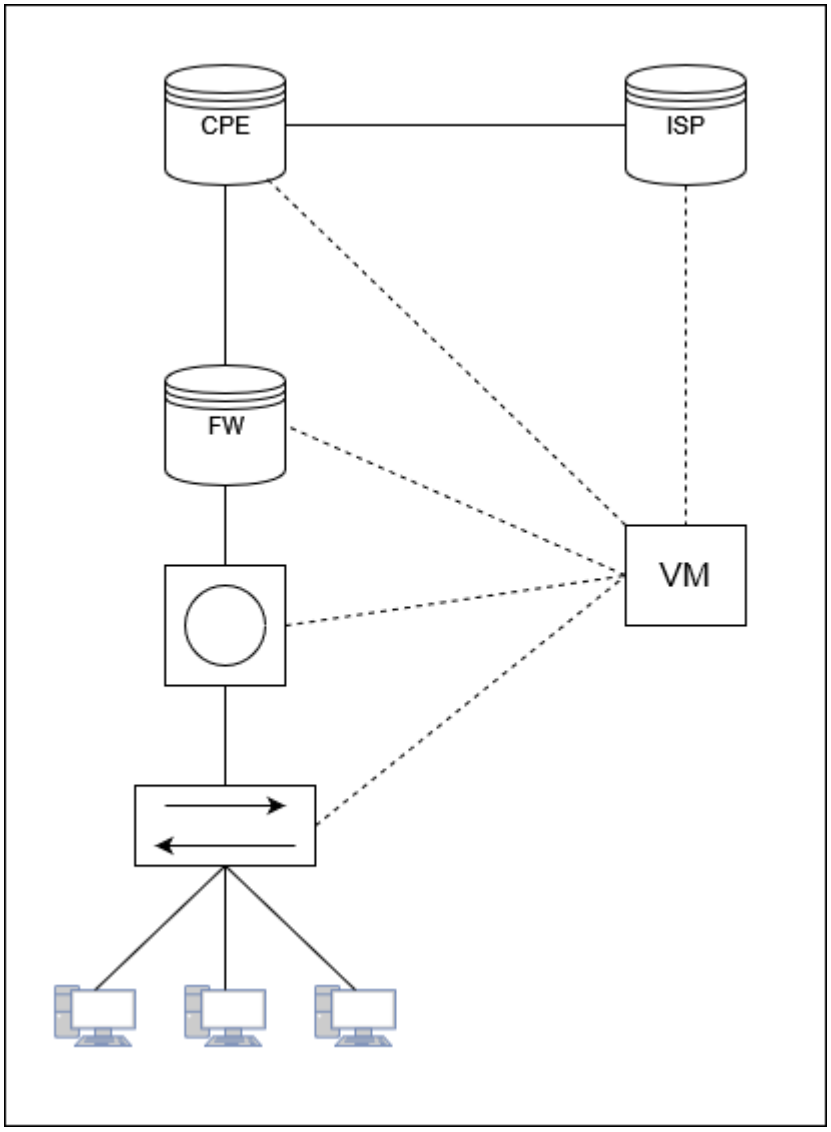
Fortificación de los Dispositivos de Red



Introducción

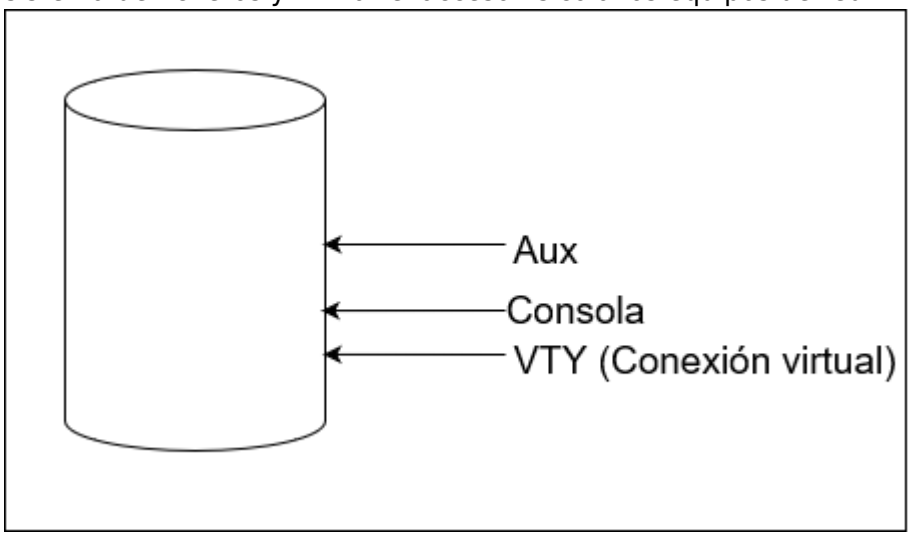
Los dispositivos de red son un elemento que debemos proteger desde diferentes punto de vista ya que están expuestos a nivel de perímetro. Tenemos 3 planos:

- 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.

El plano de gestión está enlazado a la administración de dispositivos.

1. Consola (Line Console 0): se usa para administrar el router cuando viene de fábrica o cuando se produce una catástrofe total. Lo malo es que conectarse por vía consola suele ser incómodo.
2. Acceso remoto (Line VTY 0-15): puede ser por telnet (no seguro) y SSH v2 (Seguro)
3. Protocolo SNMP: Permite monitorizar y configurar los dispositivos, aunque en general se usa para monitorización.

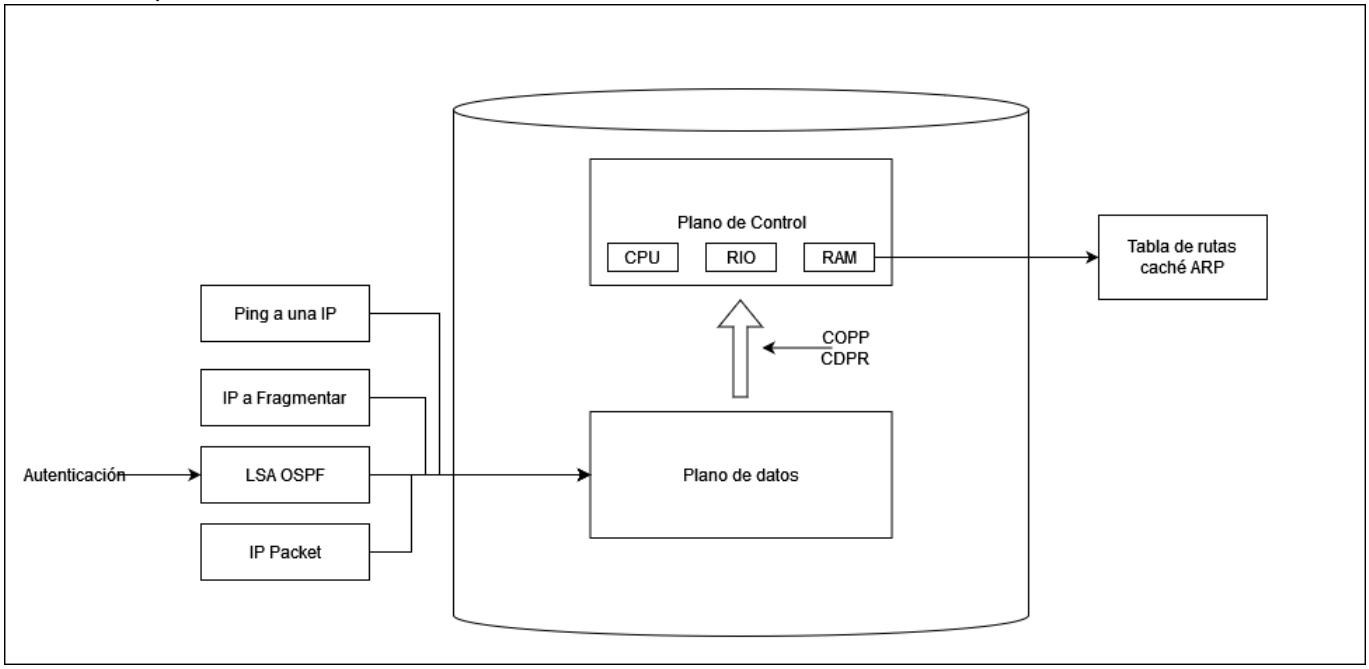
Para asegurar estos puntos de acceso a la gestión se recomienda establecer métodos de autenticación:

1. Contraseña de línea: Contraseña especificada durante la configuración inicial, método muy poco seguro. Comandos clave: “login” y “password”
2. Configuración de usuarios locales: cuando se añaden usuarios locales la contraseña de línea

queda desactivada. Comandos clave: “login local” y “username () password”

3. Autenticación AAA: Permite definir métodos alternativos de autenticación, por ejemplo, la utilización de usuarios que se encuentren en un servidor externo. También se pueden usar métodos de autenticación de backup, de forma que puedes dejar un segundo método de autenticación en caso de que falle el servidor externo. AAA permite también autorizar, asignando niveles de privilegio a los usuarios, limitando que usuarios pueden configurar el router.

Los equipos de cisco tienen 16 niveles de privilegios, cuando uno hace login entra en nivel 1 y en cuanto se hace “enable” se pasa a nivel 15. Lo malo de este sistema es que si alguien tiene nivel 15 puede acceder a todos los comandos de los otros niveles, lo que hace que no sea posible crear usuarios especializados con acceso solo a ciertos comandos.



Buenas prácticas

- Configurar mecanismos de autenticación de protocolos de enrutamiento
- Implementación de técnicas que limiten los paquetes que deben ser procesados por la cpu con CoPP y CPPr:
  - CoPP: Control Plane Policing: Filtros para cualquier tráfico dedicado a las IPs del router. Se puede aplicar al tráfico de gestión. Evita ataques basados en el envío masivo de datos.
  - CPPr: Control Plane Protection: Permite llevar a cabo un proceso de filtrado más detallado. Consideran 3 interfaces distintas en función al tipo de tráfico que debe manejar.
    - Host subiterface: maneja el tráfico hacia una interfaz física o lógica del router
    - Transit subiterface: Gestiona el tráfico del data plane que necesita la intervención de la CPU antes de enviarlo
    - CEF-Exception subinterface: relacionado con el tráfico que procesa el DEF que produce situaciones excepcionales

Seguridad en el Plano de Datos

Recomendaciones:

- Implementación de ACLs para filtrar tráfico directamente
    - Se debe permitir solo tráfico autorizado en la política de seguridad
    - Se previene el IP Spoofing
- Funcionalidades de firewall
    - CBAC: Context Based Access Control
    - ZBF: Zone Based Firewall
- IPS: implementación software
- TCP intercept
    - Evita ataques SYN-FLOOD
- Unicast Reverse Path Forwarding
    - Compruea la dirección IP de origen de los paquetes.

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=redes:fortificacion&rev=1726848498

Last update: **2024/09/20 16:08**