VPN 服务器安全性控制的实现策略

Realization Tactics for VPN Server Security Control

邓 昶　刘小晶　(嘉兴学院信息工程学院　314001)

摘要:VPN(Virtual Private Network,虚拟专用网络)技术的基本点是化公为私,每个企业可以临时从公用网中挖走一部分地盘供自己使用,于是,企业网络想连接到哪里都可以,保密性、安全性、可管理性的问题也容易解决。本文就 VPN 服务器安全性控制的实现策略进行阐述。

关键词:VPN　隧道(Tunneling)　LAC(接入服务器)　LNS(网关)　L2TP(隧道协议)　ssh

1　对 VPDN(即拨号 VPN,也称远程访问虚拟网,即 AccessVPN)认证服务器安全性控制

VPN 网络中通常有一个或多个安全服务器,安全服务器除了提供防火墙和地址转换功能外,还通过与隧道设备的通信提供加密、身份查验和授权功能,它们也提供各种信息,如带宽、隧道端点、网络策略和服务等级等,而拨号用户使用 VPDN 业务时具体的认证过程存在一次认证和二次认证两种情况,一次认证是指 VPDN 用户接入企业内部网只需要内部网作认证,即 LAC(接入服务器)端对于 VPDN 用户进行身份验证;二次认证是指 VPDN 用户接入企业内部网除需要企业内部作认证外,还要求各级 VPDN 业务管理中心对于用户与 LAC 间建立 PPP 连接作一次认证,即在 VPDN 用户拨入 LAC 时,即使被发现是 VPN 用户(比如通过用户名中的域名),仍需要与接入服务器端的 Radius 认证系统服务器进行用户身份验证。如果验证不通过,则用户不能使用 VPN 业务。在 VPN 用户通过接入服务器端的身份验证时,将和普通用户类似受权限限制,不能任意访问网内资源,在建立 L2TP 隧道时,通道两端需要相互验证。最终接入内部网认证由用户实现,在这种情况下,用户需要有自己认证服务器。

假如 VPN 网络布署如图 1 所示(已安装上设计好的企业 VPN 认证管理系统和 VPN 计费管理系统),每个拨号网关(硬/软件)在接入 internet 时,首先在策略服务器相应的目录下注册自己当前的 IP,并取得同组的各上线网关/客户端的此时 IP 地址。接下来发起通讯的这一方,就可以根据获得的对端网关的 IP 地址,建立相应的 VPN 连接并进行通讯了。

而拨号用户使用 VPDN 业务时具体的认证过程实现步骤如下:

1.1　一次认证方式

① VPN 用户拨 XX,用户与 LAC 间建立 PPP 连接,然后将用户完整域名和口令送至 LAC 的认证服务器,根据域名判断是总部业务还是分公司业务。

② LAC 将域名信息送至分公司 VPDN 业务管理中心的认证服务器。分公司 VPDN 业务管理中心的认证服务器根据域名判断是总部业务还是分公司业务。

②' 如果是总部业务,则分公司 VPDN 业务管理中心的认证服务器将域名信息转发至总部业 VPDN 务管理中心的认证服务器。

③ 如果是分公司业务,则认证服务器根据用户注册的信息向 LAC 发送建立 L2TP 隧道的对应参数。

③' 如果总部业务,总部认证服务器根据用户注册的信息经过分公司认证服务器转接向 LAC 发送建立 L2PT 隧道的对应参数。

④ LAC 根据接收到的参数与 LNS(网关)之间首先建立 L2TP 隧道(首先建立控制连接,再建立数据连接),然后建立 Session 连接,在 Session 成功建立后,LAC 通知对应的认证服务器开始计费。VPDN 用户与 LNS 之间进行 PPP 握手,LAC 向 LNS 发送用户的完整域名和口令。

⑤ 企业内部网管理系统认证服务器对用户进行

认证。

⑥ 如果认证成功则向远端分配内部网地址。

⑦ VPDN 用户与 LNS 成功建立 PPP 连接，开始进行通信。

一次认证处理流程（如图 2）：

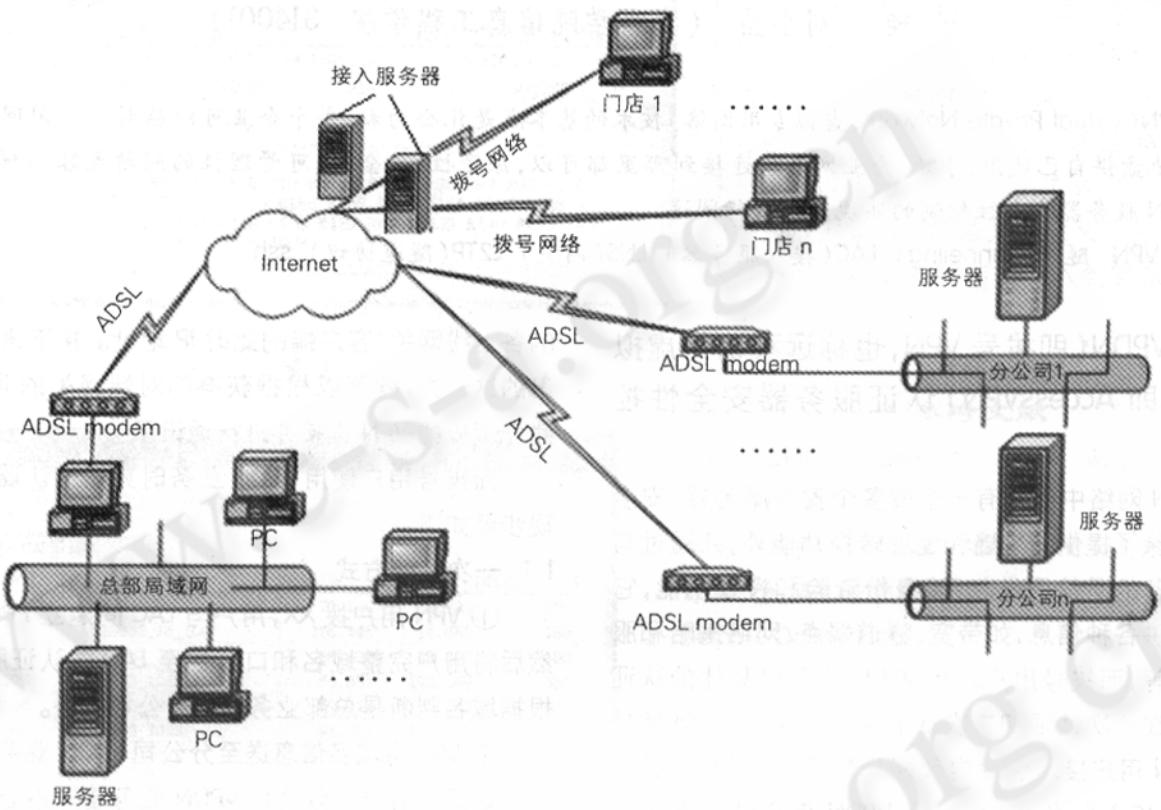

图 1

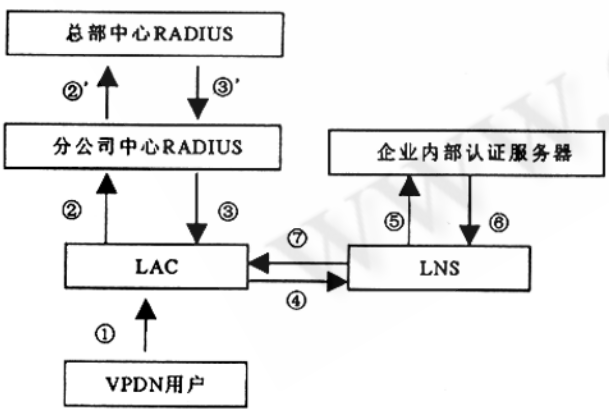

图 2

1.2 二次认证处理流程

二次认证处理流程图如图 3：

① VPDN 用户拨 XX，用户与 LAC 间建立 PPP，然后将用户完整域名和口令送至 LAC 的认证服务器，且根据域名判断是总部业务还是分公司业务。

② LAC 将域名信息送至分公司 VPDN 业务管理中心的认证服务器，分公司 VPDN 业务管理中心的认证服务器根据域名判断是总部业务还是分公司业务。

②' 如果是总部业务，则分公司 VPDN 业务管理中心的认证服务器将域名信息转发至总部 VPDN 业务管理中心的认证服务器。

③、③' RADIUS 根据用户域名，到用户数据库中查询用户信息。

④、④' 用户数据库核实用户密码，返回用户信息（含权限）。

⑤ 如果是分公司业务，RADIUS 根据权限信息为客户授权，并根据授权信息限制客户访问，同认证务器根据用户注册的信息经向 LAC 发关建立 L2TP 隧道的对应参数。

⑤' 如果总部业务，RADIUS 根据权限信息为客户授权，并根据授权信息限制客户访问，同时总部认证服

务器根据用户注册的信息经过分公司认证服务器转接向 LAC 发送建立 L2TP 隧道的对应参数。

⑥ LAC 为客户建立 PPP 连接。

⑦ 在一次认证成功后，用户启动 WINDOWS 拨号网络。

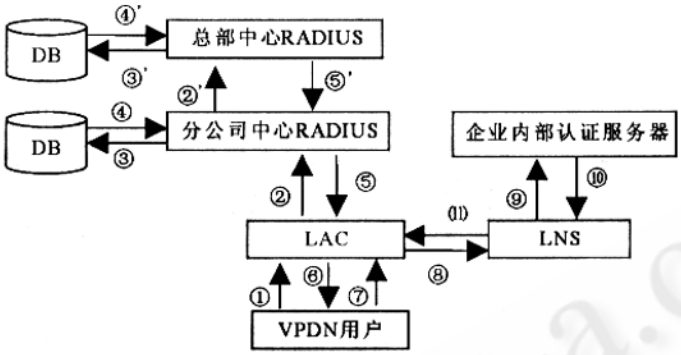

图 3

⑧ LAC 在确认一次认证成功后，根据接收到的参数与 LNS 之间首先建立 L2TP 隧道（首先建立控制连接，再建立数据连接），然后建立 Session 连接，在 Session 成功建立后，LAC 通知对应的认证服务器开始计费。VPDN 与 LNS 之间进行 PPP 握手，LAC 向 LNS 发送用户的完整域名和口令。

⑨ 企业内部网管系统认证服务器对用户进行认证。

⑩ 如果认证成功则向远端分配内部网地址。

⑪ VPDN 用户与 LNS 成功建立 PPP 连接，开始进行通信。

2　网服络务器安全性设置

为了保障主机、免受黑客攻击，提高网络安全意识，我们可进行如下几个方面的改进工作：

（1）关掉不必要的服务

#vi /etc/inetd. conf（通常情况下只保留 telnet 和 ftp 服务，其它服务全部关掉，出于安全考虑，建议关掉 ftp 服务，需要使用时再放开）

（2）去掉不必要启动脚本

例如：#mv S88sendmail. S88sendmail

通常不用的脚本包括：

/etc/rc2. d/

S888sendmail、S76nscd、S73nfs、client、S74autofs、S801p、S72autoinstall、S70uucp、S74xntpd、S30sysid. net、S71sysid. sys、S93cacheos. finish、S73cachefs. daemon、S80PRESERVE、S89bdconfig、S47asppp、S80spc

S71rpc（如果系统装有 DiskSuite 软件，则不能移去此服务）。

（3）系统文件权限控制

创建/. rhsts 文件，内容为空，权限为 0400

#touch /. rhosts

#chmod 0400 /. rhosts

创建/etc/hosts. equiv，内容为空，权限为 0400

#touch /etc/hosts. equiv

#chmod 0400 /ect/hosts. equiv

改名/usr/sbin/snoop 为/usr/sbin/poons，权限为 0000

#mv /usr/sbin/snoop /usr/sbin/poons

#chmod 0000 /usr/sbin/poons

去掉/var/adm/vold. log 的组和其它的访问权限

#chmod og－rwx /var/adm/vold. log

记录连续 5 次错误登陆的信息

#touch /var/adm/loginlog

#chgrp sys /var/adm/logiinlog

#chmod 600 /var/adm/loginlog

记录 INETD 连接的所有信息，在 inetd 低端的启动行中增加"－t"参数

#vi /ect/init. d/inetsvc

在最后行的/usr/sbin/inetd － s 后加"－t"参数，为防止某些缓冲溢出，在/etc/system 中增加如下设置（只在 sun4u/sun4d/sun4m 系统中有效）：

Set noexec_user_stack＝1

Set noexec_user_stack_log＝1

3　网络系统安全防护

在数据服务器与外网通过硬件和软件防火墙隔离。硬件防火墙由路由器担任，负责对有恶意 IP 地址来的 IP 包过滤。对主机安装 TcpWrapper 安全软件，对于能访问该主机的 IP 进行严格限制，访问控制是基于 IP 地址和域名。TcpWrapper 它能以统一的方式保护各种不同服务器，配置了 tcp_wrapper 后，再连接到具体的服务进程上，这样 tcpd 就有机会查看远程系统是否

被允许访问，并能将连接的情况通过 syslog 记录下来，包括请求的种类，时间和连接的来源地址。

由于网络上的数据传输是不安全，因此出现了 key 等方式来保护口令的安全。然而这些认证系统只是保证了口令等特别敏感信息的安全，而不能保证连接之后的传输数据的安全性，从而为了保证数据传输的安全，就必须先对数据加密后再进行传输。但传统的 unix 所提供的 telnet，ftp，rlogin 等标准服务有着诸多的安全隐患：没有有效的认证机制、网络连接中所有的传输数据（包括账号口令！）均为明文、容易导致各种形式 spoof 数据等。以往发现各种版本的 unix 系统的 telnet，ftp 都存在溢出问题，使攻击者通过这些服务得到超级用户的权限。一个好的替代方式就是使用 ssh，它是从网络应用程序入手，使用成熟的 public/private key 机制对网络中数据包进行加密，使处于两端的数据通信能够在一个加密通道中进行，从而从根本上解决了网络明文数据传输的问题，除了加密道中的数据。使用 ssh 还可以得到一些额外的好处，比如：端口转发、数据压缩、源代码开放等。Ssh 认证方式按在实现时的认证顺序有：

第一种认证方式：如果系统提供了基于 r 的认证方式，同时在 openssh 中许可了这种认证方式，则用户允许登录认证。需要注意的是这种认证方式在 openssh 中出于安全考虑默认是不允许的。

第二种认证方式：如果系统提供了基于 r 的认证方式，同时客户端主机的 host key 在服务器端的/etc/ssh_known_hosts 中或是在对应用户家目录下 $HOME/.ssh/known_hosts 文件内，则用户允许继续认证过程。

第三种方式：是基于 rsa 的认证，我们知道 rsa 是基于公钥的加密方式的，这种方式加密和解密是依靠独立的密钥的，每个用户都产生自己唯一的钥匙对，公钥分发出去，私钥自己保存，对欲加密的数据使用公钥加密，则先要使用对应的私钥对已加密数据进行解密。这种算法实现安全保障的最重要一点就是公钥与私钥之间没有关联，公钥不可能推导出私钥。为了使用 rsa 认证，用户需要将自己的公钥放在服务器端自己家目录下，保存为 $HOME/.ssh/authorized_keys，同时只有服务器中 authorized_keys 中列出的用户才能进行认证。

采用这种认证方式时，当用户发出登录请求，客户端的 ssh 程序会告诉服务器端自己打算使用哪个钥匙对，然后服务器端在自己的 authorized_keys 中检查是否存在该用户的公钥，不存在，则拒绝用户，存在，则发给该用户公钥加密过的随机数字，上面提到，只有使用对应的私钥才能对公钥加密数据进行解密。只有该用户正确解密，认证过程才能继续进行。系统中的每个用户都可以利用 ssh－keygen 生成自己的钥匙对，并保存在自己家目录下的.ssh 下，公钥保存为 identity.pub，私钥保存为 identity。上面讲到，为了实现 rsa 认证，用户需要把自己的公钥（identity.pub）拷贝到服务器端家目录下。并改名为 authorized_keys。这样的话用户登录服务器时，不需要输入口令即可以成功登录。最后：如果上述条件均不满足，则 openssh 进入基于普通的 passwd 认证方式，此时网络上传输所有数据都是加密的。

每一台想要通过 ssh 访问的服务器都需要运行 sshd 进程，首先需要执行以下三行命令来创建服务器的密钥信息，如果你运行过 sshd 进程而且在/usr/local/etc/目录下有密钥的话，那么执行以下命令后，密钥会被覆盖。

```
#ssh－keygen －t rsa1 －f /usr/local/etc/ssh_host_key －N ""
#ssh－keygen －t dsa －f /usr/local/ect/ssh_host_dsa_key －N ""
#ssh－keygen －t rsa －f /usr/local/ect/ssh_host_rsa_key －N ""
```

参考文献

1 Greating and Implementing Virtual private Networks，钟鸣、魏允韬（译），机械出版社。

2 信息安全（检测鉴别监控技术与系统安全性能评估分析），陈远春，人民出版社。

3 MPLS 和 VPN 体系结构 CCIP 版（英文版），［美］Lvan Pepelnjak 人民邮电出版社。