Universidad Autónoma Metropolitana Unidad Azcapotzalco

División de Ciencias Básicas e Ingeniería

Licenciatura en Ingeniería en Computación

Modalidad: Experiencia profesional

“**Redundancia de enlaces”**

Alumno:

Lizeth Maribel Casañas Jiménez, 206202084

Empresa:

Fujifilm de México S.A. de C.V.

Jefe Directo:

Jesús Gómez Garduño

Gerente de Sistemas

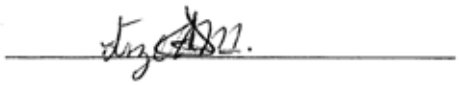
Trimestre: 2016 Primavera

Declaratoria

Yo, **JESUS GOMEZ GARDUÑO** declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la 12 Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Jesús Gómez Garduño

Yo, **LIZETH MARIBEL CASAÑAS JIMENEZ**, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Lizeth Maribel Casañas Jiménez

Contenido

Pág.

Propuesta

Resumen Ejecutivo

Descripción de la empresa

Fujifilm de México es una empresa dedicada a la imagen y fotografía, además está innovando en el campo de la medicina y materiales de alta funcionalidad, así como muchas otras industrias de tecnología avanzada.

Departamento

El departamento de sistemas es el responsable de los sistemas de información, de administrar y proporcionar la infraestructura necesaria para la operación de las actividades en cada departamento, así como mantener las comunicaciones de la empresa, por lo cual existen las áreas de infraestructura y telecomunicaciones, soporte técnico, sistemas operativos y seguridad informática.

Descripción técnica de las actividades asociadas al puesto

Administrador de red. Este puesto tiene las siguientes funciones asignadas:

a. Administración, operación y gestión de Servidores Windows
b. Análisis, detección y prevención de vulnerabilidades de seguridad TI. Como lo es corregir errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, ya que actualmente existen muchas amenazas que tratan de accesar remotamente a los ordenadores.
c. Administración y operación de enlaces de comunicación en redes WAN y LAN.
d. Administración de seguridad perimetral (corta fuegos Palo Alto y Fortinet).
e. Administración de herramientas para DRP (Plan de Recuperación de Desastres).
f. Crear la documentación necesaria y requerida para el mantenimiento y capacitación de herramientas y plataformas.
g. Atender los requerimientos expedidos por las áreas usuarias, por ejemplo falla de conexión a la red inalámbrica, falla en acceso a carpetas compartidas, falla en conexión alámbrica, etc.

Descripción detallada del proyecto

Mi participación dentro del Departamento de Sistemas en los siguientes proyectos:

PROYECTO 1. Redundancia de enlaces

Surgido de la necesidad de garantizar la alta disponibilidad de los servicios y aplicaciones de la empresa para sus empleados, clientes y proveedores, se requiere realizar la redundancia entre el enlace principal y secundario tanto en el CEDIS como en el corporativo. Por lo cual se crearon políticas de salida a Internet tanto en el corta fuegos Fortinet y en Palo Alto que permita el enrutamiento hacia cualquiera de los enlaces si alguno de estos falla. Con lo cual se asegura el flujo de comunicación. En la Figura 1 se muestra el estado inicial de la red.

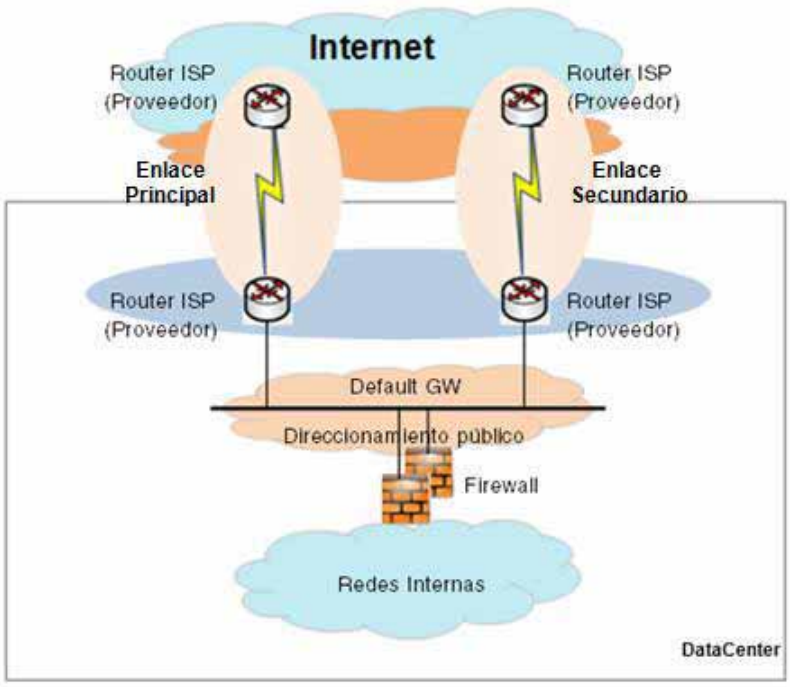


Figura 1. Diagrama inicial de la red.

En las figuras 1 y 2 se muestra flujo de comunicación si alguno de los enlaces falla.

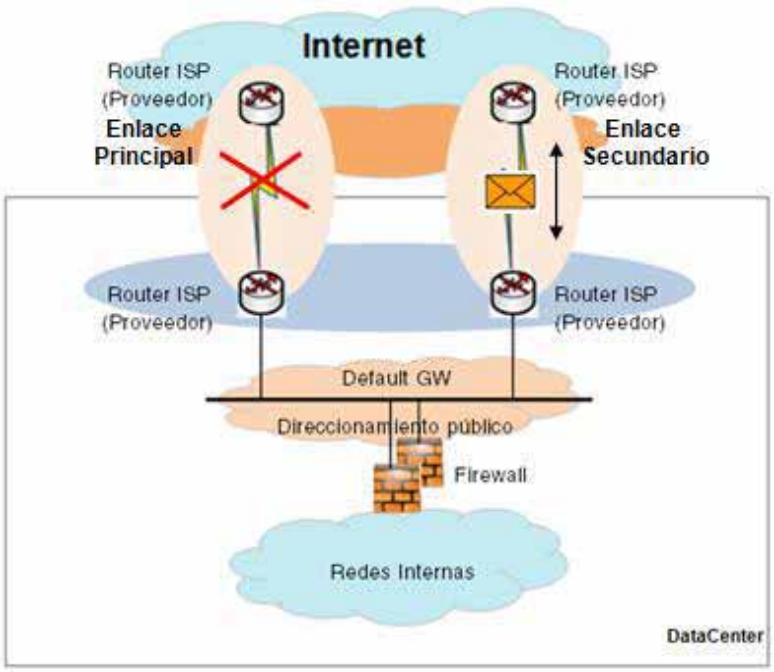


Figura 2. Falla en el enlace principal.

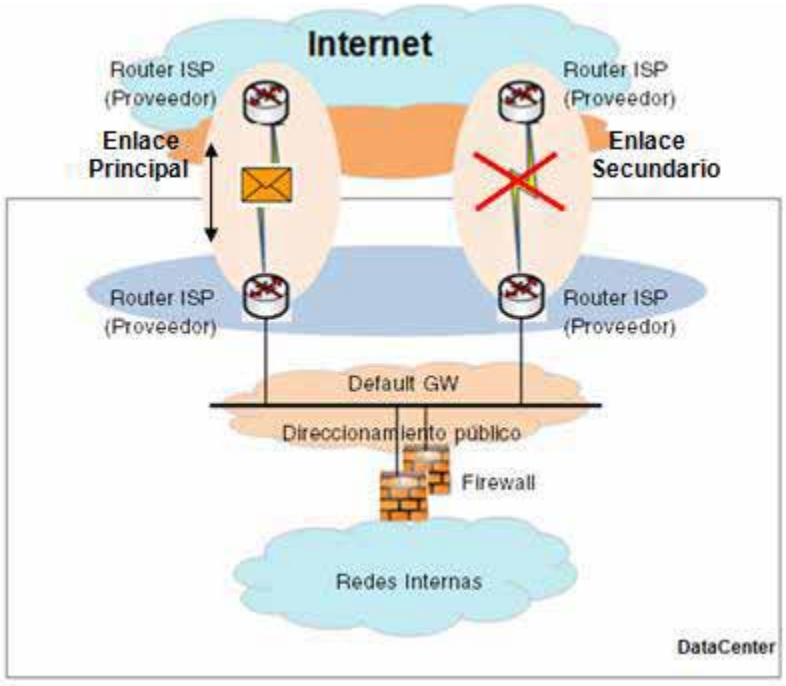


Figura 3. Falla en el enlace secundario.

Descripción de la funcionalidad

Router ISP (Proveedor): Dispositivos físicos que envía y recibe el servicio de internet para la empresa, los cuales son administrados por el proveedor.

Corta fuegos: Dispositivos PAN500 (Palo Alto Network) y Fortigate 60C ubicados en el DataCenter, los cuales son administrados por el Administrador de red. Ambos dispositivos están diseñados para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

En el PAN500 se realizo lo siguiente:

En Device > High Availabiity > Link and Path Monitoring se activó Failure Condition (Condiciones de fallo) para el carrier de salida del enlace primario y secundario. Con lo cual se logró monitorear la caída de alguno de los dos enlaces.

Por con siguiente en Policies > Policy Based Forwarding (PBF) se crean dos políticas las cuales se habilitaran en cuanto no responda alguno de los ping del carrier de salida a alguna IP de internet (por ejemplo 8.8.8.8 Google). En la Figura 4 se muestra un ejemplo de la política basada en forwarding.

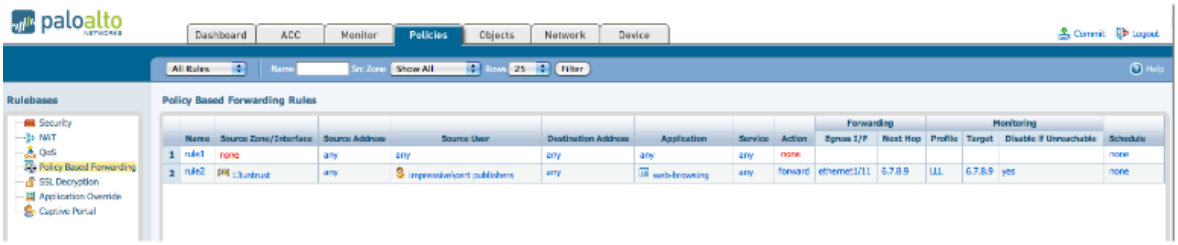


Figura 4. Ejemplo de política basada en forwarding (PBF).

En el Fortigate 60C se realizó lo siguiente:

En System > Network > Routing se crearon dos static routes para WAN1 y WAN2, los cuales son el enlace primario y secundario. En la Figura 5 se muestra un ejemplo de políticas de ruteo estático.

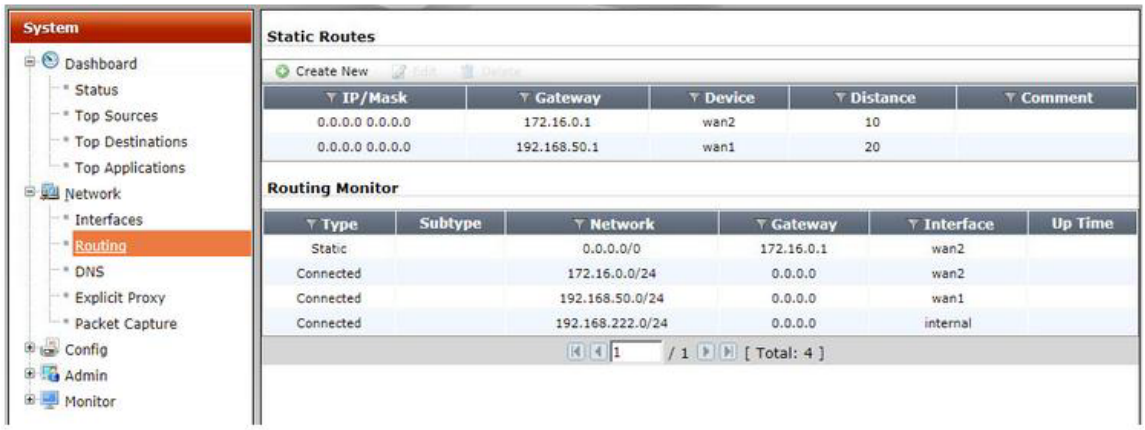


Figura 5. Ejemplo de configuración de políticas de ruteo estatico.

Después en System > Router > Settings se activa el Dead Gateway Detection, que permite monitorear la caída de alguno de los enlaces como se muestra en la Figura 6.

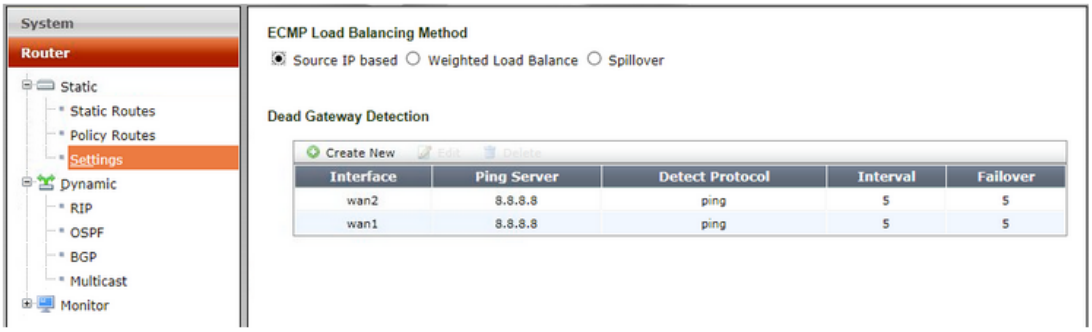


Figura 6. Ejemplo configuración de Dead Gateway Detection.

Con lo cual se logró garantizar la alta disponibilidad de los servicios de la empresa y balancear el tráfico en ambos enlaces tanto en el corporativo como en el CEDIS. Teniendo una participación al 100 %.

PROYECTO 2. Detección, corrección y prevención de vulnerabilidades

Se realizó un análisis de los servicios, infraestructura y comunicación existentes actualmente en la empresa para detectar posibles vulnerabilidades. De lo cual se derogaron sub-tareas para corregir y eliminar, como el bloqueo de puertos, eliminación de cuentas de VPN, de AD (Directorio Activo) y cuentas de correo de ex-colaboradores; reduciendo la perdida de información con valor al negocio. Se instalaron parches de seguridad en los Servidores para que permitan eliminar ataques de malware y spyware. Se configuraron nuevas políticas de salida a internet que bloqueen sitios y aplicaciones que pongan en riesgo la estabilidad e información como se muestra en la Figura 7. Se aplicó seguridad al contenido de las carpetas asignadas a cada departamento, creando grupos de distribución en el Directorio Activo para cada departamento y este fue asignado a la carpeta correspondiente, optimizando los privilegios de cada colaborador sobre los documentos existentes en ellas. Teniendo una participación en este proyecto del 100%.

Figura 7. Ejemplo de Políticas de Seguridad para la salida a Internet.

PROYECTO 3. Sanity Check de servidores y dispositivos periféricos

Para mejorar la calidad de respuesta de los servicios y aplicaciones para clientes internos y externos, se realizaron mantenimientos en unidades de disco en Servidores Físicos y Virtuales; como lo es la depuración y asignación de espacios independientes para datos, aplicativos y servicios. También se acondicionó una unidad específica para la memoria virtual (PageFile) en cada uno de los servidores para mejorar el performance como se muestra en la Figura 8.
Para evitar caídas o perdidas en los servicios y aplicativos se realizo la migración de estos a otros servidores con mejor performance. Con una participación en este proyecto del 100%.

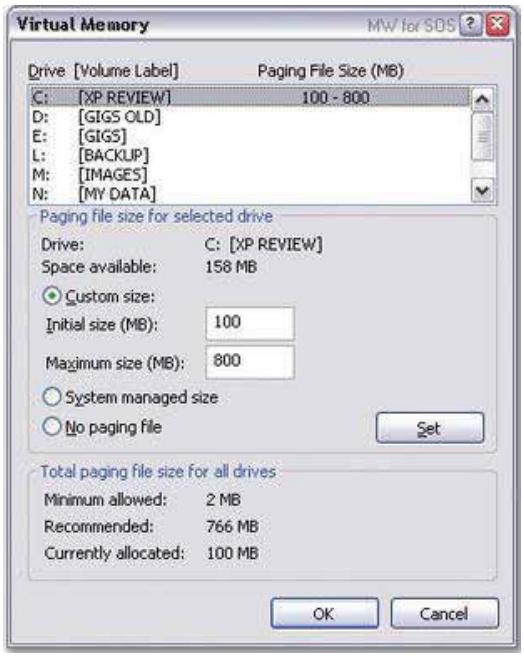


Figura 8. Ejemplo de configuración de PageFile.

PROYECTO 4. Implementación y puesta a punto de herramienta para DRP

El objetivo principal era contar con una herramienta que permitiera la recuperación de archivos, aplicativos y servidores en caso de contingencia. Se instaló una consola de Acronis la cual permite realizar el Backup and Recovery de archivos, aplicativos y servidores. En dicha consola se crearon planes o tareas para realizar los respaldos o recuperación de documentos o aplicativos, como se muestra en la Figura 9. Teniendo una participación en este proyecto del 100%.

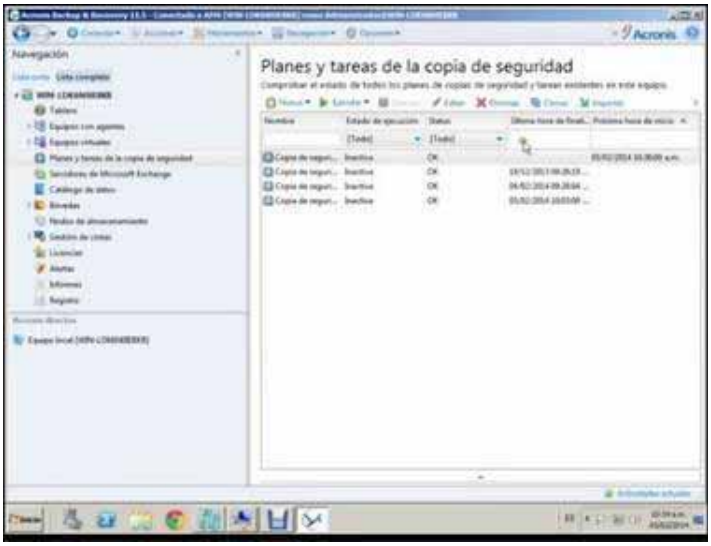


Figura 9. Consola de administración de Acronis.

PROYECTO 5. Administración y mantenimiento del software de Control de Acceso

La empresa por instrucción de RH requería la restructuración de los accesos a las diferentes áreas, es por ello que se le solicito al departamento de sistemas dar de alta nuevos niveles de accesos, registrar las credenciales de los nuevos colaboradores y dar de baja los registros de las tarjetas de ex-colaboradores. Teniendo una participación en dicho proyecto del 100%.

PROYECTO 6. Documentación de Servicios y Aplicativos

- Elaboración de inventario de Servidores.
- Elaboración de inventario de IP's privadas y públicas.
- Elaboración de inventario de accesos de VPN.
- Creación de manuales de herramientas.

Con una participación del 100% en dicho proyecto.

PROYECTO 7. Implementación, puesta a punto y administración del Portal de HelpDesk

Para mejorar la atención a solicitudes de usuarios y medir el trabajo realizado por el área de sistemas; se implementó el portal de HelpDesk dando de alta los usuarios y haciendo pruebas de solicitud para validar el flujo de la herramienta. Se crearon reportes mediante consulta de información a la base de datos para la medición de SLA, un ejemplo de ello se muestra en la Figura 10. Una vez que se valido el funcionamiento de la Plataforma se crearon manuales, uno para el uso del departamento de sistemas y otro para los departamentos restantes. También de igual forma se dio una capacitación sobre el uso de la misma.

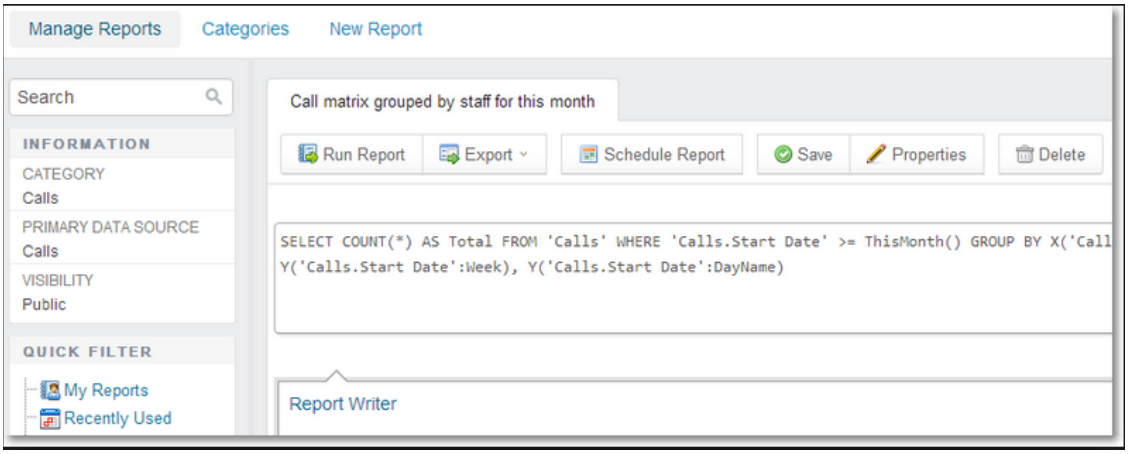


Figura 10. Ejemplo de consultas a la base de datos para la elaboración de reportes.