# Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 7:36:43 PM

Selected by: Ruud Leurs

| | |
|---|---|
| **Requirement** | **Correct date and time** |
| **Description** | Every system or application must use the central internal NTP platform as a time source or a directly connected time server. External sources are not permitted. The time zone must be configured with the local time zone. |
| **Supplement** | It is important that all systems and applications have the same time at same moment. To accomplish this, it is necessary that everything synchronizes with the same time source or a directly connected time server. This way, all systems or applications will use a stratum 1 or stratum 2 timestamp.<br><br>Besides the fact that this accomplishes consistency in time, we also accomplish that systems are not influenceable through third party sources. Because of this, systems do not only have the correct time, but the time is also trustworthy.<br><br>It is permitted to set up an NTP server that is used to synchronize other systems deeper in the network. In this case, the NTP server must synchronize with the central NTP platform by using it as the only source. For example: Within a Windows domain it is enough if the domain controller with the PDC role is configured to use the central NTP platform if all other domain servers and clients are configured to synchronize their time with the PDC.<br><br>Please note that NTP does not synchronize time zone or daylight savings time. Therefore, it is necessary to configure this locally. If in doubt, configure the time zone GMT+1. |
| **ID** | KSP-RE-37 |
| **Version** | 2.1 |
| **Date** | November 2, 2018 |
| **Rationale** | Logging |
| **Rationale** | Connect to Security Operations Centre (SOC) |
| **Rationale** | Configuring date and time |

| | |
|---|---|
| **Requirement** | **Stratum 0 sources for NTP servers** |
| **Description** | Time sources that are part of the central KPN NTP platform must use a minimum of two different stratum 0 sources. |
| **Supplement** | Stratum 0 sources are e.g. Global Navigation Satellite Systems (GNSS) like GPS or Galileo, atom clocks, or the radio signal DCF77.<br><br>It is only permitted to use GNSS as a time source when mitigations are implemented against spoofing or jamming of the GNSS signal. This can be done by implementing e.g. a GPS firewall or a reference clock that must be used to detect the skew of time. |
| **ID** | KSP-RE-711 |
| **Version** | 1.1 |
| **Date** | November 2, 2018 |
| **Rationale** | Connect to Security Operations Centre (SOC) |
| **Rationale** | Configuring date and time |

| | |
|---|---|
| **Requirement** | **Connect to Log Monitoring** |
| **Description** | Networks, systems and applications must be connected to Log Monitoring of the KPN SOC. |
| **ID** | KSP-RE-718 |
| **Version** | 1.0 |
| **Date** | November 2, 2018 |
| **Rationale** | Logging |

| | |
|---|---|
| **Requirement** | **Connect to Intrusion Detection Monitoring** |
| **Description** | Networks, systems and applications must be connected to Intrusion Detection Monitoring of the KPN SOC. |
| **ID** | KSP-RE-719 |
| **Version** | 1.0 |
| **Date** | November 2, 2018 |
| **Rationale** | Logging |

| | |
|---|---|
| **Requirement** | **Connect to Vulnerability Monitoring** |
| **Description** | Networks, systems and applications must be connected to Vulnerability Monitoring of the KPN SOC. |
| **ID** | KSP-RE-720 |
| **Version** | 1.0 |
| **Date** | November 2, 2018 |
| **Rationale** | Logging |

| | |
|---|---|
| **Requirement** | **Connect to Anti-DDOS Monitoring** |
| **Description** | Directly accessible networks, systems and applications must be connected to Anti-DDOS Monitoring of the KPN SOC. |
| **ID** | KSP-RE-721 |
| **Version** | 1.0 |
| **Date** | November 2, 2018 |
| **Rationale** | Logging |