MINISTERIO DE EDUCACIÓN PÚBLICA

DIRECCIÓN DE INFORMÁTICA DE GESTIÓN

DEPARTAMENTO DE REDES Y TELECOMUNICACIONES

MANUAL DE CONFIGURACIONES DE REDES Y TELECOMUNICACIONES

CÓDIGO: DIG-DRT-MAN-02

Noviembre, 2021

TABLA DE CONTENIDOS

1 HISTORIAL DE REVISIONES

Fecha actualización	Versión	Descripción	Responsable
Febrero, 2012			Delia Calderón Quirós.
Mayo, 2012	4		Pablo Ariel Mora Segura.
Noviembre, 2021	5	Actualización general del documento considerando los lineamientos estipulados por la Contraloría General de la República en las Normas de Control Interno para el Sector Público, así como la infraestructura tecnológica que posee el MEP en la actualidad.	Ronny Rojas Vargas. German Peraza Castro. Ana Marcela Barrantes.

2 INTRODUCCIÓN

Basados en la necesidad de brindar mayor y mejores soluciones de conectividad, así como el tratar de garantizar la continuidad del servicio, se desarrolla un manual de procesos con el cual se pretende crear estándares de configuraciones y servicios, abarcando todos los posibles escenarios tecnológicos que se encuentran en los edificios centrales y oficinas descentralizadas del Ministerio de Educación, permitiendo orientar al personal de la Dirección de Informática de Gestión, en los protocolos y pasos recomendados a seguir para configurar un equipo de acceso a la red.

El objetivo del manual es brindar un conocimiento básico de la estructura de las redes existentes, y operar como una guía para la implementación de soluciones en corto tiempo, con la garantía de que éstas serán compatibles y funcionales con los procesos y aplicaciones que se ejecutan en el ministerio.

Este marco de referencia garantiza que las configuraciones de los equipos serán homogéneas, por lo que cualquier funcionario con los privilegios y conocimientos necesarios, sin importar su ubicación física, o conocimiento de la plataforma, podrá

atender solicitudes de los usuarios, y realizarlas con la menor cantidad de inconvenientes posibles.

3 DESCRIPCIÓN

La estructura del documento detalla la forma básica en la que se deben realizar las configuraciones de los diferentes equipos en la red ministerial, detallando desde una conexión *LAN*, hasta una conexión *WAN*, además muestra algunas implementaciones adicionales en la red que podrían ser requeridas para brindar conectividad a los usuarios finales.

Describe la estructura de conectividad detallada por edificio, sobre el tipo de conexión con el que se cuenta y sus usos, para que en caso de ser necesario se pueda usar como referencia para dar el soporte requerido, además para tener un panorama más claro de la red a nivel de conectividad entre edificios.

Se hace referencia al inventario de los equipos distribuidos por edificios, los cuales en su mayoría son para el acceso de usuarios y pocos de ellos en el *CORE* o conexión de núcleo de red.

La estructura de conectividad en las direcciones regionales muestra un mismo esquema de manera global, los cambios importantes son en el direccionamiento propio de cada dirección regional.

4 OBJETIVOS

4.1 Objetivo General

Desarrollar un estándar aplicado a la configuración de los diferentes equipos de comunicación con los que cuenta el ministerio, definiendo los pasos básicos para poner en operación un servicio en el menor tiempo posible y garantizar su continuidad, manteniendo a la vez el balance entre la seguridad de la red y el acceso a la información por esencial para el desarrollo de las actividades y procesos cotidianos de los usuarios.

4.2 Objetivos Específicos

- Identificar los tipos de equipo de red con los que cuenta el Ministerio de Educación en sus distintas oficinas.

- Determinar los lineamientos de seguridad que deben prevalecer en toda labor de configuración de la red con el propósito de asegurar el tráfico de información y la integridad de los datos.
- Establecer los lineamientos técnicos y de configuración que se deben seguir para la correcta implementación y configuración de los servicios de red.
- Detallar los procedimientos especiales para la implementación de configuraciones alternativas o de contingencia en caso de ser requeridas para satisfacer una necesidad especifica.
- Promover a todo el equipo de trabajo de la Sección de Redes y Telecomunicaciones el uso de este manual.
- Implementar las estandarizaciones establecidas en este manual a todos los equipos del Ministerio de Educación Púbica.
- Ampliar la cantidad de personas capaces de poder brindar una respuesta o un diagnóstico de un servicio en corto tiempo sin depender de los administradores de la red, mejorando la imagen de la dirección y ampliando la gama de servicios.

5 ALCANCE

El manual brindará la capacidad y el soporte para configurar e implementar un equipo activo en la red mediante una ejecución básica y oportuna, capaz de operar, ya sea por requerimiento de una nueva instalación o bien como contingencia en caso de fallas del equipo actual; permitiendo un mejoramiento en la continuidad de los servicios brindados por la sección.

6 DEFINICIONES Y ABREVIATURAS:

6.1 Abreviaturas:

ADSL: *Línea de Suscripción Digital Asimétrica*.

AP*:* Punto de acceso Inalámbrico.

DHCP: Dynamic Host Configuration Protocol.

DNS: Sistema de Dominio de Nombres (Domain Name System).

DMZ: Una zona desmilitarizada (**demilitarized zone**) o red perimetral.

DRE: Direcciones Regionales de Educación.

ICE: Instituto Costarricense de Electricidad.

IPS: Sistema de prevención de intrusos.

ISP: Proveedor de Servicios de Internet (ICE / RACSA).

LDAP: El protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol).

Mbps: Megabits por segundo.

RACSA: Radiográfica Costarricense S.A.

VPN: Redes Privadas Virtuales.

6.2 Definiciones:

Access Point: Son dispositivos que se encargan de realizar conexiones de tipo inalámbrico entre las computadoras y la red ministerial realizando filtros de conectividad entre los usuarios admitidos y los externos que no deben tener acceso a la red.

Active Directory: *(AD)* es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo.

Concentrador de VPN: Son equipos que soportan las conexiones entrantes de otros dispositivos levantando canales seguros y directos para la transmisión de la información, los cuales manejan mecanismos de encriptación y seguridad que brindan una alta confiabilidad.

Controlador de dominio: Es un servidor que ejecuta el sistema operativo *Windows* Server en el que un administrador ha implementado los servicios de dominio Active Directory.

Core: Un núcleo de procesador (o simplemente "núcleo").

Download: Descarga se utiliza frecuentemente para la obtención de contenido a través de una conexión a Internet, donde un servidor remoto recibe los datos que son accedidos por los clientes a través de aplicaciones específicas, tales como navegadores.

Enclousure: Cápsula**.**

Endpoint: Es un dispositivo informático remoto que se comunica con una red a la que está conectado.

Firewalls: Conocidos como muros de fuego, son dispositivos encargados de la seguridad estos realizan un cierre de puertos para evitar posibles ataques externos hacia la red interna, los *firewalls* se pueden encontrar tanto a nivel de *hardware* como de *software*, estos últimos son los que se instalan en los equipos de los usuarios finales para mejorar la seguridad.

Hotfixes: Revisión, parche rápido o parche en caliente (por su acepción original), es un único paquete que incluye información —normalmente en forma de uno o más ficheros— que es utilizado para solucionar un problema en una pieza de *software*.

IEEE: El Instituto de Ingenieros Eléctricos y Electrónicos, es la sociedad técnico-profesional más grande y prestigiosa del mundo, dedicada a promover y divulgar los avances científicos en las áreas de Ingeniería Eléctrica, Electrónica, Energética, Informática y afines.

IPS: Son equipos con la capacidad de los *firewall* pero cuentan con la capacidad integrada de realizar análisis del trafico entrante y saliente para bloquear los posibles ataques o infecciones a los equipos que integran la red, además cuentan con una capacidad de realizar un filtro de páginas web para asegurar el uso adecuado de los recursos**.**

IPSec: Seguridad del protocolo de Internet, es un marco normalizado para asegurar las comunicaciones de IP mediante el cifrado y autenticación de cada paquete IP en un flujo de datos.

LAN: Una red de área local, es un grupo de computadoras y dispositivos periféricos que comparten una línea de comunicaciones común o un enlace inalámbrico a un servidor dentro de un área geográfica específica.

Logs: Registro, es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático.

MPLS: Son las siglas de *Multiprotocol Label Switching* (conmutación de etiquetas multiprotocolo), una técnica que unifica la transferencia de diferentes tipos de datos a través de una misma red, para superar las limitaciones de velocidad y mejorar el flujo de trabajo de Internet.

OSI: *Open System Interconnection* (Modelo de interconexión de sistemas abiertos), que es la propuesta que hizo la Organización Internacional para la Estandarización (ISO) para estandarizar la interconexión de sistemas abiertos.

Rack: Estructura metálica o soporte cuya misión es alojar sistemas informáticos y redes de telecomunicaciones.

Routers: Dispositivos que se encargan de interconectar y dar acceso a los equipos que conforma la red interna hacia los diferentes edificios, además de ser los encargados de redirigir el trafico entrante y saliente de las aplicaciones y del acceso a internet.

Servidor Blade: Es un equipo autónomo y compacto que consta de un bastidor de servidores (conocido como chasis), el cual, alberga numerosas placas de circuitos delgadas y modulares.

Open Source: Código abierto.

Switch: Equipo de comunicación que permite la interconexión entre las computadoras de usuario final y los servidores de aplicaciones, enlaces de comunicación y acceso a internet; este equipo cuenta con la capacidad de realizar una segmentación del tráfico para mejorar el rendimiento de las aplicaciones.

Update: Proviene de la lengua inglesa que significa "actualizar", "modernizar". El término *update* está profundamente relacionado con la tecnología, ya que el mismo se utilizar para actualizar *softwares*, sistemas operativos, programas de computación, juegos, entre otros.

Vlan´s: Acrónimo de virtual *LAN* (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

Virtualizar: El concepto de virtualización hace referencia a una tecnología que permite la ejecución de varias máquinas virtuales sobre una máquina física con el objetivo de aprovechar al máximo los recursos de un sistema y que su rendimiento sea mayor.

VMware: Es un sistema de virtualización por *software* que proporciona un ambiente de simulación de la ejecución de varios ordenadores dentro de otro de manera simultánea.

WEB: Conjunto de información que se encuentra en una dirección determinada de internet.

7 AUTORES:

MT. César Morera Madrigal, Jefe de la Sección de Redes y Telecomunicaciones.

8 ACTUALIZADO POR:

German Peraza Castro, Departamento de Redes y Telecomunicaciones.

Ronny Rojas Vargas, Departamento de Redes y Telecomunicaciones.

Ana Marcela Barrantes Arias, Departamento de Gestión y Control Informático.

9 DIRECTRICES

Este manual no debe ser de conocimiento público dado que incorpora información complementaria y fundamental sobre la estructura y seguridad de la red del Ministerio de Educación Pública.

Todo equipo de red que sea instalado en las oficinas del Ministerio de Educación Pública, debe ser configurado con base en los lineamientos establecidos en este manual, para asegurar que cualquier funcionario de la sección pueda interpretar la configuración del equipo.

10 TIPOS DE EQUIPOS QUE CONFORMAN LA RED MINISTERIAL

La red del ministerio se encuentra conformada por una serie de dispositivos de telecomunicaciones (equipos activos de red) que se encargan de realizar la conectividad, tanto entre los diferentes edificios arrendados como también, el servicio que le brinda la conexión al usuario final que usa los servicios.

Entre la lista de equipos podemos encontrar:

- *Switches,*
- *Router* (enrutadores),
- *Firewalls* (muros de fuego),
- Concentradores de *VPN,*
- Servidores,
- *IPS* (Sistemas de prevención de intrusos),
- *Access Point* (equipo de acceso inalámbrico).

Nota: El *Firewall* y el *IPS* están en un mismo equipo ya que son nueva generación. (*Next Generation Firewall*).

Todos con la finalidad de dar un servicio ágil y seguro a los funcionarios del Ministerio de Educación.

11 INVENTARIO DE EQUIPOS QUE COMPONEN LA RED

A continuación, se detalla el inventario de equipos de telecomunicaciones existente por sitio:

11.1 Antigua Embajada Americana

En este edificio se concentran la mayor parte de los servicios, en cuanto a la estructura de telecomunicaciones de la red ministerial por la arquitectura de este edificio.

La red en este edificio está compuesta por:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	Aruba	6200F	12	Funcionan como equipos de acceso y distribución de la red.
Switch	HP	7503	1	Conforma el *CORE* de la red recibiendo las conexiones entrantes de los equipos de acceso así como de los servidores que se encuentran en el sitio. Es un equipo modular.
IPS / Firewall	Check Point	6600	2	Se encargan de la gestión e interconexión de los *VPN* con las direcciones regionales en un enlace de 100 Mbps con el ICE, además se encarga de brindar la conexión a internet manejando el filtrado de contenidos web y los bloqueos de posibles ataques en la red y la *DMZ*. Estos dos equipos están configurados en alta disponibilidad (HA).
Router	HP	3024	2	Se utilizan para los enlaces de Internet de los que hace uso el sitio *WEB* (ICE) y *DMZ* (RACSA). Cada equipo es independiente.
Router	Aruba	7030	1	Soportan los enlaces *MPLS* entre los edificios Torre Mercedes, Raventós, Antiguo CENADI, BCT, Uruca, Porfirio Brenes y IDC Guatuso (Data Center ICE), este servicio es de 60Mbps.
Router	HP	3024	1	Se encarga de comunicar contra todas las DRE que tenga el servicio *MPLS* para uso de los sistemas internos del MEP y servicios externos como los de Integra.
Router	HP	3024	1	Se encarga de comunicar contra el Tribunal Supremo de Elecciones (TSE) para consultas del padrón con respecto a uso de los sistemas MEP.
Router	Aruba	7030	1	Se encarga de establecer las comunicaciones contra el Ministerio de Hacienda para el servicio de Integra *WEB*. Posee dos enlaces, uno con el ICE de 30Mbps y otro con RACSA de 10*Mbps* como *backup*.

Access Point	Cisco	Aeronet 1242G	7	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Servidor	HP	DL380	1	Servidor encargado de los respaldos mediante DataProtector.
Enclousure	HP	C7000	1	Se encarga de la administración de los servidores tipo *blade*.
Enclousure	HP	*Sinergy*	1	Se encarga de la administración de los servidores tipo Sinergy.
BLADES	HPE	BL460c G9	2	Servidores encargados de virtualizar los servidores que corren sobre a *DMZ* del Ministerio.
BLADES	HPE	*Sinergy* 480 G10	7	Servidores encargados de virtualizar los servidores que corren los sistemas en producción del Ministerio.

11.2 Edificio Torre Mercedes

En la estructura de conexión de este edificio el cual concentra los servicios más importantes en la atención del público, se cuenta con una forma de interconexión basada en líneas principales y de respaldo en la siguiente estructura:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	Aruba	6200F	11	*Switches* de acceso que son los que brindan el soporte de conexión a los usuarios finales.
Switch	3COM	4210	3	*Switches* de acceso que son los que brindan el soporte de conexión a los usuarios finales
Switch	HPE	3810M	1	*Switches* de acceso que son los que brindan el soporte de conexión a los usuarios finales
Switch	HPE	5510	1	*Switches* de acceso que son los que brindan el soporte de conexión a los usuarios finales.
Switch	Aruba	2530	1	*Switches* de acceso que son los que brindan el soporte de conexión a los usuarios finales.
Switch	Aruba	6300M	2	Se encargan de realizar la comunicación entre los pisos del edificio soportando la carga de tráfico que es obtenida de

				los 11 *Switches* de acceso. Los *switches* de *CORE* se encargan adicionalmente de dar la interconexión a los servidores que se encuentran en el piso 5 del edificio operando a velocidades de 1 *Gbps* entre el servidor y el equipo de acceso al usuario final.
IPS / Firewall	*Check Point*	6600	1	Se encarga de soportar la carga del tráfico de internet, realizando filtrado de contenido *web* así como *VPN* secundario para las DRE por si falla la Antigua Embajada. Este equipo soporta un enlace en fibra de 40*Mbps* hacia internet para todo el edificio.
Router	Aruba	9012	1	Se encargan de realizar el enrutamiento entre los edificios. Tiene un enlace *MPLS* del ICE en Fibra óptica en 30 Mbps.
Router	HP	3024	1	Se utiliza para recibir el enlace de Internet de los que hace uso el edificio.
Access Point	Cisco	Aeronet 1242G	9	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Servidor	HPE	BL460c G9	2	Servidores que soportan los ambientes de desarrollo, pruebas y contingencia para los departamentos de la DIG.

11.3 Edificio CENADI

La plataforma de comunicaciones del edificio del antiguo CENADI se encuentra distribuida la siguiente manera:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	Aruba	6200F	17	Distribuidos entre el *RACK* principal y los cuartos de telecomunicaciones, para dar conexiones a los usuarios así como una conectividad a internet.
Switch	Aruba	6300M	2	Con funcionalidad en capa 3 (modelo *OSI*) como *CORE* de la red *LAN*.
Router	Aruba	9012	1	Realiza el enrutamiento en el enlace *MPLS* del ICE en Fibra óptica en 10 *Mbps* contra todos los edificios. Es *router LAN*.

IPS / Firewall	*Check Point*	6200B	1	Soporta el tráfico entrante y saliente para internet sobre el servicio de Internet limitado por regla de firewall dado que tiene que compartir servicios con el IDP. Se encarga de administrar la *DMZ* del portal de educatico.
Router	Aruba	9012	1	Recibe el enlace de Internet puro de 60*Mbps* y da soporte al IDP para las videos conferencias.
Access Point	Cisco	Aeronet 1242G	4	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Servidor	HP	ML380c	1	Servidor encargado de virtualizar roles de Antivirus, Directorio Activo, Distribuidor de Actualizaciones e Impresiones.

Nota: Se cuenta con un enlace de 4 *Mbps* en *HDSL* para los servicios del IDP del Instituto Uladislao Gámez.

11.4 Edificio Raventós

En el edificio Raventós se encuentra la siguiente distribución de equipos:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	Aruba	6200F	24	Distribuidos entre los 7 pisos para el acceso de usuarios.
Switch	Aruba	6300M	2	Es el *CORE* del edificio e interconecta cada piso.
Router	Aruba	9012	1	Es el *router LAN* y tiene un enlace *MPLS* del ICE en Fibra óptica en 30 *Mbps* contra todos los edificios.
IPS / Firewall	*Check Point*	6200B	1	Para el acceso a internet, cuenta con enlace de 40 *Mbps* en fibra con el ICE.
Router	HP	3044	1	Se utiliza para recibir el enlace de Internet de los que hace uso el edificio.
Access Point	Cisco	Aeronet 1242G	18	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Servidor	HP	ML380c	1	Servidor encargado de virtualizar roles de Antivirus,

				Directorio Activo, Distribuidor de Actualizaciones e Impresiones.

11.5 Antigua Escuela Porfirio Brenes

La red de la Antigua Escuela Porfirio Brenes tiene una estructura sencilla donde se encuentran:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	Aruba	6200F	14	Dan conexión de acceso a los usuarios.
Switch	Aruba	6300M	2	*CORE* de la red *LAN* del edificio.
Router	Aruba	9012	1	Es el *router LAN*, tiene un enlace *MPLS* del ICE en fibra óptica en 30 *Mbps* contra todos los edificios.
IPS / Firewall	*Check Point*	6200B	1	Soporta un servicio de Internet en fibra óptica con el ICE de 20 *Mbps*.
Access Point	Cisco	Aeronet 1242G	2	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Servidor	HP	ML380c	1	Servidor encargado de virtualizar roles de Antivirus, Directorio Activo, Distribuidor de Actualizaciones e Impresiones.

11.6 Edificio BCT

Su infraestructura de telecomunicaciones está compuesta por:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	Aruba	6200F	9	Dan conexión de acceso a los usuarios.
Switch	Aruba	6300M	2	*CORE* de la red *LAN* del edificio.
Router	Aruba	9012	1	Es el *router LAN*, tiene un enlace *MPLS* del ICE en fibra

				óptica en 40 *Mbps* contra todos los edificios.
Router	Aruba	9012	1	Se encarga de establecer las comunicaciones contra el Ministerio de Hacienda para el servicio de Integra *WEB*. Se usa como enlace secundario si falla el de Antigua Embajada. Tiene una velocidad de 10*Mbps*.
IPS / Firewall	*Check Point*	1590	1	Soporta un servicio de Internet en fibra óptica con el ICE de 30 *Mbps*.
Access Point	Cisco	Aeronet 1242G	5	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Servidor	HP	ML380c	1	Servidor encargado de virtualizar roles de Antivirus, Directorio Activo, Distribuidor de Actualizaciones e Impresiones.

11.7 Edificio Uruca

Su infraestructura de telecomunicaciones está compuesta por:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	HP	2530	5	Dan conexión de acceso a los usuarios, según la cantidad de estos por regional.
Access Point	Cisco	Aeronet 1242G	1	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Router	Aruba	9012	1	Es el *router LAN*, tiene un enlace *MPLS* del ICE en fibra óptica en 10 *Mbps* contra la Antigua Embajada para uso de los sistemas MEP.
IPS / Firewall	*Check Point*	1590	1	Se encarga de la seguridad perimetral además de realizar un filtrado de contenido web para la protección de los usuarios. Recibe el enlace de Internet.
UPS	-	-	1	Respaldado eléctrico para garantizar la continuidad del servicio y así como la protección adecuada de los equipos.

11.8 Direcciones Regionales

Para cada dirección regional se ha implementado una plataforma estandarizada compuesta por los siguientes elementos:

Tipo de equipo	Marca	Modelo	Cantidad	Descripción
Switch	HP	2530	5	Dan conexión de acceso a los usuarios, según la cantidad de estos por regional.
Access Point	Cisco	Aeronet 1242G	1	Ofrecen mayor movilidad y aumentar la cobertura en cada sitio y según la cantidad de estos en el edificio. Son de conexión en 54*Mbps*. *IEEE* 802.11 a/b/g.
Router	HP	3012	1	Es el *router LAN*, tiene un enlace *MPLS* del ICE en fibra óptica en 2 *Mbps* contra la Antigua Embajada para uso de los sistemas MEP.
IPS / Firewall	*Check Point*	1590	1	Se encarga de la seguridad perimetral además de realizar un filtrado de contenido *web* para la protección de los usuarios, así como de establecer el *VPN* entre la dirección regional y las oficinas centrales (Antigua Embajada como primario y Torre Mercedes como respaldo de contingencia). Recibe el enlace de Internet.
UPS	-	-	1	Respaldado eléctrico para garantizar la continuidad del servicio y así como la protección adecuada de los equipos.
Workstation	HP	Workstation Z440	1	Servidor encargado de virtualizar roles de Antivirus, Directorio Activo e Impresoras.

12 DIRECTRICES Y ROLES DE RED

Se procede a describir las indicaciones existentes para la red institucional, así como los roles que desempeñan los principales equipos en esta.

12.1 Seguridad

Existen niveles de seguridad tanto físicos como lógicos.

La seguridad física incluye la aplicación de barreras físicas y procedimientos de control como medidas preventivas en caso de que la información confidencial se vea amenazada. Implementar mecanismos de control y seguridad del sistema informático y dispositivos de acceso remoto para proteger el *hardware* y los dispositivos de almacenamiento de datos. Este tipo de seguridad se centra en cubrir las amenazas provocadas por los seres humanos y la naturaleza del entorno físico en el que se encuentra el sistema.

Para la seguridad física se tienen establecidos controles de acceso mediante llave magnética en los centros de datos principales (Antigua Embajada, Torre Mercedes, Porfirio Brenes, Raventós y CENADI).

Además se cuenta con cámaras de seguridad dentro de los centros de datos de Antigua Embajada y Torre Mercedes, que garantizan la certeza del personal que ingresa a la ubicación física de los equipos de comunicación y servidores que brindan los servicios al Ministerio.

La seguridad lógica se refiere a controles específicos establecidos para gestionar el acceso a los sistemas informáticos y espacios físicos en los centros de datos. El uso de puertas cerradas para proteger la entrada a la sala de servidores del centro de datos puede ser la mejor práctica de seguridad física, pero tener que participar en la autenticación de dos factores para abrir la puerta es una forma lógica de seguridad. Este método de seguridad del centro de datos también se extiende a los sistemas informáticos. Las contraseñas y los perfiles de usuario son métodos comunes para restringir el acceso, lo que garantiza que solo el personal autorizado pueda acceder a sistemas críticos como los servidores.

La seguridad lógica ayuda a proteger contra amenazas llamadas ciberataques, pero también puede proteger los centros de datos de sí mismos. Ya sea por negligencia o mala intención, el error humano es una de las causas más comunes de tiempo de inactividad y otras desgracias de TI. Al implementar protocolos de seguridad lógicos y actualizar constantemente las listas de acceso de los usuarios, el Ministerio puede garantizar que nadie pueda acceder a sus valiosos datos sin autorización.

Los funcionarios autorizados están basados según el rol que desempeñan dentro de cada uno de sus departamentos. A nivel de dominio existe el usuario administrador de dominio que tiene todos los permisos sobre la totalidad de servidores dentro del dominio, las credenciales de este usuario están custodiadas en la caja fuerte de la Dirección de Informática.

Para los equipos de comunicaciones existen contraseñas complejas de seguridad para ingresar a los distintos módulos de acceso que permiten estos equipos. Esta contraseña es administrada por los compañeros encargados según su rol de mantener en correcto funcionamiento las comunicaciones del Ministerio de Educación.

Para el acceso lógico a servidores se cuenta con una contraseña de Administrador Local administrada por los compañeros encargados según su rol, de mantener en correcto funcionamiento los servidores.

Las contraseñase para el acceso a servidores de Base de Datos y Sistemas de Información están gestionadas por el personal de los departamentos descritos.

12.2 Controladores de Dominio

Existen dos controladores de dominio principal (*DC* por sus siglas en ingles de *Domain Controler*) ubicado en el Centro de Computo del Edificio de la Antigua Embajada.

En los otros edificios del centro de San José existe al menos un controlador de dominio secundario. Los 2 principales objetivos de estos controladores de dominio secundarios son:

- Mantener un sistema distribuido de la Base de Datos de usuarios del dominio (*Active Directory*), previniendo una posible falla del equipo principal, esto permite mantener respaldos de la base de datos de usuarios del dominio.
- Garantizar que los usuarios de red en cada uno de esos edificios obtengan los servicios de red y validación a nivel local disminuyendo el consumo de ancho de banda de los enlaces de comunicación.

Para cada uno de los edificios de oficinas centrales como en las direcciones regionales, se cuenta con un servidor *DHCP*, que se encarga de asignar las direcciones *IP* a las computadoras de los usuarios.

Como parte de los procesos del Departamento de Redes y Telecomunicaciones es garantizar el correcto funcionamiento de toda la infraestructura como servicio que conlleva tanto equipo de comunicación, seguridad y servidores.

Para los servidores se cuenta con una tarea mensual según recomendación del fabricante, de aplicar actualizaciones a los Sistemas Operativos para garantizar un correcto funcionamiento, y bloquear cualquier falla de seguridad. Con respecto al antivirus está instalado en todos los servidores y mediante su consola de administración centralizada, se garantiza que los servidores siempre contarán con la última distribución de vacuna, para evitar infecciones cibernéticas.

13 EQUIPOS DE COMUNICACIONES (ROUTER Y FIREWALL)

Se describen los roles e información básicas de los principales equipos de comunicaciones. Esta descripción se hará por edificio y será para los edificios Antigua Embajada Americana, BCT, Raventós, Torre Mercedes, CENADI y Bodegas

de Proveeduría en la Uruca. En el resto de edificios los equipos de comunicación son administrados por los encargados de redes, por lo que ellos tienen el conocimiento de cómo están configurados los mismos.

13.1 Edificio Antigua Embajada Americana

Línea	Tipo	BW	Descripción
Internet/ *VPN* Regionales	*MPLS* Fibra	100 *Mbps*	Este servicio se conecta al distribuidor de Fibra del ICE se utiliza para habilitar internet a los usuarios de ese edificio. Cualquier otra dirección *IP* está bloqueada en este *firewall* y este además se encarga de gestionar el uso de servicio de Internet. Adicionalmente por este servicio se brinda la conexión por *VPN* Internet para las direcciones regionales dado su ancho de banda y su estabilidad para la transmisión de datos.
***MPLS* Edificios Centrales**	MPLS Fibra	60 *Mbps*	Este servicio funciona como concentrador de todos los enlaces de Fibra de los Edificios Torre Mercedes, Raventós, Porfirio Brenes, BCT, CENADI, y las Bodegas de proveeduría en la Uruca, el cual opera por medio de la tecnología *MPLS* para la transmisión de datos.
DMZ	Internet Fibra	70 *Mbps*	El *Router* solamente está configurado con una ruta default a Internet. Este enlace se utiliza para brindar los servicios del sitio web ministerial.

13.2 Edificio BCT

Línea	Tipo	BW	Descripción
Internet	Fibra	30 *Mbps*	Servicio de Internet para la navegación de los usuarios.
***MPLS* Edificios Centrales**	*MPLS* Fibra	40 *Mbps*	Enlace principal de datos para uso de los sistemas MEP.

13.3 Bodega de Proveeduría (Uruca)

Línea	Tipo	BW	Descripción
Internet Usuarios	Fibra	10 *Mbps*	Servicio de Internet para la navegación de los usuarios.

MPLS **Edificios Centrales**	*MPLS* Fibra	10 *Mbps*	Enlace principal de datos para uso de los sistemas MEP.

13.4 Edificio Porfirio Brenes

Línea	Tipo	BW	Descripción
Internet	Fibra	20 *Mbps*	Servicio de Internet para la navegación de los usuarios.
MPLS Edificios Centrales	*MPLS* Fibra.	30 *Mbps*	Enlace principal de datos para uso de los sistemas MEP.

13.5 Edificio Raventós

Línea	Tipo	BW	Descripción
Internet	Fibra	40 *Mbps*	Servicio de Internet para la navegación de los usuarios.
MPLS **Edificios Centrales**	*MPLS* Fibra.	30 *Mbps*	Enlace principal de datos para uso de los sistemas MEP.

13.6 Edificio Torre Mercedes

Línea	Tipo	BW	Descripción
Internet	Fibra	40 *Mbps*	Servicio de Internet para la navegación de los usuarios.
MPLS **Edificios Centrales**	*MPLS* Fibra.	30 *Mbps*	Enlace principal de datos para uso de los sistemas MEP.

13.7 CENADI

Línea	Tipo	BW	Descripción
Internet / Videoconferencias	Fibra	60 Mbps	Enlace de Internet destinado para la los servicios de videoconferencia del Instituto Uladislao Gámez y la navegación de los usuarios del edificio.
***MPLS* Edificios Centrales**	*MPLS* Fibra	10 *Mbps*	Enlace principal de datos entre la CENADI y la Antigua Embajada para el tráfico de datos y servicios entre ambos edificios.
Internet / Técnica	*ADSL*	4 *Mbps*	Enlace de Internet para las salas de reuniones de la Dirección de Educación Técnica.

Se adjunta el direccionamiento de todas las subredes gestionadas por el Departamento de Redes y Telecomunicaciones.

Edificio	Dirección o rango	Descripción
Antigua Embajada	10.10.0.X /16	Para uso en servidores.
Antigua Embajada	10.10.1.X /16	Para uso en equipos de *router*, *firewall* y el *switch* de *core*.
Antigua Embajada	192.168.15.X /24	Administración de los *switch* del edificio.
Antigua Embajada	192.168.253.X /24	Para uso en la infraestructura *blade* y *VMware*.
Antigua Embajada	192.168.252.X /24	*ILO* de los equipos en la infraestructura blade.
Antigua Embajada	10.17.X.X /16 y 10.15.X.X /16	Segmento de los usuarios MEP.
Antigua Embajada	172.16.0.X /24	Invitados o visitas MEP.

Antigua Embajada	10.73.0.X /24	Central Telefónica – Servicios Generales.
Antigua Embajada	20.20.13.X /24	*DMZ* en *LAN*.
Torre Mercedes	10.13.0.X /22	Para uso en servidores y equipos de telecomunicaciones.
Torre Mercedes	10.13.4.X /22	Segmento de los usuarios MEP.
Torre Mercedes	10.13.8.X /22	Segmento de los usuarios MEP.
Torre Mercedes	10.13.12.X /22	Segmento de los usuarios de informática.
Torre Mercedes	10.70.0.X /24	Central Telefónica – Servicios Generales.
Torre Mercedes	192.168.251.X /24	Para uso en la infraestructura *blade* y *VMware*.
Torre Mercedes	10.2.1.X /24	Administración de los *switch* del edificio.
Torre Mercedes	192.168.102.X /30	Red privada entre *router LAN* y *firewall*.
Torre Mercedes	172.16.10.X /24	Invitados o visitas MEP.
Torre Mercedes	172.16.11.X /24	Visitas - reuniones MEP.
Raventós	10.11.0.X /16	Para uso en servidores y equipos de telecomunicaciones.
Raventós	10.26.2.X /24 10.26.3.X /24	Segmento de los usuarios MEP.

	10.26.4.X /24 10.26.5.X /24 10.26.6.X /24 10.26.7.X /24	
Raventós	10.2.2.X /24	Administración de los *switch* del edificio.
Raventós	192.168.101.X /30	Red privada entre *router LAN* y *firewall*.
Raventós	10.71.0.X /24	Central Telefónica – Servicios Generales.
Raventós	172.16.60.X /24	Invitados o visitas MEP.
Raventós	172.16.61.X /24	Invitados o visitas MEP.
Porfirio Brenes	10.16.0.X /24	Para uso en servidores y equipos de telecomunicaciones.
Porfirio Brenes	10.16.2.X /24	Segmento de los usuarios MEP.
Porfirio Brenes	192.168.103.X /30	Red privada entre *router LAN* y *firewall*.
Porfirio Brenes	10.2.3.X /24	Administración de los *switch* del edificio.
Porfirio Brenes	172.16.53.X /24	Invitados o visitas MEP.
BCT	10.23.0.X /23	Para uso en servidores y equipos de telecomunicaciones.
BCT	10.23.2.X /23 10.23.4.X /23 10.23.6.X /23	Segmento de los usuarios MEP.

BCT	192.168.104.X /30	Red privada entre *router LAN* y *firewall*.
BCT	172.16.13.X /24	Invitados o visitas MEP.
BCT	10.74.0.X /24	Central Telefónica – Servicios Generales.
BCT	10.2.5.X /24	Administración de los *switch* del edificio.
CENADI	10.14.0.X /16	Para uso en servidores y equipos de telecomunicaciones.
CENADI	10.22.1.X /24 10.22.2.X /24 10.22.4.X /24 10.22.6.X /24 10.22.7.X /24	Segmento de los usuarios MEP.
CENADI	10.22.12.X /24	Laboratorio.
CENADI	172.16.9.X /24	Sala capacitación IDP.
CENADI	172.20.10.X /24	Laboratorio.
CENADI	172.16.10.X /24	Invitados o visitas MEP.
CENADI	10.72.0.X /24	Central Telefónica – Servicios Generales.
CENADI	10.14.200.X /24	Control de acceso.
CENADI	10.2.4.X /24	Administración de los *switch* del edificio.
Uruca	192.168.228.X /24	Para uso de toda la red en usuario MEP y administración de equipos de

		telecomunicaciones.

13.8 Direcciones Regionales

Se describe la información de los equipos de comunicaciones en las direcciones regionales. Es importante resaltar que este esquema aplica únicamente para las regionales que tienen alguno de los servicios de conectividad (enlaces dedicados) requeridos para establecer la conexión con la central ministerial.

La Dirección de Informática de Gestión ha hecho una serie de esfuerzos por dotar de este tipo de servicio a todas las direcciones regionales y de esta forma integrar las redes de cada regional a la red ministerial, para la instalación de los servicios de comunicaciones se depende del proveedor de servicios en el país (el ICE):

13.8.1 Firewall / IPS Regional:

Este equipo es utilizado para habilitar la conexión a Internet de la dirección regional para la navegación de los usuarios y cuenta con los filtros de contenidos *WEB* para evitar accesos a sitios no autorizados, también genera el *VPN* por Internet para conectar la red de la regional a la red ministerial como medida de contingencia cuando el *MPLS* falla en el *router*.

Tiene 3 interfaces en uso; una conecta con el *router* para bajar las comunicaciones a la *LAN*, otra conecta con los centro de formación del IDP y la otra interfaz recibe el enlace de Internet.

Para poder gestionar las interfaces se tiene que ingresar a la *IP* reservada para el equipo, esto se puede observar en la consola de gestión de la plataforma y requiere que se instale un programa propietario de la marca del equipo.

13.8.2 Router Regionales:

Este equipo es utilizado para comunicar cada DRE hacia la Antigua Embajada por el servicio *MPLS* del ICE de 2*Mbps* para dar acceso a los sistemas de información del MEP.

Funciona como *router LAN* en cada DRE.

Tiene 3 interfaces en uso; una es de conexión con el *switch* para dar servicio *LAN*, otra es de conexión *MPLS* y la otra conexión va con el *firewall*.

Los enlaces *MPLS* están configuración con túneles *IPSec* para dar encriptación al tráfico de red y estás conexiones llegan al *router* 10.10.1.16 en la Antigua Embajada,

este posee todas las configuraciones y consecutivos de red para seguir creciendo cuando surjan DRE nuevas.

Cualquier configuración que se requiera replicar en una DRE nueva se puede ingresar al *router* y copiar lo que se necesite, los *router* siempre son 192.168.X.254 en las DRE.

Se adjunta el direccionamiento de todas las subredes gestionadas por el Departamento de Redes y Telecomunicaciones.

Edificio	Dirección o rango	Descripción
DREs	192.168.192.0 /19	Cada segmento en el 3er octeto incrementa en 1 para distinguir a cada DRE, la máscara en /24 en cada dirección regional.
DRE San José Oeste	192.168.224.0 /24	
DRE San José Norte	192.168.225.0 /24	

14 PROCESOS DE ACTUALIZACIÓN DE ANTIVIRUS

El Ministerio cuenta con dos plataformas de antivirus:

La primera es de Symantec que cuenta con una consola de administración centralizada, que permite mantener al día, todos los clientes de antivirus de las computadoras de escritorio que usan los funcionarios, y los servidores que requieren una actualización diaria de las vacunas, así como un inventario del estado de estos.

La ruta y manuales de instaladores están en \\10.10.0.37\Paquetes de instalación o \\10.10.0.38\Paquetes de instalación, son redundantes.

La segunda es *Microsoft Endpoint* que está siendo utilizada exclusivamente por los servidores relacionados al *Microsoft System Center Configuration Manager (SCCM)* que es la plataforma centralizada de inventario de Sistema Operativo de todos los equipos terminales de los funcionarios. El *Microsoft Endpoint* cuenta con una plataforma centralizada de administración para calendarizar escaneos y actualizaciones a los servidores del *SCCM* en los distintos edificios del MEP.

15 PROCESO DE ACTUALIZACIÓN DE SISTEMA OPERATIVO DE LOS SERVIDORES

El Ministerio cuenta con el *software de Microsoft* llamado *Windows Server Updates Services (WSUS).*

Después del segundo martes de cada mes, el ingeniero a cargo de dicha tarea, debe ingresar a la consola del *WSUS* para realizar un procedimiento de revisión, sincronización y aprobación de las actualizaciones que requiere cada uno de los servidores que conforman la granja de servidores del Ministerio, sean estos de pruebas, desarrollo o producción.

Las actualizaciones a los servidores deben realizarse de manera manual y controlada para evitar fallas a los procesos y servicios que se ejecutan en estos.

16 HABILITAR EL BLOQUEO PARA COPIA DE ARCHIVOS DE AUDIO EN EL SERVIDOR

Para los servidores de archivos donde se ejecuta el servicio de carpetas compartidas, es requerido configurar filtros que garanticen la integridad de la información ahí contenida.

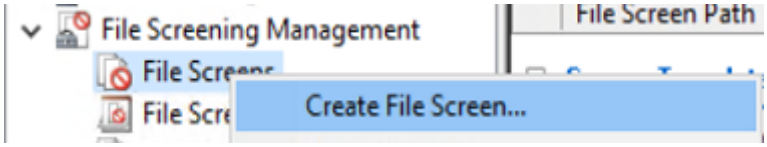
Para configurar los filtros de contenido se han predefinido 4 tipos de plantillas que deben aplicarse.

1. Filtrar todo el contenido ejecutable, imágenes, videos y audio.
2. Filtrar todo el contenido ejecutable, videos y audio.
3. Filtrar todo el contenido ejecutable.
4. Sin filtros.

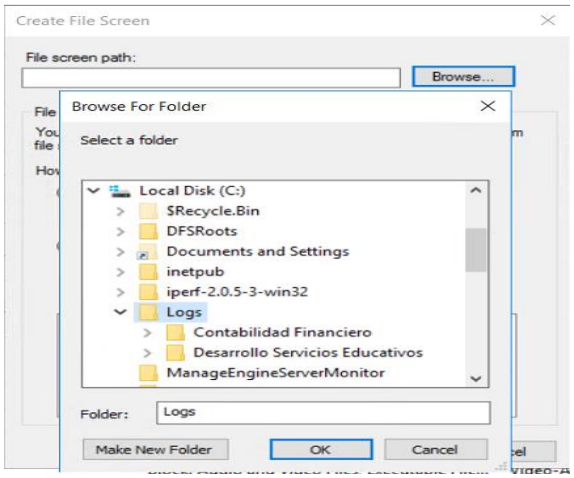
Según la funcionalidad de la carpeta que se crea, se debe aplicar una de las 4 plantillas.

Se debe ingresar al Administrador de Recursos del Servidor, y seleccionar la opción de filtros.

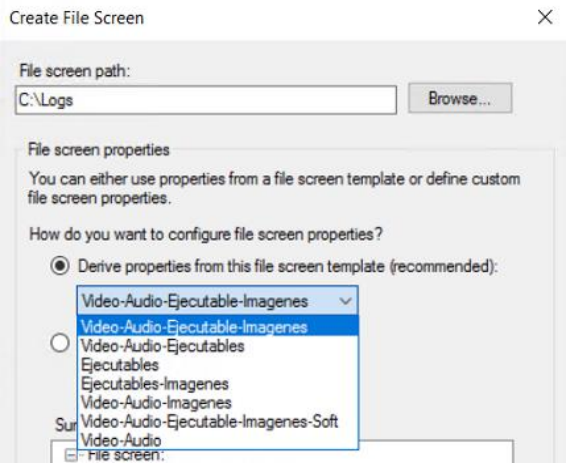
Crear un filtro de contenido.



Navegar a la ruta de la carpeta donde se aplicará el filtro y seleccionarla.



Se selección la plantilla de filtro a aplicar a la carpeta y queda aplicado el filtro según se necesite.



17 CONFIGURACIÓN DE CISCO AIRONET 1242G SERIES *ACCESS PONT*

Este procedimiento es para realizar la configuración de los *Access Point* cuando se encuentran creadas *Vlan's* que permita difundir varios *SSID*.

La configuración se puede realizar de dos maneras desde su interfaz *web* o desde su línea de comandos (CLI), en este caso se realiza por medio de la interfaz *web*.

Primeramente hay que ingresar en el navegador a la dirección del AP configurada anteriormente en el caso del MEP en el rango del edificio correspondiente, autenticándose con los usuarios previamente establecidos para la administración de estos dispositivos, en esta pantalla inicial cargara los datos de *logs*, usuarios o clientes conectados y dirección *IP* del equipo.

Creación de las *Vlan's* en el *Access Point*.

Ingresar en el menú de la izquierda en la opción de *SERVICES*, posteriormente se habilita un submenú y en este marcamos *VLAN,*

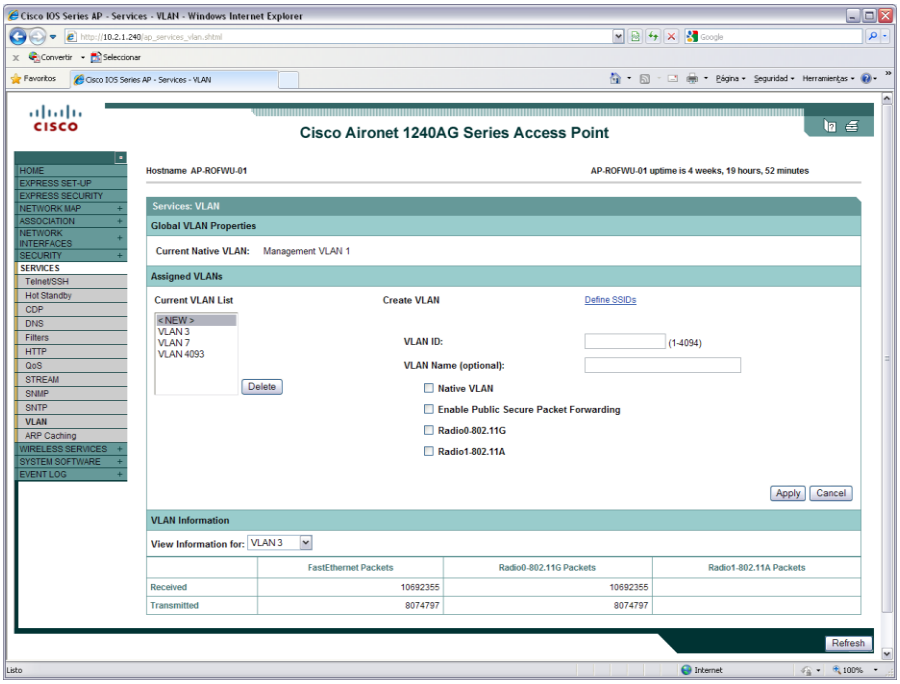


Figura 10.

Seleccione la opción de New e iniciamos con la creación de la *Vlan*,

Vlan ID (ingresamos el número de la *Vlan* definida en el *Switch* previamente),

Vlan Name (Descripción del uso de la *vlan* eje: usuarios, invitados),

Radio0-802.11G (habilitarla para que las pc con tecnología 802.11G se puedan conectar) y aplicar la configuración.

17.1 Para habilitar la autenticación por WAP

Se ingresa en *SECURITY, Encryption Manager*, en la opción Set *Encryption Mode* and *Keys for VLAN* seleccione el *ID* de la *Vlan* que vamos a modificar, posteriormente *Encryption Modes* marque *Cipher* con las opciones de *AES CCMP*.

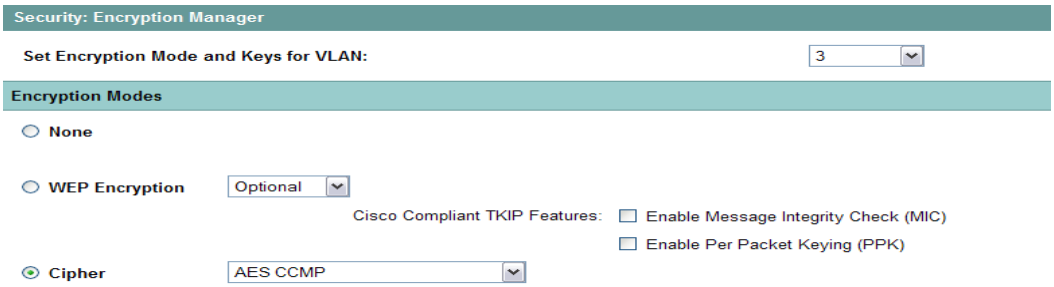


Figura 11.

Luego configure los *SSID* para ser difundidos, Ingresar en *SECURITY,* posteriormente en *SSID Manager* y marcar la opción de *NEW*.

En el *SSID* se debe poner el nombre del *SSID* que se desea mostrar en las PC y la *VLAN* a la cual van a tener acceso.

Radio0-802.11G El radio en el que se conectarán en este caso es B/G.

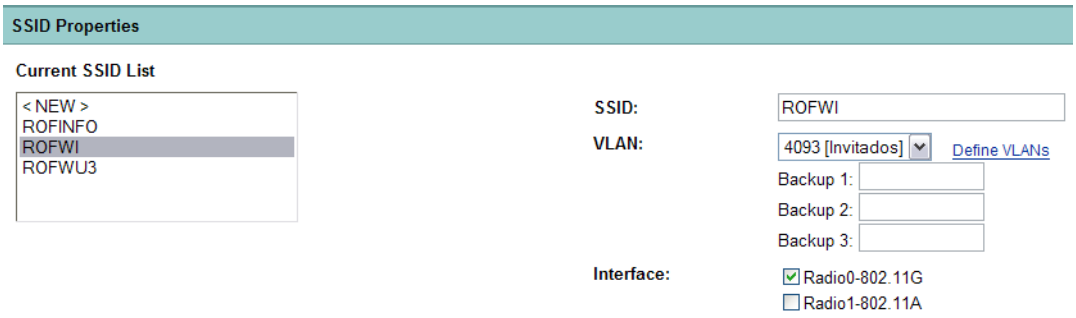


Figura12.

Para ingresar la clave con la que se autentican los usuarios se debe ingresar, para ello, hay que bajar hasta *Client Authenticated Key Management*, en la autenticación marcar *Key Management* en Mandatory y en la parte de *WAP* marcar *Enable WPA (WPA* (para invitados) / *WPAv2* (para usuarios internos)).

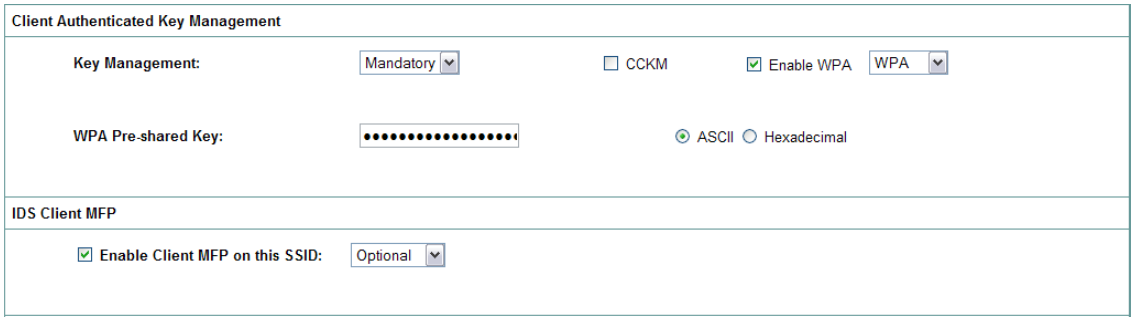


Figura 13.

Finalmente, habilitar el único *SSID* que se va a difundir y va a ser visible para los usuarios, bajando hasta la opción *Guest Mode/Infrastructure SSID Settings* y buscar el *SSID* deseado.

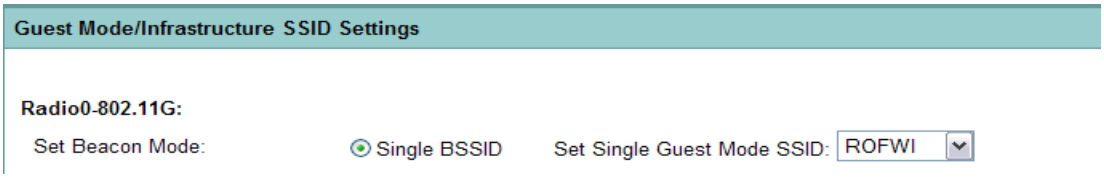


Figura 14.

Con esta configuración sólo uno de todos los *SSID* son publicados, todos se mantienen activos pero sólo a nivel de usuarios se ve el que se definió anteriormente en este caso *ROFWI.*

Nota importante: Para este caso, las *Vlan* de administración deben estar *untagged* para que no pasen etiquetados por los puertos del *switch* y se puedan administrar remotamente, y para los equipos *3com* (5500g), se debe aplicar el comando *port trunk pvid vlan* 2, sobre la interfaz del *switch* que conecta el AP.

18 CONFIGURACIÓN DE ROUTER O FIREWALL/IPS

18.1 Configuración para Firewall / IPS

Por su funcionalidad, el *Firewall/IPS* marca *CheckPoint*, actualmente se encuentra como concentrador de *VPN* para las direcciones regionales y conexiones remotas para usuarios que requieran conexión y gestión remota de servicios.

Estos equipos actualmente se encuentran bajo la modalidad de arrendamiento y no son propiedad del MEP, por lo cual existe un contrato con la empresa Soluciones Seguras, para que ellos puedan configurar los equipos nuevos e instalarlos para su uso dado que tienen que colocar los licenciamientos respectivos para que puedan ser gestionados por la consola.

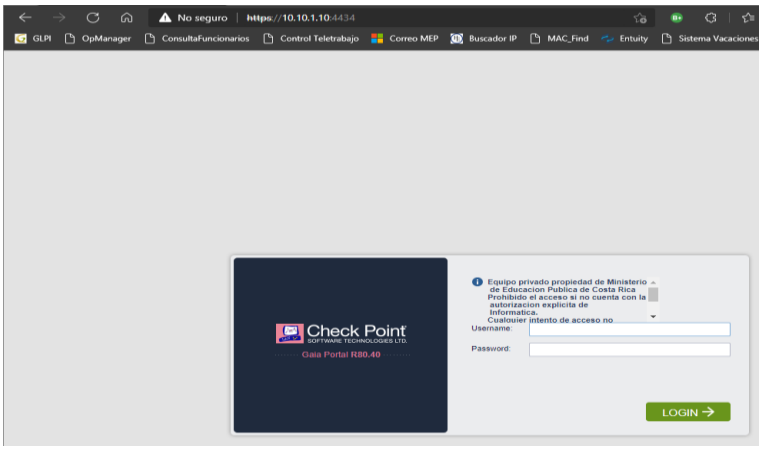
La consola de toda la plataforma *checkpoint* es la IP 10.10.1.26 y requiere que se instale un programa en su máquina para que pueda realizar configuraciones de acceso; permitir o denegar tráfico.

Esta plataforma se divide en dos partes: GAIA y Consola.

18.1.1 GAIA

Se ingresa por *web* para configurar ciertos parámetros como IP en las interfaces, rutas estáticas, actualizaciones de *software*, servicios de *DHCP, Policy Based Routing (PBR)* entre otros.

Para ingresar a modo de ejemplo https://10.10.1.10:4434 es importante colocar el puerto 4434.



Para el caso de los equipos implementados se ingresa por la dirección *LAN* establecida (ejemplo https://10.10.1.10) con el usuario y clave ya definidos.

Para configurar el *Firewall/IPS* se necesitan la siguiente configuración básica, que son fundamentales para la operatividad del equipo:

Configurar las interfaces *LAN* y *WAN* del equipo, ingresar en el menú de *network management*, luego escoger la opción *Network interface*, seleccionar la interfaz (ejemplo eth3), clic al botón edit para colocar la *IP* deseada. (Imagen 1 y 2).

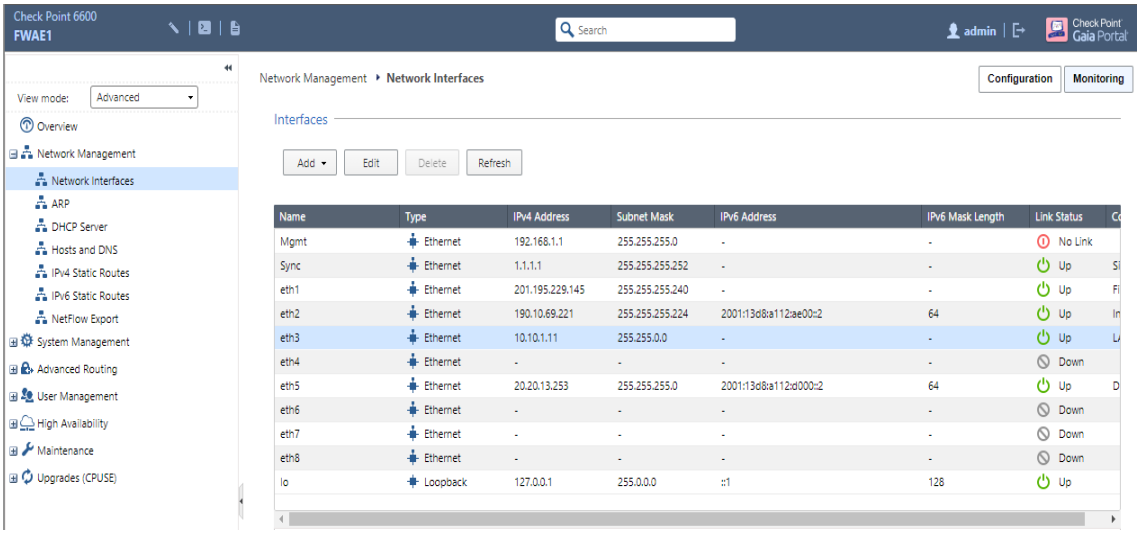


Imagen 1.

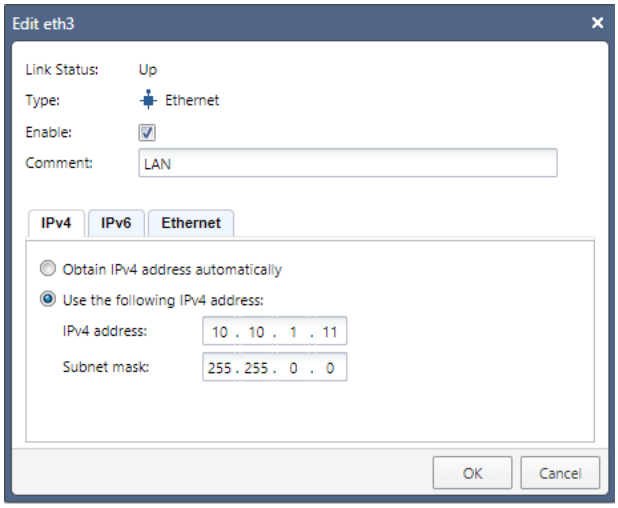


Imagen 2.

Posteriormente, se procede a configurar rutas estáticas de acuerdo a lo que se requiera realizar, para ingresar vamos al menú *Network Management*, opción *IPv4 Static Routes* (imagen 3), y agregamos una ruta con el botón *Add*, llenamos los campos (imagen 4) con los datos requeridos y en la parte de *Add Gateway* seleccionamos *IP Address* (imagen 5) para colocar la puerta de enlace de la red (imagen 6) y le damos OK.

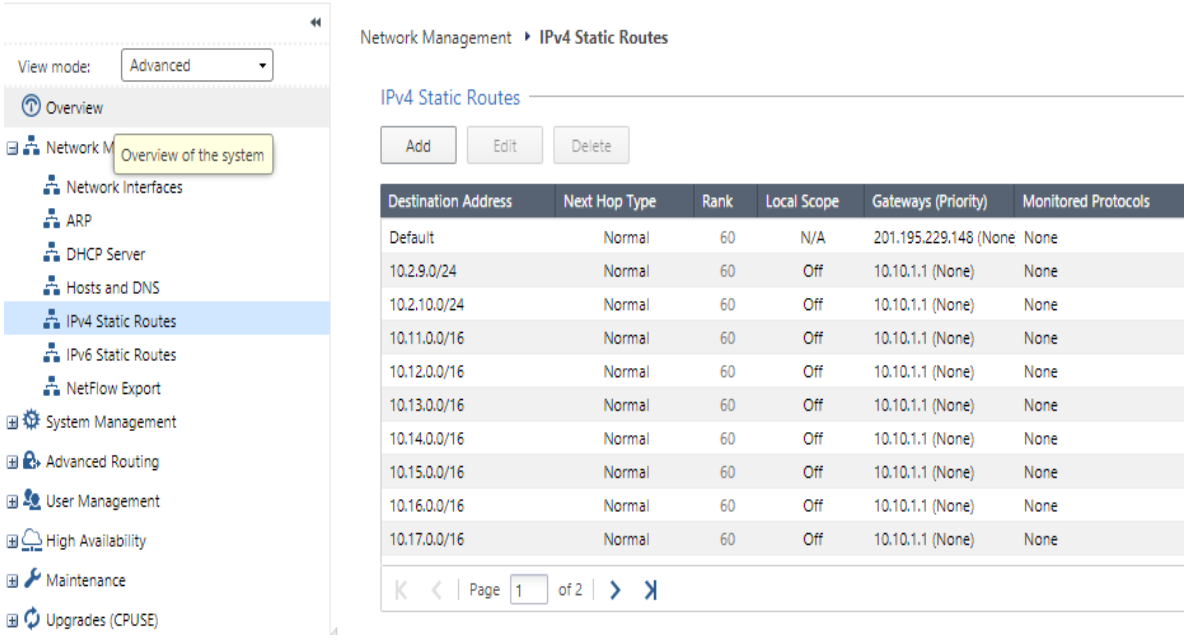


Imagen 3.

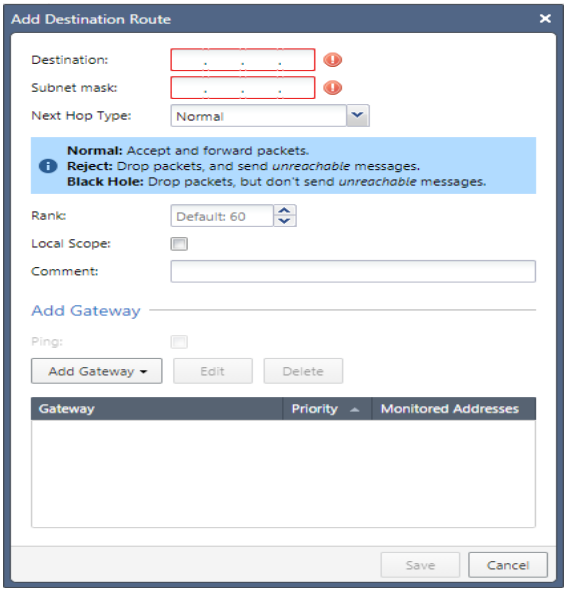


Imagen 4.

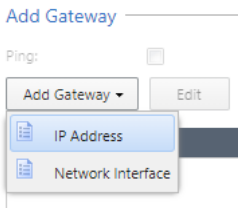


Imagen 5.

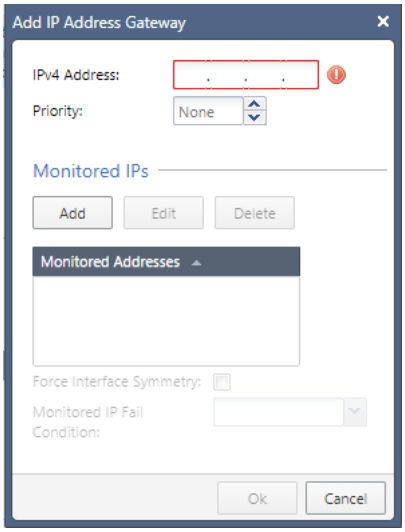


Imagen 6.

Otro punto es que las actualizaciones se encuentra en la Menu *Overview* en la opción *Software Update*, aquí se indican cuantas están disponibles, al ingresar se selecciona el *hotfixes* o paquete que se desee y se le da descargar (*download*) o *install Update* (imagen 8), cabe recalcar que la instalación de la actualización requiere un reinicio del equipo por lo cual el edificio perderá momentáneamente la navegación web o en ocasiones muy esporádicas el parche de seguridad trae algún otro parámetro que pone inestable el equipo y se requiere regresar a la versión anterior. Conversar con la empresa Soluciones Seguras para más detalles y si el parche es requerido de acuerdo a las reglas que se usan.

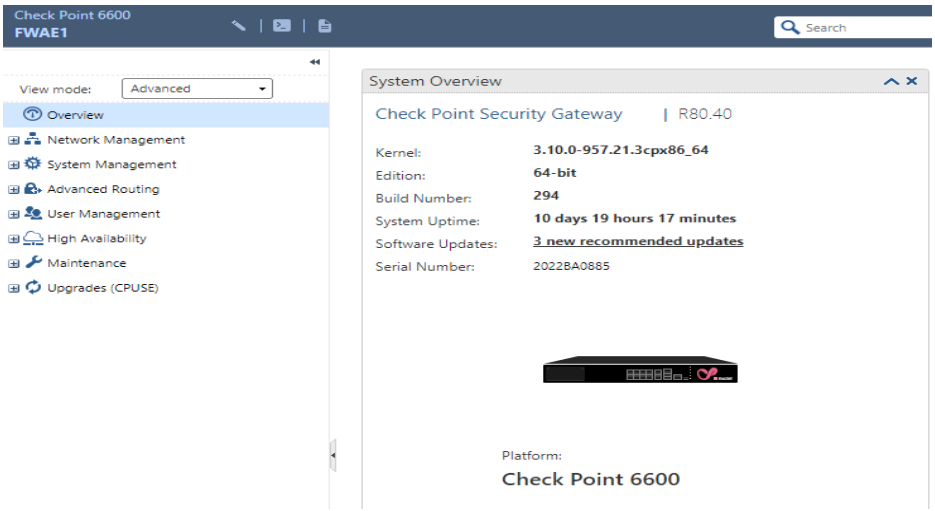


Imagen 7.

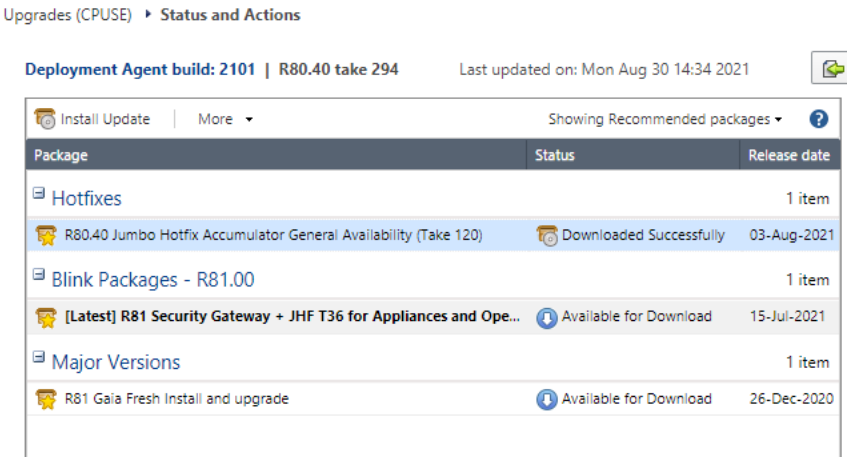


Imagen 8.

Otro punto son los PBR, estos se configurar solo en la *DMZ* de la Antigua Embajada y se encuentra en el menú *Advanced Routing*, en la opción *Policy Based Routing* (imagen 9), esto se usa para cruzar tráfico de *DMZ* hacia *LAN* (viceversa) y puedan alcanzar el servicio. Se divide en dos secciones; *Action Tables* (imagen 10) y *Policy Rules* (imagen 11). Ser muy cuidadosos en esta parte si no está seguro llame a la empresa Soluciones Seguras para que ellos realicen la configuración.

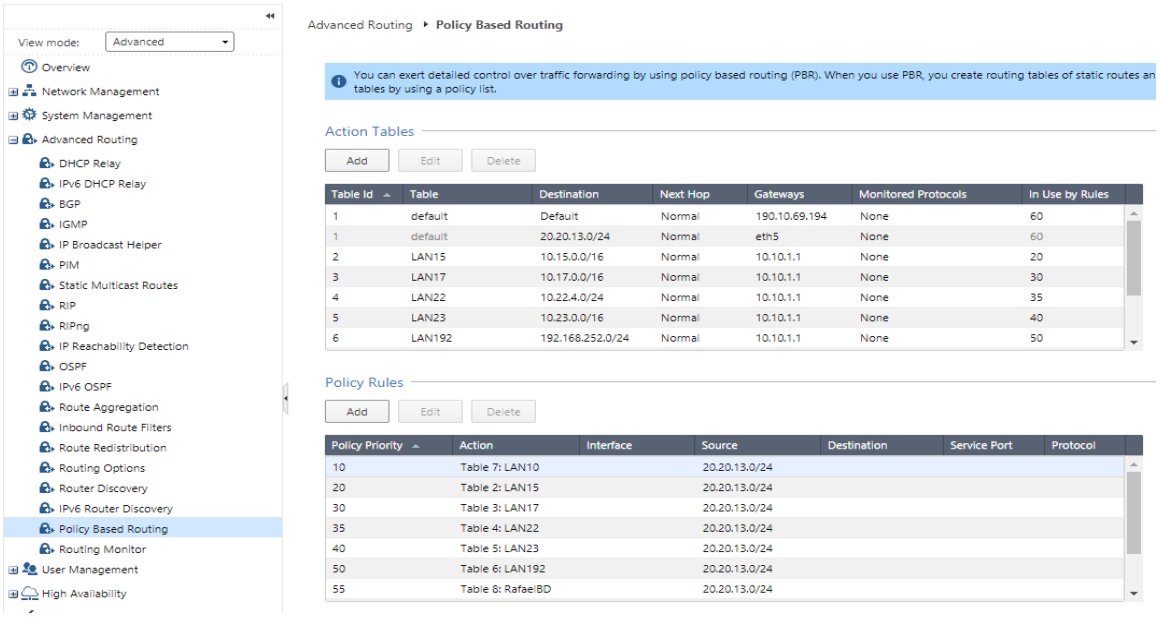


Imagen 9.

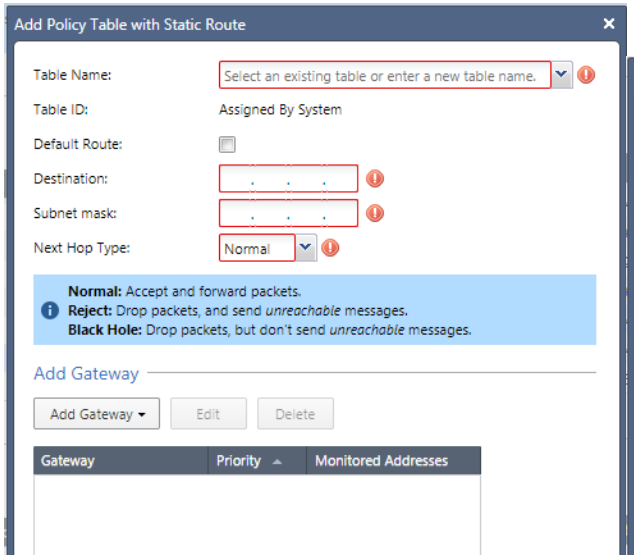


Imagen 10.

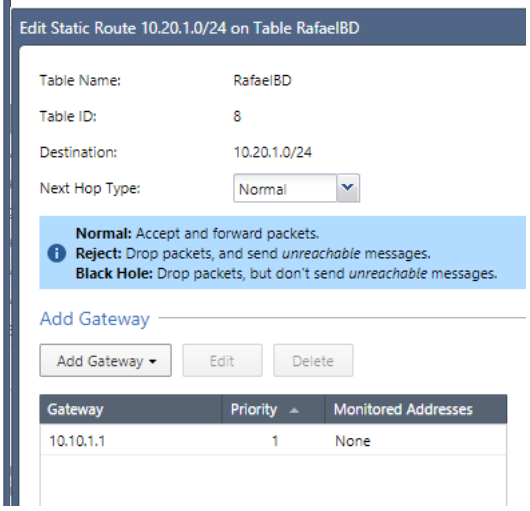


Imagen de ejemplo

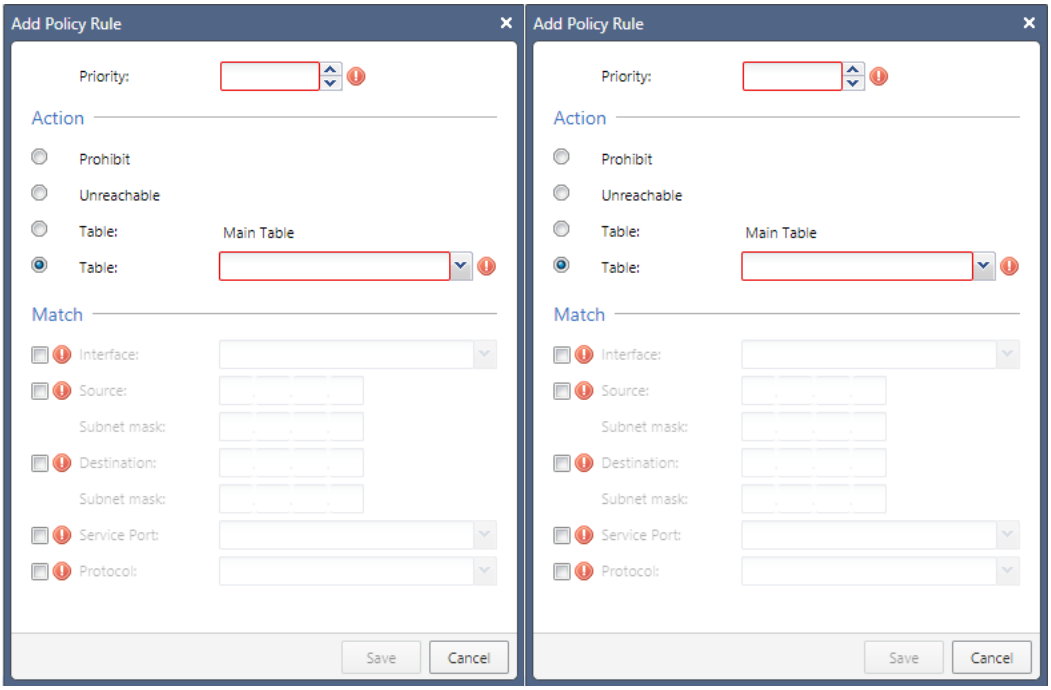


Imagen 11. Imagen de ejemplo

Otro punto es el servicio de *DHCP*, este se configura en el menú *Network Management*, la opción *DHCP Server*. Aquí se habilita el *check Enable DHCP Server* si es la primera vez. (Imagen 12).

Clic al botón *Add* y configuras los parámetros requeridos. (Imagen 13 y 14).

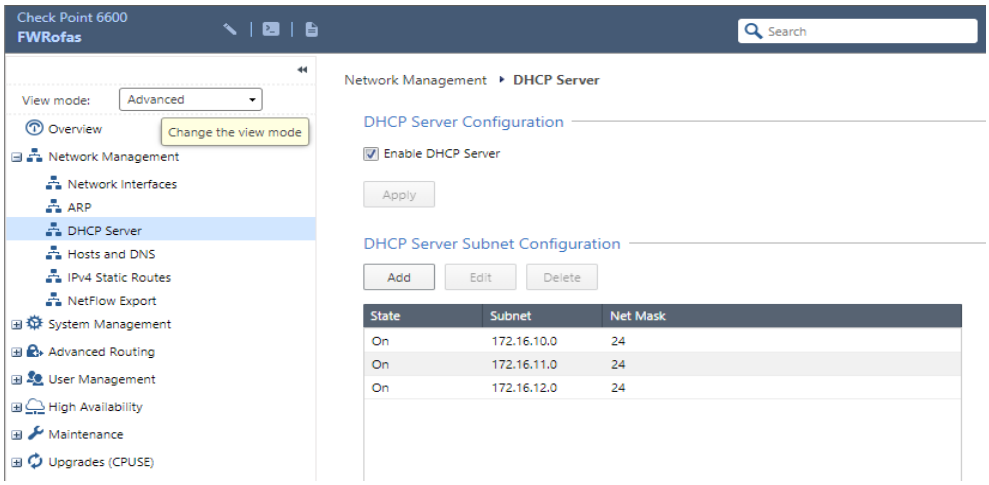


Imagen 12.

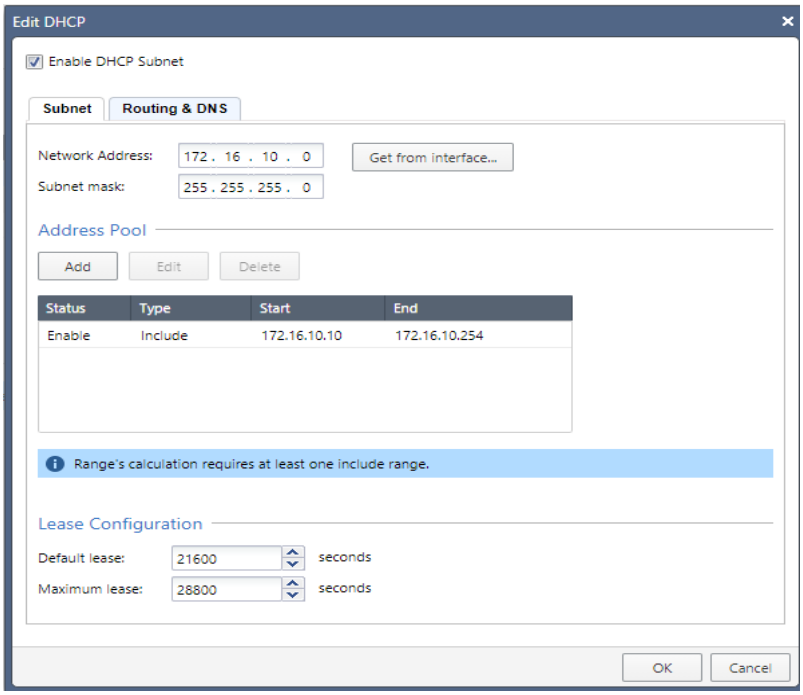


Imagen 13.

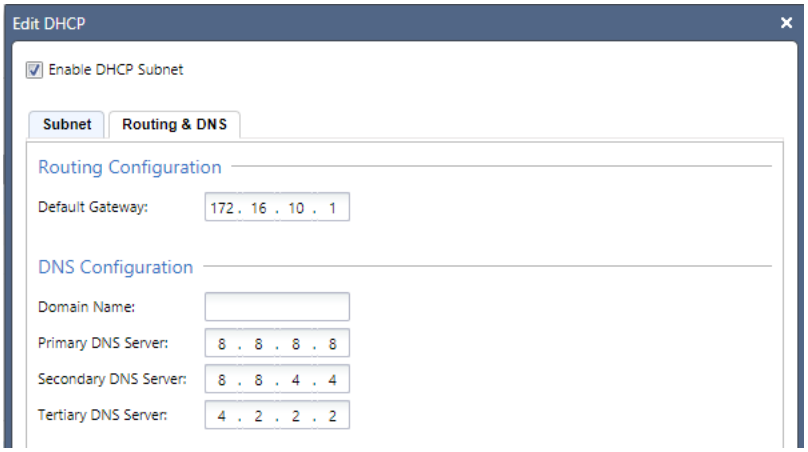


Imagen 14.

De esta manera se termina de parametrizar de forma básica la GAIA.

18.1.2 CONSOLA

Ahora veremos parte de la consola y como crear reglas, permitir/denegar tráfico y aplicaciones.

Para descargar la consola necesita entrar por GAIA a cualquier equipo de la serie 6000 de oficinas centrales, en el menú *Maintenance*, la opción *Download SmartConsole* y le das clic al botón *Download*, una vez descargado se instala y continúa el proceso de instalación, solo *next* a todas las ventanas.

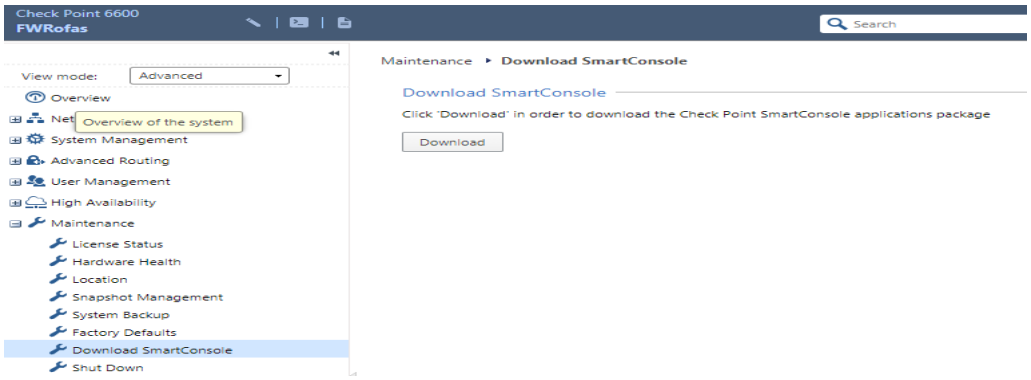


Imagen 15.

Buscas el programa *smartconsole* r80.40 instalado en su máquina (versión a la fecha de la redacción de este manual, imagen 16) y lo ejecuta.

Se abre una ventana (imagen 17) y colocas la *IP* de la consola que es 10.10.1.26 además del usuario y contraseña respectiva.

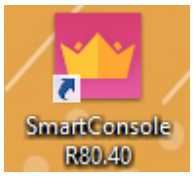


Imagen 16.

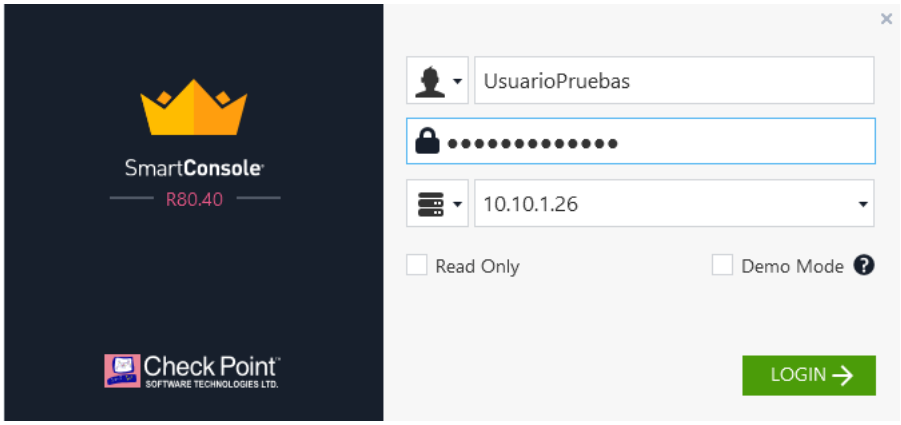


Imagen 17.

Una vez que hemos ingresado, nos aparecerá los 3 diferentes grupos de políticas que existen que son: DRES, EdificiosPrincipales y Antigua Embajada (parte superior izquierda), sobre estos crearemos las diferentes reglas de acceso o denegación de acuerdo a lo que se requiera (imagen 18).

Ahora para crear una regla básica de Firewall nos vamos a la parte de *Access Control* en la parte de *Policy*, escogemos la opción *Security* (Imagen 19). En esta opción solo entran en juego los protocolos como *TCP* y *UDP*, ósea la apertura/denegación de puertos específicos que vamos a configurar.

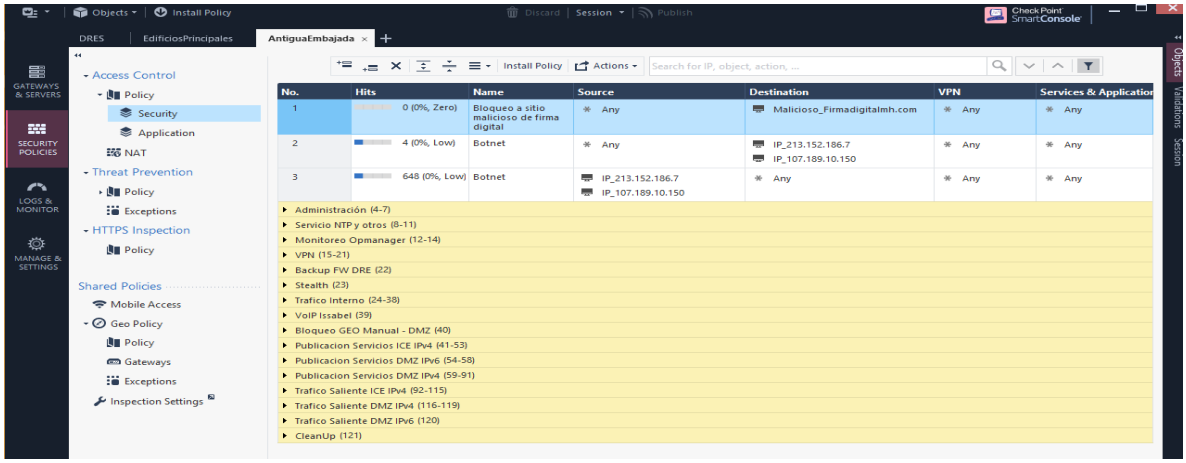


Imagen 18.

Imagen 19.

Planeamos donde vamos a crear la regla para tener un orden en el *Firewall*, a modo de ejemplo la regla de *VoIP Issabel* (Imagen 21A) nos muestra cómo se configura en este modo con los objetos ya terminados.

Creamos una regla nueva: nos colocamos sobre la regla 39 porque deseamos colocar la regla nueva debajo de ella, por lo tanto le damos clic derecho con el mouse, escogemos la opción *new rule, below* (Imagen 21B).

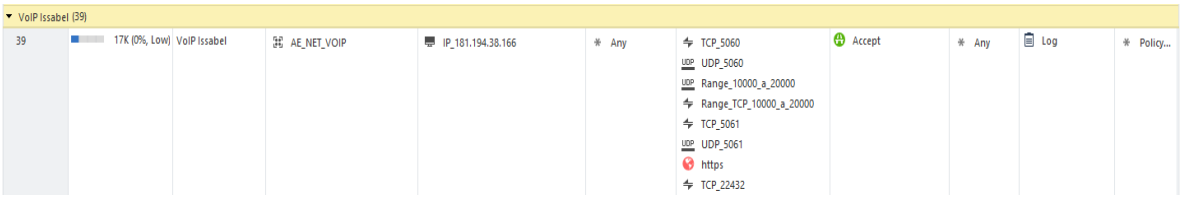


Imagen 21A.

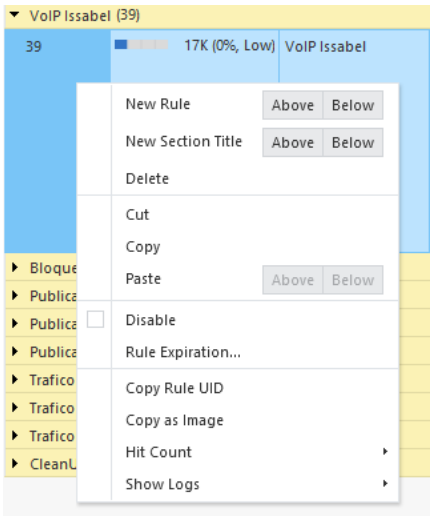


Imagen 21B.

En cada columna podemos agregar objetos ya creados o configurar objetos nuevos como *IP*, puertos *TCP*, entre otros.

Si necesitamos crear un objeto nuevo porque es una *IP*, en la columna *Source o Destination* sobre la regla, damos clic derecho y *add new ítems*… (Imagen 22).

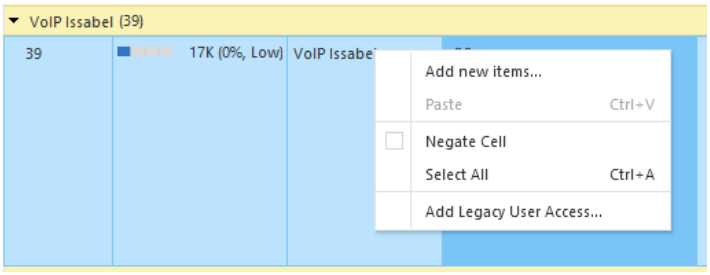


Imagen 22.

Nos aparece una ventana (imagen 23) para buscar el objeto si fuera el caso pero como vamos a crear uno nuevo le damos al icono  y nos aparecen varios opciones (imagen 24) para crear desde un host, un segmento de red, un rango de direcciones, un grupo para incluir dentro de una cantidad determinada de objetos para no estar colocando uno por uno como ejemplo *AE_NET_VOIP*. Siguiendo con el ejemplo le damos a host y llenamos los campos requeridos por la ventana (imagen 25). El nombre descriptivo los ponemos con “IP_10.17.60.1” seguido en el campo Descripción breve del objeto para saber qué hace o a quién pertenece, la *IP* como tal se coloca en *IPv4 address*. Damos OK.

Imagen 23.

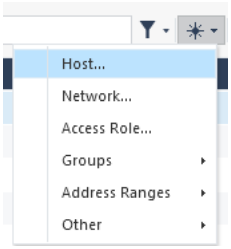


Imagen 24.

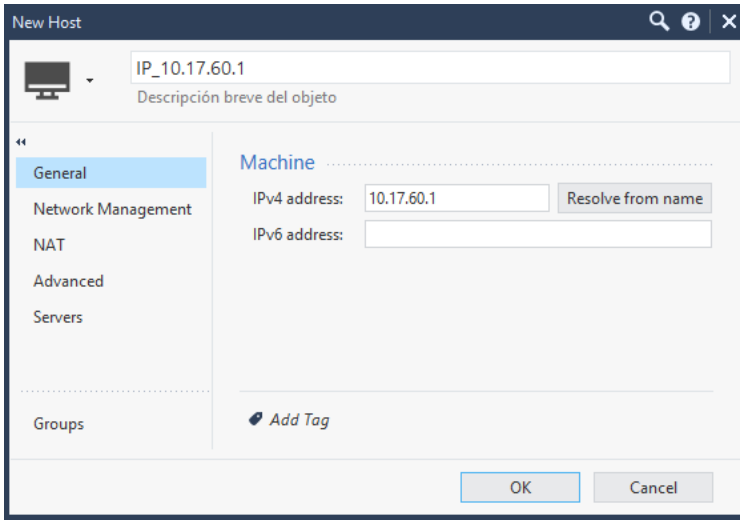
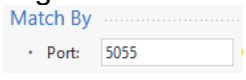


Imagen 25.

Para la parte de los protocolos que vamos a permitir/denegar trabajamos sobre la columna *Services & Applications*, hacemos el mismo proceso anterior, clic derecho sobre la columna, clic a *Add new ítems*…, en la siguiente ventana (imagen 23) buscamos el objeto ya que son protocolos estándar pero si deseamos crear uno nuevo le damos clic al icono  y escogemos el protocolo (imagen 26) que deseamos, a modo de ejemplo escogemos el TCP y escribimos un nombre descriptivo *TCP_5055*, en la parte Match By: 

colocamos el puerto correspondiente que el *firewall* va a gestionar. Damos clic OK.

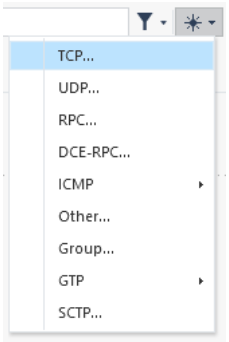


Imagen 26.

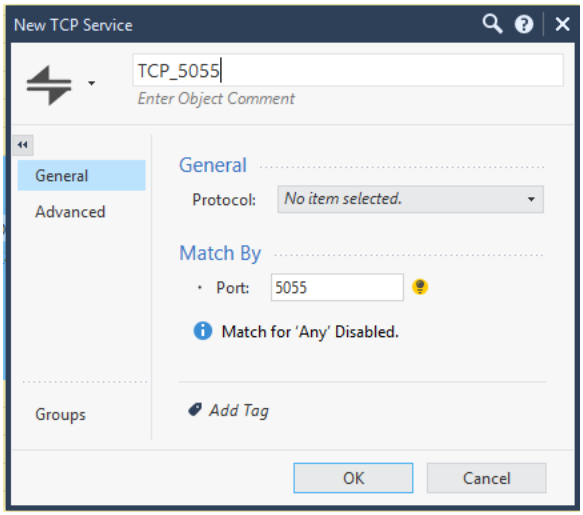


Imagen 27.

Ya por ultimo decidimos que vamos hacer con ese tráfico, si es permitido o denegado. Clic derecho sobre la columna *Action* en la regla como tal y escogemos alguna de las dos opciones: *Accept o Drop*.

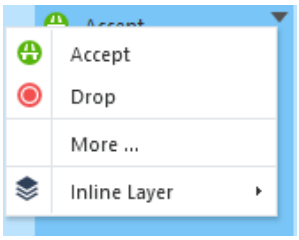


Imagen 28.

Ahora vamos a crear reglas de aplicaciones que son ya los programas, aplicaciones como tal o plataformas *web* que detecta el *firewall*.

Sobre *Access Control*, en *Policy*, opción *Applications*, analizamos sobre cuál de todas las reglas creadas deseamos colocar la nueva que vamos a configurar, es importante que ninguna regla anterior nos permita/bloquee, ya que llevan un consecutivo y en ese orden el *firewall* validará si el tráfico es permitido o no, empezando con la primera regla y bajando.

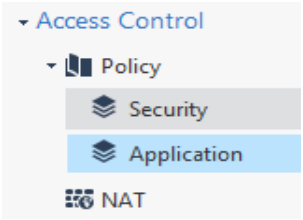


Imagen 29.

Hacemos el mismo proceso anterior para crear reglas: nos colocamos sobre la regla #44 porque deseamos colocar la regla nueva debajo de ella, por lo tanto le damos a la opción new rule, *below* (Imagen 21A).

Llenamos los campos *source* con objetos ya creados o creamos nuevos como vimos en los ejemplos anteriores y en el campo destination colocamos Internet (si el tráfico va a salir hacia Internet pero si va a *LAN o DMZ* colocamos la red o host correspondiente) (podemos arrastrar el objeto de otra regla y colocar tipo copiar y pegar), ahora en la columna *Services & Applications* vamos a poner aplicaciones (*oneDrive*) o plataforma (youtube), las buscamos ya que aquí no podemos crear ya que estas predefinidas por el equipo pero si deseamos incluir URL si podemos crearlas.

Crear *URL* nueva: damos clic derecho sobre la regla en la columna *Services & Applications*, nos aparece un cuadro (imagen 30) y damos a *Add new ítems*…

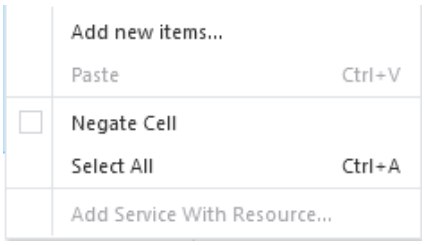


Imagen 30.

Luego en la siguiente ventana, clic al icono y escogemos la opción *Application/Site* que muestra la imagen 31 y nos aparece otra ventana (imagen 32) que llenamos un campo descriptivo para identificarla a modo de ejemplo "URL_Paginas_Permitidas" y damos clic al icono + para agregar la url, es estos casos escribimos así (sin las comillas): "*." El * significa todo lo que exista para la izquierda de la *URL* lo va incluir porque a veces es muy difícil saber que más existe para allá, ahora "." Significa la división del dominio, entonces va a permitir a modo de ejemplo tarcoles.ice.go.cr y si deseamos permitir todo los que sea "go.cr" entonces hacemos *.go.cr y podemos ser tan específicos como queramos o tan global como queramos.

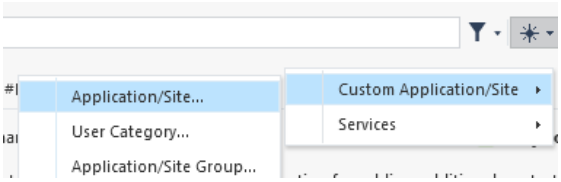


Imagen 31.

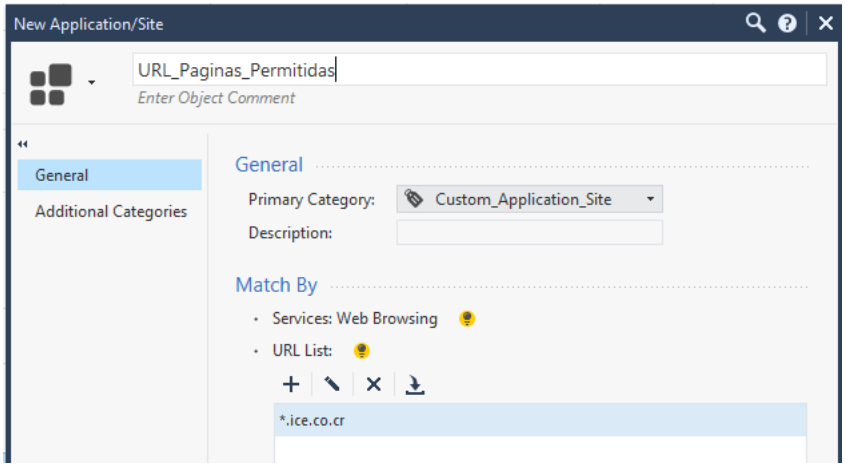


Imagen 32.

Ya existen grupos de *URL* creados así que podemos validar si la *URL* que deseamos colocar puede o no entrar en esos grupos y solo actualizamos la lista con el icono +.

Hora que nuestra regla ya le definimos un *source*, un *destination* y un *services & applications*, tenemos que colocar en la columna *Action* que vamos hacer con ese tráfico si lo permitimos o lo bloqueamos como vimos en el ejemplo anterior, ahora en la columna *Track* si deseamos que registren *logs* o no (imagen 33) y por último

dependiendo de qué grupo de políticas estemos instalando podemos indicar a que firewall específicos deseamos instalar las reglas (imagen 34).

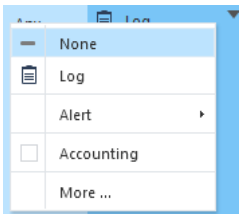


Imagen 33.

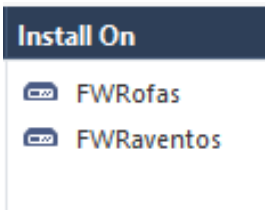
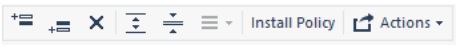


Imagen 34.

Ahora para terminar de aplicar la regla y que entre en funcionamiento, le damos clic al botón *Install Policy* en la parte superior central de la pantalla.



Seleccionamos a que *firewall* deseamos instalar (esto varía dependiendo de qué grupo de políticas este configurando) y damos clic al botón *install* (imagen 35).

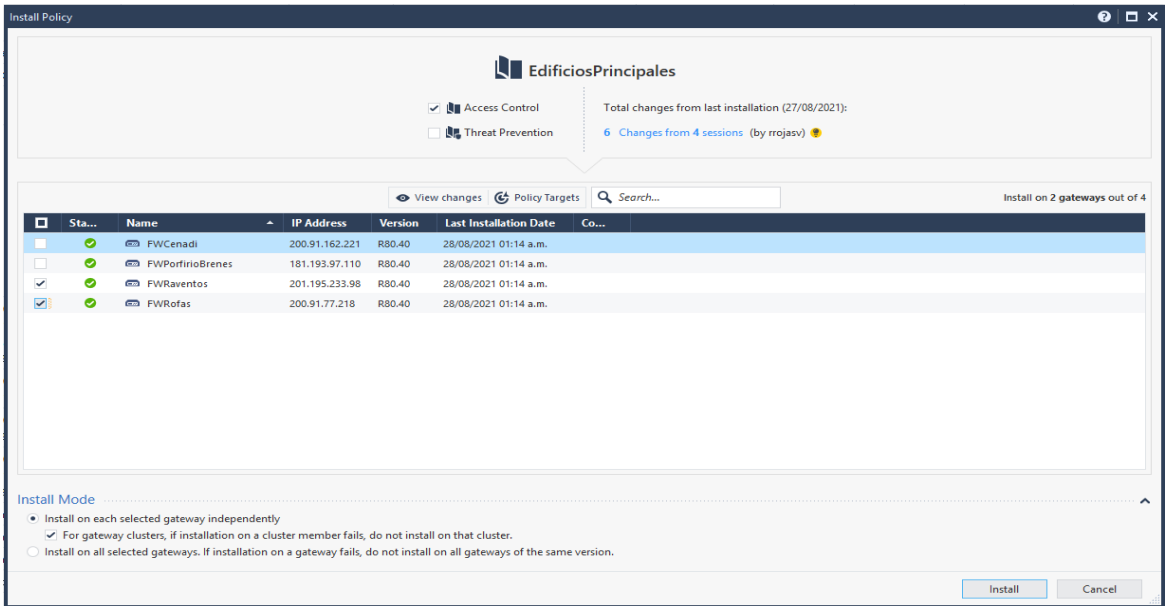


Imagen 35.

Ahora la parte de *NAT* sirve para publicar servicios, “convertir” una *IP LAN* en *IP WAN* y puedan alcanzar los servicios desde Internet, esto se acostumbra para *DMZ* en la mayoría de las veces.

Hacemos el mismo proceso que hemos venido realizando escogemos el orden donde queremos que entre a regir la regla, aquí cambian un poco los nombres de la columnas pero es el mismo principio.

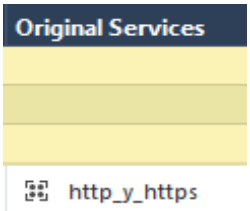
No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
Nat Manuales (1-6)								
1	Net_Turrialba2	Net_AE	Any	Original	Original	Original	Policy Targets	

Si queremos que desde Internet lleguen a un servicio nuestro recién publicado lo hacemos de este modo:

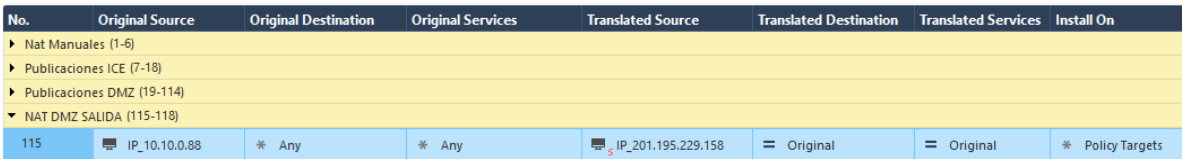
No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
Nat Manuales (1-6)								
Publicaciones ICE (7-18)								
Publicaciones DMZ (19-114)								
19	Any	IP_190.10.69.199	http_y_https	Original	IP_20.20.13.2	Original	Policy Targets	

El campo Original *Source* se coloca en *"Any"* que representa cualquier parte del mundo. Original *Destination* la *IP* Pública asignada al server a nivel lógico y el campo *Translated Destination* la *IP LAN* de nuestro server, además el campo Original *Services* que indica que puerto está abierto.

Nota: en las reglas viejas para el campo Original *Services* aparecen protocolos pero en las reglas nuevas se deja en *"Any"* y bloqueamos por reglas de *firewall* como vimos en los ejemplos anteriores.



Si queremos que un servidor nuestro salga a la calle con una *IP* pública en específico para que algún tercero lo pueda ver, lo hacemos de este modo:



No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On
Nat Manuales (1-6)							
Publicaciones ICE (7-18)							
Publicaciones DMZ (19-114)							
NAT DMZ SALIDA (115-118)							
115	IP_10.10.0.88	Any	Any	IP_201.195.229.158	Original	Original	Policy Targets

Original *Source* colocamos la *IP LAN* del server y en *Translated Source la IP* pública de pool de direcciones que el MEP dispone.

Hemos terminado de configurar el *firewall* con los procesos cotidianos.

Recordar que estos firewall están bajo un contrato de arrendamiento y la empresa Soluciones Segura dispone de una mesa de servicio (ayuda@solucionesseguras.com) para a atención de casos/fallas y solicitudes de cualquier tipo de configuración sea básica o avanzada.

18.2 Configuración de Router

Para la configuración del *router* son necesarios los siguientes implementos:

- Cable consola,
- Cable de red (RJ45),
- Computador PC o Portátil, con puerto serial,
- Cable de poder del *Router*.

Posteriormente, ingresar al Hiper terminal del equipo o cualquier otro software que cuente con esta función.

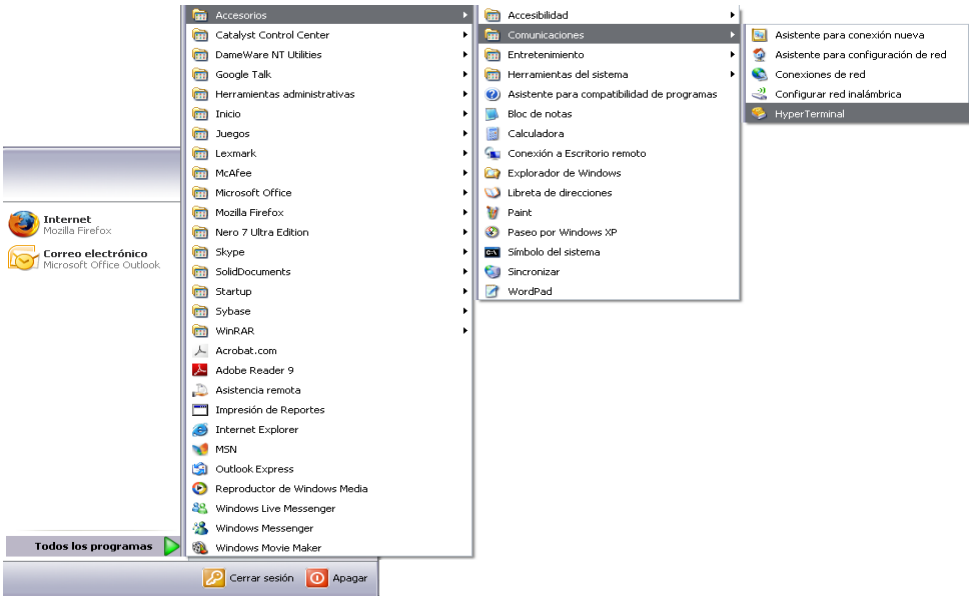


Figura 36.

Ingrese en el *Hyper* terminal y cree una conexión nueva con el nombre que desee y que pueda identificar más adelante.

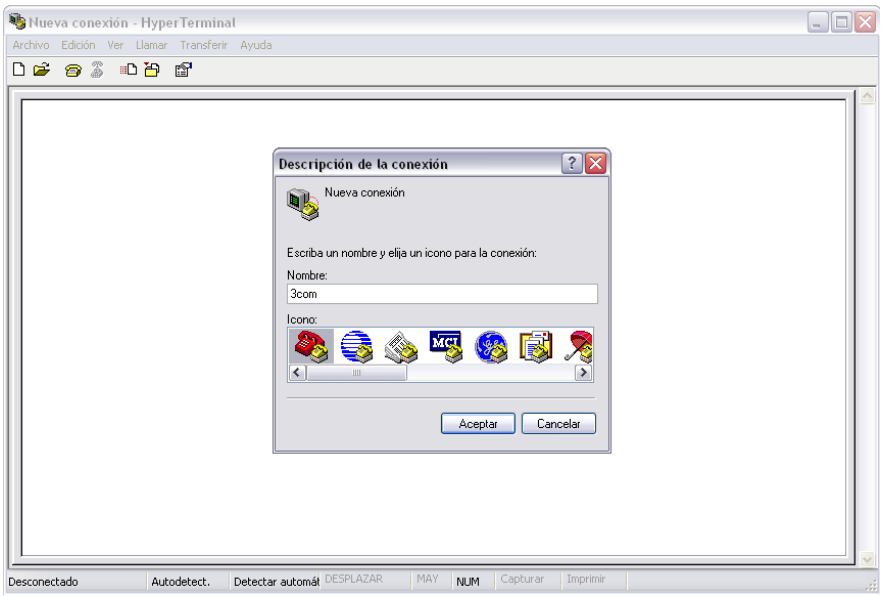


Figura 37.

Seleccione el puerto donde estará conectado el cable de consola (puerto serial) como se muestra en la figura 38, y posteriormente seleccione la configuración donde

los bits por segundo deben estar en 9600, bits de datos 8, paridad ninguno, bits de parada 1, control de flujo ninguno como se muestra en la figura 39.

Figura 38.

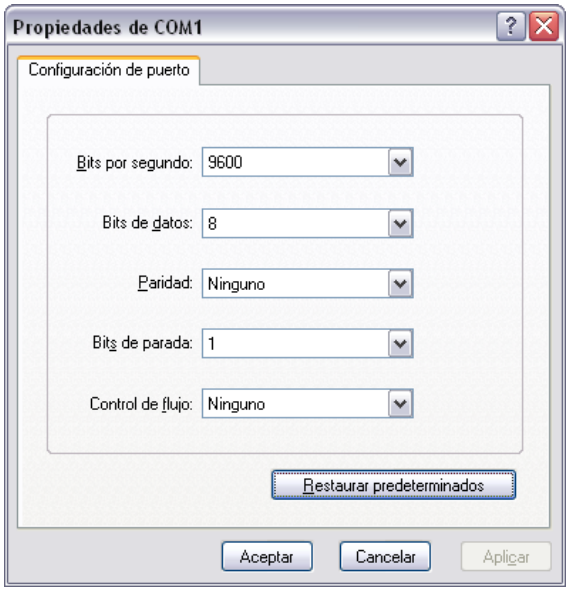


Figura 39.

En caso de tener que realizar la conexión remota (no desde la consola del equipo) se puede utilizar el telnet al equipo con la dirección *IP* local, ingresando el usuario y la clave establecidos. Los *router* tiene una segunda clave para ingresar al modo privilegiado donde se realizan la mayoría de las configuraciones, se usa el comando SUPER y se coloca la contraseña respectiva.

Figura 40.

Dentro de la configuración se detallan aspectos importantes sobre las rutas estáticas y documentación de los puertos utilizados en cada conexión.

En la siguiente línea se detalla la configuración de las rutas estáticas de la subred 10.12.x.x que se dirige al edificio Antigua Embajada, Raventós, Porfirio Brenes en la siguiente sintaxis.

Ejemplo:

ip route-static 10.10.0.0 255.255.0.0 192.168.20.3

ip route-static 10.11.0.0 255.255.0.0 192.168.20.3

ip route-static 10.16.0.0 255.255.0.0 192.168.20.3

Para cada interfaz se debe colocar el direccionamiento que tendrá el servicio así como una breve descripción de que es lo que interconecta el puerto.

interface *Ethernet1,*

description Interfaz hacia la *LAN,*

ip address 10.12.1.4 255.255.0.0

Dentro de la consola se debe manejar el estándar de comandos establecidos por el fabricante como el “show run” o “dis cur” para ver configuraciones y el “exit” o “quit” para salir de la sesión.

Se puede ingresar a los diferentes *router* de la plataforma ministerial para verificar que configuración básica desea realizar y ver comandos específicos.

Comandos básicos:

Configure terminal (conf t): ingresar al modo global de configuración dependiendo del modelo del equipo,

Show run ó dis cur: sirve para ver toda la configuración del *router o switch,*

Interface giga0/1: para ingresar a la interfaz específica y realizar configuración,

Interface Tunnel10 mode *ipsec*: para crear una interfaz de túnel en *ipsec,*

ip route-static 0.0.0.0 0.0.0.0 10.99.99.99,

acl basic 2000: para crear lista de acceso.

Estos equipos están bajo un contrato de mantenimiento con la empresa Corporación FONT, ellos tiene una mesa de servicio (servicio@font-tecnologia.com) donde se puede escalar los casos de fallas/problemas o solicitudes de configuración básica así como específicas.

Se requiere cierto conocimiento o capacitación en la programación de los *router* o *switch*, adquiridos por algún programa de entrenamiento (*CiscoNetwork*, *HP Network*, entre otros) para entender comandos básicos y cuales con los segmentos del equipo y que se puede configurar en ellos, ya que son términos globales de configuración y aplican para todos. Los comandos específicos si pueden variar de un fabricante a otro pero para eso la mesa de servicio de FONT o la guía de algún *router* de la plataforma ministerial para que replique los comandos de acuerdo a lo que se requiera en su momento.

19 CONFIGURACIÓN E INSTALACIÓN DEL GLPI

GLPI es software libre distribuido bajo licencia GLP, que facilita la administración de recursos informáticos. GLPI es una aplicación basada en *Web*, que permite registrar y administrar los inventarios del *hardware* y el *software* de una empresa, optimizando el trabajo de los técnicos.

GLPI incluye también *software* de mesa de ayuda para el registro y atención de solicitudes de servicio de soporte técnico, con posibilidades de notificación por correo electrónico a usuarios y al mismo personal de soporte, al inicio, avances o cierre de una solicitud.

Entonces con el GLPI se puede:

- Levantar incidencias sobre el funcionamiento de *hardware* o problemas de *software,*
- Consultar las reservas de materiales.

El primer paso es descargar de la página http://www.glpi-project.org/spip.php?article41 el archivo de GLPI.

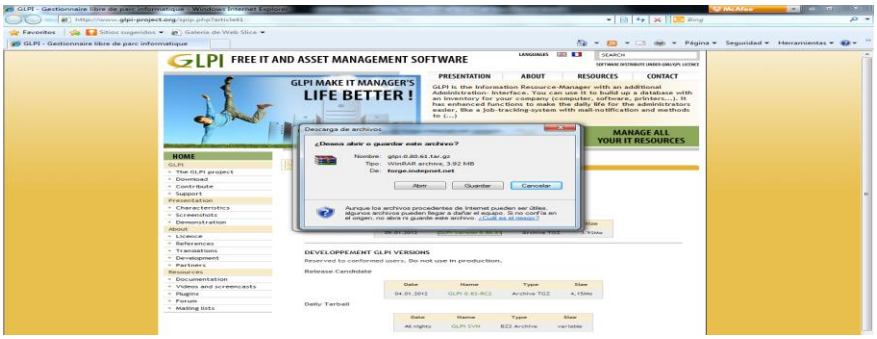


Figura 107.

El segundo paso sería descomprimir el archivo *winzip* del GLPI y copiar la carpeta GLPI en la ruta: c:/xampp/htdocs.

NOTA: Xampp debe estar instalado sobre *Windows* previo.

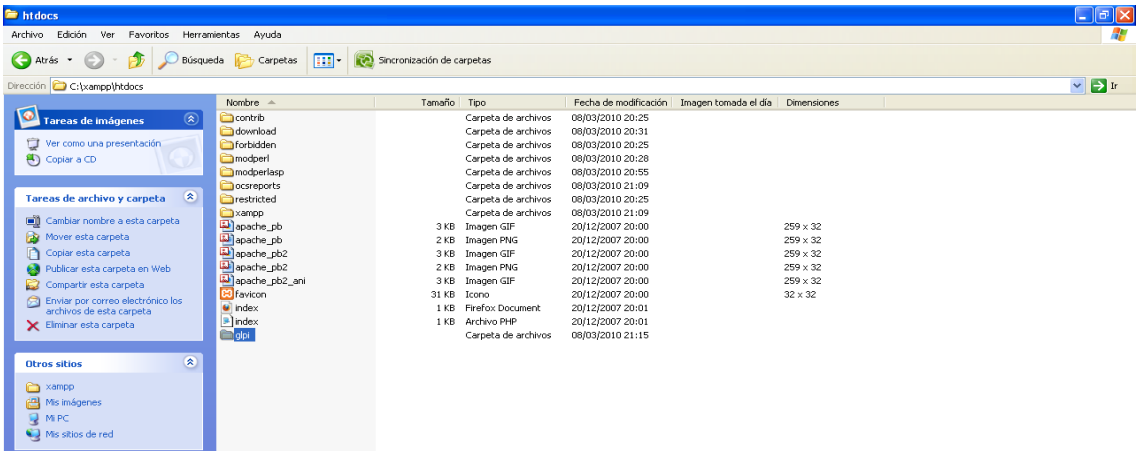


Figura 108.

Abrir el Internet Explorer e ingresar a http://localhost/glpi/install/install.php

Seleccionar el idioma en la pantalla y darle click en OK.

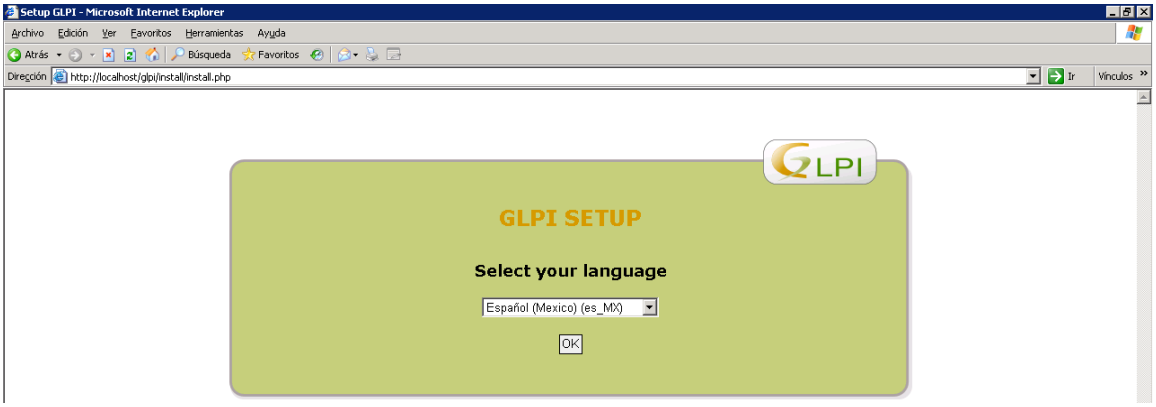


Figura 109.

Marcar la casilla de “He leído y ACEPTO los términos de la licencia enunciados arriba” y darle un click al botón continuar, para aceptar los términos de la licencia.

Figura 110.

Darle click al botón de Instalación.

Figura 4.80.

Atención con la aparición de este error.

El sistema valido que el requisito de memoria este configurado en el archivo de configuración php.ini.

Se debe ingresar y modificar dicho archivo para la corrección del problema.

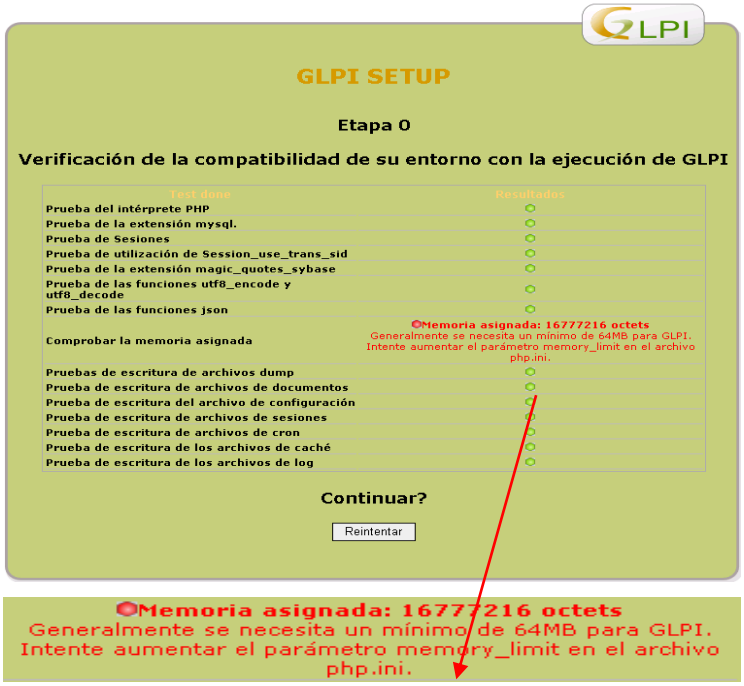


Figura 111.

Dicho archivo se encuentra en la ruta c:\xampp\apache\bin.

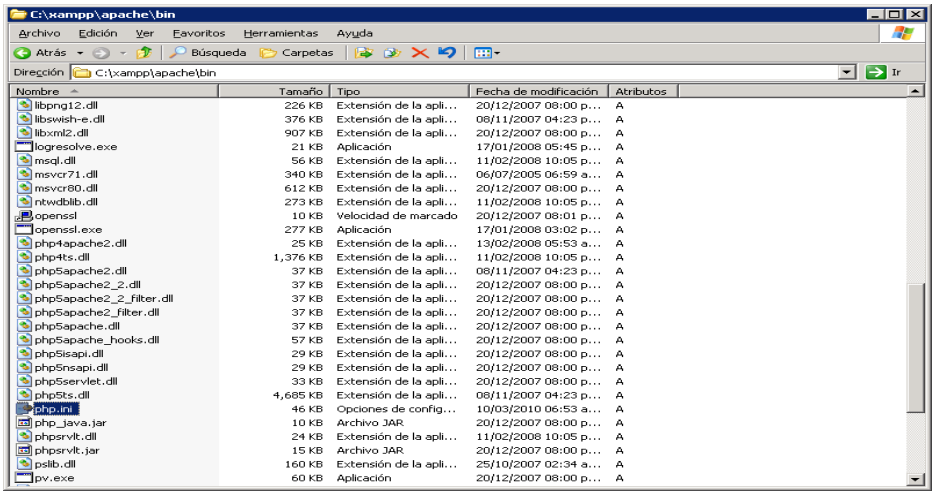


Figura 112.

Se ingresa al archivo y se edita,

Se debe editar en la sección *Resource Limits*, la opción de *memory_limit*.

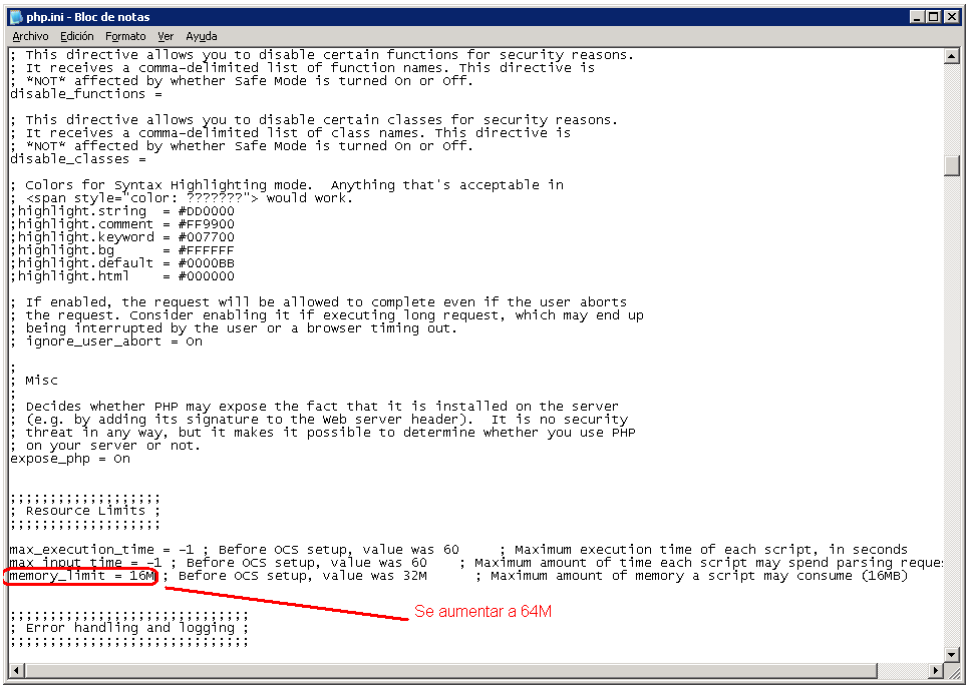


Figura 112.

Luego de modificado esto ya se puede continuar con la instalación pues pasa los requisitos de verificación.

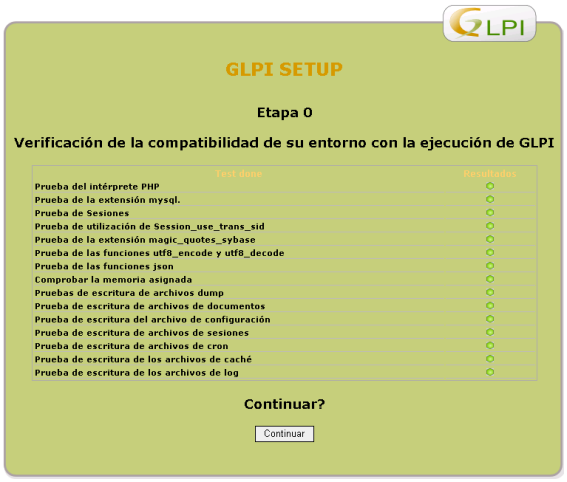


Figura 113.

Se ingresan el usuario y contraseña para conectarse al servidor.

Figura 114.

Se selecciona la Base de Datos mysql.

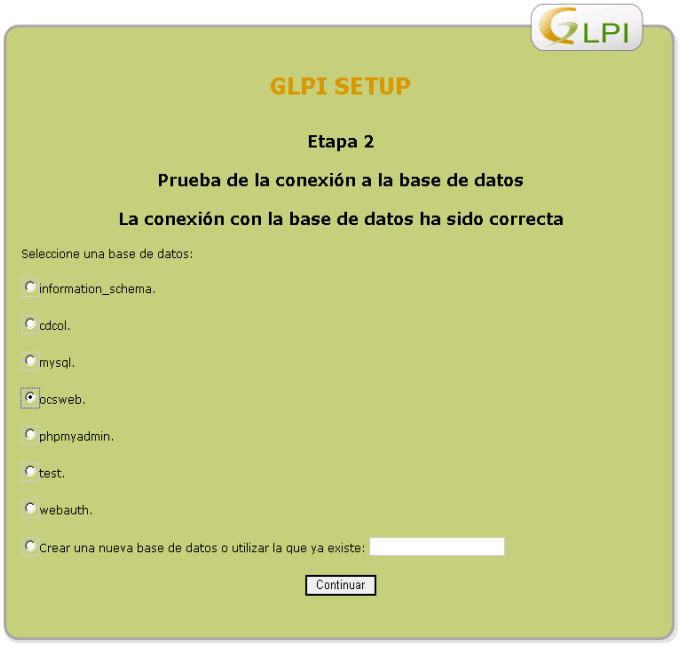


Figura 115.

Lo anterior hace que se inicialice la Base de Datos.

Figura 116.

Se termina la instalación y se indican los usuarios y contraseñas de inicio (o por default) que utiliza el sistema.

Figura 117.

Pasos para configurar la conexión al *LDAP*.

Por default la opción de *LDAP* viene deshabilitada y no se puede configurar.

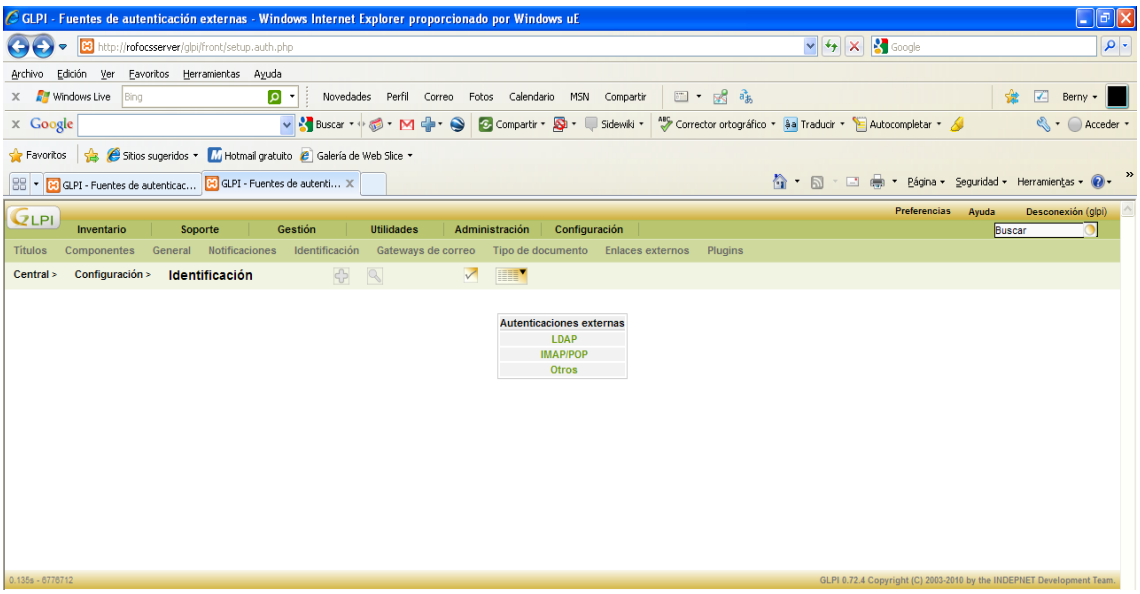


Figura 118.

Se debe editar el archivo php.ini (se ubica en la ruta c:\xampp\apache\bin) y quitar el ";" que deshabilita esa opción.

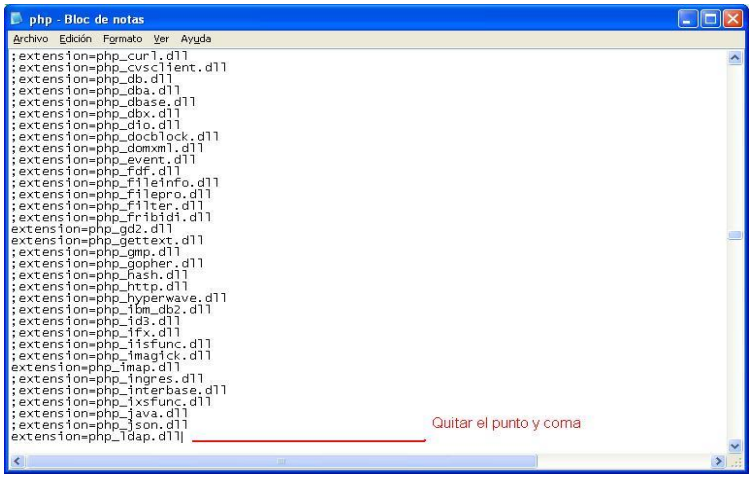


Figura 119.

Luego de esto ya se puede ingresar a la pantalla de configuración de conexión *LDAP*. Seguidamente ir a configuración, identificación.

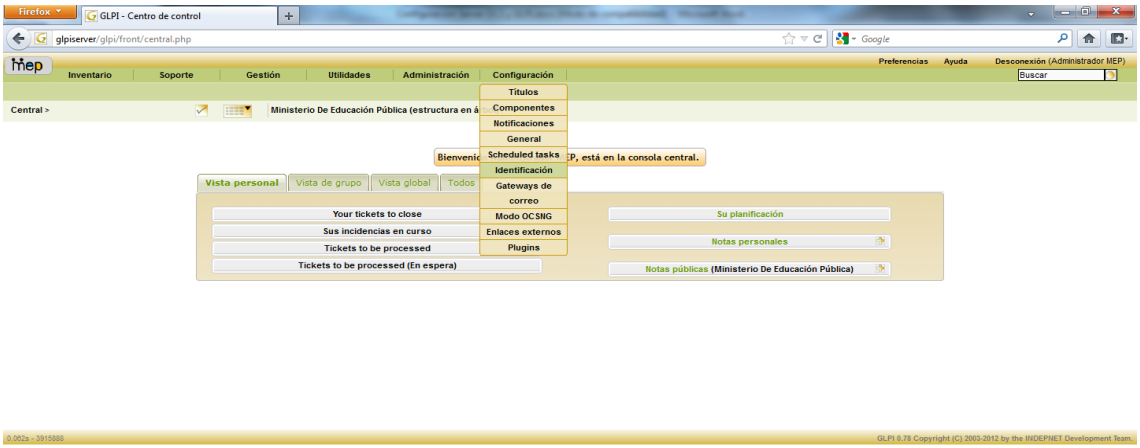


Figura 120.

Seleccione LDAP.

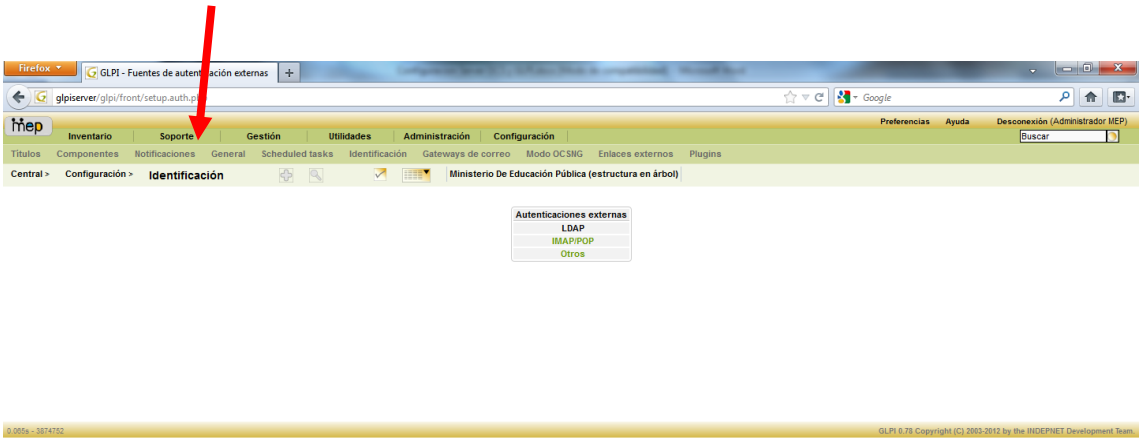


Figura 121.

Seleccione el icono de más para agregar un enlace a datos en nuestro caso el AD.

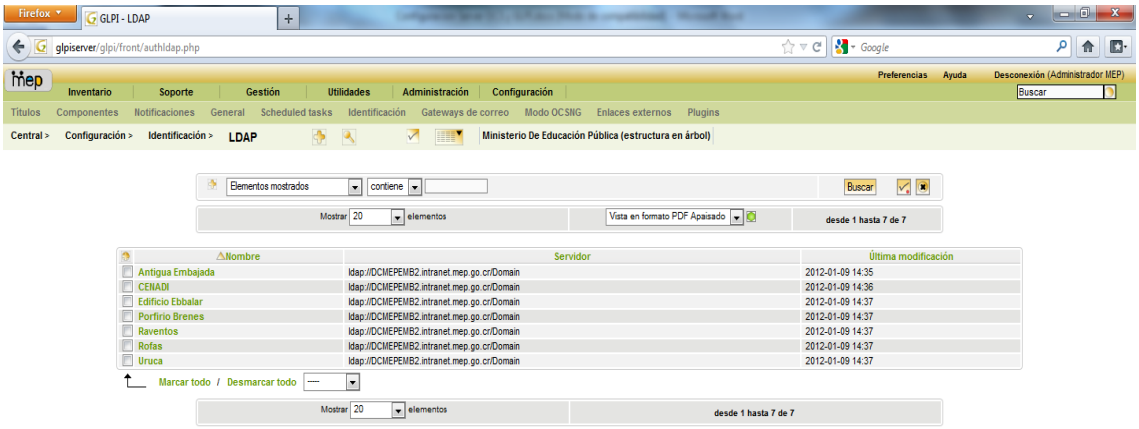


Figura 122.

Se completan todos los campos de la siguiente manera.

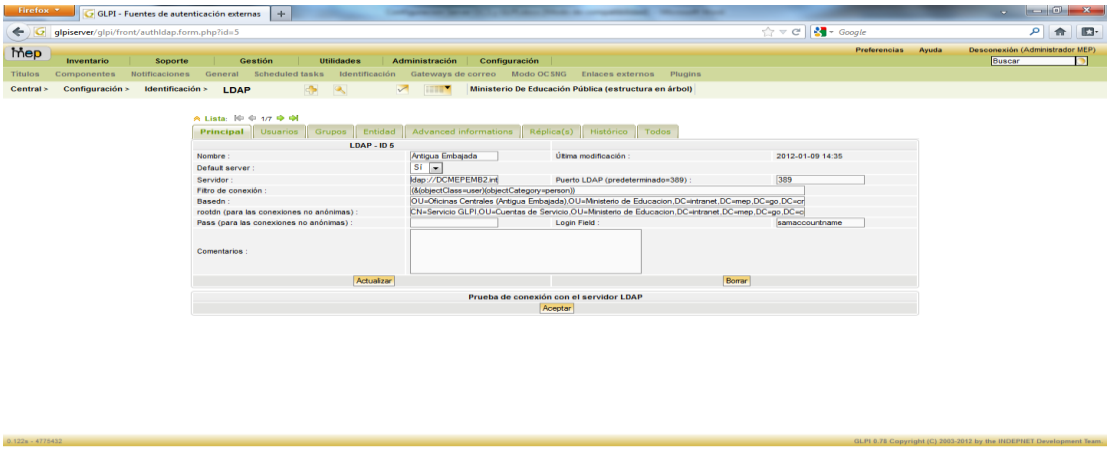


Figura 123.

Nombre: Descripción de la conexión,

Servidor: ldap://NombreServidor.intranet.mep.go.cr,

Filtro de conexión: (&(objectClass=user)(objectCategory=person)),

***Basedn*:** *Ruta de la OU donde se buscará la autenticación:* OU=Oficinas Centrales (AntiguaEmbajada),OU=Ministerio de Educacion,DC=intranet,DC=mep,DC=go,DC=cr *Para este ejemplo buscará dentro de la OU=Oficinas Centrales,*

***Rootdn*:** *Objeto "usuario" que se utilizará para autenticar la aplicación con AD, con toda la ruta de su ubicación. Ej.* CN=Servicio GLPI, OU=Cuentas de *Servicio,OU*=Ministerio de Educacion,DC=intranet,DC=mep,DC=go,DC=cr,

***Pass:** Contraseña del objeto "usuarios" del paso anterior,*

Loginfield: samaccountname,

Luego probar la conexión.

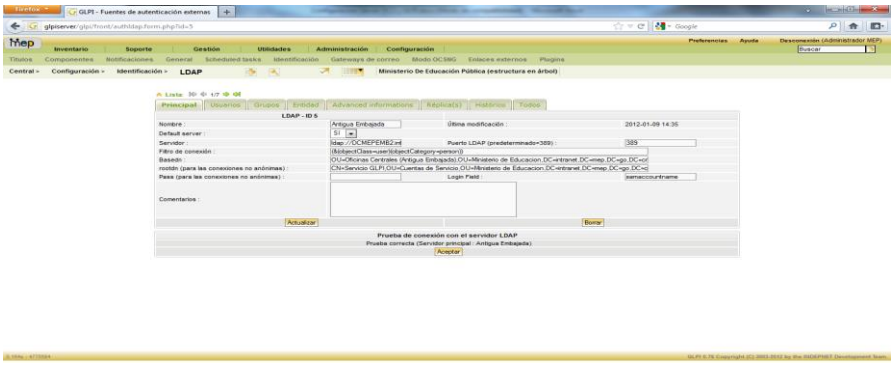


Figura 124.

Ya se pueden agregar los usuarios según manual de Administración de Usuarios.

20 DOCUMENTO DE REFERENCIA

Lic. Salazar Rojas Berny (2008). *"Manual de los procesos de mantenimiento preventivo y correctivo de los equipos de cómputo y telecomunicaciones"*. San José: Dirección de Informática de Gestión. Ministerio de Educación Pública.

21 FIRMAS

---------- INTENCIONALMENTE DEJADO EN BLANCO ----------

MINISTERIO DE EDUCACIÓN PÚBLICA
DIRECCIÓN DE INFORMÁTICA DE GESTIÓN

HOJA DE REVISIÓN Y ACEPTACIÓN

Manual de Configuraciones de Redes y Telecomunicaciones

CÓDIGO: DIG-DRT-MAN-02

ACTUALIZADO POR:	
German Peraza Castro	GERMAN ALBERTO PERAZA CASTRO (FIRMA) Firmado digitalmente por GERMAN ALBERTO PERAZA CASTRO (FIRMA) Fecha: 2021.10.15 09:21:59 -06'00'
Ronny Rojas Vargas	RONNY GERARDO ROJAS VARGAS (FIRMA) Firmado digitalmente por RONNY GERARDO ROJAS VARGAS (FIRMA) Fecha: 2021.10.15 09:39:52 -06'00'
Ana Marcela Barrantes Arias	ANA MARCELA BARRANTES ARIAS (FIRMA) Firmado digitalmente por ANA MARCELA BARRANTES ARIAS (FIRMA) Fecha: 2021.10.14 16:36:04 -06'00'
NOMBRE	FIRMA
REVISADO POR:	
Berny Salazar Rojas	BERNI SALAZAR ROJAS (FIRMA) Firmado digitalmente por BERNI SALAZAR ROJAS (FIRMA) Fecha: 2021.10.21 13:03:21 -06'00'
Kattia Paniagua Alfaro	KATTIA MARCELA PANIAGUA ALFARO (FIRMA) Fecha: 2021.10.22 08:34:06 -06'00'
NOMBRE	FIRMA
APROBADO POR:	
José Sandí Zúñiga	JOSE MANUEL SANDI ZUÑIGA (FIRMA) Firmado digitalmente por JOSE MANUEL SANDI ZUÑIGA (FIRMA) Fecha: 2021.10.22 09:20:36 -06'00'
NOMBRE	FIRMA

FECHA: Noviembre-2021