密级：■公开使用　□内部使用	**受控状态：**受控文件

IPSec/SSL VPN 综合安全网关
产品白皮书

版本号 **V2.3**

(2022 年 9 月版)

声明

一、本白皮书是IPSec/SSL VPN综合安全网关V2.3的产品说明书。本资料版权归北京数字认证股份有限公司所有。白皮书中的任何部分未经本公司许可，不得转印、影印或复印。

二、本资料将定期更新，如欲获取最新相关信息，敬请访问北京数字认证股份有限公司网站 www.bjca.cn 。

三、您的宝贵意见和建议请发送至：

北京数字认证股份有限公司

北京市海淀区北四环西路68号左岸工社15层

☎ 电话(TEL)：010-58045600

📠 传真(FAX)：010-58045678

📪 邮政编码：100080

✉ 电子信箱：market@bjca.org.cn

目录

1 产品概述

随着信息化技术的高速发展，网上证券、网上银行、电子政务、电子商务、OA 等应用逐步加深，与人们工作和生活息息相关的各种事项逐步从现场转向互联网上办理，海量的信息和数据以网络为媒介传输，在此背景下，如何实现重要信息、数据的安全传输和访问成为互联网业务应用面临的核心问题。

对于应用来说，在公共网络上传输敏感业务数据需要进行传输环节的机密性和完整性保护，以防止数据被泄露、篡改和破坏。

对密评检测来说，网络与通信安全、设备与计算安全、数据与应用安全需要确保数据传输与身份鉴别的安全性。

北京数字认证股份有限公司自主研发的 IPSec/SSL VPN 综合安全网关，可有效解决数据传输环节的机密性和完整性保护问题。

1.1 产品简介

IPSec/SSL VPN 综合安全网关是一款集数据传输加密、身份鉴别等功能于一体的应用网关产品，遵循国家密码管理局相关规范，采用国家密码管理局公布的 SM2、SM3、SM4 等国产密码算法。

IPSec/SSL VPN 综合安全网关主要解决数据传输安全问题，通过 SSL 反向代理、IPSec 隧道、身份鉴别等手段来确保用户接入、数据传输和内部网络资源的安全。可广泛应用于金融、公安、教育、卫生、政务以及交通等行业。

1.2 术语和缩略语

术语

名词	解释
SSL 协议	为网络通信提供安全及数据完整性的一种安全协议。
IPSec 协议	由 IETF 制定的端到端的确保基于 IP 通信数据安全性的一种网络层协议，可以提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

缩略语

缩略语	英文	中文
VPN	Virtual Private Network	虚拟专用网络
HTTP	HyperText Transfer Protocol	超文本传输协议
HTTPS	HyperText Transfer Protocol Secure	超文本传输安全协议

2 产品架构和技术特点

产品框架图

产品架构主要分为会话加速、通道加密、身份认证、密码加速、后台管理等部分；

- 会话加速：为代理应用服务提供 SSL 卸载、SSL 加壳、连接复用、高速缓存等功能，可有效提升应用服务器性能，增强处理效率。
- 通道加密：支持 HTTP、TCP、FTP、UDP 等传输协议；提供 SSL、TLS、DTLS、IPSec 等安全协议。
- 身份认证：支持基于国密证书的单双向认证方式
- 密码加速：产品具备硬件密码卡和密钥与配置管理功能；支持国密算法 SM2、SM3、SM4 等
- 后台管理：网关后台管理支持证书管理、黑白名单管理、状态监控、日志审计、负载均衡、热备/集群等功能。

IPSec/SSL VPN 综合安全网关具有以下技术特点：

- ✓ 功能丰富：集身份认证、数据传输加密等功能于一体，支持国密算法，通过 SSL 加密通道、IPSec 隧道、身份认证和权限控制等手段来确保用户接入安全、数据传输安全和内部网络资源安全。
- ✓ 可扩展性强：采用标准模块化架构，所有协议和接口均遵循标准规范，不改变企业现有应用结构，同时满足未来业务扩展的需要。
- ✓ 容易操作：对于管理员来说，界面操作方便快捷，功能逻辑清晰；对于用户来说，提供完全高效透明的服务。
- ✓ 安全性高：运用了加密、过滤、备份、冗余服务屏蔽等安全手段，建立健全的系统安全机制，保证系统本身的合法和安全。
- ✓ 遵循标准:

  GM/T 0022-2014　　《IPSec VPN 技术规范》

GM/T 0024-2014　《SSL VPN 技术规范》

GM/T 0026-2014　《安全认证网关产品规范》

GM/T 0028-2014　《密码模块安全技术要求》

GM/T 0039-2015　《密码模块安全检测要求》安全等级第二级相关要求

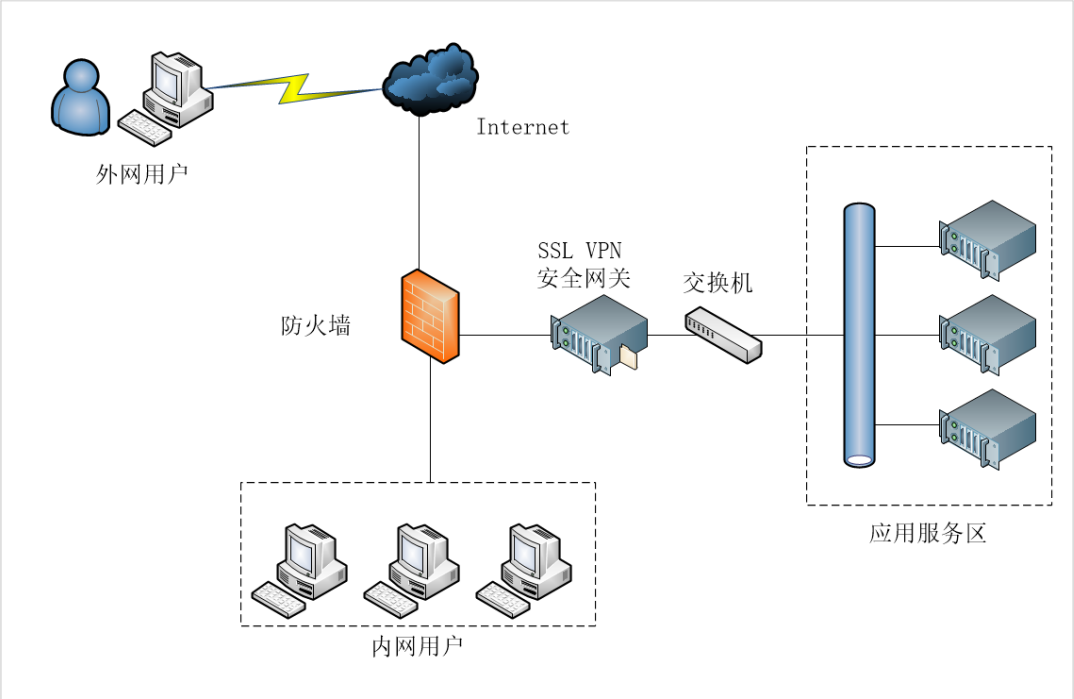
3 产品功能

产品功能	功能说明
主要功能	
SSL 代理	实现基于数字证书的服务器端与客户端的双向认证，多种形式的证书透传功能能够非常方便地在应用层实现基于数字证书的安全认证。
SSL 加速	全面提升 SSL 的处理性能，解决当前单向、双向 SSL 处理的瓶颈，可以极大地减轻 CPU 处理 SSL 加解密运算的负担，提高系统接入速度。
SSL 安全传输	支持在标准的 SSL/TLS 协议下，通过数字证书实现数据加密传输。
SSL 卸载	通过将应用访问过程中 SSL 的加解密过程转到 IPSec/SSL VPN 综合安全网关之上，从而减少服务器端的性能压力，提升客户端的访问响应速度。
HTTP 压缩	提高窄带宽访问应用的速度、保证服务质量。
WEB 高速缓存	基于内存的反向代理 Web 高速缓存功能，可以有效降低服务器的访问压力。
TCP 交付安全	支持 TCP+SSL/TLS 的安全传输通道交付服务，能够满足基于 SSL/TLS 安全协议的 TCP 网络应用系统，或是无安全策略的传统 TCP 网络应用系统，实现传输通道的快速安全保障与加速。
证书认证功能	
多站点证书	系统可以配置多个站点证书，不同的服务可以配置不同的设备证书。 支持 IPSec/SSL 证书一键导入。
多证书链	一个 SSL 服务可同时配置多条证书链，验证不同 CA 机构的用户证书。
多种证书支持	支持国内大多数第三方 CA 机构的数字证书。
证书信息传递	系统可以将用户证书信息包括扩展项信息传送给后台应用系统。
支持国密算法	支持 SM4 对称算法，SM2 非对称算法，SM3 摘要算法等国产密码算法。
证书状态验证	支持证书作废状态的 CRL 验证； 支持 OCSP 在线验证证书作废状态。
应用支持功能	

B/S 应用安全代理	支持 B/S 模式的安全代理，HTTPS 方式。
C/S 应用安全代理	支持 C/S 模式的安全代理，TCPS 方式。
双向 SSL 身份认证	支持双向 SSL 认证方式，客户端证书与服务器证书双方均需要相互认证。
单向 SSL 身份认证	支持单向 SSL 认证方式，只需要认证服务器证书。
多服务支持	系统可以创建多个 SSL 服务，保护不同的应用服务；也可以采用同一个 SSL 服务保护多个应用服务（需安装客户端）。
支持国际 SSL 标准协议	支持 SSL3.0、TLS1.1、TLS1.2 等国际标准协议。
支持应用重定向功能	支持在有防火墙 NAT 映射的情况下正常访问有重定向的网站。
管理功能	
WebGUI 管理控制台	基于 Web 形式的图形管理控制界面，可对设备进行管理、维护、监控等操作；支持数字证书登录及验证码功能。
管理员权限管理	管理员可根据需要来设置对应的管理权限，如不可修改操作但可查看系统信息等。
系统备份/恢复	可以备份当前服务配置，保证系统瘫痪时的快速恢复。
恢复出厂设置	系统具有恢复默认设置功能，方便使用。
日志管理	提供日志查看、条件过滤、导出等功能。支持日志告警。
日志发送	系统将日志以 SYSLOG 的方式发送到指定服务器。
软件升级	提供软件在线、离线升级，一键自动软件版本升级更新。
系统历史查询统计	支持对 CPU、内存、磁盘 IO、网络连接数、服务等资源使用情况信息的图形化统计。
系统自检	检查系统配置的正确性并生成正确性检查报表，用于快速地找出系统配置中可能存在的问题。
系统维护	支持 SNMP；支持基于 Web 方式的远程 SSH 访问； 支持基于 Web 方式的远程 SSH 访问；

4 产品部署

4.1 主路部署



主路部署图

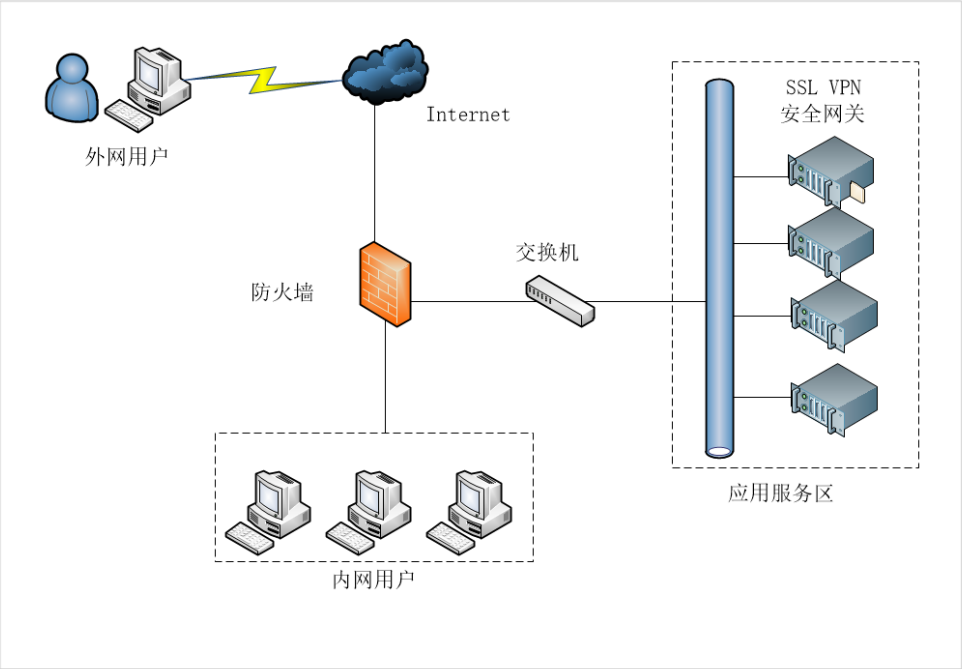
主路模式特点介绍如下：

1. 访问应用服务器使用的地址均归属于由 IPSec/SSL VPN 综合安全网关分配的地址，网关隔离用户和应用服务器间的直接联系从而保证了应用服务器区域的整体安全。

2. IPSec/SSL VPN 综合安全网关与应用服务器之间通讯均建立在加密通讯隧道基础之上，即使网络中存在信息窃取的非法行为，也只能获取到加密后的信息且无法解析信息内容，保证了应用系统用户信息隐私安全。

3. 该种部署方式需改变网络拓扑环境，属于双臂模式，由一个网口流入数据，另一个网口流出数据

4.2 旁路部署



旁路部署图

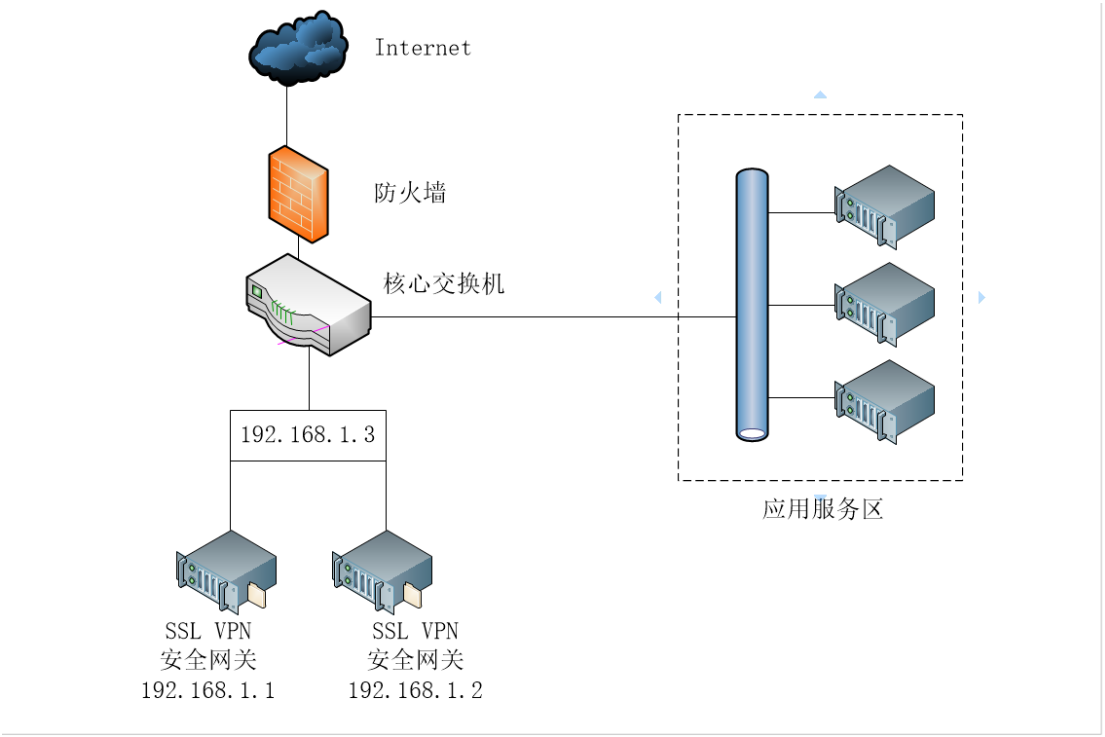
旁路模式特点介绍：

1. 与应用系统的高度兼容是该部署模式的主要特点，网关本身与应用系统部署的服务器存于一个网络区域中，可以灵活的调节用户是否需要通过身份认证才可对应用系统进行访问。

2. 该部署方式无需改造网络架构，属于单臂模式，同一网口进出数据。

4.3 多机热备部署

存在高可靠性需求的环境下 IPSec/SSL VPN 综合安全网关可以进行多机热备部署。热备部署至少需要两台同类型设备支持，逻辑上划分成一台主机，一台备机，两台设备都连接网络，两台设备之间使用虚拟地址漂移的技术调度用户访问的请求，在正常情况下由主机提供服务，当主机发生异常时系统自动切换到备机进行服务。部署方式如下图所示：



多机热备部署图

多机热备部署特点介绍：

1. 针对服务器的临时故障情况，可以避免长时间的服务中断，保证系统提供连续、可靠的服务。

2. 传统双机热备机制（“心跳侦测”机制）是使用网线（双绞线俗称“心跳线”）连接两台同类型设备互相监测设备的状态，IPSec/SSL VPN 综合安全网关的多机热备部署方案在稳定性及性能方面都优于传统的双机热备机制。

3. 支持自动回切功能。自动回切是指当主机宕机后服务主动切换至备机继续提供对外服务，在主机恢复正常运行状态后即自动的切换回主机。该功能是否启用可根据实际需求灵活配置。

5 产品规格

设备型号	CSG1500A	CSG3500A	CSG9500A
设备高度	1U	1U	2U

机箱开口	前置	前置	前置
尺寸规格（mm）	550 * 430 * 45 （长*宽*高）	550 * 430 * 45 （长*宽*高）	550*430*89 （长*宽*高）
重量	约 6.1KG	约 7.1KG	约 14KG
网络接口	4*1000M（可扩展）	4*1000M （可扩展）	4*1000M （可扩展）
电源（标配）	冗余电源	冗余电源	冗余电源
输入电压	100-240VAC	100-240VAC	100-240VAC
输入功率	400W	400W	550W
新建连接数(个/秒)	1,900	3,800	11,000
最大并发连接数(个)	130,000	275,000	555,000
国密吞吐率	500Mbps	800Mbps	2.2Gbps

6 产品优势

6.1 支持国密标准

- 支持国家密码管理局颁布《IPSec VPN 技术规范》（GMT 0022-2014）、《SSL VPN 技术规范》（GMT 0024-2014）；
- 支持国家密码管理局规定的国密 SM2/SM3/SM4 算法；
- 具有国家密码管理局颁发的商用密码产品认证证书。

6.2 强大的 SSL 性能和网络处理性能

- SSL 协议处理中使用了快速协议处理、快速证书解析、快速 CRL 解析等专有技术，大量减少证书处理和数据处理中的数据多次载入问题，最大发挥系统性能；

- 专业的硬件平台与专有的操作系统，提供了高速处理和并发能力；
- SSL 加速、HTTP 压缩、高速缓存、连接复用等前端加速功能提高系统整体响应速度，优化系统性能及用户访问体验；
- 反向代理架构和连接复用技术优化了服务器和客户端的 TCP 连接，可大幅度降低服务器的负载，极大地提高应用性能。

6.3 强大的 SSL 安全功能

- 身份鉴别高安全性，支持 SSL/TLS 协议族，支持单、双向身份认证，支持高强度加密算法，为应用提供可靠的身份认证方案，支持多种证书状态验证模式，包括 CRL（支持 LDAP、FTP、HTTP 协议）、OCSP 方式；
- 支持标准的 PKCS#10 证书请求、X.509V3 证书，支持国内外各大证书运营商的证书；
- 支持多种网络通信协议，与多种网络应用系统无缝集成，支持所有基于 TCP 协议之上的应用，包括 HTTP、FTP 等多种常用协议；
- 支持应用重定向功能，能根据用户证书属性进行应用重定向，限制或允许特定证书对应用的访问。

6.4 提高系统整体安全性

- 隔离对后台服务器的非法访问，全面的智能分析和控制功能（流量控制、应用重定向），实现按需访问；

- 内建完善的安全机制，可抵御 Dos、SYN Flood、Buffer Overflow Attacks、Parser Evasion Attacks、Directory Traversal Attacks 等恶意攻击；
- 全面的高性能网络地址转换（NAT），支持静态的基于端口的 FWD，隔离企业内网和外网，保护系统内网安全；
- 管理安全，产品支持主控端口方式管理、远程 SSH 管理、远程 Web 界面管理等多种方式，且可开启或关闭远程管理方式，产品支持多管理用户、支持一般查询和配置权限分级。

6.5 可维护性与集成性

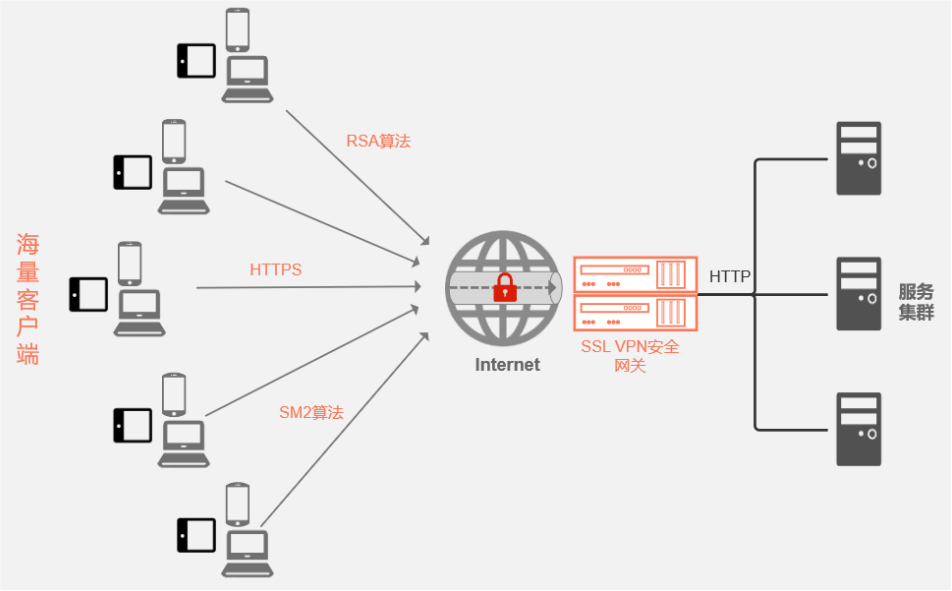
- 提供快速配置功能，可通过 Web 图形管理界面或简单易用的命令行界面，进行直观的配置和管理；实时监控图表可为排查问题、决策分析等提供参考依据；
- 具有强大的审计功能，提供包括系统、操作、访问和调试等详细的日志记录，可帮助管理员迅速的进行故障排查；
- 支持 SNMP、SYSLOG、RMON 和 Email 告警等功能，便于第三方网络管理软件集成，保障系统稳定运行；
- 具有按需定购的灵活性，能在不升级硬件的情况下增加负载均衡模块，具有高度灵活性和可扩展性。

7 产品资质

- 公安部产品销售许可
- 计算机软件著作权登记证书
- 公安部信息安全产品检测中心检测报告
- 商用密码产品认证证书

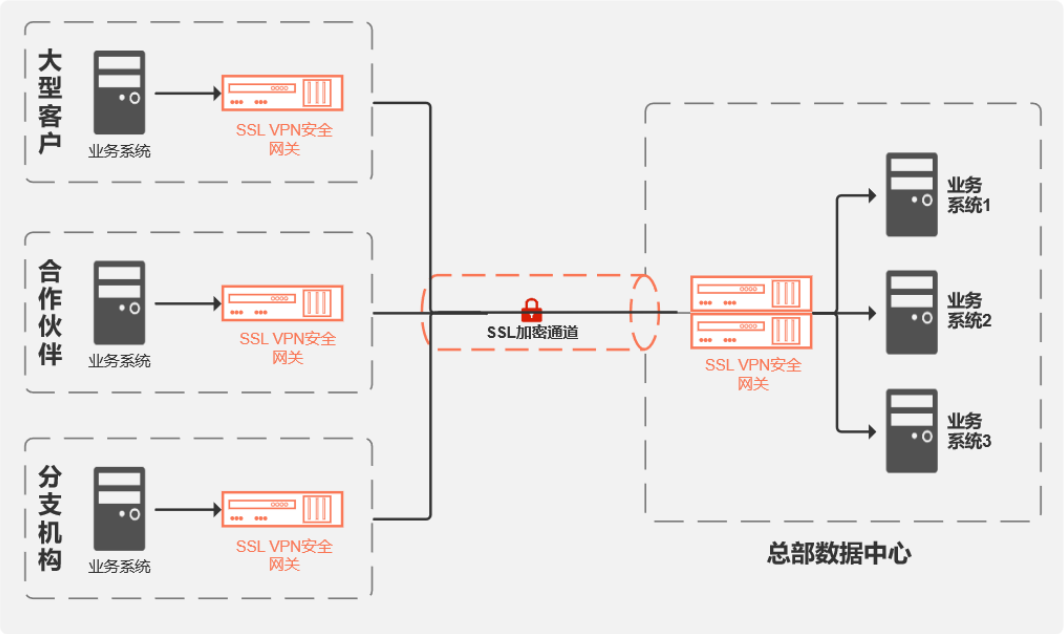
8 典型应用场景

8.1 WEB 应用 HTTP 转 HTTPS 场景



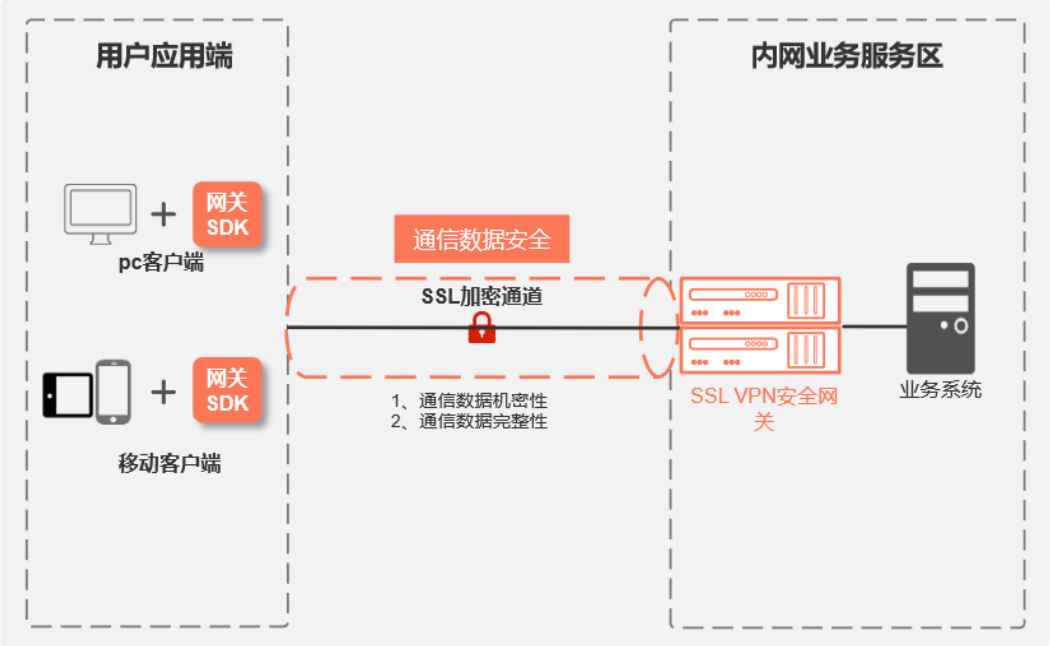
电子政务、电子商务或门户网站等需要将普通流量 HTTP 转为加密流量 HTTPS 访问。IPSec/SSL VPN 综合安全网关同时支持国密算法证书和国际算法证书，可通过使用不同的浏览器，实现不同算法访问。当用户使用普通浏览器访问时，网关将启用国际算法建立 SSL 通道，若用户使用国密浏览器访问，网关则自动切换至国密算法建立国密 SSL 通道，用户无需做任何操作。

8.2 网络安全互联（网关+网关）



网络安全互联场景用于机构间数据安全传输，确保数据传输的机密性和完整性，如数据中心与大型客户、分支机构、合作伙伴业务系统之间的数据传输，需要安全措施保障区域间数据传输安全。通过部署 IPSec/SSL VPN 综合安全网关，可以解决分支端到中心端数据安全传输问题，实现数据加密传输、连接复用、HTTP 压缩和 HTTP 改写等功能，并且支持 IPSec 隧道和 SSL 加密通道的安全协议。

8.3 应用安全互联场景（SDK+网关）



为了保证安全和合规，政府、教育、金融等领域业务系统需通过国密算法保障访问安全但大部分 PC 客户端和移动端不支持国密算法，业务系统支持国密算法也需要大量开发定制工作，研发成本高，开发周期长，开发和集成面临很大困难。通过部署 IPSec/SSL VPN 综合安全网关，并向用户终端提供国密 SDK 集成包，可以快速实现基于国密算法的 SSL 安全传输通道，提供安全服务的同时，极大地简化集成工作。