Deploying Traffic Telemetry Methods

**Network telemetry** offers extensive and useful detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed activity. It is both inexpensive and relatively simple to implement.

**Network Time Protocol**

* To maintain the most accurate time update from an authoritative time source on the network, the software clock in your network should receive time updates from an authoritative time on the network to have consistent time setting across the network.
* **Networks use NTP to synchronize** the clocks of various devices across a network.
* A secure method of providing clocking for the network is for network administrators to implement their own private network primary clocks that are synchronized to a Coordinated Universal Time (UTC)-based satellite or radio.
* if network administrators do not wish to implement their own primary clocks because of cost or other reasons, other clock sources are available on the internet, such as [http://www.ntp.org](http://www.ntp.org/), but this option is less secure.
* NTP runs over UDP, **using port 123** as both the source and destination, which in turn runs over
* NTP uses the concept of stratum to describe how many NTP hops away a machine is from an authoritative time source, a stratum 0 source.
* Ex : a stratum 2 time server receives its time from a stratum 1 time server, an. A device running NTP automatically chooses as its time source the device with the lowest stratum number that it is configured to communicate with through NTP.

NTP can get the correct time from an internal or external time source:

* Local primary clock
* Primary clock on the internet
* Global Positioning System (GPS) or atomic clock (stratum 0)

NTP is used for clock synchronization between devices and is required for these operations:

* **Logging with accurate timestamps**: Usually logs are directed to one or a few syslog servers that receive all messages, and you can view the local time stamps for all messages. If you compare logs on different devices, then synchronized time is essential to analyzing past events successfully.
* **Digital certificate validation**: When using certificates, synchronized time is necessary, because a certificate is considered valid only if the current time falls within the time (and date) interval that is specified inside the certificate. A certificate that seems to be expired is not considered valid. Similarly, a certificate that shows an issue date in the future is not valid.
* **Single sign-on (SSO) authentication mechanisms**: Some security devices support SSO authentication against Microsoft Active Directory Server. Such integration requires that time both on the security device and on the Microsoft Active Directory Server is within specific limits.
* **Stability of software-defined storage**: Cisco HyperFlex and similar products require a stable and continuous source of NTP. NTP is used for clock synchronization between different components of the system. If time differs on different components of the solution different functions, such as snapshots, can fail.

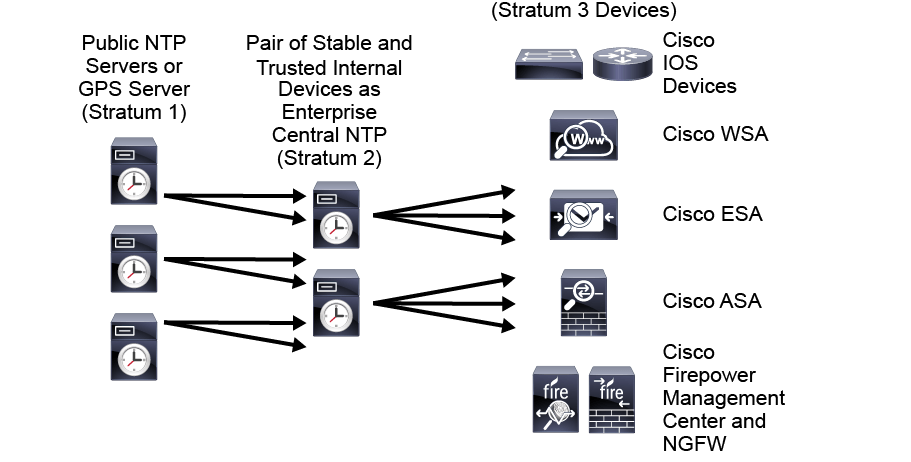
NTP architecture for enterprise

* A pair of your devices to synchronize their time to a list of public NTP servers.

1. One choice is a pair of network core devices.
2. Another choice is your redundantly deployed Windows Server Domain Controller.

* Alternative is a local NTP server with GPS (stratum 1).
* Public NTP servers and local GPS servers are typically stratum 1 which makes your lowest stratum devices stratum 2.

Three steps to configure NTP to cisco devices : Configure time zone, NTP server and NTP authentication if NTP server requires authentication.



**Specifics recommendations NTP implementation that you need to consider:**

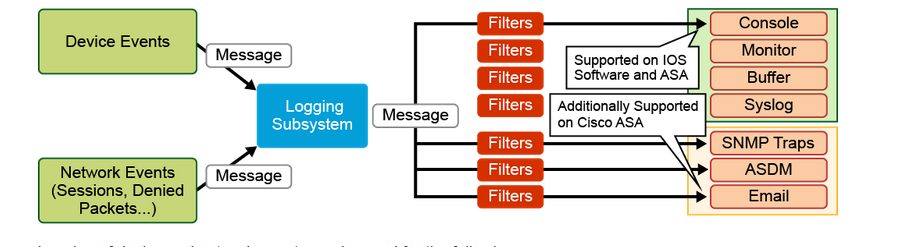
* If your Cisco FMC cannot directly reach the network NTP server, or your organization does not have a network NTP server, a physical Cisco FMC can serve as an NTP server to Cisco Firepower NGFW.
* Do not use a virtual Cisco FMC as an NTP server.
* For Cisco Firepower NGFW 4100/9300 devices, you do not set NTP through FirePower Management Center (FMC). Configure NTP in Firepower eXtensible Operating System (FXOS).
* Cisco WSA has default NTP set to time.sco.cisco.com. Cisco ESA has default NTP set to time.ironport.com.

NTP authentication

An attacker hides behind a rogue host and pretends to be a legitimate NTP server

* NTP can use encoded keys to verify timestamps supplied by NTP servers.
* NTP decrypts the password it receives and matches it with an agreed key. Once authentication is successful, the device can authorize any NTP-related action.

**Device and Network Events Logging and Export**



Logging of device and network events can be used for the following:

* Device failure notifications
* Network telemetry and forensics
* Security audit

**Severity levels**

0—Emergencies: Extremely critical "system unusable" messages

1—Alerts: Messages that require the administrator to take immediate action

2—Critical: A critical condition

3—Errors: An error message

4—Warnings: A warning message

5—Notifications: A normal but significant condition

6—Informational: An information message

7—Debugging: A debug message or a very detailed accounting message