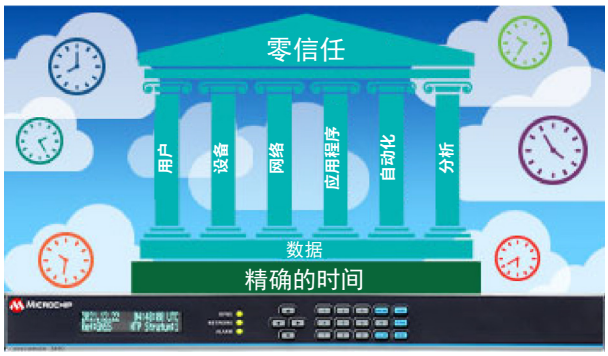
零信任网络的可信时间与互联网NTP服务器池中的时间对比

概要

对于计划推出零信任架构的组织，都应当明白这一点：从公共NTP服务器池获取时间是多么不合理，并且违背了零信任的基本概念。精确的时间对于网络运营业务至关重要，而连接至网络的时间服务器的安全性在许多方面都必须是可信的。SyncServer®网络时间服务器在提供精确的时间以及遵循零信任原则方面都非常出色。



网络时间同步的冒险抉择

使用公开可用的NTP服务器池来同步公司关键系统中的时间，这听起来可能很诱人。例如，一些公司的边缘路由器利用网络时间协议（NTP）将其内部时钟与互联网上的某个时间服务器同步。然后，这些路由器又作为公司内部网络的NTP服务器。这种获取时间戳的方法虽有风险，但成本低廉。

另一种场景就是使用主域控制器通过开启防火墙中的端口123来指向某个互联网时间服务器的IP地址。然后，域控制器通过网络级联时间。这种方法有据可查，且配置非常简单。但是，直接从互联网获取时间真的值得我们这样节省并承担风险吗？

非理性信任

零信任网络有两个主要概念：

- ***零信任：***一种绝不会以隐式方式授予信任的网络安全范例
- ***零信任架构：***面向企业资源和数据安全性的端对端方法

零信任的格言就是“从不信任，始终验证”。

如果组织依赖基于互联网的时间服务器，那么所能进行的验证，就是将NTP时间请求发送至指定IP地址时，将会返回带有两个额外时间戳的NTP数据包，仅此而已。没有任何凭据表明这个时间的精度、可靠性或安全性。

远程时间服务器将会获得隐式信任。因为组织尚未实现端对端身份验证或授权，所以它们信任该服务器并且未对其进行此类验证。这就是一种非理性信任。

换句话说，您会打开自己防火墙中的端口123，并将整个网络同步至ntppool.org上可用的4,000多个NTP服务器中某个服务器分配的IP地址吗？这种做法天然存在风险。

带来恐惧、不确定性和怀疑

信任NTP服务器池就是一个典型的非理性信任示例。NTP时间戳始终以明文形式发送，并且很容易被中间人操控。同时，由于添加至NTP时间服务器池的时间服务器（如ntppool.org中的那些时间服务器）都未经过审查，所以任何有恶意企图的人都可以将时间服务器添加至服务器池中，并且可以操控为分配到该时间服务器的NTP客户端提供的时间戳。

说一个实际案例，某个看似可信的互联网时间服务器的所有者觉得某个医疗保健服务商的NTP客户端请求时间的频率过高，因此故意将时间服务器配置为向服务商的NTP服务器提供错误的时间戳。该服务商连夜找出问题的根源就是那个异常的互联网时间服务器，但日志文件和患者数据已遭到损毁。后来该服务商部署了一个内部Stratum 1时间服务器，以防止未来出现类似的风险。

这个真实案例突出了问题的关键：日志文件及其精确的时间戳至关重要。

为什么时间很重要

信息技术（IT）安全部门负责保护数据、资源和个人信息等内容。该部门的职能之一是管理所有网络活动的对象、内容、地点和**时间**，以及验证允许连接至组织网络的每一台设备。零信任架构的创建宗旨就是帮助组织应对这些安全挑战。

避免时间戳混乱

整个网络的时间同步精度及其在网络管理和安全性方面发挥的重要作用往往不被人重视。试想一下，如果每个网络设备的时间各不相同，会出现什么后果。整个组织的网络都会出现混乱。日志文件和网络遥测的时间戳没有关联性，致使这些数据变得毫无用处。例如，系统日志本该实时接收，但日期却被倒填为上一周，使得这些数据失去了作用。仪表板将发生故障，即便没有故障，也会显示不正确的数据，并且很有可能会触发警报。关键进程要么启动太早，要么启动太晚。网络取证几乎不可能，审核将毫无意义，视频时间戳也将不正确。时间精度对任何组织的网络都至关重要，绝不可忽视。

网络时间源至关重要

我们必须考虑实现网络时间同步的时间源的对象、内容、地点和**时间**。提供网络时间协议（NTP）时间戳的时间服务器就是“内容”。如果“对象”和“地点”只是互联网NTP服务器池中某个时间服务器的IP地址，则需要考虑所接收NTP时间戳的“时间”的有效性和漏洞。直接从互联网获取时间违背了几乎所有零信任原则，且不能被视为可信时间（Trusted Time™技术）。

什么是可信时间?

假设从网络中的某个位置通过NTP实现时间同步，零信任就会引发两个关键问题。这个时间为隐式可信时间还是显式可信时间？作为连接至公司网络的设备，时间服务器本身是否与零信任网络技术兼容？

可信时间意味着时间服务器在时间的精度和合法性方面是可信的。此外，它还意味着时间服务器作为连接至网络的设备是可信的，且符合公司的零信任安全要求。

为什么说SyncServer时间服务器是可信时间服务器?

作为市场上安全性最高的可信时间网络设备，SyncServer时间服务器符合零信任模型的基本要素要求*，包括用户、设备、网络、应用程序和分析（如图1所示）。

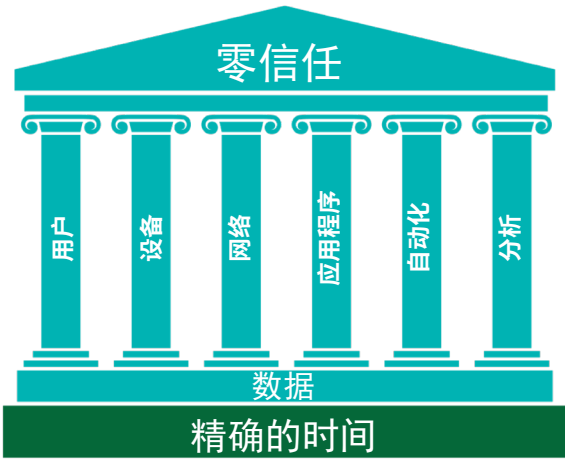


图1. 精确的时间是零信任网络的基础

SyncServer时间服务器还符合NIST特别出版物800-207：Zero Trust Architecture 中概述的核心组件要求。图2为适用核心组件的简化示意图，它展示了SyncServer时间服务器如何在NIST数据层面与控制层面之间实现互操作。

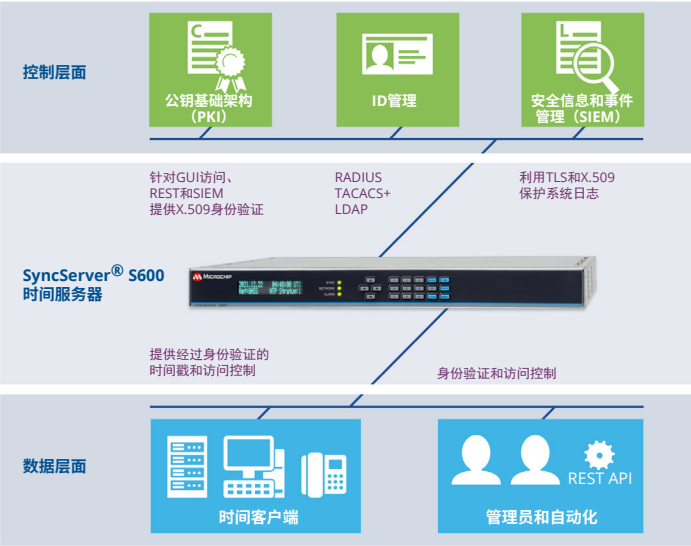


图2. SyncServer时间服务器在NIST定义的数据层面与控制层面之间的互操作性

零信任的根本前提是不对任何事物给予隐式信任，包括时间和时间服务器。有许多使用SyncServer时间服务器在零信任架构中实现可信时间的场景。我们已经为部分此类场景创建了信息图。每张图都突出显示了SyncServer时间服务器的安全技术和相关的零信任基本要素，以供参考。您可以在我们Trusted Time for Zero Trust Networks网页上查看所有信息图。

了解更多有关可信时间的信息

如果贵司准备采用零信任架构，可以参考我们的应用笔记。该应用笔记阐述了可信时间在零信任网络中如此重要的原因，并简要介绍了SyncServer网络时间服务器如何确保时间安全性以及如何遵循零信任原则。它包括SyncServer时间服务器安全性特性的详细列表，以及这些特性如何与零信任模型的基本要素保持一致。

贵司的安全团队可利用这个非常有用的检查清单（图3所示）来确定SyncServer S600/S650时间服务器是否符合公司网络的安全要求。

针对零信任架构的SyncServer S600/S650时间服务器可信时间安全检查清单

用户	1. RADIUS身份验证（用户可配置的IP端口号：1024至49151）。
	2. TACACS+身份验证（用户可配置的IP端口号：1024至49151，以及标准端口49）。
	3. LDAP身份验证（端口绑定，LADP v2或LDAP v3，最多5个LDAP服务器）
	4. REST API（每一次调用都进行用户/密码验证，或采用限时令牌）
	5. 管理安全性 a. Web会话超时（5/10/15/30/60分钟） b. 登录尝试失败锁定（使能/禁止），允许登录尝试失败3到6次 c. 登录横幅（美国政府标准横幅或自定义横幅）
	6. 用户设置 a. 密码：6至100个字符，大小写混合，由字母、数字和特殊字符组成 b. 密码到期：启用/禁用，用户设置天数 c. 用户创建/删除：用户名、密码、恢复问题和电子邮件
	7. SSH（允许/拒绝的用户）
设备	8. NTPd对称密钥 a. 生成/下载/上传对称安全密钥 b. SHA1/256/512和MD5密钥
	9. NTPd Autokey服务器（IFF标识方案）
	10. NTPd Autokey客户端（IFF标识方案）
	11. HTTPS安全管理 a. 协议：TLS 1.2和1.3 b. 加密套件：SSL_High_Encryption；SSL_High_Medium_Encryption c. 会话超时：5至1440分钟 d. 自签名证书：2048或4096 RSA密钥位；到期天数：1至1825；可定制地区代码 e. 内容安全策略（CSP）报头
	12. X.509 Cert/CSR（创建和下载证书签名请求（CSR），2048或4096 RSA密钥位）
	13. X.509安装（安装多个CA签名X.509证书）
	14. X.509映射 a. 将X.509 CA签名证书映射至HTTPS和/或系统日志 b. 适用于HTTPS和/或系统日志的相同或不同的X.509 CA签名证书
	15. X.509证书颁发机构（或可信CA证书存储区） a. 安装专有CA证书 b. 包含多种系统默认CA证书
	16. 软件升级 a. 只能从Microchip客户门户网站获取系统软件 b. 经过身份验证的用户才能访问Microchip客户门户网站 c. 需要授权才能下载系统软件和序列化授权文件 d. 系统软件映像均已加密 e. 所有下载都包括MD5和SHA散列，以交叉检查文件是否经过修改 f. 除非具有Microchip提供的正确的序列化授权文件，否则无法安装软件
	17. 报警（用户可配置多种警报，通过陷阱、日志、电子邮件和硬件中继器发送通知）
	18. 授时安全性 a. 基于BlueSky™技术的GNSS干扰及欺骗检测和防护 b. 备用时间源（NTP、PTP和IRIG） c. 防干扰GNSS天线 d. 通过原子钟升级保持时间一致
网络	19. 访问控制列表（每个LAN端口都有唯一的IPv4和IPv6访问控制列表，总共8-12个列表）
	20. 服务/系统控制（启用/禁用HTTPS、SNMP、SSH、ToD和Telnet）
	21. 数据包监控 a. 基于硬件对发往CPU的数据包进行节流，从而实现DoS/DDoS保护 b. 基于每个LAN端口对数据包进行节流 c. 可针对每个LAN端口自定义数据包接收报警阈值
	22. 用于实现网络分段的多个LAN端口 a. 只有LAN1上有管理和定时功能 b. LAN2-LAN6上只有定时功能，没有管理功能
分析	23. 安全系统日志 a. X.509验证 b. TLS安全 c. 对等验证 d. 用户可配置端口号
	24. SNMPv3 a. 身份验证加密：MD5和SHA1/224/256/384/512 b. 密钥加密，AES/128/192/256

图3. 针对零信任架构的SyncServer S600/S650时间服务器可信时间安全检查清单

符合零信任时间

SyncServer时间服务器是高度安全的可信时间网络设备，非常适合为任何组织的零信任倡议提供支持。它可确保时间及其来源的安全性，并符合零信任的基本要素要求。

资源链接

网页： Trusted Time for Zero Trust Networks

应用笔记： 《零信任网络的可信时间》

*美国技术委员会-工业咨询委员会（ACT-IAC）发布的Zero Trust Cybersecurity Current Trends，2019年4月18日

Microchip的名称和徽标组合、Microchip徽标和SyncServer均为Microchip Technology Incorporated在美国和其他国家或地区的注册商标。
Trusted Time为Microchip Technology Incorporated在美国和其他国家或地区的商标。在此提及的所有其他商标均为各持有公司所有。
© 2023, Microchip Technology Incorporated及其子公司版权所有。08/23
DS00004823A_CN