网络和通信-安全加密传输

主讲人：刘夏

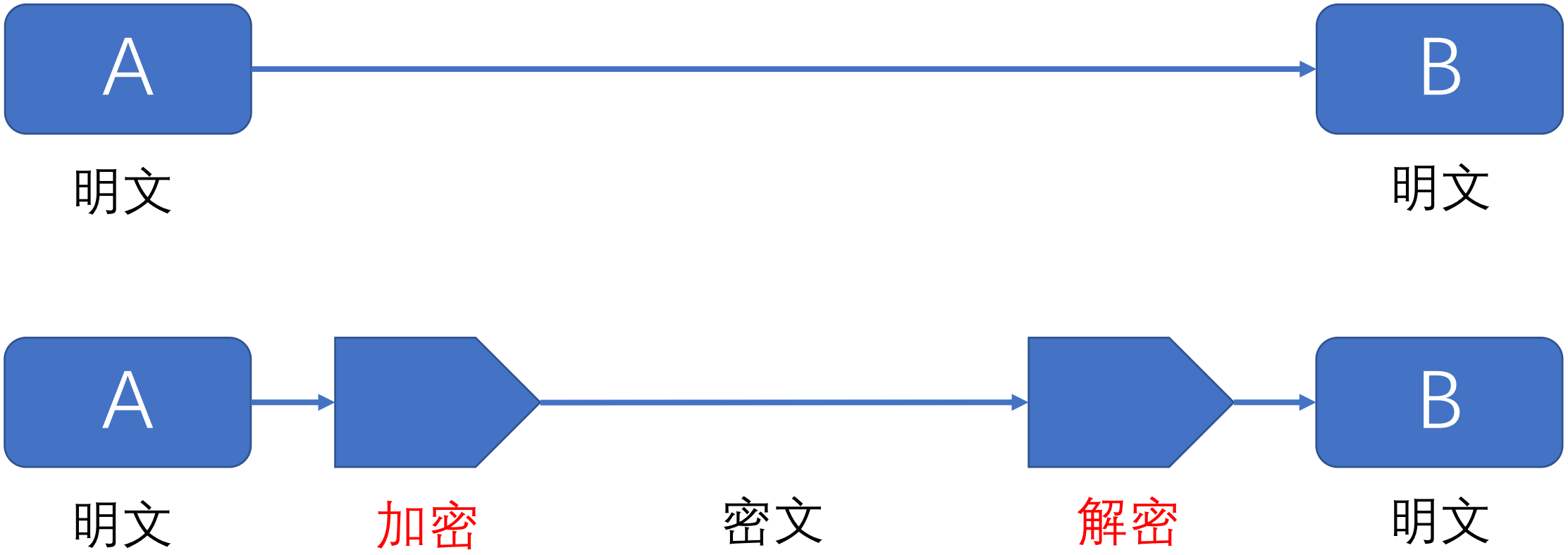
目录

CONTENTS

加密传输基本概念

PART. 01

1.1 加密传输概念



1.2 加密核心概念

3.1

机密性　confidentiality

保证信息不被泄露给非授权实体的性质。

3.2

数据完整性　data integrity

数据没有遭受以非授权方式所作的改变的性质。

3.3

真实性　authenticity

一个实体是其所声称实体的这种特性。真实性适用于用户、进程、系统和信息之类的实体。

真实性　机密性　完整性

1.2 国标39786条款

8.2 网络和通信安全

本级要求包括：

a） 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

b） 宜采用密码技术保证通信过程中数据的完整性；

c） 应采用密码技术保证通信过程中重要数据的机密性；

d） 宜采用密码技术保证网络边界访问控制信息的完整性；

e） 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性；

f） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

g） 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

1.3 加密算法在密评中

（3）问题描述：

[redacted]

[redacted]之间使用 https 协议建立通信信道，TLS 版本为 1.2，使用 AES256 算法实现集中管理通道中通信数据完整性；但所有密码算法、密钥管理均不符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。↵

1.3 加密算法简述

密码分类		国产商用密码	国际商用密码
对称加密	分组加密/块加密	SM1 SM4 SM7	DES IDEA AES RC5 RC6
	序列加密/流加密	ZUC（祖冲之）SSF46	RC4
非对称/公钥加密	大数分解		RSA DSA ECDSA Rabin
	离散对数	SM2 SM9	DH DSA ECC ECDH
密码杂凑/散列	完整校验	SM3	MD5 SHA-1 SHA-2

加密传输产品

PART. 02

2.1 VPN

VPN即Virtual Private Network
虚拟专用网络:

在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN可通过服务器、硬件、软件等多种方式实现。

2.1VPN产品工作逻辑

真实性 机密性 完整性

2.1VPN产品工作逻辑

先协商　　再工作

2.1 VPN产品类型

真实性 机密性 完整性

2.2 IPSecVPN技术架构

2.2 SSLVPN握手技术

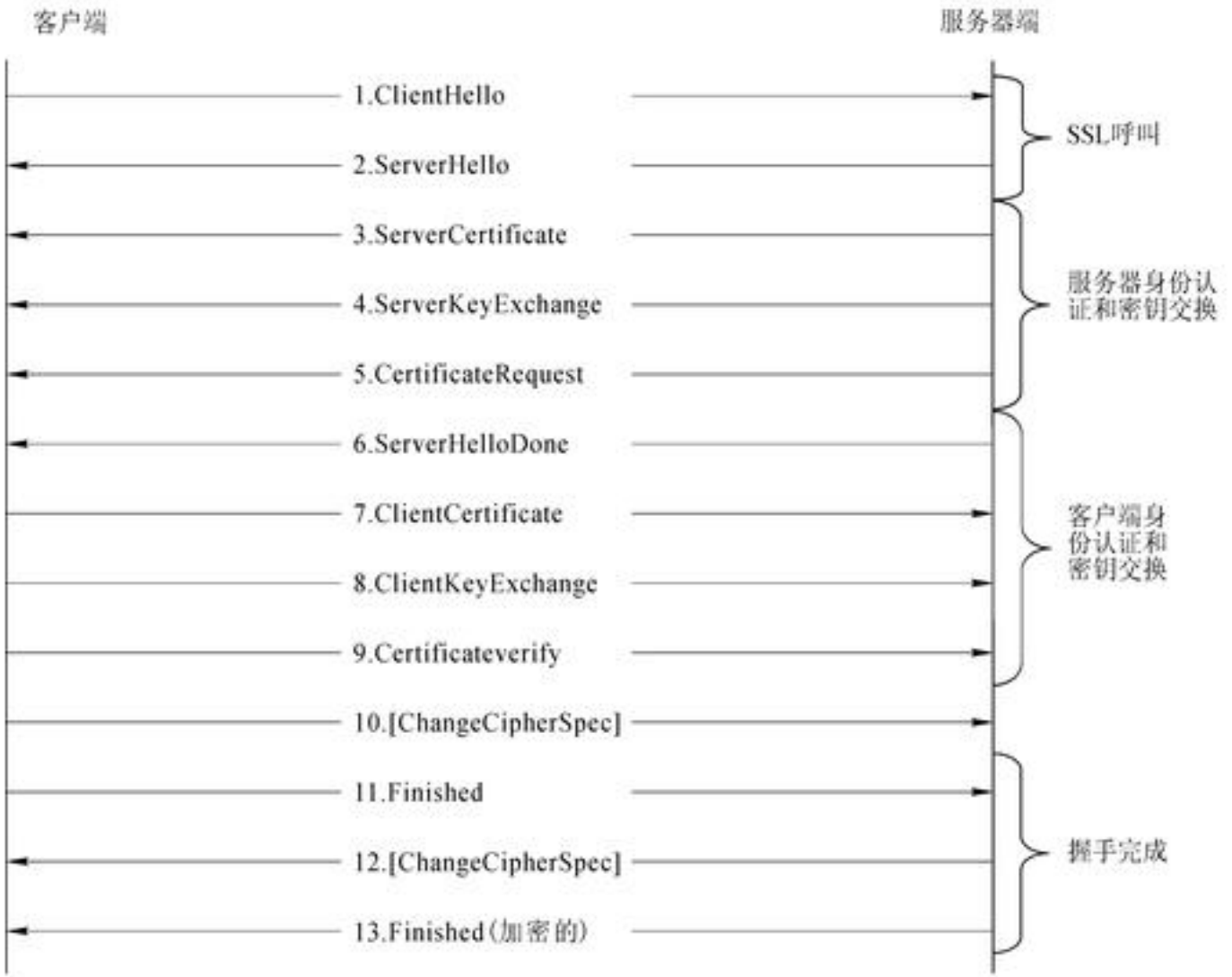
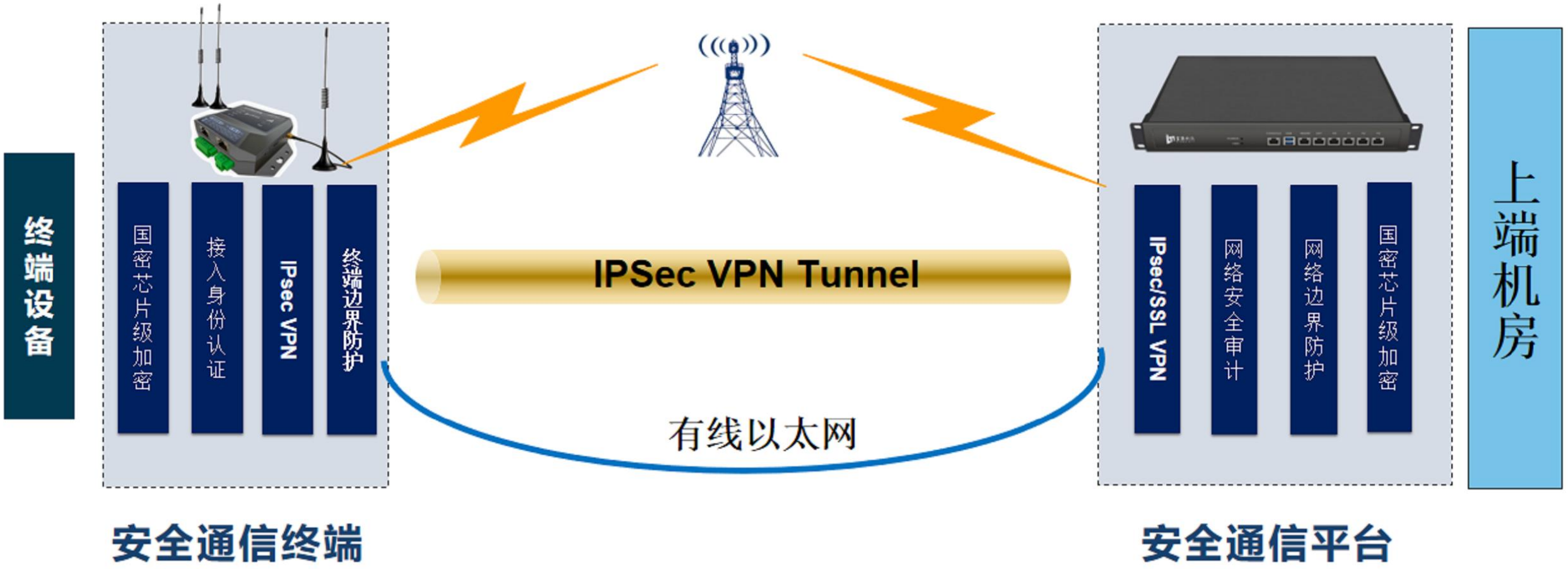
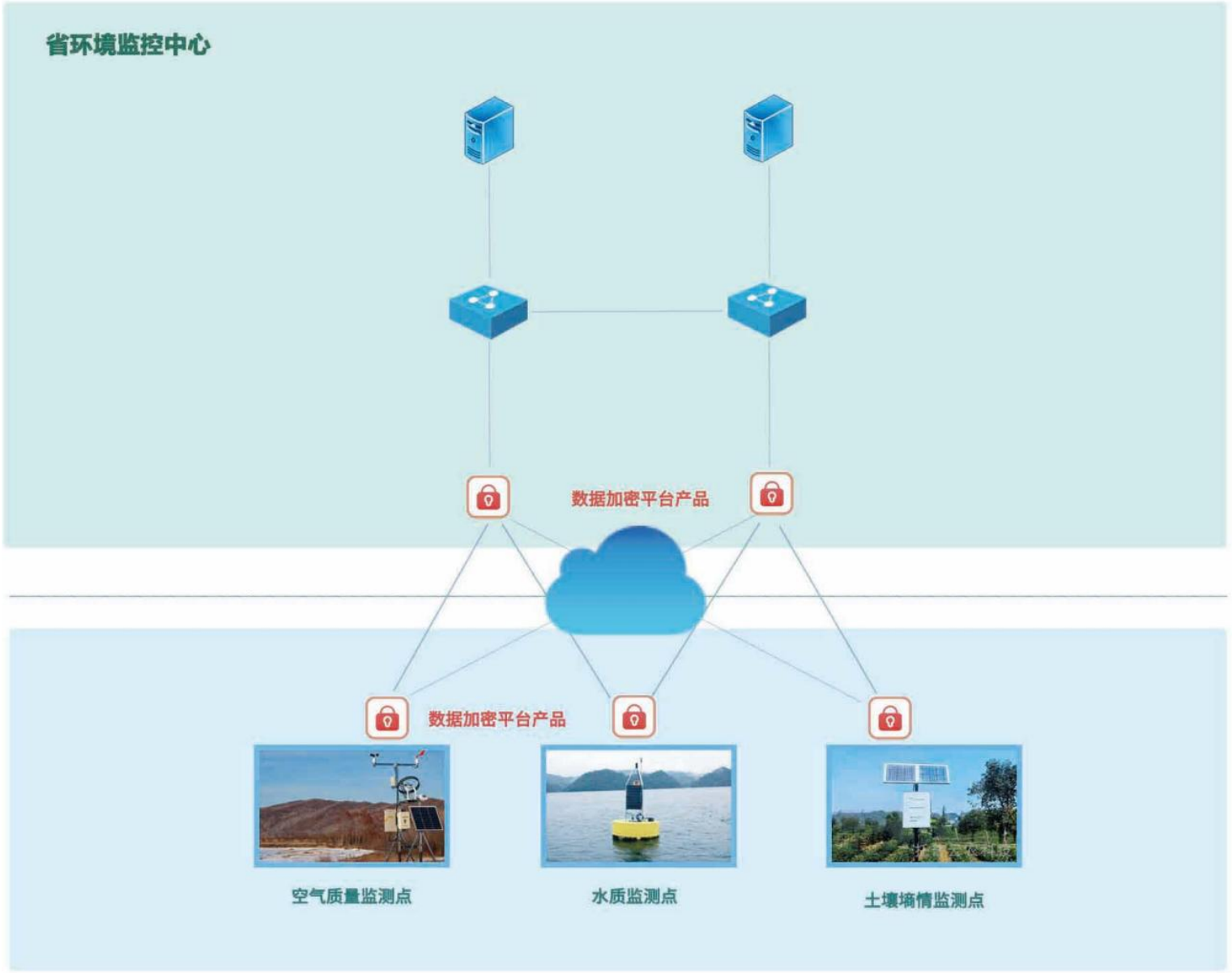


图 1　SSL 握手过程

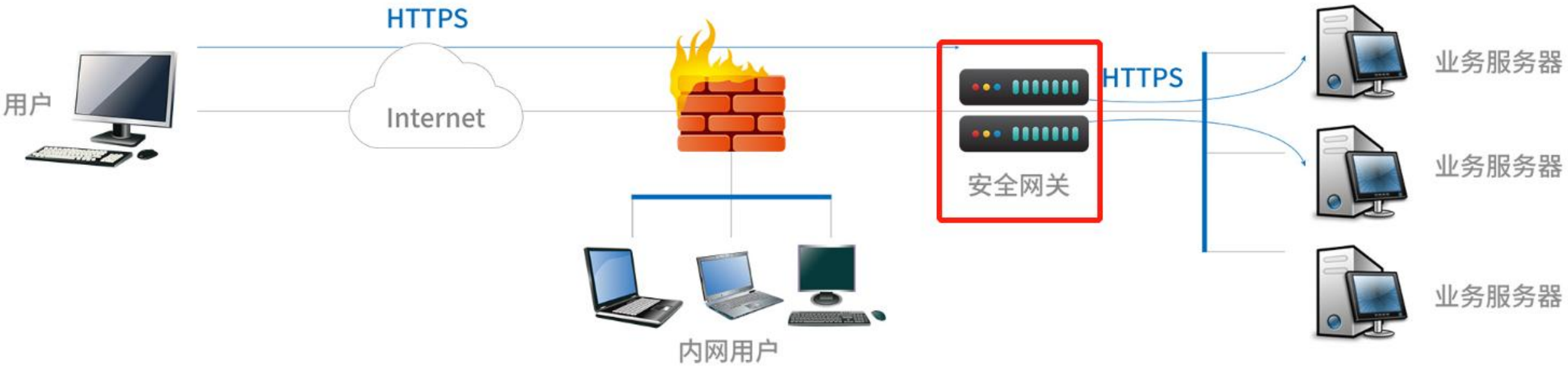
2.3 IPSecVPN架构图



2.2 IPSecVPN实际应用



2.3 SSLVPN架构图



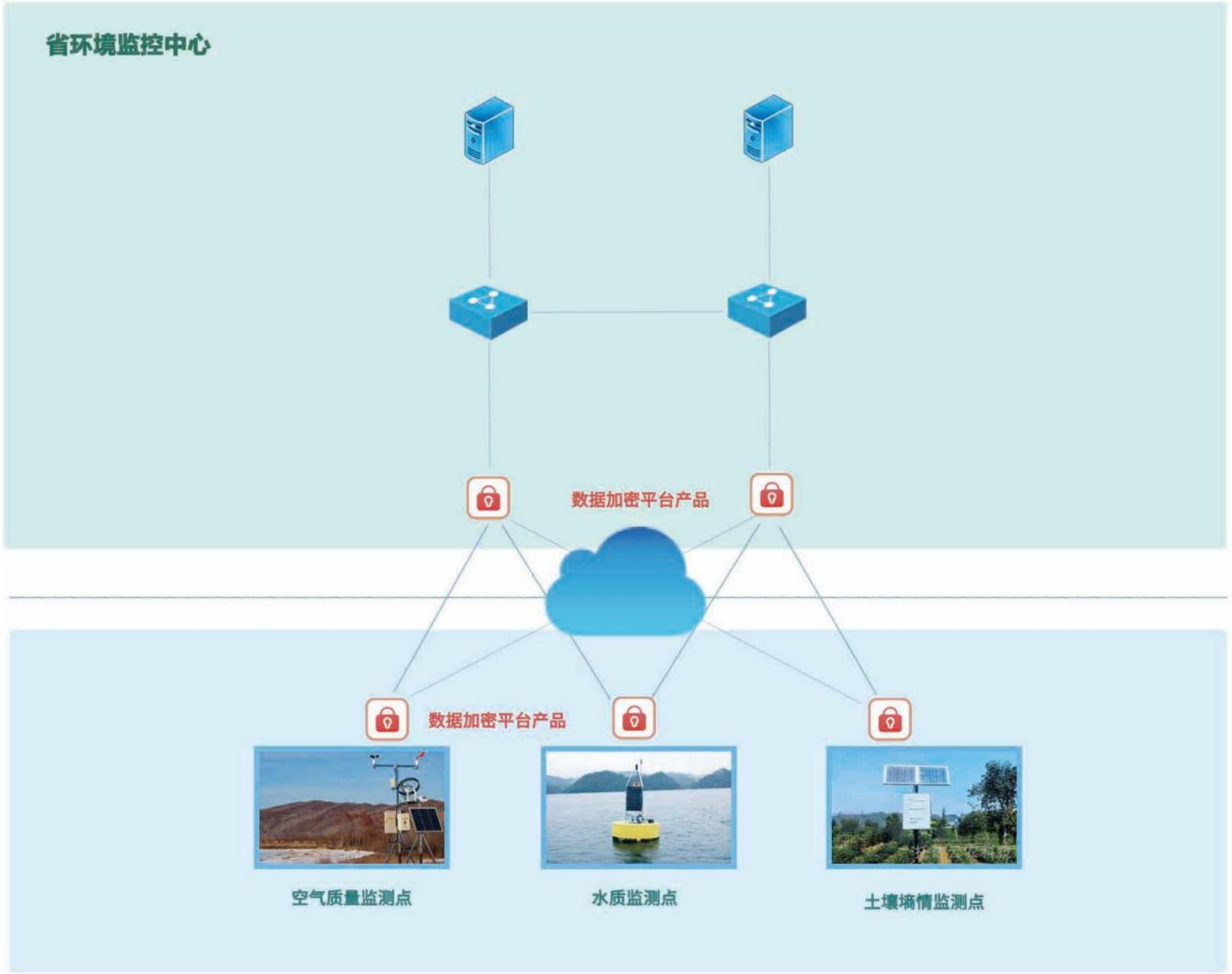
2.4 VPN技术总结

	IPSec VPN	SSLVPN
解决的问题	端到端	端到点
默认端口	500	443
使用协议	UDP	TCP
系统要求	无	操作系统（windows linux 等）
部署形式	两端部署	中心侧+终端软件

加密传输应用

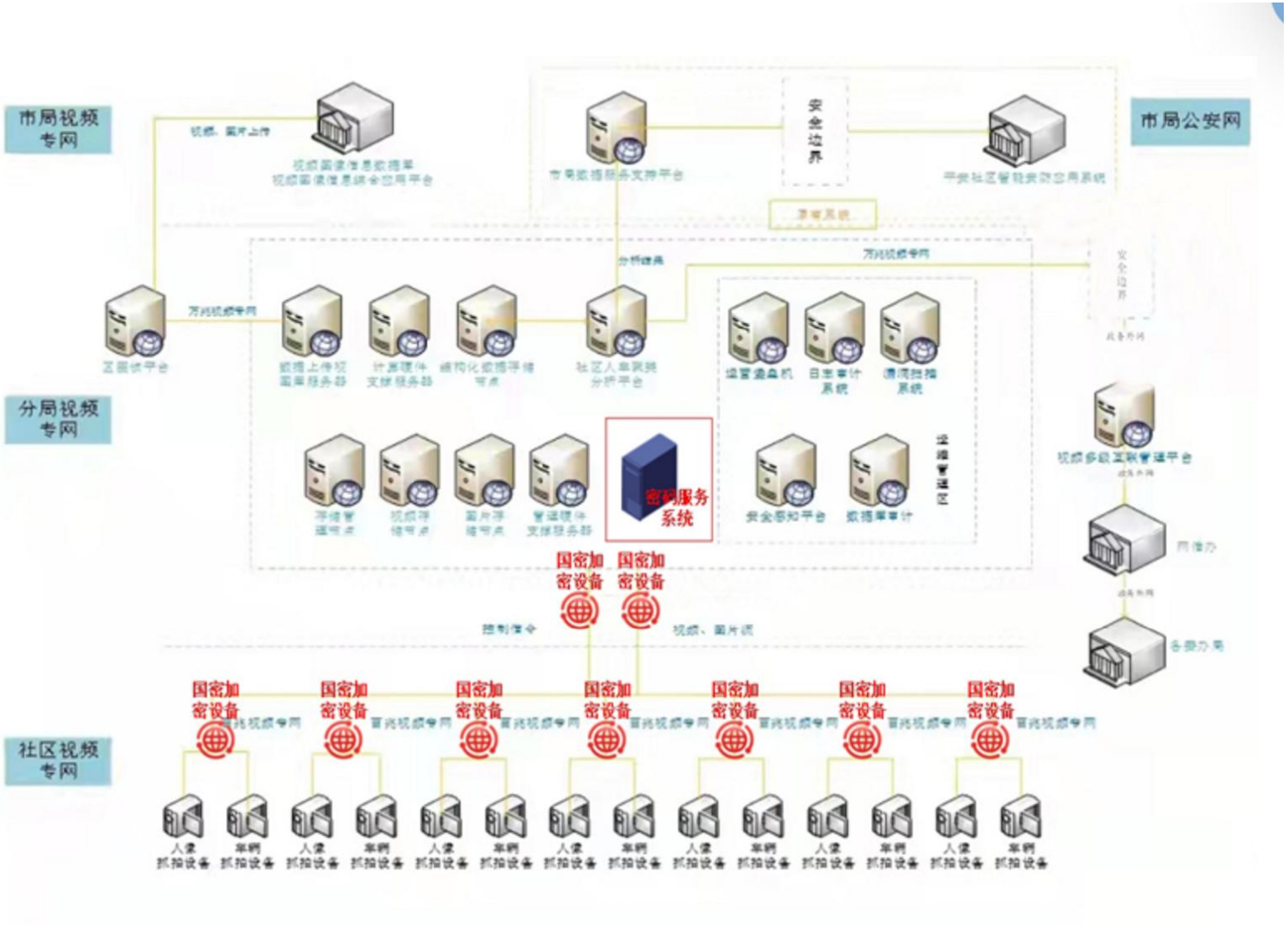
PART. 03

3.1IPSec VPN监测应用

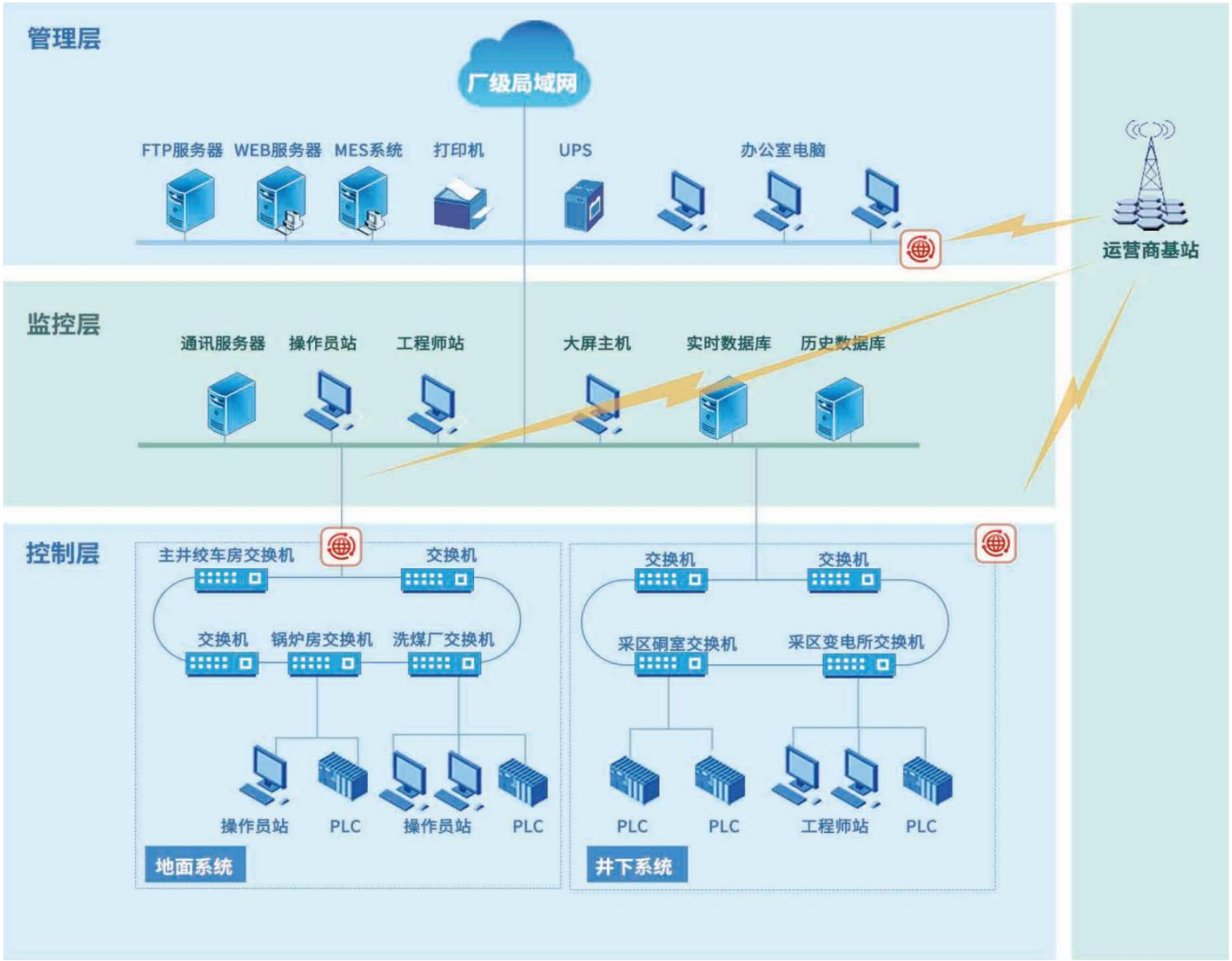


3.1IPSec VPN视频应用

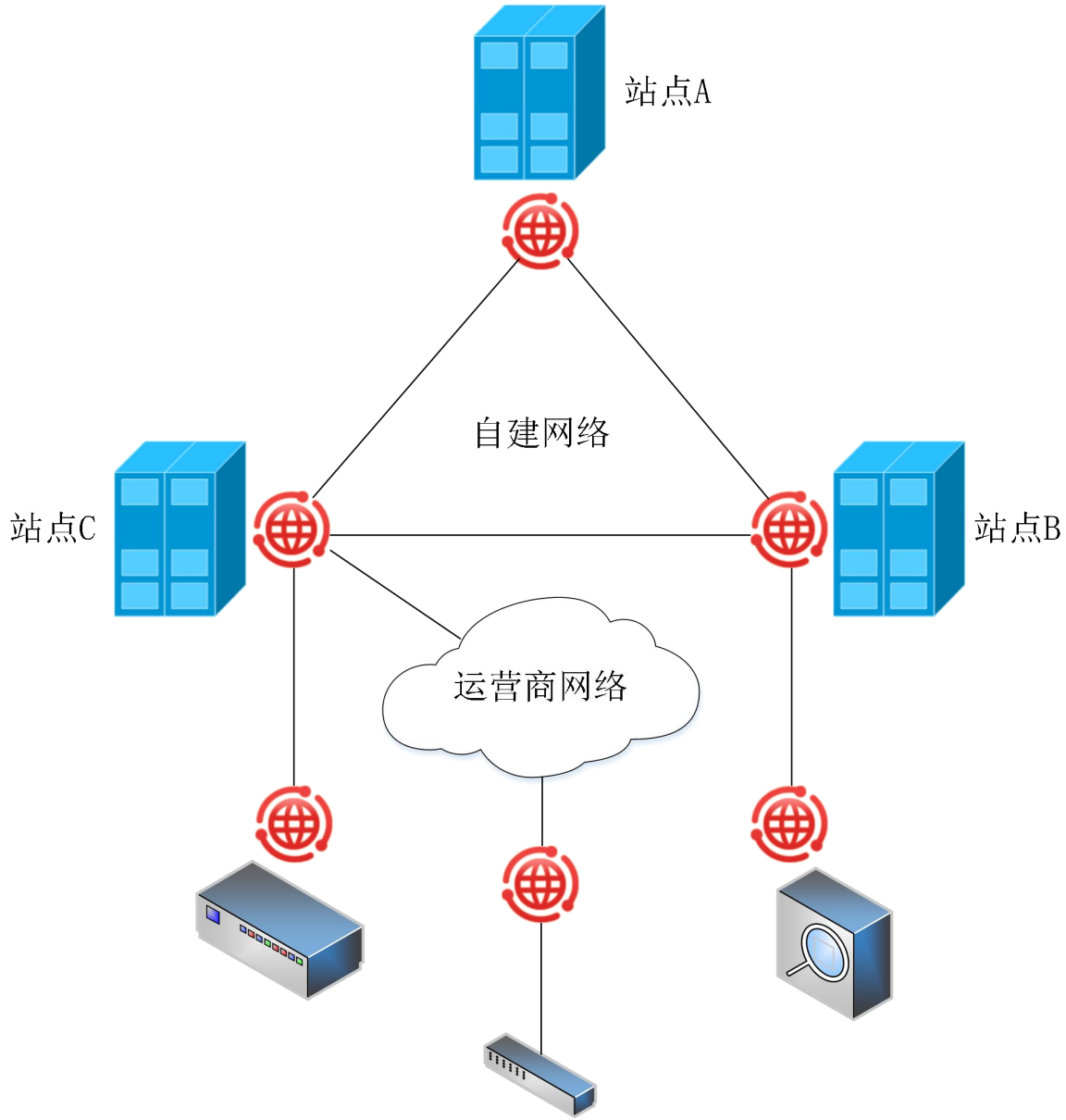
产品列表
国密门禁系统
视频监控系统
IPSec VPN终端
VPN综合安全网关
安全认证网关
服务器密码机
身份认证系统（CA一体机）
安全浏览器
智能密码钥匙
系统集成
软件开发
人员管理
规章制度



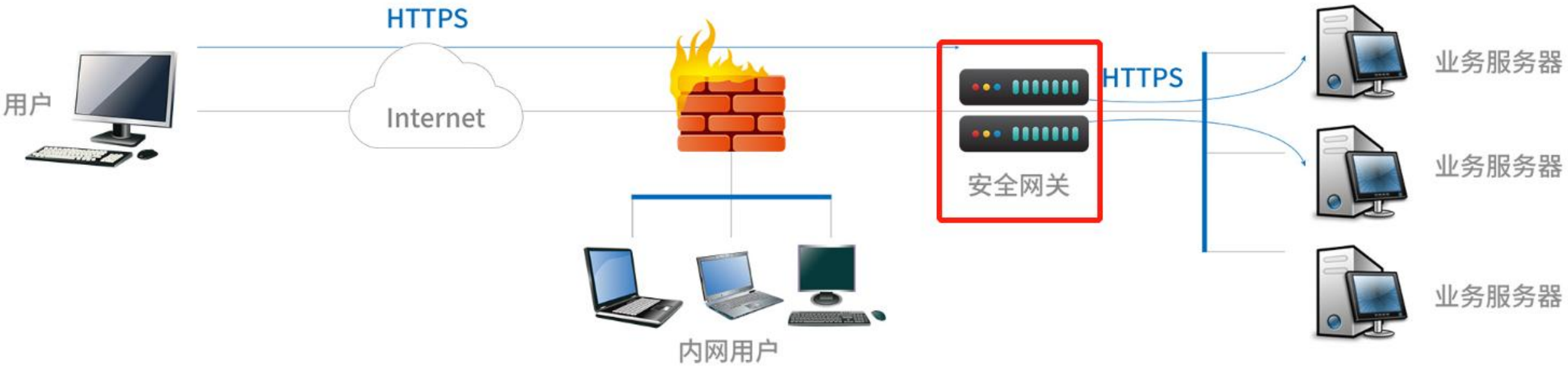
3.1IPSec VPN工业应用



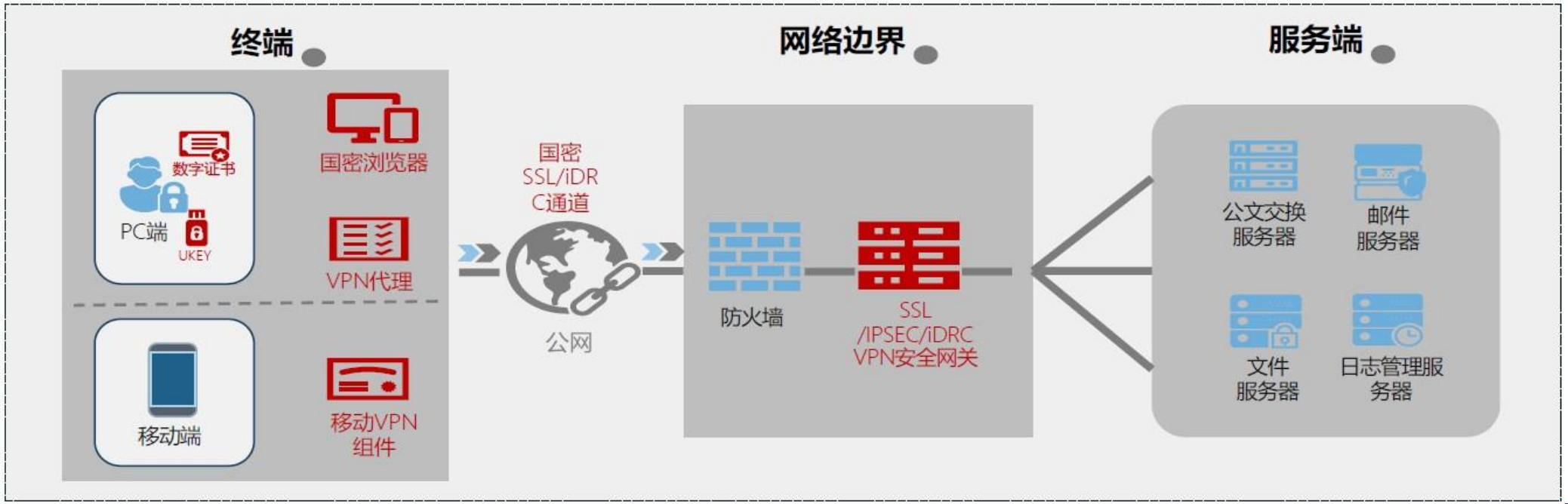
3.1IPSec VPN组网



3.2 SSLVPN应用场景



3.3VPN应用设计



网络和通信安全层面，密评要求指标：

①身份鉴别（应）

②通信数据完整性（宜）

③通信数据机密性（应）

④访问控制完整性 （宜）

⑤安全接入认证（可）

改造方案：

①通过国密IPSEC VPN确保人员身份的真实性

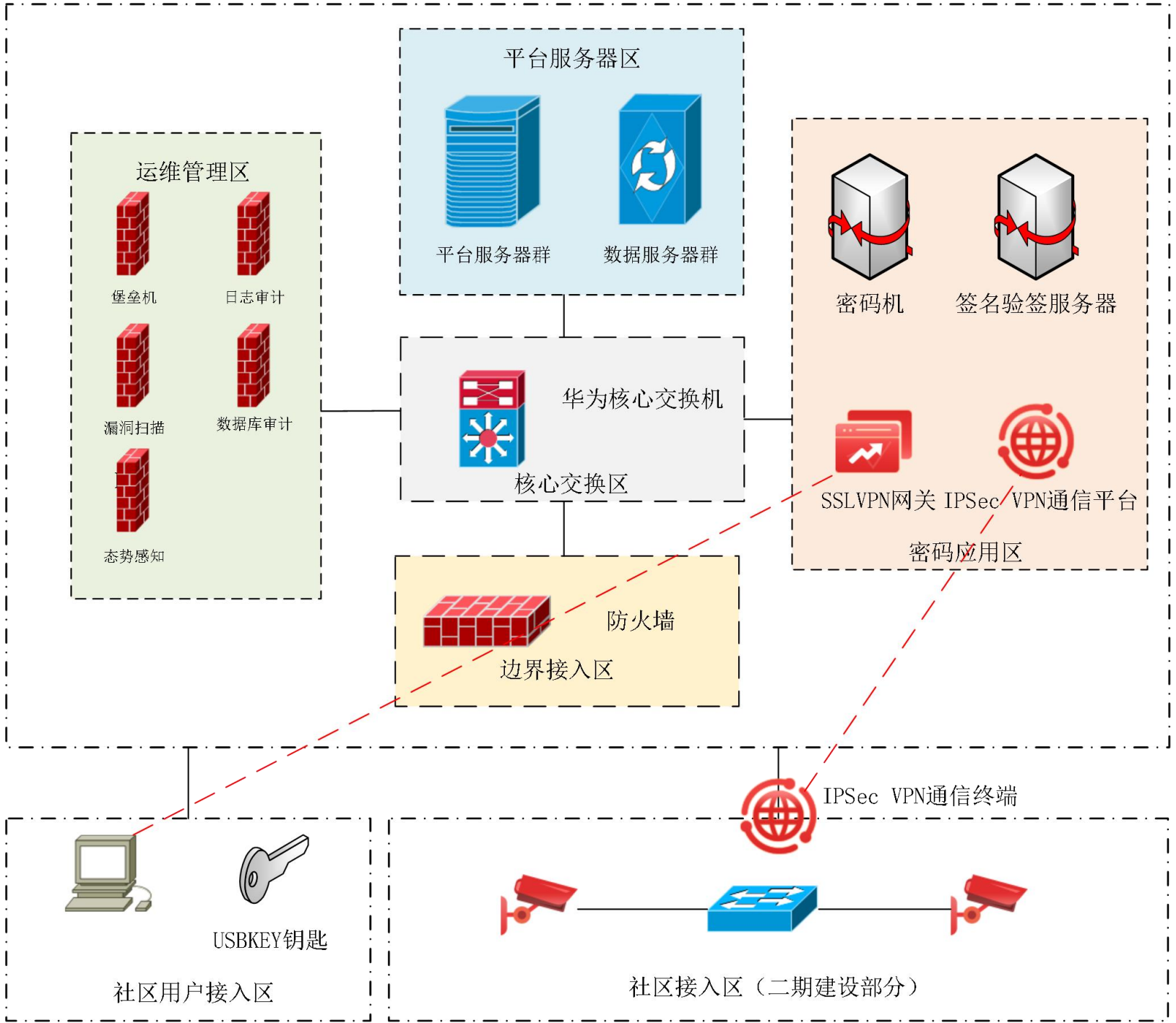
②安全网关在通信时通过SM3运算保障了数据完整性

③安全网关创建国密IPSec VPN通道保障了数据通信机密性

④安全网关通过SM3对网络边界访问控制信息做完整性运算

⑤通过安全网关的控制策略对外部接入设备进行权限认证

3.3VPN综合应用


平台服务器区
平台服务器群
数据服务器群
运维管理区
堡垒机
日志审计
漏洞扫描
数据库审计
态势感知
华为核心交换机
核心交换区
密码机
签名验签服务器
SSLVPN网关
IPSec VPN通信平台
密码应用区
防火墙
边界接入区
IPSec VPN通信终端
USBKEY钥匙
社区用户接入区
社区接入区（二期建设部分）

加密传输产品和密评

PART. 04

4.1 国标39786条款

8.2 网络和通信安全

本级要求包括：

a） 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

b） 宜采用密码技术保证通信过程中数据的完整性；

c） 应采用密码技术保证通信过程中重要数据的机密性；

d） 宜采用密码技术保证网络边界访问控制信息的完整性；

e） 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性；

f） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

g） 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

4.2 密评量化规则

表 2 测评指标权重表

要求维度	安全层面序号 i	安全层面	测评单元序号 j	测评单元	安全层面权重（w_i）	指标权重 $w_{i,j}$			
						第一级	第二级	第三级	第四级
密码技术应用要求	1	物理和环境安全	（1）	身份鉴别	10	0.4	0.7	1	1
			（2）	电子门禁记录数据存储完整性		0.4	0.4	0.7	0.7
			（3）	视频记录数据存储完整性		/	/	0.7	0.7
	2	网络和通信安全	（1）	身份鉴别	20	0.4	0.7	1	1
			（2）	通信数据完整性		0.4	0.4	0.7	1
			（3）	通信过程中重要数据的机密性		0.4	0.7	1	1
			（4）	网络边界访问控制信息的完整性		0.4	0.4	0.4	0.7
			（5）	安全接入认证		/	/	0.4	0.7

4.3 加密传输的意义

满足合法合规要求，明确责任和工作方法

提高安全意识，合理分配网络安全投资

强化传统防御方式，让安全建设更加体系化

感谢倾听！

天津市商用密码行业协会