

Hillstone[®]
SSL VPN
解决方案

山石网科通信技术(北京)有限公司
www.hillstonenet.com

Hillstone SSL VPN解决方案

1. 背景介绍

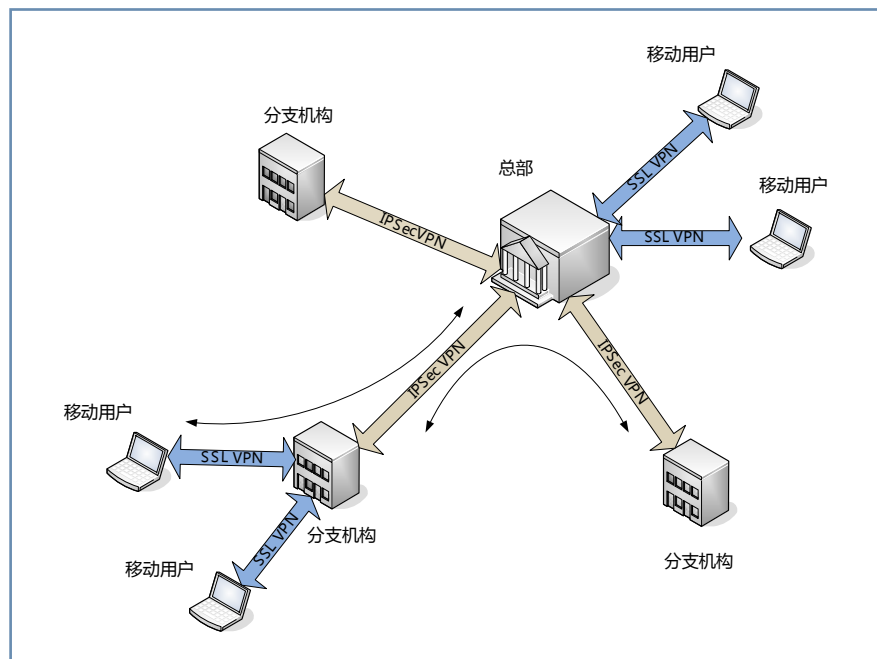
Internet的发展改变了许多公司的内部网络结构。传统上租用专线来建立分支机构互联的企业开始需要访问互联网，另一方面，使用互联网进行互联也可以节省许多费用。VPN技术的出现可以让许多远程办公室和移动用户安全地接入企业的内部网络。

基于IPSec的VPN技术一度是唯一的选择。IPSec建立在国际标准之上，可以保证不同厂商之间的产品互联互通。但是IPSec也有它的弱项，就是远程客户需要预先安装客户端软件，且客户端的配置、使用和维护极为复杂。

随着互联网的发展和网页浏览器(例如微软的Internet Explorer)的大量预装使用，一个新型的基于SSL的VPN技术出现了，为远程安全访问提供了另一种选择。

Hillstone的VPN解决方案可以支持IPSec和SSL两种方式。Hillstone的VPN技术结合了两者的优点，在通过IP层面的连接充分保障应用兼容的同时，也提供了细粒度的访问控制。

图 1: Hillstone IPSec/SSL VPN整体解决方案 ▶



Hillstone的IPSec VPN支持点对点 and 星型连接拓扑，可以使用基于策略或者路由的方式来实现远程办公室之间的互联。移动用户可以通过Hillstone的SSL VPN接入分支机构或者总部的内网。

Hillstone的SSL VPN无需预先安装和配置客户端，所有的安装和升级都可以在远程接入时自动完成，把IT部门的负担减少到最低，同时集成了基于SSL的用户认证机制。Hillstone的SSL VPN和IPSec VPN都可以是基于路由的，这样可以保证用户的全网访问；同时，通过配置Hillstone的VPN接入网关，可以对用户接入和内网访问实现细粒度的访问控制，保障某些特定的网络资源只能被授权的用户访问。

Hillstone SSL VPN 支持

- 基于IP层面的接入，兼容所有基于IP的应用
- 私有IP地址分配
- 内网的DNS和WINS服务器，提供内部域名解析
- 多种加密算法
- 自动配置路由
- 多个用户域，每个域可以使用自己的认证服务器
- 通过本地用户数据库、微软的Active Directory、LDAP、RADIUS，或通过USB证书，或两者的组合实现身份认证
- 对接入用户和PC的硬件绑定。支持用户和PC的一对一，多对一，一对多和多对多的绑定
- 对接入用户的实时监控
- 基于用户身份的访问控制可以提供细粒度的访问控制。这种用户身份可以是用户名、部门的组合
- 多SSL VPN接入通道提供更高的安全性
- 在客户端和接入网关处的多重访问记录
- 用户管理

2. IPSec VPN vs. SSL VPN

IETF为IPSec VPN及其相应的密钥交换协议制定了一系列标准。这种基于标准的技术保障了来自不同厂家的产品的互联互通。通过标准制定的加密算法和通讯协议，都经过了严密的审查，其安全性也得到了保证。

IPSec VPN是一项成熟的技术，目前有许多基于硬件的解决方案来保障它的高性能，是远程办公室点对点互联的优选方案。

但是，IPSec VPN存在先天的易用性问题。实施IPSec方案不仅需要人工发放认证的材料，如用户名和密码等；用户还需要知道所使用的加密和认证算法，内网路由配置等诸多繁琐事宜，当然还需要预装客户端软件等。这些不便在移动用户远程访问尤其是个问题，在大规模实施过程中给用户带来了难以负担的工作量和费用。

进一步分析移动用户远程访问的情况，IPSec VPN缺乏自然的用户认证方式。除了使用证书来认证用户以外，许多厂商还使用XAUTH或L2TP-over-IPSec等复杂的接入方式来认证用户身份。这为VPN的配置增加了许多复杂度降低效

率，而且非常不易于用户理解。

第一代的SSL VPN技术在2000年发展出来之后被立即应用于移动远程接入，其基于浏览器的接入方式使远程访问更易于实施。同时通过使用HTTPS协议，可以轻易地实施双向认证：客户端可以通过验证HTTPS服务器证书的方式确认服务器的身份；然后服务器可以通过验证客户端的用户名和密码，或者进一步加入硬件证书、密钥等多种方式确认客户身份。

但是SSL VPN并不适用于点对点的远程连接，因为接入时它需要用户认证，而且只能从客户端到服务器单向启动连接。而IPSec VPN可以从任何一方启动连接，并且借助IPSec非常成熟的硬件加速技术，其连接性能远高于SSL VPN。

同时，由于SSL VPN没有标准化，所以不同厂家的产品无法实现互联。

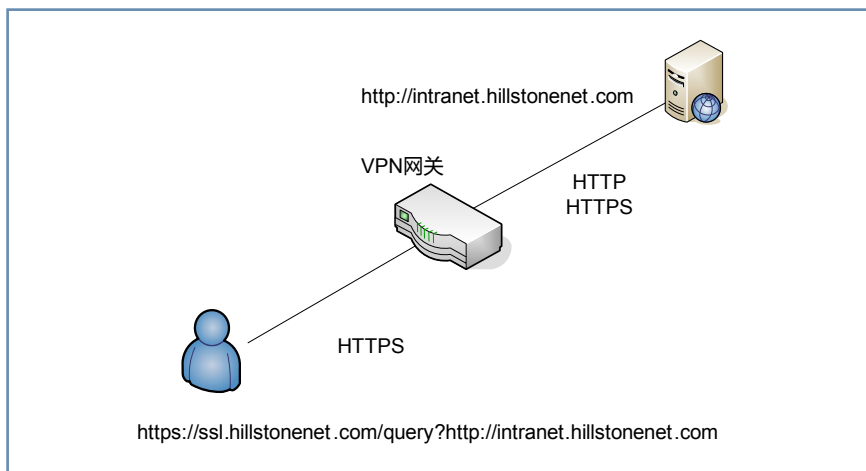
从以上的分析来看，SSL VPN和基于IPSec的VPN技术是非常互补的。SSL VPN非常适用于移动用户远程接入的情形，而IPSec VPN在端对端的互联时更为适合。Hillstone的产品已经集成了这两种VPN方式，为用户提供了更完善的VPN解决方案。

3. SSL VPN的发展

HTTP和应用的匿名代理

第一代的SSL VPN只是一个HTTPS的匿名代理服务器。其核心技术就是改写URL链接。除了匿名代理最初的HTTPS请求，SSL VPN网关会把内网的相应HTTP URL的内容从HTTPS的URL中提炼出来。然而，URL改写技术很难完善。这是由于不断有新的网页描述语言，如 Javascript、Java Applet、Flash等，都有内嵌的URL或可以产生其他URL的描述语言脚本。同时各个厂商对这些语言脚本的翻译支持程度也不尽相同。

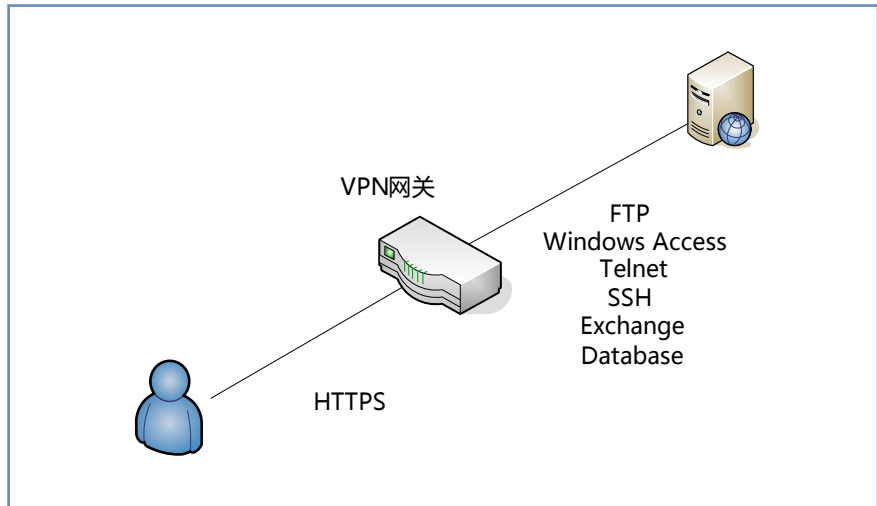
图 2: HTTP到HTTPS代理



SSL VPN厂商也在逐步加入对各种应用的支持。应用匿名代理是把不同的应用转为HTTPS访问的技术。不同的厂家可能会支持不同的应用。最常见的应用

包括FTP，微软邮件系统 Exchange，Windows文件访问。有些厂家则会支持数据库应用。大多数情况下，用户需下载ActiveX或Java Applets所组成的脚本程序。

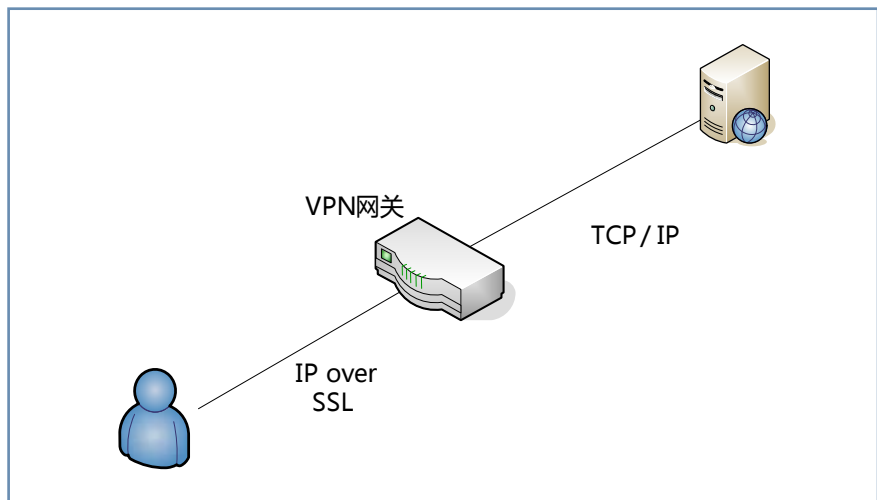
图 3: 应用代理 ▶



IP 隧道

很快SSL VPN厂家就发现通过增加代理来支持各种类型的应用不具备可持续发展性。第二代的SSL VPN增加了对IP协议的支持。这个技术就叫做IP隧道。IP隧道对各种IP应用提供了良好的支持，而不需要为各种新应用去开发新的代理软件。

图 4: IP隧道 ▶



但是这种方式有一个大问题。把TCP应用包在SSL隧道里传输会带来一系列严重的TCP over TCP的问题。在广域网的连接上，如果有数据包丢失（这在广域网很常见），即使很少，那么SSL隧道的TCP和应用的TCP协议栈都会通过重发去恢复那个丢失的数据包，这样会带来严重的性能下降。即使没有这个问题，SSL 的加密性能也会大大低于IPSec在类似硬件平台上的性能。

4. Hillstone SecureConnect VPN

SSL实施

Hillstone SecureConnect VPN 是Hillstone结合传统SSL VPN和IPSec VPN的优越性，而开发的新一代 SSL VPN解决方案。

和传统SSL VPN一样，客户在第一次通过浏览器登录系统时，VPN服务器会通过脚本来自动下载并安装ActiveX客户端。这个客户端无需配置，而且可以自动升级。

其次，用户第二次登录时除了可以通过网页登录以外，也可以通过VPN客户端直接登录。VPN客户端会自动保存上次登录的服务器信息，包括域名（或IP地址），端口及用户名。

客户端的设置是在SecureConnect服务器中心配置的。每个用户在登录后都会被分配一个私网IP地址，同时，内部的DNS和WINS设定也会下发到客户端，这样用户访问的内部域名也可以被正确解析。

同样，路由设置也是在SecureConnect服务器中心配置并自动下发的。这样客户可以选择只有某些流量通过VPN隧道传送。该路由配置可以十分灵活，例如只有去内网服务器的流量才上VPN隧道，而普通的公网网页浏览仍然走正常路上网。

加密和认证算法也是在SecureConnect服务器中心配置并自动下发到客户端的。加密的密钥等信息是在SSL认证登录的阶段自动协商完成。

IPSec数据通道

Hillstone SecureConnect VPN利用IPSec的数据通道来传输用户数据。IPSec无TCP连接的特性避免了传统在SSL上建立IP隧道而引发的TCP-over-TCP的问题，在高延迟，易丢失的广域网应用时对性能提升大有助益。

IPSec是建立在IP隧道的基础上，所以自身对所有IP应用的兼容性非常好。Hillstone 的所有产品都内建IPSec硬件加速，相较其他厂家基于软件的SSL加密方式性能提高1到2个数量级。Hillstone的硬件加密加速支持所有国际通用的加密认证算法，包括DES、3DES、AES 128/192/256位、MD-5、SHA-1等，以及中国国密算法SCB-2。

基于身份的访问控制

Hillstone率先引入基于身份的访问控制，可以为用户提供细粒度的访问控制。用户登录后，用户的身份由用户名或其所属的用户组决定。一个用户在不同的情形下可以有不同的用户身份。

根据用户身份，管理员可以通过配置访问策略的方式实现用户对资源的访问控制。访问策略可以是基于用户或用户组的，甚至是基于用户在特定情况下的特定身份，例如同一用户从公网登录访问时的访问权限会比从内部登录时的权限有较大的限制。

Hillstone基于身份的访问策略可以支持一系列应用控制

- QoS: QoS 配置可以支持如下特性
 - ◆ 针对IP 的QoS
 - ◆ 针对服务的QoS
 - ◆ 流量整形及流量控制
 - ◆ 保证最小带宽
 - ◆ 优先级
 - ◆ 标记（与Cisco兼容）
 - ◆ 低延迟
- P2P/IM控制
- 内容过滤
- 时间表：允许根据时间表打开或关闭策略
- 应用安全

用户和PC的硬件绑定

Hillstone SecureConnect VPN支持用户和PC的硬件绑定，满足一些客户对安全性的更高的要求。客户端针对每一台PC生成一个PCID，可以要求用户和PC具备一定的绑定关系才允许用户登录。支持的绑定有一个用户对一台PC，一个用户对多台PC，多个用户对一台PC等灵活的部署。

PC和用户的绑定可以手工绑定，也可以自动学习。针对一些超级用户，管理员可以有选择的对其放开绑定的检查。管理园还可以定义一些PC开放给所有的用户使用。

SecureConnect VPN 功能

Hillstone SecureConnect VPN支持多个用户域。每个用户域可以有自己的认证服务器组。这样不同的用户组可以通过同一个VPN域服务器登录，给VPN接入管理带来了极大的方便。然后服务器根据用户的身份来分配访问权限。

SecureConnect VPN可以通过微软的Active Directory、LDAP、Radius、本地用户数据库，或通过USB证书，或二者的组合来认证客户。

通过Web界面，管理员可以实时监控登录的用户，包括其登录时间，上下行流量和连接数等。

Hillstone的VPN网关同时支持多个SSL VPN接入，可以为用户提供最大的安全性和通用性。例如，使用同一个VPN网关可以配置一个外部SSL VPN接入主页

来提供远程接入，同时也可以再配置一个内部的接入主页让访客或无线局域网用户接入。

常见的应用之一: 远程接入

图 5: 远程访问解决方案 ▶

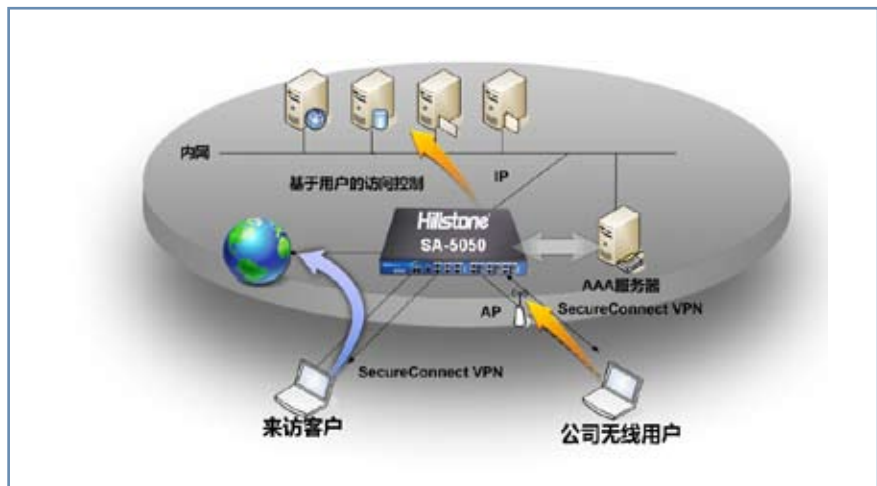


Hillstone SecureConnect 是第三代的SSL VPN解决方案，最适宜远程接入。这个应用案例适用于出差员工接入内网工作。SecureConnect可以让出差员工接入内网，而且在管理员允许的情况下，访问内网的资源，如同员工在办公室工作一样。企业可以使用已有的Active Directory 或Radius 服务器。

进一步，这种连接可以是双向的，在配置允许的情况下，出差员工的资源（如电脑上的文件等）也可以被内网访问。

常见的应用之二:内网控制

图 6: 内网间控制 ▶



有些公司会为访客提供上网接入，但是又不希望开放内网给访客。同时在某些情况下员工又需要通过同一网络接入内网。典型的例子是在会议室内，在Hillstone VPN网关控制下，客人可以连到Internet，同时内部员工可以通过SecureConnect接入内网。这种方式也可以应用于无线局域网的例子，为无线网络的应用提供最大的安全性和便利性。

5. 结论

Hillstone SecureConnect 是新一代的SSL VPN解决方案。它使用SSL启动VPN连接，同时利用IPSec做数据隧道从而避免了SSL VPN的性能和兼容性的瓶颈。通过Hillstone专有的基于身份的访问控制可以实现细粒度的内网访问控制。

Hillstone的VPN网关结合最新的多核处理器技术，VPN硬件加速，高性能的交换芯片，可以为客户提供高性能，并极具可扩展性的SSL VPN解决方案。



山石网科通信技术(北京)有限公司

www.hillstonenet.com

北京总部

地址: 北京市海淀区上地七街1号
汇众大厦3层
邮编: 100085
电话: +86(10)8289 7229
传真: +86(10)8289 9814

上海办事处

地址: 上海市陕西北路1388号
银座企业中心1721室
邮编: 200060
电话: +86(21)6149 8205
传真: +86(21)6149 8001

成都办事处

地址: 成都市总府路2号
时代广场A座26层2625
邮编: 610016
电话: +86(28)6606 7115
传真: +86(28)6606 7199

广州办事处

地址: 广州市天河区天河路208号
粤海天河城大厦13层1363室
邮编: 510620
电话: +86(20)2826 1950
传真: +86(20)2826 1999

服务热线: 400-650-0259

Copyright © 2008, Hillstone Networks, Inc. 版权所有，保留所有权利。

Hillstone Networks, Hillstone Networks标识, Hillstone, Hillstone标识, StoneOS, StoneManager, Hillstone SA-2003, Hillstone SA-2005, Hillstone SA-2010, Hillstone SA-5020, Hillstone SA-5040, Hillstone SA-5050, Hillstone SR-330, Hillstone SR-530和Hillstone SR-550为Hillstone公司的商标。所有其他商标和注册商标均为本公司的财产。

本文所包含信息可能会有所修改，恕不另行通知。