天翼云 AOne 零信任服务
产品使用指南

天翼云科技有限

目录

1. 概述

新兴科技的迅猛发展不仅造就了蓬勃发展的数字产业，也推动了各行各业的数字化转型浪潮。其中，云计算、5G 为代表的新型基础设施成为“数字新基建”的重要组成部分，容器、微服务为代表的云原生技术深刻影响着企业数字应用系统的构建，大数据、智能分析加速实现数据驱动的业务转型，机器学习及物联网等在改变企业生产运作方式，数字化技术已经成为企业的核心竞争要素。

2020 年，突如其来的疫情更是加速了各个机构与企业的数字化步伐，业务重构、应用上云、云端存储、远程办公、移动服务已经逐渐成为常态。与此同时，数字化进程加速所带来的一系列数据安全、网络安全、应用安全、终端安全以及人员安全日渐成为企业在数字化进程中的不可忽视的问题。随着企业加大数字化的投入，应用越来越复杂，接入越来越多元、边界越来越模糊，使安全边界的威胁面不断增加，极大增加了安全防护的复杂度。不仅如此，随着企业应用的数字化改造，提升员工体验并带来便利的同时，也面临着移动端数据泄露账号密码泄露、特权账号共享、内部员工违规操作、设备风险等众多内部引发的安全风险。令人防不胜防的外部攻击，日益加剧的内部威胁以及不断加大力度的监管，使得传统边界思维的安全架构已经不堪重负，迫切需要新一代的安全架构应对数字时代的多元复杂挑战。

1.1 背景

1.1.1 社会/政府/企业构建新一代安全体系过程中面临多重挑战

在构建新一代安全体系的过程中，社会、政府和企业都面临着多重挑战。

首先，随着信息技术的不断发展，网络安全威胁也日益增加，黑客攻击、恶意软件和网络钓鱼等攻击手段不断翻新，给安全保障带来了极大的挑战。

其次，安全技术的更新换代速度较快，企业需要不断跟进新技术、新方法，以应对不断变化的威胁。此外，安全管理的复杂性和成本也是构建新一代安全体

系时需要克服的难点。

最后，由于全球化和信息化的趋势不可逆转，跨国安全合作和信息共享也成为了构建新一代安全体系时需要面对的挑战。

1.1.2 新兴技术带来全新安全挑战

新兴科技的发展使得传统安全架构难以应对日益复杂的安全形势。新兴技术的使用对企业信息安全防护带来了巨大压力。84%的受访机构负责人表示，使用容器、微服务等云原生技术增加了企业的内部应用安全的管理难度;79%认为物联网和设备管理等技术使得企业需要拓展安全管理范畴:77%认为公有云和混合云等云计算架构加速了企业信息化基础设施的不断进化。同时，各行业使用场景也造成了不同的信息安全需求。例如，由于跨行业、跨机构数据分享场景不断增加，受访政府负责人更加强调大数据、API 对企业内部数据安全防控的要求。

1.1.3 传统安全架构面对内部安全威胁和外部网络攻击

传统安全架构面对内部安全威胁和外部网络攻击都存在一定的局限性。在传统安全架构中，通常采用边界防御和内部访问控制来保护企业网络和数据安全。但是这种安全模式往往存在盲区，无法对内部员工的恶意行为进行有效监控和防范。同时，外部网络攻击手段也越来越复杂和隐蔽，传统安全架构的防御能力也面临很大的挑战。因此，企业需要采用更加先进的安全技术和策略，例如零信任安全模式、人工智能和机器学习等技术，来提高网络安全的可靠性和保障企业的信息安全。

1.1.4 重塑传统边界安全防护势在必行

为了应对各种复杂的安全挑战，越来越多的企业与机构加入到零信任的实践过程中，而企业对零信任架构的重视与投入，反过来又推动了零信任产业的发展，呈现出一种共生闭环发展的态势。零信任的核心技术软件定义边界SDP(SoftwareDefinedPerimeter)，身份识别与访问管理(IAM)与微隔离(MSG)在不断

提高发展形成定制化的的解决方案同时衍生的新技术不断发展，特别是 IAM 和安全策略方面正在逐步面向核心应用场景不断增强。零信任作为新一代的安全模型还与各种新兴技术例如云计算、大数据、可信/隐私计算、人工智能、物联网等融合发展，为数字化转型保驾护航。

1.2 零信任概述

传统的安全模型依赖于基于边界的安防方式，即建立一个安全的网络边界，在边界部署包括防火墙、入侵检测、WAF 等安全设备，形成的安全防护自然切分出企业内外网，同时默认内网的一切都是可信的。然而随着新一代信息技术的快速演进，云计算、大数据、物联网、移动办公等新技术与业务的深度融合，网络的复杂性不断增加，其安全威胁和风险更是不断涌现，边界意识逐渐淡化，默认以物理边界内外网来判断安全威胁的应用模式无法抵御多重安全挑战，在此背景下，“从不信任、始终验证”的零信任（ZeroTrust）理念应运而生。

1.2.1 基本概念

零信任是一种安全模式，它假定在企业网络内部和外部的所有用户、设备和应用程序都不能被信任，需要经过身份验证和授权后才能访问企业的资源。零信任的核心理念是“永远不信任，始终验证”，它通过对用户和设备的身份、访问环境和行为进行实时评估和监控，来保护企业的信息安全。零信任不仅仅是一种技术，更是一种安全文化和策略，需要企业在人、技术和流程等方面进行全面的改变和升级。

1.2.2 零信任安全理念

全球数字化转型的逐渐深入让云计算、大数据、物联网等新技术演进速度加快，越来越多的网络服务需要兼容移动互联网、物联网、5G 等新兴技术，同时支持远程办公、多云环境、多分支机构、跨企业协同等复杂网络应用场景，保障终端和用户可以从任何 IP 地址接入服务网络。然而企业机构的传统网络安全模

式专注于边界防御，授权主体（资源请求的终端用户、应用以及其他非人类实体）可广泛地访问内网资源，因此，环境内未经授权的横向移动一直是企业机构面临的最大挑战之一。

零信任的理念和技术精准对应了市场的需求，根据 EvanGilman 在《Zero Trust Networks》书中所述，零信任网络建立在五个假设前提之下：

- 应该始终假设网络充满威胁；
- 外部和内部威胁每时每刻都充斥着网络；
- 不能仅仅依靠网络位置来确认信任关系；
- 所有设备、用户、网络流量都应该被认证和授权；
- 访问控制策略应该动态地基于尽量多的数据源进行计算和评估。

零信任的安全理念认为企业内外部用户都不可信，需要对每个用户的身份和访问权限进行验证和授权。这种模式下，企业需要在网络和数据访问的每个环节都进行认证和授权，而不是仅仅在边界处进行控制。这样可以避免攻击者通过窃取用户凭据或者利用漏洞等方式进入企业网络，从而保护企业的数据安全。零信任安全模式需要采用多层次的安全策略来实现，例如多因素认证、访问控制、加密、日志审计等。这些策略可以帮助企业建立起一个更加可靠和安全的网络环境，提高企业的安全性和可靠性。

1.2.3 演进过程

2004 年：以“寻求网络去边界化趋势下的全新安全架构及解决方案“为目的而成立的耶利哥论坛最早体现零信任理念。

2010 年：咨询机构 Forrester 首席分析师 JohnKindervag 首次提出“零信任”这一术语，认为零信任本质是以身份为基石的动态访问控制，即以身份为基础，通过动态访问控制技术，以细粒度的应用、接口、数据为核心保护对象，遵循最小权限原则，构筑端到端的安全边界。

2011-2017 年：GoogleBeyondCorp 实践落地，发表系列论文，验证了零信任安全在大型网络场景下的可行性。

2013 年：国际云安全联盟在零信任理念的基础上提出了软件定义边 SDP，并发布了 SDP 标准规范 1.0，进一步推动零信任从概念走向落地。

2017 年：Gartner 提出持续自适应风险与信任评估 CARTA 的概念，零信任是实现 CARTA 的基本步骤。随后，分析师 Riley 将 CARTA 的概念改编成了零信任网络访问（ZTNA），ZTNA 包括持续自适应风险和信任评估，在不影响可用性的情况下提供最大的安全性。

2018 年：Forrester 发布年度零信任扩展生态系统 ZTX 研究报告，探索零信任架构在企业中的应用，系统性对零信任厂商的能力进行评估。

2019 年：Gartner 的市场报告中，采用了零信任网络访问（ZTNA）作为主题。

1.3. 产品定位

天翼云 AOne 零信任服务依托覆盖全国的边缘节点，提供以身份认证与动态信任为基础的企业远程访问，颠覆传统 VPN、IAM 的“一次验证 + 静态授权”模式，提供更加安全、便捷、统一的安全接入服务，安全边界全方位覆盖，全面保障企业办公安全。

AOne 零信任服务能够：

- 灵活部署到分布式边缘云端，支持按需动态扩展；
- 基于天翼云边缘安全节点，叠加 WAF，抗 D 等安全插件能力，抵御恶意攻击，实现简单、安全的远程访问管理；
- 针对不同的用户访问场景、不同的企业应用，提供一体化的配置管理功能；
- 通过多因素身份验证、访问策略和行为分析等技术手段，为用户提供更加安全可控的服务；
- 通过便捷的连接器部署实现跨数据中心的网络打通，统一接入访问；
- 覆盖企业应用访问全周期的安全防护能力，如访问请求拦截、流量转发、信息采集、流量管控、流量加密、建立双向认证的访问通道等能力；
- 无论访问企业应用的是员工，合作伙伴，还是用户，基于多因子认证以及多源评估策略引擎，实现对用户访问持续认证，可信授权；

- 通过多维动态授权评估引擎，对用户访问行为，根据设备，身份，行为，终端基线，环境感知等多维度聚合分析，实时检测不安全访问行为，及时降权，阻断恶意访问。

从而帮助企业轻松地从根本上解决安全问题并提供卓越的访问体验。

2. 产品架构

天翼云 AOne 零信任服务整体架构：

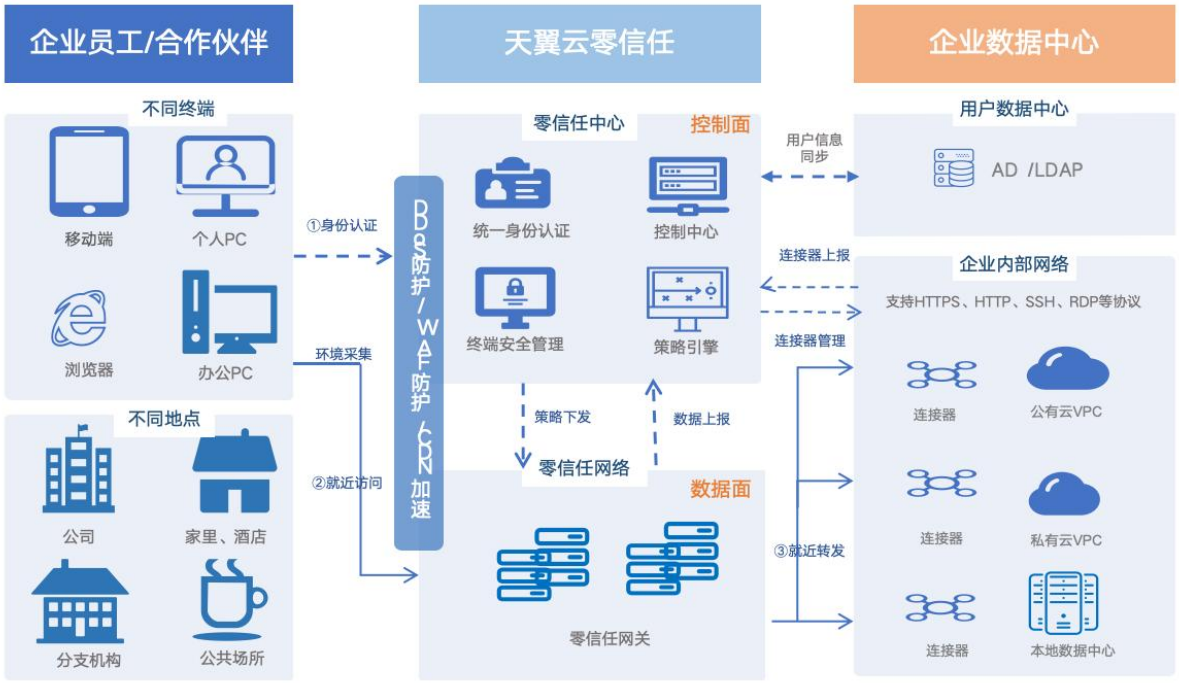

图 1 天翼云 AOne 零信任服务产品架构

天翼云 AOne 零信任服务整体架构依托天翼云遍布全国的边缘节点，基于身份认证与动态信任为基础构建全新的企业远程办公网，采用控制面板和数据面分离，零信任网关进行持续认证，安全策略实时执行；零信任中心进行身份安全校验、终端设备评估，日志等进行可信评估，最终联动零信任网关进行降权、阻断、强验证等快速处置。零信任核心组件为零信任中心、零信任客户端、零信任网关、连接器四大部分组成，各自职责如下：

零信任客户端：主要进行流量劫持、隧道创建，PC 端和移动端具有对应客户端，同时支持 APP 进行 SDK 集成。同时 PC 的客户端提供终端安全检测能力，

对接入的终端环境进行实时采集和上报，提供给零信任中心进行信任评估。其中，只有授权过的可信客户端才能连接零信任中心和网关，同时，非全流量引流，仅针对配置的应用资源进行引流零信任网关，可在零信任中心使用域名、IP、IP 段形式配置应用资源。

零信任中心：作为整个 AOne 零信任服务的配置策略管理、身份认证、运营中心。客户端登录时负责进行准入策略、身份信息确认，登录认证成功后进行下发客户端所需连接网关、引流资源等信息，进行隧道创建。同时，零信任中心可支持客户端、网关、连接器策略管理，并根据多维度的信息进行持续动态授权评估，若可信评分较低，则会执行降权、二次认证、阻断处理。同时可进行展示企业使用情况，包括各类行为日志审计、数据分析等。

零信任网关：作为数据访问的接入点，进行链路串联，并根据零信任中心下发的策略进行实时监测、执行，主要是作为安全处置的载体，包含 Web 入侵检测、横向扫描、应用权限二次校验、精细的访问控制等。

连接器：部署于企业应用资源网络内，用于连通企业内部应用资源。采用连接器可以使网络路由架构更灵活，可满足不同场景需求。比如实现跨数据中心统一接入：在不同的数据中心部署连接器，将不同数据中心的企业应用与对应连接器关联，则可实现跨数据中心统一接入。

2.1 登录认证过程

①登录客户端，输入企业认证标识+账号密码（或者扫码认证），向中心发起身份认证，并传递终端环境信息

②中心通过提交的身份认证信息、终端环境信息，根据已配置的管控策略，判断是否符合准入条件（比如是否是属于正常时间、正常地点登录、是否属于可信设备等）、身份账号信息认证，认证成功后返回客户端，并提供对应加密 token 用于后续客户端通信

③客户端获取配置的路由表、就近的边缘网关，开始启动，创建隧道，在

虚拟网卡添加路由进行引流

2.2 应用资源访问过程

①访问应用资源 A，客户端将先判断是否属于内部资源（即是否有添加到对应虚拟网卡路由），若是内部资源，则流量引流到网关，非内部资源则默认不处理。

②网关进行权限二次校验、策略处置，异常行为则进行阻断、降权等处置，正常则进行转发给连接器。

③连接器则转发到内部应用，最终获取资源。

3. 产品功能

3.1 用户与组织

企业员工在登录零信任客户端时需要进行身份认证，则需要进行用户信息都管理，支持多种身份源接入管理：

方式一：平台手动创建或批量导入用户与组织信息，支持用户信息的增删改查，并可提供对应 API 进行管理本地用户

方式二：已对接的第三方身份源接入，如企业微信、钉钉等。绑定企业微信等身份源后则可通过企业微信进行扫码认证。

方式三：通过标准协议接口将企业内部身份源信息进行同步。目前支持 SCML2.0 协议，实现 IAM 和应用之间的身份信息传递。配置遵循标准 SCIM 协议的应用系统为数据源，将组织机构、用户数据同步到平台。

通过以上方式导入用户与组织关系（一个用户仅能在一个组织下），还能通过平台创建用户组进行管理，可针对不同人员特点进行创建用户组。

零信任服务授权是采用最小权限管控，可针对用户、组织、用户组进行人员身份授权对应应用，若授权组织、用户组则对应组织、用户组内增加用户，则默

认继承授权。

3.2 应用资源管理

目前越来越多应用是采用 HTTP、HTTPS 代理模式，走 Web 应用类型，但是在内部实际应用场景里，还是存在很多的 TCP、UDP 层协议，比如内部聊天工具、SSH 远程访问、虚拟桌面等，当前零信任服务支持 TCP 四层所有协议，包括 SSH、RDP 等协议，以及 UDP 等相关协议应用。目前对比传统 VPN，除了提供 IP 接入外，还提供域名接入管理，可以更精细化管理权限，并且避免业务 IP 频繁变更的问题。通过接入配置后进行下发到客户端、网关、连接器进行隧道建立，可根据实际场景选择使用。

IP 资源：可选择 TCP、UDP 协议接入。用户通过登录客户端认证通过后，将获取到零信任控制下发的 IP 资源路由表，客户端将对应路由写入到虚拟网卡中进行引流，同时通过 HTTPDNS 获取就近的零信任网关地址，与对应网关建立隧道，隧道数据加密后传输到网关，网关会进行二次校验访问 IP、用户权限，再进行对应转发到连接器，连接器进行转发给内部系统资源。

域名资源：可选择 HTTP、HTTPS 协议接入。用户通过客户端认证通过后获取对应域名+fake IP（构建域名虚拟 IP，避免 IP 资源重复或域名解析相同 IP 等情况），通过 fake IP 进行写入虚拟网卡进行引流，同时通过 HTTPDNS 获取就近的零信任网关地址，与对应网关建立隧道，隧道数据加密后传输到网关，网关会进行二次校验访问 fake IP 的域名与用户权限，再进行对应转发到连接器，连接器进行转发给内部。

注意事项：若域名资源在用户本地静态 HOST，则客户端会按照 HOST 的 IP 进行引流判断权限，非域名粒度判断，若该 IP 未授权则对应应用则无法访问，若有域名解析配置需求建议通过域名解析管理进行配置。

3.3 域名解析管理

基于应用资源可采用域名接入方式，所以涉及域名最终回到内部系统的具体IP获取问题，正常情况会通过连接器所在服务器的默认DNS进行域名解析，同时可以通过域名解析管理进行配置。

连接器DNS自定义：可自定义对应连接器采用的DNS，即通过该连接器的域名资源都采用该DNS进行生效处理。

域名DNS自定义：可通过指定域名具体的DNS服务器地址进行管理，即对应域名采用该DNS进行解析，域名DNS比连接器DNS更优先。

域名静态HOST：若不具备DNS解析，则可配置静态HOST具体IP，若域名业务发生IP变化需及时变更。

3.4 应用授权

默认所有应用资源均未授权，新增应用后默认所有人不可访问。可基于用户、组织、身份以及对应的资源进行授权，建议最小化权限授权，即非必要不对对应用户开放对应资源权限，避免权限粗放、越权行为。

在客户端应用资源可查看已授权资源，未授权资源不可见，若用户访问未授权应用，则客户端会进行提示报错，建议用户向管理员申请应用授权。

3.5 连接器管理

图 2 访问链路图

使用零信任网络访问您的企业内部系统之前，您需要通过安装连接器，实现企业员工要访问的内部应用系统资源和零信服务边缘节点的网络连通，连接器使企业网络分布管理更灵活，尤其是解决多数据中心、混合云的企业场景。

连接器需要在企业内部网络进行安装，可选择云上服务器（云主机）、虚拟机或物理服务器进行部署安装，零信任管理控制台提供连接器新增、安装命令、路由配置等管理。连接器目前仅支持 Docker 容器化部署模式，控制台提供连接器安装命令、以及对应需要开放端口，连接器需要反向连接到零信任边缘网关，所以如果存在防火墙配置，需要放行部署的服务器或虚拟机出方向 443、 xxx 端口，具体端口号请在生成连接器后的页面获取。同时内部系统需要保障与对应连接器可连通，若有白名单设置，内部系统需将连接器进行加白。

连接器高可用：连接器可采用同个安装命令在多台服务器进行安装，实现主备双活方式保障连接器高可用，平台通过心跳包实时查看连接器状态，进行连接器管理。

路由配置：连接器可用于多个数据中心管理，所以若存在多个连接器，则对应应用资源则需要选择一个连接器进行回源（因为应用资源可能部署在不同数据中心，需要通过打通该中心的连接器进行回到内部服务器），目前会生成默认连

接器，所有应用资源会默认走默认连接器，若有特殊情况，则需要需要路由配置，即指定对应应用资源通过哪个连接器进行回到内部系统。

3.6 终端管理

3.6.1 客户端版本发布

客户端版本获取通过 CDN 加速方式，保障版本下载速度，避免并发时产生拥塞。同时客户端版本发布会经过严格内部测试、公测后再进行转为稳定版，最终客户在控制台、客户端客户端获取的均为稳定版，公测版本会根据租户等进行筛选用户进行推送，推送后可选择是否升级为公测版本。

目前零信任服务提供 PC、移动端、SDK 集成方式。

3.6.2 用户终端设备查看

终端设备列表将全面、直观地展示企业用户终端接入的信息，包括设备 ID、终端名称、操作系统、客户端版本、用户、IP 地址、Mac 地址、登录状态，最后登录时间等，可实时有效的展示用户终端设备情况。

3.6.3 用户登录信息

终端登录日志将记录并展示每一次终端登录的信息，包括用户登录的出口 IP、登录方式、状态等

3.6.4 终端错误日志

客户端异常时将获取错误情况进行上报，主动并实时关注客户端情况，上报内容主要包含客户端版本、操作系统、错误编码、错误信息

3.6.5 终端限速

可根据企业场景进行单客户端限速，零信任服务产品超量（使用量超过购买量）将进行自动限速。

3.6.6 终端登录安全

支持二次认证设置，即账密登录后需要通过手机短信验证码等进行二次认证后才可访问；同时支持密码设置要求，如不允许设置弱密码、密码有效期、密码重试约束等。

3.7 终端接入

客户端下载登录时仅需要输入企业认证标识（唯一标识）+账号密码（或扫码）进行登录，登录后可见以下模块：

用户在线状态：登录后将进行启动网卡、隧道建立，完成后才显示为在线状态，才可访问对应内网资源

工作台：可根据用户自定义定制工作台内容，比如企业公告、工单等接入

应用资源：可见已授权资源，未授权资源不可见，并且若已配置入口 URL，则可根据资源图标进行快速访问

我的收藏：即针对常用应用资源进行收藏，收藏后可快速查找访问

用量统计：针对单用户的带宽、流量进行实时统计展示

我的设备：显示用户最近登录情况，以及该用户的所有登录设备进行管理，若企业开启授权激活，若有新设备进行登录时，需要通过旧设备进行激活授权

设置：展示用户基本信息，如账号、手机号、版本信息等，可重置手机号、密码等基本操作

3.7 零信任安全策略

3.7.1 可信设备管理

设备终端越来越多，企业的系统被各类设备访问，安全管理若无法有效区分是否是安全设备、还是非法设备，则有可能导致攻击者窃取账号后，直接使用非

法设备进行登录访问，获取数据。主要针对可信设备管理分为以下几点：

- 企业可信设备录入：即由企业进行全面采购设备或对员工自有设备可进行入域等管理，则可录入可信设备，仅允许企业录入的设备进行登录。
- 可信设备授权：企业可针对每次新登录设备（即之前从未登录过的设备，则未进入可信设备库）进行授权，在未授权激活期间可配置降权访问（即仅访问重要等级低的应用）或阻断。
- 新设备激活：主要针对用户已绑定设备，若再使用其他新设备登录时，需要进行新设备激活，可通过旧设备认证或管理员认证激活才可使用。
- 设备共享：设定是否允许设备多人使用，避免存在安全风险。

3.7.2 准入策略

可通过不同维度设置准入条件，仅满足准入条件的用户才可通过认证登录成功，主要常用策略条件如下：

是否开启指定软件：如内置防火墙是否开启、是否运行指定的杀毒软件等

访问行为是否异常：根据用户平时行为进行记录分析，判断是否存在异常，如是否在异常时间登录、异常地点、异常的访问 IP 地址等

终端环境是否符合企业要求：根据设定的终端环境条件进行判断，如 mac 地址、IP 地址、访问地点、访问时间等

3.7.3 环境感知

实时获取终端环境情况，进行实时判别是否存在符合条件，若存在异常则根据策略执行阻断、降权、二次认证等处理，主要环境感知包含以下内容：

是否开启指定软件：如内置防火墙是否开启、是否运行指定的杀毒软件等

终端环境是否符合企业要求：根据设定的终端环境条件进行判断，如 mac 地址、IP 地址、访问地点、访问时间等

是否设备存在安全性问题：基于攻击者常用的攻击维度，进行设备环境安全性判别，如计算机是否存在隐藏账户、是否开启 FTP、Telnet、共享等功能

3.7.4 横向扫描防护

横向扫描主要指的是黑客在利用某个点获取网络访问权后，进行收集系统其他信息来实时精确的攻击行为。如果没有合适的预防措施，则可能导致黑客获取某个点的访问权后，扩大攻破其他点，造成影响面扩大。所以针对横向扫描的行为进行设定不同策略模版，如 IP 类横向渗透防护、域名类横向渗透防护，主要都是针对单用户进行不同协议、端口、地址的组合判断其频次，若高于异常则进行阻断或挑战认证。

3.7.5 内外网隔离

可针对常用的互联网域名、ip 设定黑白名单进行互联网行为控制，客户端搭配快捷上下线能力，保障用户体验，那么内外网隔离在安全性上如何防范钓鱼行为呢？主要通过互联网流量白名单设置：仅设置需访问、且安全的域名或 IP 为白名单，仅放行白名单内的互联网流量，其他均不可访问，则达到效果就是访问互联网（非白名单）则无法访问企业企业内网，访问企业内网，则断开互联网（非白名单）链接，则可以实现：

员工在内网访问时不小心点击钓鱼链接/文件，该断网效果能阻断钓鱼软件连通到点击钓鱼的受害者电脑，避免内部系统可访问的这时候被攻击者扫描攻击。

员工在互联网访问时点击钓鱼链接被远端控制，这时候隧道关闭，没有访问部门内系统的权限，钓鱼远控程序扫描不到内网系统。若用户重新登录零信任访问内网，此时钓鱼远控会被即时阻断。

3.7.6 Web 入侵检测

联动自研的 Web 应用防火墙能力，可实现内网的域名应用进行入侵检测，进行恶意特征识别及防护，在对流量清洗和过滤后，将正常、安全的流量返回给

服务器，避免网站服务器被恶意入侵导致性能异常等问题，从而保障网站的业务安全和数据安全。

业务流程：访问对应应用时，流量引流到对应零信任网关，网关识别属于入侵检测范围，则转发至 WAF 防护模块进行流量检测处理，处理完成后将流量转发至零信任网关，零信任网关进行转发至连接器回源

注意：零信任网关和 WAF 检测模块同机部署

3.8 日志审计

提供全面、多维度的日志信息，以便企业进行审计、管理。

- 用户访问日志审计：提供全面的用户访问行为日志，用户行为可视可查可控。
- 平台操作日志审计：每一个通过平台进行的策略均记录操作对象、时间、人员等信息。
- 威胁防护日志：网关威胁情况进行相应处置，并记录展示
- 准入日志：准入判别情况进行记录
- 登录日志：客户端登录情况进行记录

4. 安全能力

4.1 身份安全

4.1.1 用户信息管理

零信任中心统一管理用户信息，支持多维度用户信息创建，同时支持企业现有 LDAP 通过标准协议进行同步用户信息，用户数据均脱敏存储

4.1.2 多因子认证

除了传统的账号密码登录外，支持短信、OTP 等多维多二次认证，可以根据

客户需求进行选择认证方式，并自适应场景开启二次认证。

4.1.3 密码复杂度管理

支持自定义密码策略，管理密码复杂度，密码约束规则，密码有效期等

4.1.4 设备安全管控

企业的系统被各类设备访问，零信任可以邪乎企业有效区分是否是安全设备、还是非法设备，避免直接使用非法设备进行登录访问，获取数据，比如企业可信设备录入、可信设备授权、新激活等

4.2 接入安全

4.2.1 业务隐身

对比传统 VPN 需要提供具体 IP、端口进行接入，直接将企业的 IP 和端口进行暴露在前面，很容易出现爆破、漏洞等问题，零信任服务采用业务全面隐身，需要进行登录认证后才获取边缘网关地址，部署在 VPC 网络中的连接器反向建立隧道，源站服务器地址、端口也实现隐身，此外提供业务系统统一的登录入口，登录认证成功后可见已授权的内部系统、应用，实现应用系统的全面隐身

4.2.2 传输加密

全流量 SSL 加密传输，防止通信数据被劫持产生泄漏问题。

4.2.3 准入管控

可通过不同维度设置准入条件，仅满足准入条件的用户才可通过认证登录成功，主要常用策略条件如是否开启指定软件、访问行为是否异常、终端环境是否符合企业要求等

4.3 访问安全

4.3.1 最小权限授权

针对用户、组织、用户组精细化进行授权到具体的应用地址，可以避免权限粗放引起的问题

4.3.2 持续行为感知

实时获取终端环境情况、用户访问行为判断，比如是否存在高危端口、隐藏账户，或者出现端口扫描等行为，则会进行阻断、挑战认证、降权等处理

- 阻断：主要是在一定时间不允许进行内网行为访问，管理员可以审核行为后放行
- 挑战认证：主要是二次认证，比如再次通过手机验证码进行认证
- 降权：即针对应用进行设定重要等级，若存在异常行为则不允许访问高等级应用，并及时通知管理员

4.3.3 访问安全

提供 DDoS、web 应用防火墙等能力插件，提升企业办公安全

4.4 数据安全

4.4.1 全链路加密

全流量 SSL 加密传输，同时数据都做了脱敏处理，防止通信数据被劫持产生泄漏问题。

4.4.2 API 安全管控

采用自研 API 安全能力，提供自身平台全方位 API 安全治理与枋湖，可针对与客户端等对接的 API 进行资产管理，实时监测 API 风险，智能识别和阻断 API 攻击，且对应 API 均做了二层 token 校验，全面保障 API 传输得安全性

4.4.3 屏幕水印

客户可根据自身安全需求，启用屏幕水印，开启后则在对应工作期间内，屏幕展示相应的水印信息，保障企业数据安全。

5.平台稳定性

5.1 访问性能

零信任服务基于 CDN 的分布式资源、智能调度、路由选路等能力，可以大大提升访问速度，从测试数据来看通过零信任访问对比直连内部系统地址速度可提升 40%。主要基于以下几点：

- CDN 丰富的分布式资源：可支持三网资源访问，部分可落地到具体地市级
- 智能调度，负载均衡：根据客户端、连接器位置提供就近的零信任网关，比如客户端在北京，则零信任网关也在北京，进行就近接入，连接器在上海，则会通过上海的零信任网关进行回到连接器
- 智能选路，协议优化：零信任网关内部进行弹窗，则优选择最佳路径，并采用内部私有协议进行提升访问速度

5.2 服务高可用

- 网关基于分布式集群部署架构，集群内所有节点都可以承载业务，若某个节点故障后，会将该节点流量转移至其他节点服务，避免单点故障影响产品服务的情况。同时本身节点会进行多维度探测，判断机器性能、实时探测时延，若高于阈值，则也会及时进行相关切换
- 零信任中心部署两个数据中心，保障多中心多活，一旦出现严重的区域性灾害，则启动另一套中心服务，不影响业务
- 连接器主备多活：支持连接器多活部署，实时检测连接器服务情况，进行及时切换选路，保障服务

6. 应用场景

6.1 远程办公场景

6.1.1 需求背景

随着数字时代的快速发展，远程办公也越来越普遍，随之带来的就是更多的不同终端、不同的位置、不同的人员、不同的业务都需要接入企业的办公网，安全风险持续攀升。从远程办公的业务需求来看，主要分成几个使用场景：

1）企业员工、合作伙伴有远程办公、访问内网应用需求

2）企业需要保护敏感数据和应用程序，需要实时监测和响应安全事件

3）使用 VPN 产品，存在频繁掉线，企业数据泄露等安全问题

6.1.2 场景痛点

基于用户体验、企业安全管理成本考虑，存在以下问题：

1）访问体验差：容易发生账号借用、盗用情况，容易登录掉线；

2）灵活性差：需提前规划方案，整体周期长，难以应对突发流量；

3）访问不安全：只进行一次用户鉴权，无持续安全验证，且身份验证强度不足。

4）安全性问题：VPN 漏洞频发，需常常维护修复，同时应用暴露公网，遗留安全隐患。

6.1.3 解决方案与价值

AOne 零信任服务依托覆盖全国的边缘节点，提供以身份认证与动态信任为基础的企业远程访问，颠覆传统 VPN、IAM 的“一次验证+静态授权”模式，在有效提升用户访问性能的同时，更是强化企业安全，降低企业运维成本。

1）用户体验佳：扫码登录，支持多种终端，并可有效管控用户设备安全

2）架构灵活、访问速度快：分布式架构，可满足全国、三网接入。员工 3）3）就近接入，动态扩容应对业务突发，访问速度可有效提升

4）访问安全：内网应用隐身，有效防止攻击入侵，集成 WAF、抗 D

5）权限管控：精细化权限动态管控，规避越权

6.2 企业办公安全防护

6.2.1 需求背景

社工钓鱼手法花样多，重要场景更是成为攻击对象，靠复杂的管理方式和员工的自觉来保障也很难保障安全，尤其是重保等场景，对企业安全管理要求更高。

6.2.2 场景痛点

1）企业的系统被各类设备访问，安全管理若无法有效区分是否是安全设备、还是非法设备，则有可能导致攻击者窃取账号后，直接使用非法设备进行登录访问，获取数据

2）企业安全管理依赖员工意识，需要复杂管理手段，降低工作效率的同时往往也很难规避人工疏漏导致的安全问题

3）传统 VPN 的接入安全不具备终端安全管控策略，无法满足企业的安全需求发展

6.2.3 解决方案与价值

图 4 攻击链路分析

基于攻击者常用手段，逐个进行击破

1）应用隐身：对网络中的服务器、应用等资源进行隐身，让攻击者(黑客、病毒、木马) 找不到攻击目标。内外部业务均可使用，快速提升护网能力

2）防护扫描&渗透：提供横向扫描、Web 入侵防御等手段

3）内外网隔离：可针对常用的互联网域名、ip 设定黑白名单进行互联网行为控制，客户端搭配快捷上下线能力，保障用户体验

4）最小权限，动态授权：基于员工动态设定网络安全防护策略，实现策略授权最小化，降低授权风险，解决因定边界策略风险

5）终端设备安全管控：提供终端数据管控、可信设备评估、准入处理，保障终端设备的访问安全性

6.3APP 无感集成

6.3.1 需求背景

移动互联网发展越来越快，越来越多企业会采购或者自行实现内部管理系统 APP 化，如 OA 系统，以便可以更快捷的开展企业业务

6.3.2 场景痛点

1）企业采用 APP 或者小程序接入办公平台，若开放至公网，则公网暴露面过大，很容易被攻击者进行嗅探攻击

2）移动办公方式很难进行权限管理，且与企业内部权限无法统一管理

3）无感知访问企业内网资源，需要复杂改造

6.3.3 解决方案与价值

AOne-零信任 SDK 解决方案，移动端 APP 通过集成轻量级 SDK，即可让移动 APP 安全接入内网业务系统，帮助企业员工在任何时间、任何地点，任何设备，

安全、快速地开展办公业务。

1）SDK 集成，无感接入：APP 集成 SDK，通过 APP 认证信息进行交互，无需二次登录。

2）数据安全，业务隐藏：端口默认关闭，防止非法扫描、渗透无响应，应用漏洞无法直接利用

3）动态权限管控：根据终端身份和访问环境多种属性进行细粒度的访问控制, 并动态及时自动响应处置

7.部署实施

7.1 连接器部署实施

7.1.1 连接器部署选型指导

连接器所安装部署的虚拟机或者服务器的配置要求：

虚拟机或服务器配置：

CPU：2-4 核

内存：4-8 GB

磁盘：40 GB 以上

操作系统：CentOS 7 版本及以上

网络配置：可以访问公网。如果存在防火墙配置，需要放行部署的服务器或虚拟机出方向 443、 xxx 端口，具体端口号请在生成连接器后的页面获取。

为保障访问连接高可用，建议您一个本地连接器实例安装并启动至少 2 个服务器或虚拟机。

7.1.2 云上连接器部署方式

连接器作为打通企业应用系统网络到零信任网络的网络媒介。可根据企业的实际场景需求选择不同的部署方式。当企业有如下场景时，可选择在云主机实例部署连接器。

云上部署，可根据如下情况判断所需场景是否需选配公网带宽和弹性公网IP：

连接器需具备出网访问能力，但不必须配置公网 IP 和公网带宽。对于使用 NAT 网关进行内外网映射访问的企业，可以复用共享带宽和原有 NAT 网关绑定的公网 IP 进行出网。对于没有可以共享的 NAT 网关和带宽，则需要给部署云主机实例的。

7.1.2.1 远程访问企业内网/云上 VPC 网络资源

场景说明：该场景主要是企业的内网资源位于云上，且需要访问到企业的内网局域网网段地址，例如企业在云上划分的 VPC 网段。

部署方式：为确保连接器能访问到云上 VPC 的局域网段，需要在相同 VPC 网络中的云主机实例进行连接器安装。同时连接器需具备出网访问的能力，可根据企业实际资源进行出网能力配置，若企业的 VPC 网络使用 NAT 网关进行内外网映射访问，则无需采购额外弹性公网 IP，只需连接器所在服务器通过地址映射到统一的公网出口 IP 进行出网访问。

若企业有多个 VPC 网段，且在相同的资源池区域内，可以做通过做 VPC 之间的对等连接，这样只需要在其中一个 VPC 网段内部署连接器。其中对等连接建立后若 PING 对应的 IP 不通，需关注如下三点，1、对等连接是否正确建立；2、主机防火墙是否关闭或放通 ICMP；3、安全组是否放通入方向 ICMP。

7.1.2.2 访问企业具备公网 IP 的应用资源

场景说明：该场景主要是企业有部分公网应用需要进行远程访问，但是又不想将公网应用暴露在互联网。

部署方式：需要通过零信任 VPN 访问收敛访问来源 IP 地址，此时企业可采购云上云主机实例并在该主机实例部署连接器，然后将应用地址配置在该连接器上进行回源。同时，将企业公网 IP 的应用资源防火墙进行限制，仅允许连接器出网 IP 的访问，这样就能达到收敛企业公网应用暴露面的目的。

远程接入数据流：

1) 零信任中心和零信任网关由天翼云提供接入点服务，远程接入的用户，通过登录零信任客户端，在客户端登录页输入账号和密码进行认证登录，访问统一的天翼云公网 IAM 域名进行身份合法性校验。

2) 认证成功后，零信任中心开放该企业用户所对应的天翼云网关接入点，企业用户通过客户端和天翼云网关建立私有隧道连接，此时用户的客户端显示登录成功，状态为在线。

3) 用户完成登录上线后，在客户端应用资源页面点击对应的应用图标或者是在浏览器输入应用地址进行内网访问。此时客户端会根据用户访问的地址是否是企业接入零信任的应用地址进行精准引流转发到零信任网关，对于非企业的零信任应用地址的访问不会转发到零信任网关。

4) 零信任网关接收到客户端的访问流量，检验应用信息，根据企业在零信任中心所配置的该应用对应的关联连接器进行路由转发，将对应流量转发到对应的连接器。

5) 云上连接器使用隧道和零信任网关建立连接，接收到零信任网关转发过来的访问流量，根据访问的目的地址，转发到企业具体的应用地址。对于 VPC 的访问，此时转发到相同 VPC 网段内的访问流量里。对于基本公网 IP 的应用资源的访问，此时转发到对应的公网应用地址。

7.1.3 本地机房连接器部署方式

对于打通本地机房，本地数据中心的网络场景，需要把连接器部署在对应的

本地机房网络服务器内，这样连接器才能访问到对应的局域网内网网络。此时连接器需具备出网能力，部署后须在出口防火墙配置连接器所在服务器的出网访问映射，放行访问到零信任网关和零信任中心的端口。

远程接入访问数据流：

1) 零信任中心和零信任网关由天翼云提供接入点服务，远程接入的用户，通过登录零信任客户端，在客户端登录页输入账号和密码进行认证登录，访问统一的天翼云公网 IAM 域名进行身份合法性校验。

2) 认证成功后，零信任中心开放该企业用户所对应的天翼云网关接入点，企业用户通过客户端和天翼云网关建立私有隧道连接，此时用户的客户端显示登录成功，状态为在线。

3) 用户完成登录上线后，在客户端应用资源页面点击对应的应用图标或者是在浏览器输入应用地址进行内网访问。此时客户端会根据用户访问的地址是否是企业接入零信任的应用地址进行精准引流转发到零信任网关，对于非企业的零信任应用地址的访问不会转发到零信任网关。

4) 零信任网关接收到客户端的访问流量，检验应用信息，根据企业在零信任中心所配置的该应用对应的关联连接器进行路由转发，将对应流量转发到对应的连接器。

5) 本地机房连接器使用隧道和零信任网关建立连接，接收到零信任网关转发过来的访问流量，根据访问的目的地址，转发到企业具体的应用地址。对于本地机房集群内其他 IP 的访问，转发到对应的同机房内的内网服务器地址。

7.1.4 高可用部署方式

零信任连接器使用 Docker 部署，为保障网络高可用和稳定性，建议企业在每个数据中心创建一个连接器，然后将该连接器安装命令部署到至少 2 台以上服务器或云主机，实现多活模式，多活模式下，对该数据中心的访问会根据等价路

由算法进行负载均衡，保障网络访问的稳定可靠。

7.1.5. Docker 以及连接器部署安装

零信任连接器当前只支持 Docker 部署，若所需部署的服务器没有 Docker 环境，可以按照如下方式部署 Docker 环境：

step 1: 安装必要的一些系统工具

sudo yum install -y yum-utils device-mapper-persistent-data lvm2

Step 2: 添加软件源信息

sudo yum-config-manager --add-repo https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo

Step 3

sudo sed -i 's+download.docker.com+mirrors.aliyun.com/docker-ce+' /etc/yum.repos.d/docker-ce.repo

Step 4: 更新并安装 Docker-CE

sudo yum makecache fast

sudo yum -y install docker-ce

Step 5: 开启 Docker 服务

sudo service docker start

#Step 6: 开启 Docker 服务开机自启动

sudo systemctl enable docker

在具备 Docker 环境后，登录天翼云边缘安全加速平台控制台，访问零信任服务栏目下的网络管理，新增连接器，生成安装命令，复制安装命令进行部署。

例如：

docker pull ehub.ctcdn.cn/security-waf/sec-agent:latest && docker run -d --name sec-connector-xxxxb97b446059d477168xxxx --privileged=true --restart=always -v /etc/hosts:/etc/hosts -e TOKEN='xxxxxxxxxxxxx==' ehub.ctcdn.cn/security-waf/sec-agent:latest

8. 典型案例

8.1 某大型企业远程办公案例

8.1.1 项目背景及目标

某大型企业员工数量约 2000 人，分布在广州、北京、厦门等不同的地点，存在多地办公，移动办公的诉求，同时内部系统应用非常多，企业对安全性要求非常高。客户希望解决以下问题：

满足多地、移动办公：全国办公人员数量庞大，位置分散，需要统一的远程办公接入手段满足多地、移动办公

重保等场景可保障安全性：企业有安全要求较高，在两会、亚运会等重要场景是攻击者钓鱼的对象，需要保障安全性

内部系统权限管理：企业内部应用系统多，权限管理非常复杂，希望可以简化运维管理

8.1.2 项目整体规划

多终端、多协议接入：AOne 零信任提供统一接入方式，不同终端满足随时接入

丰富的资源提供就近接入：针对用户的办公点分配资源，结合智能调度满足就近资源，提高访问速度

多维度安全策略保障：针对重保、日常场景定制安全策略，可有效防范钓鱼、入侵等行为

内部权限精细化管理：可针对应用进行细分权限，并提供对接授权接口，可集成至企业内部工单进行标准流程管理

8.1.3 项目成果

安全性

全面提升远程办公安全：接入内部应用总计 546 个，在线用户超 1300+。通过最小化权限分配、全流量白名单管理、客户端杀毒软件监测、横向扫描防护，有效防止社工钓鱼、安全攻击。

保障内部应用安全：攻击防护超 180w 次，攻击峰值 1.8w/5 分钟，攻击类型集中在访问控制、敏感信息泄露、命令注入。

效率提升

针对每个用户、设备和应用进行精细访问控制，减少了不必要的等待时间和操作步骤。企业员工平均节省 30 分钟操作时间。

安全管理员实时监测网络流量和用户行为，快速响应安全事件，成功率 100%。

成本效益

节省 20%的网络安全成本（包含服务器、运维成本）。

9. 产品优势

9.1 提升用户体验

- 使用更加简单、便捷：员工无需进行繁杂的网络配置，仅需输入企业认证标识+账号密码或企业微信、钉钉等方式进行扫码登录，管你是在家里、在公司、在上班或者出差路上，提供不同类型终端满足随时随地接入
- 使用更加的快速、稳定：分布式集群提供高可用服务，结合智能负载均衡实现动态扩容、智能选路，有效提升访问速度，解决传统 VPN 性能差的问题

9.2 全面增强企业安全性

- 业务全面隐身，隐藏服务器端口、地址，避免增加暴露面，遗留安全隐患；
- 多维身份认证、准入判断、设备安全管控，结合终端环境感知确保身份可信、设备可信，安全登录
- 精细化最小权限管控，持续动态授权，控制权限，防止越权
- 应用访问提供横向扫描、web 入侵检测等能力，全访问保障企业安全，避免数据泄漏等

9.3 释放运维压力，降低运营成本

- 全场景办公行为审计，记录葛蕾日志，可视化展示，清楚知道谁在什么时候、用什么设备、什么方式登录，并进行了什么访问行为，让企业员工行为可视、可查、可控
- 提供一体化自助配置平台，可支持应用、权限、身份、安全策略配置一键下发；并提供可视化展示报表，运行情况一目了然
- 无需部署多套网络架构，支持多数据中心统一接入，降低网络配置管理复杂度