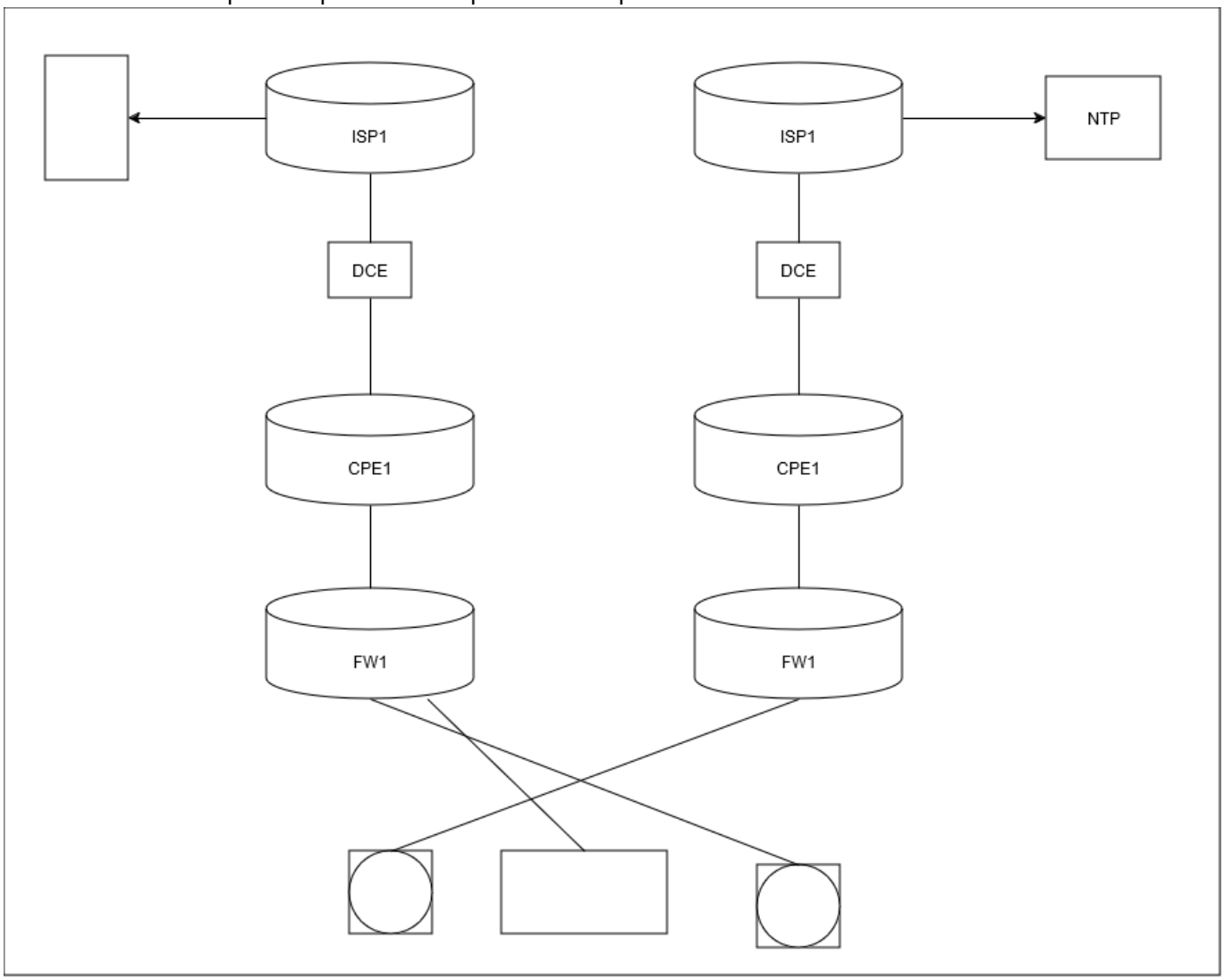
[Redes Seguras] Monitorización

La monitorización de red es una disciplina que nos ayuda a controlar que la red funciona adecuadamente y que se comporta dentro de unos parámetros de rendimiento aceptables. También se puede analizar la cantidad de tráfico que circula y por donde circula. Las herramientas más utilizadas son:

- Syslog: Recoge mensajes relacionados con los eventos de los dispositivos o los mensajes generados por IPDS
- SNMP: Monitorización dee equipos de red desde el punto de vista de consumo de ancho de banda y uso de CPU, es necesario que antes estén debidamente sincronizados y en hora.

La validez de certificados es muy importante. IP SLA (IP Service Agreepent) es un contrato sobre disponibilidad que se realiza con el proveedor de internet. En caso de cisco tenemos un servicio con el mismo nombre que nos permite comprobar la disponibilidad.

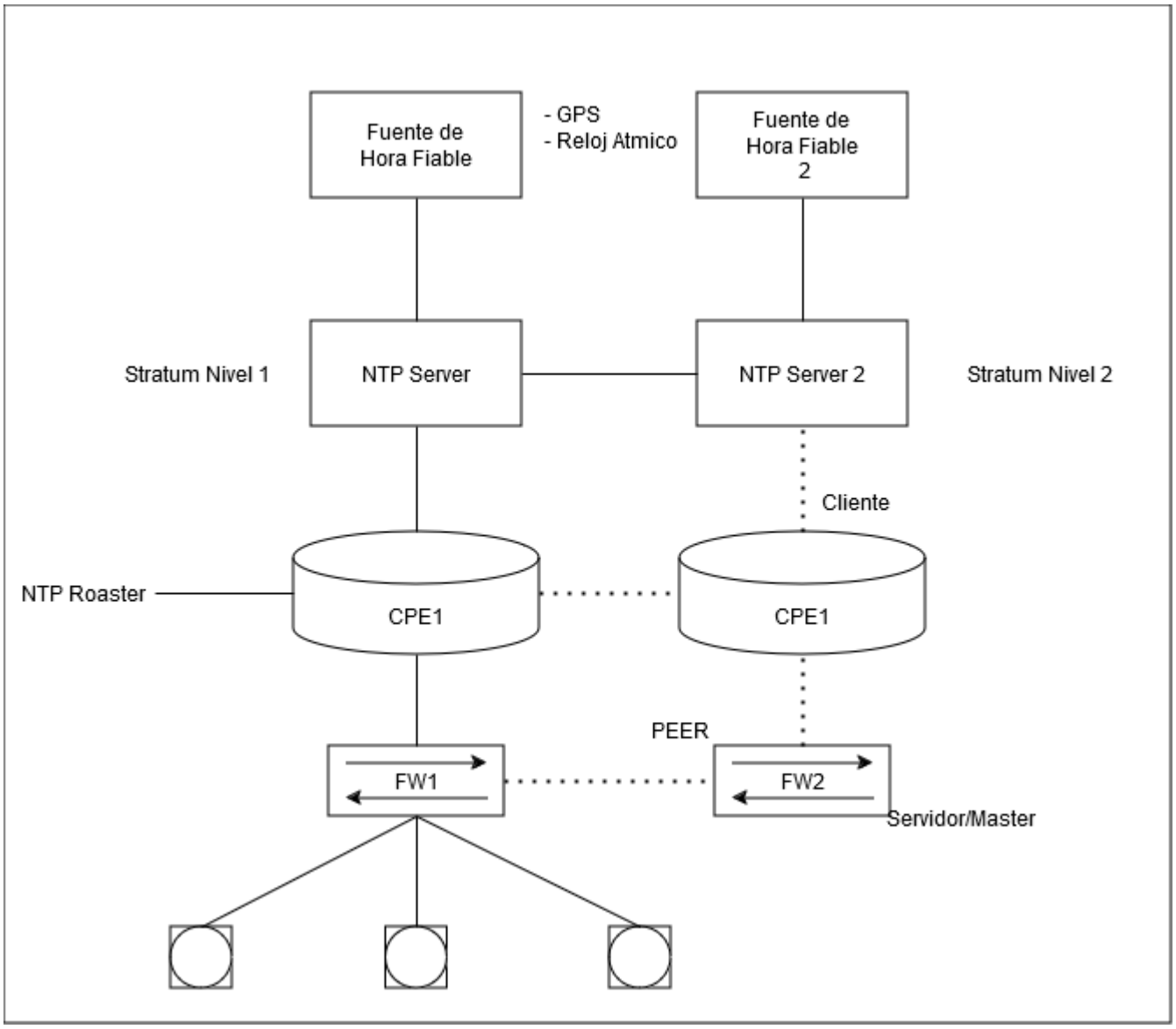


Configuración manual de sistema

- Show Clack
- showClokck
- clock.

NTP es un protocolo de capa de aplicación para compensar la desviación horaria.

Network Time Prtocol (NTP)



NTP nunca se sincroiniza con una máquina que está sincronizada consigo misma. Tampoco tiene en cuenta información que se separe del resto de valores obtenidos por NTP. NTP puede operar en 4 modos: Servidor: Proporciona info a los clientes Cliente: Obtiene información del servidor Peer o Simetric: Se basa en la configuración de un grupo de peers de bajo nivel stratum que sirven de backup mutuos. Broadcast/Multicast: Se aplica donde la necesidad de precisión es modesta. Los clientes no necesitan especificar la IP del servidor. Se configura un server como broadcast y la dirección de subred par aenviar este tipo de trafico.

Protección de NTP

Se pueden usar ACLs y Autenticación para la configuración interna, para dar fiabilidad a la configuración externa se recomienda utilizar certificados, de forma que la información vaya firmada con clave privada y se pueda descifrar con una clave pública.

Syslog

Es un mecanismo que permite a un dispositivo proporcionar información acerca de errores y notificaciones importantes del sistema. Los servidores de syslog almacenan los mensajes importantes. Los mensajes se reciben por el puerto UDP 514. Cuando tenemos mensajes de log se nos proporciona una información textual para que pueda ser interpretado por el administrador del sistema. Los mensajes de syslog también hacen referencia al nivel de gravedad y a la tecnología específica afectada. En Cisco hay 8 niveles que van del 0 al 7, siendo los de nivel 0 los más graves y los de nivel 7 los menos graves:

- Emergency (level 0)
- Alert (Level 1)
- Critical (Level 2)
- Error (Level 3)
- Warning (level 4)
- Notice (Level 5)
- Informational (Level 6)
- Debugging (Level 7)

Infraestructuras a las que hacen referencia los mensajes de syslog:

- IP
- OSPF
- SYS operating SYstem
- IPSec
- Route Switch Processor (RSP)
- Interface

Formato de mensajes syslog:

- Facility: Referencia la tecnología afectada
- Severity: Del 0 a 7 en función de gravedad
- Mnemonic: Código de identificacion del mensaje de error
- Message-text: cadena de texto que describe la condición.

Configuración de Syslog

con “logging trap <level>” podemos establecer el nivel de severidad de un mensaje. Con Show Logging podemos mostrar el contenido de los archivos de log locales