腾讯智慧安全
行 业 安 全 解 决 方 案

腾讯 T-Sec

应用级智能网关

腾讯科技有限公司

2019 年 11 月

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

腾讯科技有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但腾讯科技有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

目录

第1章 序言

随着全球数字化转型浪潮的到来以及威胁环境的持续变化，云计算、大数据、物联网等技术推动 IT 架构发生巨变，网络边界是企业安全体系的第一道防线，边界防护通过在网络中实现安全域隔离、精细化控制和实时攻击阻断，提供安全架构、被动防护等核心能力的支撑，其在纵深防御体系中占有极为重要的战略地位。

网络与安全的界限日益模糊，网络与安全重叠的部分越来越多，网络与安全的重叠让企业网络架构变得更加复杂，网络边界上的业务和应用也面临新的挑战。互联网和企业内网之间，企业内网不同网段之间，需要在网络安全隔离前提下，迎合物联网、5G 网络等新技术发展趋势，更好的保障安全的同时，实现业务系统/应用系统的高效互联互通。

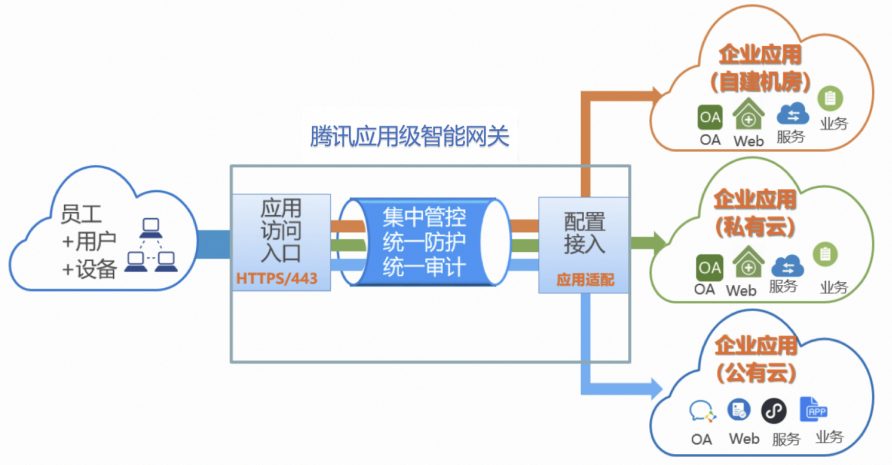
第2章　产品简介

2.1 T-Sec 应用级智能网关

应用级智能网关是腾讯智慧安全针对企业安全上云和数字化转型提供的企业网络边界处的应用访问管控和安全防护系统，应用级智能网关针对企业应用提供统一的安全高效的访问入口，在恶意威胁进入企业网络之前监测和阻止，有效保护公司核心业务和数据，切实解决企业应用在边界处的现实安全访问问题。

腾讯应用级智能网关支持公有云和私有云模式，支持企业应用从自建机房 IDC、企业私有云和公有云等各种方式接入，灵活适配。

应用级智能网关通过应用层数据安全防护加身份验证技术，让内网业务统一以 WEB 的形式被外部授权用户访问，也可以 API 接口的形式被调用，可实现对访问者和访问资源的细粒度控制，以单个应用为最小控制单元，对网络边界的访问行为进行精准管控。



2.2 产品特性

2.2.1 稳定安全可靠的跨网功能

用户访问企业应用和服务的权限，从传统网络层级升维到应用层级，避免 VPN 对企业内网过度暴露的同时，让企业对应用的访问管理更透明，管控更有的放矢。支持负载均衡和异地灾备等，保障服务稳定可靠。

2.2.2 访问零信任设计

基于腾讯安全零信任策略和架构，遵循最小最少权限原则，构建基于身份的可信赖计算

机制，保障用户对企业应用的安全访问。对用户的异常行为进行判定，不放过任何可疑行为。

2.2.3 集中管理

集中应用管控，管控粒度更精确。支持把企业应用的域名/端口进行收敛。在不影响应用使用和无改造的情况下，对外仅统一暴露 HTTPS/443 端口，高效预防恶意威胁，令企业免于高危端口的攻击。

2.2.4 应用层数据安全防护

对于流经数据进行安全防护，可对应用层数据支持动态脱敏和水印保护等高级安全防护功能，可接入或定制高级安全策略，有效保障企业业务安全。

2.2.5 全面日志审计

支持对包括管理员在内的各类用户的操作、访问行为进行多维度日志审计，可作为有效的事件追溯和事故分析的保障和依据。

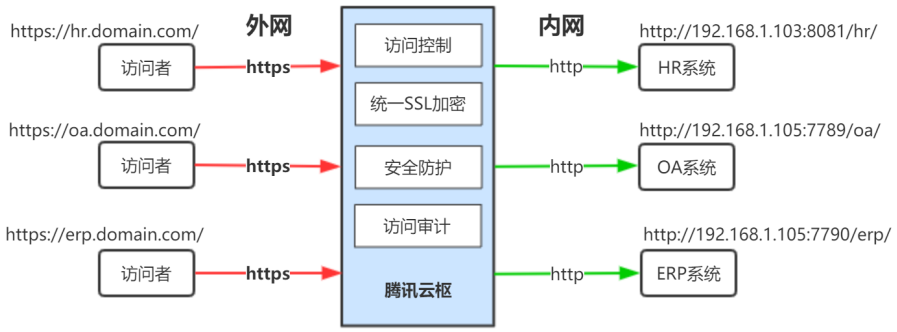
第3章 核心功能

3.1 应用代理

应用级智能网关本身支持负载均衡和弹性扩容，提供高性能、高可用和高吞吐量的企业应用代理服务，支持目前市面流行的 QQ、IE、Chrome、Firefox、Safari 等主要桌面浏览器和移动浏览器。

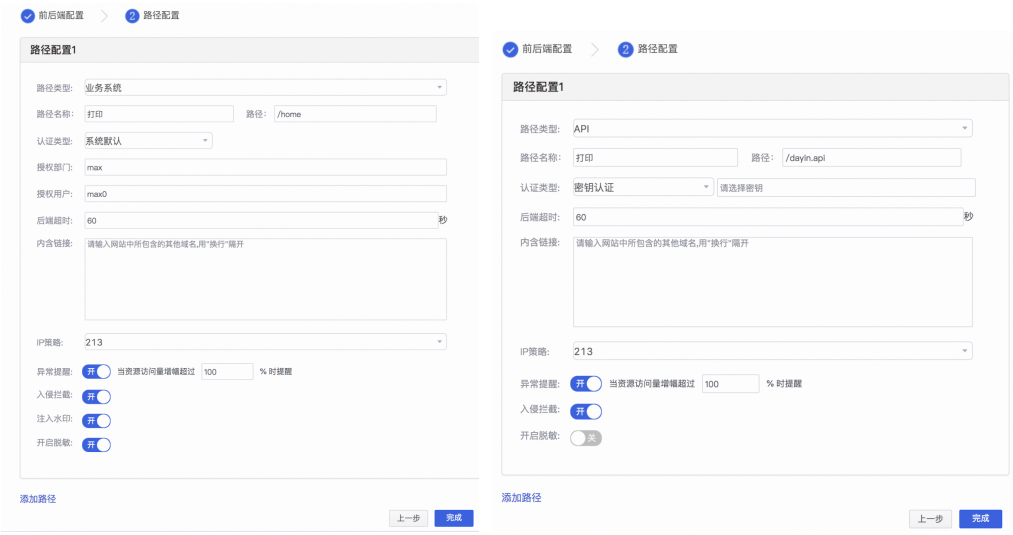
支持对 HTTP、HTTPS 网络协议的代理，方便用户从往外网访问内网企业应用和服务。

在不影响企业现有应用的前提下，对外统一收敛协议和端口，避免高危端口的对外暴露。



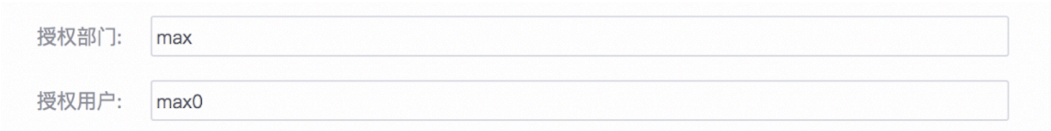
3.2 应用集中管理

对 web 应用、API 进行集中管控，可直观展示各应用/API 接口对外提供哪些服务、应用状态，及安全防护策略等信息，并提供紧急关停功能（一键实现应用批量下线控制）。



3.3 访问控制

对内网应用及 API 接口进行鉴权和访问控制。可对内网 web 应用进行用户访问权限的分配达到管控目的，仅有授权用户可访问。



3.4 身份认证和授权

应用级智能网关支持多种认证方式，包括短信认证、企业微信扫码认证、密钥对认证、第三方认证等（当添加的资源是 web 业务系统时，可采用短信认证或企业微信扫码认证；当添加的资源是 API 接口时，可采用密钥对认证的方式）。

- 短信认证

短信认证技术是一种快捷安全的认证解决方案。短信认证分为手机短信终端和短信认证服务器两部分。 终端用户在既有移动设备的基础上，通过手机短信中获取的验证码 来进行用户认证，就可以安全的访问网络资源。系统集成腾讯短信认证服务，也兼容第三方短信认证服务。

- 企业微信扫码认证

随着办公移动化，企业微信越来越多的进入企业用户的日常工作中，腾讯应用级智能网关集成企业微信认证方式， 为企业提供一体化的集成方案。

- 密钥认证

API 接口的密钥对认证也是常见的鉴权方式之一。应用级智能网关会对每个访问请求进行身份验证，即每个请求都需要在参数中包含签名信息（Signature）以验证请求者身份。签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey，二者内容没有关系、无法相互推算。当请求的签名和服务器的签名计算进行相等验证通过时，则放行此请求。该验证方式的安全性高，且占用计算资源和网络资源都很少。

- 第三方认证体系

可通过接口对接，数据订阅同步等方式接入第三方认证体系。

3.5 高级安全防护

具备明水印、暗水印、敏感数据过滤脱敏等安全能力，可接入或定制高级安全策略和规则，有效保障企业业务安全。

- 对业务数据的保护-网页水印

在经过应用级智能网关代理的业务上自动添加页面水印保护。

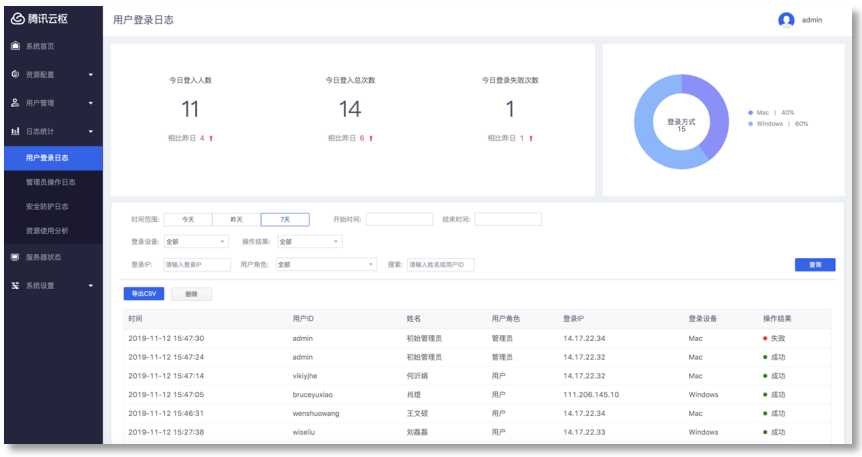
- 应用层数据脱敏

在数据输出到页面之前对敏感数据进行脱敏处理，支持手机号，身份证信息，自定义关键词等数据的脱敏保护。

3.6 日志和审计功能

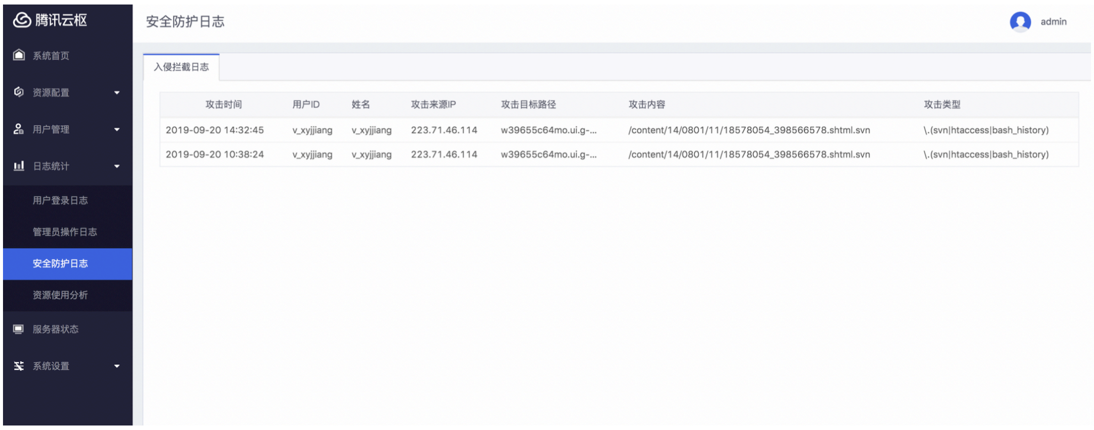
全面记录用户日志、管理员日志等，用户使用腾讯应用级智能网关中所有产生的请求信息都会有记录，管理员可以用过管理后台直接查看所有的访问日志，支持回溯审计。

- 用户登录日志

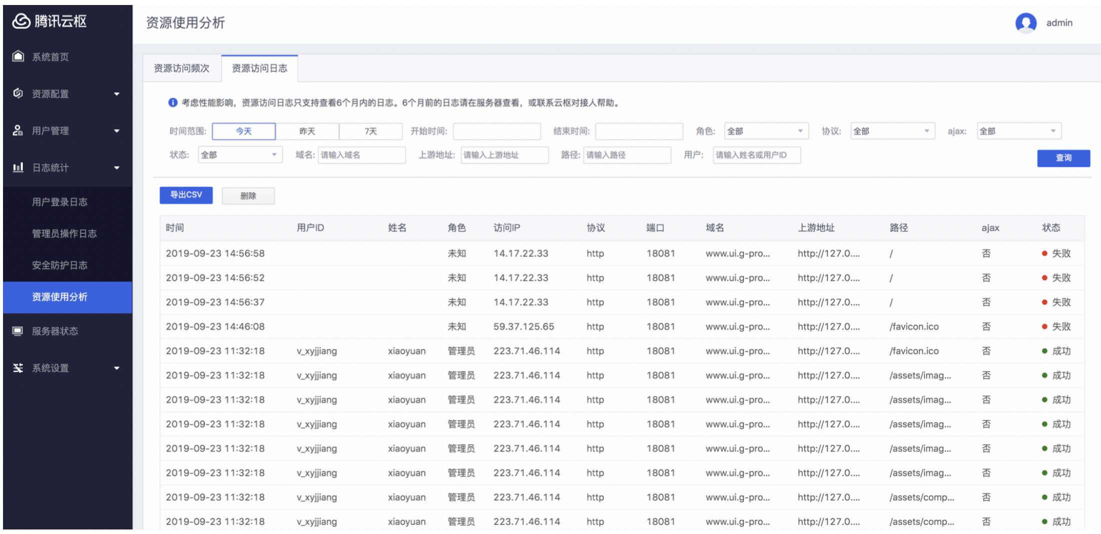


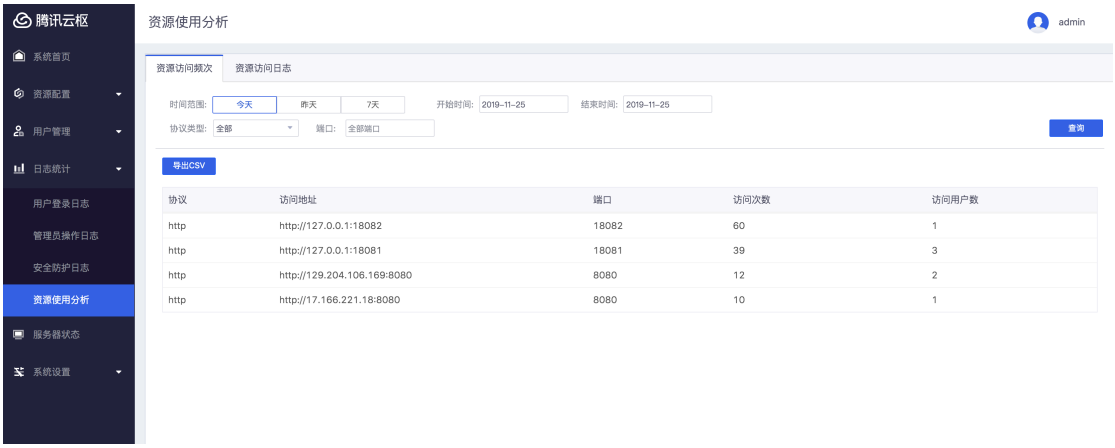
- 后台操作日志

- 入侵拦截日志



- 业务访问日志





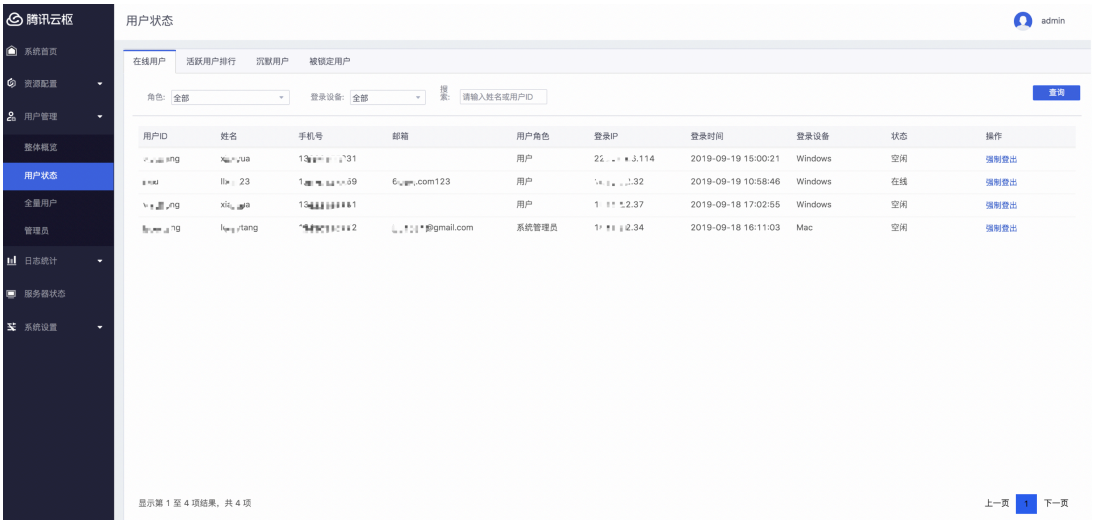
3.7 统一管理后台

应用和被访问情况的可视化展示，哪些应用对外开放，被什么人访问，管理员一目了然。主要包含：应用管理、代理管理、用户管理、审计管理、系统管理等核心模块 。

除了核心管理模块意外，统一管理后台还包含如下功能：

- 在线用户管理

  在线用户展示和强制登出等 。



- 会话超时控制功能

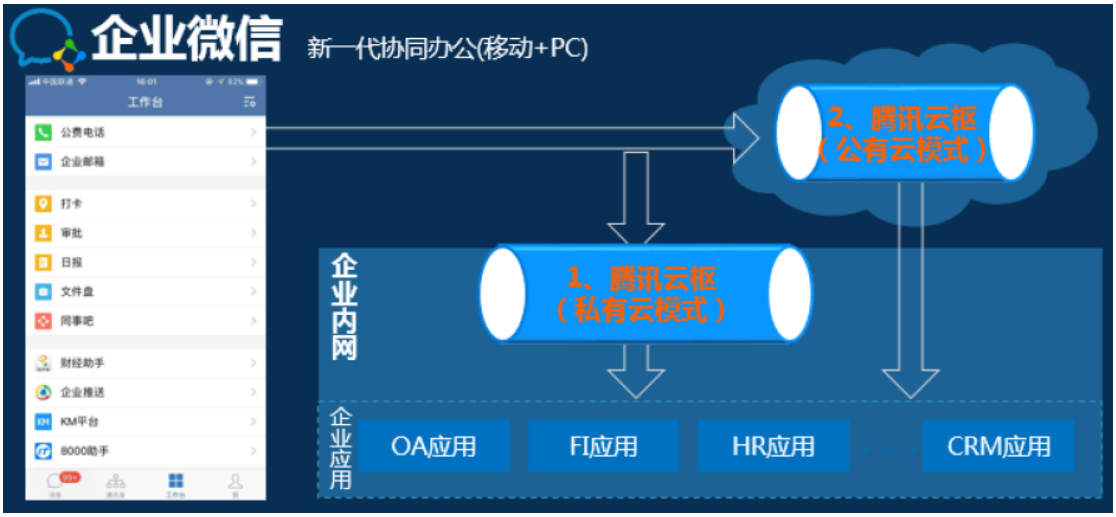
  为了防止用户在没有主动注销的情况下离开导致的安全风险，腾讯应用级智能网关提供了实时检测用户行为的功能。当检测到客户端在指定时间内没有任何访问请求的时候，就会自动注销用户。

- 实时监控能力

应用级智能网关可对资源异常访问情况、服务器异常情况、异常用户登录情况等等进行实时监测预警，企业管理员可在应用级智能网关管理后台设置阈值，若超过管理员设定的值，则会通过企业微信通知到设定的被通知人

3.8 企业微信联动

企业微信和应用级智能网关集成助力企业微信 ，通过企业微信工作台，打通企业内网应用，提高企业移动办公效率。



第4章 产品优势

4.1 远程访问安全、稳定

腾讯应用级智能网关授权的访问在企业应用层级，不会开放网络层级的访问，对外开放的访问权限更小、更精确、也更安全。通过 HTTPS 协议进行数据传输，信息加密，安全可靠。

4.2 无网络改造成本

企业现有应用可以直接接入腾讯应用级智能网关，不需要做额外改造，有效降低企业 IT 成本。

4.3 统一访问体验

无需安装客户端，通过 WEB 浏览器即可对企业内部业务系统进行访问，业务访问使用统一的入口，简单方便。

4.4 访问零信任

改变传统以网络为基础的信任，建设以应用为基础基于身份的信任机制。无差别对待从特定网络连接的用户，信任机制与其获得的服务和权限的高低无关；并针对用户的适度风险感知能力，全面过滤非法访问；同时实现动态访问控制，即所有对服务的访问行为必须经过认证、授权和加密处理。

第5章　部署模式及用户使用

5.1 应用级智能网关部署模式

应用级智能网关部署在网络出入口处，能够被外网访问，同时能够访问到内网被连接的应用服务。应用级智能网关作为企业外网的唯一出口，其他需要对外提供服务的业务统一通过应用级智能网关输出。对企业现有网络结构无需改造，接入即用。

5.1.1 硬件要求

方面	建议配置（单机或者多机）

CPU	8 核心 CPU
硬盘	1T*2
网卡	万兆网卡*2
内存	16G 以上内存

5.1.2 网络要求

- **应用接入的网络要求**

  主机能访问互联网

  能被互联网访问，需开放 443/80 端口

  需要有外网域名 （例如 ys.qq.com）

  域名做泛指向解析，例如：*.ys.qq.com 指向主机外网 IP

5.1.3 安装部署

部署在网络边界处，例如局域网和局域网之间的网络边界，或在内网和外网边界处。