纳源通信

纳源零信任网关

产品白皮书

纳源通信

NAYUAN COMMUNICATION

南京纳源通信技术有限公司

目录

版权说明 4

商标信息 4

适用对象 4

获取帮助 4

1. 零信任概述 5

1.1. 零信任简介 5
1.2. 零信任理念 5
1.3. 零信任发展 6
1.4. 零信任技术 7
1.5. 零信任愿景 7

2. 需求背景 8

2.1. 业务需求 8
2.2. 合规需求 8
2.2.1. 中华人民共和国网络安全法 8
2.2.2. 网络安全等级保护基本要求（GB/T 22239-2019） 8

3. 产品概述 10

3.1. 产品理念 10
3.2. 产品架构 11

4. 产品功能 12

4.1. 访问权限身份化 12
4.2. 账号全生命周期管理 12
4.3. 多因素身份认证 12
4.4. 终端安全检测 12
4.5. 资产隐匿与隔离 13
4.6. 访问权限控制 13
4.7. 动态安全评估 13
4.8. 通信协议加密 13
4.9. 应用单点登录 13

4.10. 应用水印防泄露 14
4.11. 敏感数据检测 14
4.12. 审计记录与查询 14

5. 特性与价值 15

5.1. 统一安全管理 15
5.2. 身份与权限始终验证 15
5.3. 用户体验更便捷 15
5.4. 资产隐身更安全 15
5.5. 访问权限更清晰 15
5.6. 部署方便易落地 16

6. 应用收益 16

6.1. 管控风险 16
6.2. 降低成本 16
6.3. 改善管理 16
6.4. 安全合规 17

版权说明

© 版权所有 2005-2022，南京纳源通信技术有限公司

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属纳源通信公司所有，受到有关产权及版权法保护。任何个人、机构未经纳源通信公司的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

商标信息

Safetybase、LogBase 均是杭州南京纳源通信技术有限公司注册商标，受商标法保护。

适用对象

本文档适合于各行业信息部门相关技术人员、服务人员、信息系统审计人员等。

获取帮助

安全相关资料可以访问公司网站：http://www.logbase.cn

您也可以通过 Email 来获取资料或反馈信息：support@logbase.cn

获取更详尽有关纳源通信网络安全专业服务信息、商务信息，您可通过如下方式联系我们：

24 小时服务热线：400-678-1500

企业 QQ 客服：400-678-1500

1. 零信任概述

1.1. 零信任简介

随着云计算、大数据、物联网、移动办公等新技术与业务的深度融合，网络安全边界也逐渐变得更加模糊，传统边界安全防护理念面临巨大挑战。传统的网络安全架构理念是基于边界的安全架构，企业构建网络安全体系时，首先寻找安全边界，把网络划分为外网、内网、DMZ 区等不同的区域，然后在边界上部署防火墙、入侵检测、WAF 等边界防护类产品。

这种网络安全架构假设或默认了内网比外网更安全，在某种程度上预设了对内网中的人、设备和系统的信任，忽视加强内网安全措施。不法分子一旦突破企业的边界安全防护进入内网，会像进入无人之境，将带来严重的后果。

在这样的背景下，零信任架构（Zero Trust Architecture,ZTA）应运而生。它打破传统的认证，即信任、边界防护、静态访问控制、以网络为中心等防护思路，建立起一套以身份为中心，以识别、持续认证、动态访问控制、授权、审计以及监测为链条，以最小化实时授权为核心，以多维信任算法为基础，认证达末端的动态安全架构。

1.2. 零信任理念

最早提出零信任一词的是 Forrester 研究咨询公司的分析员 John Kindervag，他提出了三个核心理念：

- 不再以一个清晰的边界来划分信任或不信任的设备；
- 不再有信任或不信任的网络；
- 不再有信任或不信任的用户。

所以与传统的边界模型“信任但验证”不同，零信任的原则是“从不信任、始终验证”。传统网络安全都专注于边界防御，授权主体可广泛访问内网资源，而根据 Evan Gilman《Zero Trust Networks》书中所述，零信任网络建立在五个假设的前提之下：

- 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。

简而言之默认情况下不应该信任网络内部和外部的任何人/设备/应用，需要基于认证和授权重构访问控制的信任基础。零信任对传统访问控制机制进行了颠覆，其本质是以身份为基石的动态可信的访问控制。

1.3. 零信任发展

零信任的最早雏形源于 2004 年成立的耶利哥论坛(Jericho Forum)，其成立的使命正是为了定义无边界趋势下的网络安全问题并寻求解决方案。2010 年，零信任这个术语正式出现，并指出默认情况下所有的网络流量都是不可信的，需要对访问任何资源的任何请求进行安全控制，零信任提出之初，其解决方案专注于通过微隔离对网络进行细粒度的访问控制以便限制攻击者的横向移动。

随着零信任的持续演进，以身份为基石的架构体系逐渐得到业界主流的认可，这种架构体系的转变与移动计算、云计算的大幅采用密不可分。2014 年开始，Google 基于其内部项目 BeyondCorp 的研究成果，陆续发表了多篇论文，阐述了在 Google 内部如何为其员工构建零信任架构。BeyondCorp 出发点在于仅仅针对企业边界构建安全控制已经不够了，需要把访问控制从边界迁移到每个用户和设备。通过构建零信任，Google 成功地摒弃了对传统 VPN 的采用，通过全新架构体系确保所有来自不安全网络的用户能安全地访问企业业务。

通过业界对零信任理论和实践的不断完善，零信任已经超越了最初的网络层微分段的范畴，演变为以身份为基石的动态可信访问控制，聚焦身份、信任、业务访问和动态访问控制等维度的安全能力，并通过信任等级对权限进行动态调整，形成具备较强风险应对能力的动态自适应的安全闭环体系。能够覆盖云环境、大数据中心、微服务等众多场景的新一代安全解决方案。

1.4. 零信任技术

在零信任的安全理念和战略被提出后，在业界引起了极大的关注，出现了各种技术实现，其中三大技术“SIM”（SDP，IAM，MSG）具有重大影响力，并影响了随后的一个标准，由美国国家技术标准局 NIST 制定的《零信任架构》。

SDP（软件定义边界）

CSA（国际云安全联盟）于 2013 年成立了 SDP 工作组，由美国中央情报局 (CIA) 的 CTO Bob 担任工作组组长，并于 2014 年发布了 SPEC 1.0；通过构建虚拟的企业边界，以及基于身份的访问控制来实现，目标是应对边界模糊化带来的粗粒度控制问题，以及保护企业数据安全。

IAM（身份及访问管理）

基于早期的“基于角色的访问控制(Role-Based Access Control,RBAC)”，定义和管理每个网络用户的身份角色及其所需资源的访问权限，根据网络用户身份角色生命周期，对其所需资源访问权限进行动态管理

MSG（微隔离）

由 Gartner 在其软件定义数据中心(Software Defined Data Center, SDDC)的相关技术体系中提出，提供主机（容器）间安全访问控制，区别于过去的安全域间的安全访问控制，对东西向流量进行可视化管理，云安全的核心技术模块。

1.5. 零信任愿景

依托 IAM 技术、终端环境感知技术，重构企业身份体系和身份策略，推动网络人员身份的可信任；改变传统的认证方式，构建先认证后连接和持续认证机制，提升网络的防护能力；结合终端、EDR、业务行为、网络态势等因素，建立持续信任评估机制和模型，支撑动态自适应访问控制权限管理，保护业务和数据的安全性；支撑远程办公、大数据中心、云安全平台等多种场景的安全防护。

2. 需求背景

2.1. 业务需求

企业应用上云正在逐渐普及，根据《中国企业上云指数(2018)》报告，全国企业上云比例已达 43.9%，美国企业上云率已经达到 85%以上。同时移动办公的需求也在日益增加，员工、合同工、合作伙伴等都会需要随时随地在任何设备上访问使用，增加了便捷性，提高了生产率，但同时也带来了新的安全风险。网络边界的界限变的越来越模糊，全新的变化带来了全新的挑战：

无边界：空间、时间等的无界化，打破了传统的网络边界和区域防护。

不确定：人员、设备、应用等的不确定性带来安全策略和安全防护的挑战；

威胁：种类多、变化多、动态化、攻击面大、危害大、目标明确、组织严密、手段先进、隐蔽性好等，使得堵不胜堵、防不胜防。

2.2. 合规需求

2.2.1. 中华人民共和国网络安全法

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

2.2.2. 网络安全等级保护基本要求（GB/T 22239-2019）

- **身份鉴别**

1. 应对登录网络设备、操作系统和数据库系统的用户的用户进行身份鉴别；
2. 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

3. 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

- **访问控制**

1. 应启用访问控制功能，依据安全策略控制用户对资源的访问；
2. 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
3. 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

- **安全审计**

1. 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；
2. 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；
3. 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

3. 产品概述

3.1. 产品理念

纳源零信任网关基于“零信任”的架构理念，建立以身份为基石、业务安全访问、持续信任评估和动态访问控制，这些关键能力构建一个安全的网络访问解决方案。其核心思想是默认情况下不应该信任网络内部和外部的任何人/设备/系统，基于身份认证和授权重构访问控制的信任基础。纳源零信任网关的设计理念:

身份鉴别

用户在访问业务之前，必须经过基于 SPA 认证、PKI 机制、MFA 认证、设备认证，终端与环境检测等方式，才能访问授权业务;

资产隐匿

零信任网关、资产与资产之间均隐身不可见，防止嗅探及 DOS 攻击，从任何访问来源或资产之间访问，均需进行 SPA 认证;

持续性验证

所有访问请求使用 TLS 加密，验证每一个访问请求和数据包，确保身份和访问权限的有效性;

最小权限授权

用户只能访问授权 IP、端口、账号，资产之间相互隔离，只允许信任关系访问;

实时访问分析

基于访问客体（账号、设备、IP 等），实时检测设备、环境、IP、访问主体等变化及敏感内容的检测与越权行为分析，进行预警或者阻断;

动态信任评估

基于访问关系，动态检测与分析访问客体（账号、设备、IP 等）与访问主体的特征，进行动态权限回收，确保最小权限原则。

3.2. 产品架构

纳源零信任网关由零信任客户端，零信任网关和零信任服务端组成，功能包括包含用户管理、资产管理、身份认证、终端检测、SDP、WEB 代理、访问授权、智能分析和审计记录等模块组成。实现了用户的账号全生命周期管理，资产的隐身与访问授权，访问的身份认证、环境检测、权限控制、安全通信、动态评估及审计记录。

4. 产品功能

4.1. 访问权限身份化

纳源零信任网关通过对每个用户分配一个单独的数字身份，实现访问权限身份化。在用户访问时对其进行身份验证（包括账号、设备、环境），并根据其身份授权指定的资源以及在其整个访问授权周期中监控和验证这些身份的权限及数据。确保用户基于最小访问权限原则下，能够正确的访问其需要访问的资源。

4.2. 账号全生命周期管理

纳源零信任网关支持账号的全生命周期管理，通过 AD 域、LDAP、钉钉、企业微信及其他 Oauth2.0 等方式进行账号的自动同步，实现全自动化的账号生命周期管理，无需管理员手动操作管理，减少繁琐复杂的身份信息管理工作，同时也可以通过及时关停人员账号和减少授权错误率来提升企业整体的业务安全系数。

4.3. 多因素身份认证

纳源零信任网关支持账号的多因素认证，通过 Google 验证器、短信、邮件等二次验证以及钉钉、企业微信和其他 Oauth2.0 授权认证等方式，为账号认证额外增加一层保护，进一步提高帐号安全性。

4.4. 终端安全检测

纳源零信任网关支持终端安全检测，强制对用户终端实施企业安全策略，检查用户补丁安装、安全软件启用以及高危端口开放情况，通过终端安全检测方可进行连接认证，确保用户终端安全，防止失陷终端接入，阻止威胁入侵，有效加强用户终端的主动防御能力。

4.5. 资产隐匿与隔离

纳源零信任网关支持资产微隔离，通常黑客已经攻占了一个服务器，那么他就可以利用这个服务器做跳板，进一步攻击网络中的其他服务器。资产隐匿与隔离可以阻止这种来自内部的横向攻击与探测。通过对服务器的访问权限控制，只允许受信服务器访问自身的指定端口，遵循最小访问权限原则，可以有效的阻断勒索病毒在内部网络中的蔓延，降低黑客的攻击面。

4.6. 访问权限控制

纳源零信任网关通过访问权限的集中管理，实现对用户、设备、环境、系统、应用及账号进行精细化的访问权限配置，遵循最小访问权限原则，确保用户与资源间具有所需执行必要任务的最小权限，避免过大以及不必要的权限所带来的安全隐患。

4.7. 动态安全评估

纳源零信任网关通过对访问权限的动态评估，对长期不访问的资源权限进行动态回收，如需访问可再次申请，避免一些人为授权失误或者权限冗余，将这些不必要的访问权限进行回收，确保其最小访问权限。

4.8. 通信协议加密

纳源零信任网关支持通信协议加密，由于明文传输协议带来了诸多不安全因素如协议劫持、协议破解、中间人攻击等方式，造成网络攻击、渗透及数据泄露等安全事件。纳源零信任网关通过对网络与 WEB 代理，对原本协议进行代理加密，防止网络数据被嗅探，减少不必要的安全隐患。

4.9. 应用单点登录

纳源零信任网关通过表单代填及 Oauth 认证方式，实现对 WEB 应用的账号的 SSO，用户登录后选择相应应用及账号即可完成登录，无需再次输入应用账号及密码，也可根据用户当前登录账号进行 SSO。

4.10. 应用水印防泄露

纳源零信任网关支持对 WEB 应用访问嵌入水印，水印样式、字体、颜色、透明度及大小等均可任意配置，且不影响用户的体验与操作；可以提高威慑性，避免敏感数据被截图、拍摄与复制，如果泄露可根据水印标记进行溯源追责。

4.11. 敏感数据检测

纳源零信任网关支持对 WEB 应用的敏感信息识别，在用户访问敏感数据时，通过不同的敏感信息规则，对命中敏感信息的访问进行阻断、脱敏以及告警，能够有效的防止敏感信息数据泄露的安全事件发生。

4.12. 审计记录与查询

纳源零信任网关支持所有访问、认证日志的记录，可通过用户访问时间、IP、应用等条件进行查询，快速定位访问事件，对异常访问事件进行追踪溯源。

5. 特性与价值

5.1. 统一安全管理

纳源零信任网关通过对资源的统一安全管理，包括用户、资产、应用、访问权限等管理，极大的简化了管理员的日常维护工作，减少分散管理所带来的用户、权限等不一致的安全隐患。

5.2. 身份与权限始终验证

纳源零信任网关通过对网络及协议的代理，实现包级别的访问认证，每一个访问的数据包都进行 SSL 校验，确保数据包的合法性，拒绝一切非法请求的数据包，并实时检测用户环或安全级别变化，一旦异常马上拒绝。

5.3. 用户体验更便捷

纳源零信任网关基于多种 MFA 认证方式，直接通过验证码、钉钉或企业微信扫码等方式即可登录，无需再因为密码的安全性、繁琐、丢失所烦恼；登录门户后可直接选择应用，不需再保存标签或者记录 URL，选择应用后并直接完成 SSO 单点登录，无需二次输入账号信息。

5.4. 资产隐身更安全

纳源零信任网关基于 SDP 与微隔离技术，实现对自身及资产的隐匿，防止被嗅探及攻击；所有访问资产都需要通过纳源零信任网关的严格认证，确保了只允许拥有访问权限的用户的访问。

5.5. 访问权限更清晰

纳源零信任网关通过统一的访问权限管理，可更加清晰对所有用户、资产之间的访问权限进行管理及可视化，无需要再通过防火墙或交换机配置复杂的 ACL 控制，降低网络维护和排查工作量。

5.6. 部署方便易落地

纳源零信任网关落地无需对网络进行任何改造，旁路接入即可，也需要对 WEB 及服务器进行改造，即插即用，降低维护成本，节省大量改造费用。

6. 应用收益

6.1. 管控风险

纳源零信任网关通过身份认证、资产隐身、权限控制等方式大大提高数字资产安全性，增加了攻击者的难度，可以帮助企业降低运营风险。对敏感信息及攻击行为进行追踪分析，从而使得风险能够快速识别，无论是较难防的 APT 高级持续威胁还是内鬼，企业可以快速的采取相应的风险应对手段，进行有效的防范，因此可以有效地降低总体安全风险。

6.2. 降低成本

纳源零信任网关通过策略与动态评估，将不需要访问资源的用户、设备与应用的权限进行回收，基于最小权限原则，使得恶意行为受到限制，缩小被攻击面，大大降低了安全事件的数量，使得企业能够节约时间与人力资源来迅速恢复少数的安全事件。另外使资产隐身对让攻击者难以嗅探及发现，这样使得系统和应用存在一些新出现漏洞不会被立即利用，给予企业足够的修补周期，也可以降低消耗在漏洞与补丁管理的成本。

6.3. 改善管理

纳源零信任网关对企业资产统一管理认证，使得企业资产得到更有效的控制，无论资源分布在企业内部各部门，还是在公有云、混合云，多云环境中。基于资产访问关系，对网络环境更加清晰可见，对访问权限管理更加便捷，通过资产隐身与隔离来防御包括外部、云服务商及管理员在内的恶意行为，大大提高企业安全管理。

6.4. 安全合规

纳源零信任网关解决方案与新出台的重要安全法律、法规、标准高度吻合，例如《网络安全法》、《网络安全等级保护 2.0》、《数据安全法》与《个人信息保护法》、GDPR（通用数据保护条例）、FedRAMP（联邦风险与授权管理计划）等。架构本身已经具有多项安全控制措施满足合规条款，能够充分减少违规事件，同时使得网络架构更清晰，让合规审计工作更加容易进行，有效的满足安全合规。