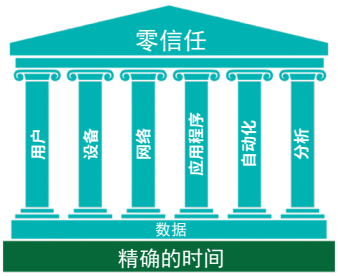
零信任网络的可信时间

SyncServer® S600时间服务器是可信时间的基本来源，有助于确保零信任网络平稳运行



概要

时间是确保日志文件准确的关键要素，这些文件定义了零信任网络中所有活动的对象、内容、***时间***和地点。

精确可靠且安全的可信时间（Trusted Time™技术）是零信任网络的基础。如果没有可信时间，身份验证机制将失效，必要日志文件时间戳将不一致，零信任分析将不可靠，取证将受阻，同时还会出现其他一些问题。

不仅时间必须正确无误，而且时间服务器还必须遵循零信任原则，并适合相应的零信任架构。

SyncServer® S600时间服务器是高度安全的可信时间网络设备，非常适合为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，包括用户、设备、网络和分析[i]。

主要特性

- 高度安全的网络时间服务器
- 身份验证时间戳
- 安全系统日志
- X.509证书/PKI
- RADIUS/TACACS+/LDAP
- 经过强化的用户界面
- 时间源验证
- 网络分段支持

精确的时间是零信任的基础。时间就是对象、内容以及何时何地管理和监控零信任网络的“时间”。“时间”是日志文件中的精确时间戳。美国国家标准与技术研究所（NIST）的零信任标准中包括日志时间戳[ii]，而美国白宫近期针对实现与网络安全事件相关的零信任和补救能力颁布了总统行政令，其中定义了日志文件的时间戳格式和时间来源[iii]。

网络安全依赖于具有精确时间戳的日志文件。用于零信任分析的安全信息和事件监控（SIEM）系统依赖精确及时的网络遥测技术。其中包括精确的日志文件时间戳，用以识别安全事件、策略违规、欺诈行为、运行问题、审计和取证分析，以及内部调查、确定基线和确定运行趋势及长期问题[iv]。

时间戳源自时间同步服务器和系统。至少要在生成SIEM日志文件的系统之间实现时间同步，以防止出现时间轴混乱以及阻碍快速事件响应和故障诊断等问题。

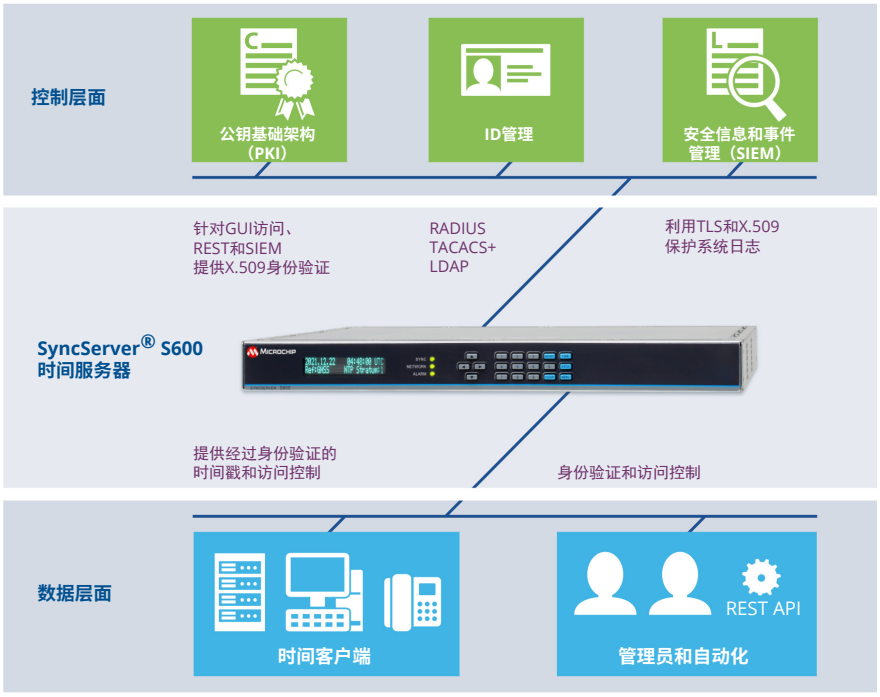
时间服务器可为网络服务器实现时间同步。SyncServer S600时间服务器等设备可以为生成重要SIEM日志文件的关键网络服务器提供精确、可靠且安全的时间源。

无论是从时间服务提供商还是零信任网络的角度来看，S600都是零信任网络上的安全强化设备，并在设计中融合了零信任用户、设备和网络基本要素原则。

经过验证的时间至关重要。根据定义，网络时间协议（NTP）数据包以明文方式发送，这使其在传输过程中容易被操控。为实现零信任时间同步，必须启用NTP身份验证，以确保S600与NTP客户端之间的关联是可信的，同时确认时间戳未经任何修改。

时间服务器必须适合零信任范式。可信时间是确保零信任网络正常运行和充分强化的必要条件。如果零信任网络中缺少最基本的精确同步时间概念，则许多零信任基本要素将无法可靠运行。

SyncServer S600时间服务器是零信任网络的可信时间源。S600是支持零信任网络基本要素的基础，可通过安全、精确和可靠的全网时间同步功能实现精确的日志文件时间戳。



具有时间服务器管理访问权限的用户必须经过身份验证和授权

用户

SyncServer S600时间服务器的第一道防线是基于每个端口的LAN访问控制列表，这些列表支持对网络进行物理和逻辑微分段。

由于时间服务器必须由人工或机器配置，所以我们使用RADIUS、TACACS+和LDAP等协议提供访问所需的可靠身份验证和授权。

时间服务器还需要严格控制本地访问，包括强密码要求、超时、到期和轮换等。

SyncServer时间服务器还配备了可靠的REST API机器接口，该接口要求每一次调用都使用凭证或限时令牌进行身份验证。

时间服务器是零信任网络上的一个设备，在零信任网络上，关于该设备的一切都必须经过身份验证，且必须是可信的

设备

从最基本的层面上看，在时间客户端与S600之间使用对称密钥验证可确保时间数据包在传输过程中未经任何修改。创建用于验证授时数据包的散列时应使用强密钥（如SHA 256/512）。

用于配置该设备的S600 Web图形用户界面功能丰富，虽然从易用性的角度来看令人满意，但在其他方面仍必须进行大幅度的强化，应使用X.509 CA签名证书进行S600与用户浏览器之间的身份验证，并结合高度安全的TLS 1.3对链路进行加密。

零信任还包括时间服务器的软件更新。只有经过身份验证和授权的用户才能下载S600软件。软件映像都经过加密，以防止被修改，同时还提供散列，以确保在传输过程中未经任何修改。这些下载的软件中还包括控制S600软件安装的加密授权文件。软件安装前，S600会对序列号、版本和软件完整性进行验证。

SyncServer时间服务器的系统软件是专门定制且经过强化的最新嵌入式Linux®发行版，仅包括操作定制硬件所需的内容。这可大大减少潜在的攻击面，因为S600中甚至不可能出现/加载可能与Linux大规模发行版中的CVE（Common Vulnerability and Exposure）漏洞存在关联的软件。

Stratum 1 S600的时间源自GNSS卫星系统，而该卫星系统已不再被认为是值得信赖的系统。GNSS干扰和欺骗威胁变得越来越普遍，这意味着我们现在必须采取零信任姿态。

GNSS验证主要是监控本地射频环境中是否存在异常，以及验证接收的GNSS信号中的数据。S600通过嵌入式BlueSky™技术的干扰和欺骗检测以及防护功能来持续验证GNSS。

时间服务器不仅要对网络进行物理和逻辑分段，还要防御DoS攻击

网络

S600可将零信任网络划分为多个边界，它整合了4至6个相互隔离的LAN端口，以便为最多6个隔离的网络分段提供NTP/PTP定时服务。端口之间不存在任何交叉流量；每个端口都有双重访问控制列表，且所有端口都可以采用独立的网络配置。

管理访问权限严格限制在单个LAN端口，以进一步与网络隔离。

为防御DoS攻击，S600采用了独特的NTP Reflector技术来防止出现主机溢出和报警，该技术可提供高线速和高容量NTP服务，以及数据包限制，以防止出现主机溢出和警报。尽管超过用户设定阈值的网络流量会触发预警，但S600只提供授时数据包服务。在任何时候都不会出现DoS负载导致S600 CPU故障的威胁。

时间服务器可提供实时管理防御所需的可靠时间轴基础分析

分析

分析依靠网络遥测数据来得出有关实施零信任网络的各种见解。从根本上说，这些数据就是包含时间戳的日志文件，时间戳提供了事件或活动的“时间”。除了对网络中所有发送日志的设备进行时间同步外，S600还提供必要的日志。

日志不得以明文形式[v]发送，而是应该以安全系统日志的形式发送。发送任何日志之前，S600安全系统日志会整合由SIEM进行验证的X.509 CA签名证书以及对等验证的身份验证信息，以检查SIEM的X.509证书。一旦建立了信任，就会通过TLS发送系统日志数据，以防止篡改或窃听日志文件。

通过对安全系统日志和HTTPS web GUI使用不同的X.509 CA签名证书，可进一步强化S600。

对“从互联网免费获取时间”的非理性*隐式信任*

从公共互联网时间服务器获取时间违背了零信任的所有原则和宗旨，并且对互联网上恰好返回NTP时间请求的某个IP地址授予了隐式信任。

这种未经验证且公开播发的时间服务器与其他公开播发的时间服务器一样不在零信任安全范畴之内。该时间服务器提供的时间戳在传输过程中很容易被操控，且它易受DoS攻击而导致服务中断，并可能被用于DoS放大攻击或遭受GNSS干扰和欺骗攻击。

除了可能无法跟踪无效时间戳之外，还无法查看或控制远程时间服务器的时间来源，亦无法对其管理采取任何控制措施，因此这类服务器不适合作为零信任网络中的时间服务资源。

零信任要求所使用的关键时间服务器在零信任范畴之内，并要求对此类服务器进行保护、验证和监控，以确保向网络提供安全、精确且可靠的基本时间服务。

SyncServer S600系列时间服务器助您顺利通过下一次零信任审核

在零信任网络中配置妥当后，SyncServer S600时间服务器可满足所有适用的基本要素要求，能够向零信任网络提供精确、可靠且安全的可信时间。

TRUSTED TIME™ FOR ZERO TRUST NETWORKS

参考资料

i 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

ii NIST特别出版物800-207 Zero Trust Architecture，2020年8月

iii 美国白宫发布的Executive Order on Improving the Nation's Cybersecurity，2021年5月12日；

美国总统行政办公室发布的M-21-31号备忘录Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents，2021年8月27日；

美国总统行政办公室发布的M-22-09号备忘录Moving the U.S. Government Toward Zero Trust Cybersecurity Principles，2022年1月26日

iv NIST特别出版物800-92 Guide to Computer Security Log Management

v National Security Agency Cybersecurity Report、Hardening SIEM Solutions和A Technical Report from Network Infrastructure Security，2019年10月29日

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

Microchip的名称和徽标组合、Microchip徽标及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。8/23
DS00004549B_CN

MICROCHIP