

L2TP over IPSec 技术在私有桌面云中的应用

杨菲菲,孙 婧,王 彬
(国家气象信息中心,北京 100081)

摘 要:随着国家气象信息中心内部私有桌面云系统的发展,希望通过多种接入设备随时随地访问业务数据和应用、提高工作效率的需求越来越迫切。文中提出了外部网络访问内网桌面云系统的网络方案,利用 Internet 等外部网络通过移动终端等多种设备访问桌面云系统,满足业务需求。由于外部网络的复杂性,保障安全传输成为该方案的技术关键。文中阐述了 L2TP over IPSec 技术的原理、适用性及其安全策略,并给出了利用 L2TP over IPSec 安全隧道技术实现该网络方案的思路及完整的接入过程、配置方法以及相应的代码,实现了基于此方案的国家气象信息中心私有桌面云系统试点建设的实例,取得了良好的收益,充分表明了 L2TP over IPSec 技术在外网访问私有桌面云的应用中的适用性。

关键词:L2TP over IPSec;SVN;桌面云;隧道;L2TP;IPSec

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2015)10-0160-06

doi:10.3969/j.issn.1673-629X.2015.10.035

Application of L2TP over IPSec Technology in Private Desktop Cloud

YANG Fei-fei,SUN Jing,WANG Bin
(National Meteorological Information Center,Beijing 100081,China)

Abstract:With the development of internal private desktop cloud system in National Meteorological Information Center,more and more urgently,it's necessary to improve work efficiency by accessing data and APPs with multiple access devices anywhere anytime. Propose the network solution for the external network to access the intranet desktop cloud system,utilizing the Internet and other external network through mobile terminals and other devices to access the desktop cloud system,satisfying business demand. Due to the complexity of the external network,to ensure the safe transmission is key technology in this project. Describe the principle,applicability and security strategy of L2TP over IPSec technique,by using the L2TP over IPSec security tunneling technology,also provide the thoughts,whole access procedure,configuration methods and the corresponding code to achieve the program,and implement an experiment construction instance of private desktop cloud system in National Meteorological Information Center accordingly. This project obtains significant benefits,which fully indicates the applicability of the L2TP over IPSec technology to access the private network in the desktop cloud.

Key words:L2TP over IPSec;SVN;desktop cloud;tunnel;L2TP;IPSec

0 引 言

随着云计算的发展,基于云的应用交付逐步成为行业发展的必然趋势^[1]。出于对信息安全的顾虑,很多企业和行业用户摒弃面向公众的云计算中心,建立完全由用户自行掌控的数据中心—私有云,最为常见的是采用桌面云计算架构解决方案^[2]。现有桌面云一般是采用传统 PC 机或者专用的云终端设备作为前端设备,在使用场地和可用设备数量的灵活性上有所限制。但随着平板电脑和智能手机的飞速发展,用户体验了终端设备多元化便利的同时,也希望能够随时随地访问应用和数据,提高工作效率。因此迫切需要建

立用户随时随地可以访问的私有桌面云系统^[3-4]。

1 建设概况

气象系统内部也面临着同样的困境和难题,随着用户信息化建设的不断深入,软硬件的运行情况和用户各部门业务的捆绑越来越紧密,IT 软硬件承担的责任也越来越重,对信息部门的系统安全、运营和维护管理的要求越来越高。国家气象信息中心希望借助于桌面虚拟化技术集中管理,从而实现标准化桌面及安全计算,在支持业务连续性的同时大幅节省桌面管理成本。

收稿日期:2014-12-22

修回日期:2015-03-26

网络出版时间:2015-09-23

基金项目:2014 年国家预警工程建设项目(财预[2014]01 70 号)

作者简介:杨菲菲(1984-),女,硕士,工程师,研究方向为数据存储管理与云计算。

网络出版地址:<http://www.cnki.net/kcms/detail/61.1450.TP.20150923.1509.078.html>

2 外网访问桌面云网络设计方案

出于安全考虑,基于不同的网络情况,桌面云系统采用不同的登录方式。局域网内部终端允许直接通过访问接口登陆到桌面云系统,外部终端需通过安全认证、以加密方式接入后再连接访问接口进行登陆。由于局域网的属性,安全问题相对比较可控,且用户只能在办公区域才能访问此网络,对地域性要求较苛刻,灵活性较弱。利用 Internet 等外部网络通过智能手机、平板电脑等移动终端访问桌面云系统在实际中需求更多,其对地域没有限制,灵活度高,是主流的访问方式。但外部网络情况复杂,安全问题不可预见,故如何安全高效地使用 Internet 等外部网络访问桌面云系统成为试点建设的技术关键^[5-6]。

用户使用移动终端通过 Internet 等外部网络登录桌面云系统最大的问题就是保障传输的安全性,考虑使用一个接入网关来保障传输安全。此次试点建设使用的设备是 SVN5530。

由于中心总体网络结构的复杂性,此次建设的目的是移动终端使用外部网络访问桌面云系统的体验性,故以最小的代价将 SVN 网关接入现有网络,采用旁挂式接入,开放端口 TCP: 80, 8080, 443, 28510, UDP: 500, 4500, 1701。

将 SVN 网关与现有云桌面服务器放到同一个交换机下,划分与内网桌面云用户相同的网段的地址。如:内网桌面云用户地址为 70.0.0.1-70.0.0.20,那么划分给 SVN 的终端内网地址可以是 70.0.0.21-70.0.0.40(或者是后面其他地址),具体的地址数量以具体的 license 数量为准。因外网用户需要通过外部网络拨入 SVN,使用一个外网 IP 地址与 SVN 网关自身接入的内网 IP 地址做 1:1 的静态映射,完成接入,如图 1 所示。

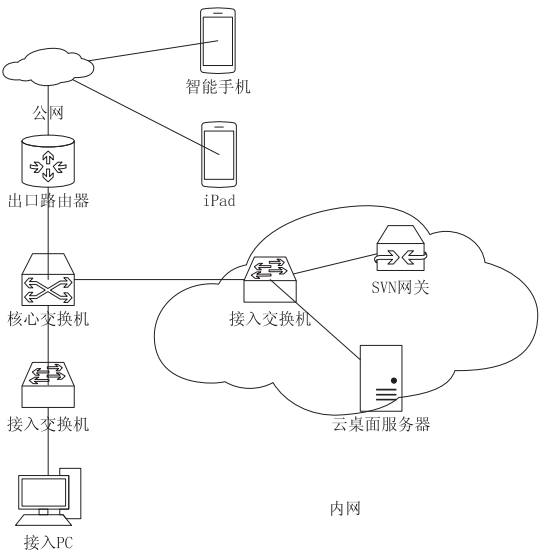


图 1 外部网络访问内网桌面云组网图

2.1 L2TP over IPSec 技术在移动终端接入时的应用

目前,L2TP 和 IPSec 是应用最为广泛的虚拟专用网(VPN)技术。

L2TP 协议是由 IETF 起草,微软、Ascend、Cisco、3COM 等公司参与制定的二层隧道协议,它结合了 PPTP 和 L2F 两种二层隧道协议的优点,已经成为 IETF 有关 2 层通道协议的工业标准,支持多种传输协议和远程访问。由于是基于 UDP 的数据链路层协议,L2TP 不保证数据消息的可靠投递,若数据报文丢失,不予重传,不支持对数据消息的流量控制和拥塞控制,安全性不强^[7-8]。

IPSec 能够提供较强的 IP 层安全机制,通常用于保护经过“不确定安全的网络”的数据流,避免 IP 数据包受到破坏,工作在 OSI 模型的第三层,适于保护基于 TCP 或 UDP 的协议,但是对多协议封装等功能的支持存在不足。

基于两者的特点,使其综合使用成为可能,使用 IPSec 为 L2TP 提供安全性的保护^[9-10]。

用 IPSecAH 或 IPSecESP 来保护 L2TP 分组,就能够对 L2TP 分组提供鉴别、整性、抗重播攻击、数据保密性保护和有效的密钥管理。这样,有利于把 L2TP 低成本、主动权、互通性与 IPSec 的高度安全、可靠的优势发挥出来,取长补短,建立一个既提供对多协议的封装,又提供认证和加密功能的 VPN^[11-13]。

接入时,移动终端向 SVN 发起连接,第一步进行 IPSec 协商建立 IPSec 隧道,然后再进行 L2TP 协商对身份进行认证,建立 L2TP over IPSec 隧道连接,用来传输移动终端与 SVN 之间的通讯数据,这些数据先使用 L2TP 封装第二层数据,再使用 IPSec 对数据进行加密以保证数据的安全性。接入流程如图 2 所示。

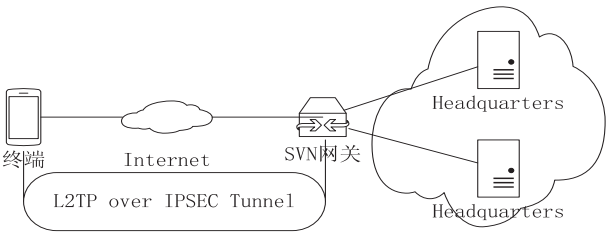


图 2 移动终端接入流程图

2.2 L2TP over IPSec 的配置参数及步骤

由于 L2TP over IPSec 参数很多,而且要求服务器端与客户端的参数保持一致,整理主要的参数与数据,如表 1 所示。

按照表 1 中的参数及数据,L2TP over IPSec 主要的配置思路如下:

首先完成 SVN 网关的接口配置,将 SVN 的接口加入网络区域,并完成 SVN 网关的安全域间包过滤配置和路由配置。

表 1 数据规划

配置项	数据
网关接口配置	接口号:GigabitEthernet 0/0/1 IP 地址:202. 38. 160. 1/24
	接口号:GigabitEthernet 0/0/2 IP 地址:172. 16. 250. 1/24
Virtual-Template 接口	接口号:Virtual-Template 1 IP 地址:222. 222. 222. 222/24
虚拟网关	网关名称:vg1 IP 地址:202. 38. 160. 1/24
	用户接入时的域名:vg1. dom
地址池	地址池名称:IP pool 1 地址 范围: 172. 16. 251. 1/24 ~ 172. 16. 251. 100/24
	认证方式:PAP 隧道验证:关闭
L2TP 配置	L2TP 组:l2tp-group 1 用户认证名称:vpduser 用户认证密码:Admin@123
	IKE 加密算法:AES-CBC IKE DH 组:group2 IKE 协商模式:主模式 IKE 预共享密钥:12345678
IPSec 配置	封装模式:传输模式 安全协议:ESP ESP 协议验证算法:SHA1 ESP 协议加密算法:AES 建立方式:策略模板

注:表中数据均为测试数据,并非实际业务数据情况

配置 SVN 侧的 L2TP 参数,包括创建虚拟接口模板、配置 L2TP 参数等。

配置 SVN 侧的 IPSec 参数,包括定义需要保护的数据流、IKE 安全提议、IKE 对等体、IPSec 安全提议和 IPSec 安全策略等,由于外网设备接入时的 IP 地址不固定,故在 SVN 侧使用安全策略模板方式配置 IPSec 安全策略,并将 IPSec 安全策略应用到接口上。

配置 SVN 侧的 L2TP 网络扩展功能。在 Domain 下创建 IP 地址池,用于分配给接入的外网设备,并配置用户名、密码,用于外网用户接入认证。

最后给外网接入设备配置移动终端参数,使用移动终端系统(Android 和 iOS)自带的拨号软件接入内网网络。

2.3 移动终端通过 SVN 接入内网的代码实现

1)配置接口的 IP 地址。

```
[ SVN ] interface GigabitEthernet 0/0/1
[ SVN - GigabitEthernet 0/0/1 ] ip address 202. 38.
160. 1 24
[ SVN - GigabitEthernet 0/0/1 ] quit
[ SVN ] interface GigabitEthernet 0/0/2
[ SVN - GigabitEthernet 0/0/2 ] ip address 172. 16.
```

250. 1 24

```
[ SVN - GigabitEthernet 0/0/2 ] quit
```

2)将 Virtual-Template 接口加入 LAN/WAN/DMZ 区域中的任意一个网络区域。并开启 SVN 接收和发送 L2TP 隧道报文的实际物理接口所在区域和 Local 区域之间的包过滤。

SVN 缺省开放域间包过滤规则是除 Local 区域外的 LAN/WAN/DMZ 区域可以正常通信。使用时,请先检查 SVN 设备各接口所在网络区域间的包过滤规则,确保基本的网络通信正常。

3)配置 SVN 侧的 L2TP 特性。

(1)创建并配置虚拟接口模板。

当认证方式为 VPND、LDAP 或 AD 时,本端 PPP 协议对远端设备的验证方式必须为“PAP”。

```
[ SVN ] interface virtual-template 1
[ SVN - Virtual - Template1 ] ip address 222. 222.
222. 222 24
[ SVN - Virtual - Template1 ] ppp authentication-mode
pap
```

```
[ SVN - Virtual - Template1 ] ppp timer negotiate 10
[ SVN - Virtual - Template1 ] quit
```

(2)开启 L2TP 服务。

```
[ SVN ] l2tp enable
```

(3)创建 L2TP 组,绑定虚拟接口,并关闭隧道验证功能。

```
[ SVN ] l2tp-group 1
[ SVN - l2tp1 ] tunnel name SVN
[ SVN - l2tp1 ] allow l2tp virtual-template 1
[ SVN - l2tp1 ] undo tunnel authentication
[ SVN - l2tp1 ] quit
```

(4)配置 SVN 侧的 IPSec 特性。

①配置需保护的数据流,使用 L2TP 报文的端口 1701 作为匹配条件。

```
[ SVN ] acl number 3001
[ SVN - acl - adv - 3001 ] rule permit udp source-port
eq 1701
[ SVN - acl - adv - 3001 ] quit
```

②创建 IKE 安全提议,IKE 加密算法 AES-CBC, IKE DH 组为 DH-group2。

```
[ SVN ] ike proposal 4
[ SVN - ike - proposal - 1 ] encryption-algorithm aes -
cbc
[ SVN - ike - proposal - 1 ] dh group2
[ SVN - ike - proposal - 1 ] quit
```

③配置 IKE 对等体,引用 IKE 安全提议 4,设置预共享密钥参数。

```
[ SVN ] ike peer 1
[ SVN-ike-peer-peer1 ] ike-proposal 4
[ SVN-ike-peer-peer1 ] pre-shared-key 12345678
[ SVN-ike-peer-peer1 ] quit
④配置 IPSec 安全提议,设置封装模式为传输模式,ESP 协议验证算法为 SHA1,ESP 协议加密算法为 AES。
[ SVN ] ipsec proposal 1
[ SVN - ipsec - proposal - p1 ] encapsulation - mode transport
[ SVN-ipsec-proposal-p1 ] esp authentication-algorithm sha1
[ SVN-ipsec-proposal-p1 ] esp encryption-algorithm aes
[ SVN-ipsec-proposal-p1 ] quit
⑤配置 IPSec 安全策略,SVN 侧使用模板方式建立 IPSec 安全策略,接收多个设备发起拨号请求。
[ SVN ] ipsec policy-template mobile1 10
[ SVN - ipsec - policy - templet - template1 - mobile1 - 10 ] security acl 3001
[ SVN - ipsec - policy - templet - template1 - mobile1 - 10 ] ike-peer 1
[ SVN - ipsec - policy - templet - template1 - mobile1 - 10 ] proposal 1
[ SVN - ipsec - policy - templet - template1 - mobile1 - 10 ] quit
[ SVN ] ipsec policy mobile 1 isakmp template mobile1
⑥在 SVN 接口上应用安全策略。
[ SVN ] interface GigabitEthernet 0/0/1
[ SVN-GigabitEthernet 0/0/1 ] ipsec policy mobile
[ SVN-GigabitEthernet 0/0/1 ] quit
(5)配置 SVN 侧的网络扩展功能。
①进入虚拟网关“vg1”。
[ SVN ] v-gateway vg1
②外部设备接入时的域名“vg1. dom”,并配置地址池。
[ SVN ] aaa
[ SVN-aaa ] domain vg1. dom
[ SVN-aaa-domain-vg1. dom ] ip pool 1 172. 16. 251. 1 172. 16. 251. 100
[ SVN-aaa-domain-vg1. dom ] quit
[ SVN-aaa ] quit
③在虚拟接口模板中绑定地址池。
[ SVN ] interface Virtual-Template 1
[ SVN-Virtual-Template1 ] remote address pool 1
```

```
[ SVN-Virtual-Template1 ] quit
④创建用户名和密码。
[ SVN ] v-gateway vg1
[ SVN-vg1 ] vpndb
[ SVN-vg1-vpndb ] user vpdnuser password Admin@123Admin@ 123
(6)接入设备为 Android(以 4.0 版本为例)系统的终端主要配置步骤。
①手机选择添加 VPN 网络,并配置如图 3 所示参数,本次测试数据中的 IPSec 预共享密钥为“12345678”。
```



图 3 手机客户端截图(1)

②编辑添加的 SVN,配置用户名、密码。账号 vpdnuser 的密码为 Admin@ 123,并选择“连接”,见图 4。



图 4 手机客户端截图(2)

- ③连接成功即可访问内网资源。
- (7)接入设备为 IOS(以 6.0 版本为例)系统的终端主要配置步骤。
- ①手机选择添加 VPN 配置,并配置如图 5 所示参数。



图 5 手机客户端截图(3)

- ②打开连接开关,连接成功即可访问内网资源。
- 2.4 测试结果的观察和分析

移动终端向 SVN 发起连接,进而会触发 IPSec 协商建立 IPSec 隧道,然后再进行 L2TP 协商对身份进行认证,建立 L2TP over IPSec 隧道连接,完成移动终端与 SVN 间的数据通信。由此可以发现,确实是首先进行 IPSec 协商,之后再进行 L2TP 隧道建立,也就是说 IPSec 实现了对 L2TP 的加密。

- 下面使用一些命令行表示测试的结果。
- (1)在 SVN 上执行 display ikesa 和 display ipseca brief 命令可看到 IKE 和 IPSec 隧道建立成功。

```
<SVN>displayikesa
currentikesa number:2
-----
conn-idpeer  flag  phase  vpn
-----
56 1.1.1.2   RDv1:2  public
55 1.1.1.2   RDv1:1  public

<SVN>displayipseca brief
currentipseca number:2
currentipsec tunnel number:1
-----
SrcAddressDstAddressSPI  Protocol Algorithm
-----
```

```
1.1.1.2202.38.160.1 1069578828 ESP E: AES; A:
HMAC-SHA1-96;
202.38.160.1 1.1.1.2 2759494786 ESP E: AES; A:
HMAC-SHA1-96;
```

- (2)用户连接 VPN 后,在 SVN 上执行 display l2tp tunnel 命令可看到隧道建立成功。

```
<SVN>display l2tp tunnel
Total tunnel = 1
-----
LocalTIDRemoteTIDRemoteAddressPort      Sessions  RemoteName
-----
16 1.1.1.2 1701 1 client1
```

- (3)在 SVN 上执行 display l2tp session 命令可看到会话连接建立成功。

```
<SVN>display l2tp session
Total session = 1
-----
LocalSIDRemoteSIDLocalTID
-----
271 1
```

- (4)执行 display access-user 命令可以查看已上线用户。

```
[SVN2260]display access-user domain vg1.dom
-----User access index:0
State:Used Username:vpdnuser@vg1.dom
User access VLAN/PVC: 0
User MAC:-
User IP address:1.1.1.2
VPN-Instance:Public
User access type:PPP
User authentication type:PPPAuthentication
Current authen method:Invalid
Authen result:Success
Current author method:Invalid
Author result: Success
Action flag:Idle
Authen state: Authed
Author state:Idle
Accounting method:No accounting
Accounting state:Ready ACL-number:- Priority:-
Up CAR enable:NO
Up average rate:0(bps)
Up peak rate:0(bps)
Down CAR enable:NO
Down average rate:0(bps)
Down peak rate:0(bps)
Up packets number( high,low) : (0,42)
Up bytes number( high,low) : (0,5757) Down packets number( high,low) : (0,0)
```


Down bytes number (high, low) : (0, 0)

3 结束语

文中基于本单位的现状,重点介绍了外部网络访问内网云桌面的网络接入方案,并提出了由 L2TP 提供隧道服务,IPSec 提供安全服务的 L2TP over IPSec 技术在网络接入方案中的实现思路、配置方法以及相应的代码实现,并用测试数据充分说明了此方案的可行性。方案满足了试点建设中外网用户通过移动设备灵活高效地接入内网访问桌面云服务器的相关需求,收到了良好的体验效果。

但是由于试用规模的限制,考虑使用开放相关端口的方法实现接入,这样对于现有的网络改动最小。若是大规模的相关建设,应考虑对于网络做进一步的分离,这将是今后的一段时间内需要研究的内容。

参考文献:

[1] 刘 鹏. 云计算[M]. 第 2 版. 北京:电子工业出版社, 2011.

[2] 王 郑,韩 焱,单联春. 通信运营商桌面云运用探讨[J]. 电信科学,2011(S1):16-22.

[3] Celesti A,Tusa F,Villari M. Three-phase cross-cloud federation model;the cloud SSO authentication[C]//Proc of 2010 second international conference on advances in future Internet. Venice;IEEE,2010;94-101.

[4] Rittinghouse J W,Ransome J F. Cloud computing;implemen-

(上接第 159 页)

[9] 王建伟,荣莉莉. 基于袭击的复杂网络上的全局相继故障[J]. 管理科学,2009,22(3):113-120.

[10] 韩传峰,张 超,刘 亮. 关键基础设施网络连锁反应模型[J]. 系统仿真技术,2010,6(2):121-125.

[11] Duenas-Osorio L,Vemuru S M. Cascading failures in complex infrastructure systems[J]. Structural Safety,2009,31(2):157-167.

[12] Murray A T,Matisziw T C,Grubescic T H. Critical network infrastructure analysis;interdiction and system flow[J]. Journal of Geographical Systems,2007,9(2):103-117.

[13] Matisziw T C,Murray A T,Grubescic T H. Exploring the vulnerability of network infrastructure to disruption[J]. The Annals of Regional Science,2009,43(2):307-321.

[14] 周军学,易立新. 网络重要基础设施脆弱性评价模型及其应用[J]. 中国安全科学学报,2010,20(11):72-77.

[15] Agrawal R,Imielinshi T,Swami A. Mining association rules

tation,management and security[M]. Beijing:China Machine Press,2010.

[5] Li Z,Wan Q L,Zhang X P,et al. Study on the SSO caused by HVDC link in hybrid AC-DC power systems[C]//Proc of 9th IET international conference on AC and DC power transmission. London;IEEE,2010;1-5.

[6] Orawiwattanakul T,Yamaji K,Nakamura M,et al. User-controlled privacy protection with attribute-filter mechanism for a federated SSO environment using shibboleth[C]//Proc of 2010 international conference on P2P,parallel,grid,cloud and Internet computing. [s. l.]:[s. n.],2010.

[7] 贾湘兴. 虚拟专用网络承载协议—L2TP 的实现[D]. 成都:电子科技大学,2003.

[8] Townsley W,Valencia A. Layer two tunneling protocol (L2-TP)[S]. RFC 2661,1999.

[9] Li H,Dai Y S,Tian L,et al. Identity-based authentication for cloud computing[C]//Proc of international conf on cloud computing. Beijing:[s. n.],2009;157-166.

[10] Aymerich F M,Fenu G,Surcis S. An approach to a cloud computing network[C]//Proc of ICADIWT. Ostrava;IEEE,2008;113-118.

[11] 季 超,楚艳萍. 基于 L2TP/IPSec 的安全隧道技术方案[J]. 河南大学学报:自然科学版,2004,34(1):94-96.

[12] Patel B,Aboda B. Securing L2TP using IPsec[S]. RFC 3193, 2001.

[13] 朱昌盛,余冬梅,王庆荣,等. IPSec 与 L2TP 结合构筑的虚拟专用网络[J]. 计算机工程,2002,28(11):105-107.

between sets of items in large database[C]//Proceedings of ACM SIGMOD conference on management of data. Washtoning,DC:ACM,1993;207-216.

[16] Park J S,Chen M S,Yu P S. An effective hash based algorithm for mining association rules[C]//Proc of 1995 ACM-SIGMOD international conference on management of data. San Jose,CA:ACM,1995;175-186.

[17] Savasers A,Omiecmsn E,Navathe S. An efficient algorithm for mining association rules in large databases[C]//Proc of 1995 international conference on very large databases. Zurich,Switzerland:[s. n.],1995;432-443.

[18] Toivonen H. Sampling large databases for association rules[C]//Proceedings of the 22nd international conference on very large databases. Bombay,India:[s. n.],1996;134-145.

[19] Han J,Pei J,Yin Y,et al. Mining frequent patterns without candidate generation;a frequent-pattern tree approach[J]. Data Mining and Knowledge Discovery,2004,8(1):53-87.

L2TPoverIPSec技术在私有桌面云中的应用



作者：[杨菲菲](#)，[孙婧](#)，[王彬](#)，[YANG Fei-fei](#)，[SUN Jing](#)，[WANG Bin](#)
作者单位：[国家气象信息中心, 北京, 100081](#)
刊名：[计算机技术与发展](#)[ISTIC](#)
英文刊名：[Computer Technology and Development](#)
年，卷(期)：2015(10)

引用本文格式：[杨菲菲](#).[孙婧](#).[王彬](#).[YANG Fei-fei](#).[SUN Jing](#).[WANG Bin](#) [L2TPoverIPSec技术在私有桌面云中的应用](#)

[期刊论文]-[计算机技术与发展](#) 2015(10)