The Network Time Protocol (NTP) is a vital system used to synchronize time across computers and network devices, ensuring accurate and consistent timestamps, security events, and system logs throughout the environment. In this network topology, the AAA virtual machine (VM) operates as the internal NTP server, while all other hosts—such as Debian VMs and Mikrotik routers—act as NTP clients and synchronize their clocks with the AAA server.

## NTP Security Policy Overview

NTP security in this network is founded on restricting access, authenticating sources, and minimizing exposure to external threats. The AAA server's NTP service is hardened by only synchronizing with trusted upstream servers and permitting only internal hosts to request time synchronization. The default policy for access is restrictive: internal networks are allowed to sync but cannot modify, peer, or query the server, and the public is denied all requests. Additionally, logging is enabled and restricted to the NTP user, local fallback clocks are configured, and NTP listens only on trusted interfaces to reduce attack surface.

## Security Measures for NTP Server

- Only trusted time sources are used for synchronization, such as Google and pool.ntp.org servers.
- Internal network ranges (NAC, DMZ, supplicant networks) are specifically allowed to synchronize with the AAA server, using strict access control policies.
- Unauthorized modification, configuration queries, or monitoring requests are disabled using configuration options like `restrict default kod nomodify notrap nopeer noquery` and `disable monitor`.
- Monitoring and logging are enabled for NTP operations, with log directories securely owned by the NTP service account.
- Only designated interfaces are bound for NTP communications to prevent exposure to untrusted networks.

## Security Measures for NTP Clients

- Clients, including Debian hosts and Mikrotik routers, are configured to synchronize exclusively with the AAA NTP server and do not act as servers themselves.
- Access controls prevent clients from accepting queries or serving time to other devices, reducing the potential attack surface.
- Monitoring and periodic verification of time synchronization on clients help detect anomalies, ensuring the integrity of the time distribution.
- NTPsec service on clients is set to start only after the network is available, supporting robust operation and minimizing risk due to misconfiguration.

## Operational and Monitoring Practices

- NTP configurations and logs should be reviewed regularly for suspicious activity, such as unexpected queries or failed synchronization attempts.
- Software updates for NTPsec are essential for patching vulnerabilities and maintaining security.
- The use of fallback clocks and monitoring mechanisms enhances reliability even if upstream NTP sources become unavailable.

This security policy ensures that all devices maintain accurate and secure time synchronization while effectively managing access and minimizing exposure to network-based attacks.