Nikawal

Nikawal
零信任安全解决方案

2023年12月

嘉兴二川科技有限公司

CONTENTS/目录

第一章：

零信任安全的发展与概念

零信任安全的发展与概念 - 企业网络安全新常态

- 随着业务的发展需要，远程办公需求激增，接入的个人设备的安全性成为企业最薄弱的环节
- 远程办公需求下带来的安全问题 也成为企业网络安全的新常态

数字化转型趋势

1. 协同办公
2. 产业链的深化合作
3. IT架构变化（云）

趋势带来的安全性挑战

零信任安全的发展与概念 - 网络安全合规要求更加严格

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：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

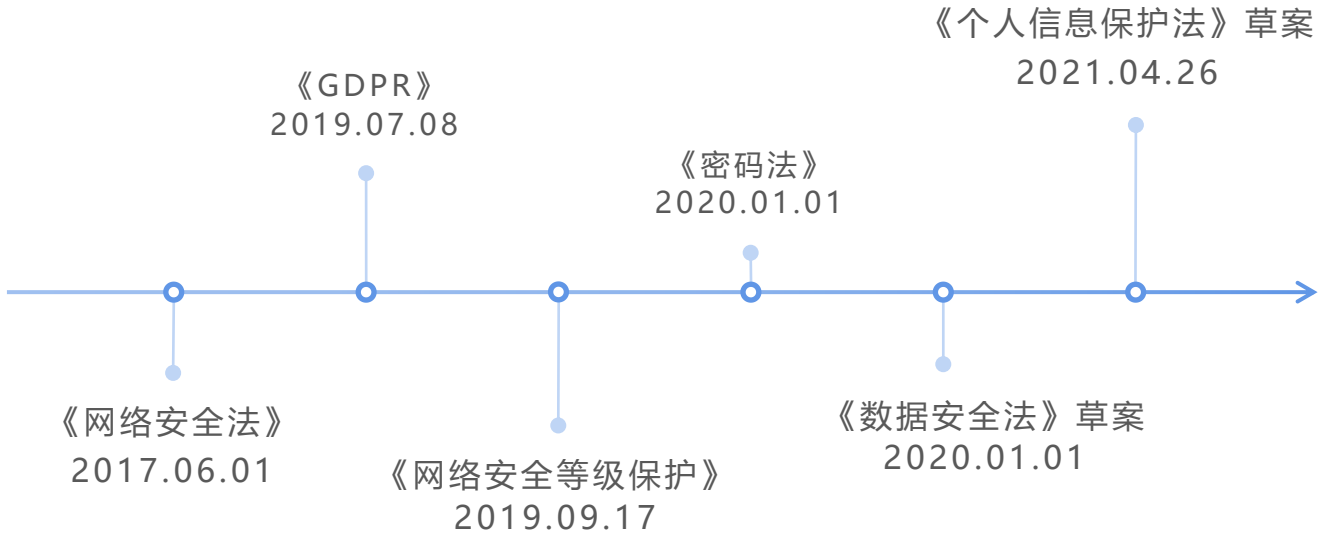
（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。



零信任安全的发展与概念 - 企业安全建设所面对的挑战

如何用一个更符合安全趋势的理念来开展整体的安全建设?

网络边界消失

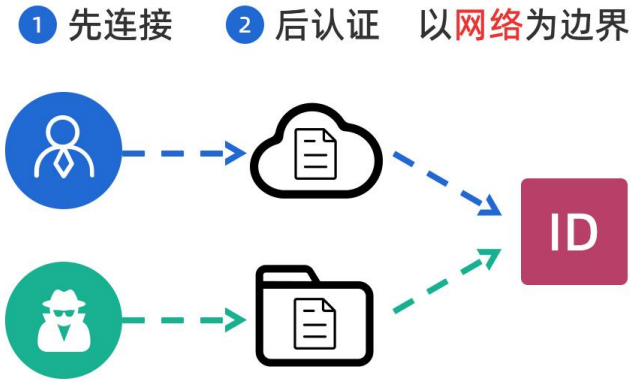
新型网络攻击

数字化转型新挑战

满足安全合规

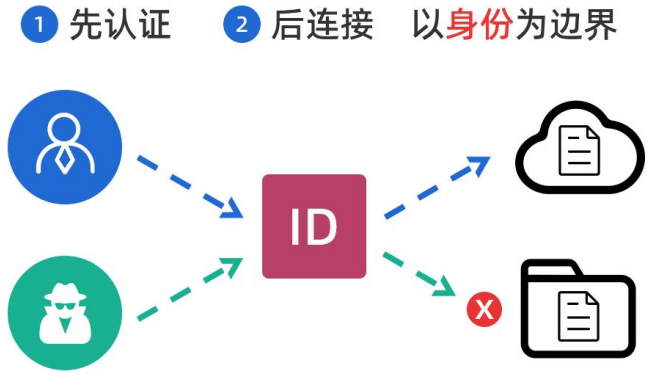
零信任安全的发展与概念 - 运用零信任理念来构建企业的安全体系

传统架构



- 通过防火墙、VPN、IDS/IPS等设备建立企业的网络边界
- 构建基于内网的信任体系，认为网络内部的人员与设备是可信的

零信任架构



- 从不信任，始终验证
- 基于身份、设备、应用等
- 看不见、拿不走、可追溯、能销毁
- 云端管、动静用、前中后
- 防范和保护：隐身于防护并存
- 智能化和自适应

零信任安全的发展与概念 - 什么是零信任

Q 什么是零信任?

A 零信任既不是技术也不是产品，而是一种安全理念。 “永不信任，始终验证”

（在假定网络环境已经被攻陷的前提下，当执行信息系统和服务中的每次访问访求时，都需要进行人/ 设备/应用等尽肯能多的安全因素进行全面、动态、智能的访问控制验证。以降低其决策准确度的不确定性，并通过端到端的加密，保证资源访问的安全性。）

安全理念

- 永不信任，始终验证
- 网络环境无时无刻不危险
- 网络内部外部时时受到威胁
- 网络位置无法决定可信度
- 所有人/物/网流均需认证授权多源动态智能安全策略

安全战略

- 领导团队自上而下推动与引导
- 管理能力与技术能力双驱动
- 战略高于单一产品
- 咨询赋能发挥优势

安全架构

- 零信任参考架构
- 零信任IAM身份访问管理
- SDP软件定义边界
- MSG微隔离

零信任安全的发展与概念 - 零信任的功能特性

降低风险

强化资产的发现，任何应用与服务都会被识别并给予身份，对敏感信息的攻击途径会被分析，数据流图使网络的透明度增加

安全合规

使安全审计师更容易看清网络，便于审计工作并减少违规发现，其架构本身已经具有多项安全控制措施满足合规条款，包括国际与行业安全标准等

降低成本

将保护目标聚焦到负载与数据，通过策略与控制排除不需要访问资源的用户/设备/应用，恶意行为被限制大大降低安全事件数量，企业有更多时间与资源来迅速恢复少数的安全事件，降低业务成本

有效控制

在公有云，混合云，多云环境下把网络通信限制在有身份被验证的负载中，防止包括云服务商管理员在内的各方向攻击

业务敏捷

摈弃了静态边界防御的慢速与不方便的检查，安全不再是业务的绊脚石，使业务能更快上线，用户的安全体验更好，增加了业务的速度与敏捷性

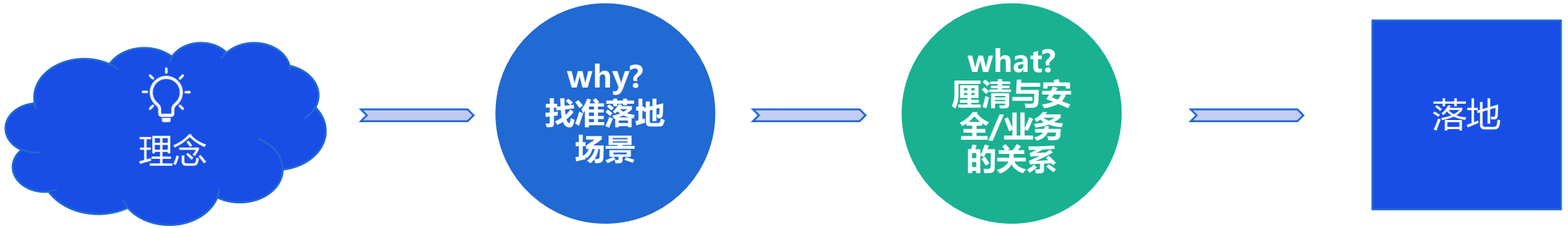
改善管理

对于数字化转型依赖软件与应用的组织机构，零信任能很好地支持DevOps，使应用部署适配业务优先级减低各组织部门之间的摩擦

第二章：

零信任安全的探索与实践

零信任安全的探索与实践 - Nikawal的零信任探索之路



零信任安全的探索与实践 - Nikawal的零信任阶段性解决方案

阶段一： 安全的基石，身份与设备的重塑

零信任安全的探索与实践 - Nikawal的零信任阶段性解决方案

阶段二： 构建多维的访问控制策略及体验

- 动态身份验证
- 内网隧道打通

零信任安全的探索与实践 - 零信任模型框架

业务场景层	远程办公 / 产业互联网 / 工业互联网 / 企业上云 / 供应链 / 外部协作 / 其他
技术安全层	身份 / 终端 / 网络 / 应用 / 基础设施 / 数据
职能安全层	身份 / 终端 / 网络 / 应用 / 基础设施

第三章：

零信任安全应用场景和解决方案

零信任安全应用场景和解决方案 - 应用场景多样化

远程办公

随着远程办公的普及，当员工需要在家中或其他地点访问企业资源时，零信任可以确保只有经过身份验证和授权的用户才能访问网络资源，无论他们身在何处。

多云和混合云环境

组织可能使用来自不同云服务提供商的服务，或者同时使用公有云和私有云。零信任策略可以帮助统一管理复杂的多云和混合云环境中的访问权限，并确保数据安全。

合作伙伴和第三方访问

组织通常需要与合作伙伴、供应商和其他第三方共享资源。零信任可以为这些外部实体分配临时访问权限，并限制其访问范围，防止数据泄露。

内外网混合办公

为企业职场、分支提供内外网一致的访问体验，解决内网权限策略失效等安全问题，实现基于身份的访问控制和动态评估，减少安全运维工作量、提升实际安全效果。

零信任安全应用场景和解决方案 - 应用场景（远程办公）

- **身份认证以及多维度的安全评估，实现无边界安全办公**

安全性更高

- 控制与数据平面分离，产品更稳定
- 终端安全一体化，安全运营闭环
- 业务隐身到零信任网关后，缩小攻击面

用户体验更好

- 网络抖动或IP跳变时，仍能保持不掉线
- 弱网络环境下，实现业务网络加速

扩展性更强

- 动态已扩容，性能强

零信任安全应用场景和解决方案 - 应用场景（移动安全办公）

- **企业微信/飞书/LDAP/钉钉第三方组织管理接口打通，实现移动安全办公**

第三方联动

第三方组织接口打通，完成身份信息同步，实现快捷的业务访问

收敛暴露面

企业应用通过零信任网关对外提供服务，减少攻击面

移动办公平台

动实现基于第三方的安全移动办公平台，为客户提供脱敏的安全能力

零信任安全应用场景和解决方案 - 应用场景（全球SASE接入）

- **基于云架构零信任安全体系**

云原生安全赋能业务

客户可轻松构建自己的物业安全体系

轻量交付动态扩容

业务安全体系的建设，支持动态扩容

安全服务、运维托管

可享受云原生提供的各类安全服务，提升业务运维效率

零信任安全应用场景和解决方案 - Nikawal零信任产品解决方案

产品概况

NSPA(Nikawal Secure Private Access) 是以SASE(Secure Access Service Edge)为安全框架的零信任(ZTNA)解决方案，帮助企业更好的保障企业的网络安全。企业通过NSPA，可以安全的让成员连接企业的应用，更好的保护企业的应用。NSPA是云原生的服务，分钟级别的交付替换传统的VPN方案。

零信任安全应用场景和解决方案 - Nikawal零信任产品优势

基于身份

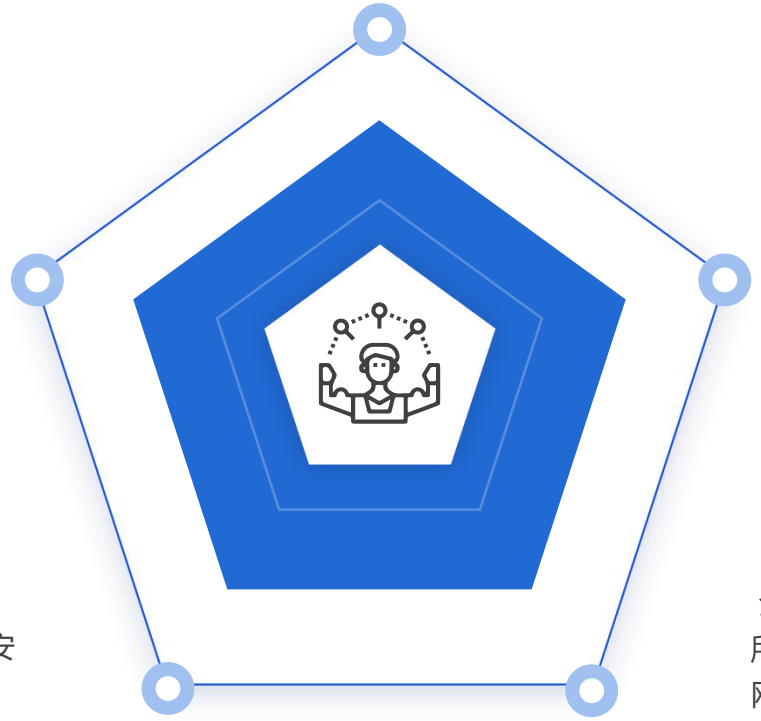
点传统的VPN是通过打通到应用的网络，来访问应用，只要进入网络就可以访问网络中的任何应用。传统VPN如果需要区分访问者，主要通过分配IP，然后针对不同IP分配不同的防火墙规则。而基于身份的方式，和网络进行解藕，可以更灵活的配置规则，尤其是在环境复杂的网络下。

可靠性

连接用户终端和应用终端的云网络，使用云原生技术，高可靠的分布式部署在公有云，私有云，机房等环境。同时支持对应用部署多个应用终端，达到云网络和应用都高可靠。

灵活性

企业自助通过平台增加和修改应用，增加和调整企业成员，灵活根据态势来调整策略，保障企业应用安全。



安全连接

应用无需针对访问者开放端口，接受请求，做复杂的配置。应用只需允许应用终端来访问，通过应用隐藏来提升应用安全。应用终端和客户终端都通过tls加密和云网络安全连接，保证通信数据安全。

统一管控

企业通过NSPA，可以对企业所有应用进行统一管理，对企业所有成员访问应用的权限，策略进行统一配置。无论应用所在网络环境多复杂，通过简单的配置就可以保护企业网络和应用的安全。NSPA还提供了强大的统计功能和监控功能，全局了解企业成员和应用的实时和历史数据。

零信任安全应用场景和解决方案 - 产品价值

替换传统VPN和防火墙

用户直接连接到应用程序，而不是网络，最大限度地减少了攻击面，消除了通过网络对网络中应用的攻击。

满足多样化的远程访问

支持远程用户、总部、分支机构和第三方合作伙伴等对内部应用访问。

阻止用户的危害行为

通过上下文分析、风险检测、威胁隔离，降低来自用户的潜在危害行为。

降低产品总拥有成本（TCO）：

通过统一平台，无需采购各种产品，就可以为用户，设备，第三方等提供安全，可靠的网络。

零信任安全应用场景和解决方案 - 产品组件

用户终端

用户终端是访问应用的主体，包含IOS，Android 移动用户端，包含Windows，Macos 电脑用户端。

云网络

云网络部署在云中,idc机房,企业机房等提供网络通信连接，网络安全等。云网络和客户终端，应用终端一起作为一个整体来保护企业应用。

应用终端

应用终端将企业保护的应用安全得连接到云网络中。应用终端支持硬件形式交付，也支持软件形式：比如容器镜像，虚拟机等。

网络插件

用户可以通过用户终端访问应用，也可以使用插件访问应用。应用使用应用终端连接云网络，也可以使用插件连接云网络。

管理平台

管理平台管理和配置企业所有用户，用户终端，应用终端；管理和配置访问应用的策略；实时洞察当前用户访问应用的行为。

零信任安全应用场景和解决方案 - 产品特性

NSPA提供了零信任网络安全功能，保障应用安全，无论用户以何种方式访问应用。NSPA精准提供用户访问应用的流日志，洞察网络行为；隐藏应用，减少应用被攻击情况；动态细粒访问策略，最小化灵活的授权成员允许访问的应用。

应用网络环境松耦合

NSPA保护企业应用，和企业应用所在网络环境松耦合。无论应用所在网络环境怎样，只要部署的应用终端达到两个条件，就可以达到零信任网络。第一，应用终端可以访问应用；第二，应用终端可以访问云网络。

隐藏应用

应用无需对所有外部访问者提供服务，而是只允许应用终端访问应用。应用终端一端连接云网络，另外一端连接应用，以桥梁身份间接提供客户终端访问应用，从而减少应用被攻击面。

流日志

NSPA提供流日志功能，记录客户终端的访问和响应流量，帮助企业监控成员访问应用行为。通过NSPA，企业可以洞察任何一个员工通过什么客户终端在什么时间访问了企业哪个应用。除此之外，NSPA通过AI大数据分析，可以推测员工访问应用行为是否异常。

多样化态势

NSPA支持多样化态势，针对成员访问应用，支持的态势有：时间，客户终端使用的系统，客户终端使用的软件版本，客户终端当前请求的IP地址等。

零信任安全应用场景和解决方案 - 产品特性

云网络

NSPA将网络功能云化部署在公有云，私有云，机房等。通过云原生技术，高可靠的连接客户终端和应用，为企业提供零信任网络安全。

分流

客户终端支持4层和7层分流功能，根据管理平台配置，应用的流量送到云网络中，对于非应用流量，客户终端直接访问。

基于身份

NSPA提供基于身份的应用访问，用户终端提供全网唯一的身份信息访问应用。

动态策略

默认保护应用是最小化限制成员访问应用，NSPA支持动态策略，可以根据态势实时动态调整成员访问应用的策略。

DNS服务

客户终端支持DNS服务，对于客户终端7层请求，可以快速响应，降低客户终端访问应用的延时。

应用健康检查

NSPA支持健康检查功能，可以周期性发送探测报文，检查应用的连通性。

零信任安全应用场景和解决方案 - Nikawal产品的零信任架构

终端设备准入

- 零信任环境检查持续验证
- 终端设备认证
- 多因素身份认证、单点登录

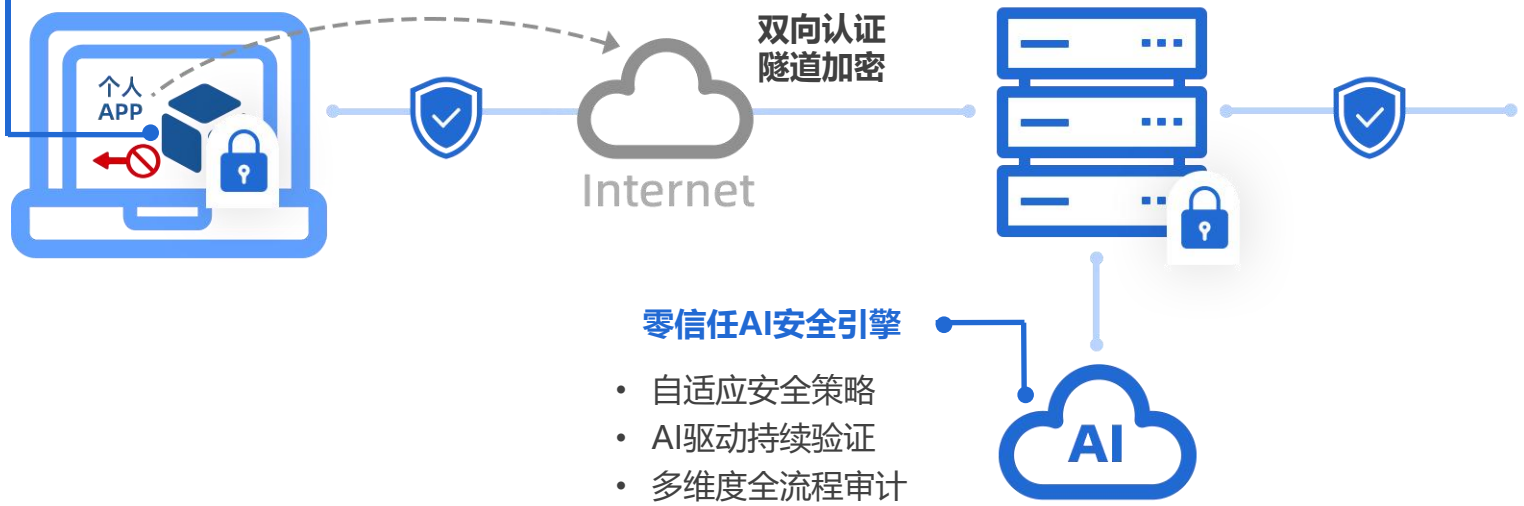
零信任安全网关

- 基于身份与属性
- 精细化访问控制
- 最小权限访问

双向认证
隧道加密

零信任AI安全引擎

- 自适应安全策略
- AI驱动持续验证
- 多维度全流程审计



业务系统

业务对外不可见

- 文件系统
- CRM系统
- 邮件服务器
- ERP系统
- 管理信息系统

零信任安全应用场景和解决方案 - Nikawal零信任核心能力架构图

身份安全	多种接入方式：token、本地化身份识别.....	手机软token	单点登录	第三方服务

链路安全	设备安全					应用安全	接入安全
	终端安全防护	应用管理	安全基线检测	数据保护	扩展能力		
身份-终端-应用-业务访问控制策略	补丁	软件统计数据	合规检测	外设控制	数据备份	远程特征收集	公有云接入安全
流量加密	基础加固	软件开发	漏洞补丁检测		文件保护	白名单	私有云接入安全
服务隐藏	实时防护	脚本分发	审计日志	文件变更审核	远程协助	进程审计	混合云接入安全
全球加速		文件分发	访问控制		办公应用		

Nikawal

THANK YOU

感谢您的观看

嘉兴二川科技有限公司

2023年12月