第 5 章 典型案例

VPN 利用加密管道在互联网内传播信息，使用本地数据线的架设和租借来满足世界范围内的数据传输要求。VPN 还可以实现远程的网络访问服务，这种服务相对于以往的跨地域网络访问服务具有较高的性价比。VPN 在资源利用率、安全性、扩展性方面具有较好的表现，近年来得到广泛应用。本章主要针对 VPN 的应用场景给出应用案例，通过本章的学习，应了解 VPN 的实际应用环境与解决方案。

5.1 企业安全邮件办公解决方案

5.1.1 需求分析

1. 应用背景

邮件系统是现代企业内外信息交流的必备工具之一。随着互联网的迅速普及以及企业自身信息化建设的进展，大型企业对邮件系统提出了更高的要求。并且在不同行业领域中，邮件系统也呈现了不同的行业需求。

在大型企业中，由于人员众多，层级复杂，分支机构庞大，业务分部地域广，从而要求邮件系统必须有助于提升企业的信息共享和办公效率，安全稳定，并且应用丰富，与现有协同办公系统集成，同时满足随时随地移动办公的需求。

政府部门为了实现组织结构和工作流程的重组优化，建立精简、高效、公平的政府运作模式，纷纷开展电子政务系统建设。在中国，电子政务建设已经成为今后一个时期信息化工作的重点。政府先行，将带动国民经济和社会发展信息化。而邮件系统作为电子政务的基础工具，正是利用信息技术实现高效办公、提升服务水平、实施信息化管理的关键环节。

2. 用户需求

用户需求主要体现为以下两方面。

1）企业办公安全性

企业内部很多重要的数据需要通过邮件系统传递和共享，但是邮件收发过程也是这些数据最易被攻击、窃取的关键过程。所以，提高邮件在传输、下载、外发等过程中的安全可靠性就显得十分重要。

越来越多的企业员工通过移动终端进行邮件收发，移动终端也就变成了安全隐患。

因为移动终端携带木马病毒，导致下载到本地的敏感数据被窃取，这种事件频频发生。在BYOD(Bring Your Own Device，自带设备办公)的大趋势下，提升移动终端的安全性，对落地数据进行加密以防止泄露，显得尤为重要。

传统邮件都是通过公共网络传输的，即使经过加密处理，也因为密钥算法强度太低而易被攻破。将邮件系统与 SSL VPN 相结合，在传输中采用国密算法，可以大大提升破解难度，解决传输安全问题。

2）企业办公易用性

员工在差旅中无法及时收发邮件，进行日程管理和会议安排。在移动办公环境下，需要通过移动终端连接 VPN 进行远程办公，以提升办公便捷性。

企业的 OA、财务、IM、ERP 等众多系统需要分别登录，十分烦琐，需要通过邮件系统实现横向整合。

此外，超大附件无法上传，经常造成网络拥堵。海外邮件经常发生丢信、退信现象。邮件系统容易宕机，严重影响公司日常业务沟通。这些问题都需要加以解决。

5.1.2　解决方案

本解决方案是针对目前的 BYOD 移动办公需求以及企业邮件办公安全需求，实现企业移动办公安全性、快速性、易用性、全面性，在保障移动办公人员高效访问办公业务的同时，可以提供更为安全可靠、用户体验更佳的一体化安全邮件解决方案。

安全邮件解决方案部署框架如图 5-1 所示。该方案将网络分为 4 个逻辑结构区域：用户端、接入端、DMZ 以及企业内网。其中，移动终端安装了移动终端安全管理系统客户端(同时支持 Android、iOS 系统)，在该客户端中已经集成了 VPN SDK，用户无须手动建立 VPN 连接。

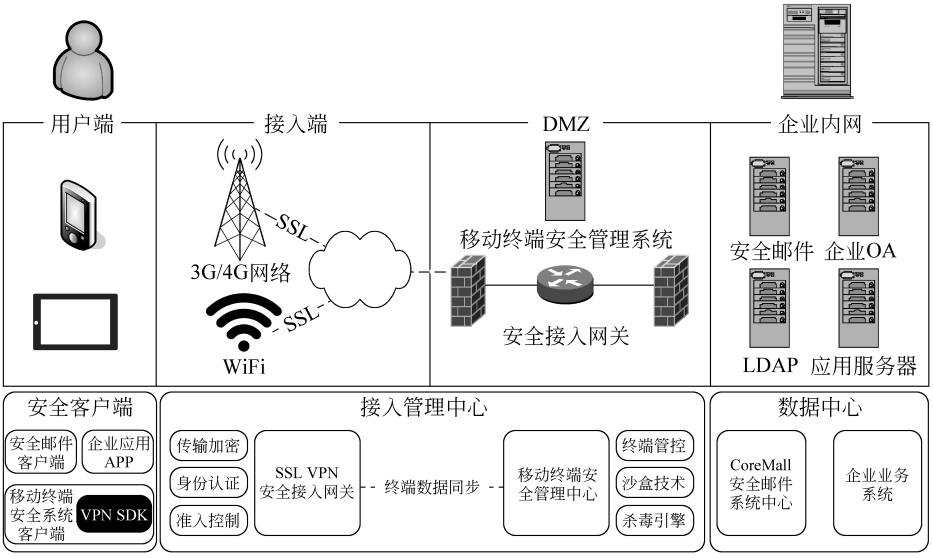

图 5-1　安全邮件解决方案部署框架

终端用户可通过直连、3G/4G 网络或者 WiFi 连接到 SSL VPN 安全接入网关，传输隧道都通过国密算法进行加密，以确保传输安全。SSL VPN 安全接入网关可单臂旁挂在核心交换机旁，不改变企业原有网络架构。移动终端安全管理系统管理平台与 SSL VPN 安全接入网关会实时进行终端违规、准入状态同步，从而联合对用户身份、终端扫描安全性、应用权限等进行准入控制。

数据中心部署安全邮件服务器端、企业 OA、CRM 等业务系统。当用户通过身份认证和权限匹配后，可访问内网邮件、办公系统。

解决方案联动方式如图 5-2 所示。在安全客户端中，已经集成了 VPN SDK，并且已安装安全邮件客户端，客户端作为工作区的唯一入口。当用户完成认证，进入工作区时，SSL VPN 会在后台自动建立连接。工作区与 Android 系统桌面保持风格一致，以增强用户体验。

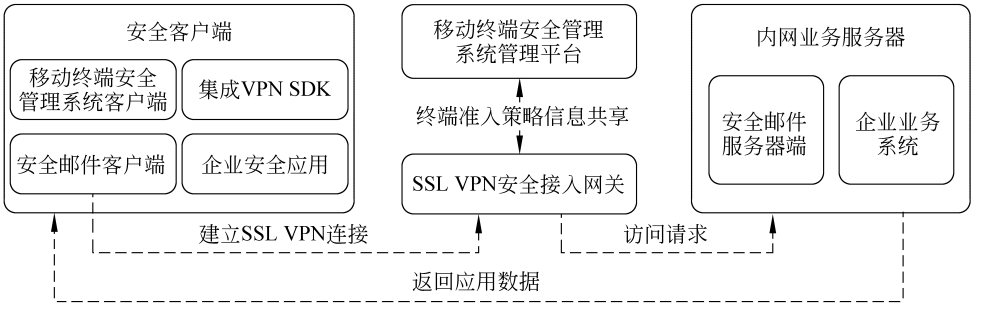

图 5-2　安全邮件解决方案联动方式

用户发起访问请求时，会先进行工作区认证，认证通过后，请求到达 SSL VPN 接入网关进行终端准入策略校验。SSL VPN 设备与移动终端安全管理系统管理平台部署在同一区域，终端准入策略信息可实时共享。当移动终端安全管理系统管理平台通过终端准入策略校验后，会告知 SSL VPN 设备，完成 SSL VPN 隧道的建立。随后，请求被发送到邮件服务器，最终将应用数据返回终端。

1）客户端数据安全

通过移动终端安全管理系统，可利用沙箱技术在终端上建立企业安全独立工作区，企业所有的数据只能在工作区中访问，企业内部应用也只能在工作区中运行，个人数据不能进入工作区，同时工作区的应用也不能调用个人数据，真正地实现公私数据隔离，确保企业数据的安全。

通过安全邮件客户端下载到本地的附件和数据都以加密（采用 AES256 或 SM4 算法）方式保存。这些附件和该数据与个人区隔离，即使外发到其他终端设备上也是加密状态，无法进行破解。

2）服务端数据安全

邮件系统支持邮件密级、附件密级和人员密级。邮件密级有 6 个级别，由高到低依次为机密、秘密、核心商密、普通商密、内部、公开。邮件密级有效地保护了企业邮件通信的安全。邮件加密包括 PKI 加密、CoreMail 加密、IBC 加密等方式。

邮件系统将企业所有进出邮件实时(定时)存储在归档服务器中,可对归档的邮件进行审计、监察、恢复、检索等管理操作,满足三员分立、资料防泄露、搜索法律证据、恢复历史邮件等多种功能需求。

邮件系统支持多重反垃圾邮件机制,通过反垃圾双引擎过滤、CAC(Coremail Anti-spam Center,反垃圾邮件服务运营中心)在线服务和邮件密级控制,可在内部进行监控和审核,增强了信息资源的安全保障力度。

3) 数据传输安全

企业数据通过 SSL VPN 加密隧道传输,链路加密算法同时支持商密算法(AES、3DES 等)和国密算法(SM1/SM2/SM3/SM4)。采用专业的 VPN 网关设备,在原有 SSL 加密算法基础上提升加密强度,大幅提升破解难度。

4) 终端安全管控

管理员可通过登录移动终端安全管理系统管理界面对终端设备进行统一安全管理,包括远程锁定终端设备、擦除工作区数据、注销/重启设备、锁定工作区、统一推送消息等操作。当员工设备丢失或被窃取时,可第一时间上报给管理员,由管理员对丢失设备进行定位、锁定、数据擦除等操作。本方案的移动终端安全管理系统管理界面如图 5-3 所示。

图 5-3　移动终端安全管理系统管理界面

移动终端安全管理系统集成了专业的防病毒引擎。企业管理员通过管理界面可以实时对终端设备进行扫描杀毒,保障终端设备免受病毒侵扰,避免移动终端被攻击者利用,成为渗透企业内网的跳板,确保终端本身和企业数据的安全。同时,管理员通过管理界面可以统计病毒个数以及未清除的病毒个数等。

5) 身份权限安全

本方案将 VPN SDK 集成到安全客户端当中,作为统一入口。用户可对工作区设置图形锁定码,以免被他人冒用。在进入工作区后,SSL VPN 会自动建立,免去手动建立连接的烦琐过程。另外,管理员可以通过 Web 管理界面设置设备的安全接入准则,可以通过手机号、IMSI 等设备属性设置设备准入条件。本方案的设备准入条件配置界面如图 5-4 所示。

图 5-4　设备准入条件配置界面

移动终端安全管理系统管理平台与 SL VPN 安全接入网关保持信息同步，当终端有违规现象，如设备 ROOT、杀毒检测未通过、有越权行为时，移动终端安全管理系统管理平台会将违规信息同步给 SSL VPN 安全接入网关，自动断开 SSL VPN 连接。

准入流程如图 5-5 所示。

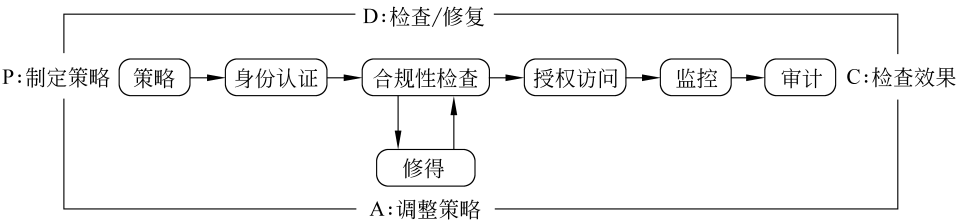

图 5-5　准入流程

6）日志审计安全

在本方案中，移动终端安全管理系统管理平台、SSL VPN 安全接入网关和邮件服务器均有日志记录，以方便管理员查看，且符合国家标准对审计的要求。

移动终端安全管理系统管理平台重点对终端操作进行审计，支持对用户违规事件、策略事件、日常事件等进行日志审核，可详细记录用户设备终端的日常事件信息，并可在管理平台进行搜索和筛选。另外，管理平台对管理员的操作也同样有日志记录，可具体记录管理员对各模块的操作。

SSL VPN 安全接入网关重点对用户访问应用状态进行审计，可查看系统运行状态和用户业务访问日志，并提供在线用户的监控。也可以将日志信息存储在本机的存储设备中，还可以将日志导出到远端的日志服务器中。在将日志导出到日志服务器时，系统会根据管理员配置的日志过滤条件对日志进行筛选。

安全邮件服务器端可根据安全保密管理规定对系统功能进行详细划分，严格控制各类管理员的权限，防止发生权限越界或无法管控的现象，使其符合安全保密要求。管理员按照权限分为系统管理员、安全保密管理员和安全审计员，与系统管理相关功能由系统管理员负责，与系统安全相关的功能由安全保密管理员负责，与系统审计相关的功能由安全审计员负责。

5.1.3　方案优势

本方案有以下 6 个优势。

1）统一的安全管理平台

通过移动终端安全管理系统提供统一的安全管理平台，企业管理员可以高度灵活可控地管理多种多样的移动终端设备，包含市场上主流的 Android、iOS 系统终端。

2）灵活的注册方式

可以以多种灵活的方式注册、下载、安装、激活移动终端安全管理系统，例如短信、邮件或二维码。

3）安全数据防泄密机制

本方案通过终端工作区落地数据加密、链路 VPN 隧道传输加密和服务端邮件加密，实现“云、管、端”全方位防护。并且，安全邮件专用客户端基于 IBC 非对称加密技术，采用 SM9 算法，可对邮件正文和附件进行加密后再发送邮件。该技术除了可对邮件加密以外，还可进行数字签名和身份认证，从而全方位保证邮件安全。

4）企业内部应用统一下发

企业可通过移动终端安全管理系统应用市场统一封装、分发企业合规应用，防止盗版软件对终端数据的窃取。

5）云查杀技术

移动终端安全管理系统集成了专业的防病毒引擎，能够无死角查杀恶意代码，实现了新病毒秒级查杀和系统修复功能，能够保障设备免受病毒侵扰，避免移动终端被攻击者利用，成为渗透企业内网的跳板。

6）高可用性

采用灵活的组织通讯录管理、高级日程会议功能，多组织多域名，可实现跨部门/区域轻松沟通。支持海外镜像加速、全球 AWS(Amazon Web Service，亚马逊 Web 服务)云服务群技术，对海外邮件场景也有良好的可用性。

5.2　企业蓝信 VPN 一体化办公解决方案

5.2.1　需求分析

1. 应用背景

互联网推动各行各业在技术、思维、理念、模式等方面发生了全方位的改变，人们的生

产、工作、生活方式也出现了全新的智能生态的变化。移动信息化已逐步成为企业信息化建设的“标配”,企业也将做出改变和调整,以适应时代发展的需要。具体到工作方式,其中重要的一点就是要积极利用移动互联网技术,配置企业级安全专属移动工作平台,以促进企业经营管理能力和工作水平的提高。

随着互联网访问量的增加以及移动存储技术及商务模式的发展,企业对员工移动办公、远程接入总部内网办公的需求越来越迫切。传统的互联网接入服务已经无法满足企业需求。如何实现网络中的数据隔离、服务器隔离,构建安全的业务子网,以保障企业日常安全的交流和办公,已成为 IT 管理者面临的重大问题。

2. 用户需求

用户需求主要体现在以下两方面。

1) 身份认证和终端安全的保障

企业数据涉及企业的敏感和保密信息,对访问者接入身份的认证非常重要。因此,如何有效识别访问者的身份,判断接入终端的安全性,实现访问权限控制,是保障企业信息安全需要解决的重要问题。

2) 数据传输方式中的安全隐患

现在很多企业内部已应用了各种业务系统,各业务系统之间实现了数据共享。蓝信 VPN 作为移动沟通办公平台,可以实时调用业务数据以实现移动办公,如果终端和企业服务器之间的通信通过公网线路直接进行,那么数据就存在着被篡改和窃取的风险。蓝信 VPN 的业务模式能够有效消除数据传输方式中的安全隐患。

5.2.2 解决方案

1. 移动办公一体化解决方案

为实现企业移动办公一体化,采用网神 VPN 对接蓝信客户端的方案,打造专业的企业级 IM、私有化部署、企业专用的一体化办公方案。网神 VPN 采用国密算法进行加密,支持 SM1/SM2/SM3/SM4 国密算法,安全强度高,破解难度大,保证数据在通过 SSL VPN 加密隧道传输时可以抵御中间人攻击。此外,网神 VPN 全面支持 IPv6 安全接入,满足下一代互联网安全接入要求,为企业远程接入提供了较好的解决方案,只要使用浏览器就能够访问企业总部的资源,如 Windows、Linux、UNIX、Mac OS 等系统的文件和应用程序,而不需要安装任何客户端软件。蓝信 VPN 安全平台架构如图 5-6 所示。

在蓝信 VPN 安全平台中,为保证数据的安全性,在进行通信时,首先由蓝信客户端与 VPN 网关建立 SSL 安全加密通道,VPN 授权蓝信客户端访问内网蓝信服务器端。在蓝信客户端与服务器端建立安全连接后,用户完成蓝信 VPN 平台的登录认证。此时,蓝信客户端生成单点登录 Token,调用 VPN SDK 进行单点登录认证,VPN 网关调用蓝信开放平台认证接口,完成 Token 的验证,认证通过后,将用户认证信息缓存在 VPN 网关。最后,用户在访问蓝信客户端中的内网服务(如内网图文消息、内网 OA)时,网神 VPN SDK 和 VPN 网关对用户进行授权,用户就可以正常访问企业内网的服务。

同时,蓝信 VPN 平台采用以下 9 个安全策略来保证方案的安全性。

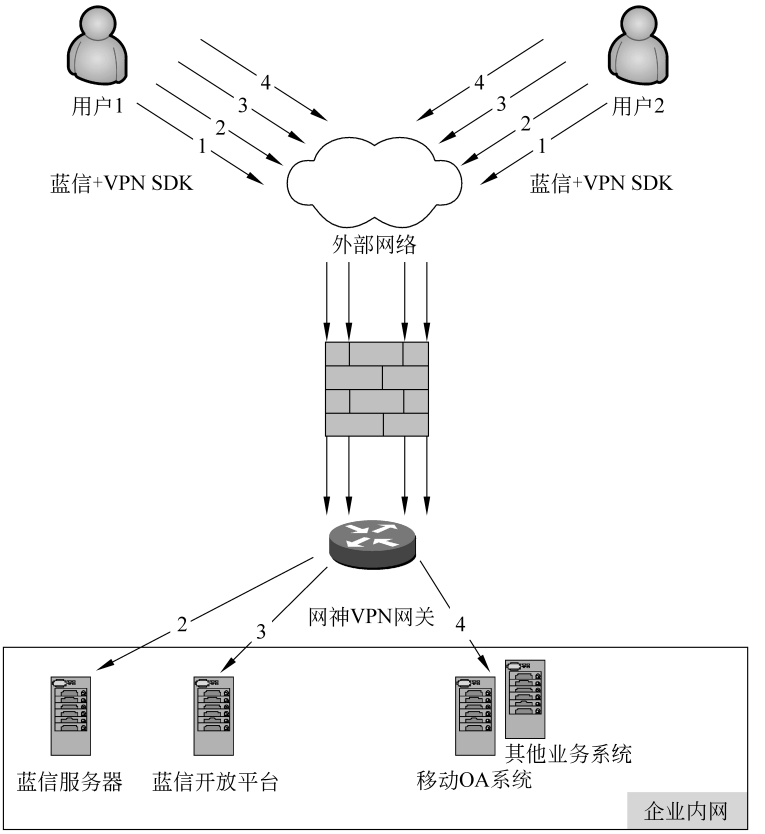

图 5-6　蓝信 VPN 安全平台架构

1）用户密码安全

在蓝信 VPN 平台中，用户密码采用 MD5 加盐（salt）存储，限制同一用户密码重置次数，以防范暴力破解验证码；限制同一用户重复登录次数，以防范暴力破解密码。

蓝信 VPN 安全平台用户密码多次使用 MD5 加密，以确保密码非明文存储，单向加密，不可解密。另外，对用户密码进行 MD5 加盐，以确保不同用户即使密码相同，加密结果也各不相同。为了限制 Web 登录次数，在用户连续 3 次输入错误后，再次输入时，提示输入图片验证码，以防范暴力破解。蓝信 VPN 平台在服务器端采取了一系列措施，如生成验证码时禁止采用伪随机算法，同一用户在同一客户端上连续 5 次输入错误之后将被锁定 1h（1h 内拒绝处理该用户在该客户端的登录操作），以保证用户密码的安全性。

2）客户端数据安全

为保证客户端数据的安全，蓝信 VPN 安全平台由用户设置本地安全口令，同时将安全口令和屏幕锁密码关联，在本地不对安全口令进行缓存，以安全口令对客户端数据库整体加密，输入安全口令后方可查看本地数据。同时对客户端存储进行加密（AES 128 位加密），使用 SQLCipher 对客户端 SQLite 数据库进行整体加密（基于 AES 128 位加密算法），以防止客户端数据泄露。

3）服务器端数据安全

为保证服务器端数据的安全，蓝信 VPN 安全平台对服务器端敏感数据加密存储（AES 128 位加密）。

为防止拖库后的信息泄露以及数据库管理员查看敏感信息，对服务器端存储的公告、调查问卷、系统通知、短信等敏感信息进行加密存储，为每类数据分配一个密钥。

密钥及加密算法由应用服务器控制。对密钥采用私有加密算法保存，使应用服务器和数据库相互独立，以防范加密密钥泄露。

4）应用安全

为保证客户端应用安全，蓝信 VPN 安全平台对以下漏洞进行防范处理：

（1）防范 CSRF、XSS、暴力破解等其他漏洞。

通过规范 refer 并进行检查以防范 CSRF（Cross-Site Request Forgery，跨站请求伪造）漏洞。另外，使用 WAF（Web Application Firewall，Web 应用防火墙，具体为 Nginx Web 应用防火墙模块 naxsi）以防范 XSS 漏洞。

（2）防范本地文件包含漏洞。

将 Web 服务器设置为不使用 root 启动，以防止恶意代码通过攻击服务进程盗用 root 权限。同时设置参数中不能传送根目录（/），以防范恶意代码读取系统文件。

（3）防范客户端 WebView 中的 XSS 漏洞。

服务器端可以对非法 URL 直接返回错误，客户端可以对 WebView 链接进行检查过滤。

5）信息安全

为保证客户端应用安全，蓝信 VPN 安全平台设置了灵活的隐私可见性策略，每个人只能看到被允许看到的通讯录信息。信息安全包括基本可见性管理和高级可见性管理。

（1）基本可见性管理。

基本可见性管理有以下 5 种策略：全员可见、本部门可见、仅管理员可见、隔级向上不可见和单位内隔级向上不可见。

（2）高级可见性管理。

高级可见性管理有以下 3 种策略：个人对个人（部门）不可见、可见不可用（仅能看到头像、名字、职务，不能查看蓝名片）、完全不可见。

6）传播安全

为保证信息的传播安全，蓝信 VPN 安全平台可以设置管控信息传播的模式，支持高级可见性设置，每个人只能看到被允许看到的通讯录信息，防止联系人泄露。具体包括以下措施：

（1）可以限制普通用户建立群聊、群发的群大小。

（2）支持设置组织内敏感词。对组织中的敏感词提前进行设置，在群聊和群发时，无法发出包含敏感词的内容，但私信聊天不受敏感词影响，以此控制信息传播的内容。

（3）支持审核公告内容。创建公告时可设定公告的发布范围。每次发送公告时，只能在发布范围内选择接收者。另外，组织内可设立审核员，审核通过的公告才可发送。但是审核机制不影响组织成员的群聊、群发，只控制信息的传播范围。

7）传输安全

为保证信息的传输安全，蓝信 VPN 安全平台自定义私有协议，参考 SSL 加密传输算法，使用服务端公私钥对进行非对称加解密，使用 AES 128 位加密进行对称加解密。

同时，保证仅核心人员掌握私有协议，所有协议交互均进行传输加密；关键信息非对称加密，密码（单向加密后的数据）、密钥等关键数据采用非对称算法加密后传输（客户端公钥加密，服务器端私钥解密），除蓝信服务器端外，均不可解密；传输加密参考 SSL 的加密方式，客户端使用服务器端公钥对随机生成的对称密钥进行非对称加解密，传输过程中使用 AES 128 位加密算法进行对称加解密。

8）网络安全

为保证网络安全，蓝信 VPN 安全平台可以对内网和外网进行隔离设置，仅开放必要端口以满足企业业务需求。服务器部署区分 DMZ 区和核心区，公网的用户只能访问 DMZ 区的 Web 服务和协议服务，核心区服务器只能由 DMZ 区的服务器访问；服务器仅开放与应用有关的端口；数据库仅对应用服务器开放读写访问权限，其他用户及应用仅有读权限。以此保证网络的安全。

9）系统安全

为保证系统安全，蓝信 VPN 安全平台对系统的权限有以下设置：

（1）细分运维权限，严格管理系统用户。针对系统管理、软件部署升级、日常维护等情况，设置不同的用户管理权限；设置关闭系统默认账号，定时账号登出，只开通 SSH 安全登录；另外，对系统用户、数据库用户设置复杂密码，定期更换；同时对用户登录进行记录，内容包括用户登录使用的账号、登录是否成功、登录时间及关键操作命令。

（2）平台管理员需使用 CA 证书登录，以防范账号口令泄露。

（3）平台管理员/操作员的敏感操作采用双密码认证。

平台管理员/操作员在对系统进行操作前，需向与蓝信 VPN 安全平台合作的第三方认证中心申请 CA 证书。平台管理员可以绑定证书或修改绑定证书，另外，平台管理员仅可使用绑定的 CA 证书登录系统，以降低账号口令泄露风险。

2. 方案优势

本方案具有以下优势。

（1）内部沟通安全快捷。

企业内网业务可通过安全接入网关远程发布，用户通过蓝信安全客户端即可访问企业内网业务。安全的身份认证机制保证了内部的即时工作沟通，沟通信息安全可追溯。

（2）业务数据安全访问。

蓝信安全客户端作为移动办公平台，除自身功能外，还可以方便地对接各种工作系统，作为移动网的统一工作入口。员工上班后，只需用手机打开蓝信，不需要其他应用，以保障业务系统的数据安全接入，并且保证数据在本地存储的安全和在传输过程中的安全。

（3）个性化专属平台。

可根据用户身份匹配访问权限，做到内网系统细致授权；可进行远程应用发布，以方便将业务系统迁移到移动终端，组织自由的安全私有化工作专属平台，实现实名化、组织