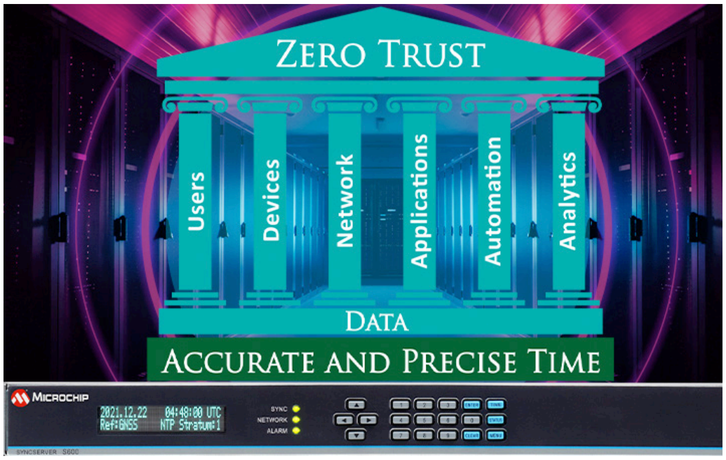
What Is Trusted Time for Zero Trust Data Center Networks and Why Does it Matter?

Summary

Organizations rolling out a Zero Trust Architecture to on-premise data centers and collocated data center enclaves must care about accurate time synchronization of this distributed network and the security of the time servers providing it. Accurate time is essential for distributed network operations, and the security of the time servers attached to the network must be trusted in many respects. The SyncServer® network time server is unsurpassed in both its ability to deliver accurate time as well as in its compliance with the principles of Zero Trust.



Why Time Matters

Information Technology (IT) security is responsible for protecting data, resources, personal informa-tion and much more across distributed data centers. Part of that role is managing the who, what, where and **when** of all network activity as well as validating every device allowed to connect to the organization's network. Geographically separated data centers present a time synchronization challenge related to the **when** of network activity. Asymmetric path delays between data centers lead to nearly unknowable time offsets if a single network time server is expected to keep the whole network in sync. Time offsets lead to timestamp mismatches in log files, leading to reduced integrity of network management systems that are aggregating network wide activity for monitoring and security purposes.

Avoiding Timestamp Chaos

Network-wide time synchronization accuracy and the essential role it plays in network management and security are often taken for granted. Imagine what would happen if every network device in every data center had a different time. Chaos would break out across the organization's network. Log files and network telemetry would be useless as logs and telemetry timestamps would not correlate. For example, syslogs that might be received in real time but erroneously timestamped would not be helpful. Dashboards would fault, or at least present incorrect data, and would most likely trigger alarms. Critical processes would either start too soon or too late. Network forensics would be nearly impossible, audits would be meaningless, video timestamps would be incorrect, etc. Time accuracy across data centers is important and it does matter.

Network Time Source Matters

It is important to consider the who, what, where and **when** of the source of time for network time synchronization. Time servers providing the Network Time Protocol (NTP) timestamps are the "what." If the "who" and "where" are merely the IP addresses of time servers from an Internet NTP server pool near a data center, then consideration needs to be given to the validity and vulnerability of the "when" of the NTP timestamps that are received. Time from the Internet violates just about every principle of Zero Trust and cannot be considered trusted time.

What Is Trusted Time?

Trusted time means the time server is trusted with respect to the accuracy and legitimacy of the time. It also means the time server is trusted as a device connected to the network and is compliant with the company's Zero Trust security requirements.

Why the SyncServer® Time Server is a Trusted Time Server.

As the most secure trusted time network device available, a SyncServer time server complies with the fundamental pillars of the Zero Trust model*, which include users, devices, network, applications and analytics as shown in Figure 1.

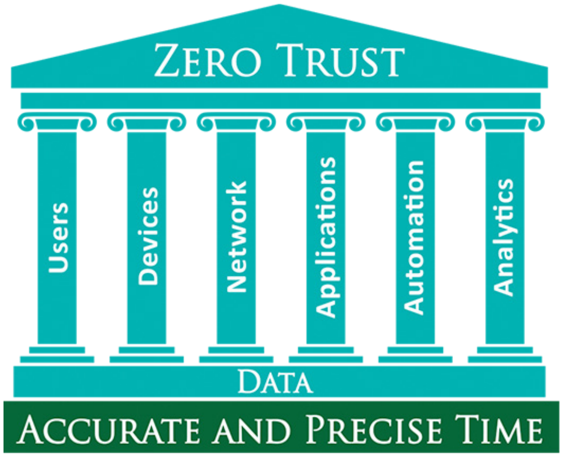


Figure 1. Accurate and precise time are foundational to Zero Trust networks

The SyncServer time server also conforms to the core components outlined in NIST Special Publication 800-207: Zero Trust Architecture. Figure 2 is a simplified representation of applicable core components showing how the SyncServer time server interoperates between the NIST-defined data plane and control plane.

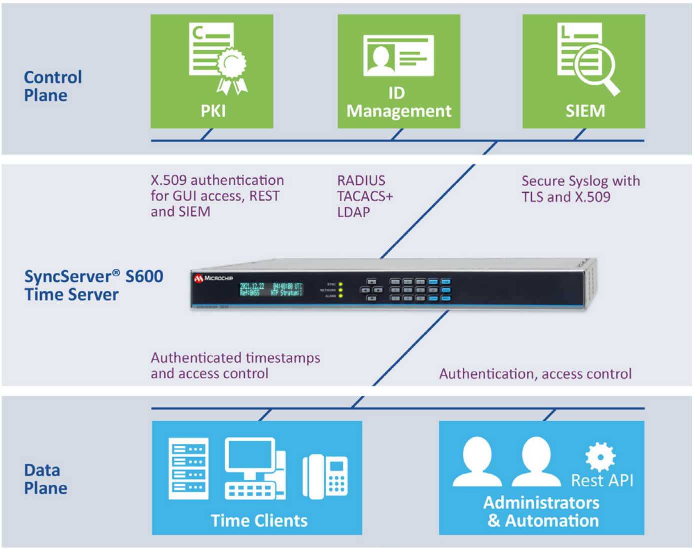

Control Plane
PKI
ID Management
SIEM
X.509 authentication for GUI access, REST and SIEM
RADIUS TACACS+ LDAP
Secure Syslog with TLS and X.509
SyncServer® S600 Time Server
Authenticated timestamps and access control
Authentication, access control
Data Plane
Time Clients
Rest API
Administrators & Automation

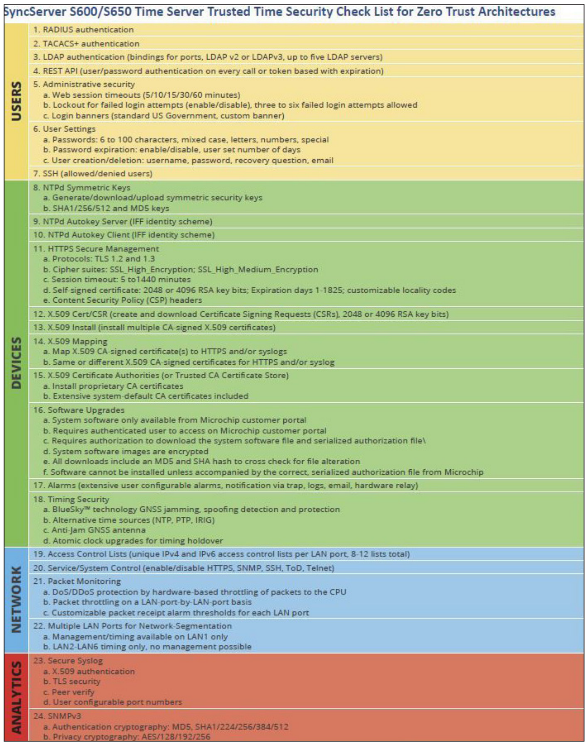
Figure 2. Interoperability of the SyncServer time server between the NIST-defined Data Plane and Control Plane

The base Zero Trust premise is to not grant implicit trust to anything, which includes the time and the time server. There are many possible scenarios for implementing trusted time in a Zero Trust architecture using a SyncServer time server. We have created infographics for some of these scenarios. In each graphic, the security technology in the SyncServer time server and the related Zero Trust pillars are highlighted for easy reference. You can view all the infographics on our Trusted Time for Zero Trust Networks web page.

Learn More About Trusted Time

If your organization is moving towards a Zero Trust Architecture across its data centers, we have created an application note that explains why trusted time is so important in a Zero Trust network. This short document explains how the SyncServer network time server ensures the security of time and complies with Zero Trust principles. It includes a detailed list of the SyncServer time server's security features and how they align with the Zero Trust model's pillars.

Your company's security team can use our helpful checklist, shown in Figure 3, for determining the SyncServer S600/S650 time server's compliance with your network's security requirements.



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

Figure 3. SyncServer S600/S650 time server trusted time security check list for Zero Trust architectures

Be Zero Trust Time Compliant

As the most secure trusted time network device, the SyncServer time server is best suited to support Zero Trust initiatives at geographically distributed data centers. It ensures the security of time and its sources, as well as complies with the fundamental pillars of Zero Trust.

Links to Resources

Web Page: Trusted Time for Zero Trust Networks

Application Note: Trusted Time for Zero Trust Networks

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