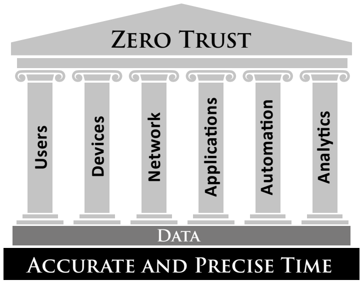
Trusted Time™ for Zero Trust Networks

The SyncServer® S600 Time Server is the foundational source of Trusted Time, which enables smooth operation of Zero Trust networks



Summary

Time is central to accurate log files that define the who, what, *when* and where of all activity in a Zero Trust network.

Trusted Time which is accurate, reliable and secure, is foundational to Zero Trust networks. Without it, authentication mechanisms will fail, essential log file timestamps will not align, Zero Trust analytics will be unreliable, forensics will be hampered, and the list goes on.

Not only must the time be correct, but the time server must also be compliant to Zero Trust principles and fit accordingly in a Zero Trust Architecture.

As the most secure Trusted Time network device, the SyncServer S600 time server is best suited to support Zero Trust initiatives. It ensures the security of time and its sources, as well as complies with the fundamental pillars of Zero Trust including Users, Devices, Network and Analytics[i].

Key Features

- Most secure network time server
- Authenticated timestamps
- Secure syslog
- X.509 certificates/PKI
- RADIUS/TACACS+/LDAP
- Hardened user interface
- Time source validation
- Network segmentation support

Accurate time is foundational to Zero Trust. Time is the "when" of the who, what, when and where of managing and monitoring a Zero Trust network. "When" is an accurate timestamp in a log file. The National Institute of Standards and Technology (NIST) standard on Zero Trust includes timestamps for logs[ii], and recent White House Executive Orders for implementing Zero Trust and remediation capabilities related to cybersecurity incidents define the log file timestamp format and the source of the time[iii].

Cyber security relies on log files with accurate and precise timestamps. Security Information and Event Monitoring (SIEM) systems used in Zero Trust analytics rely on accurate and timely network telemetry. This includes accurate log file timestamps to help in identifying security incidents, policy violations, fraudulent activity, operational problems, auditing and forensic analysis, internal investigations, establishing baselines, and identifying operational trends and long-term problems[iv].

Timestamps originate from time synchronized servers and systems. At a minimum, the systems generating the log files for the SIEM must be time synchronized with each other to prevent timeline chaos and hampering of rapid incident response and fault diagnosis.

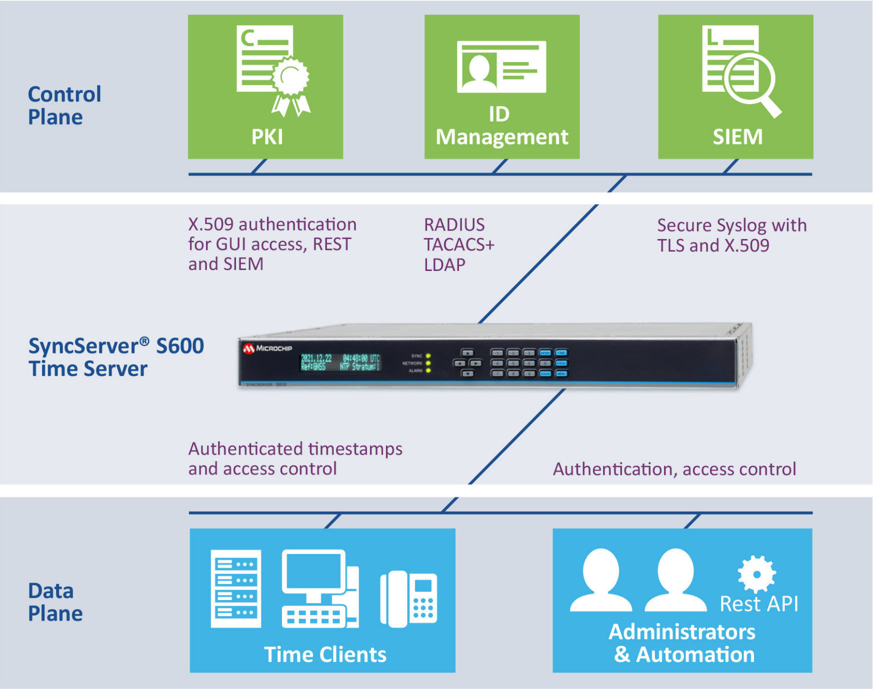
Time servers provide the time synchronization for network servers. A device such as the SyncServer S600 time server is the accurate, reliable and secure source of time for critical network servers that generate vital log files for the SIEM.

The S600 is security hardened to reside on the Zero Trust network, both from a time service provider to the Zero Trust network standpoint, as well as incorporating Zero Trust User, Device, and Network pillar principles in its design.

Authenticated time is essential. Network Time Protocol (NTP) packets are, by definition, sent in the clear, which makes them subject to easy manipulation in transit. For Zero Trust time synchronization, NTP authentication must be enabled to ensure the S600 and NTP client association is trusted and confirm the timestamps are unaltered.

Time servers must fit in the Zero Trust paradigm. Trusted Time is an essential aspect of a properly functioning and adequately hardened Zero Trust network. Without the most basic notion of accurate and synchronized time across the Zero Trust network, many of the pillars of Zero Trust will not function reliably.

The SyncServer S600 time server is the trusted time for Zero Trust Networks. The S600 is foundational in support of the pillars of Zero Trust networking, enabling accurate log file timestamps through secure, accurate and reliable network-wide time synchronization.


Control Plane
PKI
ID Management
SIEM
X.509 authentication for GUI access, REST and SIEM
RADIUS TACACS+ LDAP
Secure Syslog with TLS and X.509
SyncServer® S600 Time Server
Authenticated timestamps and access control
Authentication, access control
Data Plane
Time Clients
Rest API
Administrators & Automation

Users With Management Access to the Time Server Must Be Authenticated and Authorized

Users

The first line of defense in the SyncServer S600 time server are port-by-port LAN access control lists which support the physical and logical micro-segmentation of the network.

As time servers must be configured by either humans or machines, protocols such as RADIUS, TACACS+ and LDAP provide the robust authentication and authorization needed for access.

Time servers also need strict control over local access including robust password requirements, timeouts, expiration, rotation and more.

The SyncServer time server is also equipped with a robust REST API machine interface that requires that every call be authenticated with credentials or a time-limited token.

The Time Server is a Device on the Zero Trust Network where Everything About it Must be Authenticated and Trusted

Devices

At the most basic level, symmetric key authentication used between time clients and the S600 ensures time packets are not altered in transit. Strong keys, such as SHA 256/512, should be used to create the hashes to authenticate the timing packets.

While the very feature rich S600 web GUI used to configure the unit is appreciated from an ease-of-use standpoint, that interface must be extremely hardened. To achieve that end, X.509 CA-signed certificates should be used to authenticate the S600 to the user's browser coupled with very secure TLS 1.3 based encryption of the link.

Zero Trust also includes software updates for the time server. Only authenticated and authorized users are allowed access to S600 software downloads. Software images are encrypted to prevent modifications and hashes are provided to ensure there are no modifications in transit. These downloads also include encrypted authorization files that control S600 software installation. Before software installation, the S600 authenticates serial numbers, versions and software integrity.

The SyncServer time server's system software is a custom tailored, hardened, current and embedded Linux® distribution including only what is needed to operate the custom hardware. This greatly decreases any potential attack surface as software that might be found connected to a Common Vulnerability and Exposure (CVE) in a broad Linux distribution is likely not even present/loaded in the S600.

The GNSS satellite system, from which the Stratum 1 S600 obtains its time, can no longer be assumed to be trustworthy. GNSS jamming and spoofing threats are becoming more prevalent, which means that a Zero Trust posture must now be taken.

GNSS validation takes the form of monitoring the local RF environment for anomalies and validating the data in the received GNSS signals. The S600 does this with embedded BlueSky™ technology jamming and spoofing detection and protection capabilities to continuously validate GNSS.

The Time Server Should Segment the Network Physically and Logically as Well as Defend Against DoS Attacks

Network

Facilitating segmented-perimeters of the Zero Trust network, S600s incorporate from four to six isolated LAN ports to provide NTP/PTP timing services to up to six different network segments. There is no cross traffic between ports; each port has dual access control lists, and all ports can have unique network configurations.

Management access is strictly limited to a single LAN port for further isolation from the network.

For DoS attack protection, S600s incorporate unique NTP Reflector technology that provides line speed, high-capacity NTP service as well as packet limits to prevent host overrun and alarms. Network traffic above user-set thresholds trips alarms while the S600 services only timing packets. At no time is there ever a threat a DoS load will fault the S600 CPU.

Time Servers Provide the Reliable Timeline Foundation Analytics Required to Manage Defenses in Real Time

Analytics

Analytics relies on network telemetry data to provide the insights enforcing Zero Trust. These data are fundamentally log files that contain timestamps providing the "when" of the event or activity. Aside from time synchronizing all devices on the network that are sending logs, the S600 also provides essential logs.

Logs should never be sent in plaintext[v], but rather via secure syslog. Before any logs are sent, the S600 secure syslog incorporates X.509 CA-signed certificates to be authenticated by the SIEM as well as peer verified authentication to check the X.509 certificate of the SIEM. Once trust has been established, syslog data is sent via TLS to prevent log file tampering or eavesdropping.

The S600 can be further hardened by using a different X.509 CA-signed certificate for secure syslog and the HTTPS web GUI.

Irrational *Implicit Trust* of "Free time from the Internet"

Acquiring time from a public Internet time server breaks every principle and tenet of Zero Trust and grants implicit trust to an IP address somewhere on the Internet that happens to return an NTP request for time.

This unauthenticated, publicly advertised time server, which is outside every Zero Trust security perimeter, in a pool with other publicly advertised time servers, provides a timestamp that can be manipulated easily in transit, is subject to DoS attacks curtailing service, and can potentially be used in DoS amplification attacks or be subject to GNSS jamming and spoofing.

Aside from likely being impossible to trace a bad timestamp, there is no visibility or control over where the remote time server is getting its time, or any of the controls surrounding its management, which makes it an unsuitable time service resource for use in a Zero Trust network.

Zero Trust requires the critical and essential time server be inside the perimeter, protected, authenticated and monitored to assure security, accuracy and reliability of foundational time services to the network.

Pass Your Next Zero Trust Audit With the SyncServer S600 Series Time Server

The SyncServer S600 time server, when properly configured in a Zero Trust network, meets all of the applicable foundational pillars to provide accurate, reliable, secure and Trusted Time to the Zero Trust network.

TRUSTED TIME™ FOR
ZERO TRUST NETWORKS

References

i American Council for Technology-Industry Advisory Council (ACT-IAC), Zero Trust Cybersecurity Current Trends April 18, 2019

ii NIST Special Publication 800-207 Zero Trust Architecture, August 2020

iii The White House, Executive Order on Improving the Nation's Cybersecurity, May 12, 2021;

Executive Office of The President, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, M-21-31, August 27, 2021;

Executive Office of The President, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, M-22-09, January 26, 2022

iv NIST Special Publication 800-92, Guide to Computer Security Log Management

v National Security Agency Cybersecurity Report, Hardening SIEM Solutions, A Technical Report from Network Infrastructure Security, October 29, 2019

SyncServer S600/S650 Time Server Trusted Time Security Check List for Zero Trust Architectures

USERS	1. RADIUS authentication
	2. TACACS+ authentication
	3. LDAP authentication (bindings for ports, LDAP v2 or LDAPv3, up to five LDAP servers)
	4. REST API (user/password authentication on every call or token based with expiration)
	5. Administrative security a. Web session timeouts (5/10/15/30/60 minutes) b. Lockout for failed login attempts (enable/disable), three to six failed login attempts allowed c. Login banners (standard US Government, custom banner)
	6. User Settings a. Passwords: 6 to 100 characters, mixed case, letters, numbers, special b. Password expiration: enable/disable, user set number of days c. User creation/deletion: username, password, recovery question, email
	7. SSH (allowed/denied users)
DEVICES	8. NTPd Symmetric Keys a. Generate/download/upload symmetric security keys b. SHA1/256/512 and MD5 keys
	9. NTPd Autokey Server (IFF identity scheme)
	10. NTPd Autokey Client (IFF identity scheme)
	11. HTTPS Secure Management a. Protocols: TLS 1.2 and 1.3 b. Cipher suites: SSL_High_Encryption; SSL_High_Medium_Encryption c. Session timeout: 5 to1440 minutes d. Self-signed certificate: 2048 or 4096 RSA key bits; Expiration days 1-1825; customizable locality codes e. Content Security Policy (CSP) headers
	12. X.509 Cert/CSR (create and download Certificate Signing Requests (CSRs), 2048 or 4096 RSA key bits)
	13. X.509 Install (install multiple CA-signed X.509 certificates)
	14. X.509 Mapping a. Map X.509 CA-signed certificate(s) to HTTPS and/or syslogs b. Same or different X.509 CA-signed certificates for HTTPS and/or syslog
	15. X.509 Certificate Authorities (or Trusted CA Certificate Store) a. Install proprietary CA certificates b. Extensive system-default CA certificates included
	16. Software Upgrades a. System software only available from Microchip customer portal b. Requires authenticated user to access on Microchip customer portal c. Requires authorization to download the system software file and serialized authorization file\ d. System software images are encrypted e. All downloads include an MD5 and SHA hash to cross check for file alteration f. Software cannot be installed unless accompanied by the correct, serialized authorization file from Microchip
	17. Alarms (extensive user configurable alarms, notification via trap, logs, email, hardware relay)
	18. Timing Security a. BlueSky™ technology GNSS jamming, spoofing detection and protection b. Alternative time sources (NTP, PTP, IRIG) c. Anti-Jam GNSS antenna d. Atomic clock upgrades for timing holdover
NETWORK	19. Access Control Lists (unique IPv4 and IPv6 access control lists per LAN port, 8-12 lists total)
	20. Service/System Control (enable/disable HTTPS, SNMP, SSH, ToD, Telnet)
	21. Packet Monitoring a. DoS/DDoS protection by hardware-based throttling of packets to the CPU b. Packet throttling on a LAN-port-by-LAN-port basis c. Customizable packet receipt alarm thresholds for each LAN port
	22. Multiple LAN Ports for Network-Segmentation a. Management/timing available on LAN1 only b. LAN2-LAN6 timing only, no management possible
ANALYTICS	23. Secure Syslog a. X.509 authentication b. TLS security c. Peer verify d. User configurable port numbers
	24. SNMPv3 a. Authentication cryptography: MD5, SHA1/224/256/384/512 b. Privacy cryptography: AES/128/192/256