# Taller de administración de redes y servicios de comunicaciones

## Proyecto edición 2024

### 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.

### Descripción

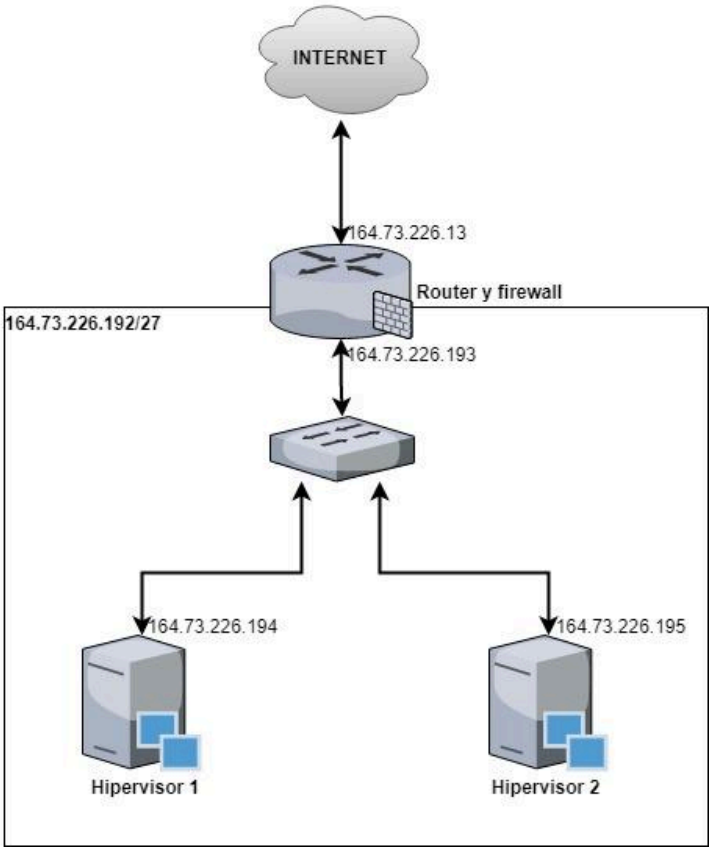
La infraestructura a disposición consta de un router con OpenWRT y dos equipos destinados a servidores, en estos servidores se virtualizarán el resto de los equipos donde se implementarán los servicios. La virtualización se hará utilizando la herramienta Proxmox.

La red disponible para el proyecto es la 164.73.226.192/27

El dominio a utilizar será un subdominio de cure.edu.uy que será elegido por los estudiantes (nombre de la “empresa” o del grupo), por ejemplo tadmin.cure.edu.uy.

Los datos necesarios para ingresar a los mismos se darán en clase, se recomienda guardarlos bien para evitar futuros inconvenientes y atrasos.

En la siguiente figura se puede ver un diagrama con la arquitectura fìsica de la red y la IP asignada a cada interfaz.




## Servicios a implementar

Para la aprobación del proyecto deben estar implementados en su totalidad (instalados, configurados, documentados y funcionando) los siguientes servicios:

- Instalación de servidores
- Firewall
- Acceso remoto y control de acceso
- Manejo de logs
- DHCP
- DNS (primario y secundario)
- Monitoreo
- Servidor Web (HTTPS), CMS
- Automatización de procesos
- Respaldos
- Correo electrónico, políticas y seguridad
- Almacenamiento en la nube
- LDAP
- VPN
- Servicio opcional entre VoIP, WAF o Proxy

El grupo puede proponer la implementación de algún otro servicio de red que le interese y quiera probar.

**Además se debe incluir la documentación de los temas administrativos de la red, como planillas de instalación, descripción de políticas, etc.**

## 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 siguientes temas:

- Firewall
- Acceso remoto y control de acceso (fail2ban)
- DHCP
- DNS
- Monitoreo
- Servidor Web (HTTPS)
- Servidor Web y CMS
- Automatización y Ansible
- Servidor de correo, políticas y seguridad
- Respaldos

y una entrega final que cubre la totalidad de los temas. En cada entrega se tendrá una instancia de defensa donde cada grupo presentará las tareas y el trabajo realizado, luego se harán preguntas grupales e individuales que pueden incluir consultas concretas sobre algún

servicio o la presentación de algún escenario que el estudiante deberá resolver (por ejemplo, caída de un servicio, cambio de configuración, etc).

IMPORTANTE: La evaluación es acumulativa, algo que se vio o preguntó para la entrega intermedia puede ser retomado en la entrega final.

IMPORTANTE: Cualquier tema se le puede preguntar a cualquier estudiante, por lo que todos deben estar al tanto del trabajo de todos.

IMPORTANTE: Durante la defensa, en caso de que se solicite un cambio de configuración o alguna otra tarea práctica el estudiante podrá contar con la documentación generada y bibliografía publicada en el EVA, por lo que se recomienda tener la documentación prolija y completa.

## Recomendaciones

- Documentar a medida que se va avanzando, no dejar todo para el final.
- Está perfecto dividir tareas, hacer reuniones para puestas en común y así enterarse de en qué están los demás.
- Ser prolijo para trabajar sobre los servidores, coordinarse para no sobreescribir el trabajo de los demás, tener en cuenta que algunos servicios dependen de otros.
- Tener MUCHO CUIDADO cuando se trabaje sobre el firewall o configuraciones que puedan bloquear el acceso remoto, en caso de “quedar afuera” los estudiantes deberán concurrir de forma presencial al CURE a solucionar el problema y debido a la situación de pandemia esto puede retrasar mucho el trabajo del equipo.
- Como en la vida real pueden surgir muchos imprevistos (por ejemplo que se apague un equipo,que algo se rompa, etc), tener esto en cuenta en la planificación y administración del tiempo (NO DEJAR TODO PARA ÚLTIMO MOMENTO).
- Quien administra el dominio de nivel superior y la red en la cual estamos es el departamento de sistemas del CURE (soporte-rocha@cure.edu.uy).

# ANEXO I - Metodología de las evaluaciones

## Defensa intermedia

En la defensa intermedia se evaluará lo siguiente:

1. **Documentación**: documentación generada por el grupo, la misma debe cumplir con lo solicitado en la letra (por más detalle ver ANEXO II).
2. **Presentación**: cada grupo debe presentar el trabajo realizado hasta el momento. El público objetivo de la presentación debe ser el “cliente” o la “gerencia” por lo que no se espera que se muestren archivos de configuración ni sea técnicamente muy detallada. (Máximo 10 minutos).
3. **Funcionamiento**: deben mostrar todos los sistemas instalados, configurados y funcionando, es responsabilidad del grupo encontrar la mejor forma de mostrarlo y ensayarlo previamente. Si el sistema tiene varias funciones deben mostrar todas. (Máximo 15 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 o muestra del funcionamiento.

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

Fecha y modalidad a confirmar.

## Defensa final

En la defensa finalse evaluará lo siguiente:

1. **Documentación**: documentación generada por el grupo, la misma debe cumplir con lo solicitado en la letra (por más detalle ver ANEXO II). Importante agregar las correcciones de la defensa intermedia.
2. **Presentación**: cada grupo debe presentar el trabajo realizado hasta el momento. El público objetivo de la presentación debe ser el “cliente” o la “gerencia” por lo que no se espera que se muestren archivos de configuración ni sea técnicamente muy detallada. (Máximo 12 minutos).
3. **Funcionamiento**: deben mostrar todos los sistemas instalados, configurados y funcionando, es responsabilidad del grupo encontrar la mejor forma de mostrarlo y ensayarlo previamente. Si el sistema tiene varias funciones deben mostrar todas. (Máximo 20 minutos).
4. **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 o muestra del 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 II - 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
- 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

**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

**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)