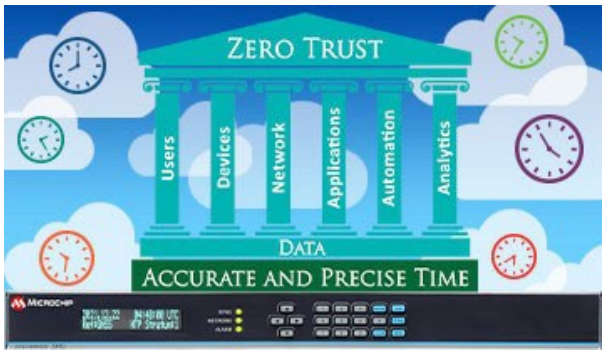
Trusted Time for Zero Trust Networks Versus Time From Internet NTP Server Pools

Summary

An organization that is rolling out a Zero Trust Architecture should understand how irrational it is to get time from public NTP server pools and how it violates the fundamental concepts of Zero Trust. Accurate time is essential for network operations, and the security of the time server that is 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.



The Risky Choice for Network Time Synchronization

It can be tempting to use publicly available NTP server pools to synchronize the time on key corporate systems. For example, some corporate edge routers use Network Time Protocol (NTP) to synchronize their internal clocks with time servers somewhere on the Internet. These routers then operate as the NTP server for the internal corporate network. This is an inexpensive though risky solution for getting timestamps.

Another scenario is using a primary domain controller to point to the IP address of an Internet time server through a port 123 hole in the firewall. The domain controller then cascades the time through the network. This is well documented and fairly easy to configure. But is free time from the Internet really worth the perceived savings and risk?

Irrational Trust

Zero Trust networks have two primary concepts:

- **Zero Trust:** A cybersecurity paradigm that trust is never granted implicitly
- **Zero Trust Architecture:** An end-to-end approach to enterprise resource and data security

The motto of Zero Trust is *Never Trust, Always Verify*.

If an organization relies on an Internet-based time server, all that can be verified is that when an NTP time request is sent to a given IP address, an NTP packet with two additional timestamps is returned. That's all. There is no indication of how accurate, reliable or secure that time is.

The remote time server is being granted implicit trust. Because the organization has not implemented end-to-end authentication or authorization, they have trusted it and not verified it. This is irrational trust.

To put it another way, would you open port 123 in your firewall and synchronize your entire network to an IP address assigned from one of over 4,000 NTP servers reportedly available at ntppool.org? There are inherent risks in doing this.

Fear, Uncertainty and Doubt Realized

Trusting NTP server pools is a good example of irrational trust. NTP timestamps are always sent in the clear and can be easily manipulated by man-in-the middle scenarios. Also, because time servers added to NTP time server pools, such as those at ntppool.org, are not vetted, anyone with malicious intent can add a time server to the pool and manipulate the timestamps that are provided to NTP clients assigned to it.

In a real-world case, a seemingly trustworthy Internet time server was configured to deliberately deliver wrong timestamps to a healthcare provider's NTP servers because the time server owner felt the NTP clients were requesting the time too frequently. The healthcare provider's log files and patient data were ruined through the night until the rogue Internet time server was identified as the source of the problem. The healthcare provider proceeded to deploy an in-house stratum 1 time server to prevent similar risks in the future.

This real-world example highlights the crux of the issue: log files and their accurate timestamps matter.

Why Time Matters

Information Technology (IT) security is responsible for protecting data, resources, personal information and much more. 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. The Zero Trust Architecture was created to help address these security challenges.

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 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 backdated to the previous week 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 any organization's network 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 an IP address of a time server from an Internet NTP server pool, 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?

Assuming time is getting synchronized using NTP from somewhere for your network, Zero Trust raises two key questions. Is the time implicitly or explicitly trusted? And is the time server itself, as a device connected to the company's network, compatible with Zero Trust networking technologies?

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.

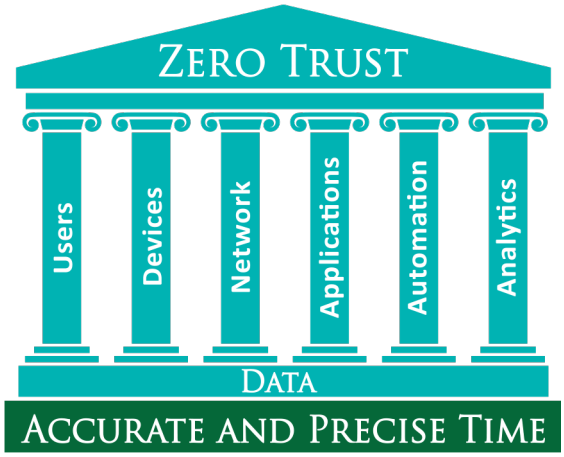


Figure 1. Accurate and precise time are foundational to Zero Trust networks

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 data plane and control plane.

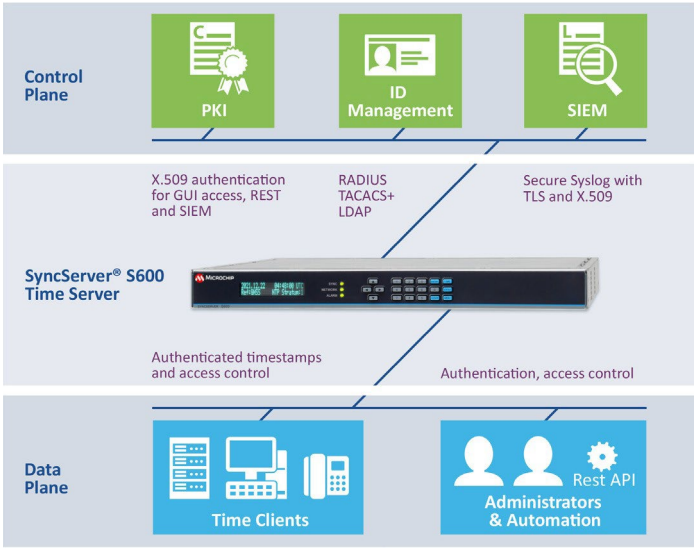


Figure 2. Interoperability of the SyncServer time server between the NIST-defined Data Plane and Control Plane

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.

Learn More About Trusted Time

If your organization is moving towards a Zero Trust Architecture, 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 any organization. It ensures the security of time and its sources, as well as complies with the fundamental pillars of Zero Trust.

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