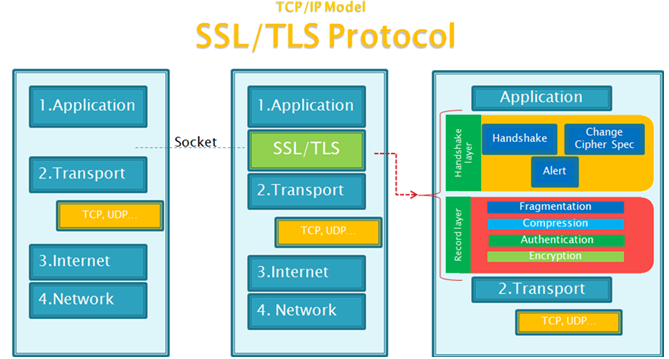
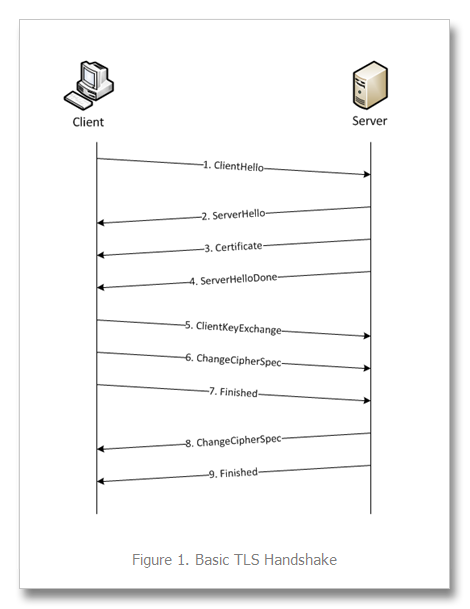
**[SSL与TLS的区别](http://kb.cnblogs.com/page/197396/)**

作者: [hengstart](http://hengstart.iteye.com/" \t "_blank)  发布时间: 2014-01-05 13:09  阅读: 91453 次  推荐: 18   [原文链接](http://hengstart.iteye.com/blog/840561" \t "_blank)   [[收藏]](javascript:add_to_wz())

[](http://www.vircom.com/security/how-to-use-ssltls-to-secure-your-communications-the-basics/)

[](https://devcentral.f5.com/articles/ssl-profiles-part-1#.Usjke2QW3Qw)

SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为[网络通信](http://www.baike.com/wiki/%E7%BD%91%E7%BB%9C%E9%80%9A%E4%BF%A1" \t "_blank)提供安全及数据完整性的一种[安全协议](http://www.baike.com/wiki/%E5%AE%89%E5%85%A8%E5%8D%8F%E8%AE%AE" \t "_blank)。TLS与SSL在传输层对网络连接进行加密。SSL为Netscape所研发，用以保障在Internet上数据传输的安全，利用[数据加密](http://www.baike.com/wiki/%E6%95%B0%E6%8D%AE%E5%8A%A0%E5%AF%86" \t "_blank)(Encryption)的技术，可确保数据在网络上的传输过程中不会被截取及[窃听](http://www.baike.com/wiki/%E7%AA%83%E5%90%AC" \t "_blank)。SSL协议位于TCP/IP协议与各种应用层协议之间，为[数据通讯](http://www.baike.com/wiki/%E6%95%B0%E6%8D%AE%E9%80%9A%E8%AE%AF" \t "_blank)提供安全支持。

SSL：（Secure Socket Layer，安全套接字层），位于可靠的面向连接的网络层协议和应用层协议之间的一种协议层。SSL通过互相认证、使用数字签名确保完整性、使用加密确保私密性，以实现客户端和服务器之间的安全通讯。该协议由两层组成：SSL记录协议和SSL握手协议。

　　TLS：(Transport Layer Security，传输层安全协议)，用于两个应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS记录协议和TLS握手协议。

　　SSL是Netscape开发的专门用户保护Web通讯的，目前版本为3.0。最新版本的TLS 1.0是IETF(工程任务组)制定的一种新的协议，它建立在SSL 3.0协议规范之上，是SSL 3.0的后续版本。两者差别极小，可以理解为SSL 3.1，它是写入了RFC的。

**SSL (Secure Socket Layer)**

　　为Netscape所研发，用以保障在Internet上数据传输之安全，利用数据加密(Encryption)技术，可确保数据在网络上之传输过程中不会被截取。目前一般通用之规格为40 bit之安全标准，美国则已推出128 bit之更高安全标准，但限制出境。只要3.0版本以上之I.E.或Netscape浏览器即可支持SSL。

　　当前版本为3.0。它已被广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输。

　　SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。SSL协议可分为两层： SSL记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。 SSL握手协议（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

**SSL协议提供的服务主要有：**

　　1）认证用户和服务器，确保数据发送到正确的客户机和服务器；

　　2）加密数据以防止数据中途被窃取；

　　3）维护数据的完整性，确保数据在传输过程中不被改变。

**SSL协议的工作流程：**

　　服务器认证阶段：

　　1）客户端向服务器发送一个开始信息“Hello”以便开始一个新的会话连接；

　　2）服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户的“Hello”信息时将包含生成主密钥所需的信息；

　　3）客户根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器；

　　4）服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

　　用户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回（数字）签名后的提问和其公开密钥，从而向服务器提供认证。

　　从SSL 协议所提供的服务及其工作流程可以看出，SSL协议运行的基础是商家对消费者信息保密的承诺，这就有利于商家而不利于消费者。在电子商务初级阶段，由于运作电子商务的企业大多是信誉较高的大公司，因此这问题还没有充分暴露出来。但随着电子商务的发展，各中小型公司也参与进来，这样在电子支付过程中的单一认证问题就越来越突出。虽然在SSL3.0中通过数字签名和数字证书可实现浏览器和Web服务器双方的身份验证，但是SSL协议仍存在一些问题，比如，只能提供交易中客户与服务器间的双方认证，在涉及多方的电子交易中，SSL协议并不能协调各方间的安全传输和信任关系。在这种情况下，Visa和MasterCard两大信用卡公组织制定了SET协议，为网上信用卡支付提供了全球性的标准。

　　TLS(Transport Layer Security Protocol)：安全传输层协议

　　安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成： TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。较低的层为 TLS 记录协议，位于某个可靠的传输协议（例如 TCP）上面。

　　TLS 记录协议提供的连接安全性具有两个基本特性：

* 私有――对称加密用以数据加密（DES 、RC4 等）。对称加密所产生的密钥对每个连接都是唯一的，且此密钥基于另一个协议（如握手协议）协商。记录协议也可以不加密使用。
* 可靠――信息传输包括使用密钥的MAC进行信息完整性检查。安全哈希功能（ SHA、MD5 等）用于 MAC 计算。记录协议在没有 MAC 的情况下也能操作，但一般只能用于这种模式，即有另一个协议正在使用记录协议传输协商安全参数。

　　TLS记录协议用于封装各种高层协议。作为这种封装协议之一的握手协议允许服务器与客户机在应用程序协议传输和接收其第一个数据字节前彼此之间相互认证，协商加密算法和加密密钥。 TLS 握手协议提供的连接安全具有三个基本属性：

* 可以使用非对称的，或公共密钥的密码术来认证对等方的身份。该认证是可选的，但至少需要一个结点方。
* 共享加密密钥的协商是安全的。对偷窃者来说协商加密是难以获得的。此外经过认证过的连接不能获得加密，即使是进入连接中间的攻击者也不能。
* 协商是可靠的。没有经过通信方成员的检测，任何攻击者都不能修改通信协商。

　　TLS的最大优势就在于：TLS是独立于应用协议。高层协议可以透明地分布在TLS协议上面。然而， TLS 标准并没有规定应用程序如何在TLS上增加安全性；它把如何启动 TLS 握手协议以及如何解释交换的认证证书的决定权留给协议的设计者和实施者来判断。

**协议结构**

　　TLS 协议包括两个协议组――TLS记录协议和TLS握手协议――每组具有很多不同格式的信息。在此文件中我们只列出协议摘要并不作具体解析。具体内容可参照相关文档。

　　TLS记录协议是一种分层协议。每一层中的信息可能包含长度、描述和内容等字段。记录协议支持信息传输、将数据分段到可处理块、压缩数据、应用MAC 、加密以及传输结果等。对接收到的数据进行解密、校验、解压缩、重组等，然后将它们传送到高层客户机。

　　TLS连接状态指的是TLS记录协议的操作环境。它规定了压缩算法、加密算法和MAC算法。

　　TLS记录层从高层接收任意大小无空块的连续数据。密钥计算：记录协议通过算法从握手协议提供的安全参数中产生密钥、 IV 和MAC密钥。

　　TLS 握手协议由三个子协议组构成，允许对等双方在记录层的安全参数上达成一致、自我认证、例示协商安全参数、互相报告出错条件。

**关系就是。。。。并列关系**

　　最新版本的TLS（Transport Layer Security，传输层安全协议）是IETF（Internet Engineering Task Force，Internet工程任务组）制定的一种新的协议，它建立在SSL 3.0协议规范之上，是SSL 3.0的后续版本。在TLS与SSL3.0之间存在着显著的差别，主要是它们所支持的加密算法不同，所以TLS与SSL3.0不能互操作。

　　1．TLS与SSL的差异

　　1）版本号：TLS记录格式与SSL记录格式相同，但版本号的值不同，TLS的版本1.0使用的版本号为SSLv3.1。

　　2）报文鉴别码：SSLv3.0和TLS的MAC算法及MAC计算的范围不同。TLS使用了RFC-2104定义的HMAC算法。SSLv3.0使用了相似的算法，两者差别在于SSLv3.0中，填充字节与密钥之间采用的是连接运算，而HMAC算法采用的是异或运算。但是两者的安全程度是相同的。

　　3）伪随机函数：TLS使用了称为PRF的伪随机函数来将密钥扩展成数据块，是更安全的方式。

　　4）报警代码：TLS支持几乎所有的SSLv3.0报警代码，而且TLS还补充定义了很多报警代码，如解密失败（decryption\_failed）、记录溢出（record\_overflow）、未知CA（unknown\_ca）、拒绝访问（access\_denied）等。

　　5）密文族和客户证书：SSLv3.0和TLS存在少量差别，即TLS不支持Fortezza密钥交换、加密算法和客户证书。

　　6）certificate\_verify和finished消息：SSLv3.0和TLS在用certificate\_verify和finished消息计算MD5和SHA-1散列码时，计算的输入有少许差别，但安全性相当。

　　7）加密计算：TLS与SSLv3.0在计算主密值（master secret）时采用的方式不同。

　　8）填充：用户数据加密之前需要增加的填充字节。在SSL中，填充后的数据长度要达到密文块长度的最小整数倍。而在TLS中，填充后的数据长度可以是密文块长度的任意整数倍（但填充的最大长度为255字节），这种方式可以防止基于对报文长度进行分析的攻击。

　　2．TLS的主要增强内容

　　TLS的主要目标是使SSL更安全，并使协议的规范更精确和完善。TLS 在SSL v3.0 的基础上，提供了以下增强内容：

　　1）更安全的MAC算法

　　2）更严密的警报

　　3）“灰色区域”规范的更明确的定义

　　3．TLS对于安全性的改进

　　1）对于消息认证使用密钥散列法：TLS 使用“消息认证代码的密钥散列法”（HMAC），当记录在开放的网络（如因特网）上传送时，该代码确保记录不会被变更。SSLv3.0还提供键控消息认证，但HMAC比SSLv3.0使用的（消息认证代码）MAC 功能更安全。

　　2）增强的伪随机功能（PRF）：PRF生成密钥数据。在TLS中，HMAC定义PRF。PRF使用两种散列算法保证其安全性。如果任一算法暴露了，只要第二种算法未暴露，则数据仍然是安全的。

　　3）改进的已完成消息验证：TLS和SSLv3.0都对两个端点提供已完成的消息，该消息认证交换的消息没有被变更。然而，TLS将此已完成消息基于PRF和HMAC值之上，这也比SSLv3.0更安全。

　　4）一致证书处理：与SSLv3.0不同，TLS试图指定必须在TLS之间实现交换的证书类型。

　　5）特定警报消息：TLS提供更多的特定和附加警报，以指示任一会话端点检测到的问题。TLS还对何时应该发送某些警报进行记录。

SSL与远程接入VPN

**[企业认领](http://www.baike.com/docClaimApply.do?action=showClaimDocApply&docTitle=SSL%E4%B8%8E%E8%BF%9C%E7%A8%8B%E6%8E%A5%E5%85%A5VPN" \t "_blank)**

开放分类：[图书](http://fenlei.baike.com/%E5%9B%BE%E4%B9%A6/?prd=zhengwenye_left_kaifangfenlei" \t "_blank" \o "图书)[科技](http://fenlei.baike.com/%E7%A7%91%E6%8A%80/?prd=zhengwenye_left_kaifangfenlei" \t "_blank" \o "科技)

《SSL与远程接入VPN》，作　者：（美国）Jaxib Frahim1，　出版社： 人民邮电出版社。

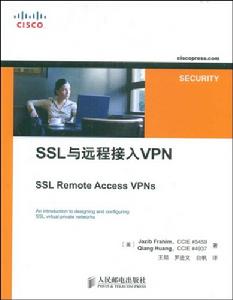
[编辑摘要](javascript:void(0);)



### 目录

* 1**[版权信息](javascript:void(0)" \o "版权信息)**
* 2**[内容简介](javascript:void(0)" \o "内容简介)**
* 3**[作者简介](javascript:void(0)" \o "作者简介)**
* 4**[编辑推荐](javascript:void(0)" \o "编辑推荐)**
* 5**[目录](javascript:void(0)" \o "目录)**
* 1**[版权信息](javascript:void(0))**
* 2**[内容简介](javascript:void(0))**
* 3**[作者简介](javascript:void(0))**
* 4**[编辑推荐](javascript:void(0))**
* 5**[目录](javascript:void(0))**

## 版权信息/SSL与远程接入VPN [编辑](http://www.baike.com/wiki/SSL%E4%B8%8E%E8%BF%9C%E7%A8%8B%E6%8E%A5%E5%85%A5VPN" \t "_self)

[](http://tupian.baike.com/a4_41_56_01200000030851134373563863925_jpg.html)

书 名：SSL与远程接入VPN   
  
　　作　者：（美国）Jaxib Frahim1、（美国）Qiang huang著，王喆 罗进文 白帆 译   
  
　　[出版社](http://www.baike.com/sowiki/%E5%87%BA%E7%89%88%E7%A4%BE?prd=content_doc_search" \t "_blank" \o "出版社)： [人民邮电出版社](http://www.baike.com/sowiki/%E4%BA%BA%E6%B0%91%E9%82%AE%E7%94%B5%E5%87%BA%E7%89%88%E7%A4%BE?prd=content_doc_search" \t "_blank" \o "人民邮电出版社)   
  
　　出版时间： 2009   
  
　　[ISBN](http://www.baike.com/sowiki/ISBN?prd=content_doc_search" \t "_blank" \o "ISBN)：9787115196392   
  
　　开本： 16   
  
　　定价：45.00 元

## 内容简介/SSL与远程接入VPN [编辑](http://www.baike.com/wiki/SSL%E4%B8%8E%E8%BF%9C%E7%A8%8B%E6%8E%A5%E5%85%A5VPN" \t "_self)

　　《SSL与远程接入VPN》提供了对[SSLVPN](http://www.baike.com/sowiki/SSLVPN?prd=content_doc_search" \t "_blank" \o "SSLVPN)技术的全面指导，并讨论了如何在能够使用CiscoSSLVPN的设置上实现SSLVPN。全书内容可分为3个部分，第1部分包括第1章和第2章，概述了远程访问VPN技术，并介绍了SSLVPN技术；第2部分包括第3章和第4章，介绍了基于不同设计考虑的CiscoSSLVPN产品系列；第3部分包括第5章、第6章和第7章，介绍了构成SSLVPN解决方案的各组件的安装、配置、部署和故障排除。   
  
　　《SSL与远程接入VPN》旨在为网络专业人员提供系统性的指导。读者需要具备TCP/IP和组网的基本知识，熟悉Cisco路由器/防火墙及其命令行界面，并对整个SSLVPN解决方案有一个整体的认识。

SSL VPN

[编辑](javascript:;) [锁定](http://baike.baidu.com/view/10812319.htm" \t "_blank" \o "锁定)

SSL VPN是解决[远程用户](http://baike.baidu.com/view/1541147.htm" \t "_blank)访问公司敏感数据最简单最安全的解决技术。与复杂的IPSec VPN相比，SSL通过简单易用的方法实现信息远程连通。任何安装浏览器的机器都可以使用SSL VPN， 这是因为SSL 内嵌在浏览器中，它不需要象传统IPSec VPN一样必须为每一台客户机安装客户端软件。

中文名

SSL VPN

针对对象

[远程用户](http://baike.baidu.com/view/1541147.htm" \t "_blank)

需要工具

任何安装[浏览器](http://baike.baidu.com/view/7718.htm" \t "_blank)的机器

特    点

通过简单易用的方法

SSL

安全套接层

目录

1 [SSL介绍](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "1)

2 [VPN介绍](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "2)

3 [技术演变](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "3)

4 [定义](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "4)

5 [特征](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "5)

6 [国内现状](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "6)

▪ [深信服SSL VPN](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "6_1)

▪ [市场状况](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "6_2)

▪ [产品介绍](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "6_3)

▪ [产品荣誉](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "6_4)

▪ [产品功能亮点](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "6_5)

▪ [客户案例](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "6_6)

7 [特点](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "7)

8 [优点](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "8)

9 [产品纵览](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "9)

10 [选购注意事项](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "10)

▪ [应用需求](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "10_1)

▪ [安全需求](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "10_2)

▪ [易于管理维护](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "10_3)

▪ [性能](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "10_4)

▪ [服务](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "10_5)

▪ [结束语](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "10_6)

11 [技术现状](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "11)

12 [发展前景](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "12)

13 [VPN技术](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "13)

14 [使用说明](http://baike.baidu.com/link?url=0_MMO5KTwDN_3AtDIisIdl-u7m-U_tAIIEJWWYhmaVC8rzq_Lin3Nxd3wj3_rIBuxnr0c4fdaYpsQSCMm8N8c8GltI6Rhq-9l1E4oXJyBHq" \l "14)

SSL VPNSSL介绍

[编辑](javascript:;)

SSL（安全套接层）协议是一种在internet上保证发送信息安全的通用协议，采用[B/S结构](http://baike.baidu.com/view/268862.htm" \t "_blank)（Browser/Server，浏览器/服务器模式）。它处在应用层，SSL用公钥加密通过SSL连接传输的数据来工作。SSL协议指定了在应用程序协议和TCP/IP 之间进行数据交换的安全机制，为TCP/IP连接提供数据加密、服务器认证以及可选择的客户机认证。

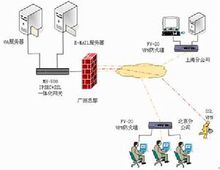
SSL协议可分为两层：SSL记录协议(SSL Record Protocol）：它建立在可靠的[传输协议](http://baike.baidu.com/view/441895.htm" \t "_blank)（如TCP）之上，为高层协议提供[数据封装](http://baike.baidu.com/view/262940.htm" \t "_blank)、压缩、加密等基本功能的支持。SSL握手协议(SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行[身份认证](http://baike.baidu.com/view/1014826.htm" \t "_blank)、协商[加密算法](http://baike.baidu.com/view/155969.htm" \t "_blank)、交换加密[密钥](http://baike.baidu.com/view/934.htm" \t "_blank)等。

SSL VPNVPN介绍

[编辑](javascript:;)

VPN的英文全称是“Virtual Private Network”，翻译过来就是“[虚拟专用网络](http://baike.baidu.com/view/480950.htm" \t "_blank)”。顾名思义，虚拟专用网络我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在[Internet](http://baike.baidu.com/view/11165.htm" \t "_blank)上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买[路由器](http://baike.baidu.com/view/1360.htm" \t "_blank)等硬件设备。VPN技术原是路由器具有的重要技术之一，一句话，VPN的核心就是在利用公共网络建立虚拟私有网。

[虚拟专用网](http://baike.baidu.com/view/16118.htm" \t "_blank)（VPN）被定义为通过一个公用网络（通常是[因特网](http://baike.baidu.com/view/1706.htm" \t "_blank)）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业公司分支机构、商业伙伴及供应商同公司的[内部网](http://baike.baidu.com/view/21848.htm" \t "_blank)建立可信的安全连接，并保证数据的安全传输。

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/5f9e93b14eca4c150823023f?fr=lemma%26ct=single)SSL VPN技术

[虚拟专用网](http://baike.baidu.com/view/16118.htm" \t "_blank)可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全外联网虚拟专用网。

针对不同的用户要求，VPN有三种解决方案：远程访问虚拟网（[Access VPN](http://baike.baidu.com/view/1542730.htm" \t "_blank)）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN），这三种类型的VPN分别与传统的远程访问网络、企业内部的Intranet以及企业网和相关合作伙伴的企业网所构成的Extranet（外部扩展）相对应。

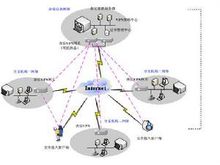
目前很多单位都面临着这样的挑战：分公司、经销商、合作伙伴、客户和外地出差人员要求随时经过公用网访问公司的资源，这些资源包括：公司的内部资料、办公OA、[ERP系统](http://baike.baidu.com/view/86915.htm" \t "_blank)、[CRM系统](http://baike.baidu.com/view/676475.htm" \t "_blank)、[项目管理系统](http://baike.baidu.com/view/2091970.htm" \t "_blank)等。现在很多公司通过使用[IPSec VPN](http://baike.baidu.com/view/1207621.htm" \t "_blank)来保证公司总部和分支机构以及移动工作人员之间安全连接。

对于很多IPSec VPN用户来说，IPSec VPN的解决方案的高成本和复杂的结构是很头疼的。存在如下事实：在部署和使用软硬件客户端的时候，需要大量的评价、部署、培训、升级和支持，对于用户来说，这些无论是在经济上和技术上都是个很大的负担，将远程解决方案和昂贵的内部应用相集成，对任何IT专业人员来说都是严峻的挑战。由于受到以上IPSec VPN的限制，大量的企业都认为IPSec VPN是一个成本高、复杂程度高，甚至是一个无法实施的方案。为了保持竞争力，消除企业内部信息孤岛，很多公司需要在与企业相关的不同的组织和个人之间传递信息，所以很多公司需要找一种实施简便，不需改变现有网络结构，运营成本低的解决方案。

SSL VPN技术演变

[编辑](javascript:;)

随着应用程序从C/S 结构向Web 的迁移，企业必须面对一个新的挑战，就是如何在不影响最终用户使用的前提下实现在任何地方灵活访问这些应用程序。在最近20 年

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/245e8bca4e12a2c7c8176838?fr=lemma%26ct=single)SSL VPN技术

间，用户和管理层听到因为安全原因不能够在公司以外访问内部应用程序的声音不绝于耳。在70 年代，人们对[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)概念几乎等同于从远端的办公地点访问应用程序，这需要设置非常昂贵的WAN 网并租用连接线路。

到了80 年代，一小部分用户可以使用[调制解调器](http://baike.baidu.com/view/1074.htm" \t "_blank)直接拨号到modem banks 或他们自己的PC 上，但是使用费用相当高昂只能有非常有限的小部分人使用。而且在那时候，在家使用个人电脑才刚刚成为主流，远程访问需求还不是很大。随着90 年代的来临， 在家用PC 盛行的同时，移动电脑开始显现，在家办公也开始兴起。公司管理者和销售员们开始在外出出差的时候携带他们的笔记本电脑，他们需要实时访问公司内部信息，设立IPSec VPN 可以保护用户[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)。它可以提供足够的安全性，但是问题是安装和维护相当麻烦。任何在PC 上的改变对VPN 而言可能都是一场灾难，最终用户不得不硬着头皮忍受这些变化，因为他们别无选择。即使是现在，你也很难找到一个用户，他的VPN 一点儿问题也没有。从管理员的角度来讲，使用IPSec VPN 不仅仅意味着要对客户端进行安装和调试，而且还需要调整整个网络的结构。在[数据包](http://baike.baidu.com/view/25880.htm" \t "_blank)进行传输时NAT 不能完全工作正常，有时候会出现连接断开的现象，改变[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)设置可以解决这一问题但是必须要做大量的管理工作。如果IT 管理部门可以完全控制从后端到客户的网络结构，其管理复杂性可以忍受；当IT 管理部门不能完全控制时，管理复杂性就要成倍增加。这种情况同样发生在本地NAT 和防火墙对合作伙伴，在家里或在酒店。

如今， 公司开始把眼光放在他们是否选择了合适的安全[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)系统上。使用IPSec VPN 和租用WAN 线路对于不经常更改网络结构的用户来说是非常好的选择。如果情况并非如此，用户就需要另做选择。现在，已经有公司开始考虑使用架构在[因特网](http://baike.baidu.com/view/1706.htm" \t "_blank)上的SSL 协议，在不破坏已有[网络布局](http://baike.baidu.com/view/4555497.htm" \t "_blank)的前提下进行安全远程访问。SSL 是通过因特网进行加密传输保护一种常用方法，许多公司对他们的[内部网](http://baike.baidu.com/view/21848.htm" \t "_blank)和外部网执行了SSL 设置，通过SSL VPN 进行[访问控制](http://baike.baidu.com/view/469056.htm" \t "_blank)。

SSL VPN定义

[编辑](javascript:;)

SSL VPN 的发展对现有SSL 应用是一个补充，它增加了公司执行[访问控制](http://baike.baidu.com/view/469056.htm" \t "_blank)和安全的级别和能力。

SSL VPN 还对那些因为使用[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)应用系统而降低公司安全性的企业有所帮助。从属性上讲，拨号可以保证相对安全性，因为特定的电话线可以确认用户的身份。客户端/[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)和旧版本的VPN 自身也拥有一定级别的安全保障能力，因为客户端软件是需要安装的。但是，以这样的[安全策略](http://baike.baidu.com/view/160028.htm" \t "_blank)和属性， 不可否认，黑客入侵、安全威胁、身份欺诈呈增长趋势。现在，使用SSL VPN，安全特性已经发生了改变，人们可以通过浏览器访问应用程序。

如果把SSL 和VPN 两个概念分开，大多数人都清楚他们

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/6648d73dd5143e869e3d6239?fr=lemma%26ct=single)SSL VPN技术

的含义，但是有多少人知道他们合在一起的意思呢？从学术和商业的角度来讲，因为他们代表的含义有所不同，因而常常会被曲解。

SSL 通过加密方式保护在互联网上传输的数据安全性，它可以自动应用在每一个浏览器上。这里，需要提供一个[数字证书](http://baike.baidu.com/view/16501.htm" \t "_blank)给Web[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)，这个数字证书需要付费购买，相对而言，给应用程序设立SSL 服务是比较容易的。如果应用程序本身不支持SSL， 那么就需要改变一些链接，这只与应用程序有关。对于出现较大信息量的情况，建议给SSL 进行加速以避免流量瓶颈。通常SSL 加速装置为热插拔装置。

VPN 则主要应用于虚拟连接网络，它可以确保数据的机密性并且具有一定的[访问控制](http://baike.baidu.com/view/469056.htm" \t "_blank)功能。过去，VPN 总是和IPSec 联系在一起，因为它是VPN 加密信息实际用到的协议。IPSec 运行于网络层，IPSec VPN 则多用于连接两个网络或点到点之间的连接。

以上我们简要介绍了SSL和VPN，现在我们要了解一下SSL和VPN是怎样结合在一起的？大量理论可以证明SSL的独特性以及VPN所能提供的安全远程访问控制能力。到目前为止，SSL VPN是解决远程用户访问敏感公司数据最简单最安全的解决技术。与复杂的IPSec VPN相比，SSL通过简单易用的方法实现信息远程连通。任何安装浏览器的机器都可以使用SSL VPN， 这是因为SSL 内嵌在浏览器中，它不需要象传统IPSec VPN一样必须为每一台客户机安装客户端软件。这一点对于拥有大量机器（包括家用机，工作机和客户机等等）需要与公司机密信息相连接的用户至关重要。人们普遍认为它将成为安全[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)的新生代。

SSL VPN特征

[编辑](javascript:;)

从概念角度来说，SSL VPN即指采用SSL （Security Socket Layer）协议来实现远程接入的一种新型VPN技术。SSL协议是[网景](http://baike.baidu.com/view/478896.htm" \t "_blank)公司提出的基于WEB应用的安全协议，它包括：[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)认证、[客户认证](http://baike.baidu.com/view/3032919.htm" \t "_blank)（可选）、SSL链路上的[数据完整性](http://baike.baidu.com/view/702953.htm" \t "_blank)和SSL链路上的数据保密性。对于内、外部应用来说，使用SSL可保证信息的真实性、完整性和保密性。目前SSL 协议被广泛应用于各种浏

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/8697397f63f3024929388a3b?fr=lemma%26ct=single)SSL VPN技术

览器应用，也可以应用于Outlook等使用TCP协议传输数据的C/S应用。正因为SSL 协议被内置于IE等浏览器中，使用SSL 协议进行认证和[数据加密](http://baike.baidu.com/view/696431.htm" \t "_blank)的SSL VPN就可以免于安装客户端。相对于传统的IPSEC VPN而言，SSL VPN具有部署简单，无客户端，维护成本低，网络适应强等特点，这两种类型的VPN之间的差别就类似C/S构架和B/S构架的区别。[1]

一般而言，SSL VPN必须满足最基本的两个要求：

⒈ 使用SSL 协议进行认证和加密；没有采用SSL 协议的VPN产品自然不能称为SSL VPN，其安全性也需要进一步考证。

⒉ 直接使用浏览器完成操作，无需安装独立的客户端；即使使用了SSL 协议，但仍然需要分发和安装独立的VPN客户端 （如Open VPN）不能称为SSL VPN，否则就失去了SSL VPN易于部署，免维护的优点了。

SSL VPN国内现状

[编辑](javascript:;)

SSL VPN深信服SSL VPN

SSL VPN市场状况

国际权威市场研究机构Frost&Sullivan在2014年发布了《中国SSLVPN市场分析报告》，自2005年推出IPSec/SSL二合一VPN产品以来，深信服在中国市场取得了长足的进步。2008年，深信服以31.1%的市场占有率，首次成为市场第一。如今，凭借实力出众的产品以及深受大型企事业单位认可的服务，深信服已连续六年获SSLVPN市场占有率第一。

SSL VPN产品介绍

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/e850352ac65c1038ccff45b0b6119313b07e893b?fr=lemma%26ct=single)

深信服为您提供高速、易用、安全且高度可靠的SSLVPN产品。作为中国SSLVPN领域的绝对领导者和中国SSLVPN核心技术标准制定者，深信服SSLVPN解决方案已拥有超过18000家客户，在政府、金融、运营商、能源、教育、大中型企业等各个领域都得到了广泛应用。在中国入选世界五百强的企业中，有近70%的企业选择了深信服SSLVPN解决方案。同时，随着BYOD和云计算的趋势愈演愈烈，SSLVPN有望成为移动安全领域的重要组件，来保障云访问的安全性。

轻松移动办公

深信服SSLVPN可助您轻松使用笔记本、桌面PC、智能手机、Pad等移动终端设备实现安全、便捷的远程接入内网，在降低运营成本的同时大幅提高企业的生产效率。

EasyConnect远程应用发布

深信服EasyConnect采用应用虚拟化的技术，通过SSLVPN将企业内网的应用程序界面以图形的方式呈现在智能终端之上，无需开发APP，即可通过深信服EasyConnectAPP将各办公系统发布到IOS或Android系统的终端上使用，轻松实现安全高效的移动办公。

App安全加固

深信服EasyApp安全加固解决方案通过在App中集成VPN安全模块，无需开发人员花费大量时间和精力进行二次开发，即可保证企业用户的办公App安全接入，实现从用户登陆、数据传输、服务器端和终端设备等方面的安全防护。

第三方远程接入

深信服SSLVPN为您提供完整的第三方远程接入方案，融合了多种加速技术并进行细致的应用权限访问控制，让您的第三方合作伙伴能享受快速资源共享体验的同时，实现应用的安全、可控的访问。

内网分区逻辑隔离保护

深信服SSLVPN通过细致的权限划分、多种认证安全机制、客户端安全检查等多项技术为您实现安全、可靠、低成本、灵活度高的网络逻辑隔离方案。

关键业务信息系统安全加固

深信服SSLVPN提供完整的关键业务信息系统安全加固方案，提供完整的身份认证机制及访问过程保护，并具有专利技术主从帐号绑定指定用户的应用访问帐号，杜绝帐号冒用及越权访问。

防范WLAN非法访问

深信服SSLVPN为您提供安全的WLAN接入方案，通过SSLVPN进行WLAN接入的统一认证，严格控制访问用户，防止信息泄漏，保护应用安全。

SSL VPN产品荣誉

连续6年获SSLVPN市场占有率第一

国家SSLVPN技术标准核心制定者

推出全球第一款IPSec/SSLVPN二合一VPN（2005年）

国内唯一一家入选GartnerSSLVPN魔力象限厂商

申请SSLVPN专利技术30余项

率先在SSLVPN领域开发了远程应用发布（应用虚拟化）技术

入围多家核心单位集采：中央政府、国税总局、招商银行等

SSLVPN客户端并发授权已累计使用超过260万个

SSL VPN产品功能亮点

最安全：端到端的安全防护体系，采用业内领先加密技术，提供多种身份认证方式、主从绑定等特色功能，保证用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全；

最快速：通过多线路智能选路、单边加速等多项专利技术，从链路、传输、数据、引用，层层优化，访问速度可提升80%，给每个接入用户不同以往的畅快体验；

最好用：完整支持Windows、Linux、MACOS、IOS、Android等主流操作系统，办公电脑、笔记本、智能手机、pad等设备均可适配使用；化繁为简的部署及使用，管理简单，使用方便，支持非对称集群，实现高性价比弹性扩容；

全面支持移动互联网：深信服EasyConnect应用虚拟化技术及App安全加固解决方案，帮助用户完美实现移动业务，保障移动办公及业务的安全。

SSL VPN客户案例

中国人民共和国最高人民法院、中国海关总署、中国人民银行总行、招商银行、北京移动、江苏联通、南方电网、中国科学院、北京大学、招商局集团、华润集团等。

F5公司-FirePass SSLVPN

F5于2000年底进驻中国，并在国内推出先进的SSL VPN解决方案。早在2004年12月15日，全球应用流量管理专家美国[F5](http://baike.baidu.com/view/418394.htm" \t "_blank)公司在北京发布了其最新款的网络安全产品，包括[应用防火墙](http://baike.baidu.com/view/2474127.htm" \t "_blank)TrafficShield和[安全套接字层](http://baike.baidu.com/view/6241732.htm" \t "_blank)[虚拟专用网](http://baike.baidu.com/view/16118.htm" \t "_blank)（SSL VPN）解决方案FirePass控制器。著名互联网安全领域专家、F5公司全球[网络安全产品](http://baike.baidu.com/view/948081.htm" \t "_blank)市场总监Andrew Stern和F5中国市场渠道总监柯文联合向外界发布了这两款产品。

TrafficShield应用防火墙为企业的web应用及基础架构提供最全面的安全保护，防御普通与目标攻击。该产品中应用的应用流程模型（AFM）利用积极安全逻辑根据用户会话信息、用户输入内容、及应用响应内容对每一个[事务](http://baike.baidu.com/view/121511.htm" \t "_blank)进行验证。在此种高安全模式下，仅允许有效应用流量通过，并阻止其它一切请求。

F5 FirePass控制器通过向企业用户提供访问网络应用及资源所需的性能、安全性、管理性及可靠性来满足企业组织的[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)需求。终端用户将受益于其在任何地点、使用任何设备、处于任何访问模式（包括拔号、DSL、cable及[无线网络](http://baike.baidu.com/view/5030.htm" \t "_blank)）下对网络的无缝接入的特性。

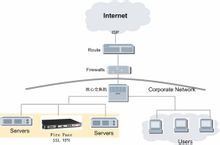
F5 SSL VPN应用案例

面对企业感到莫名的难题，F5公司通过成熟的系统方案，减少使用IPSec的运营维护成本，使[IT管理](http://baike.baidu.com/view/647545.htm" \t "_blank)人员的工作效率大大提高。

企业用IPSec的[VPN](http://baike.baidu.com/view/19735.htm" \t "_blank)用于连接远程移动用户，这种VPN在某些地点受到某些地区[ISP](http://baike.baidu.com/view/855.htm" \t "_blank)的影响，或者受某些网络设备的影响，不能正常访问公司总部的内部企业网络。为解决这种莫名的难题，F5公司提供一个专业级的技术方案。

F5公司将F5的[SSL](http://baike.baidu.com/view/16147.htm" \t "_blank)VPN产品部署在企业的内部核心[交换机](http://baike.baidu.com/view/1077.htm" \t "_blank)上，这样做是保证不会对用户的原有网络造成任何影响，而只需要在边界[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)上做一个地址转换，这样远程移动用户或者分支机构就可以先通过防火墙访问SSLVPN产品，进入到企业内部网络中，进行企业内部Intranet的访问；同时，远程移动和分支不受任何接入的限制。

解决方案如图示：

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/91ef76c6a7efce1b163eff69af51f3deb48f657f?fr=lemma%26ct=single)F5 SSL VPN解决方案

赛蓝ssl vpn

安全性

多种安全认证，支持指纹认证、短信认证、USB KEY认证、U-KEY认证；国密办认证体系、动态令牌认证、X.509数字证书认证、LDAP，Radius等第三方服务器认证、E-MAIL账户认证，MAC地址绑定认证、VIP用户认证，并提供多种混合模式认证；点对点全程加密，客户对资源的每一次操作都需要经过安全的身份验证和加密，确保点到点的远程访问安全。因为是直接开启应用系统，并没在网络层上连接，攻击机会相对就减少。CYLAN SGA VPN还保护不同协议间的通信，增强安全性。

经济性

只需要在总部放置一台硬件设备，就可以实现所有用户的远程安全访问快速地接入服务，支持LAN-TO-LAN互访。

可扩展性

支持单臂双臂模式，支持多站点及多站点分级管理，可以满足企业多部门分级管理的需求，可部署在网络中任一节点处，可以随时根据需要，添加需要发布的服务器资源，因此无需影响原有网络结构。

访问控制

可以根据用户的不同身份，给予不同的访问权限，提供VIP用户来符合企业特殊要求，细致的用户锁定策略,支持时段锁定和管理员解锁两种方式，还可以对每个访问人员进行数字签名，保证每笔数据的不可否认性，为事后追踪提供了依据。

部署与管理成本

部署容易、维护方便、发布快捷、使用简单，降低了部署客户软件的复杂性，缩减了客户的人力管理成本。

低带宽特性

即便使用CDMA和GPRS上网方式也可以流畅的运行您广域网络上的应用，即使是大型的C/S软件也仅仅需要20K的带宽。

高级管理

支持CA中心，可以申请/颁发/吊销证书，支持自签名证书和第三方证书导入，支持PKI体系；支持数据库认证(MYSQL、ORACLE、SYBASE)，支持第三方用户导入(文本、数据库)。

网神SSL VPN

简介

网神SecSSL 3600是一款多功能VPN网关，其提供基于SSL 协议+IPsec协议的二合一VPN服务和网络防火墙服务，实现数据传输和保护；采用成熟的VPN技术实现用户应用客户端与应用业务的跨地域、跨网络互连；采用多种认证协议实现对用户的身份的全面认证；并通过详细的日志信息提供全面、翔实的审计服务。

网神SecSSL 3600采用SSL协议在远端用户与网关之间建立VPN连接，保证数据在传输过程中不被窃听、重放、窜扰等，针对每一个用户的接入，采用认证技术确保用户的身份为可信的。网关可以与LDAP/AD/Radius/证书认证服务器互动，提供了灵活多样的认证解决方案。

网神SecSSL 3600无需预先安装客户端软件，家庭办公用户、移动办公用户和合作伙伴等即可轻松安全地访问企业内部网。产品不仅能保护Web应用，而且支持广泛的基于TCP/UDP的多种应用。为了提高远程接入的使用范围，还提供网络连接模式，它允许远程接入的客户访问企业内部网络的任意IP资源，也可以实现两个局域网络之间的互联。

网神SecSSL 3600内置IPsec协议功能模块，网络防火墙功能模块和网络入侵检测已经应用防火墙功能模块，在为用户提供SSL-VPN服务基础之上，能够为用户提供全面的网络安全防护解决方案。

网神SecSSL 3600提供全面的日志、审计和监控功能，管理员可以查看用户使用系统的历史纪录、当前系统的运行状态和当前在线用户的实时信息。

产品亮点

All in One VPN技术，实现各种终端安全接入，集成SSL-VPN与IPsec VPN，同时支持windows, Linux, Mac, iOS, Android的全网络接入，使用更灵活，业务支持更全面。

用户桌面远程唤醒功能，实现随时随地办公与节能减排的最佳平衡，管理员可以为用户注册用户的桌面电脑，这样用户在登录系统后可以通过远程唤醒的方式启动办公的桌面电脑，实现远程访问自己的办公主机；

多链路智能选路技术，实现对远程用户接入的快速响应，支持多条链路接入，即满足不同运营商的带宽差别，又能实现冗余备份；

领先的虚拟安全桌面技术，确保业务数据远端不落地，虚拟安全桌面使得用户的桌面数据都在虚拟安全桌面里面，业务数据不会泄漏，满足客户当前形势下的防数据泄漏要求。

灵活组合的认证模式，确保用户身份安全，支持多种认证方式组合；支持用户终端的绑定，确保用户身份的安全和仿冒；

支持动态短信授权，确保关键业务访问可控，满足审计要求，用户访问关键业务的时候，可以设置短信临时授权，这种功能对于外包业务人员访问企业业务数据具有满足企业IT系统高安全的作用。

具备应用审计，能够对应用业务命令进行审计，对远程接入用户的http, telnet应用，可以记录用户的命令，并展现日志报表，从而使得远程接入部分满足对外包接入人员的安全审计合规性要求。

SSL VPN特点

[编辑](javascript:;)

SSL VPN的客户端程序，如Microsoft Internet Explorer、Netscape Communicator、Mozilla等已经预装在了终端设备中，因此不需要再次安装；

SSL VPN可在NAT代理装置上以透明模式工作；

SSL VPN不会受到安装在客户端与[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)之间的[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)等NAT设备的影响，穿透能力强；

SSL VPN将远程安全接入延伸到IPSec VPN扩展不到的地方，使更多的员工，在更多的地方，使用更多的设备，安全访问到更多的企业网络资源，同时降低了部署和支持费用； 客户端安全检查和授权访问等操作，实现起来更加方便。

SSL VPN可以在任何地点，利用任何设备，连接到相应的网络资源上。IPSec VPN通常不能支持复杂的网络，这是因为它们需要克服穿透防火墙、IP地址冲突等困难。所以IPSec VPN实际上只适用于易于管理的或者位置固定的地方。可以说从功能上讲，SSL VPN是企业远程安全接入的最佳选择。

但是虽然SSL VPN具有以上众多的优点，却由于SSL协议本身的局限性，使得性能远低于使用IPSec协议的设备。用户往往需要在简便使用与性能之间进行痛苦选择。这也是第二代VPN始终无法取代第一代VPN的原因。

SSL VPN优点

[编辑](javascript:;)

1、方便。实施[ssl](http://baike.baidu.com/view/16147.htm" \t "_blank)vpn只需要安装配置好中心网关即可。其余的客户端是免安装的，因此，实施工期很短，如果网络条件具备，连安装带调试，1-2天即可投入运营。

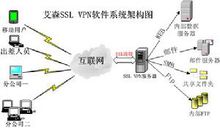
2、容易维护。sslvpn 维护起来简单，出现问题，就维护[网关](http://baike.baidu.com/view/807.htm" \t "_blank)就可以了。实在不行，换一台，如果有[双机备份](http://baike.baidu.com/view/4271261.htm" \t "_blank)的话，备份机器启动就可以了。

3、安全。sslvpn 是一个安全协议，数据全程加密传输的。另外，由于ssl网关隔离了内部[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)和客户端，只留下一个web浏览接口，客户端的大多数病毒木马感染不到内部服务器。而[ipsec vpn](http://baike.baidu.com/view/1207621.htm" \t "_blank)就不一样，实现的是ip级别的访问，远程网络和本地网络几乎没有区别。局域网能够传播的病毒，通过vpn一样能够传播。

SSL VPN产品纵览

[编辑](javascript:;)

随着SSL[VPN](http://baike.baidu.com/view/19735.htm" \t "_blank)应用的逐渐加温，越来越多的企业开始采纳SSL VP

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/f7426d8d44a93c53b21bba05?fr=lemma%26ct=single)SSL VPN技术

N的网络架构，来解决企业的[远程](http://baike.baidu.com/view/856599.htm" \t "_blank)访问需求。SSL VPN技术帮助用户通过标准的Web浏览器就可以访问重要的企业应用。这使得企业员工出差时不必再携带自己的笔记本电脑，仅仅通过一台接入了Internet的计算机就能访问企业资源，这为企业提高了效率也带来了方便。由于[SSL](http://baike.baidu.com/view/16147.htm" \t "_blank)VPN不像[IPSec VPN](http://baike.baidu.com/view/1207621.htm" \t "_blank)那样要购买和维护远程客户端或软件，因而要比后者造价低很多。现在许多企业对于SSL VPN的需求非常强烈，而且未来这种企业网络安全需要还将持续增长。许多国际网络安全厂商正在对SSL VPN这种新型业务形态进行重点投资，取代目前的IPSec系列产品将成为一种趋势。

产品应用

SSL VPN网关位于[企业网](http://baike.baidu.com/view/154900.htm" \t "_blank)的边缘，介于企业[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)与[远程用户](http://baike.baidu.com/view/1541147.htm" \t "_blank)之间，控制二者的通信。SSL VPN采用标准的[安全套接层](http://baike.baidu.com/view/525499.htm" \t "_blank)（SSL）对传输中的[数据包](http://baike.baidu.com/view/25880.htm" \t "_blank)进行加密，从而在[应用层](http://baike.baidu.com/view/239619.htm" \t "_blank)保护了数据的安全性。在不断扩展的互联网Web站点之间、无线热点和客户端间、远程办公室、酒店、传统交易大厅等场所，SSL VPN克服了IPSec VPN的不足，用户可以轻松实现安全易用、无需客户端安装且配置简单的[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)，从而降低用户的总成本并增加远程用户的工作效率。而同样在这些地方，设置传统的IPSec VPN非常困难，甚至是不可能的，这是由于必须更改[网络地址转换](http://baike.baidu.com/view/875777.htm" \t "_blank)（NAT）和[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)设置。

产品选购

对广大的用户来说要挑选一个明显的SSL VPN产品最爱比较困难，虽然有的SSL VPN产品表现一般，但是，多数[SSL](http://baike.baidu.com/view/16147.htm" \t "_blank)VPN产品是各有其优势。有的SSL VPN产品提供了一个成熟的应用层防火墙，有的SSL[VPN](http://baike.baidu.com/view/19735.htm" \t "_blank)产品提供了范围最为广泛的应用转换功能。SSL VPN产品是否最终令人满意，还取决于用户对自己需求的了解程度，适合自己的是最好的。

SSL VPN的发展主要是为了迎合用户在[远程](http://baike.baidu.com/view/856599.htm" \t "_blank)访问时能实现性价比的高要求。到目前为止，SSL VPN已经应用于各行各业，有企业用户，也有SOHO用户。用户在选购SSL VPN时，应根据自身特点和不同企业的业务规模，选择适合自己的SSL VPN产品。最好的选择，就是适合自己的。

一般，在选购SSL VPN产品时要注意以下几个问题：

具有强力的安全保障：首先是用户端接入的安全；其次是数据传输的安全；再次是内部资源的访问安全。

支持全面应用的连接。

使用操作性强，易于管理和维护。

运行要稳定，无网络中断。

不会因为处理[SSL](http://baike.baidu.com/view/16147.htm" \t "_blank)而降低了运行速率。

良好的综合性能和服务。

市面上的SSL VPN精品

目前，国内外的网络设备[商都](http://baike.baidu.com/view/19763.htm" \t "_blank)相继推出了自己SSL VPN产品，其中包括F5、Cisco、华为、ArrayNetworks等著名设备供应商。下面，我们罗列了目前市面上的主要的SSL VPN产品。

F5公司FirePass SSL VPN系列

F5的Fire Pass SSL VPN设备通过采用标准We b浏览器为用户提供了一种安全访问企业应用和数据的方式。无论在家中还是在路上，FirePass出色的性能、可扩展性、易于使用特性以及安全特性，均有助于提高工作效率，并保持企业数据的安全。

FirePass可提供

·安全兼容系统自动侦测，防止病毒感染。

· 与业内数量最多的病毒扫描及[个人防火墙](http://baike.baidu.com/view/973385.htm" \t "_blank)解决方案（超过100种不同的防病毒(AV）和个人防火墙版本）自动集成。

· 自动拦截受感染的文件上传或电子邮件附件。

· 自动重新路由并隔离受感染或非兼容的系统，将其放入自我补救网络(self remediation network）中——以减少呼叫帮助中心的次数。

·安全工作区可防止窃听及窍取敏感数据。

· 使用随机键输入系统进行安全登录，可防止按键记录器窃听。

· 由于能够与Fire Pass可视化策略编辑器完全集成，因此，可创建基于端点访问您的网络及您公司的安全配置文件的定制模板策略。

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/8ad4b31c8701a18b21a349e59e2f07082938fed4?fr=lemma%26ct=single)F5 Fire Pass SSL VPN可视化策略编辑器

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/f636afc379310a553f88855eb74543a9832610ef?fr=lemma%26ct=single)F5 Fire Pass SSL VPN资质

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/38dbb6fd5266d0166674c582972bd40735fa352e?fr=lemma%26ct=single)F5 Fire Pass SSL VPN

主要优势

一流的策略管理——独特的可视化策略编辑器能够提供直观、易用的“指向并点击”（poin-tand-click）界面，在降低管理成本的同时，轻松管理精细访问策略。

集成的端点安全性——提供安全虚拟工作区、预先登录终端完整性检查，以及端点信任管理等功能，从而解除了您的后顾之忧，使您无需浪费精力于管理事务。

广泛的应用支持——可实现从管理的及非管理的客户端设备从任何地方轻松、安全地访问电子邮件，Web门户、网络文件服务、[终端服务](http://baike.baidu.com/view/186609.htm" \t "_blank)、客户关系管理系统以及其它主要企业应用。

广泛的客户支持——Fire Pass可提供广泛的多平台支持，允许用户从Windows（98、2000、ME、XP、Vista）、MAC、Linux和Pocket PC客户端安全访问网络。还支持全新的Vista客户端操作系统和IE7。

企业级可扩充性与性能——在单一且易于管理的设备上可支持高达2,000个并发会话。通过与F5 BIG-IP本地流量管理器的集成，可支持几万个并发会话。借助任意IP应用流量的压缩和Web应用的[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)端高速缓存功能，可以优化最终用户的体验。

广泛的互操作性——借助Active Directory、Radius、LDAP、PKI、RSA ACE及其它方式，为现有网络基础设施和身份管理系统提供支持。所提供的Web门户集成产品可支持Java applets、Javascript重写及其它技术（已通过VPNC认证）。

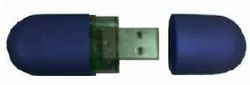
业内领先全球的高可用性——与F5 BIG-IP广域流量管理器的独特集成，能够于发生站点灾难时在整个WAN上提供高度可用性。故障切换支持在站点内提供高度可用性。

适用于大中型企业

Quidway SecPath 1000F 防火墙

Quidway SecPath 1000F[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)是华为3Com公司开发的新一代专业防火墙设备，支持SSL VPN，同时支持多种VPN业务可以作为大中型企业的内部防火墙设备，也可以作为中小企业的出口防火墙设备。

Quidway SecPath 1000F防火墙支持外部攻击防范、内网

[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/a8ad941372c76791f6039e06?fr=lemma%26ct=single)SSL VPN技术

安全、[流量监控](http://baike.baidu.com/view/5119004.htm" \t "_blank)、网页过滤、邮件过滤等功能，能够有效地保证网络的安全；采用ASPF[状态检测技术](http://baike.baidu.com/view/3897158.htm" \t "_blank)，可对连接过程和有害命令进行监测，并协同ACL完成动态包过滤；提供多种智能分析和管理手段，支持邮件告警，支持多种日志，提供网络管理[监控](http://baike.baidu.com/view/4340.htm" \t "_blank)，协助网络管理员完成网络的安全管理；支持AAA、NAT等技术，可以确保在开放的Internet上实现安全的、满足可靠质量要求的网络；支持多种VPN业务，如L2TP VPN、IPSec VPN、GRE VPN、华为动态VPN、SSL VPN等等，可以构建Internet、Intranet、Access等多种形式的VPN；提供基本的路由能力，支持RIP/OSPF/BGP/路由策略及[策略路由](http://baike.baidu.com/view/1138604.htm" \t "_blank)；支持丰富的QoS特性，提供流量监管、[流量整形](http://baike.baidu.com/view/3344032.htm" \t "_blank)及多种队列调度策略。

Quidway SecPath 1000F[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)提供两个固定的10/100/1000M自适应GE口，支持光口和电口两种形式。提供一个MIM 扩展槽位，支持多功能接口模块[热插拔](http://baike.baidu.com/view/7091.htm" \t "_blank)，目前可选的接口模块有1FE/2FE/4FE/1GE/2GE/HDC六种。提供双电源[冗余备份](http://baike.baidu.com/view/3093981.htm" \t "_blank)解决方案（AC+AC，DC+DC两种机型），提供机箱内部环境温度检测功能，并支持[网管](http://baike.baidu.com/view/6076.htm" \t "_blank)，可满足电信级产品的高可靠性要求。

Array SPX5000

Array SPX5000是全球领先的应用智能安全设备供应商[Array Networks](http://baike.baidu.com/view/3495321.htm" \t "_blank)推出一款面向大型企业网络核心应用的产品设备：新一代SSL VPN远程安全接入产品。这款新品的推出，不仅标志着Array Networks产品性能的显著提升,更表明了Array Networks进一步巩固了在高端企业市场的领先地位。

Array SPX5000是面向大型企业和电信运营商核心业务/应用的新一代SSL VPN产品。它能保证企业客户在任何时间、任何地方，以任何接入设备，都可以通过Internet安全地访问企业的核心应用。由于其[并发用户数](http://baike.baidu.com/view/2280853.htm" \t "_blank)达到64000个，250个VLAN（虚拟[局域网](http://baike.baidu.com/view/788.htm" \t "_blank)）和128个虚拟门户；对于大型企业/电信网络来说，无论在安全保密、性能，还是在可扩展性方面，Array SPX5000的表现都非常优秀； Array SPX5000可向各大机构提供最强大的网络安全和Web应用优化功能，包括利用SSL VPN登录访问Web应用和传统应用、身份管理、[应用层防火墙](http://baike.baidu.com/view/3165517.htm" \t "_blank)，以及基于Web的流量管理等等。值得一提的是Array SPX5000的反应速度要比以往的SSL VPN快近2倍，并且能够保持近千兆的[线路速率](http://baike.baidu.com/view/190221.htm" \t "_blank)进行SSL通讯传输。达到如此高的传输指标，对于SSL VPN产品来说还是第一次，这就意味着取代大型企业中以往所应用的[IPSec VPN](http://baike.baidu.com/view/1207621.htm" \t "_blank)[网关](http://baike.baidu.com/view/807.htm" \t "_blank)的日子不远了。

Cylan SGA 600系列安全网关

CYLAN SGA 600系列安全网关适合于中大型规模的企业，它用于满足移动用户、分支机构、供应商、合作伙伴等对IT资源（如基于Web的应用、Unix应用、企业邮件系统、[文件服务器](http://baike.baidu.com/view/566090.htm" \t "_blank)、FTP服务器、[远程控制](http://baike.baidu.com/view/51293.htm" \t "_blank)、C/S应用系统等）的远程安全接入的需求。这样，企业就可以利用自身的网络平台，建立一个安全的VPN网络。所有远端用户的访问都是经过标准Web浏览器内置的加密套件进行加密并经过[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)端认证许可的，即经过授权用户只要能上网，就可以通过浏览器接入远程的[应用服务器](http://baike.baidu.com/view/995472.htm" \t "_blank)，建立安全SSL VPN隧道。CYLAN SGA利用浏览器来协助用户在任何地方任何时间安全的访问公司的任何资源。另外，Cylan SSL VPN产品还可以实现智能手机的接入（如iphone\ipad\android\windows mobile）。

iGate SSL VPN 4.0

与同类产品相比，iGate4.0是目前市场上惟一一款集成双因素[身份认证](http://baike.baidu.com/view/1014826.htm" \t "_blank)令牌的SSL VPN设备，iGate Pro集成应用了硬件SSL加速装置。新推出的iGate4.0与原有产品相比，提高了SSL接入能力，完全可以支持全网连接；简化了安装和管理，使原有Web用户界面变得更加简单易用；新增加了对PKI的支持能力和客户端策略检查功能，具备了更高级别的安全性。此外，iGate4.0还增加了对基于Web的PDA或其他移动设备的支持能力。这次重大升级，使iGate在产品性能、易用性等方面都有了长足进步，并一跃成为目前市场中最具实力的[SSL](http://baike.baidu.com/view/16147.htm" \t "_blank)[VPN](http://baike.baidu.com/view/19735.htm" \t "_blank)产品。

iGate SSL VPN 4.0是一款基于SSL的移动[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)设备，它通过[Internet](http://baike.baidu.com/view/11165.htm" \t "_blank)在[远程](http://baike.baidu.com/view/856599.htm" \t "_blank)访问双方建立安全通道，使移动用户可以轻松访问公司内部资源。适用于大型企业，政府部门 的采用。iGate可以通过多种方式确保信息的安全性，主要包括：

采用专用硬件对Web和非Web应用程序的通讯进行SSL加密。

采用硬件令牌和口令登录相结合的方式确保远程访问的合法性。

通过客户端完整性扫描确定远程访问环境的安全性，并相应调整对内部资源的访问权限。

会话结束后清除客户端[临时文件](http://baike.baidu.com/view/898304.htm" \t "_blank)，防止泄漏敏感数据。

集成现有用户数据库，按照角色集中管理和控制访问权限。

iGate作为惟一入口，有效隐藏内部信息，杜绝[网络攻击](http://baike.baidu.com/view/133739.htm" \t "_blank)。

丰富的[访问控制](http://baike.baidu.com/view/469056.htm" \t "_blank)和日志[管理工具](http://baike.baidu.com/view/1251417.htm" \t "_blank)；全面支持PKI认证、无线设备和PDA等。

Cisco VPN 3000系列集中器

VPN 3000系列集中器是[Cisco](http://baike.baidu.com/view/21537.htm" \t "_blank)公司发布的一款SSL VPN产品，由通用的[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)[虚拟专网](http://baike.baidu.com/view/241864.htm" \t "_blank)（VPN）平台和将高可用性、高性能和可扩展性与当今最先进的加密和认证技术结合在一起的客户机软件组成。利用Cisco VPN 3000集中器系列，客户可以充分发挥最新VPN技术的优势，极大地降低通信费用。特别是，该产品是业界唯一的能够提供现场可更换和客户可升级部件的可扩展平台。这些称为可扩展加密处理（SEP）模块的部件使用户可以轻松地增加容量和吞吐量。

Cisco客户可以在众多的VPN 3000[集中器](http://baike.baidu.com/view/1280045.htm" \t "_blank)中选择最适合自己需求和应用的具体型号，这些型号支持各种企业客户，包括从只有不到100个远程访问用户的小公司到有多达10000名同时[远程用户](http://baike.baidu.com/view/1541147.htm" \t "_blank)的大型机构。不论Cisco VPN 3000集中器的哪一种版本，都可以在不增加更多费用的情况下提供Cisco VPN客户机，并给予不受限制的安装许可证。Cisco VPN 3000集中器提供非[冗余](http://baike.baidu.com/view/104445.htm" \t "_blank)和冗余两种配置，允许客户构建最稳健、最可靠和经济高效的网络。另外，还提供高级[路由](http://baike.baidu.com/view/18655.htm" \t "_blank)功能，如OSPF、RIP和网络地址转换（NAT）。

UU200系列

UU200 iSTAR系列产品中的发布单元（Publisher），它位于[应用服务器](http://baike.baidu.com/view/995472.htm" \t "_blank)子网络中。由于UU200对应用程序是透明的，因此可以将应用服务器所提供的各种服务、文件、甚至于子网络安全的发布出来。通过SSL协议以及end to end加密技术，使用者可以安全的使用Publisher所发布的服务。UU200 iSTAR 系列产品主要特点：在[应用层](http://baike.baidu.com/view/239619.htm" \t "_blank)建立用户访问管理。对应用程序透明，能发布Web,[Client/Server](http://baike.baidu.com/view/83263.htm" \t "_blank)应用程序及文件共享。子网络虚拟接入（UURemote、UUSoft）为选项功能。UU200可以选择以Public IP进行连接配置，或是通过UUExchange/UUSwitch连接：此时的UU200可以使用Private IP进行连接配置。使用cluster技术，支持[负载均衡](http://baike.baidu.com/view/51184.htm" \t "_blank)。

UU200 iSTAR 系列产品适应有公共[静态IP地址](http://baike.baidu.com/view/3192408.htm" \t "_blank)和没有公共静态IP地址的企业，后者需要连到UUExchange/UUSwitch。适合大中型企业建立SSL VPN。

神獒VPN L（SSL）系列产品

神獒L（SSL）系列VPN产品是北京巨龙数码自主研发的SSL VPN系统，无需安装客户端软件，只需通过浏览器（Browser）便可安全的访问企业内部受控资源，建立安全快速高效的VPN隧道，更好的实现用户端的安全控制及节约整体项目成本。神獒L系列VPN是基于[数字证书](http://baike.baidu.com/view/16501.htm" \t "_blank)和SSL技术实现的独立[安全系统](http://baike.baidu.com/view/173312.htm" \t "_blank)，无需改变应用系统的网络结构和应用模式。

SSL VPN选购注意事项

[编辑](javascript:;)

选择哪种SSL VPN取决于终端用户需要访问的应用程序类型。基于浏览器的SSL VPN最适合访问网页应用程序或下载文件，同时也方便BYOD工作者从任意设备接入，包括智能机和平板电脑。瘦和胖客户端支持更广泛的用途但是没有那么好的兼容性，这使得它们更适用于平板电脑。出于灵活性和安全性的考虑，把SSL和IPsec VPN结合起来是一个不错的解决方法。拥有一个混合VPN，远程工作人员就可以使用各种不同设备接入，每个接入的终端用户都可以找到客户端所需的精确类型并连接到网络。[2]

SSL VPN由于其强大的功能和实施的方便性应用越来越广泛，市场上的SSL VPN品牌也越来越多，如何选择适合自己的产品是需要用户仔细考虑的一个问题，本文从下面几个方面描述如何选择SSL VPN产品：

SSL VPN应用需求

选择VPN是为了支持[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)内部网络的应用，因此这一点也是最先需要考虑的一点，目前，大多数SSL VPN支持我们日常经常会用到的[邮件系统](http://baike.baidu.com/view/1677840.htm" \t "_blank)、[OA系统](http://baike.baidu.com/view/615109.htm" \t "_blank)、CRM/ERP等等，但并不是所有的应用SSL VPN都能够提供支持，如动态端口的应用就只有部分SSL VPN能够提供支持。因此，在决定使用一款SSL VPN前一定要先确定是否能支持你的应用。

SSL VPN安全需求

要构建一个安全的系统，不仅仅需要传输过程安全，还要提高系统安全性，以下几个方面是缺一不可的：

1 传输过程安全

传输的过程加密强度是确保内部数据不在传输过程中被黑客盗取的关键因素。传输过程加密强度越高，传输安全性就越有保障。目前，拥有128位加密以上的SSL[VPN](http://baike.baidu.com/view/19735.htm" \t "_blank)产品是比较适宜的，56位DES加密相对强度低，选择时需要特别注意。

2 用户[身份验证](http://baike.baidu.com/view/121510.htm" \t "_blank)

用户名加密码的验证方式安全性相对较低，除了用户名和密码外，能提供其他的双因素验证方式的产品更加具有优势，如支持PKI体系等？

3 客户端设备的安全性：

客户端设备是否安装了个人[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)、[防病毒软件](http://baike.baidu.com/item/%E9%98%B2%E7%97%85%E6%AF%92%E8%BD%AF%E4%BB%B6" \t "_blank)等。如果客户端设备不够安全，比如有[木马程序](http://baike.baidu.com/view/206666.htm" \t "_blank)，那么系统依然存在安全隐患。目前部分SSL VPN能够提供客户端环境检测，比如检测客户端是否安装了防火墙和防病毒软件。

4 完成访问后，客户端需要清除客户端机器的缓存

在移动用户完成远程访问后，是否就万事大吉了呢？当然不是，黑客或不法分子可以通过拷贝、复制驻留在客户端缓冲区内数据盗取企业机密。

5[服务端](http://baike.baidu.com/view/1087294.htm" \t "_blank)的日志跟踪

SSL VPN[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)应该提供访问统计和跟踪功能，这样管理员能够根据日志随时掌握系统访问情况。

对于以上这些安全特性，SafeNet iGate SSL VPN均能够提供支持。

⒈SafeNet iGate 使用高强度的128位加密技术。

⒉对于远程移动用户，iGate能够结合PKI体系以及本地[活动目录](http://baike.baidu.com/view/97899.htm" \t "_blank)，值得一提的是，SafeNet独有的iKey双因素[身份认证](http://baike.baidu.com/view/1014826.htm" \t "_blank)USB Key与iGate SSL VPN完美结合，充分实现安全的双因素身份验证功能。

⒊SafeNet iGate支持客户端环境检测功能，SafeNet iGate能够设定访问策略，当客户端不符合某个条件时，系统将禁止用户登陆。

⒋为此，SafeNet iGate在用户离线后可自动清除用户[缓冲区](http://baike.baidu.com/view/266782.htm" \t "_blank)的内容。另外，在拔除iKey后，访问也会自动中断。

⒌SafeNet iGate在用户界面上集成了日期查询功能，能够非常方便的进行日志跟踪。

SSL VPN易于管理维护

SSL[VPN](http://baike.baidu.com/view/19735.htm" \t "_blank)的突出优势之一就在于移动性强、易用性强。但这些特性往往会增加管理难度。因此用户在选购SSL VPN时要重点考虑产品的管理性能。产品要做到界面简单，使用方便，灵活、细致地设置访问权限，采用基于用户/组/角色的认证机制，每个文件、网址或应用都可进行单独设置，使[访问控制](http://baike.baidu.com/view/469056.htm" \t "_blank)更易于管理。

SafeNet iGate 提供两个Web方式的管理UI，一个是Simple－UI，一个是Classic－UI，把常用的设置和不常用的设置分别开来，这样大大降低了管理维护的复杂性。

SSL VPN性能

由于是集中系统，SSL加速决定整个网络的吞吐量。如果SSL加速跟不上，[远程](http://baike.baidu.com/view/856599.htm" \t "_blank)接入就会比实际的Internet接入[带宽](http://baike.baidu.com/view/10821.htm" \t "_blank)低很多。有的SSL VPN产品采用专门的SSL加速硬件，从而提高了VPN的响应速度。另外，通过[数据压缩技术](http://baike.baidu.com/view/1320634.htm" \t "_blank)，还对所有的传输数据进行压缩后再进行传输，这样就提高了整个网络的运行效率和实用性。

SafeNet iGate配置硬件[SSL加速卡](http://baike.baidu.com/view/2527339.htm" \t "_blank)，能够大大提高访问速度，另外iGate 还提供[数据压缩](http://baike.baidu.com/view/286827.htm" \t "_blank)功能，能够大大增加[网络吞吐量](http://baike.baidu.com/view/34810.htm" \t "_blank)。

SSL VPN服务

除了上面提到的几点外，具有良好服务也至关重要。SSL VPN还是一个在不断发展的技术，更新的可能会比较快，提供SSL VPN的厂家是否具有良好的产品服务质量、渠道响应速度和本地支持能力也非常重要。比如承诺免费或低费用升级，等等。

SSL VPN结束语

SSL VPN的发展迎合了用户对低成本、高性价比远程访问的需求。现在，它已经广泛应用于各行各业。选购SSL VPN时，用户还要根据自身特点和不同的业务模式，选择适合自己的SSL [VPN](http://baike.baidu.com/view/19735.htm" \t "_blank)产品，再次强调，VPN是正在发展的技术，更新换代可能会比较快，因此用户在选购时可以少考虑一些扩展性，多注重产品的实用性。毕竟，只有适合自己的，才是最理想的选择。

SSL VPN技术现状

[编辑](javascript:;)

最近SSL VPN的市场突飞猛进，各种媒体上相关SSL VPN的文章也很多，但是目前存在很多的关于SSL VPN的误区，随便在网上搜索就可以看到很多错误的说法：

⒈ SSL VPN和IPSec VPN各有优缺点，SSL VPN只能适用于web应用；

⒉ XX国内厂商推出了廉价集IPSec VPN与SSL VPN于一体的设备，必将大大促进VPN的市场推广；

⒊ 经过使用Spirent[Avalanche](http://baike.baidu.com/view/6438607.htm" \t "_blank)测试，XX厂家的SSL VPN产品的TPS（每秒新建用户数）达到了1300， 最大在线用户数可以达到64’000个，完全可以适用大型的商业应用。

这就引入了几个问题：

⒈ 究竟SSL VPN有哪些功能?是否只能解决web应用?

⒉ 什么才是一个真正的SSL VPN产品?怎样区别市场上林林总总的号称的SSL VPN产品?

⒊ 如何衡量SSL VPN产品的性能?

下面逐个回答问题：

1 究竟SSL VPN有哪些功能?是否只能解决web应用?

SSL VPN的出现是为了解决IPSec VPN的固有缺点而出现的，SSL VPN继承了IPSec VPN的远程使用与内网使用体验一致、与应用无关的优点，避免了因有客户端而导致的使用维护不便、某些网络条件下无法接通、带来大量病毒和[蠕虫](http://baike.baidu.com/view/2596.htm" \t "_blank)的入侵、无法与企业现有认证[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)结合、无法审计等问题，从功能上有网络访问、网上应用程序、Windows文件共享、[移动电子邮件](http://baike.baidu.com/item/%E7%A7%BB%E5%8A%A8%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB%B6" \t "_blank)、应用程序访问、传统[主机](http://baike.baidu.com/view/23880.htm" \t "_blank)、终端服务器等众多功能，可以提供C/S应用和B/S应用访问，并非只能解决web应用。这其中最为重要的是网络访问功能，SSL VPN的网络访问功能避免了IPSec VPN的缺点而又继承了IPSec VPN的优点。

2 什么才是一个真正的SSL VPN产品?怎样区别市场上林林总总的号称的SSL VPN产品?

现在有很多厂商声称自己的产品是SSL VPN，或者说融合了IPSec VPN和SSL VPN的功能，实际上大部分的厂商只是实现了SSL VPN中的网上应用程序，也就是Web[反向代理](http://baike.baidu.com/view/1165595.htm" \t "_blank)的功能，某国内厂商大肆宣称的集IPSec VPN与SSL VPN于一体的设备也只是在原有的IPSec VPN的设备上加了一个Web反向代理的功能而已，根本不能称之为真正的SSL VPN产品。那么什么才是一个真正的SSL VPN产品?

前文说到SSL VPN从功能上说有网络访问、网上应用程序、Windows文件共享、移动电子邮件、应用程序访问、传统主机、[终端服务器](http://baike.baidu.com/view/1116910.htm" \t "_blank)等众多功能，其中网络访问是SSL VPN最为重要和标志性的功能，只有具备了网络访问这个看似IPSec VPN而又从根本上解决了IPSec VPN缺陷的功能才称得上是一款真正的SSL VPN产品。当然为了安全性考虑的终端安全检查和审计、与企业认证[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)的结合等功能也是一款优秀SSL VPN的必备功能。

vpnc中有通过该组织认证的SSL VPN厂商列表，也可以说，只有在这儿能够查到的SSL VPN厂商的产品，才是真正的SSL VPN产品。

3 如何衡量SSL VPN产品的性能?

谈到SSL VPN产品的性能，首先要区分的是SSL Server和SSL VPN，SSL Server相当于SSL VPN中的反向代理功能，二者的要求是不一样的，SSL Server面对的是业务系统，如电子商务网站、网上银行等等，它强调的是性能，目前国内可见的SSL Server产品性能可达20000TPS和4百万同时在线用户数；而SSL VPN面向的是远程接入即管理系统，它强调的是易于使用和管理、安全性等等，一个SSL VPN用户的登录包括SSL握手、认证、授权、记录日志等过程，其中认证、授权、记录日志所耗费的时间远远高于SSL握手，不可能达到SSL Server那样高的性能，如果需要非常高的性能，要使用多台SSL VPN堆叠来实现。

Spirent[Avalanche](http://baike.baidu.com/view/6438607.htm" \t "_blank)是一款优秀的基于Web应用的测试仪器，但只适用于测试SSL Server性能，不适用于测试SSL VPN的性能，某厂商的设备集合了SSL Server 和SSL VPN的功能，虽然SSL Server的性能在业界根本不入流，但显然会高于SSL VPN的性能。该厂商利用大家对于SSL Server和SSL VPN之间认识的混淆，到处宣称使用SpirentAvalanche测试证明自己的SSL VPN具有很高的性能，实际上从[测试过程](http://baike.baidu.com/view/651488.htm" \t "_blank)可以发现，测试的只是其中SSL Server的性能。

SSL VPN的[性能测试](http://baike.baidu.com/view/106187.htm" \t "_blank)，因为涉及建立VPN隧道，非常复杂，只能使用业界某些测试软件如LoadRunner 加上厂家自己的动态库来实现，只能在厂家自己的测试实验室来做，试图用某种测试仪器来统一测试所有厂家的SSL VPN性能是行不通的，所以只能参考各个厂家自己提供的性能，当然，要区分大的上市企业公布的真实的性能指标的和某些小企业不负责任的信口胡言。

SSL VPN发展前景

[编辑](javascript:;)

SSL VPN的出现，使得原来基于IP安全的IPSec VPN厂商不得不重新思考它们的产品方略。我们知道基于IP安全协议的IPSec VPN已经占领了很大一部分市场，成为VPN市场的主流。但是随着SSL VPN技术的出现，基于[IP协议](http://baike.baidu.com/view/2802.htm" \t "_blank)的IPSec VPN正经受着一场前所未有的考验。但是不是SSL VPN会取代现有的IPSec VPN成为主流呢？

虽然SSL VPN有许多相对IPSec VPN的优点，但这些对于主流应用VPN的客户--大、中型企业来说这些优点就显得不是很重要了。

据有关网络安全专家认为这就目前的SSL VPN技术来讲是不可能的。主要体现在目前的SSL VPN应用非常有限，仅适用于基于Web的应用。SSL的支持者认为，当企业工作人员需要[远程访问](http://baike.baidu.com/view/183974.htm" \t "_blank)Web应用如电子邮件或者接入企业内网的时（因为SSL可以绕过[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)和代理[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)）才应用，SSL只不过是一种更低廉而且更容易部署的选择而已。况且目前，传统的IPSec VPN厂商为了满足这部分用户的需求，正在匆忙地为其产品增加SSL性能，这样只能单独提供SSL性能的VPN产品就可能大受冷落了。

市场研究家们预计在今后几年中，SSL VPN设备的全球销售将会出现持续增长，但同时也表明IPSec VPN设备不会因SSL VPN设备的增长而受到大的影响，相反也会技术快速增长，因为整个VPN市场将在近几来得到极快的增长。Infonetics研究公司预测，SSL VPN市场将会从2002年的5600万美元增长到2005年的8.4亿美元。IPSec VPN设备也将从2002年的15亿美元增长到2005年的25亿美元。

随着基于Web的应用越来越多，以及远程接入需求的增长，SSL可能会成为一个热门市场，成为传统IPSec VPN设备厂商需要考虑的一个发展方向。Check Point公司就曾于去年7月发布过一款SSL VPN产品，它认为SSL对于需要通过Extranet与业务合作伙伴交换数据但又不想安装VPN客户端的企业来说非常理想。其他IPSec VPN厂商像北电网络和SonicWall都持此观点。北电网络于去年9月发布了Alteon SSL设备；SonicWall则在两年以前收购Phobos的时候就开始提供SSL产品了。

其他IPSec VPN支持者，如[赛门铁克](http://baike.baidu.com/view/326323.htm" \t "_blank)，正在计划如何将SSL安全技术集成进它的产品中。另外一些小厂商，如Aspelle、Air Gap、Aventail、Neoteris和Whale等通信公司都已经意识到SSL VPN市场需求增长。

有些企业客户认为需要同时拥有SSL和IPSec VPN。他们想为部分数量有限的员工提供IPSec VPN连接（如采用Cisco的VPN设备），因为他们需要访问企业的生产系统和其他非Web应用。但同时，也为大多数员工提供SSL VPN（如使用Whale的e-Gap远程接入产品）的[远程](http://baike.baidu.com/view/856599.htm" \t "_blank)接入，可供其接入Intranet和电子邮箱。

Whale公司的SSL产品只需运行在该企业[数据中心](http://baike.baidu.com/view/754520.htm" \t "_blank)的一台[服务器](http://baike.baidu.com/view/899.htm" \t "_blank)上。利用这种无客户端接入方式，企业就能够提供安全的连接，而不需要改写上万台最终用户设备上的程序。

如目前纽约的德勤咨询公司就在混合使用SSL和IPSec VPN。该公司的大多数员工都可以通过SSL VPN（Aventail产品）接入企业网络，少数员工则通过IPSec VPN（北电网络产品）接入，因为这些员工需要访问运行在该企业4个数据中心中的应用。德勤的CIO Larry Quinlan就很喜欢SSL VPN，因为它具有可穿越[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)而不必重新配置防火墙的性能。他说，“这很重要，因为安全部门不必着急去重新配置防火墙了。” Quinlan认为，SSL的缺陷在于只能访问Web应用。但IPSec也有其缺陷，因为它不容易穿越防火墙，所以当移动工作人员需要在旅店或分支办公地点接入企业网时就难以实现。

因为SSL只能用于Web应用，让一些用户有所退避。[芝加哥](http://baike.baidu.com/view/36045.htm" \t "_blank)的一家个人服务公司Divine就主要采用了NetScreen公司的IPSec VPN，因为它的很多[远程工作](http://baike.baidu.com/view/2502095.htm" \t "_blank)人员都是咨询师，需要访问企业众多的应用程序，不可能只限定在Web应用上。Divine的网络服务部经理Chuck Horvat说，他们还没有发现需要使用SSL VPN的理由。不过，该公司也有一个Web应用前端和内置的SSL加密。远程工作人员通过[身份认证](http://baike.baidu.com/view/1014826.htm" \t "_blank)和口令可获得访问公司邮箱和目录的权限。

Horvat说，“对我们来说，拥有[IPSec VPN](http://baike.baidu.com/view/1207621.htm" \t "_blank)管道是最好的，因为我们的人有很多应用需要访问。他们可以通过SSL获得电子邮件，但大多数人需要的应用都不是电子邮件。虽然有另外一种选择是很不错，但每个人的需求是非常不同的。”

所以，虽然目前有很多人都认为SSL VPN将会取代IPSec VPN，但大多数工业观察家却认为这两种VPN将会共存，因为两者的市场空间都不小，而且可以相互补充。

从以上的分析我们可以看到SSL VPN在未来几年中的发展前景，但是更多的专家们认为，目前处于竞争的IPSec VPN与SSL VPN将很快走向结合。因为它们都有各自的优点，而且各自的缺点又不是能通过自身的技术可以克服的。

SSL VPNVPN技术

[编辑](javascript:;)

Array Networks SSL

Array Networks SSL VPN可以为任何规模的企业组织提供强大而且高性能的安全访问接入。SPX系列产品使用存在于所有的Web浏览器上的SSL安全协议，无需安装任何客户端软件，无论在任何地方，无论使用哪种接入终端。

SSL VPN使用说明

[编辑](javascript:;)

SSL VPN使用说明（IE6）

点击IE，选择“工具”，“Internet选项”，选“安全”

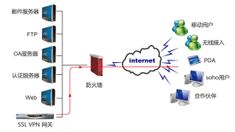
点击“受信任的站点”，再点击“站点”

选择“查看证书”

选择“安装证书”，选“下一步”两次，再按“完成”

选择“是”，退回安全警报，选“是”，配置完成。输入用户和密码登录即可。登录帐号是使用人姓名首字母+“."+单位名称首字母，初始密码是上报用户办公室电话号码。[1]

词条图册 [更多图册](http://baike.baidu.com/pic/SSL%20VPN/198325?fr=lemma" \t "_blank)

[[](http://baike.baidu.com/pic/SSL%20VPN/198325/0/3b292df5e0fe9925578af7e037a85edf8cb171f8?fr=lemma)](http://baike.baidu.com/pic/SSL%20VPN/198325/0/3b292df5e0fe9925578af7e037a85edf8cb171f8?fr=lemma" \o "" \t "_blank)

[词条图片(12)](http://baike.baidu.com/pic/SSL%20VPN/198325/0/3b292df5e0fe9925578af7e037a85edf8cb171f8?fr=lemma" \o "" \t "_blank)

参考资料

1.  [SSL VPN使用说明](http://baike.baidu.com/redirect/218cmWzubCnXXJqrvUbm6Ua494a77dlZnju_jPR6Hyr-b-JiU9nEQFVGUhMoP1oUlSiLG9DTMiyPK3qzuncH8FTnvJ6Y" \t "_blank) ．.[引用日期2015-02-27]

2.  [BYOD安全：SSL VPN](http://baike.baidu.com/redirect/8a001TdscMAxZZmhNsMFXnyGZev73vnK7nUEvnMUVKFnMwcr5MuLzM7O9Q04OlwIpFcTtxq6zd8j16OMQkoSrqn9xMHkaFPupwG1k0mszQdC9y4" \t "_blank) ．TechTarget网络[引用日期2015-09-23]

**心脏出血**（英语：Heartbleed）

# Heartbleed

[编辑](https://baike.baidu.com/item/Heartbleed/javascript:;)

本词条由[“科普中国”百科科学词条编写与应用工作项目](https://baike.baidu.com/science" \t "https://baike.baidu.com/item/Heartbleed/_blank) 审核 。

**心脏出血**（英语：Heartbleed），也简称为**心血漏洞**，是一个出现在[加密](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86" \t "https://baike.baidu.com/item/Heartbleed/_blank)程序库[OpenSSL](https://baike.baidu.com/item/OpenSSL" \t "https://baike.baidu.com/item/Heartbleed/_blank)的[安全漏洞](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E6%BC%8F%E6%B4%9E" \t "https://baike.baidu.com/item/Heartbleed/_blank)，该程序库广泛用于实现互联网的[传输层安全](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%B1%82%E5%AE%89%E5%85%A8" \t "https://baike.baidu.com/item/Heartbleed/_blank)（TLS）协议。它于2012年被引入了软件中，2014年4月首次向公众披露。只要使用的是存在缺陷的OpenSSL实例，无论是服务器还是客户端，都可能因此而受到攻击。此问题的原因是在实现TLS的[心跳](https://baike.baidu.com/item/%E5%BF%83%E8%B7%B3" \t "https://baike.baidu.com/item/Heartbleed/_blank)扩展时没有对输入进行适当验证（缺少[边界检查](https://baike.baidu.com/item/%E8%BE%B9%E7%95%8C%E6%A3%80%E6%9F%A5" \t "https://baike.baidu.com/item/Heartbleed/_blank)），因此漏洞的名称来源于“心跳”（heartbeat）。该程序错误属于[缓冲区过读](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA%E8%BF%87%E8%AF%BB" \t "https://baike.baidu.com/item/Heartbleed/_blank)，即可以读取的数据比应该允许读取的还多。

**中文名**

心脏出血

**外文名**

Heartbleed

**类    型**

紧急安全警告

**来    自**

[OpenSSL](https://baike.baidu.com/item/OpenSSL" \t "https://baike.baidu.com/item/Heartbleed/_blank)

**又    名**

heartbleed bug

## 目录

1. 1 [漏洞描述](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "1)
2. 2 [发现历程](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "2)
3. 3 [技术原理](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "3)
4. ▪ [获取密码](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "3_1)
5. ▪ [入侵技术](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "3_2)
6. ▪ [检测工具](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "3_3)
7. 4 [影响危害](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "4)
8. ▪ [漏洞影响](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "4_1)
9. ▪ [漏洞危害](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "4_2)
10. ▪ [涉及中国](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "4_3)
11. 5 [操作建议](https://baike.baidu.com/item/Heartbleed/13580882?fr=aladdin" \l "5)

## 漏洞描述

[编辑](https://baike.baidu.com/item/Heartbleed/javascript:;)

Heartbleed漏洞，这项严重缺陷(CVE-2014-0160)的产生是由于未能在memcpy()调用受害用户输入内容作为长度参数之前正确进行边界检查。攻击者可以追踪OpenSSL所分配的64KB[缓存](https://baike.baidu.com/item/%E7%BC%93%E5%AD%98" \t "https://baike.baidu.com/item/Heartbleed/_blank)、将超出必要范围的[字节](https://baike.baidu.com/item/%E5%AD%97%E8%8A%82" \t "https://baike.baidu.com/item/Heartbleed/_blank)信息复制到缓存当中再返回缓存内容，这样一来受害者的内存内容就会以每次64[KB](https://baike.baidu.com/item/KB/331" \t "https://baike.baidu.com/item/Heartbleed/_blank)的速度进行泄露。 [1]

## 发现历程

[编辑](https://baike.baidu.com/item/Heartbleed/javascript:;)

Heartbleed漏洞是由安全公司Codenomicon和[谷歌](https://baike.baidu.com/item/%E8%B0%B7%E6%AD%8C" \t "https://baike.baidu.com/item/Heartbleed/_blank)安全工程师发现的，并提交给相关管理机构，随后官方很快发布了漏洞的修复方案。2014年4月7号，程序员Sean Cassidy则在自己的博客上详细描述了这个漏洞的机制。

## 技术原理

[编辑](https://baike.baidu.com/item/Heartbleed/javascript:;)

### 获取密码

2014年4月9日，Heartbleed（意为“心脏出血”）的重大[安全漏洞](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E6%BC%8F%E6%B4%9E" \t "https://baike.baidu.com/item/Heartbleed/_blank)被曝光，一位安全行业人士在[知乎](https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E" \t "https://baike.baidu.com/item/Heartbleed/_blank)上透露，他在某著名电商网站上用这个漏洞尝试读取数据，在读取200次后，获得了40多个用户名、7个密码，用这些密码，他成功地登录了该网站。 [2]

### 入侵技术

[SSL](https://baike.baidu.com/item/SSL" \t "https://baike.baidu.com/item/Heartbleed/_blank)（[安全套接层](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E5%A5%97%E6%8E%A5%E5%B1%82" \t "https://baike.baidu.com/item/Heartbleed/_blank)）协议是使用最为普遍网站加密技术，而[OpenSSL](https://baike.baidu.com/item/OpenSSL" \t "https://baike.baidu.com/item/Heartbleed/_blank)则是开源的 SSL 套件，为全球成千上万的web服务器所使用。Web服务器正是通过它来将密钥发送给访客然后在双方的连接之间对信息进行加密。URL中使用 https打头的连接都采用了SSL加密技术。在线购物、网银等活动均采用SSL技术来防止窃密及避免中间人攻击。

Heartbleed漏洞之所以得名，是因为用于安全传输层协议（TLS）及数据包传输层安全协议（[DTLS](https://baike.baidu.com/item/DTLS" \t "https://baike.baidu.com/item/Heartbleed/_blank)）的 Heartbeat扩展存在漏洞。Heartbeat扩展为TLS/DTLS提供了一种新的简便的连接保持方式，但由于OpenSSL 1.0.2-beta与OpenSSL 1.0.1在处理TLS heartbeat扩展时的边界错误，攻击者可以利用漏洞披露连接的客户端或服务器的存储器内容，导致攻击者不仅可以读取其中机密的加密数据，还能盗走用于加密的密钥。

### 检测工具

史上最严重的资安漏洞OpenSSL的Heartbleed漏洞，攻击全球三分之二的网站，如何自保。

所幸网络上出现多种Heartbleed漏洞检测服务，可以让民众检查正在此用的网路服务是否安全，若是不安全的网站，就避免使用任何与帐号、密码有关的交易功能。

网络服务提供者也应该利用这些工具，即刻检查自己维护的伺服器，避免因Heartbleed漏洞而受到攻击，导致用户资料被窃。

**Heartbleed test**

意大利资安专家Filippo Valsorda (@FiloSottile)率先开发出来的Heartbleed检测工具，以模拟OpenSSL Heartbleed漏洞的入侵方法，开发出来的检测工具。只要输入网站的网址，便可以测试网站是否受Heartbleed漏洞影响。例如输入妈妈经网站，就发现妈妈经失血了。

**ossible.lv Heartbleed test**

由资安公司Possible.lv开发的Heartbleed检测工具，只要输入网址就可以测试网站是否受Heartbleed漏洞影响。

**LastPass Heartbleed Checker**

由密码管理工具厂商LastPass开发的检测工具，只要输入网址便可以测试网站是否受Heartbleed漏洞影响。

**Qualys SSL Labs Server Test**

由Qualys SSL LABS提供的SSL测试，不仅可以测试[伺服器](https://baike.baidu.com/item/%E4%BC%BA%E6%9C%8D%E5%99%A8" \t "https://baike.baidu.com/item/Heartbleed/_blank)是否受Heartbleed漏洞影响，还可以为伺服器的加密安全性评等。

**Chrombleed**

Heartbleed来袭，但上网不用怕，Chromebleed是Google Chrome浏览器的扩充功能，只要安装之后，在每一次浏览网页时，便会主动弹跳出网页是否受Heartbleed漏洞影响的讯息。

## 影响危害

[编辑](https://baike.baidu.com/item/Heartbleed/javascript:;)

### 漏洞影响

通过读取网络服务器内存，攻击者可以访问敏感数据，从而危及服务器及用户的安全。敏感的安全数据，如服务器的专用主密钥，可使攻击者在服务器和客户端未使用[完全正向保密](https://baike.baidu.com/item/%E5%AE%8C%E5%85%A8%E6%AD%A3%E5%90%91%E4%BF%9D%E5%AF%86" \t "https://baike.baidu.com/item/Heartbleed/_blank)时，通过被动[中间人攻击](https://baike.baidu.com/item/%E4%B8%AD%E9%97%B4%E4%BA%BA%E6%94%BB%E5%87%BB" \t "https://baike.baidu.com/item/Heartbleed/_blank)解密当前的或已存储的传输数据，或在通信方使用完全正向保密的情况下，发动主动中间人攻击。攻击者无法控制服务器返回的数据，因为服务器会响应随机的内存块。

漏洞还可能暴露其他用户的敏感请求和响应，包括用户任何形式的[POST](https://baike.baidu.com/item/POST" \t "https://baike.baidu.com/item/Heartbleed/_blank)请求数据，会话[cookie](https://baike.baidu.com/item/cookie" \t "https://baike.baidu.com/item/Heartbleed/_blank)和密码，这能使攻击者可以[劫持](https://baike.baidu.com/item/%E5%8A%AB%E6%8C%81" \t "https://baike.baidu.com/item/Heartbleed/_blank)其他用户的服务身份。在其披露时，约有17%或五十万通过认证机构认证的互联网安全[网络服务器](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "https://baike.baidu.com/item/Heartbleed/_blank)被认为容易受到攻击。[电子前哨基金会](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E5%89%8D%E5%93%A8%E5%9F%BA%E9%87%91%E4%BC%9A" \t "https://baike.baidu.com/item/Heartbleed/_blank)，[Ars Technica](https://baike.baidu.com/item/Ars Technica" \t "https://baike.baidu.com/item/Heartbleed/_blank)，和[布鲁斯·施奈尔](https://baike.baidu.com/item/%E5%B8%83%E9%B2%81%E6%96%AF%C2%B7%E6%96%BD%E5%A5%88%E5%B0%94" \t "https://baike.baidu.com/item/Heartbleed/_blank)都认为心脏出血漏洞是“灾难性的”。

漏洞让特定版本的openSSL成为无需钥匙即可开启的“废锁”，入侵者每次可以翻检户主的64K信息，只要有足够的耐心和时间，就可以翻检足够多的数据，拼凑出户主的银行密码、私信等敏感数据。对此安全专家提醒，网友在网站完成修复升级后，仍需及时修改原来的密码。

在公告发布之日，Tor项目在其博客发布公告，并表示任何在互联网上寻求“强健的匿名或隐私”的人应该“在事情解决之前，接下来的几天里完全远离互联网“。他们还建议，Tor中继运行者和隐蔽服务运行者在修补OpenSSL后，应撤销及生成新密钥，但也指出，Tor中继使用两套密钥和多跳设计最大限度地减少了窃取单一中继的影响。

加拿大税务局（CRA）因心脏出血安全漏洞，关闭了电子服务网站。

平台维护者，如维基媒体基金会，建议他们的用户更改密码。

[GitHub](https://baike.baidu.com/item/GitHub" \t "https://baike.baidu.com/item/Heartbleed/_blank)上的一个统计数据分析了2014年4月8日前1000个访问量最大的网站，发现受影响的网站包括[Yahoo](https://baike.baidu.com/item/Yahoo" \t "https://baike.baidu.com/item/Heartbleed/_blank)、[Imgur](https://baike.baidu.com/item/Imgur" \t "https://baike.baidu.com/item/Heartbleed/_blank)、Stack Overflow、[Slate](https://baike.baidu.com/item/Slate" \t "https://baike.baidu.com/item/Heartbleed/_blank)和[DuckDuckGo](https://baike.baidu.com/item/DuckDuckGo" \t "https://baike.baidu.com/item/Heartbleed/_blank)。安全的网站包括[Google](https://baike.baidu.com/item/Google" \t "https://baike.baidu.com/item/Heartbleed/_blank)、[Facebook](https://baike.baidu.com/item/Facebook" \t "https://baike.baidu.com/item/Heartbleed/_blank)、[Wikipedia](https://baike.baidu.com/item/Wikipedia" \t "https://baike.baidu.com/item/Heartbleed/_blank)、[Twitter](https://baike.baidu.com/item/Twitter" \t "https://baike.baidu.com/item/Heartbleed/_blank)及[Amazon](https://baike.baidu.com/item/Amazon" \t "https://baike.baidu.com/item/Heartbleed/_blank)。

**受影响的OpenSSL版本：**

最后更新于2014年4月9日，据Heartbleed和OpenSSL网站上的信息。

**受影响：**

OpenSSL 1.0.2-beta

OpenSSL 1.0.1 - OpenSSL 1.0.1f

除非针对CVE-2014-0160的操作系统补丁已经安装，而没有更改库版本，如[Debian](https://baike.baidu.com/item/Debian" \t "https://baike.baidu.com/item/Heartbleed/_blank)、[Red Hat Enterprise Linux](https://baike.baidu.com/item/Red Hat Enterprise Linux" \t "https://baike.baidu.com/item/Heartbleed/_blank)（及其派生版，如[CentOS](https://baike.baidu.com/item/CentOS" \t "https://baike.baidu.com/item/Heartbleed/_blank)、Amazon Linux）或[Ubuntu](https://baike.baidu.com/item/Ubuntu" \t "https://baike.baidu.com/item/Heartbleed/_blank)（及其派生版，如[Linux Mint](https://baike.baidu.com/item/Linux Mint" \t "https://baike.baidu.com/item/Heartbleed/_blank)）。

**不受影响：**

OpenSSL 1.0.2-beta2（将来版本）

OpenSSL 1.0.1g

OpenSSL 1.0.0（及1.0.0的分支版本）

OpenSSL 0.9.8（及0.9.8的分支版本）

要解决此漏洞，建议服务器管理员或使用1.0.1g版，或使用-DOPENSSL\_NO\_HEARTBEATS选项重新编译OpenSSL，从而禁用易受攻击的功能，直至可以更新服务器软件。

**Metasploit最新版本：**

针对CVE-2014-0160的测试和攻击脚本([Python](https://baike.baidu.com/item/Python" \t "https://baike.baidu.com/item/Heartbleed/_blank)/[Perl](https://baike.baidu.com/item/Perl" \t "https://baike.baidu.com/item/Heartbleed/_blank))已广泛传播。著名渗透测试框架[Metasploit](https://baike.baidu.com/item/Metasploit" \t "https://baike.baidu.com/item/Heartbleed/_blank)在最新版本中添加了对CVE-2014-0160的嗅探支持。

### 漏洞危害

Heartbleed能让攻击者从[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "https://baike.baidu.com/item/Heartbleed/_blank)内存中读取包括用户名、密码和信用卡号等隐私信息在内的数据，已经波及大量互联网公司。

受影响的服务器数量可能多达几十万。其中已被确认受影响的网站包括 Imgur、OKCupid、Eventbrite 以及 FBI 网站等，不过 Google 未受影响。

Github2014年4月9日发布了一个受影响网站的列表，在这个列表上发现了诸多知名互联网企业，例如雅虎、Stackoverflow.com、Outbrain.com、OKCupid.com、Steamcommunity.com、 Slate.com和 Entrepreneur.com等。其中很多网站都表示他们已经解决了这个问题。

OpenSSL“心脏出血”漏洞的严重性远比想象的严重，一些用户没有考虑到手机上大量应用也需要账号登陆，其登陆服务也有很多是OpenSSL搭建的，因此用户在这阶段用手机登陆过网银或进行过网购，则需要在漏洞得到修补后，更改自己的密码。

**更改密码：**

下面的网站已经发布公告，因受漏洞影响，建议用户更改密码：

Akamai Technologies。

Amazon Web Services。

[Ars Technica](https://baike.baidu.com/item/Ars Technica" \t "https://baike.baidu.com/item/Heartbleed/_blank)。

[GitHub](https://baike.baidu.com/item/GitHub" \t "https://baike.baidu.com/item/Heartbleed/_blank)。

[LastPass](https://baike.baidu.com/item/LastPass" \t "https://baike.baidu.com/item/Heartbleed/_blank)- LastPass自身并没有被影响，但建议用户修改所有储存在LastPass的受影响网站账户的密码，特别是有GitHub、OkCupid或[雅虎](https://baike.baidu.com/item/%E9%9B%85%E8%99%8E" \t "https://baike.baidu.com/item/Heartbleed/_blank)帐户的“每个人”。 LastPass提供了一个页面，公众可以检查网站是否受影响。2014年4月9日，LastPass开始向用户报告已知受心脏出血影响的存储了密码的网站。

[Mojang](https://baike.baidu.com/item/Mojang" \t "https://baike.baidu.com/item/Heartbleed/_blank)。

PeerJ。

SoundCloud。

SparkFun。

Stripe (公司)。

[Tumblr](https://baike.baidu.com/item/Tumblr" \t "https://baike.baidu.com/item/Heartbleed/_blank)。

Wikimedia。

[Wunderlist](https://baike.baidu.com/item/Wunderlist" \t "https://baike.baidu.com/item/Heartbleed/_blank)。

**受影响的软件**

[IPCop](https://baike.baidu.com/item/IPCop" \t "https://baike.baidu.com/item/Heartbleed/_blank) 2.1.4发布于2014年4月8日，修复了“每个人都在谈论的OpenSSL库”。

[LibreOffice](https://baike.baidu.com/item/LibreOffice" \t "https://baike.baidu.com/item/Heartbleed/_blank) 4.2.3发布于2014年4月10日，修复了CVE-2014-0160

LogMeIn声称“更新了我们依赖于OpenSSL的许多产品及部分服务”。

### 涉及中国

ZoomEye系统的扫描：根据该系统扫描，中国全境有1601250台机器使用443端口，其中有33303个受本次OpenSSL漏洞影响。443端口仅仅是OpenSSL的一个常用端口，用以进行加密网页访问；其他还有邮件、即时通讯等服务所使用的端口，因时间关系，尚未来得及扫描。

ZoomEye是一套安全分析系统，其工作原理类似Google Spider，会持续抓取全球互联网中的各种服务器，并记录服务器的硬件配置、软件环境等各类指标，生成指纹，定期对比，以此确定该服务器是否存在漏洞或被入侵。在此次“心脏出血”漏洞检测中，给该系统后面加上一个“体检”系统，过滤出使用问题OpenSSL的服务器，即可得出存在安全隐患的服务器规模。

从该系统“体检”结果看，比三万台问题服务器更令人惊心的，是这些服务器的分布：它们有的在银行网银系统中，有的被部署在第三方支付里，有的在大型电商网站，还有的在邮箱、即时通讯系统中。

自这个漏洞被爆出后，全球的黑客与安全专家们展开了竞赛。前者在不停地试探各类服务器，试图从漏洞中抓取到尽量多的用户敏感数据；后者则在争分夺秒地升级系统、弥补漏洞，实在来不及实施的则暂时关闭某些服务。这是最危险的地方：黑客们已经纷纷出动，一些公司的负责人却还在睡觉。而如果黑客入侵了服务器，受损的远不止公司一个个体，还包括存放于公司数据库的大量用户敏感资料。更为麻烦的是，这个漏洞实际上出现于2012年，谁也不知道是否已经有黑客利用漏洞获取了用户资料；而且由于该漏洞即使被入侵也不会在服务器日志中留下痕迹，所以还没有办法确认哪些服务器被入侵，也就没法定位损失、确认泄漏信息，从而通知用户进行补救。

## 操作建议

[编辑](https://baike.baidu.com/item/Heartbleed/javascript:;)

1. 不要在受影响的网站上登录帐号——除非确信该公司已经修补了这一漏洞。如果该公司没有通告相关进展，可以询问他们的客服团队。

一些网站（包括雅虎和OKCupid）受了影响但表示他们已经解决了全部或部分问题，如果不放心，可以在Filippo网站上查看各个网站安全与否，如果被标为红色就暂时不要登录。

很多人的第一反应是赶快修改密码，但是网络安全专家的建议是等到网站确认修复再说。

2. 一收到网站的安全修补确认，就立即修改银行、电子邮件等敏感帐号的密码。即便你采用了两步认证（即在密码之外多一重验证信息），推荐修改密码。

3. 不要不好意思联系掌握个人的数据的小企业以确保个人信息安全。雅虎和Imgur等知名公司当然知道这个问题，但是一些小企业可能还没发现它，所以个人要积极主动地维护个人信息安全。

4. 密切关注未来数日内的财务报告。因为攻击者可以获取服务器内存中的信用卡信息，所以要关注银行报告中的陌生扣款。

但是，即便按照上述方法操作，网页浏览活动也依然存在一定风险。Heartbleed甚至能影响追踪网站用户活动的浏览器[Cookie](https://baike.baidu.com/item/Cookie/1119" \t "https://baike.baidu.com/item/Heartbleed/_blank)，所以只访问不登录也有风险。

参考资料

* 1.Carvalho M, DeMott J, Ford R, et al. Heartbleed 101[J]. IEEE security & privacy, 2014, 12(4): 63-67.
* 2.Wheeler D A. Preventing Heartbleed[J]. IEEE Computer, 2014, 47(8): 80-83.