“验证零信任安全”白皮书

目录

简介

本文档介绍与零信任相关的信息，以及如何使用该信息来保护企业。

执行摘要

零信任代表一种模型，该模型假定任何用户、设备或应用程序（无论是网络外部还是网络内部）都不能视为安全，并且必须验证每个用户或应用程序才能允许其访问网络资产。

在虚拟化和内部资源快速迁移到公共云、私有云和混合云中，这一概念已变得更加重要。

零信任一词由Forrester在2010年发布其零信任网络架构报告时创建。

切记，零信任必须作为业务层面的战略开始实施，以保护重要的业务利益和计划。

零信任支柱

什么是零信任？

零信任是一种战略方法，它包含各种技术，有助于为当今的基础设施实现更切实的安全保护。它是一个安全架构和企业方法，旨在有效地协调当今的技术、实践和策略的组合。

它代表着我们安全方法的发展历程，提供了一种全面、可互操作且全面的解决方案方法，将多个供应商的产品和服务融为一体。

零信任基于许多已确立的技术，例如网络分段、多因素身份验证和网络访问控制。

零信任为何重要

零信任有助于保护企业免受未授权用户、漏洞和网络攻击。您可以持续验证用户和设备的身份，并仅允许他们执行其工作所需的权限，从而将安全事件的风险降至最低。

市场研究表明，全球零托管安全市场规模预计将从2022年的270亿美元估计值到2027/2028年的600亿美元，届时复合年均增长率约为17%。

动机：

- 基于目标的网络攻击频率提高
- 数据保护和信息安全的法规增长
- 降低业务和组织风险的需求更大
- 随着越来越多的服务迁移到云，集中式数据部署超越了数据边界，并放大了安全风险。
- 在整个访问过程中确认用户身份的需要，而不仅仅是在初始阶段

一次勒索软件攻击造成的损失高达500万美元。网络犯罪分子在针对企业时不会区别对待。

最近的CIO和CISO调查显示，零信任是五大优先事项之一。CISO表示，向远程工作的转变、劳动力短缺以及网络安全攻击的大幅增加都要求保护他们在企业中的现有系统。

传统与零信任模型

传统环境是在环境构建之后添加安全性的环境。通常，它们是平面网络，其防御措施围绕网络边缘构建，以阻止来自Internet的攻击。

零信任通常用于强调通过加密、安全计算机协议、动态工作负载和数据级身份验证和授权相结合的方式在多个级别上保护组织的系统和数据的需求，而不是仅仅依赖于外部网络边界。

随着工作负载越来越多地通过云交付，而移动终端成为应用和数据访问的规范，传统的以外围为中心的安全架构效率较低。

零信任架构框架

零信任架构框架处理对系统、应用和数据资源的访问限制，这些限制适用于那些特别需要访问并已经过验证的用户和设备。他们必须持续进行身份认证和安全状态验证，以确保每个资源获得适当的授权才能提供访问权限。

该框架基于NIST特别出版物800-207，旨在提供将零信任安全概念迁移并部署到企业环境的路线图。

有效的零信任架构框架可跨这七个主要核心组件进行协调和集成。

- 零信任网络是零信任策略的一个重要特征，零信任策略是指对网络进行分段或隔离网络资产，以及保持对网络之间通信的控制。此外，它还可以确保可信连接的安全，以扩展远程使用的工作空间。
- Zero Trust Workforce包含用于限制和实施用户访问的方法，其中包括用于对用户进行身份验证以及持续监控和管理其访问权限的技术。这种访问由DNS、多重身份验证和网络加密等技术提供保护。
- 零信任设备解决了隔离、保护和管理所有联网设备的需求，随着移动性和物联网的加深，这些设备不断增长，为攻击者创造了极大的漏洞。
- 零信任工作负载可保护运行关键业务流程的前后应用堆栈。专注于保护数据中心内应用、数据和服务之间的东/西流量，以更好地保护关键应用。
- 零信任数据是指对数据进行分类和分类的方法，与保护和管理数据的技术解决方案相结合，包括数据加密。
- 可视性和分析是指为自动化和协调提供感知，使管理员不仅能够看到而且能够了解其环境中的活动（包括实时威胁的存在）的技术。
- 自动化和协调包括机器学习算法和人工智能等工具和技术，可自动对网络和数据中心资产进行分类，并建议和应用分段和安全措施、策略和规则自动生效；因此，可减轻安全团队的负担并加速攻击缓解。

零信任和分段

每个基于网络的资源都必须以最小权限原则加以保护和分割。这最好通过资产管理系统来实现，该系统可以控制各种用途的凭证和访问权限。

零信任分段需要包括品牌保护、有限的攻击面、提高的网络稳定性，以及支持快速服务部署。

为了进一步实现对单个资源的保护，可以使用微分段。当标记值插入到以太网帧中以唯一地标识资源时，可以使用可扩展组标记(SGT)。此外，基础设施设备包括智能交换机、路由器或下一代防火墙，这些设备可用作网关设备来保护每项资源。

可视性、分析和自动化

必须全面了解组织的所有资产以及与这些资产关联的任何活动。这是零信任的基础。

为了提供动态的策略和信任决策，需要不断收集分析信息。我们的零信任架构方法侧重于SDN策略的核心逻辑组件，通过策略引擎和策略管理员形成一个控制平面，以限制通过数据平面中的策略实施点访问资源。

零信任架构所需的功能，可提供更好的网络环境、学习和保证，以安全地完成任务：

- 对访问用户、设备、应用、工作负载和数据的精细微分段。
- 执行安全策略的任意位置，包括LAN、WAN、数据中心、云和边缘。
- 全面的身份管理 — 将身份和访问管理扩展到包括用户、设备、应用、工作负载和数据的身份，这些身份通过软件定义的访问成为新的微型边界。
- 利用全球威胁情报和源的集成威胁防御。
- 对组织网络的完全自动化、灵活控制，以按照实现目标所需的规模、性能和可靠性安全地运行。

零信任步骤

全面零信任安全性的关键是将安全性扩展到整个网络环境，无论是局域网、数据中心、云边缘还是云。合规性当然是强制性的。

这种安全性必须包括您组织的网络环境的全面可视性。全面零信任中心的主要步骤如下：

- 识别设备和敏感数据。对设备、敏感数据和工作负载进行识别和分类。
- 了解您的敏感数据流。
- 构建您的零信任分段策略。每个基于网络的资产都必须以最小权限和严格执行的精细控制的原则进行保护和适当分段，以便用户仅能访问执行其工作所需的资源。
- 实施策略和状态。这可以通过Cisco DNAC或ISE等平台执行。
- 持续监控零信任环境。实施安全分析以实时监控和分析安全事件并快速识别恶意活动。持续检查并记录内部和外部的所有流量。

实现可信访问

要实现全面的零信任安全性，组织必须将其零信任方法扩展到整个员工、工作场所和工作负载。

- 零信任员工队伍 — 用户和设备必须经过身份验证和授权，访问权限和权限必须持续监控和管理，以保护资源。
- 零信任工作空间 — 必须控制整个工作空间的访问，包括云和边缘。
- 零信任工作负载 — 必须在整个应用堆栈（包括云中的容器、虚拟机监控程序和微服务以及传统机构数据中心之间）实施精细访问控制。

思科是Forrester认可的零信任领导者，是整个网络（内部和云中）实现零信任的有力倡导者。您不仅可以将您的思科网络基础设施作为零信任架构的重要基础，还可以了解其他有助于您的组织实现零信任的关键思科零信任安全功能。

思科安全产品组合

以下内容可用于构建成功的零信任框架：

- 通过Cisco Duo为用户、设备和应用提供无障碍、安全的访问
- 通过Cisco Umbrella实现灵活的云安全
- 通过思科安全防火墙的智能数据包检测
- 通过安全终端(正式为AMP)的高级恶意软件防护
- 通过Cisco AnyConnect保护VPN和远程访问
- 通过Cisco Tetration提供整体工作负载保护
- 使用思科身份服务引擎(ISE)保护网络分段
- 通过思科安全工作负载实现应用可视性和微分段
- 通过Cisco SecureX集成安全平台
- 统一的SASE解决方案，通过Cisco+安全连接提供即服务订用
- Cisco Zero Trust Strategy服务提供的专家指导
- 通过咨询、咨询和解决方案服务提供支持和端到端服务

摘要

零信任的一个最简单的方法是“从不信任并始终验证”。 这适用于每个网络连接、每个会话，以及访问关键应用、工作负载和数据的每个请求。

零信任安全框架围绕组织网络中的每个资源创建本地化的微边界防御。如果设计正确，这些框架可以保护资产，无论资产位于何处。

降低风险的一个有效方法是控制对特权及共享数据的访问，并采用最小特权原则。此安全模型通过API实现协调，并与工作流程自动化平台集成，从而提供对用户和应用的可视性。

成功实施零信任有助于确保组织整个信息技术环境的安全和无缝操作，并实现对组织关键工作负载、应用和数据的持续受信任访问，从而增强组织的任务。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。