赛蓝 SGA 技术白皮书

深圳市赛蓝科技有限公司

Shenzhen Cylan Technology Co., Ltd

2009年2月

目录

序言

当前大多数远程访问解决方案是利用基于 IPSec 安全协议的 VPN 网络的情况下，一种最新的研究表明近乎 90%的企业利用 VPN 进行的内部网和外部网的联接都只是用来进行因特网访问和电子邮件通信，另外 10%的用户是利用聊天协议和其它私有客户端应用，属非因特网应用。而这些 90%的应用都可以利用一种更加简单的 VPN 技术--SGA 来提供更加有效的解决方案。基于 SSL 协议的 VPN 远程访问方案的更加容易配置和管理，网络配置成本比起目前主流的 IPSec VPN 还要低许多，所以许多企业已经开始转而利用基于 SSL 加密协议的远程访问技术来实现 VPN 通信了。

VPN技术可以扩展企业的内部网络，使在外工作的员工和合作伙伴通过标准、公用的因特网访问他们的内部网络。它相对传统的专线网络方案的主要优势是各项费用将大大降低。专线网络需要在合作伙伴或者远程员工与公司总部之间有一个物理封闭的网络连接，或者采用远程拨号访问方案，或者采用T1之类的数字专线连接。VPN是一个非常实用的技术，它允许客户（包括员工）和合作伙伴利用标准的因特网进行廉价连接，它允许采用IPSec安全协议方案。事实上，在VPN技术中包括许多加密和安全协议，SSL就是其中一个，同样主流VPN应用的IPSec也是其中的一种。所以总的来说IPSec VPN与SGA是VPN技术在两种不同的安全协议下实现VPN通信的两种平等方案。所以理解SGA的关键就在于理解SSL这一安全协议。

SSL的英文全称是“Secure Sockets Layer”，中文名为“安全套接层协议层”，它是网景（Netscape）公司提出的基于WEB应用的安全协议。SSL协议指定了一种在应用程序协议（如Http、Telenet、NMTP和FTP等）和TCP/IP协议之间提供数据安全性分层的机制，它为TCP/IP连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。

对于电子商务应用来说，使用SSL可保证信息的真实性、完整性和保密性。SSL数据的私

密性：在传输过程中可以使数据保持隐藏，不被非法查看；SSL的真实性和完整性：因为在有关数字加密、安全协议有关的技术可以确保数据在传输过程中不被修改或者损坏； SSL连接的可靠性：数据加密的另一个数学特征是可以证明事件的发生。在使用SSL协议的通信中，每一个应用是一个安全的独立体，而不像IPSec那样，操作与应用脱节。要使用SSL协议进行VPN通信，则所进行的远程通信应用必须能识别SSL技术，不过现在常见的应用一般都能识别SSL技术的，如IE、Netscape浏览器，OutLook、 Eudora 邮件应用等。

目前SGA主要应用于采用VPN与远程网络进行通信的应用主要是基于Web的客户，这些Web应用目前主要是内部网页游览、电子邮件及其它基于Web的查询工作。

一、CYLAN SGA 产品简介

CYLAN SGA安全网关系列产品是以国际标准SSL协议为基础的，自主研发的，专为企业定制的基于应用层设计的远程接入产品,CYLAN SGA为企业远程接入提供了最好的解决方案，它使传统的VPN 解决方案得到了升华，能让用户无论在世界的任何地方，只要使用浏览器就能够访问到公司总部的资源，如WINDOWS、LIUIX、UNIX等系统的商业文件和应用程序，而不需要安装任何客户端软件，CYLAN SGA可以集中管理企业内部的应用布置，配置细粒度的访问策略，可以更安全地实现权限权限控制，可以让不同级别的用户使用不同的应用。

CYLAN SGA的C/S转B/S功能，让用户能够远程安全使用企业的ERP系统，而无需安全客户端软件，WEB代理技术可以让用户访问企业内部的OA，网站或邮件系统，SSO功能让用户能够安全而方便地使用企业内部资源，从而实现了统一应用，统一管理， CYLAN 加密的SSL协议可以保护通过因特网的讯息、交易、和电子商务的安全，SSL防止直接的网络连接，与IPSec VPN不同，CYLAN SGA 的基于代理主机的SGA通过终止网络边缘的连接而提供一个附加的安全层。这就意味着只有经过授权的用户才被获准接入，而非法远程用户绝不会直接连接

到你的网络。这降低了恶意的或意外的病毒攻击。CYLAN SGA产品，对访问者进行了强制的安全检查，也可以在其使用特殊的安全应用时隔离其和外部网络的联系，从而保护应用的高安全性。

CYLAN SGA严格制度管理控制技术能够使你明确而容易地定义资源安全的发布，细粒度控制接入可以到用户级、资源级-甚至下到URL和文件级的权限。全范围身份认证方法的支持：Cylan SGA支持广泛范围的鉴别系统，包括用户名/密码、数字认证、LDAP、RADIUS、RSA SecurID 标记和其它通用的双因素等认证系统。CYLAN SGA提供了额外的安全性功能特性，以适应各种接入的设备。例如，若从公共网吧改进安全性，SSL提供一个“话路终止”功能部件。能够使用户阻挡认证形式的AutoCompletion，所以，用户不会粗心地将密码信息留在一个网吧。CYLAN SGA产品让用户轻松而安全地实现远程访问，让公司的网络应用布署更灵活，同时，CYLAN SGA还可以为企业最大化地节约成本，而且，CYLAN SGA 会为企业用户提供最好的整体解决。

CYLAN SGA通过結合SSL和代理技术來减少风险终端控制技术检测、保护使用者环境，从而授权使用者的访问级别，策略执行不仅基于使用者名称，还能检测使用者环境的信任级别，可以针对那些需要特殊环境的使用者，提供最好的解决方案。

CYLAN SGA 提供了用户自己定义界面的功能 ，用户可以根据自己的个性，定制入口界面，用户还可以把登录的 LOGO 换成自己公司的，并且，可以让不同的用户定制属于自己的界面，让用户真正体验 CYLAN 产品的感受。

二、 CYLAN SGA 功能介绍

2．1 SSL 应用发布

CYLAN SGA提供了很强的WEB代理功能，CYLAN SGA所支持的浏览器类型包含Html，Dhtml, Jsp, Asp,Java applet, Active, Cookies等各种Web技术。 可以让远程用户安全地使用内部的WEB资源，具体如下：

2．1．1 B/S 软件的应用

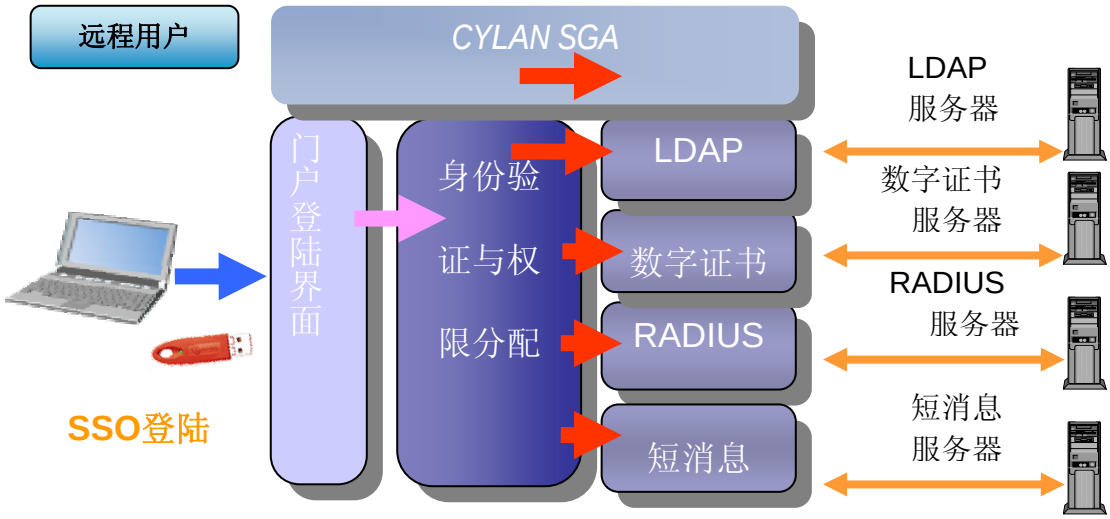
通过 CYLAN SGA 可以发布企业内部 B/S 软件系统，如 OA，B/S 架构的应用软件，最初的 B/S 应用，是通过前端的路由器或防火墙转发应用端口来实现的，但安全性和可靠性没有保障，而且数据在公网上传输是没有加密的，通过 CYLAN SGA 就可以轻松解决这个问题。

2．1．2 企业站点的应用

企业内部有很多站点应用，如大集团公司内部有很多网站，上面有很多内部新闻，信息公告等，这个网站是不能公开发布的，必须是企业内部的人员才可以访问，另外，远程的员工和出差员工也可能要看这些信息，这就要有一个安全的访问方式，CYLAN SGA 的 WEB 应用可以为企业用户解决这个问题，首先，在 CYLAN SGA 上发布站点资源，包括外部的站点（网站在外部或托管的），然后，给用户作个认证方式，这样，企业用户就可以安全地使用内部站点的资源了。

2．1．3　单点登录功能（SSO）

CYLAN SGA 产品，给应用系统复杂且多的企业，提供了一个全新的基于应用的安全管理方式，他可以结合企业目录服务,对一个内部网络用户进行集中式应用的权限分发和管理(即统一的身份认证和访问控制)，通过内置的 SSO（Single sign on）单点登陆,将不同应用的不同身份认证方式,不同的访问权限,进行一个有效的整合,方便了用户的使用,简化了多次的登陆过程和网络管理员在权限管理上的复杂性.



CYLAN 将门户 WEB 和权限控制、身份认证、SSO 进行了统一的整合，只要经过一次身份合法确认后，权限内的其他应用就不用再次输入密码了，有效地解决了企业应用系统多时输入过多密码的不便。

2．1．4　C/S 应用发布

CYLAN SGA 对 C/S 架构的应用，提供了一个更好的解决方案，就是能让用户在游览器里就能够使用自己的 C/S 程序，而无需安装软件的客户端。以前，我们在用 C/S 软件的时候，总是这样设计的，首先，要先装好一台服务器，然后，在上面装好 C/S 应用的服务器端软件及数据库，最后，用户还要在客户端电脑上安装 C/S 应用软件的客户端，然后，用户在使用的时候，先运行自己电脑上的软件客户端，再联到服务器端，最后，才可以使用这个软件，那个这个应用如何在互联网上使用呢？我们一个企业的 ERP 应用来作个分析：

传统方案，首先还是要在总部装一台服务器并装好 ERP 的服务器端，并且，要把服务器软件的应用端口要映射到公网上，远程用户电脑上装上 ERP 客户端，然后，用 ERP 客户端去联服务器端，这样，远程用户可以使用这个软件系统。

CYLAN 方案，总部先装好一台 ERP 服务器，然后，前面装一台 VPN，远程用户不用装 ERP 的客户端软件，直接可以用浏览器以 VPN 的形式去访问 ERP 服务器。

以上两个方案，我们作个比较

	远程用户的客户端软件	加密	认证	跨平台	安全性	速度	易用性	软件维护
方案一	要装	无	无	WINDOWS	不好	慢	一般	复杂
方案二	不用装	有	有	支持 JAVA 浏览器的任何平台	好	快	好	简单

从上表可以看出，方案二的优势非常明显，CYLAN SGA 的 C/S 转 B/S 应用为企业提供了既安全，又简单的远程应用解决方案，是企业用户 C/S 应用的最佳选择。

2．1．5　TCP 端口应用

CYLAN SGA 还提供了一种更灵活的应用方式，TCP 端口应用，这种应用可以发布总部服务器上任何一个 TCP 端口，如 1433，21，80 等，远程用户只要通过 SSL 认证后，即可直接使用这个发布的 TCP 端口，这种应用给企业应用布署提供了更灵活的解决方案，适合于复杂的网络环境及应用环境，而且这个方式也可以弥补一些 WEB 应用中的不足和一些复杂的 WEB 应用，为企业提供了一个可伸缩性的解决方案。利用 TCP 发布的端口应用，远程用户可安全地，透明的访问总部服务器的资源，如内部的 MAIL 系统，远程用户可以利用 TCP 应用，直接使用自己的 MAIL 系统，TCP 端口应用的透明方式，使用户无需修改自己的 MAIL 参数，而直接可以使用内部 MAIL 系统，给用户使用带来了极大的方便性。

2．1．6　SSL 隧道模式

针对于企业应用中的 UDP 应用，及语音和视频流应用，CYLAN SGA 提供了全隧道模式，这个隧道模式完全支持网络层以上的所有应用，而且，还可以让网络管理人员在远程能够访问到企业内部的所有电脑及网络设备；只要远程用户通过 CYLAN SGA 界面开启客户端隧道功能，就可以访问总部已发布的网络资源了，并且，还可以双向访问，CYLAN SGA 隧道模式，为企业用户提供了更加完整的远程应用解决方案。

2．2 LAN TO LAN 的解决方案

对于异地网络互联，分公司和总部的互联的应用需求，CYLAN SGA 还提供了 LAN TO LAN 的完美解决方案，只要总部和分公司各安装一台 SGA，就可以轻松实现两个内部网络的互联，真正地把不同地区的两个局域网联在一起，让用户感觉不到地域的间隔，就象访问内网一样来访问总部的资源，给用户访问带来极大的方便。

支持 IPSEC 协议互联，支持 IPSEC 客户端接入，为远程用户提供了一个完整的解决方案，另外，还支持 PPTP SERVER，当用户选用此功能时，在登录 SSL 时，SSL 会自动建立一条 PPTP 隧道到 SSL 上，省去了用户的配置过程，应用更加方便。

2．3　远程用户安全性检查

CYLAN SGA 针对远程用户还提供了一种安全性检查机制，当远程用户在使用 SGA 前，首先，对用户电脑系统进行一些可定制的检查，如 WINDOWS 的安全补丁，防病毒软件等有没有安装，也可以对用户的电脑进行绑定，检查用户电脑系统及硬件是不是允许访问的电脑，这样，对于企业内部来说，又多了一层安全的保护，CYLAN SGA 的远程用户安全性检查，既确保了远程用户的可信度，又可以减少由于远程接入而带来的安全隐患。

支持用户上网隔离，用户登录 SSL 后，不能使用外网资源，如 QQ、网站等，支持硬件绑定，把用户账号和电脑硬件绑定在一起，这样，可以锁定用户使用的电脑，增加用户接入的安全性，支持用户登录时的软键盘使用，可以有效防止用户端的木马记录键盘信息。

2．4　远程用户访问认证

为了提高企业门户的安全性，CYLAN SGA 提供了多种用户认证方式，包括本地用户认证，证书认证，WINDOWS AD，RADIUS，LDAP，USB-KEY，动态令牌，短信认证等，为企业用户提供了多种认证及交叉认证，从而更灵活地布转署了认证策略，让企业放心地提供远程接入，让远程访问更加安全。

此外，赛蓝 SSL 还可以使用第三方的数据库认证，如结合 SQL，ORACLE，SYBASE 等数据的账号作为 SSL 的登录认证账号，还有更高级的认证，指纹认证和邮箱账号认证。

支持多种文本账号批量导入，支持 LDAP 账号，数据库账号导入，与第三方数据库完美

结合。

支持认证顺序配置，包括第三方数据库认证，支持 VIP 用户。

用户访问策略

支持多种用户认证机制，支持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，指纹用户的增强, 支持后台管理指纹的录制和指纹的增删等 支持检验与校验模式两种方式的指纹认证模式，支持任意的类型用户的 对应用户与默认用户的分配权限的模式。

可以配置用户访问时间的控制策略，包括多个时间段，有效控制站点的开发时间。

2．5 日志审计功能

可以对用户的访问过程作详细记录，CYLAN SGA网关提供了调试、信息、告警、错误等级别的运行日志，帮助管理诊断系统。并提供了用户访问记录审计和报表来记录、跟踪用户行为。

由于VPN网关的存储空间有限，CYLAN SGA还提供了独立的日志中心。通过第三方的日志中心，管理员可查看用户的登录次数、告警次数等进行直观显示，并可直接打印和导出。CYLAN SGA安全网关丰富的日志中心，为网络管理员和决策者了解VPN资源的详细使用情况提供了最有效的数据支持。

2．6 防火墙功能

CYLAN SGA 还提供了一些防火墙功能，支持路由模式，支持 PPPOE，NAT，DHCP，用户可根据自己的需求来定制自己的防火墙规则，如根据 IP，端口，协议，时间等参数，进行对内网及外网的控制，为企业用户又提供了一层安全保护。

2．7 支持动态IP接入

由于宽带的普及以及ADSL资费的降低，国内中小型企业通常采用ADSL拨号等动态IP

的方式接入互联网。CYLAN　SGA集成了目前常用的动态域名客户端，可以轻松解决用户动态公网IP接入的问题，使的CYLAN　SGA网关在部署的时候无需固定IP，完全支持动态IP。由于CYLAN SGA内置动态域名客户端，所以，用户就不必在前端的路由器或电脑上安装动态域名软件，这样，不仅可以减少了管理员的维护量，而且，也增加了远程接入的可靠性，移动办公人员使用浏览器连接入公司内网时，也更加便捷。由于支持动态IP接入，CYLAN SGA同样也适合中小型企业。

2．8　完美的个性化定制

CYLAN　SGA 可以为远程用户创建全面可定制的登录界面，为不同角色的用户提供个性化的登录界面外观，从而改进用户体验.

三、 CYLAN SGA 工作原理和组网方式

3．1　SSL 协议介绍

SSL 是Secure socket Layer英文缩写,它的中文意思是安全套接层协议,指使用公钥和私钥技术组合的安全网络通讯协议。SSL协议是网景公司(Netscape)推出的基于 WEB应用的安全协议,SSL协议指定了一种在应用程序协议(如Http、Telenet、NMTP和FTP等)和TCP/IP协议之间提供数据安全性分层的机制,它为TCP/IP连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证,主要用于提高应用程序之间数据的安全性,对传送的数据进行加密和隐藏,确保数据在传送中不被改变,即确保数据的完整性。

SSL协议过程通过3个元素来完成：

（1）握手协议：这个协议负责配置用于客户机和服务器之间会话的加密参数。当一个SSL客户机和服务器第一次开始通信时，它们在一个协议版本上达成一致，选择加密算法和认证方式，并使用公钥来生成共享密钥。

（2）记录协议：这个协议用于交换应用数据。应用程序消息被分割成可管理的数据块，还可以压缩，并产生一个MAC（消息认证代码），然后结果被加密并传输。接收方接收数据并对它解密，校验MAC，解压并重新组合，把结果提供给应用程序协议。

（3）警告协议：这个协议用于表示在什么时候发生了错误或两个主机之间的会话在什么时候终止。

SSL协议通信的握手步骤如下：

第1步，SSL客户端连接至SSL服务器，并要求服务器验证它自身的身份；

第2步，服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链，直到某个根证书颁发机构（CA）通过检查有效日期并确认证书包含可信任CA的数字签名来

验证证书的有效性。

第3步，服务器发出一个请求，对客户端的证书进行验证，但是由于缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。但是完善的SGA安全体系是需要对客户端的身份进行证书级验证的。

第4步，协商用于加密的消息加密算法和用于完整性检查的哈希函数，通常由客户端提供它支持的所有算法列表，然后由服务器选择最强大的加密算法。

第5步，客户机和服务器通过以下步骤生成会话密钥：

客户机生成一个随机数，并使用服务器的公钥（从服务器证书中获取）对它加密，以送到服务器上。 服务器用更加随机的数据（客户机的密钥可用时则使用客户机密钥，否则以明文方式发送数据）响应。使用哈希函数从随机数据中生成密钥。使用会话密钥和对称算法(通常是RC4，DES，3DES)对以后通讯的数据进行加密。

在SSL通信中，服务器方使用443端口，而客户方的端口是任选的。

3．2　SGA技术实现

SGA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。SGA网关位于企业网的边缘，介于企业服务器与远程用户之间，控制二者的通信。

掌握三个关键术语的含义有助于理解SGA是如何实现的。即：代理（Proxying）、应用转换（Application Translation）、端口转发（Port Forwarding）。

SGA网关至少要实现一种功能：代理Web页面。它将来自远端浏览器的页面请求（采

用HTTPS协议）转发给Web服务器，然后将服务器的响应回传给终端用户。

对于非Web页面的文件访问，往往要借助于应用转换。SGA网关与企业网内部的微软CIFS或FTP服务器通信，将这些服务器对客户端的响应转化为HTTPS协议和HTML格式发往客户端，终端用户感觉这些服务器就是一些基于Web的应用。

有的SGA产品所能支持的应用转换器和代理的数量非常少，有的则很好地支持了FTP、网络文件系统和微软文件服务器的应用转换。用户在选择网关时，必须对自己所需要转换的应用有一个很明确的了解，并能够根据它们的重要性给它们排个先后顺序。

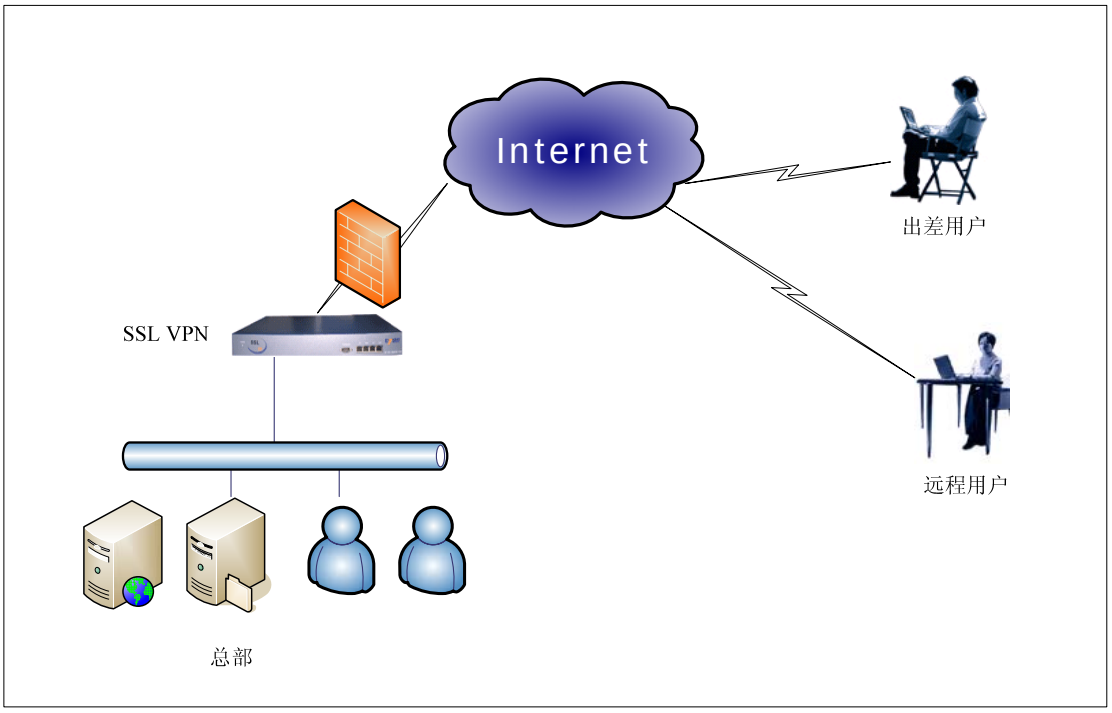
而有一些应用，如微软Outlook或MSN，它们的外观会在转化为基于Web界面的过程中丢失。此时要用到端口转发技术。端口转发用于端口定义明确的应用。它需要在终端系统上运行一个非常小的Java或ActiveX程序作为端口转发器，监听某个端口上的连接。当数据包进入这个端口时，它们通过SSL连接中的隧道被传送到SGA网关，SGA网关解开封装的数据包，将它们转发给目的应用服务器。使用端口转发器，需要终端用户指向他希望运行的本地应用程序，而不必指向真正的应用服务器。

良好的SGA产品应该具有较好的互操作性，较为细致的访问控制能力，完善的日志和认证体系以及对应用的广泛支持。

3．3 CYLAN SGA 原理和网络拓朴图

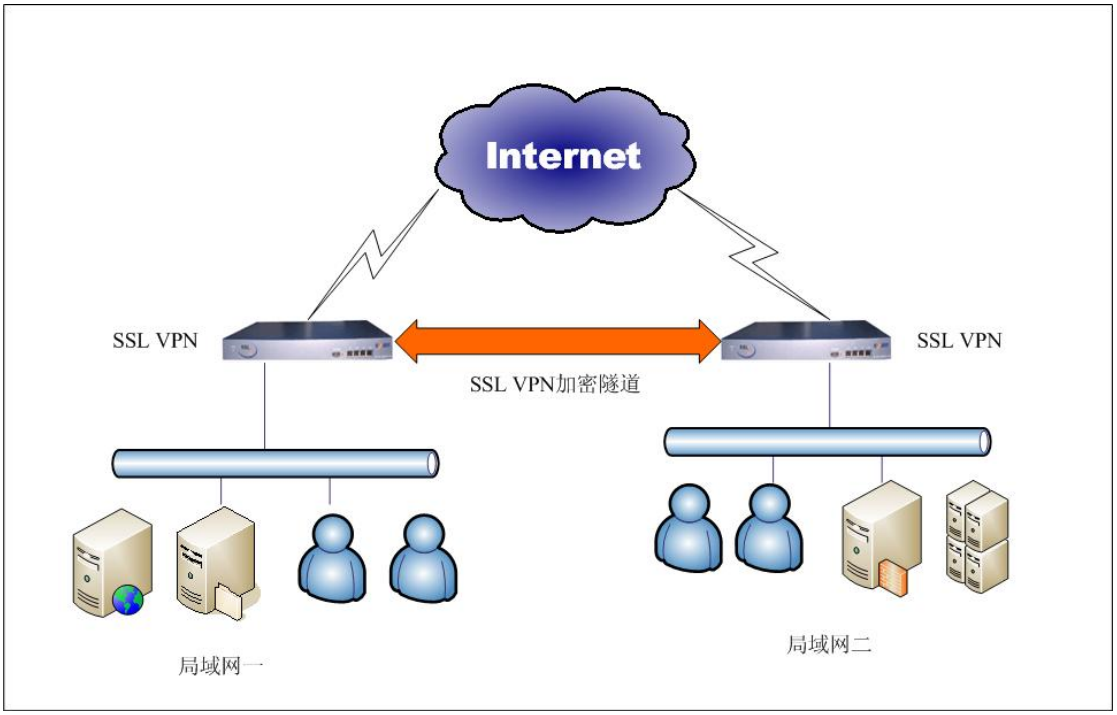
CYLAN SGA 采用了标准的 SSL 协议和多种加密和认证算法，来实现远程接入和安全性，并且扩充了 TCP 端口应用和全隧道 SSL 客户端模式，使 SSL 应用更加完美，下面介绍一下 CYLAN SGA 的网络接入图：

A、 点到 LAN 拓朴结构图



CYLAN SGA 可以接在企业的防火墙的后面，并且，SGA 要能够访问到企业内部的服务器，防火墙上要把 SSL 使用的端口（TCP 443）映射到 VPN 上，这样，远程用户就可以通过互联网联到 SGA 上了，当远程用户点击应用图标时，实际上，是 SGA 代理用户去访问服务器，这样，使访问更安全，SGA 相当于一个应用网关，集中发布企业内部资源，统一认证，统一管理，集中应用，为企业提供了一个应用门户。

B、LAN TO LAN 的网络结构



这种网络结构中，通过两台 SGA 的设备把局域网一和二联在一起，SGA 通过封装和加密，在互联网上建立起一条虚拟通道，使局域网一和二就象内网一样可以互相访问。由于，全隧道方式支持所有的 IP 层以上的应用，两边用户可以完全使用对方的资源，包括 FTP，网络邻居，数据库，语音视频流等所有应用。

四、 CYLAN SGA 的技术优势

4．1　将 C/S 应用转成 B/S 访问

传统的C/S 结构的应用系统运行性能稳定，但在进行异地分支运行时,有安装、维护成本高的缺点,尤其是在一个企业有很多C/S的应用需要分配给远程用户时,系统管理员需要给远端用户安装多个C/S的客户端,安装和维护成本更高。如下图：

现在,CYLAN SGA 可以将 C/S 的应用集中管理,使用户通过 WEB 方式,将企业 C/S 的应用按不同的用户,分配给不同的应用.也就是将多个 C/S 应用接转化为 B/S 架构，使企业集团中所有的应用系统都可使用标准的浏览器运行，同时可优化企业中 B/S 架构的应用。

使用 CYLAN SGA,可以将需要在远程安装客户端的应用程序,完全集中在中心进行管理，无需要任何客户端即无 VPN 客户端和应用程序客户端(比如用友 ERP 的远程用户,无须安装 ERP 的 CLIENT 端),仅仅使用 WINDOWS 标准的浏览器实现远程访问(包括 B/S 、C/S 应用)，简化了工作环节，与传统的 PC 组网方式相比大大地减少了维护人员的工作量，解决了 C/S 应用部署难的问题。既将 C/S 系统转换为 B/S 架构,大大降低了总体拥有成本，由于 CAB 技术完全基于中心系统运行的特性，使得网络硬件升级换代的代价大大降低，只需中心端适当升级即可，远程客户端本身不必考虑。

4．2　WEB应用功能

CYLAN SGA所支持的浏览器类型包含Html，Dhtml, Jsp, Asp,Java applet, Active, Cookies等各种Web技术，通过html智能重构技术、应用转换技术和TCP端口应用技术及IP层隧道功能，实现了对目前所有网络层以上各种静态或者动态端口应用的完全支持，包括：网上邻居、文件共享、FTP、OUTLOOK、SQL、Lotus NOTES、SYBASE、ORACLE、CITRIX等各种应用。

4．3　访问的安全性

SSL 用户在访问过程中的安全性保障是通过以下几方面进行的：

1）用户认证：本地用户认证，证书认证，WINDOWS AD，RADIUS，LDAP，USB-KEY，动态令牌，短信认证等多因子多因素强认证功能，支持硬件绑定认证，支持第三方数据库认证（SQL，SYBASE，ORACLE），支持指纹认证，支持邮箱账号认证，支持多种认证混合使用，极大的提高了远程用户可信度和安全性；

2）客户端安全检查：对用户电脑的系统进行定制检查，如 WINDOWSA 的安全补丁，防病毒软件安装等，发现不符合条件的，不允许访问到 SSL；

3）高效认证加密：用标准SSL协议内置的RC4 等加密算法和RSA128bit签名算法来保证数据的安全性和完整性；

4）细致的访问权限控制：CYLAN SGA通过独特的角色管理功能，提供了细致到每个URL和不同应用的权限划分。通过给不同用户设置不同角色来分配访问授权，一个用户可以赋予多个角色以适合各种复杂的组织结构。基于角色的访问限制为企业网络提供了较强的安全性。通过行为跟踪引擎，管理员还可以查看远程接入用户的所有访问记录。

5）自动清除访问记录，实现“零痕迹”访问

CYLAN SGA在用户结束访问以后，会自动清除Cookie，临时文件等遗留在客户端计算机上的信息，实现“零痕迹”访问，避免安全隐患。

6) 超时退出，防止窥探

为防止用户在没有注销的情况下长时间离开，导致他人窥探到SGA内的机密信息，CYLAN SGA安全网关特别加入了不活动检测引擎。当检测到客户端在指定时间内没有任何访问内网资源的流量时，SGA网关将自动弹出对话框，提示用户“SSL连接会在X秒内超时关闭，继续还是注销？”若用户在该时间内仍未选择相应动作，则CYLAN SGA安全网关将自动注销，中断会话并重新返回登录界面。

4．4 稳定性及高可用性

由于 CYLAN SGA 采用的是其于 LINUX 的内核，并对其内核进行优化，系统的稳定性得到更一步提高，加上采用特定的硬件设备，及对硬件的定制开发，使得 SGA 的稳定性更加可靠，CYLAN SGA 支持多设备进行负载均衡及 SSL 热备，从而，减少了企业在 IT 部署的采购投入，降低了企业的总体拥有成本。

4．5 低带宽运行特性

目前，用户大多通常使用ADSL 2MB的带宽，如果不采用其他加速技术，在速度上很难满足用户的正常使用,尤其是C/S系统在有大量数据库查询动作时,速度问题尤其明显，因此远程用户除考虑VPN远程连接的稳定性、VPN技术的安全性还需要考虑VPN系统对带宽的占有率，在正常情况下，提高远程VPN运行速度，大多是通过提高带宽方法来增加速度，也有通过使用CITRIX和RDP的技术来实现。现在，CYLAN SGA产品就从根本上为用户解决了速度问题.

CYLAN SGA 采用了 CAB 技术，提供了数据压缩和应用加速功能，在网络上只传输鼠

标、键盘指令和远端变化部分的屏幕信息，带宽占有量只要 30K。通过 CYLAN SGA 平台，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。

4．6 布署灵活，维护简单

CYLAN SGA 可以采用直接联公网或内部单臂模式，对于企业布署极为简单，并且，应用发布简单，可以快速的布置应用，对于远程用户来说，应用更为简单，只需打开浏览器，就可以轻松实现远程访问，由于一般只需维护总部的 SSL 和服务器，远程用户的维护量几乎为零。

4．7 远程唤醒功能

CYLAN SGA 提供了一种远程唤醒电脑功能，为远程办公和远程管理提供了极大的方便，网络管理员可以通过 SGA 远程开启服务器，远程用户可以通过 SSL 远程给自己的电脑开机，从而来实现远程办公。

五、 CYLAN 安全网关的产品介绍

目前赛蓝SGA系列产品有SGA350，SGA520，SGA580，SGA610，SGA680，CYLAN SGA安全网关适合于中小型规模的公司，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、FTP服务器、远程控制、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，建立安全SGA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。

应用领域

CYLAN SGA 提供下述情况的解决方案：企业需要通过互联网（笔记本型计算机、移动个人计算机、PDA 用户接入）达到广泛而全面性的信息存取。CYLAN SGA 能满足所有企业远程接入需要。CYLAN SGA 技术为企业提供全面的灵活性，以便更好地配合企业的安全性和改善应用部署和管理的需要，同时给企业带来一个统一的、方便的和简易的使用经验。CYLAN SGA 还提供了高可用性的负载均衡的能力，它具有可靠的冗余能力，排除了单点故障的可能性，减少系统停机时间，从而提高系统的整体性能。

产品优势

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：使用 CYLAN SGA 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：CYLAN SGA 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：CYLAN SGA 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：CYLAN SGA 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：通过 CYLAN SGA 平台，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(SQL、ORACLE、SYBASE)，支持第三方用户导入(文本、数据库)。

附录：

CYLAN SGA 功能表		
特性	功能特性	功能描述
快速性	WEB 应用加速	对 WEB 访问资源的压缩
	C/S 应用加速（CAB 技术）	通过赛蓝的 CAB 技术对数据进行压缩传输
	TCP 应用加速	TCP 端口数据压缩
	SGA 隧道流量压缩加速	对 SSL 隧道数据进行压缩传输，提高传输效率
安全性	安全算法支持	支持 DES、3DES、AES、MD5、RC4、RSA、签名算法，支持加载扩展安全算法模块
	多种身份认证	支持指纹认证、短信认证、USB KEY 认证、U-KEY 认证；CA 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、并提供多种混合手段认证
	密码保护措施	采用密码强度检测、周期性更换密码要求、防暴力破解策略、账号锁定解锁功能、管理员密码权限设置、软键盘、图形验证码等输入验证方式；
	细致的权限控制	基于角色、用户组的管理、严格细致控制访问者权限、保障接入安全
	用户账号有效期策略	根据用户角色定义账号使用时间、期限
	服务器内网保护	通过 SSL 代理访问，服务器可隔离外网访问
	客户端安全	远程用户终端操作系统、杀毒软件版本检测、登陆超时退出功能、自动清除客户端缓存和临时文件，消除上网痕迹、外网隔离功能，用户登陆 VPN 后自动断开外网连接，防止跳板攻击等。
高可用性	多平台支持	支持 3270、5250、VT、HP700 and SINX97801 应用，支持 LINUX/UNIX 应用；支持 Windows 98/ 2000/XP/2003/Vista；PDA 访问支持
	B/S 应用支持	支持所有 WEB 站点、OA、WEB MAIL 系统，支持 Html/Dhtml, Jsp, Asp, Java applet, Activx, Cookies 等各种 Web 技术；支持 FTP、Email 的 Web 访问。
	C/S 应用支持	支持所有 C/S 软件和 WINDOWS 程序的发布。包括：http，Email，Ftp，网上邻居，Notes，Outlook，Oracle, SQL 等各种动态和静态的 C/S 应用；支持内网 DNS、支持对应用的透明访问、自动定位 URL、支持隐藏服务、应用的快捷方式、自动启动服务。
	C/S 应用 WEB 化	通过设备应用发布，将 C/S 转化成 B/S 结构，远程用户无须安装客户端程序
	IP 应用支持	支持所有基于 TCP/UDP/ICMP 协议应用
	单点登录	支持 B/S 和 C/S 的应用支持单点登录，并提供加密认证功能。访问多个应用，只须输入一次密码。
	页面定制	可根据需求制作前后台登陆界面，提供模板操作，简单易用。
	用户导入	支持 AD/LDAP/RADIUS/SQL/SYBASE/ORACLE 等第三方数据库导入账户，并实时进行权限划分；支持文本账户导入，方便大量用户账户建立
	PPTP 支持	支持 PPTP windows 客户端
	管理方式	支持本地及远程的 https、Consol、SSH 等管理方式
	统一界面发布	支持列表和图标模式发布模式，应用集中管理
	信息公告	登陆前台显示信息公告窗口，企业信息及时发布

	支持重定向功能	用户在输入 http 登陆的时候，系统自动跳转到与其对应的 https 站点
	隐藏服务	对于重要的应用，可以隐藏发布，避免信息泄漏
易管理性	Web 管理界面	支持 SSL 加密的 WEB 界面进行设备配置和管理，支持简体中文\繁体中午\英文界面
	虚拟站点	根据需要配置不同的站点和分站点管理
	站点开放时间	设置站点开放时间策略
	SNMP	集成第三方管理系统，实现更强大的监控功能
	备份功能	支持本地和远程备份及恢复
	在线升级	通过远程进行设备版本升级
	系统日志	提供详细的审计和日志功能。记录访问内容请求，用户访问的时间、访问地址等信息，提供详细的系统信息，调试及错误日志，支持与第三方 Syslog 日志服务器同步。
	用户行为管理	查看用户行为完全记录，提供查询、排序、过滤等功能；可进行用户信息批量导入及各种数据库第三方导入。
	细致的用户权限管理	根据用户分配接入权限和访问权限，提供基于用户、用户组、角色、资源等多种方式的权限控制；管理员分级权限管理；实时监控用户接入情况，可进行并发限制、用户中断等操作；
可扩展性	灵活的授权策略	通过序列号进行功能和许可管理，给予用户角色时间进行任意组合的访问策略
	接入方式	支持单双臂模式，组网灵活。
	集成 IPSEC 功能	支持 LAN-TO-LAN 和 POINT-TO-LAN 的双向 VPN 隧道模式，满足全部的远程用户的应用需要。完全的网到网的互联互通。可以组成星型和网状 VPN 隧道架构