以及云计算网络安全的保障都将十分有利,从而可支持云计算技术在当今时代中的绿色化与可持续发展。

[参考文献]

[1]傅江辉.基于云计算的社交网络安全隐私数据融合方法[J].济南大学学报(自然科学版),2021,35(1):29-33.

[2]朱冬梅,金志蕾.云计算中的安全技术综述[J].中国新通信,2016,18(4):152.

[3]张振峰,张志文,王睿超.网络安全等级保护2.0云计算安全合规能力模型[J].信息网络安全,2019(11):1-7.

作者简介：

卢月静(1977--),女,汉族,北京人,大学本科,工程师,研究方向：农业信息化。

靳守业(1982--),男,汉族,山西大同人,硕士,工程师,研究方向：农业信息化。

高思宇(1978--),男,满族,北京人,大学本科,工程师,研究方向：农业信息化。

杨莹莹(1997--),女,汉族,河北人,硕士研究生,研究方向：农业信息化。