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

In this post, we will discuss why an Information Technology (IT) professional rolling out a zero trust architecture should care a great deal about accurate time synchronization of the network and the time server providing it.

What is Zero Trust?

If you're an IT professional in a company rolling out a zero trust architecture, you probably have a pretty good idea what zero trust means in your world. From a wider perspective, here are the two primary concepts to consider:

- Zero trust: a cyber security 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". That pretty much sums it up.

Chances are that if your organization is rolling out zero trust, it started with Identity and Access Management (IAM) for users. From there, it moved on to devices connected to the network, then to the network itself by implementing strategies such as micro-segmentation and then on to automation and analytics. These are called the "pillars" of the zero trust model.

The zero trust architecture is a migration from a perimeter-based security model to one where every person and device on the network is authenticated and authorized end to end. If your company is already on this path, this is not news. What may be news though, is the critical role that Trusted Time™ plays in the zero trust network. Let's first start with why time matters.

Why Time Matters

Network-wide time synchronization accuracy and the essential role it plays in network management and security are often taken for granted in managing a network. If you're not convinced, imagine what would happen if every network device had a different time. Chaos would break out across the network.

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

Log files and network telemetry would be useless. Logs and telemetry time stamps would not correlate. For example, syslogs that would 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 time stamps would be incorrect. Enough said. As you can see, time accuracy across your company's network is important and it does matter.

Because time is so important, you need to consider the "what, who, where and when" of the source of time for network time synchronization. Time servers providing the Network Time Protocol (NTP) time stamps are the "what." If the "who" and "where" are merely an IP address of a time server from the Internet or Internet NTP server pool, then you need to consider the validity and vulnerability of the "when" of the NTP time stamps that are received. This, though, is the topic of a different blog post, since free time from the Internet violates just about every principle of zero trust and cannot be considered trusted time.

What Is Trusted Time™?

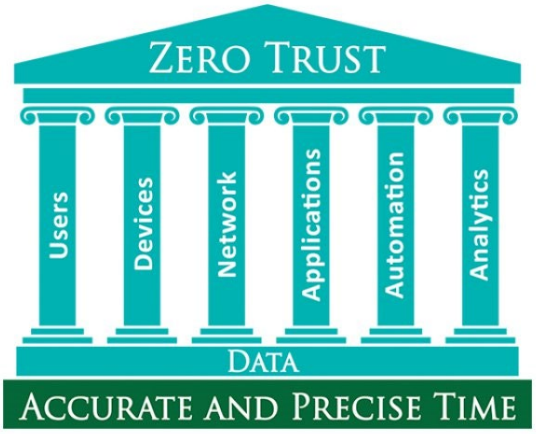
Assuming you have an **NTP network time server** in your network, zero trust raises two key questions. Is the time implicitly or explicitly trusted? And is the time server itself, as a device connected to your network, compatible with zero trust networking technologies?

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

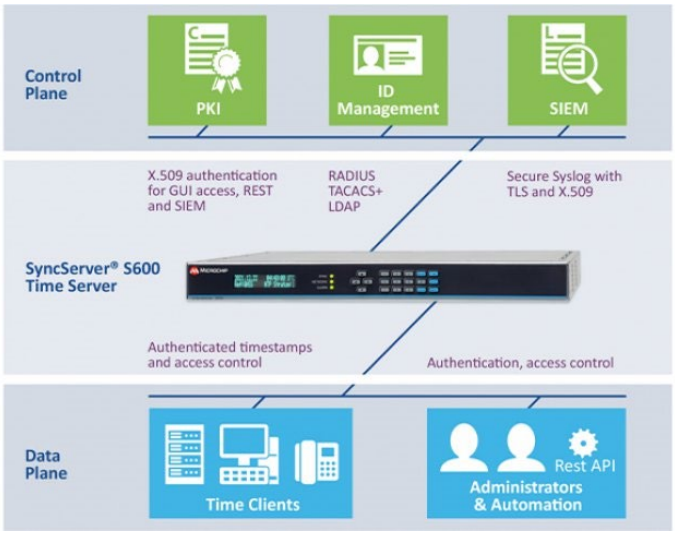
A network security team is more interested in a time server's security features than they are in verifying and validating the time stamp's accuracy or bandwidth. Since our **SyncServer® S600/S650** network time servers offer unsurpassed timing performance, let's discuss their security attributes.

As the most secure Trusted Time network devices currently available, SyncServer time servers comply with the fundamental pillars of the zero trust model, which include users, devices, network, applications and analytics.

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



The following infographic is a simplified representation of the core components outlined in NIST Special Publication 800-207: Zero Trust Architecture. It demonstrates how these pillars relate to the NIST data plane and control plane.



For example, let's discuss how you can allow an admin (user pillar) in the data plane to access the **SyncServer S600 server's** web GUI. The first step is to use the X.509/PKI infrastructure (device pillar) in the control plane to authenticate the S600 server to the browser.

After the server is authenticated, the admin submits credentials via RADIUS/TACACS+/LDAP for user authentication with the ID management system in the control plane. If access is authorized, the user is granted access to the S600 server's web GUI.

As the most secure trusted time network device, the SyncServer® S600 time server is well suited to support zero trust initiatives. It ensures the security of time and its sources and complies with the fundamental pillars of zero trust.