网络安全

# 面向云计算的零信任国密安全网关技术方案及应用

张连营

（中国电信股份有限公司上海分公天翼云能力运营中心，上海 200120）

**摘　要：**针对网络安全威胁现状、传统边界安全防护策略及零信任国密安全网关架构及关键功能模块等进行了分析，提出了在云计算环境中通过国密零信任安全网关实现安全的通信网络、安全终端环境控制等，基于零信任架构的国密安全网关更加智能、灵活，能够适应现代网络环境的需求，是保障网络安全、商用密码应用的重要手段。

**关键词：**SDP；零信任；云安全；商用密码；国密

**中图分类号：**TP393

**文献标志码：**A

**doi:** 10.11959/j.issn.1000−0801.2025078

## 0　引言

当前，网络安全威胁正在不断演进，在网络安全边界的防护措施方面，传统的基于防火墙/SSL VPN模式的安全模型无法满足新的安全需求，基于零信任架构的网络安全解决方案可以解决云计算环境面临的网络安全威胁问题。即，通过将所有业务系统隐藏在软件定义边界（SDP）之后，SDP零信任安全解决方案提供了全面的安全防护，确保云计算环境下的核心资产和敏感数据不受外部威胁的影响。

此外，传统的加密算法和安全措施已难以应对当前复杂多变的网络环境，且存在被高级威胁绕过的风险。同时，依赖国际通用加密标准也存在潜在的技术风险，因此，推广使用国产密码算法（国密）成为保障网络信息安全的紧迫任务。为此，部署支持国密的零信任安全网关，不仅能够有效保护云计算基础设施和重要数据，降低安全风险，还能推动国密算法在更多网络场景中的应用。

## 1　需求分析

针对暴露面的攻击往往是攻击者重点攻击的目标，也是安全薄弱点，同时也是后续进行内部系统攻击的重要途径。业务系统的暴露面是指在网络中，业务系统所直接或间接暴露给外部的访问接口和资产，包括应用系统的IP地址、TCP/UDP端口、API等。传统的网络安全模型通常基于网络边界进行重点防护，但随着网络攻击手段的不断演变，单纯依靠网络边界已经无法提供足够的安全保障。

根据商用密码应用安全性要求，为了确保业务系统的安全，需要构建安全的通信网络，通过结合支持国家商用密码技术的零信任安全网关解决方案，在不改变应用系统对外提供的安全服务协议的情况下，利用符合密评要求的密码技术，通过加密传输为业务访问提供安全通道，并实现用户与安全网关之间的双向身份认证和远程通信的加密传输。

**收稿日期：**2024−12−15；**修回日期：**2025−03−10

根据等保等合规要求，解决方案需要支持“对内部用户非授权联到外部网络的行为进行检查或限制”“对非授权设备私自联到内部网络的行为进行检查或限制”等要求，传统的解决方案需要通过构建终端安全管理系统来实现，本文提出的解决方案可通过零信任架构的安全客户端来实现管理要求，对于非授权的网络内外部访问行为进行监控和控制。

该解决方案通过在云计算环境中建设基于零信任架构的国密安全网关，为运维人员实现以身份为中心的安全管理模式，全面提升云计算网络安全防护水平，为云平台及云租户业务顺利开展保驾护航。后续支持横向扩展能力可为分布在其他的边缘网络应用提供国密安全接入能力。

（1）客户端安全控制

客户端的安全策略可管控，已登录到云平台的授权终端将断开与其他网络（包括互联网）的连接，满足等保等合规要求。

（2）终端环境检测

安全客户端支持登录前的环境检测功能，检测内容包括后端资源是否可以访问、是否部署杀毒软件、是否更新系统安全补丁、虚拟网卡是否正常、端口监听是否正常、设备资源使用情况等。

（3）多因素认证

除账户/口令外，支持数字证书（Ukey）、手机短信验证码等多种认证方式。支持自定义短消息内容的多因素认证，在对接短信网关时，需遵循短信对接规范。

## 2　技术实现方案

### 2.1　零信任国密安全网关架构体系

零信任国密安全网关网络系统功能架构遵循国际云安全联盟（CSA）制定的零信任架构，相关的密码技术均采用符合国家密码管理主管部门认证核准的密码技术和产品，支持云化部署或硬件部署，支持软件组件分离部署，包括控制器与安全网关的分离、控制平面与数据平面分离，以实现完全可扩展的系，提供纵深一体化的零信任安全防御体系。零信任整体架构如图1所示。

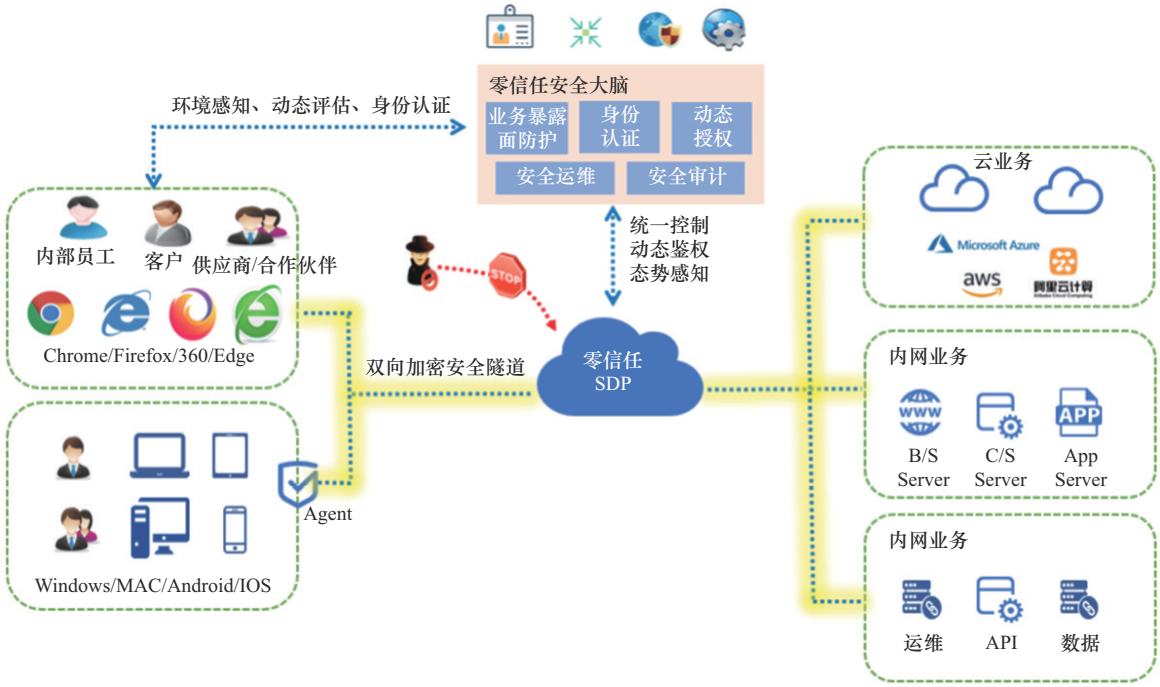


图1　零信任整体架构

（1）零信任控制器

实现可信云平台用户和云租户接入和管理及基于业务策略的动态权限管控下发。零信任控制器可与现网部署的 4A、IAM、Radius、LDAP、AD 等平台对接协同完成认证，并对所有客户端的连接信息进行日志审计，基于用户身份和终端信息，结合动态策略的下发实施“最小化”的权限管控和严格策略的动态访问控制。

（2）国密安全网关

SDP 采用先认证、再准入原则，动态、按需、最小化实现网络应用安全连接与访问。默认情况下，国密安全网关将拒绝来自零信任控制器以外的所有主机的所有通信。只有在零信任控制器得到指示后，国密安全网关才接受来自客户端的连接，从而实现云内业务系统和服务本身的网络隐身，降低“暴露面”安全管理风险，同时，国密安全网关基于动态安全策略实施云用户访问的合法性和安全性管控，国密安全网关在零信任网络架构中承担关键的枢纽作用。国密安全网关应包含数据加密传输、IPv4/IPv6 双栈、通信控制等功能。

（3）国密零信任客户端

通过让用户登录统一应用入口，实现对云用户接入终端侧环境安全的管控。作为零信任架构的重要组件，国密零信任客户端可支持多终端多操作系统适配，并搭载多种身份认证方式，除账户/密码外，支持 SM2 国密证书+口令认证、手机短信验证码、一次性口令、邮箱验证码、企业微信/钉钉扫码等多种认证方式。同时，支持双向身份认证方式，支持身份鉴别信息完整性保护，此外，实现对终端软件信息、IP 地址和硬件 ID 等信息进行采集上报。零信任国密安全网关架构如图 2 所示。

零信任国密安全网关内置密码卡，客户端可采用智能密码钥匙等方式，支持国密算法（SM2/SM3/SM4），满足国家对密码产品的国产化要求。

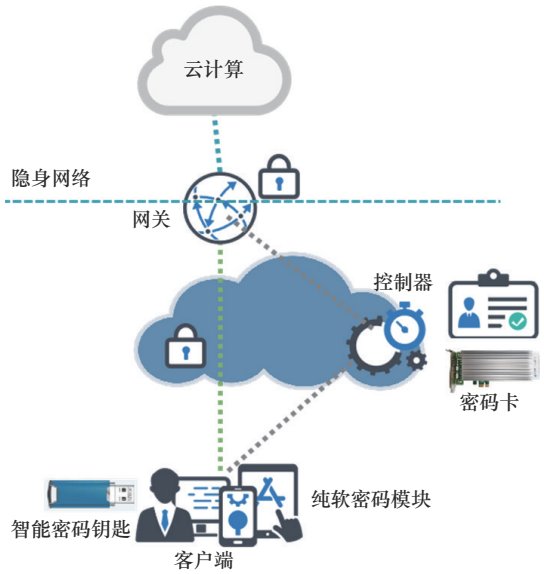


图 2　零信任国密安全网关架构

## 2.2　技术实现方案

通过零信任国密安全网关实现用户的远程通信安全合规应用，实现移动办公接入、平台访问控制等安全需求，实现用户可信身份认证、数据加密传输等功能，零信任国密安全网关部署架构如图 3 所示。

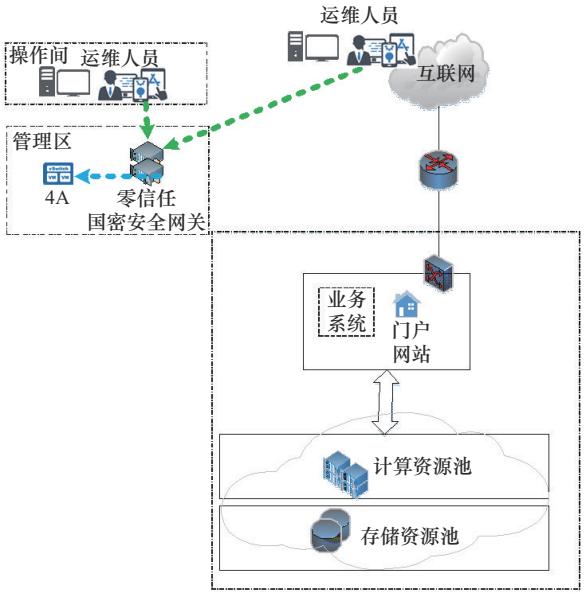


图 3　零信任国密安全网关部署架构

客户端、零信任国密安全网关（简称网关）、连接器和控制器。其中控制器、网关、连接器三者应分离，以实现一（客户端）对多（网关）对多（连接器）的分布式网络架构，提高网络的可扩展性和可用性。控制平面和数据平面应分离，以实现高可靠性。

国密安全网关内置密码卡，逻辑网络架构如图4所示。

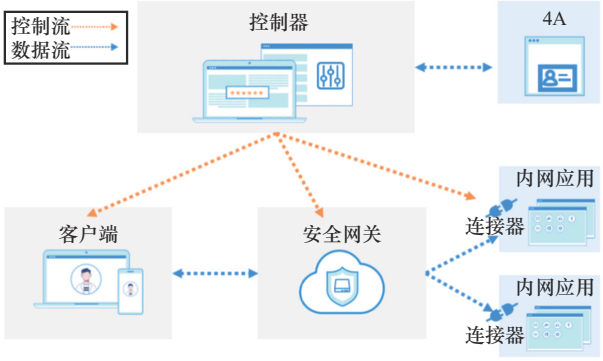


图4　国密安全网关逻辑网络架构

（1）客户端：客户端与控制器通信以请求它们可以连接的网关列表及权限列表，并具备网关网络质量探测和故障自动切换调度能力。客户端须向控制器提供诸如硬件ID、本机终端软件及版本、补丁更新情况、IP地址、Wi-Fi信息、DNS、地址位置之类的信息，以便控制器检查客户端身份是否合法。

（2）控制器：控制器对所有网关、连接器、客户端进行管理，制定安全策略，确定哪些客户端可以与哪些业务进行通信。控制器也可以将所需要的信息中继到外部认证服务，例如现网部署的4A系统进行认证。控制器同样需具备日志审计功能，对所有客户端的连接信息和访问行为进行日志记录及审计。

（3）国密安全网关：安全网关为靠近用户侧的主体网关，具备分布式边缘部署能力，用户能在任意位置就近接入、就近安全防护。默认情况下安全网关拒绝未经过身份验证的所有通信，只有在校验合法身份后网关才放行通信。安全网关具备网络隐身、访问控制、应用访问自动选路、访问代理、传输加密等功能，在所有访问主体对目标客体资源进行访问之前，都必须通过国密安全网关的预认证，预认证的目的是确认用户及其终端是否安全可信。在确认是合法用户、合法终端、安全环境后，建立客户端与国密安全网关之间的加密隧道，为后续的网络访问行为做准备。国密安全网关内置密码卡，支持SM2_SM4_SM3隧道模式，支持国密标准SSL/TLS协议，安全网关应具备动态弹性扩缩容能力，并具备扩展成安全服务边缘的能力，支持对远程访问、移动办公等场景的互联网访问安全防护。

（4）连接器：连接器部署在应用网络侧，靠近被防护的云应用资源，是安全网关的延伸。具备反向连接、网络隐身、传输加密、身份验证等功能。连接器需要支持快速部署和低资源占用，适应应用业务快速变化的特性，支持在分钟级别即可将新的业务节点接入到零信任网络，具备零信任访问和防护能力。

#### 2.2.1　基于SPA网络隐藏技术

单包认证（single-packet authorization，SPA），是一种轻量级的认证协议，遵循RFC4226，SPA是SDP的重要核心组件，Client-Controller、Controller-Gateway、Client-Gateway之间都采用了SPA单包认证方式进行认证。零信任SDP通过SPA端口敲门实现只有合法身份的用户才能访问服务端口，默认情况下该敲门服务将拒绝一切不合法的连接请求，只响应通过校验的合法报文并进行校验与控制。

采用单包认证技术可以实现暴露面安全控制。业务系统的暴露面是指在网络中，业务系统直接或间接暴露给外部的访问接口和资产，包括应用系统的IP地址、TCP/UDP端口、API等。传统的安全模型通常基于网络边界进行防护，比如传统的VPN必然会暴露服务的IP及端口信息，

无法避免恶意的扫描及暴露渗透等攻击风险。单包认证可以实现服务与目标资产的隐藏，通过与防火墙结合，利用动态防火墙技术进行防护，使非认证用户或来自外部的攻击者无法通过端口扫描发现完全网关的IP及服务端口，从而实现服务及资产的隐身，满足暴露面管理要求。

此外，零信任安全防护只有对通过身份认证的用户才做报文响应，认证失败也不做任何响应，从而可以抵御各种DoS/DDoS攻击，通过服务及资产隐身，可有效抵御针对控制器和网关的DoS/DDoS的网络攻击。

零信任国密安全网关基于新一代安全架构进行创新与实践，保障端到端网络与信息安全，将云业务、云网络资产等从互联网上隐藏起来，通过接入安全认证、动态防火墙、国密加密双向隧道等技术隐藏真实网络，攻击者无法攻击不可视的攻击目标，因此极大地提高了攻击门槛与代价。

2.2.2　安全传输功能

国密安全网关支持SM2、SM3、SM4密码运算、随机数生成等功能。密码运算功能由内置的密码卡提供，随机数生成由密码卡上的两个WNG8数字物理噪声源芯片提供，确保所有的加密操作和密钥生成都是基于真正的随机数，提高了系统的安全性。

参考国家商用密码管理和零信任标准规范相关要求，SDP国密安全网关以身份为中心进行动态访问控制，以“先认证，再连接”的方式，实现更加严格的访问准入控制，保障云计算网络信息安全。软件遵循技术标准，符合GM/T 0028-2014《密码模块安全技术要求》安全等级第二级，采用经国家密码管理局认可国密标准SM2、SM3、SM4的算法，并符合相关密码标准规范，具备密码应用功能，在云计算平台及业务安全准入控制、浏览器安全访问、移动安全管理平台等领域进行广泛应用。

为实现用户终端安全防护，系统支持采用安全终端或SDK嵌入方式，与国密安全网关控制器形成可信的用户身份认证，并对接入终端信息进行检测与核查。客户端上线向控制器发起单包认证（SPA）请求。每个客户端生成一批加密因子，客户端与控制器使用一套相同的算法根据时间，客户端环境可以计算出当前使用哪个加密因子，结合时间生成一个密钥，然后使用国密标准SM4加密算法加密身份验证报文。

国密安全网关实现了和用户客户端双向身份认证，即安全网关认证用户，用户也要认证安全网关，实现客户端远程通信的加密通信，支持国密算法SM2、SM3、SM4等进行隧道加密传输。

2.2.3　安全客户端

国密安全网关客户端支持Windows/MAC、Android、Linux及SDK等形态，结合环境感知模块基于动态的策略，对终端用户进行权限管控，资源访问控制等。

安全客户端通过与控制器、网关进行有效联动，有效保障了访问后端业务系统的安全。国密安全客户端主要为实现终端安全防护，支持采用安全终端App或SDK嵌入方式或B/S形式，与零信任国密安全网关内的控制器形成可信的用户身份认证，并对接入终端信息进行检测与核查，确保它们满足组织的安全策略，包括检查操作系统和应用程序的更新、防病毒软件的安装、防火墙规则的配置等，同时可实现终端安全基线扫描，帮助用户全面了解终端运行环境的安全性以及实现安全准入控制，保证接入终端的可靠性，从而实现在终端访问应用资源的动作是一个安全的、可溯源的、可管可控的过程。

客户端结合单包敲门技术以及多因素认证控制，与国密安全网关控制器验证成功后，在指定时间段内访问网关，与网关建立一个隧道，客户端与隧道的交互使用国密标准SM2握手，握手过程中生成SM4对称密码为以后的隧道数据加密使

用，通过隧道访问的资源网关都会判断用户有无访问资源的权限而进行放通或禁止访问。

安全客户端主要功能同需求分析部分所述。

## 3 结束语

随着云计算、大数据等技术的广泛应用，基于零信任架构的国密安全网关更加智能、灵活，能够适应现代网络环境的需求。越来越多的企业网络和云计算环境开始重视并部署支持国密的零信任安全网关，以应对复杂多变的网络安全环境，确保网络信息资产的安全与稳定。这一举措不仅符合国家信息安全战略，也顺应企业数字化转型的发展需求，是保障网络安全、推动商用密码应用、促进信息化发展的重要手段。

## 参考文献：

[1] 安全运营 . 浅谈零信任 SDP 架构下的服务隐身设计[EB]. 2021.

[2] 左英男 . 零信任架构在关键信息基础设施安全保护中的应用研究[J]. 保密科学技术, 2019(11): 33-38.

[3] 王群, 袁泉, 李馥娟, 等 . 零信任网络及其关键技术综述[J]. 计算机应用, 2023, 43(04): 1142-1150.

[4] 国家市场监督管理总局, 中国国家标准化管理委员会 . 信息安全技术 信息系统密码应用基本要求: GB/T 39786-2021[S]. 2021.

[作者简介]

**张连营**（1972– ），男，中国电信股份有限公司上海分公司天翼云能力运营中心正高级工程师，主要研究方向为网络信息安全、商用密码应用等。