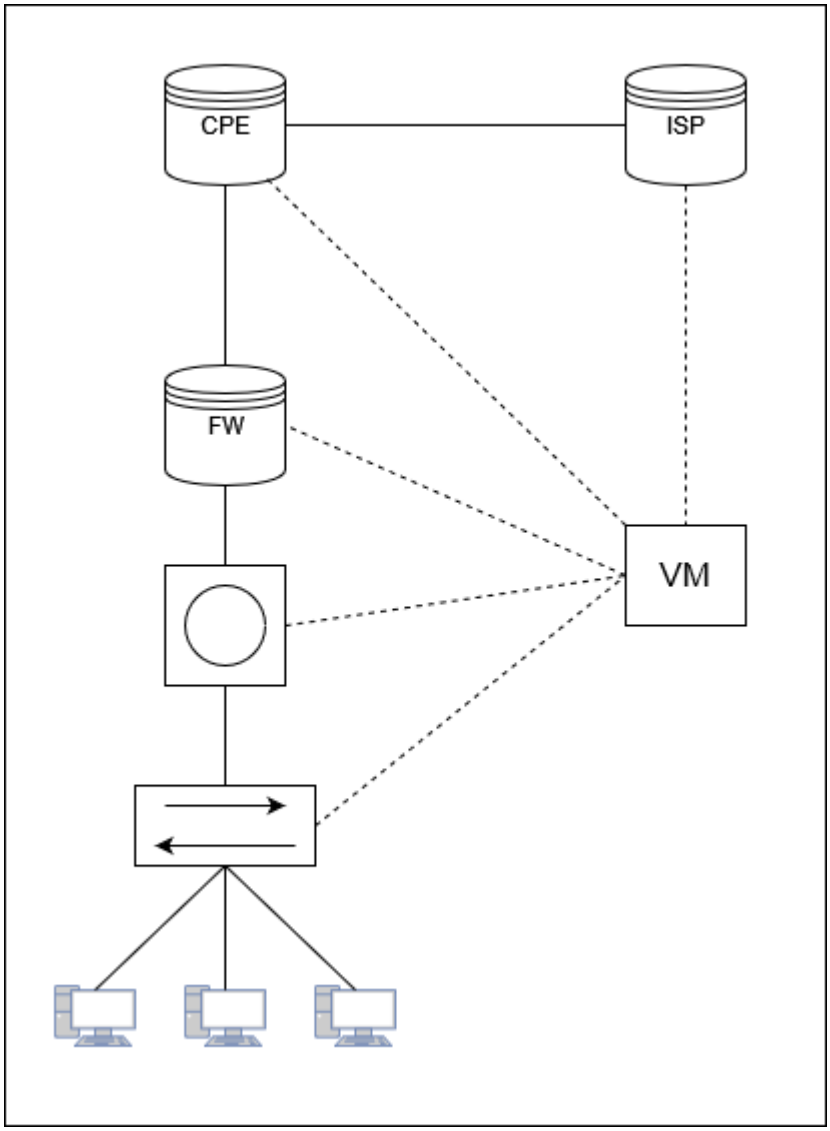
Fortificación de los Dispositivos de Red



Introducción

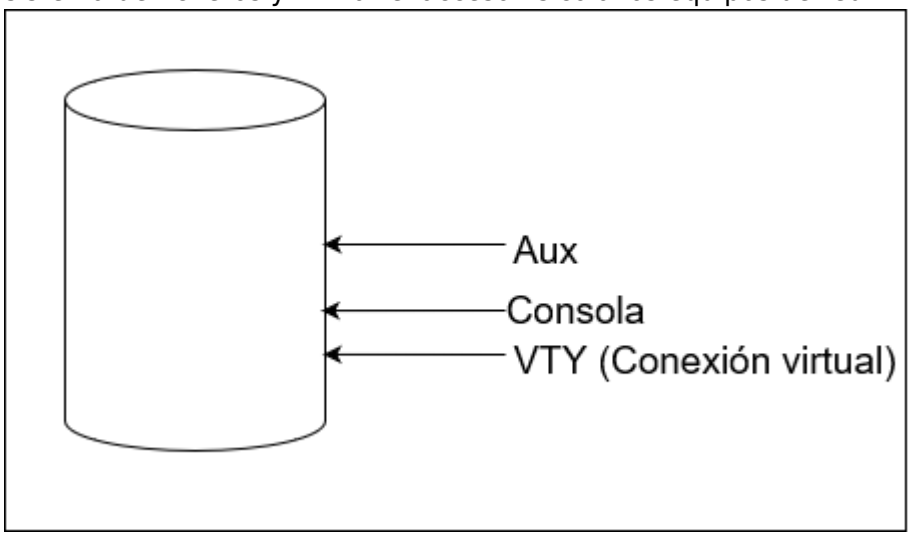
Los dispositivos de red son un elemento que debemos proteger desde diferentes punto de vista ya que están expuestos a nivel de perímetro. Tenemos 3 planos:

- Tráfico de usuario (Plano de datos)
- STP, OSPF, HSRP... (Plano de control)
- Plano de Gestión

Cada uno de estos planos necesita requerimientos de protección distintos. Existen interdependencias a la hora de proteger o configurar los diferentes mecanismos de seguridad de cada plano.

Seguridad en el Plano de Gestión

El objetivo es permitir el acceso solo a los usuarios autenticados, controlar que pueden hacer en función a sus privilegios, cifrar las comunicaciones de gestión remota (SSHv2, SSL/TLS), proteger el sistema de ficheros y limitar el acceso físico a los equipos de red.



Se puede usar protección por contraseña de línea (Menos seguro), protección con usuarios locales y otra es la utilización de AAA new Model. Lo mejor es usar una lista de métodos de autenticación:

1. AAA Server
2. BBDD de Usuarios Locales

También se debe proteger la sincronización horaria ya que si se desincroniza pueden fallar los certificados digitales al fallar la fecha. Telnet debe ser deshabilitado y el uso de SSH y TLS 1.2 es mandatorio. Se debe monitorizar de forma segura con SNMP ya sea versión 2 o 3. Buenas prácticas:

- Reestablecer contraseña tras contraseñas fallidas
- Bloquear cuentas temporalmente si se ponen contraseñas mal
- Forzar contraseñas de longitud mínima
- Definir niveles de privilegio
- Desplegar servicios AAA para autenticación
- Deshabilitar servicios no necesarios, disminuyendo así la superficie de ataque
- Utilizar infraestructuras diferenciadas para gestionar dispositivos.