Taller de administración de redes y servicios de comunicaciones

Proyecto edición 2026

Introducción

El proyecto de la asignatura consiste en el despliegue de una red empresarial típica, con sus servicios internos y algunos servicios a internet. El estudiante debe instalar, documentar, configurar y administrar los servicios indicados.

En clase se dará una introducción a cada servicio y se nombrará una herramienta que implemente dicho servicio, es responsabilidad del grupo de proyecto investigar y leer la documentación oficial de los programas a utilizar para su correcta instalación y configuración.

Las herramientas nombradas son solo una sugerencia por parte de los docentes (en general son las más utilizadas y conocidas), el grupo de estudios puede proponer otras que conozca.

Los grupos del proyecto se definirán en clase tomando en cuenta la cantidad de inscriptos al taller.

Arquitectura

En el CURE sede Rocha se encuentran los dos servidores (AMD Ryzen 7 3700x 8-core, 64GB RAM, 12 TB HDD) en los que se trabajará. Cada uno de ellos tiene instalada la plataforma de virtualización Proxmox, y ambos están conectados entre sí formando un cluster.

Cada nodo del cluster tiene asignada una IP pública:

- pve1 → 164.73.226.194
- pve2 → 164.73.226.195

Observación: para acceder al cluster se puede utilizar cualquiera de las IPs.

Los nodos Proxmox se conectan a la red del CURE a través de un router con OpenWRT, y a través de la red del CURE salen a internet.

En la figura 1 se puede ver un diagrama general de la arquitectura.

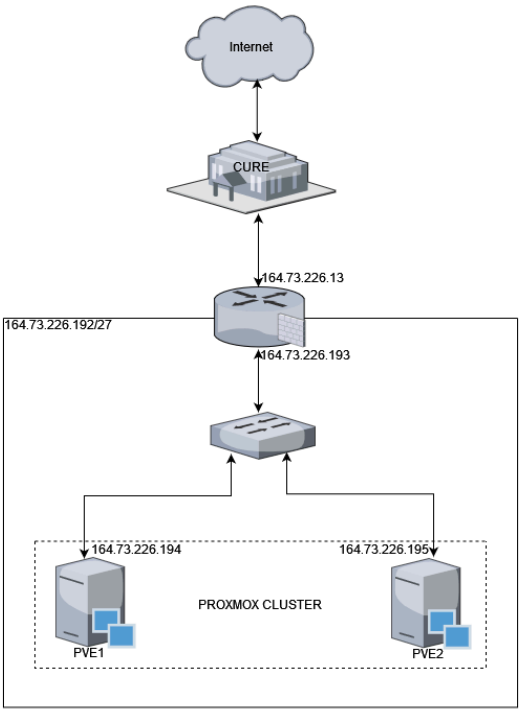

Figura 1. Diagrama general

Para el proyecto se simulará sobre Proxmox la red en la que se trabajará, que al comienzo consta de un firewall y tres zonas:

- WAN: conexión con internet, IP pública 164.73.226.20X
- LAN: switch swLAN_gX, red 192.168.1.1/24
- DMZ: switch swDMZ_gX, red 192.168.10.1/24

Observación: en todos los casos, X corresponde con el número de grupo.

El firewall no es más que una máquina virtual con tres interfaces de red (una asignada a cada zona) y el SO Pfsense Community, los switches asignados a cada zona son Linux Bridges (switches virtuales).

Tanto la configuración de los switches virtuales como el firewall con las configuraciones mínimas para tener conectividad serán dados.

En todos los casos el dominio raíz será **tectel.cure.edu.uy.**

En la figura 2 se puede ver un diagrama de la red que tendrá que administrar cada grupo.

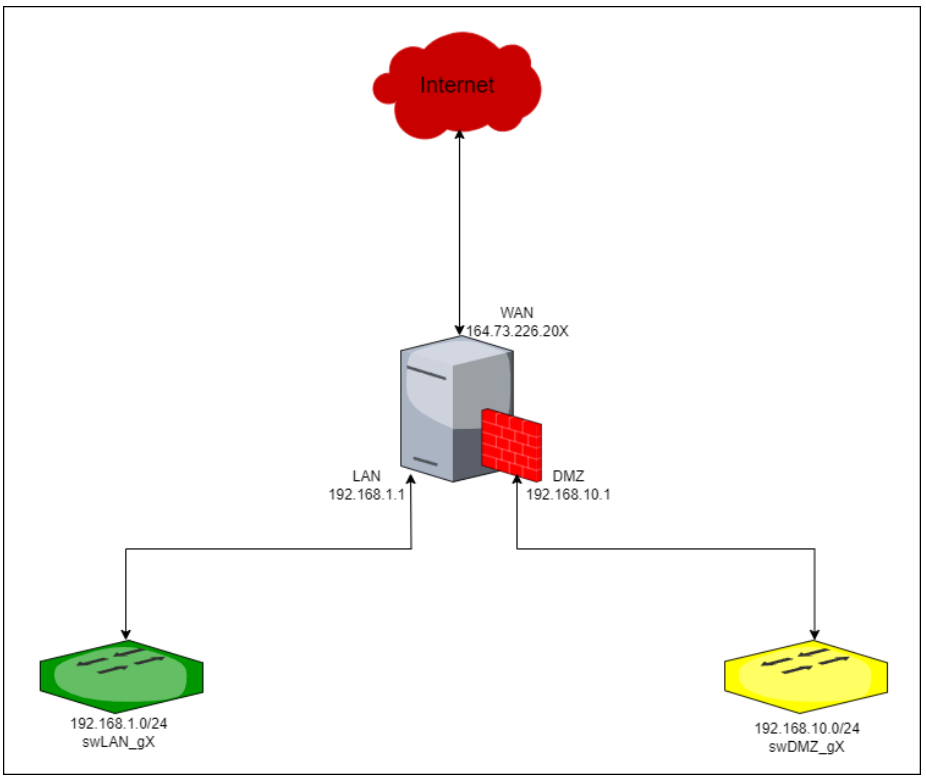

Figura 2. Red simulada del proyecto

Tareas

TODOS los temas dados en clase van para el proyecto, ya sea a través de documentación sobre el mismo, o de un sistema instalado, configurado y documentado. A continuación se presenta la lista de temas a ver en el curso:

- Instalación de servidores
  - Planilla de instalación
  - LVM
  - RAID
- Firewall
- DNS
  - Primario
  - Secundario
- DHCP
- Acceso remoto
  - SSH
  - Fail2Ban
  - Pasarela
- Monitoreo
  - Zabbix
- Logs
  - Logrotate
  - Logwatch

    - Rsyslog
    - Centralizar logs
- Servidor Web
    - Apache
    - Certificados
    - CMS
- Automatización
    - Ansible
- Respaldos
    - Políticas
    - Almacenamiento en la nube
- Correo electrónico
    - Servidor de correo
    - Políticas y seguridad
- Aplicaciones Java y BD
    - Tomcat
    - MySQL
- LDAP
    - OpenLDAP
- VPN
    - OpenVPN
- Opcional 1
    - VoIP
- Opcional 2
    - WAF y Proxy

Desarrollo

El grupo del proyecto trabajará de forma autónoma y autogestionada y quedará a su cargo la división de tareas.

Se les recomienda seguir los siguientes pasos para la instalación de cada servicio:

1. Investigación y diseño de la solución
2. Implementación
3. Verificación
4. Corrección de errores
5. Nueva verificación

IMPORTANTE: Todo el desarrollo del proyecto deberá estar debidamente documentado. De la documentación se espera:

- Descripción y marco teórico del servicio a instalar
- Proceso de instalación
- Configuraciones y aspectos fundamentales de la misma
- Pruebas y testing
- Resultados

El formato de la documentación queda a criterio de cada grupo. Se recomienda ampliamente usar LaTEX (por ejemplo https://www.overleaf.com/).

Evaluación

El proyecto consta de dos entregas, una entrega intermedia que debe cubrir los temas vistos hasta la semana anterior (o lo indicado por los docentes) y una entrega final que cubre la totalidad de los temas.

La defensa intermedia es el 25% de la nota del curso, mientras que la final el restante 75%.

Defensa intermedia

En la defensa intermedia se evaluará lo siguiente:
Documentación: documentación generada por el grupo, la misma debe cumplir con lo solicitado en la letra. (Máximo 100 hojas, por más detalle ver ANEXO I).
Presentación y prueba de funcionamiento: cada grupo debe presentar el trabajo realizado hasta el momento. El grupo debe ir contando las decisiones que tomó, problemas que tuvo, configuraciones de interés, etc, además de mostrar los sistemas funcionando correctamente. Es responsabilidad del grupo encontrar la mejor forma de mostrarlo y ensayarlo previamente. Si el sistema tiene varias funciones deben mostrar todas. (Máximo 25 minutos).

En la instancia los docentes darán una devolución de la documentación para que se corrija previo a la entrega final. Pueden haber preguntas grupales o individuales durante la presentación y prueba de funcionamiento.

La instancia es obligatoria, no presentarse significa perder el curso.

Fecha y modalidad a confirmar.

Defensa final

En la defensa final se evaluará lo siguiente:

1. **Documentación**: documentación generada por el grupo, la misma debe cumplir con lo solicitado en la letra. (Máximo 150 hojas, por más detalle ver ANEXO I).
2. **Presentación y prueba de funcionamiento**: cada grupo debe presentar el trabajo realizado hasta el momento. El grupo debe ir contando las decisiones que tomó, problemas que tuvo, configuraciones de interés, etc, además de mostrar los sistemas funcionando correctamente. Es responsabilidad del grupo encontrar la mejor forma de mostrarlo y ensayarlo previamente. Si el sistema tiene varias funciones deben mostrar todas. (Máximo 30 minutos).
3. **Oral individual**: Luego de las etapas anteriores se procederá a tomar evaluación oral individual a todos los estudiantes. En el oral se puede preguntar cualquier tema del curso, puede ser una pregunta teórica, realizar una configuración en alguno de los sistemas, instalar alguno de los sistemas, resolver alguna situación simulada

(caída de un sistema, restauración, etc), explicar alguna configuración realizada, realizar algún procedimiento, etc.

Pueden haber preguntas grupales o individuales durante la presentación y prueba de funcionamiento.

Para aprobar el curso es necesario obtener el 50% de la nota total del oral individual.

La instancia es obligatoria, no presentarse significa perder el curso.

Fecha y modalidad a confirmar.

Para todas las instancias se puede usar la documentación generada, bibliografía, internet y cualquier recurso menos la consulta a otros compañeros.

ANEXO I - Guía de temas

La idea de esta guía es orientar al grupo en la elaboración del proyecto dando un punteo de lo esperado en cada tema. No es exhaustiva ni condicionante.

Instalación de servidores

- Marco teórico del sistema operativo utilizado
- Marco teórico de LVM y RAID
- Marco teórico de EFI, UEFI, Grub
- Guia de instalación del sistema operativo
- Configuración de LVM/Raid
- Uso de LVM, comandos para LVM
- Formato de planilla de instalación
- Planilla de instalación para cada servidor

Monitoreo

- Plan de monitoreo, que servidores voy a monitorear, qué valores de cada servidor, umbral para cada valor elegido, ¿corresponde alarma?, qué hacer en caso de pasar cada umbral.
- Marco teórico Zabbix
- Instalación y configuración de Zabbix
- Zabbix con agente y con SNMP
- Host, items, graficas, triggers, actions, maps, user parameters, remote commands en Zabbix.
- Implementar en Zabbix el plan de monitoreo
    - Debe incluir valores tomados por agente y por SNMP
    - Al menos un user parameter
    - Al menos un remote command cuando se dispare un determinado trigger

Firewall

- Marco teórico, ¿Qué es?
- Reglas

- IPTables
- Firewall del router
- Probar alguna regla usando IPTables en algún servidor (NO EN EL ROUTER). Por ejemplo bloquear el acceso por SSH local.

DNS

- Marco teórico
- BIND9
- DNS primario y secundario
    - Instalación, configuración y verificación del funcionamiento
- Glue record

DHCP

- Marco teórico
- ISC-DCHP-Server/Kea
- Instalación, configuración y verificación del funcionamiento

Acceso remoto y control de acceso

- SSH y fail2ban, marco teórico
- Acceso por SSH mediante clave pública-privada
- Política de seguridad con fail2ban
- Instalación, configuración y verificación del funcionamiento de fail2ban

Logs

- Sistema de logs en Linux, marco teórico
- Herramientas para el manejo de logs
    - Logrotate
    - Logwatch
    - Rsyslog
- Marco teórico, instalación, configuración y verificación del funcionamiento de los sistemas mencionados
- Centralizar logs

Servidor Web

- Apache
    - Marco teórico
    - Instalación, configuración y verificación del funcionamiento
    - Virtual Hosts
- LetsEncrypt
    - Marco teórico
    - Instalación, configuración y verificación del funcionamiento
    - Instalar certificado en todos los sitios (interfaz web de los sistemas)
- CMS
    - Marco teórico
    - Drupal, WordPress, etc (elegir uno).
    - Instalación, configuración y verificación del funcionamiento

Aplicaciones Web

- Tomcat
    - Marco teórico
    - Instalación, configuración y verificación del funcionamiento
    - Despliegue de aplicaciones Java
- Base de datos
    - Marco teórico
    - Instalación, configuración y verificación del funcionamiento
    - Conexión con la aplicación
    - Consultas básicas
- Puestas en producción

Correo electrónico

- Marco teórico
    - Servidor de correo
    - Políticas de seguridad (dmark, dkim, spf)
    - Amavis, clamav
- Instalación, configuración y verificación del funcionamiento

Automatización

- Ansible
    - Marco teórico, instalación, configuración y verificación del funcionamiento
- Se deben configurar playbooks que automaticen la instalación de servicios, cambios de configuración, etc
- Se pueden configurar playbooks que cumplan otras funciones que el grupo considere de interés (respaldos, restauraciones. recolección de información, etc).

Respaldos y almacenamiento en la nube

- Política de respaldo: que, como cuando y donde se va a respaldar.
- Implementación de la política de respaldo
    - Scripts propios
    - BackUP PC (Instalación, configuración y verificación del funcionamiento)
    - Otros mecanismos
- Restauración de los respaldos
- Nextcloud (Instalación, configuración y verificación del funcionamiento)

LDAP

- Marco teórico
    - Estructura, OU, CN, DN, etc
- Formato LDIF
- OpenLDAP (Instalación, configuración y verificación del funcionamiento)
- Administración de OpenLDAP
    - Mediante la terminal
    - Mediante gestores (Apache Directory Studio, phpLDAPadmin, etc)
- Autenticar sistemas contra el LDAP, por ejemplo el Nextcloud
- Autenticar el acceso a puestos de trabajo contra el LDAP, por ejemplo un equipo con Ubuntu.

VPN

- Marco teórico
- OpenVPN (Instalación, configuración y verificación del funcionamiento)
- Conectarse a la red interna desde fuera mediante la VPN configurada

VoIP (Opcional 1)

- Marco teórico
- Protocolos (SIP, H.323, etc)
- Estudio de soluciones disponibles en el mercado (libres y privativas)
- Plan de numeración
- Instalación y configuración de la PBX (Se recomienda usar Asterix)
- Creación de internos, IVR, políticas de llamadas, buzón de voz, cola de espera
- Configuración de internos en teléfonos físicos y softphones
- Troncal entre dos PBXs
- Se recomienda hacer esta parte en equipos locales (notebooks, virtualbox, etc)

Proxy (Opcional 2)

- Marco teórico
- Política de seguridad del proxy
    - Bloqueo de sitios y contenido
    - Permisos por usuarios y grupos
    - Autenticación contra el LDAP
- Squid (Instalación, configuración y verificación del funcionamiento)

WAF (Opcional 3)

- Marco teórico
    - Tipos, formas de implementación
- Ataques en capa de aplicación
    - Descripción de los más importantes y comunes
    - Como un WAF protege contra ellos
    - OWASP Top 10
- Estudio de soluciones disponibles en el mercado (libres y privativas)
- Instalación, configuración de alguna solución OpenSource (por ejemplo modSecurity)
- Aparte del WAF y el firewall, ¿que otros sistemas existen para proteger nuestro sistema? (por ejemplo sistema de prevención de intrusos [IPS], firewall de última generación [NGFW], etc)