DISEÑO DE INFRAESTRUCTURA *IT* EN MATERIA DE REDES Y SEGURIDAD EN ENTORNO UNIVERSITARIO DISTRIBUIDO

MARIO ARENAS GARCÍA

MARIO ARENAS GARCÍA

ÍNDICE

1. Introducción

2. Oportunidad de proyecto

3. Temporización

4. Auditoría de infraestructuras
   4.1. Comunicaciones
   4.2. Seguridad
   4.3. Sistemas

5. Recogida de datos y requisitos
   5.1. Caudales de tráfico
   5.2. Número de usuarios y/o puestos
   5.3. Necesidades de comunicaciones
   5.4. Necesidades de seguridad
   5.5. Necesidades de sistemas
   5.6. Justificación de fabricantes

6. Diseño *CPD* estándar
   6.1. Diseño comunicaciones
      6.1.1. Capas 1 y 2 modelo *OSI*
      6.1.2. Capas 3 y 4 modelo *OSI*
   6.2. Diseño de seguridad
      6.2.1. Seguridad perimetral
      6.2.2. Seguridad corporativa
      6.2.3. Seguridad de puesto de usuario
   6.3. Diseño de sistemas
      6.3.1. Conectividad de los sistemas
      6.3.2. Bastionado del sistema

7. Diseño *CPD* extendido
   7.1. Diseño comunicaciones
   7.2. Diseño de seguridad
   7.3. Diseño de sistemas

8. Integración de las facultades en *CPD* extendido
   8.1. Enrutamiento dinámico
   8.2. Sincronización *DNS*

MARIO ARENAS GARCÍA

8.3. Requisitos en la política de seguridad
8.4. Sincronización de los datos

9. Funcionamiento de la solución
9.1. Flujos de tráfico: *intra-CPD* e *inter-CPD*
9.2. Balanceo global en *CPD* extendido
9.3. Pruebas de alta disponibilidad
9.3.1. CPD estándar
9.3.2. CPD extendido
9.3.3. Inter-CPD

10. Planes de contingencia
10.1. Caída *CPD* estándar
10.2. Caída *CPD* extendido

11. Mapas de red
11.1. Campus universitario
11.2. *CPD* estándar
11.3. *CPD* extendido
11.4. Balanceo global *DNS*

12. Anexos
12.1. Red *MacroLAN*
12.2. Direccionamiento
12.3. Presupuesto
12.4. Presentación
12.5. Bibliografía
12.6. Conclusiones

MARIO ARENAS GARCÍA

1. INTRODUCCIÓN

En el presente documento se da como fruto del encargo de la Universidad de las Mentes del Mañana de la construcción de una infraestructura completa *IT* en todas las facultades más el diseño de un *CPD* geográficamente extendido en dos situaciones geográficas alejadas.

El propósito del presente proyecto es dar cobertura a todas las necesidades en materia de comunicaciones, sistemas y seguridad que se presentan ante durante el trabajo diario. En las siguientes páginas se desgranará cómo llevar a cabo este diseño y las pruebas a realizar para asegurar el correcto funcionamiento de la solución.

Asimismo, no es objeto del presente proyecto presentar un diseño de solución de voz sobre *IP* o accesos inalámbricos *WiFi*. En lugar de eso, se cumplirá el requerimiento dela universidad de migrar los actuales sistemas que dan soporte a esas tecnologías dentro del contexto en que nos encontramos.

En el presente documento se citan explícitamente fabricantes tanto de productos de seguridad, como de comunicaciones como de sistemas que estarán distribuidos bien en formato software o *appliance*. La elección de estos fabricantes en concreto es fruto de mi experiencia profesional y de la comparación con otras tecnologías.

Por último, es necesario recordar de cara al presupuesto del proyecto, que los precios de los fabricantes no son públicos y por tanto serán aproximados. En el presente proyecto solo se tendrán en cuenta costes asociados a la compra de nuevo equipamiento pero no de licencias, mantenimientos, horas de trabajo, etc.

MARIO ARENAS GARCÍA

2. OPORTUNIDAD DE PROYECTO

La Universidad de las Mentes del Mañana (a partir de ahora UMM) cuenta con un conglomerado de diferentes facultades agrupadas en función de distintos criterios académicos. Dichas facultades forman un campus que está compuesto por un total de 5 edificios separados geográficamente dentro de un área metropolitana, en los cuales se desarrollan todas las tareas docentes y administrativas correspondientes a cada una de las carreras.

Por otra parte, la infraestructura IT de cada una de las facultades es competencia de cada una de los departamentos de informática de cada una de ellas sin un criterio global en cuanto a la integración, aplicaciones, administración y medidas de seguridad. Además, en este entorno se están observando cada vez más problemas operativos en la red telemática debido a la obsolescencia tanto de infraestructuras, como de falta de planes de contingencia y recuperación ante desastres.

Por lo comentado anteriormente, desde la UMM se pretende estandarizar y modernizar el modelo *IT* de cada una de las facultades para que pueda contar con las garantías y herramientas suficientes para un mejor desempeño de todas las labores. Esto implica diseñar un Centro de Proceso de Datos (en el futuro *CPD*) modelo para todas las facultades, con pequeñas variaciones en función de las necesidades de computación, para que se puedan mejorar los problemas antes comentados.

Por otra parte, el proyecto contempla la creación de dos *CPD* geográficamente dispersos, trabajando conjuntamente en modo activo-activo, que permita que, a pesar de que un *CPD* completo de una facultad pueda quedar inutilizado, estos *CPD* puedan seguir ofreciendo los servicios a esa facultad en concreto. Además de ofrecer respaldo operativo, estos *CPD* serán utilizados por equipos de investigación para aquellas labores que precisen de una capacidad de computación mayor.

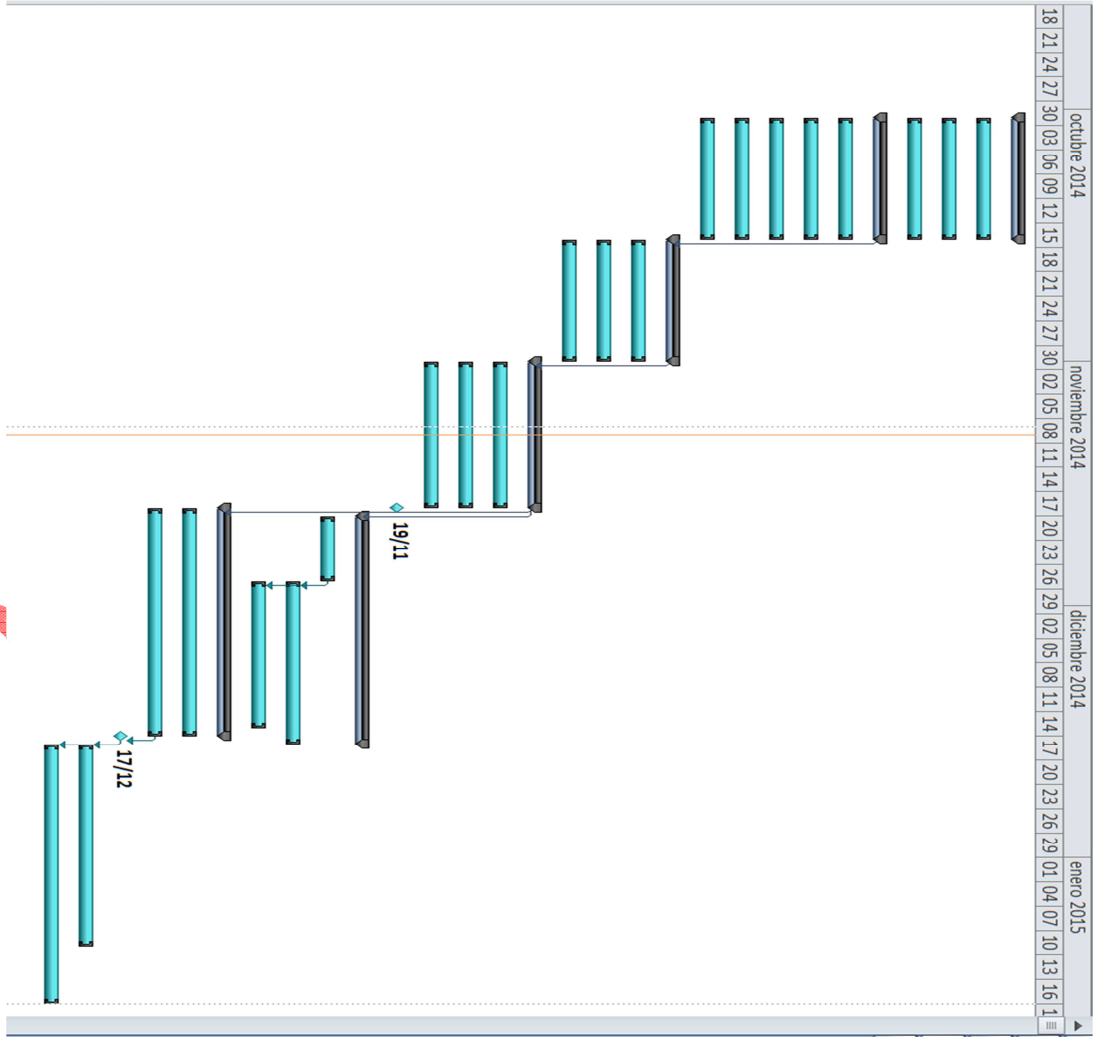
En el marco anteriormente comentado, se establecen que los principales objetivos del proyecto, pactados con la universidad en una reunión para decidir el alcance del presente proyecto, son los siguientes:

- Estandarizar la infraestructura *IT* de cada facultad.
- Diseño de *CPD* centrales en modo activo-activo.
- Interconexión de las facultades con los *CPD* centrales e Internet.
- Dotar de una seguridad acorde al tipo de datos y entorno.
- Proporcionar mecanismos de recuperación que permitan disponibilidad total.
- Dotar de equipamiento que permita a los equipos de investigación.

MARIO ARENAS GARCÍA

3. TEMPORIZACIÓN

Nombre de tarea	Duración	Comienzo	Fin
Auditoría de infraestructuras	**11 días**	**jue 02/10/14**	**jue 16/10/14**
Auditoría de comunicaciones	11 días	jue 02/10/14	jue 16/10/14
Auditoría de seguridad	11 días	jue 02/10/14	jue 16/10/14
Auditoría de sistemas	11 días	jue 02/10/14	jue 16/10/14
Recogida de datos	**11 días**	**jue 02/10/14**	**jue 16/10/14**
Caudales de tráfico	11 días	jue 02/10/14	jue 16/10/14
Número de usuarios y/o puestos	11 días	jue 02/10/14	jue 16/10/14
Necesidades de comunicaciones	11 días	jue 02/10/14	jue 16/10/14
Necesidades de seguridad	11 días	jue 02/10/14	jue 16/10/14
Necesidades de sistemas	11 días	jue 02/10/14	jue 16/10/14
Diseño CPD estándar	**11 días**	**vie 17/10/14**	**vie 31/10/14**
Diseño de comunicaciones	11 días	vie 17/10/14	vie 31/10/14
Diseño de seguridad	11 días	vie 17/10/14	vie 31/10/14
Diseño de sistemas	11 días	vie 17/10/14	vie 31/10/14
Diseño CPD extendido	**13 días**	**sáb 01/11/14**	**mar 18/11/14**
Diseño de comunicaciones	13 días	sáb 01/11/14	mar 18/11/14
Diseño de seguridad	13 días	sáb 01/11/14	mar 18/11/14
Diseño de sistemas	13 días	sáb 01/11/14	mar 18/11/14
ENTREGA PEC 2	**0 días**	**mié 19/11/14**	**mié 19/11/14**
Integración facultades en CPD extendido	**20 días**	**jue 20/11/14**	**mié 17/12/14**
Enrutamiento dinámico	6 días	jue 20/11/14	jue 27/11/14
Sincronización DNS	14 días	vie 28/11/14	mié 17/12/14
Requisitos en la política de seguridad	12 días	vie 28/11/14	lun 15/12/14
Diseño de planes de contingencia	**20 días**	**mié 19/11/14**	**mar 16/12/14**
Caída CPD extándar	20 días	mié 19/11/14	mar 16/12/14
Caída CPD extendido	20 días	mié 19/11/14	mar 16/12/14
ENTREGA PEC 3	**0 días**	**mié 17/12/14**	**mié 17/12/14**
Entrega de documentación	**18 días**	**jue 18/12/14**	**dom 11/01/15**
Presentación	**23 días**	**jue 18/12/14**	**dom 18/01/15**



4. AUDITORÍA DE INFRAESTRUCTURAS

Una de las primeras labores del proyecto es recoger aquella información útil sobre las infraestructuras actuales de cada facultad, para poder así ver, qué configuración hay actualmente en los tres puntos en los que se centrará el futuro diseño: comunicaciones, seguridad y sistemas.

Una auditoría de uno solo de los *CPD* puede ser muy costosa en tiempo y ofrecer una gran cantidad de información dependiendo del nivel de profundidad de la misma. Por eso, en los siguientes apartados se ha resumido de manera concisa las deficiencias en cada una de las materias.

4.1. COMUNICACIONES

En esta capa de la infraestructura de las facultades, comprobamos las siguientes configuraciones y/o deficiencias:

- Uso de *switches* obsoletos que en muchos casos no permiten configuración alguna.
- Utilización de *hubs* conectados tanto en la red de usuarios como en algunos puntos de redes de producción.
- No utilización de la división por redes mediante *vlan*.
- Falta de conectividad redundada en los servidores y en los propios *switches*.
- Falta de mecanismos de control de bucles en la red.
- Cableado no estructurado en ningún punto de la red (zonas de acceso, distribución y *core*).
- El balanceo de carga se lleva a cabo con dispositivos obsoletos que no permiten ciertas configuraciones necesarias.

En general, la mayoría de estas deficiencias se pueden ver en todos los *CPD* de cada una de las facultades, lo cual ofrece como resultado una red lenta, débil ante fallos y cuyo diagnóstico ante incidencias se vuelve casi imposible a este nivel.

MARIO ARENAS GARCÍA

4.2. SEGURIDAD

En esta capa de la infraestructura de las facultades, comprobamos las siguientes configuraciones y/o deficiencias:

- Utilización de mecanismos de control de accesos obsoletos: *Cisco ACL*, *IPTables*, etc.
- Falta de dispositivos de filtrado de capa 7 y de prevención de intrusos.
- Falta de una plataforma de antivirus institucional en el perímetro.
- Software antivirus obsoleto por falta de actualización de las firmas.
- Falta de control en materia de fuga o robo de datos.
- Las políticas de seguridad en los dispositivos de acceso son demasiado extensas y ofrecen agujeros de acceso a zonas sensibles de la red.
- Falta de *proxy* de navegación que controle las conexiones entrantes y salientes de acceso *web*.

Al igual que en el apartado anterior, la mayor parte de las deficiencias observadas en este apartado comprenden a todos los *CPD*. Esto produce que las facultades no sean organizaciones seguras, estén expuestas tanto al atacante externo como al interno, así como a la fuga de datos.

4.3. SISTEMAS

En esta capa de la infraestructura de las facultades, comprobamos las siguientes configuraciones y/o deficiencias:

- Falta de un estándar de sistema operativo en las redes de producción y de usuarios.
- Los puestos de usuarios no están maquetados, ni bastionados, ni están controlados por ningún agente, ni constan en ninguna base de datos de usuarios (como por ejemplo *LDAP*).
- Los servidores de producción no están actualizados ni en lo referente al sistema, ni a sus servicios, ni al aplicativo que se ejecuta sobre él.
- Los servidores de producción no están bastionados.
- Ausencia de un repositorio central de paquetes desde los que se nutran los servidores de producción sin necesidad de conectarse a Internet para actualizarse o instalar un nuevo software.
- Falta de almacenamiento suficiente tanto para las propias unidades de los servidores como para alojar copias de seguridad periódicas.
- Ausencia de política de rotado de contraseñas.

MARIO ARENAS GARCÍA

Estas deficiencias son observables también en todos los CPD que han sido auditados. Al igual que hemos visto anteriormente, estos resultados redundan en una gran facilidad de acceso al sistema, falta de funcionamiento óptimo, facilidad de robo de datos y escalados de privilegios, etc.

MARIO ARENAS GARCÍA

5. RECOGIDA DE DATOS Y REQUISITOS

En el presente apartado se mostrarán los requisitos recogidos en las distintas facultades. Estos requisitos serán uno de los elementos fundamentales a la hora de diseñar la solución, ya que en cada facultad recogeremos los siguientes datos fundamentales para el diseño:

- Caudales de tráfico.
- Número de usuarios y/o puestos.
- Necesidades de comunicaciones.
- Necesidades de seguridad.
- Necesidades de sistemas.

También es conveniente recalcar que, aunque las necesidades de cada facultad sean diferentes, es obligatorio que todas ellas cumplan una serie de estándares en las tres materias fundamentales en las que nos estamos centrando. Por tanto, puede haber diferencias mínimas, pero la filosofía de diseño será la misma.

Además, estos mismos datos servirán para dimensionar el equipamiento a elegir y para justificar en sí mismo otros aspectos del proyecto que no se tendrán en cuenta en el presente proyecto. Algunos de estos aspectos son: contratos, *SLA*, número de personas de dedicadas, tiempos de ejecución, etc.

Por último, hay que dejar claro que estos datos, aunque fundamentales, deberán ser considerados una simple base de crecimiento, es decir, debemos prever de forma aproximada el crecimiento durante los próximos años ya que es otro de los requisitos impuestos por la Universidad.

5.1. CAUDALES DE TRÁFICO

El tráfico cursado en cada una de las facultades es uno de los datos clave en la fase de diseño, ya que nos ayudará a elegir el equipamiento adecuado en cada uno de los aspectos en que estamos centrando en esta fase.

Para la recogida del caudal consumido en cada una de las facultades se han monitorizado las conexiones internas y externas para saber qué equipamiento elegir en perímetro y en la red interna, lo cual es necesario para construir principalmente la capa de seguridad.

MARIO ARENAS GARCÍA

Del tiempo de observación comentado anteriormente hemos obtenido los siguientes datos de las distintas facultades:

	INTERNET	PRODUCCIÓN
POLITÉNICA	40 Mbps	450 Mbps
QUÍMICA Y BIOLOGÍA	15 Mbps	175 Mbps
MEDICINA Y ENFERMERÍA	25 Mbps	250 Mbps
FILOLOGÍA	20 Mbps	300 Mbps
DERECHO Y EMPRESARIALES	20 Mbps	180 Mbps

El caudal medido en la conexión a Internet nos indica en cada uno de los casos los datos que se están cursando hacia otro destino del campus. Por otra parte el tráfico de producción, se refiere a los datos del entorno productivo: tráfico, web, acceso a bases de datos, *backup*, etc.

5.2. NÚMERO DE USUARIOS Y/O PUESTOS

Otro dato importante en la fase de diseño es el número de usuarios que utilizan cada una de las infraestructuras de las facultades. Este número de usuarios y/o puestos, está directamente relacionado con el consumo de recursos de todo el campus.

A priori podemos pensar que el número de puestos nos vendrá dado por el número de puestos de cada facultad, eso puede ser erróneo, ya que cada una de las facultades está dotada con acceso *WiFi*, por lo que cualquier alumno con sus credenciales podría estar conectado con su propio dispositivo.

Hipotéticamente todos los alumnos podrían estar conectados a la red *WiFi* de su facultad al mismo tiempo y utilizar los servicios de la universidad desde dichos accesos, pero como ya se ha comentado, esta plataforma tiene una infraestructura dedicada.

Pese a lo comentado anteriormente, es necesario hacer la diferenciación entre usuario y puesto de trabajo, ya que dichos puestos tienen la capacidad de generar más tráfico que los dispositivos móviles que se conecten de forma inalámbrica a la red.
Por otra parte, hay que tener en cuenta esta diferenciación a efectos de seguridad, ya que, como sabemos, los accesos inalámbricos son más vulnerables que los accesos por red cableada. Además, también es necesario implementar una infraestructura de sistemas dedicada a ello.

MARIO ARENAS GARCÍA

En este caso cada una de las facultades proporciona los datos del número de usuarios y puestos por facultad. Son los siguientes:

	PUESTOS	ALUMNOS
POLITÉCNICA	315	500
QUÍMICA Y BIOLOGÍA	150	400
MEDICINA Y ENFERMERÍA	80	300
FILOLOGÍA	130	600
DERECHO Y EMPRESARIALES	110	250

5.3. NECESIDADES DE COMUNICACIONES

Para poder concretar cuáles son las necesidades de cada una de las facultades en materia de comunicaciones, tendremos que apoyarnos en los datos del apartado anterior, en la previsión de crecimiento y en la tecnología a emplear en este caso.

Además de los datos anteriores, y para poder hacer la división de la red, contamos además con el detalle del número de los puestos de trabajo de cada departamento y servidores. En las siguientes tablas podemos ver esa clasificación:

POLITÉNICA	PUESTOS	SWITCHES
Profesores	50	2
Laboratorios	100	4
Sala ordenadores	150	4
Administración	15	1
WiFi	15	1

QUÍMICA Y BIOLOGÍA	PUESTOS	SWITCHES
Profesores	35	1
Laboratorios	50	2
Sala ordenadores	50	2
Administración	15	1
WiFi	12	1

MEDICINA Y ENFERMERÍA	PUESTOS	SWITCHES
Profesores	30	1
Laboratorios	10	1
Sala ordenadores	30	1
Administración	10	1
WiFi	10	1

MARIO ARENAS GARCÍA

FILOLOGÍA	PUESTOS	SWITCHES
Profesores	50	2
Laboratorios	10	1
Sala ordenadores	50	2
Administración	20	1
WiFi	18	1

DERECHO Y EMPRESARIALES	PUESTOS	SWITCHES
Profesores	30	1
Laboratorios	10	1
Sala ordenadores	50	2
Administración	10	1
WiFi	10	1

En el apartado WiFi únicamente se señalan los puntos de acceso que se necesitan en cada facultad para el acceso inalámbrico. Dado que no es objetivo del proyecto, en este caso nos limitaremos a dar conectividad a los equipos existentes.

Por otra parte, también hay que tener en cuenta que cada facultad dispone de varios servidores web con acceso balanceado, por lo que también se ha de tener en cuenta este dato para poder dimensionar la capa de balanceo de carga. El número de servidores por facultad es:

	SERVIDORES
Politécnica	50
Química y Biología	20
Medicina y Enfermería	10
Filología	40
Derecho y Empresariales	20

Hasta el momento hemos tenido en cuenta los requisitos de las facultades, pero es necesario tener en cuenta también, el equipamiento necesario para los dos CPD centrales. En este caso tenemos que hacer las siguientes consideraciones:

- Los accesos dispuestos para las áreas de profesores, laboratorios, sala de ordenadores, administración y *WiFi* no existirán.
- El número de servidores ha de ser mayor al de la suma de todos los servidores de las facultades debido a que el CPD extendido incluye servicios adicionales.

MARIO ARENAS GARCÍA

- El equipamiento ha de ofrecer mayores prestaciones ya que debe estar preparado para albergar todo el tráfico y todos los servicios de todas las facultades al mismo tiempo.

Con todos los datos anteriores, hacemos una recapitulación del equipamiento que es necesario aportar. Se desglosa el equipamiento que irá destinado a cada una de las facultades y a las instalaciones de los CPD centrales ya que, como se ha comentado, serán equipamientos diferentes:

	SWITCHES				
	PLANTA	DISTRIBUCIÓN	CORE	ROUTERS	BALANCEADORES
POLITÉNICA	12	2	2	2	2
QUÍMICA Y BIOLOGÍA	7	2	2	2	2
MEDICINA Y ENFERMERÍA	5	2	2	2	2
FILOLOGÍA	7	2	2	2	2
DERECHO	6	2	2	2	2
CPD EXTENDIDO	4	8	4	4	4

Para finalizar este apartado únicamente queda comentar el equipamiento elegido para este proyecto. Dados los requisitos necesarios a cumplir en esta infraestructura se ha optado escoger los *routers* y *switches* del fabricante ***Cisco*** y los balanceadores de carga del fabricante ***F5***.

5.4. NECESIDADES DE SEGURIDAD

En cuanto a las necesidades de seguridad nos vendrán dados por varios factores:

- Requisitos solicitados por la universidad.
- Cobertura para las amenazas actuales en entorno universitario.
- Volumen de tráfico a analizar.

Dado que desde el entorno de la universidad no tienen el conocimiento suficiente, los requisitos solicitados no son suficientemente concisos. En las reuniones previas al diseño del proyecto, la universidad nos hace llegar los siguientes requerimientos mínimos:

- Al menos una capa de filtrado en el acceso de los datos desde Internet.
- Firewalls de nueva generación capaces de interactuar con aplicaciones.
- Acceso a Internet controlado con proxy de navegación.
- Seguridad en el puesto de usuario.

MARIO ARENAS GARCÍA

Analizando en profundidad el entorno en el que nos encontramos vemos que es un entorno especialmente delicado en cuanto al tráfico de usuarios se refiere, es decir, los alumnos suelen utilizar distintos tipos de aplicaciones, redes sociales, navegación web, intentos de ataques internos, etc.

Por otra parte también nos encontramos en un entorno donde los datos no suponen un desafío desde el punto de vista legal. La gran mayoría de esos datos no son de especial sensibilidad legal, aunque es cierto que los datos de investigación si han de tratarse con especial cuidado.

El volumen de tráfico interno y externo recogido durante el tiempo de auditoría nos revela que no hay gran volumen de datos a analizar, por lo que seremos capaces de analizar más cantidad de datos con un equipamiento de gama media en todas las capas de seguridad.

Considerados todos los datos anteriores, y teniendo en cuenta los datos comentados anteriormente, se selecciona el siguiente equipamiento de seguridad:

	CANTIDAD
FIREWALLS	2
PROXY	2
ANTIVIRUS	*
WAF	1

Estos requerimientos serán iguales para cada una de las facultades, aunque tenemos que hacer algunas consideraciones:

- Cada facultad tendrá dos *firewalls* y *proxies* por motivos de alta disponibilidad
- Cada facultad tendrá tantas licencias de antivirus de puesto de usuario como puestos físicos haya en cada facultad.
- El firewall de aplicación web no está replicado ya que no es un elemento crítico al contar con otras capas anteriores de filtrado.

Por otra parte, en los CPD extendidos tendremos que hacer un dimensionamiento distinto, es decir, sabemos que no habrá usuarios, que tendremos datos de investigaciones propias de la universidad y que tendremos las mismas aplicaciones web dando servicio que en cada uno de las facultades.

MARIO ARENAS GARCÍA

Por tanto en el CPD extendido tendremos la siguiente relación de equipamiento para garantizar la seguridad:

	CANTIDAD
FIREWALLS	4
PROXY	2
ANTIVIRUS	*
WAF	2

Al igual que en el caso de cada una de las facultades tanto los proxies como los firewalls han sido redundados en número para proporcionar alta disponibilidad. El número de licencias de antivirus serán menos ya que esta red albergará tráfico de administración con menos puestos.

Por último, indicar que se han escogido los siguientes fabricantes para poder proteger nuestro entorno:

- *Firewalls*: ***Check Point***.
- *Proxy*: ***Blue Coat***.
- *WAF*: ***Imperva***.
- *Antivirus*: ***McAfee***.
- *Backup*: ***Veeam***.

5.5. NECESIDADES DE SISTEMAS

En último lugar en este apartado abordaremos las necesidades de la universidad de cara a este nuevo proyecto. Se verán aspectos de distinta índole como por ejemplo la conectividad, requisitos hardware, sistemas operativos, copias de seguridad, almacenamiento, *backup*, etc.

Los sistemas en producción actuales están basados en su totalidad en sistemas operativos Unix/Linux. En lugar de contar con una distribución libre, como hasta el momento están haciendo, para este proyecto se comprarán licencias de *Red Hat Enterprise* ya que de esta manera contaremos con un soporte oficial del fabricante.

En cuanto a los paquetes necesarios para el funcionamiento de las aplicaciones no es objetivo de este proyecto, por lo que se deja en manos de la universidad la decisión de los productos necesarios, así como su implementación y mantenimiento.

MARIO ARENAS GARCÍA

Continuando con los requisitos hardware, se sustituirán los servidores físicos actuales y se virtualizarán en dos servidores ***Dell*** con suficientes recursos (ver *datasheets* del punto 13.2) como para albergar todos los servidores existentes dejando margen al crecimiento futuro.

Se escoge esta opción de virtualización debido al gran ahorro de recursos que supone este método. Además, la virtualización permite poder poner al servicio de una aplicación en producción más recursos rápidamente, lo que redunda positivamente en la escalabilidad de la solución.

En cuanto al almacenamiento para los servidores de producción, hay que hacer dos distinciones:

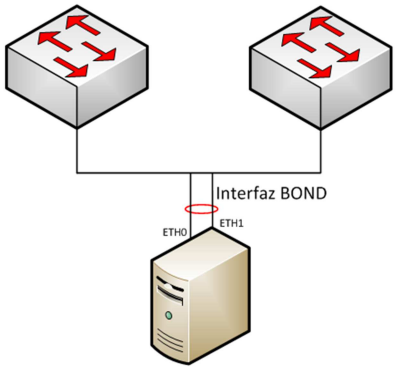
- Red *SAN*: utilizaremos este tipo de red para almacenar la aplicación de cada sistema, es decir, cada servidor ejecutará su sistema operativo desde un disco duro local, pero los datos concernientes a la aplicación y *logs* del sistema se almacenarán en una ubicación disponible mediante montaje de unidades por redes de fibra óptica directamente conectadas.
  Se estima que, de media, se necesitarán, 200 *Tb* de almacenamiento.
- Red *NAS*: utilizaremos estos recursos para poder almacenar remotamente los *backups* de las aplicaciones, sistemas, configuraciones, datos relevantes, etc. Es necesario dimensionar correctamente estos contenedores de datos, por lo que, después de hacer un estudio por facultad y estimar un crecimiento futuro, se calcula que serán necesarios al menos 500 *Tb* de almacenamiento para cubrir las necesidades de cada facultad.

Mención aparte dentro de los sistemas que estarán dedicados a las bases de datos. En este apartado contaremos con bases de datos Oracle ya que son las únicas que permiten un funcionamiento activo-activo actualmente, lo cual es necesario para acometer el diseño del CPD extendido.

Cada CPD, al igual que en el caso de los frontales de aplicación, contará con dos servidores ***Dell*** donde se alojarán todas las bases de datos que servirán a dichos frontales.
En cuanto a la conectividad de estos sistemas, dado que nos encontramos en un sistema en producción, ha de ser redundada. Esto significa que por cada interfaz de producción del servidor, tendremos que configurar un enlace *bonding* (dos interfaces físicas funcionando como una sola).

MARIO ARENAS GARCÍA

De esta forma las conexiones físicas se realizarán por duplicado hacia los *switches* de distribución directamente. Los sistemas aportarán la lógica necesaria para gestionar el tráfico que manejan a través de una u otra interfaz dependiendo de su estado. La conexión física sería de la siguiente manera:



En último lugar en este apartado reflejaremos en una tabla los servidores necesarios, así como el almacenamiento total a dotar a la universidad. Los datos se recogen en la siguiente tabla:

FACULTAD	SERVIDORES	ALMACENAMIENTO
POLITÉCNICA	2	700 TB
QUÍMICA Y BIOLOGÍA	2	700 TB
MEDICINA Y ENFERMERÍA	2	700 TB
FILOLOGÍA	2	700 TB
DERECHO Y EMPRESARIALES	2	700 TB
CPD EXTENDIDO	10	4 PB

5.6. JUSTIFICACIÓN DE FABRICANTES

A lo largo de este apartado se han hecho cálculos y dimensionamientos con cifras que nos han venido dadas por el propio proyecto o bien por estimación. Sin embargo, hay otro apartado que es necesario justificar y que hace referencia a la elección de cada uno de los fabricantes.

En primer lugar en este proyecto no se propone como reto la consecución del mismo bajo unas premisas económicas, lo cual deja libertad a la hora de poder llevar las tareas dimensionamiento y elección del equipamiento con las mejores características para este entorno.

En todos los casos se han escogido fabricantes que cumplan los siguientes requisitos:

MARIO ARENAS GARCÍA

- Gran base de equipos instalada.
- Calidad del soporte.
- Calidad de las soluciones.
- Capacidad de respuesta.
- Adecuación a estándares.
- Flexibilidad de la solución.
- Características técnicas variadas.
- Integración con otras soluciones.

En otras palabras, se han optado por fabricantes con una base de dispositivos instalada grande, que cuenten con un soporte documentado, con capacidad de respuesta en tiempo y forma correctas, es decir, desde el principio se han escogido los principales fabricantes dentro de cada sector.

Algunos de los fabricantes que se han tenido en cuenta durante el proceso de evaluación que cumplen estos requisitos son:

- **Seguridad**: los principales fabricantes de seguridad que cumplen los requisitos anteriores son:
    - *Firewall*: *Palo Alto, Check Point, Cisco ASA, Fortinet*.
    - *Proxy*: *Blue Coat*
    - *WAF*: *Imperva, Fortinet, Barracuda*
- **Comunicaciones**: los principales fabricantes del mercado que cumplen con los requisitos anteriores son
    - Enrutamiento/Conmutación: *Enterasys, Cisco* y *Juniper*.
    - Balanceo de carga: *Radware*, *F5* y *A10*.
- **Sistemas**: los principales fabricantes del mercado que cumplen con los requisitos anteriores son:
    - Servidores de procesamiento/almacenamiento: *Dell*, *HP* y *EMC*.
    - Servidores DNS: *Infoblox*.

Además de los criterios anteriores, a continuación se detalla la justificación que nos ha hecho elegir en concreto cada uno de los fabricantes elegidos:

- *Firewall*: en este caso la balanza se ha decantado por *Check Point* ya que en otros fabricantes evaluados (*Fortinet* y *Palo Alto*) no se contaba con la gestión, obtención de datos y modularidad de funcionalidades que se contaba en este.
- *Proxy*: en este caso no se han evaluado más soluciones ya que esta contaba con gran facilidad de integración y potencia de proceso.

MARIO ARENAS GARCÍA

Además, cuenta con añadidos a la función de *proxy* que enriquecen mucho la solución de seguridad (sección 9.1).

- *WAF*: en este caso la función determinante de *Imperva* frente a otros *WAF* (*Fortinet* y *Barracuda*) es que este *firewall* de aplicación es capaz de analizar, además de ataques contra *webs*, ataques contra base de datos tomando como vector la aplicación *web*.
- Balanceador: en este caso se ha elegido *F5* frente a otros competidos (*Radware* y *A10*) debido a la gran flexibilidad que nos ofrece gracias a su propio lenguaje de programación basado en scripts (*iRules*). De esta forma podremos implementar cualquier función que necesitemos.
- *Switches*: en el caso de la electrónica de red, hemos escogido *Cisco* frente a otros fabricantes (*Juniper* y *Enterasys*) gracias a su facilidad de uso (*Cisco* es considerado en muchos casos un estándar) y por su integración con la mayoría de soluciones y escenarios.
- *DNS*: en este caso se ha optado directamente por *Infoblox* ya que el resto de los competidores no ofrecían arquitectura basada en Unix/Linux y además la monitorización de URL se lleva a cabo mediante mecanismos necesarios para este entorno.
- Sistemas: en este caso se ha escogido Dell por la gran inter-operatividad con la mayoría de los fabricantes. Además, las nuevas familias de *appliances FX2* y *R730xd* proporcionan mejor rendimiento y escalabilidad en servidores pequeños.

MARIO ARENAS GARCÍA

6. DISEÑO *CPD* ESTÁNDAR

Una vez visto los requerimientos del proyecto, el estado de cada una de las facultades y las necesidades de cada una de ellas, podemos pasar a hacer un diseño de *CPD* estándar con las variaciones oportunas de equipamiento en función de cada una de las facultades.

A continuación se desglosan cada una de las capas de las áreas que comprenden este diseño. En cada una de ellas se comentará de forma generalista la solución propuesta para los *CPD*, pero a la hora de asignar equipamiento se hará distinción en cada una de las facultades.

6.1. DISEÑO DE COMUNICACIONES

En el diseño de comunicaciones tendremos en cuenta aquellos aspectos que incluyen el acceso al medio, la interconexión de los nodos clave del CPD, tipo de cableado, niveles de conmutación, balanceo de carga, enrutamiento de paquetes, direccionamientos asignados, etc.

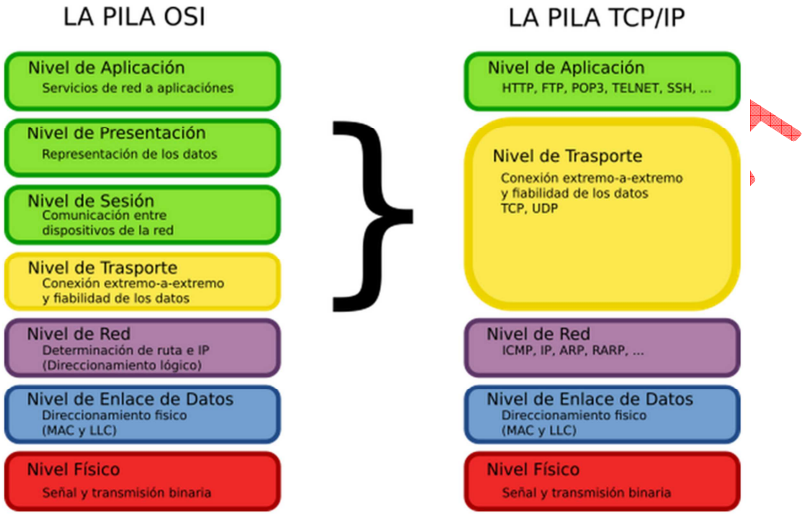
En gran medida, este diseño se basa en el modelo OSI de comunicaciones que consta de 7 capas y mediante ellas, pretende resolver la interconexión de dispositivos mediante la utilización de estándares y protocolos. El modelo OSI cuenta con las siguientes capas:

Como veremos a continuación, en este caso haremos uso de las cuatro primeras capas para seguir de forma estructurada el diseño y la

MARIO ARENAS GARCÍA

implementación del *CPD*. Por tanto, se especificaran los protocolos que sugiere dicho modelo en cada uno de los apartados.

Por otra parte, también tiene sentido hacer referencia en este caso al modelo de comunicaciones TCP/IP, que es un modelo de comunicaciones que trata de resolver los mismos problemas pero condensando las capas 4, 5 y 6 en una sola:



6.1.1. Capas 1 y 2 del modelo *OSI*

En el diseño de comunicaciones de una red, es necesario tener en cuenta tres zonas diferenciadas en la electrónica de red a efectos de equipamiento, redundancia de enlaces y funciones de cada uno de los equipos. Estos niveles son tres:

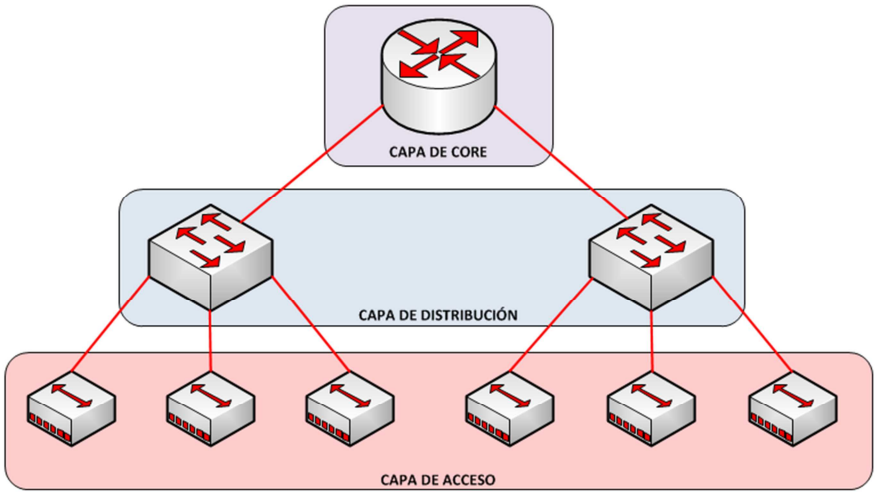
- Acceso: a esta capa de *switches* se conectarán los puestos de usuario y otros equipos finales como por ejemplo teléfonos e impresoras. Debido a que este equipamiento es el primer punto de acceso dedicado a equipos finales, no realizan prácticamente funciones avanzadas en cuanto a la conmutación de paquetes. Por tanto, esta capa hace funciones de la capa 1 del modelo *OSI* en su mayor parte.
- Distribución: esta capa de conmutación aglutina las conexiones de los *switches* de la capa de acceso y proporciona conectividad entre todos ellos. También se suelen conectar a ellos servidores de producción para proporcionar conectividad. En esta capa se suele trabajar únicamente en capa 2, por lo que es habitual encontrar

MARIO ARENAS

también agregaciones de enlace, configuraciones de *spanning-tree*, protección contra tramas *BPDU*, etc.

- Core: en esta capa se *multiplexan* todas las comunicaciones entre distintas redes. Habitualmente, esta capa es la encargada del enrutamiento dentro de la red, tanto estático o dinámico. Es habitual conectar a ellos otros equipos de comunicaciones que, a su vez, también son capaces de *enrutar* tráfico o bien, son equipos importantes en el contexto de la red, como por ejemplo, los *firewalls*.

De forma gráfica, tendríamos que, la estructura de acceso que acabamos de detallar sería la siguiente:



Aunque en el diagrama anterior no se reflejan, en la capa de distribución se crean canales de comunicación en los *switches* (*port-channel*) para poder comunicar los equipos finales conectados a los diferentes *switches* de acceso. También es posible que contemos con conexiones redundadas de ciertos servidores por lo que también será necesario crear agregaciones de enlace simples y multichasis.

Al igual que en el caso anterior, el diagrama no reflejan la redundancia de máquinas en la capa de *core*. A cada uno de los nodos pueden llegar conexiones de distintas máquinas o conexiones redundantes de una misma máquina (por ejemplo, un *bonding* de un servidor), por lo que es necesario igualmente configurar agregaciones de enlace y *spanning-tree*.

De cara a cablear la red de forma estructurada, seguiremos una política extendida llamada cableado estructurado, que no es más que un

conjunto de normas para ordenar el cableado de forma lógica para mantener el orden dentro de la red y evitar así bucles, incidencias en la red, desorganización en los armarios de comunicaciones, descontrol de los equipos conectados, etc.

En este sentido la normal del cableado estructurado nos define a su vez dos tipos de cableado diferente y que delimita el modo de empleo dependiendo de la zona de la red en la que nos encontremos:

- Cableado horizontal: la norma TIA/EIA-568A rige las normas de cableado desde la capa de acceso hasta la capa de distribución.
- Cableado vertical: es la zona de cableado que comprende entre la capa de acceso y la de distribución, y entre esta y la de *core*.

Teniendo en cuenta todo lo mencionado anteriormente, el inventario de usuarios y puestos de trabajo de cada una de las facultades del punto 5.2, el dimensionamiento de comunicaciones llevado a cabo en el apartado 5.3 y la agrupación de máquinas en vlan, llevaremos a cabo la planificación de las conexiones de forma genérica de las máquinas de la red de cada una de las facultades (punto 12.1.1).

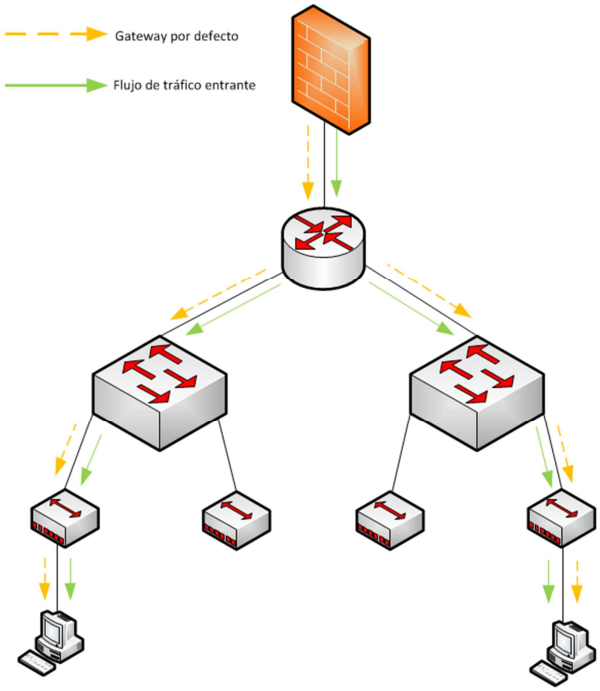
6.1.2. Capas 3 y 4 del modelo *OSI*

En este apartado veremos en detalle cuáles serán los mecanismos de enrutamiento utilizados en cada facultad. También tendremos en cuenta especialmente la capa de balanceo de carga donde se hará la redirección de tráfico a los frontales web.

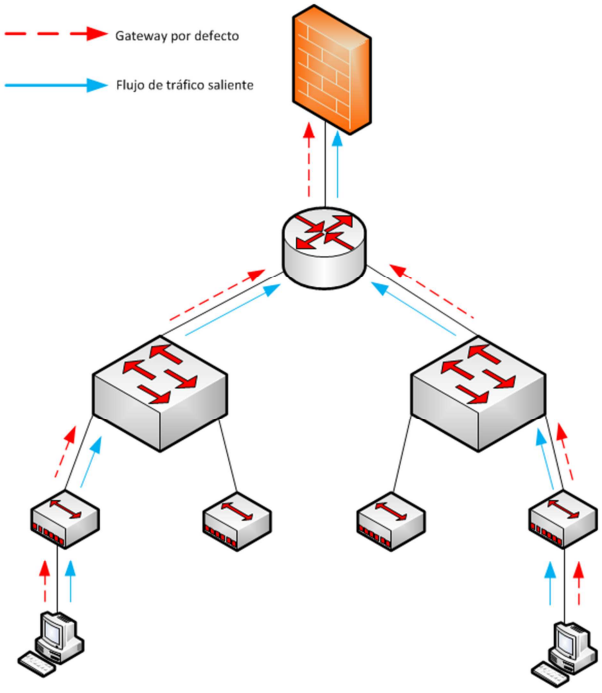
Si tenemos en cuenta en primer lugar la capa de enrutamiento, veremos que la estructura de los *CPD* no es especialmente compleja, por lo que se opta por utilizar enrutamiento estático en todas las capas de los *CPD* de cada facultad.

Si recorremos desde el punto inicial de la comunicación, el puesto de usuario o servidor, hasta el punto final de la comunicación, a efectos de nuestro *CPD*, podremos ver que la comunicación se puede resolver mediante sucesivas rutas por defecto al elemento del siguiente nivel.

MARIO ARENAS GARCÍA



Si recorremos el camino inverso, es decir, el camino que tendrían que recorrer los distintos paquetes para llegar a las redes internas (tanto de producción, como de usuarios) vemos que mediante el mismo mecanismo podemos publicar nuestros recursos al exterior.



Por otra parte hemos de tener en cuenta que, en lo tocante al diseño de la capa 3, hemos de dimensionar el direccionamiento que se le asignarán a cada una de las redes y/o *vlan* dentro de cada red en cada una de las facultades.

Para poder llevar a cabo este dimensionamiento, hay que tener en cuenta cuántos puestos de usuario y cuántos servidores y elementos de electrónica de red tenemos en cada una de ellas. En la tabla del apartado 12.4 veremos el direccionamiento de cada *CPD*.

6.2. DISEÑO DE SEGURIDAD

En el diseño de seguridad de los CPD tendremos en cuenta aspectos que involucran los accesos internos y externos, detección y prevención de intrusos, emulación de amenazas, filtrado de contenido, prevención de fuga o robo de datos, antivirus, etc.

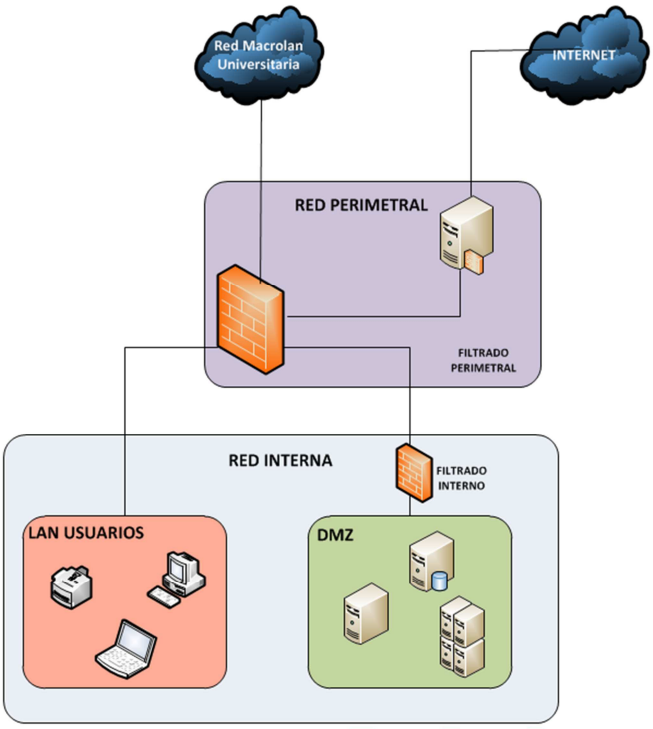
Como veremos más adelante, hemos dividido el diseño en materia de seguridad en dos apartados diferenciados: seguridad perimetral y seguridad interna. En ambos casos tendremos en cuenta diferentes cuestiones sin asumir de antemano, que el tráfico interno está libre de amenazas.

Al hacer la distinción anterior es necesario introducir una nueva zona de seguridad que estaría dentro de la zona interna: zona desmilitarizada (*DMZ*). Esta zona será donde estén ubicados nuestros servidores de producción, por tanto, hemos de tener especial cuidado a la hora de protegerla.

En nuestro caso, la *DMZ* de nuestra red está protegida por varios mecanismos de acceso, que, a su vez, realizan varias funciones de filtrado. Dado que el acceso desde Internet es potencialmente más peligroso, se han puesto medidas adicionales utilizando un sistema de filtrado adicional (*proxy*).

A modo ilustrativo, vemos en el siguiente esquema las zonas de seguridad más importantes a las que nos referiremos en lo sucesivo:

MARIO ARENAS GARCÍA



Por último, hay que señalar que el diseño de seguridad de una organización puede ser muy amplio y abarcar desde un simple bit hasta el responsable legal de un documento concreto pero, en nuestro caso, solo nos centraremos en la seguridad en las comunicaciones y sistemas en producción.

6.2.1. Seguridad perimetral

Por seguridad perimetral entendemos aquellas medidas de protección que eliminan la gran mayoría de los ataques dirigidos contra nuestra red en el punto más externo de la misma. Es recomendable que esta capa cuente con varios filtros y/o motores de análisis de amenazas.

En esta capa han de pararse prácticamente la totalidad de dichos ataques ya que, aunque en la capa interna contamos con medidas de seguridad adicionales, es el punto donde contamos con equipamiento más potente y específico.

Tal y como se puede observar en el plano de red de una facultad, en el perímetro contamos con dos sistemas de seguridad que serán los encargados de detener esas amenazas y limpiar aquel tráfico que sea susceptible de ser limpiado.

Como vemos, contamos con un firewall como único punto de entrada, pero antes de que el tráfico llegue al CPD, también hemos hecho uso de

MARIO ARENAS GARCIA

un proxy con funciones avanzadas, para la detección de amenazas en la navegación por Internet.

En primer lugar estudiaremos las funciones llevadas a cabo por el firewall:

- Filtrado de *URL*: en principio contamos con una base de datos de *URL* multicategorizada de varios miles de entradas los cuales, pueden ser utilizados para filtrar los accesos a lugares no deseados: pornografía, seguridad informática, juegos, redes sociales, etc…en nuestro caso filtraremos, además de los lugares inapropiados, aquellos que tengan que ver con juegos, redes *P2P*, *VoIP*, anonimizadores de tráfico y contenido multimedia *streaming* por Internet.
- Control de aplicaciones: actualmente las aplicaciones utilizan puertos de comunicación que típicamente han sido "propietarios" de otros protocolos. Por eso, es necesario que nuestro dispositivo sea capaz de identificar las aplicaciones que intercambian datos entre dispositivos. Hay más de 240000 aplicaciones y *widgets* soportados, por lo que, para los alumnos, no estará permitida ninguna aplicación que pueda quedar fuera de lo académico.
- Prevención de intrusos: la prevención de intrusos estará enfocada hacia las redes de producción. Por ello que tenemos que hacer recuento del tipo de sistemas, aplicaciones, protocolos, etc…que tenemos en estas redes y activemos todas las firmas y patrones relacionados. Por otra parte, contamos con un perfil de protección por defecto cuya configuración es óptima para muchos escenarios. En nuestro caso la utilizaremos de base para luego retocarla y mejorar la protección.
- Redes privadas virtuales: el firewall también hará de terminador de túneles, ya que eso nos da una doble funcionalidad. Por un lado es posible establecer *VPN* entre los *CPD* de facultades y el *CPD* extendido para poder intercambiar datos confidenciales de forma segura. Por otro lado será la forma en que se conecten los profesores e investigadores de forma externa a la universidad. Para los alumnos se proporcionará un acceso *VPN-SSL*, que es ofrece la misma funcionalidad con menor coste de recursos.
- Prevención de fuga de datos: como ya hemos comentado anteriormente, los datos son el activo más importante de una organización, por tanto utilizaremos el firewall para firmar

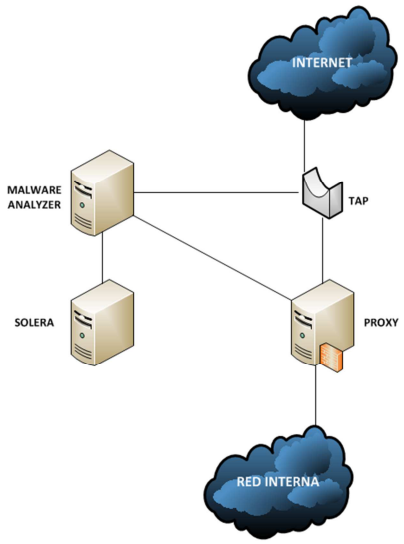
MARIO ARENAS GARCÍA

aquellos documentos confidenciales para que no puedan salir de la red. Le especificaremos que los datos tanto de las bases de datos como los que se guardan en el almacenamiento, no han de poder enviarse fuera de la red mediante ninguno de los protocolos que nos permite: *FTP*, *HTTP* y *SMTP*.

- Gestión de Identidades: la gestión de identidades dentro del entorno universitario se basará en la integración del firewall en la base de datos de usuarios institucional (directorio activo). De esta forma podremos gestionar usuarios por sus propios nombres de forma que la identidad de los usuarios queda registrada de forma unívoca y podemos localizarlos en caso de haber cometido algún acto potencialmente peligroso.
- Prevención de amenazas: la prevención de amenazas es una funcionalidad que cuenta a su vez con otras tres: antivirus, *antibot* y emulación de amenazas. Las dos primeras están basadas en firmas y en el comportamiento, pero la tercera es una técnica novedosa. Cuando se envía un fichero analizaremos el contenido y, si no se encuentra nada sospechoso, podemos simular su ejecución para comprobar si contenía una amenaza no contemplada en las firmas.

Por otra parte contamos con un proxy que está configurado en modo explícito para las peticiones internas, e implícito para las externas. Tiene una doble función: proteger a los usuarios de la navegación y proteger la entrada de peticiones malintencionadas hacia nuestra plataforma web.

Para entender el filtrado es necesario desarrollar gráficamente cuáles serían las máquinas implicadas:



MARIO ARENAS GARCÍA

La función de cada una de las máquinas es:

- *TAP*: este sencillo dispositivo de red se encargará de recibir el tráfico de Internet y, el que esté cifrado, lo copiará directamente a su salida para que llegue al *proxy*. También copia el tráfico hacia el *Malware Analyzer* para que analice el tráfico cifrado por *SSL* hacia nuestra red. A priori, puede parecer que es un punto de fallo en la red, pero el equipo está preparado para cortocircuitarse internamente incluso sin alimentación externa por lo que dejaría pasar todo el tráfico.
- *Proxy*: además de las funciones habituales de un proxy convencional, el proxy elegido en este caso puede inspeccionar el tráfico que no esté cifrado mediante tres motores distintos de detección de amenazas. Contará con el apoyo de un analizador de malware que se encargará de descifrar el tráfico y analizarlo de la misma manera que lo hace este con el tráfico en claro, por lo que, en la primera capa de acceso desde Internet contamos con una protección óptima.
- *Malware Analyzer*: este dispositivo se encargará de recibir el cifrado de Internet y su misión será, con el certificado de la aplicación dentro de sus repositorio, analizar si el tráfico contiene algún tipo de malware analizándolo con dos motores distintos. Si se produce alguna detección, indicará al proxy que rechace la conexión y, al mismo tiempo, enviará una alerta al *appliance* de monitorización (*Security Analytics*), para que podamos investigar sobre el problema detectado.
- *Security Analytics*: es la consola donde recibiremos todos los eventos de seguridad enviados tanto por el proxy como el *Malware Analyzer*. En esta consola podremos correlar ambos *logs* y detectar aún más amenazas que, a priori y por sí solas no lo parecían. Además, y como ventaja opcional, podemos enviarle *logs* (bien por *syslog*, *snmp*, etc…) de otros sistemas para que, conjuntamente con los que ya tiene, pueda de nuevo correlarlos y ver un vector de ataque de otra forma no podría detectarse.

Como vemos, contamos con dos sistemas sólidos a la entrada de cada uno de los CPD, con varios motores y sistemas de inspección tanto a la entrada como a la salida lo que, sumado a la seguridad interna de la red, debería hacer de esta una red muy segura.

MARIO ARENAS GARCÍA

6.2.2. Seguridad interna

Por seguridad interna, entenderemos todo el conjunto de mecanismos localizados en varios puntos de la red y los sistemas, que eliminen aquellas amenazas que no hayan sido descubiertas por los sistemas de seguridad perimetral.

Es muy habitual en todo tipo de redes y organizaciones que, al margen de que haya una buena política de seguridad implantada, pueda haber agujeros de seguridad por no controlar debidamente los puestos de los usuarios y los servidores.

Asuntos como falta de parcheado del sistema operativo, falta de firewall de host, conexión de dispositivos externos, usuarios malintencionados, etc…hacen que dentro de la red también se produzcan también ataques con los que hay que tener especial cuidado.

Abordaremos por tanto la seguridad dentro de los equipos de usuario final así como la seguridad en los servidores de producción sin olvidar aquellos dispositivos dedicados a seguridad con los que contamos dentro de nuestra red (*WAF*):

- Puesto de usuario: los equipos finales han de ser controlados tanto para que los usuarios no escalen privilegios dentro del mismo sistema, como para contar con un grupo de herramientas para su seguridad interna. Para ello contamos con una de las funcionalidades de control de punto final de *Check Point*. Mediante esta centralización de la seguridad del puesto final podremos controlar procesos, firewall, antivirus, dispositivos externos, etc…que estén presentes en el sistema.
- Servidor corporativo: los servidores han de estar bastionados, es decir, securizados desde sus configuración inicial contra accesos no deseados, escalados de privilegios, ataques por fuerza bruta, etc…para ello es conveniente instalar un *firewall* de servidor, restringir los usuarios e *IP* que pueden conectarse al sistema, contar con un parcheado actualizado y diseñar un sistema de enjaulado de usuarios que no afecte al sistema a pesar de que ejecute un posible atacante sobre el mismo.
- *WAF*: el firewall de aplicaciones web que hemos situado antes del acceso a los frontales web, es un dispositivo que no solo descubre la lógica y circuitos de una aplicación identificando

MARIO ARENAS GARCÍA

dinámicamente los nuevos cambios en la misma, sino que es capaz de parar ataques específicos dirigidos contra dichos entornos. Además, también es capaz de ver si una consulta de un frontal web a un servidor de base de datos es potencialmente peligrosa.

- Backup: es uno de los mecanismos más importantes a la hora de preservar la integridad de la información. Contaremos con una plataforma de *backup* para las redes de producción cuya política de es hacer una copia de seguridad semanal completo de los servidores y otra incremental diaria, de forma que siempre tendremos a salvo nuestros datos. Dichos datos serán mantenidos, al menos, el tiempo indicado por la *LOPD* y como máximo, el tiempo que sea necesario para la organización.

Como vemos, tenemos controlados los puntos con mayor riesgo dentro y fuera de la red y, aunque es cierto que hay mecanismos adicionales a los aquí expuestos, no es necesario implantar un nivel de seguridad mayor debido al entorno en que nos encontramos.

6.3. DISEÑO DE SISTEMAS

El diseño de los sistemas que prestan servicio en un entorno de producción puede ser muy complejo, puede contemplar aspectos como: permisos, usuarios, grupos, repositorios de software, conectividad, funcionalidades, esquema de directorios, etc…

En nuestro caso, de entre todos los posibles aspectos, tendremos en cuenta fundamentalmente la conectividad e integración de los mismos dentro del CPD y, a grandes rasgos, las funciones que desempeñarán cada uno de ellos y su interrelación.

En principio, y desde el punto de vista de las redes de producción de nuestros CPD, contaremos con tres tipos de sistemas: frontales web, bases de datos y servidores de almacenamiento masivo. Serán los sistemas más importantes y por tanto hay que hacer especial mención.

Por otra parte contamos con otro tipo de sistema que, aunque no puede considerarse dentro de la red de producción, sí que ofrece un servicio a la misma, es decir, se encarga de traducir los nombres en direcciones IP. Estos servidores de nombre (DNS) son fundamentales en nuestro entorno.

MARIO ARENAS GARCÍA

En general, los sistemas estarán alojados en potentes servidores de virtualización que soportarán varias decenas de servidores ejecutándose al mismo tiempo. Podremos escalar sus recursos hardware fácilmente y sustituirlos de la misma manera por lo que es la mejor fórmula.

Estos sistemas dependerán a su vez del almacenamiento ya que, por defecto, el sistema operativo de cada máquina estará ejecutándose en el servidor físico en el que están alojados, pero los datos de aplicación, logs y copias de seguridad se almacenarán en ubicaciones distintas.

6.3.1. Conectividad de los sistemas

En este apartado nos centraremos especialmente en cómo hemos de conectar los sistemas para poder contar a nivel de red con redundancia ante fallos. Hay muchas configuraciones posibles que implican a sistemas y a la capa de comunicaciones.

Abstrayéndonos de la capa física, es decir, los servidores físicos en los que se alojarán los servidores virtuales de producción ejecutarán el sistema operativo localizado en los propios discos del servidor físico donde estén localizados.

Por otra parte todos los datos concernientes a los datos de las aplicaciones, *logs* y volcados de memoria estarán almacenados, como antes comentamos, en servidores de almacenamiento masivos bien mediante una red *NAS* o *SAN*.

La diferencia de estas redes es que la red *SAN* es una red con conexión directa al servidor físico (sin pasar por ningún elemento intermedio de comunicaciones) por fibra óptica para que el trasiego de datos sea rápido y la respuesta del sistema adecuada.

Por otro lado, la red *NAS* es una red que conectará directamente, sin mediación de la electrónica de red, con los servidores de producción con un almacén o repositorio de datos de datos masivo corporativo dentro de la red.

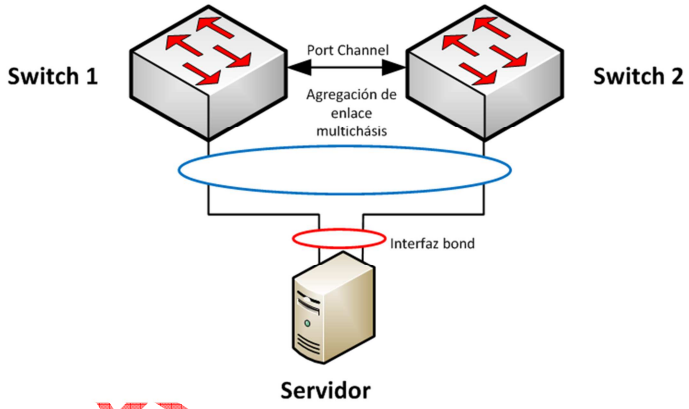
En cuanto a la conexión de los sistemas a la infraestructura de comunicaciones para dar servicio, se ha tenido en cuenta la tolerancia a fallos, es decir, cada uno de los sistemas tendrá una doble conexión en activo-pasivo.

MARIO ARENAS GARCÍA

Esta conexión, que también ha de ser configurada en los *switches* del mismo modo, permitirá que los sistemas se comuniquen con el resto de dispositivos mediante una interfaz principal con la otra a la espera en modo pasivo.

Si se produjera un fallo del interfaz del servidor y/o del *switch*, automáticamente el tráfico pasaría a cursarse a través del otro interfaz configurado pudiendo preservar de esta forma el servicio sin ningún corte o interrupción.

Como vemos en el gráfico a continuación, el servidor en cuestión se conectaría a dos *switches* con cada una de las interfaces en los modos descritos. De esta manera también tendremos redundancia ante la caída de un *switch* completo no solo de un puerto.



Por último comentar que, como ya dijimos en el apartado de comunicaciones, dentro de los CPD no tenemos ningún protocolo de enrutamiento dinámico, por tanto, habrá que configurar rutas estáticas en los sistemas.

6.3.2. Funciones de los sistemas

A lo largo de los apartados anteriores hemos estado hablando de sistemas de forma general, pero es necesario hace distinción de qué tipo de sistemas nos encontraremos típicamente en cualquier red, y en todos los CPD.

Dividiremos la función de los diferentes sistemas que tenemos en producción en seis categorías:

- Frontal web: estos sistemas están basados en un sistema operativo *Unix*/*Linux* y un servidor web instalado que hace de nexo con la aplicación que da servicio.
- Base de datos: este tipo de servidores almacenan la información propiamente dicha, es decir, son el almacén de datos de donde se nutrirán todas las aplicaciones.
- Almacenamiento: sistemas con gran cantidad capacidad de almacenaje de datos. Estos pueden ser de cualquier naturaleza: documentos, *backups*, software, etc.
- DNS: servidor de nombres es un servidor que traduce las direcciones *web* y los nombres *NETBIOS* en direcciones *IP*. Será un *appliance* dedicado.
- Directorio Activo: servidor ejecutando un sistema operativo Microsoft Windows cuya función principal es mantener una base de datos de usuarios y grupos de la organización.
- Servidor de hora: este servidor proporciona hora a todos los componentes de la red mediante el protocolo NTP. La sincronización horaria es crítica para los sistemas en producción.
- Puesto de trabajo: en este caso nos estamos refiriendo al puesto de usuario final. El sistema operativo soportado por la universidad es *Microsfot Windows* 7.

En definitiva vemos que tenemos gran variedad de sistemas y cada uno de ellos tiene su propia función. Podríamos haber hablado de otros como por ejemplo, todo lo relacionado con la voz sobre *IP* o sobre los accesos *WiFi*, pero quedan fuera del alcance del proyecto.

6.3.3. Jerarquía DNS

Dentro del diseño de la arquitectura de este modelo distribuido, se hace vital tener en cuenta la configuración y la interrelación entre los *DNS* dentro de cada uno de los *CPD* y los del *CPD* extendido, ya que contamos con un modelo de balanceo global por *DNS*.

Tener una conmutación de servicios, o balanceo global, por *DNS* significa que, a nivel de servicios, podemos hacer que el tráfico sea dirigido hacia uno u otro *CPD* dependiendo de si se observan problemas en los mismos.
En primer lugar tendremos dos servidores *DNS* en cada uno de los *CPD* centrales que serán los *DNS* primarios, en cuanto al manejo de zonas

MARIO ARENAS GARCÍA

directas de resolución de nombres se refiere. Por otro lado los, *DNS* de cada *CPD* de facultad serán los secundarios.

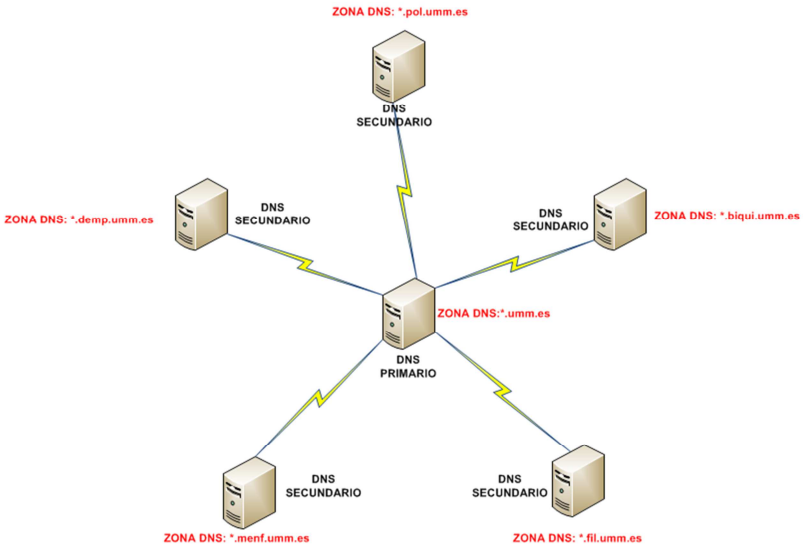
Dentro de toda la infraestructura IT de la universidad tenemos las siguientes zonas de resolución *DNS*:

FACULTAD	ZONA DNS
POLITÉCNICA	*.pol.umm.es
BIOLOGÍA Y QUÍMICA	*.biqui.umm.es
FILOLOGÍA	*.fil.umm.es
DERECHO Y EMPRESARIALES	*.demp.umm.es
PCPD EXTENDIDO	*.umm.es

Por otra parte, la configuración de los puesto de usuario en cuanto a los *DNS* se refiere será distinta, ya que todos tendrán configurado como primario el *DNS* de su red, y como secundario los *DNS* situados en el *CPD* extendido.

Esto quiere decir que, cuando un usuario o sistema necesite resolver un nombre (bien un nombre de red o bien un nombre de *URL* de un servicio en producción), consultará a su *DNS* local y en caso de no tener respuesta este la reenviará a los *DNS* del *CPD* extendido.

Gráficamente, podemos ver como estarían jerarquizados los servidores *DNS* de la universidad:



Aunque se comentará en detalle más adelante en los apartados 7.2, 8.2 y 8.3, es evidente que para poder hacer una conmutación mediante

MARIO ARENAS GARCÍA

balanceo por *DNS*, debe de haber cierta configuración específica tanto en los balanceadores como en los servidores *DNS*.

MARIO ARENAS GARCÍA

7. DISEÑO *CPD* EXTENDIDO

A la hora de comenzar a diseñar el *CPD* extendido que dará servicio a toda la universidad en caso de caída de las facultades, se puede aplicar todo lo comentado anteriormente en el diseño de los *CPD* estándar, aunque en cada caso hay que hacer algunas puntualizaciones o cambios.

Como es obvio, uno de los mayores cambios serán a nivel de comunicaciones, ya que desde el propio direccionamiento, hasta el enrutamiento (que seguirá siendo estático dentro del *CPD*), cambiarán. Este es uno de los requisitos más importantes a la hora de extender las comunicaciones.

En materia de seguridad tampoco habrá grandes cambios, aunque sí que hay que tener en cuenta algunas consideraciones que pueden repercutir en el rendimiento final de la solución. Como avance, comentar que los *cluster* de los elementos de seguridad estarán extendidos a ambos *CPD*.

Al igual que en los casos anteriores, no habrá cambios significativos en la filosofía de diseño de los sistemas y del funcionamiento de los mismos. Habrá que tener en cuenta algunas peculiaridades en cuanto a la sincronización de datos entre máquinas de distintos *CPD* se refiere.

Por último, comentar que solo se especificarán y justificarán aquellos cambios que sean de interés dentro del entorno de este CPD en concreto. Como base se tomarán conceptos mencionados en apartados anteriores y, a partir de ahí, se construirá esta solución.

7.1. DISEÑO DE COMUNICACIONES

El diseño de las comunicaciones es el mayor desafío dentro del CPD extendido. Para ello, nos apoyamos en los conceptos anteriormente explicados en los apartados correspondientes dentro del diseño de los CPD de las facultades ya que, en esencia, se trata de dos CPD iguales a los anteriores interconectados.

El diseño de interconexión entre los puestos finales y su primer acceso no cambia, aunque bien es cierto que este tipo de conexiones será menos habitual en este entorno ya que no contaremos con tantos equipos de cliente final como en las facultades.

En cuanto a las conexiones hacia la capa de distribución, tampoco habrá ningún cambio, aunque en este caso sí que conectaremos todos los sistemas, a

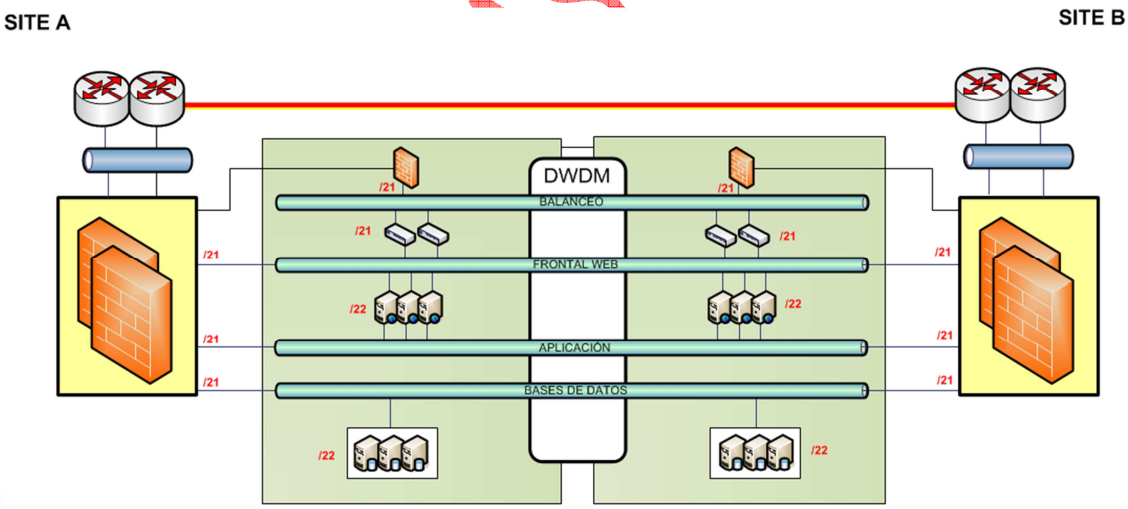
MARIO ARENAS GARCÍA

excepción de los firewalls, a esta capa de comunicaciones. La redundancia de conectividad entre estos *switches* se mantendrá igual.

Las conexiones con la capa de *core* tampoco sufrirán cambios. Estos elementos, al igual que los anteriores, no estarán extendidos de forma lógica, sino que cada *CPD*, a este nivel, se mantendrá independiente. Para la extensión de redes contamos con *switches DWDM*.

Sin embargo, hay una capa de comunicaciones que sí se ha de verse alterada; es la capa 3 que hace referencia al direccionamiento *IP*. Dado que ambos *CPD* estarán funcionando como uno solo, tanto los *firewalls*, como los balanceadores deberán poder tener conectividad directa.

Esta visibilidad se consigue mediante la configuración de una red con una máscara que englobe el direccionamiento de ambos *CPD*, es decir, que los *firewalls* y balanceadores puedan comunicarse dentro de la misma red con frontales, balanceadores, *BBDD*, etc…de cada *CPD*.



Los equipos elegidos para llevar el peso de la comunicación ya que serán aquellos que mayor interacción tengan en el entorno productivo, y por tanto, mayor conocimiento han de tener del estado de la red y de los componentes que la forma para tomar decisiones de conmutación de conexiones.
Dicho lo anterior, vamos a justificar el porqué de esta decisión:

- <u>*Firewalls*</u>: en el diseño del *CPD* extendido, los *firewalls* formarán un *cluster* de 4 miembros y no de 2 como en los *CPD* de las facultades. Esto es así por razones de redundancia y sincronización de sesiones, ya que si uno de los *CPD* cae, los *firewalls* del otro pueden seguir con el

flujo de tráfico hacia cualquier frontal de la aplicación seleccionada automáticamente.

Al mismo tiempo, los *firewalls* serán la puerta de enlace por defecto de muchos sistemas por lo que si un sistema de uno de los *CPD* necesita conectarse con otro sistema localizado en el otro *CPD*, será el *cluster* de *firewalls* el que deba conocer el enrutamiento entre los *CPD* para que dicha comunicación se produzca.

- Balanceadores: como ya sabemos, estos equipos se dedican a repartir el tráfico entre servidores que cumplen una misma función. Para que ese reparto pueda producirse entre ambos *CPD* de forma equitativa y nos aproximemos lo más posible a un reparto equitativo, es necesario que los balanceadores puedan repartir conexiones entre los distintos frontales web de ambos *CPD*.

  Por otra parte, estos balanceadores también se encontrarán configurados en *cluster* por lo que si uno de estos cae, otro del mismo *CPD* puede asumir su carga. Si cayeran dos, podrían asumir la carga los balanceadores del otro *CPD* ya que estos tendrán configurada una máscara de red cuya visibilidad se extienda a todos los frontales *web*.

La configuración de las máscaras de red y el cambio de direccionamiento no será completo, es decir, han sido diseñados para que, en caso de tener que apagar un *CPD* de una facultad, los servidores migrados sigan manteniendo la misma dirección IP pero con una máscara distinta.

Al igual que en el diseño de cada uno de los *CPD*, se ha especificado dentro de la tabla de direccionamiento del apartado 12.4 la máscara que le correspondería a los equipos de comunicaciones, seguridad y sistemas la máscara de red que le correspondería dentro de este *CPD*.

Como fruto de las necesidades de los sistemas de mantenerse sincronizados, al igual que los *firewalls* y balanceadores, tendrán sincronizadas tanto las sesiones de usuarios que interactúan con una aplicación (mediante la configuración de *cluster* de servidores) como de la propia información del sistema.

Por tanto, hay que mencionar que necesitamos crear tres redes extendidas que no aparecían anteriormente:

- Red *Vmotion*: esta red es necesaria para el movimiento lógico de máquinas virtuales desde un CPD a otro. Mediante esta red, los servidores físicos sincronizarán su estado en cuanto a rendimiento y permitirán mover máquinas por una red dedicada de un CPD al otro.

MARIO ARENAS GARCÍA

- Red *Interconnect*: esta red extendida estará dedicada a las conexiones de los servidores de BBDD. Debido a que las BBDD también estarán funcionando en activo-activo, han de tener sus tablas sincronizadas para lo cual, utilizarán esta red dedicada.
- Red de almacenamiento: puesto que todos los sistemas en de producción estarán extendidos y sincronizados, es lógico que este sistema de soporte a los sistemas de producción también lo esté. Mediante esta red aseguramos el acceso al almacenamiento en cualquier *CPD*.

Por último, comentar que en cuanto a los direccionamientos solo hay una diferencia notable. Las redes de enlace entre los *switches* y/o *routers* con los balanceadores y los *firewalls* no se pueden mantener ya que en cada *CPD* es una red distinta.

7.2. DISEÑO DE SEGURIDAD

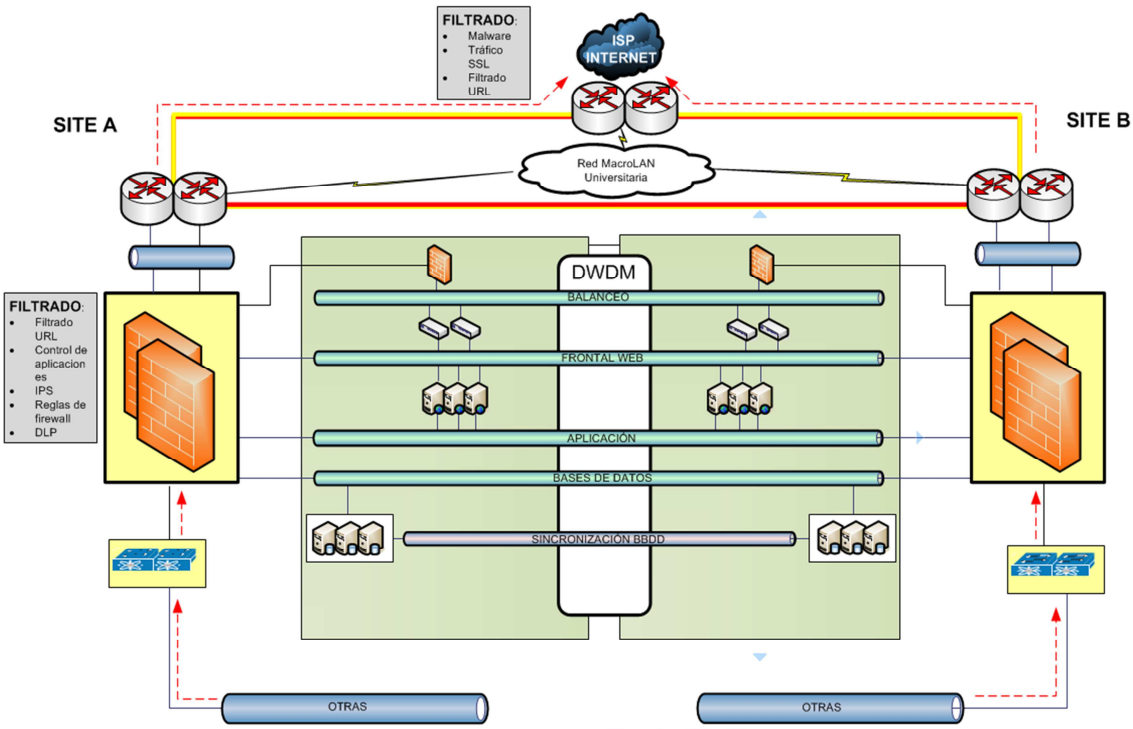
Dado que tenemos una exigencia por parte de la universidad a la hora de asegurar cada uno de los *CPD* de las facultades, tenemos igualmente el compromiso de disponer de la misma seguridad en estos *CPD* ya que en caso de caída de los anteriores, el servicio ha de ser igual.

Por tanto, es válido todo lo comentado anteriormente en materia de seguridad. Se mantendrán los mismos motores de búsqueda de amenazas y análisis de tráfico tanto en los accesos internos (dentro de la *MacroLAN* universitaria) como en los externos (*Internet*).

Al ver el plano lógico de la red del *CPD* extendido llama la atención la aparición de una nueva ubicación llamada "*ISP INTERNET*". Esta ubicación nos dará la salida a Internet en este caso en lugar de contar con un acceso dedicado en cada uno de los *CPD*.

Al tener la salida hacia Internet en otra ubicación, hemos desplazado el filtrado mediante el *proxy* hacia las instalaciones del propio *ISP*. Aun así, el filtrado mantendrá la misma filosofía que ya se ha comentado pero con un equipamiento específicamente dimensionado.

MARIO ARENAS GARCÍA



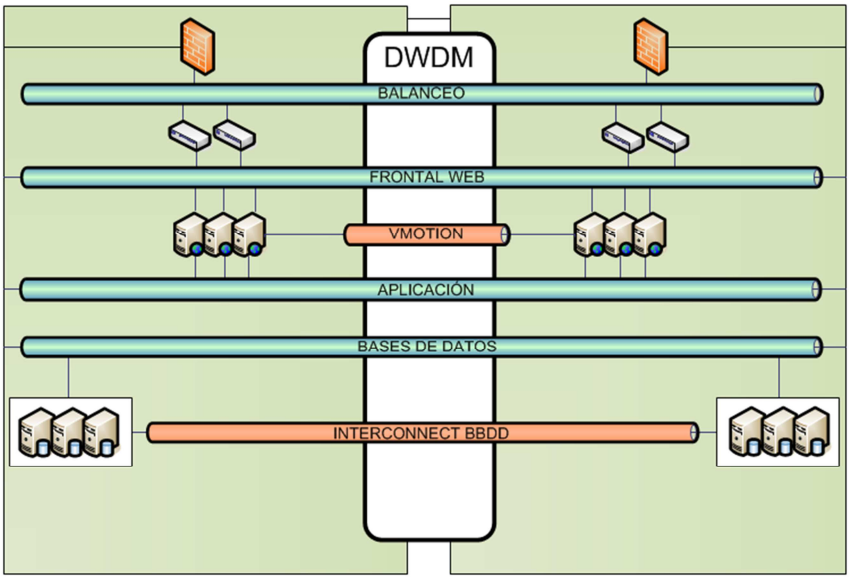
7.3. DISEÑO DE SISTEMAS

En el apartado de los sistemas hay poco que añadir ya que los mismos sistemas operativos, aplicativos y *BBDD* estarán permanentemente sincronizados entre los *CPD*. Aun así hay que tener en cuenta algunos aspectos fundamentales en cuanto a la configuración de los mismos:

- *Cluster* de aplicaciones: en la capa de frontales web donde se ejecutan las aplicaciones, hemos de crear *clusters* de frontales de aplicaciones para que, en caso de caída de uno de los *CPD* extendidos, se puedan mantener las sesiones de usuarios conectados.
- *Vmotion*: asimismo, y también en la capa de frontales *web*, será necesario configurar un mecanismo de sincronización mediante el cual podamos apagar una máquina de un *CPD* y encenderla en el otro con la misma configuración en cuestión de segundos.
- *Cluster* de *BBDD*: en la capa de consolidación de los datos también hemos de procurar un mecanismo de *cluster* entre las *BBDD* situadas en ambos *CPD* ya que, al igual que en la capa de aplicación, hemos de garantizar el funcionamiento de estos sistemas en caso de caída.
- *Interconnect*: en este caso, hemos de configurar en los nodos de las bases de datos con un mecanismo de sincronización para que todos los nodos que estén trabajando en el *cluster* tengan las mismas actualizaciones sobre los datos de las tablas de las *BBDD*.

MARIO ARENAS G

- Configuración de red: como hemos comentado en el apartado 7.1, se mantendrá la configuración de red excepto en un detalle: la máscara. Al clonar por primera vez las máquinas en el *CPD* extendido habrá que modificar la máscara de red para que puedan ver toda la red de su CPD.
- Duplicidad de servidores: por motivos impuestos en este proyecto, cuando clonemos uno de los servicios en producción en el *CPD* extendido, se hará en ambos *CPD* que lo conforman para poder funcionar luego de forma conjunta o por separado.



MARIO AR

8. INTEGRACIÓN DE LAS FACULTADES EN *CPD* EXTENDIDO

Una vez que los *CPD* estándar de cada facultad han sido puestos a punto, al igual que ha tenido que ocurrir con el *CPD* extendido, el próximo paso consiste en la integración de los primeros en este último. Este paso contiene muchas otras implicaciones que iremos desgranando.

Como veremos y entenderemos en los siguientes apartados, la integración de los *CPD* es un proceso que, aunque se realiza al principio de la vida de los mismos, hay que mantener activo y en buen estado de salud, ya que de ello dependerá el resultado del funcionamiento de la solución.

En este apartado se detallará con mayor profundidad tres aspectos clave en la infraestructura para que dicha integración sea fácil, progresiva y estable. Hay que tener en cuenta que el posible proceso de conmutación futuro de *CPD* ha de ser un proceso lo más transparente posible.

8.1. ENRUTAMIENTO DINÁMICO

En primer lugar vamos a ver qué mecanismos permiten que los datos vayan a llegar desde los *CPD* estándar hasta los *CPD* extendidos. El hecho de parametrizar adecuadamente esta capa será básico para el resto de las etapas ya de que esta capa dependerán el resto de parámetros.

Para poder hacer que los *CPD* puedan estar accesibles entre ellos implica tener implicados los dos métodos de enrutamiento que conocemos (estático y dinámico) en puntos diferentes de la topología del campus de la universidad pudiendo implementar en algún caso el protocolo más conveniente.

Visto lo anterior, vamos a especificar cuál sería el área de acción de cada uno de estos protocolos, es decir, hasta dónde llegan y en qué puntos de la red trabajan:

- Enrutamiento estático: dentro de cada uno de los *CPD* tendremos un tipo de enrutamiento basado en rutas estáticas. Esto se debe a la sencillez del entorno de los *CPD* estándar, ya que la segmentación de la que cuentan, no es suficiente para implementar un protocolo de enrutamiento dinámico basado en estado enlace o vector distancia.
  En este punto, lo que se espera de la capa de enrutamiento es que sea capaz de sacar los paquetes del *CPD* de origen hacia los nodos del operador situados en la frontera entre la entrada de los *CPD* y la red que cuenta con un enrutamiento dinámico.

MARIO ARENAS GARCÍA

Se ha detallado con anterioridad, pero es necesario remarcar que hemos de tener una configuración estática de las rutas tanto los paquetes entrantes como salientes, es decir, hemos de vigilar las rutas que ponemos en qué sentidos para que este apartado funcione.

- Enrutamiento dinámico: en este caso, y una vez que los paquetes hayan salido con origen los *CPD* estándar y destino el *CPD* extendido (igualmente ocurriría a la inversa), los paquetes han de atravesar una red de conmutación de paquetes. Esta red de conmutación cuenta con varios protocolos de enrutamiento dinámico.
  Esta red de conmutación de paquetes es propietaria del *ISP* que nos alquila la infraestructura, formada por gran cantidad de enlaces redundados, para enrutar los paquetes de forma que la comunicación sea fluida.
  En nuestro caso hemos supuesto que el servicio es contratado a Telefónica que despliega redes de áreas metropolitanas extensas llamadas *MetroLAN* (el nombre genérico es red *MacroLAN*). Se detalla esta parte en el punto 12.1 del anexo

Como es obvio este el primer paso y más importante para que puedan integrarse todos los *CPD* entre sí. El hecho de tener un protocolo de enrutamiento dinámico en el operador nos hace perder independencia y control de la red, pero es la única vía posible en estos casos.

Por otra parte, esos protocolos suelen ser estándar, es decir, en la red de conmutación alquilada se está utilizando *RIPv2* y *OSPFv2* con redistribución de rutas estáticas. Todo esto, junto con la gran capacidad de procesamiento de los elementos de red, proporciona un enlace estable y robusto.

En cuanto a la comunicación entre los diferentes *CPD* estándares, se producirá por la misma red *MetroLAN*, es decir, no habrá prácticamente diferencia con el modelo de comunicación que acabamos de detallar para el caso del *CPD* extendido.

8.2. SINCRONIZACIÓN DNS

En este apartado vamos a centrarnos en una capa más alta del servicio. Serán aquellos aspectos que estén relacionados con la resolución de nombres de los servicios que se están prestando dentro de cada uno de los *CPD* estándar y que habrán de prestarse en el *CPD* extendido en caso de caída.

MARIO ARENAS GARCÍA

La sincronización *DNS* será un mecanismo mediante el cual podremos mantener a todos los servidores de nuestra red informados de los posibles cambios que pueda haber en la infraestructura, para poder así saber a qué lugar enviar las peticiones en cada caso.

Para poder hacer lo anterior, tenemos que contar con una infraestructura jerárquica de servidores *DNS* que sea dinámica, esto es, ha de estar monitorizando continuamente estado de los servicios mediante consultas *DNS*. Veremos más adelante el funcionamiento (apartado 9.2).

Además de esta sincronización entre los *DNS* que conforman la jerarquía, es necesario que estos servidores envíen la consulta de estado de registro a los balanceadores de sus respectivos *CPD*, de esta forma sabremos, por la respuesta *DNS*, si el servicio responde correctamente o no.

8.3. REQUISITOS DE LA POLÍTICA DE SEGURIDAD

En el apartado relativo a la seguridad no es especialmente problemático a priori, aunque debido a cómo han de circular los datos por la infraestructura, sí es necesario hacer algunas indicaciones que redundarán en un mejor rendimiento a futuro de la plataforma.

Como vemos por los diagramas de red, los datos que han de intercambiarse entre los distintos *CPD*, ha de atravesar los firewalls de cada uno de ellos. Esto puede suponer un problema si no tenemos en cuenta qué datos hemos de filtrar en busca de amenazas.

En lo relativo a la política de seguridad hemos de tener en cuenta por tanto dos aspectos muy importantes de cara al rendimiento de los *firewalls* y, por extensión, de la solución completa:

- Datos de sincronización: los datos que sean relativos a las réplicas almacenadas en el *CPD* extendido no han de ser analizados por los filtros de seguridad. Se presupone que son datos seguros, y que la red *MacroLAN* también lo es por ser una red virtual privada destinada únicamente a estos fines.
- Política de seguridad: dentro de la política de seguridad de los cortafuegos, pondremos las primeras reglas que permitan este tráfico en primer lugar ya que de esta forma el procesamiento de paquetes será mucho más rápido, y no cargará a los equipos teniendo que inspeccionar continuamente la política de seguridad completa.

MARIO ARENAS GARCÍA

- Filtros avanzados: estos filtros estarán desactivados para estos datos. Al igual que comentábamos en el apartado anterior, consideramos que los datos están libres de amenazas por haber sido analizados anteriormente, por tanto, tampoco cargaremos a los cortafuegos con un análisis adicional que aporta poco valor.

Como vemos, se pondrá especial cuidado en no filtrar los accesos que permiten que los datos se estén sincronizando en tiempo real con el *CPD* extendido y así, al mismo tiempo, estamos permitiendo que los *firewalls* puedan tener mayor holgura de recursos y por tanto sean más escalables.

Por último, comentar se ha tomado esta opción en lugar de poner líneas dedicadas para estos datos debido al coste que esto supondría teniendo en cuenta que ya existe la infraestructura para hacerlo posible. Se prefiere usar el entorno existente a aislar uno para la sincronización.

8.4. SINCRONIZACIÓN DE LOS DATOS

De forma general durante este apartado estamos hablando de sincronización de los datos. Para poder tener un conocimiento más exacto necesitamos saber qué datos hemos de sincronizar, a qué sistema pertenecen, cuánto ocupan y cómo se van a sincronizar.

Los datos que se sincronizarán entre los *CPD* estándar y el *CPD* extendido serán aquellos de interés para la actividad de la universidad, es decir, toda la información relacionada con los entorno de producción y sus correspondientes BBDD donde se almacenan otros datos importantes.

Además, hay que tener en cuenta que desde el *CPD* extendido es necesario que tengamos disponible una imagen de cada servidor que necesitemos activar puntualmente en caso de contingencia, por lo que será necesario contar también con los últimos *backup* e imágenes de sistemas.

Por tanto, el estado de cada sistema, en el momento del último parcheado, ha de estar disponible en ambos *CPD*, así como los juegos de datos que han de manejar las *BBDD*. También será necesario contar con el último *backup* completo de todos los sistemas.

Por otro lado, ya hemos adelantado en apartados anteriores la cantidad de espacio necesaria en cada facultad así como en el *CPD* extendido. En esos cálculos se han tenido en cuenta todas las necesidades comentadas hasta ahora.

MARIO ARENAS GARCÍA

Para poder lanzar la sincronización de los datos de manera continua e incremental, utilizaremos dos métodos distintos:

- Protocolo *rsync*: este protocolo es utilizado en sistemas *Unix*/*Linux* para poder sincronizar los datos entre los dos servidores (el de producción en y el de *standby*). Como además de permitir la sincronización remota de forma incremental, también permite la compresión de datos, lo cual beneficia en gran manera la penalización sobre el caudal de tráfico y sobre el rendimiento de ciertos equipos.
- Oracle *sync*: las bases de datos de *RAC* cuentan con variedad de mecanismos para sincronizar los datos entre nodos de un mismo *cluster* (lo que será necesario para el *CPD* extendido) pero para la sincronización de los datos entre nodos de distintos *cluster*, se hará esencialmente mediante el mismo mecanismo anterior, es decir, será una herramienta de sistema la que se ocupe de ello.

Todo lo hablado hasta el momento guarda relación con la sincronización entre los *CPD* estándar y extendido, pero no es el único factor que hay que tener en cuenta. También tendremos que tener ambos *CPD* extendidos sincronizados de la misma manera ya que uno servirá de contingencia al otro.

Los mecanismos que utilizaremos en este caso serán los mismos, lo que supondrá un coste en el apartado de la configuración pero gracias a ella, ganaremos automatismos dentro de la red que serán vitales en caso de que se produzca una conmutación.

MARIO ARENAS GARCÍA

9. FUNCIONAMIENTO DE LA SOLUCIÓN

En apartados anteriores se han descrito comportamientos de componentes aislados de la infraestructura, o bien, se ha comentado el funcionamiento de algún apartado de forma general. En el presente apartado veremos de forma global y secuencial el funcionamiento de la solución bajo algunos supuestos.

Obviamente, dentro de una organización con una infraestructura como la que estamos tratando, no tiene un único punto de vista, es decir, tendremos que descubrir los flujos de datos del área de producción, de los usuarios y de los propios servidores.

De entre los anteriores prestaremos especial atención a los flujos y mecanismos que estén en relación con el entorno de producción y con el tráfico de control y sincronización entre los *CPD* que hacen posible la automatización en la conmutación de los servicios en caso de caída.

9.1. FLUJOS DE TRÁFICO: INTRA-CPD E INTER-CPD

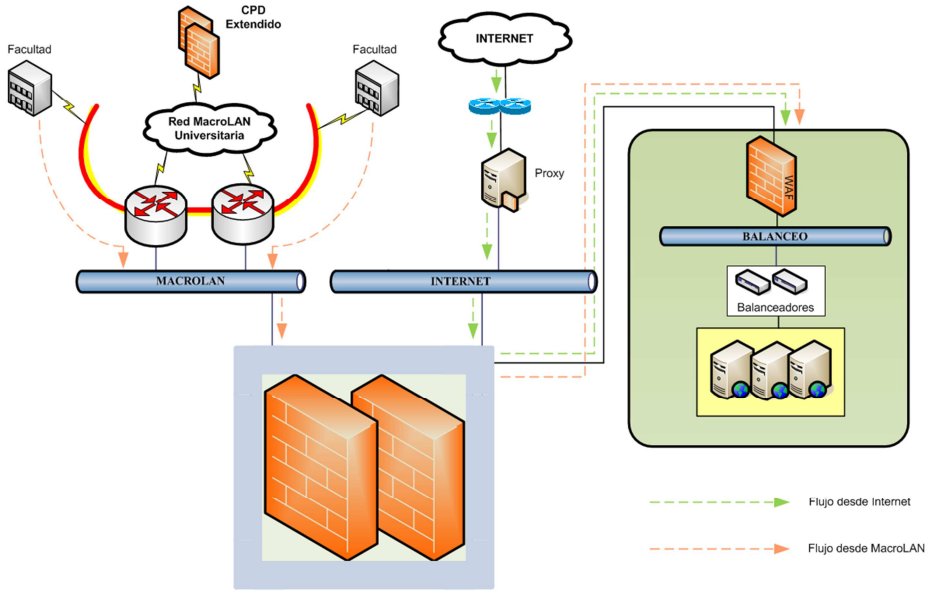
En este apartado haremos especial hincapié en los principales flujos de tráfico que se dan dentro del *CPD* y entre los *CPD* para poder explicar el funcionamiento de cada uno de los mismos. De esta forma, y con los detalles anteriormente explicados, podremos ver el funcionamiento completo.

En el caso de los flujos internos, haremos distinción fundamentalmente entre tres escenarios cuyo funcionamiento y naturaleza son bien distintos:

- Entorno de producción: en este entorno podemos categorizar el tráfico en dos tipos de flujos fundamentales :
    - Internet: este tipo de accesos se producirán desde cualquier lugar y tendrán como objetivo aquellas aplicaciones de producción que puedan ser consultadas por Internet. Estos accesos se producen por vía *web* con cifrado *SSL*.
    - Red *MacroLAN* universitaria: este tipo de accesos tienen como origen alguno de los usuarios de la red universitaria y por objetivo cualquiera de las aplicaciones de cada facultad. Estos accesos se producen vía *web* con cifrado *SSL*.

MARIO ARENAS GARCÍA

A continuación se muestran gráficamente estos flujos:

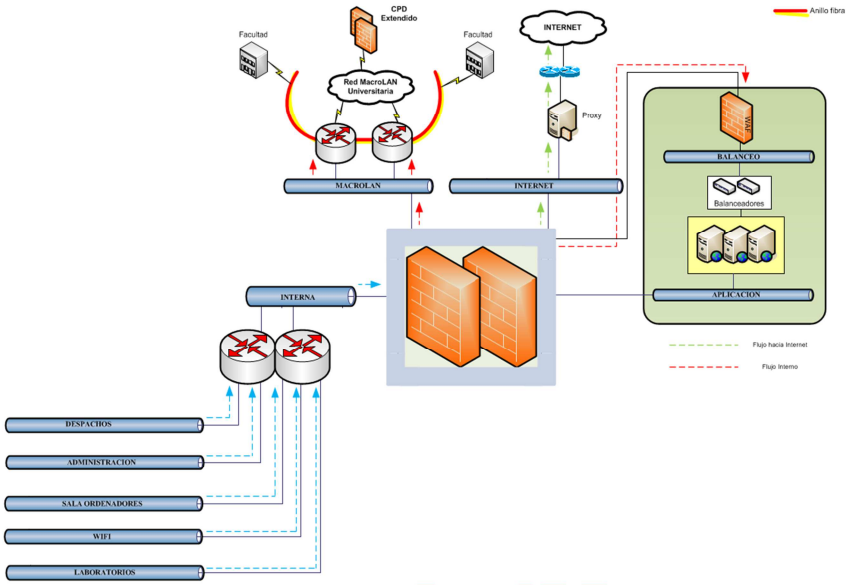


- Acceso usuarios: en los accesos de los usuarios podríamos hacer una diferenciación en dos grandes flujos de tráfico:

    - Internet: estos accesos se refieren a los flujos de datos que los usuarios establecen con cualquier destino en Internet. En este caso se utilizan gran cantidad de protocolos y aplicaciones por lo que es necesario hacer un filtrado de salida.
    - Interno: estos accesos hacen referencia al acceso de los usuarios desde sus puestos de trabajo (o bien desde su terminal móvil) hacia las aplicaciones internas. Es decir, sería el tráfico que se genera dentro de cada *CPD* o hacia otro *CPD*.

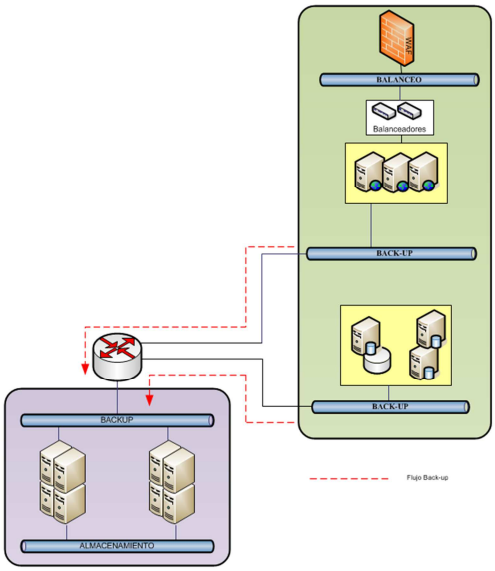
MARIO ARENAS GA

A continuación se muestran gráficamente estos flujos:



- *Backup*: este tipo de acceso se refiere a los accesos desde todos los servidores de producción hacia la plataforma de almacenado y *backup*. Dichos sistemas disponen de un enlace dedicado que no atraviesa ningún filtrado para ganar en velocidad y no perder rendimiento.

A continuación se muestran gráficamente estos flujos:



MARIO ARENAS GA

En el caso de los flujos externos de datos, nos centraremos principalmente en aquellos flujos de datos entre los *CPD* estándar y el *CPD* extendido:

- Tráfico *DNS*: en el caso de la resolución de nombres dentro de la red hemos de hacer una diferenciación entre tres tipos de flujos de tráfico:
    - Transferencias de zonas: tráfico que hace referencia a la lista de nombres que han de resolver cada uno de los DNS. Cada servidor enviará la lista de servidores que cuyo nombre puede resolver al resto.
    - Consultas *DNS*: estos flujos de datos se producirán por parte de los usuarios, de los sistemas y de las aplicaciones cuando intenten resolver el nombre de la máquina de destino y necesiten saber su IP.
    - Sincronización registros *DNS*: los registros *NS* y *A* de cada servidor han de ser monitorizados mediante consultas *DNS* para saber el estado de cada una de ellas en lo que se refiere a las entradas de los nombres de los servicios en producción.

- Sincronización datos: en este caso nos referimos a los flujos de datos que se dan entre los distintos *appliances* que alojan las máquinas virtuales con los servidores, es decir, habrá flujos de datos entre los frontales y las *BBDD* de los *CPD* estándar y extendido entre sí.

En este caso nos sirve para ilustrar el esquema jerárquico *DNS* el gráfico de la sección 6.3.3.

9.2. BALANCEO GLOBAL EN *CPD* EXTENDIDO

En este apartado se relatará el funcionamiento de la infraestructura *DNS* que permite balancear los servicios de producción. Este tipo de solución basada en balanceo por registro *DNS*, es cada vez más común debido a la agilidad en la conmutación del servicio y óptimo funcionamiento.

Debido a ello, los *DNS* del *CPD* extendido entrarán en juego cuando se produzca una caída en un *CPD* estándar por un fallo en uno de los servicios de producción. Normalmente no se suele monitorizar el estado de los registros A con consultas *DNS*, pero en nuestro caso es imprescindible.

Una vez que tenemos un servicio activado en el *CPD* extendido, y los *DNS* de cada uno de los *sites* está monitorizando el servicio en el *CPD* correspondiente,

MARIO ARENAS GARCÍA

es necesario que, además de estas monitorizaciones, configuremos la monitorización de las granjas entre los balanceadores.

Esto se consigue monitorizando la granja remota de servidores. Si hubiera algún problema, de manera similar a como sucede en el *CPD* estándar, ambos *DNS* deben de dejar de contestar al servicio ya que este se encontraría caído. Este es el peor caso, caída de los *sites*.

Si solo uno de los *sites* del *CDP* extendido cayera, ambos *DNS* han de eliminar la entradas A de dicho servicio (los servicios se encuentran activos en ambos *CPD* con *IP* distintas) y responder únicamente con la *IP* donde se encuentra el servicio activo

La caché *DNS* de cada uno de los servidores *DNS* así como los balanceadores, ha de estar establecida a un tiempo bajo ya que si este valor es alto y un cliente hace una petición sobre un servicio que está caído, el servidor *DNS* responderá lo cual sería un error.

9.3. PRUEBAS DE ALTA DISPONIBILIDAD

Además de los planes de contingencia comentados anteriormente, es necesario especificar qué pruebas concretas se llevarán a cabo para determinar que la solución es robusta y tolerante ante los posibles fallos que se han comentado hasta ahora.

De forma genérica, las pruebas de alta disponibilidad y redundancia se basarán en todos los casos en parar los servicios de un elemento de la red y ver cómo reacciona el equipo de respaldo. La prueba se repetirá de nuevo cuando activemos los servicios en el equipo principal.

Hemos de ser conscientes de que, además de las configuraciones en alta disponibilidad (entendemos por esta un activo-pasivo) en los casos en que tenemos una configuración en activo-activo se desactivarán los servicios de forma aleatoria en cualquier nodo del *cluster*.

Aclarado lo anterior, se pueden ver que hay dos entornos de análisis y pruebas bien diferentes: CPD estándar y CPD extendido. Esta diferencia se basa precisamente en el tipo de configuración de alta disponibilidad definida en el diseño. En los siguientes sub-apartados se detallan las pruebas a realizar.

MARIO ARENAS GARCÍA

9.3.1. Pruebas CPD estándar

De forma similar a cómo se ha enfocado las tareas anteriores, se planificarán y ejecutarán las pruebas de alta disponibilidad de manera que incluyan las tres áreas principales de las que se hace cargo este proyecto:

- Seguridad: en este caso las pruebas de alta disponibilidad de los dispositivos que se encuentran en modo *inline*, que son aquellos que provocarían una disrupción en el servicio en caso de caída total, se basan en la caída controlada del nodo principal y la posterior recuperación del servicio por parte de dicho equipo. Esto provocará dos momentos potencialmente peligrosos cuando se produzca un intercambio de sesiones de un dispositivo a otro.
  Estos dispositivos son todos aquellos que conforman la estructura principal de seguridad a excepción del *proxy* y las máquinas asociadas, ya que el despliegue de las mismas se hizo en modo *offline*, es decir, están situados en la red de modo que aunque caigan, no se produzca corte, aunque sí pérdida de ese servicio/funcionalidad. Los equipos implicados serían: *firewalls* y *WAF*.
- Comunicaciones: en este caso las pruebas de alta disponibilidad de los equipos de conmutación tienen que estar basadas en un entorno de activo-activo, ya que todos los *switches* y *routers* han de estar configurados de esta forma para el correcto funcionamiento de la redundancia de enlace con los sistemas y servidores de seguridad. En concreto, en este caso pararemos los servicios en uno de los nodos y posteriormente en el otro de forma aleatoria.
  En cuanto a las pruebas concernientes a los balanceadores de carga, han de estar orientadas a una configuración en alta disponibilidad, es decir, activo-pasivo por lo que, al igual que se ha comentado en el punto anterior, en primer lugar pararemos los servicios en el equipo principal y, después de comprobar que el equipo secundario asume sin problemas la carga, repetiremos la prueba sobre él.
- Sistemas: en este caso la prueba de alta disponibilidad ha de estar orientada a sistemas que se encuentran formando un *cluster* de varios servidores con sesiones de usuario sincronizadas entre ellos por lo que, al igual que el en caso de los

MARIO ARENAS GARCÍA

routers y *switches*, tenemos en cuenta que en este entorno la configuración es activo-activo. Por tanto, las pruebas que se ejecuten se circunscribirán a la parada de los servicios de forma aleatoria en los servidores de producción.

Por otro lado, no hay que olvidar que las máquinas virtuales están alojadas en cabinas de procesamiento, por lo que hay que contemplar en este caso la caída de una cabina. En cada *CPD* tenemos dos cabinas de procesamiento con una configuración de activo-pasivo, por lo que las pruebas que se llevarán a cabo serán, al igual que en los casos anteriores, paradas secuenciales de los servicios en la cabina primaria y secundaria.

En cada caso las pruebas se darán por buenas cuando no se produzca corte en el servicio, las sesiones de los usuarios se mantengan de forma transparente para estos. Cualquier caída ha de ser totalmente transparente para los usuarios finales.

9.3.2. Pruebas CPD extendido

Siguiendo el esquema del sub-apartado anterior y la lógica de las tareas anteriores, se planificarán y ejecutarán las pruebas de alta disponibilidad que incluyan nuevamente las mismas áreas, ya que en este caso su funcionamiento es distinto:

- Seguridad: en este caso las pruebas de alta disponibilidad se basarán en la parada de los servicios aleatoria de cada una de los miembros del *cluster* para comprobar que el servicio permanece estable pese a dicha caída.
- Comunicaciones: en este caso las pruebas de alta disponibilidad serán las mismas que en el caso del *CPD* estándar y que en el apartado de anterior. Hay que tener en cuenta que en este caso la prueba es más compleja por la extensión de las *vlan*.
- Sistemas: en este caso las pruebas de contingencia serán distintas a las del *CPD* estándar ya que los servidores virtuales han de poder moverse dinámicamente entre ambos *CPD*, es decir, las cabinas estarán configuradas en activo-activo.

En cada caso las pruebas se darán por buenas cuando no se produzca corte en el servicio, las sesiones de los usuarios se mantengan de forma transparente para estos. Cualquier caída ha de ser totalmente transparente para los usuarios finales.

MARIO ARENAS GARCÍA

Además, cada uno de los *sites* que componen en CPD extendido han de pasar las mismas pruebas de alta disponibilidad de la misma forma que las pasaron cada uno de los CPD estándar, ya que cada uno de ellos puede funcionar independientemente del otro.

9.3.3. Pruebas inter-CPD

Además de las pruebas de alta disponibilidad dentro de cada uno de los CPD, hay que tener en cuenta que la infraestructura de la universidad funciona como un conjunto y, por tanto, hay que tener en cuenta la interrelación entre ellos.

Siendo más concisos, estas pruebas se referirán principalmente a los mecanismos de sincronización que se inician en los *CPD* estándar hacia el *CPD* extendido. Un fallo de conectividad entre los *CPD* no debería suponer una caída sino que se active la contingencia *DNS*.

En este caso la prueba desactivar una de las interfaces de los *routers* de entrada (o del propio firewall central) de un *CPD* estándar equivale a aislar uno de estos *CPD*, por lo que mediante la sincronización *DNS*, se deberían activar todos los servicios de ese *CPD* en el *CPD* extendido.

Por otro lado el hecho de hacer la misma prueba dentro del *CPD* extendido no produce el mismo resultado ya que este consta de dos entradas desde *MacroLAN*. Con una sola de ellas activa todos los servicios se podrán dar con normalidad.

Aunque los servicios en producción no se vean afectados debido a los protocolos que se utilizan, sí se verán afectados los servicios de sincronización que tengan sesiones activas en el *router* desactivado. En este caso, habrá que volver a conectar.

MARIO ARENAS GARCÍA

10. PLANES DE CONTINGENCIA

En el presente proyecto, y siguiendo las indicaciones de la universidad, se detalla el proceso que sigue la infraestructura desplegada para poder alcanzar una alta disponibilidad automática, rápida y fiable. Este es otro de los puntos fundamentales del proyecto transmitidos por la universidad.

En primer lugar, y como ya se ha venido comentando en apartados anteriores, la solución de la alta disponibilidad está basada en el balanceo global mediante *DNS*. En este caso los protagonistas no serán solo los servidores *DNS*, sino que los balanceadores también jugarán un papel fundamental.

En primer caso se analizará el funcionamiento de la solución en el caso en que se produzca la caída de uno de los *CPD* estándar. En ese caso la contingencia natural de un *CPD* estándar será llevar los servicios al *CPD* extendido, el cual se encargará de balancear a su vez entre dos *sites*.

En el segundo caso, la gestión de la caída de uno de los *sites* del *CPD* extendido se llevará a cabo entre los 4 balanceadores y los 4 *DNS* internos. En este caso tenemos más opciones de gestionar la alta disponibilidad ya que podemos dejar que las granjas estén en activo-activo o bien en modo activo-pasivo

10.1. CAÍDA CPD ESTÁNDAR

En primer lugar debemos recordar que contamos con una infraestructura jerárquica de servidores *DNS* donde los *DNS* del *CPD* extendido los *DNS* primarios y los *DNS* del resto de los *CPD* estándar, los *DNS* secundarios. A su vez, cada *DNS* de cada facultad será el primario dentro de cada facultad.

Esto es así debido a que todos los servidores y puestos finales de usuario, utilizarán como *DNS* primario el que esté en su *CPD* por varios motivos:

- Rapidez en la resolución de nombres.
- Cada *DNS* conoce y monitoriza el estado de los servicios de producción de cada *CPD* mediante consultas *DNS* a las *URL* correspondientes.
- Descarga de tráfico a los *DNS* centrales.

De esta forma los *DNS* de cada *CPD* estarán haciendo consultas constantemente a los registros A de su base de datos de nombres. Cuando una *URL* no responda en un tiempo establecido, el servidor *DNS* de ese *CPD* dejará de contestar a las consultas *DNS*.

MARIO ARENAS GARCIA

En ese momento el servicio se levantará en el *CPD* extendido (los balanceadores están configurados para activar granjas de servidores en el *CPD* extendido como entorno de *backup* por si falla las granjas de los *CPD*) y serán los *DNS* secundarios de los clientes los que contesten.

Esos *DNS* secundarios serán precisamente los *DNS* del *CPD* extendido. Para que la consulta no falle en ese momento, el cliente ha de configurar en su equipo el *DNS* primario del *CPD* extendido como *DNS* primario para su red, ya que de esta manera conseguiremos reenviar las peticiones que no han sido atendidas.

10.2. CAÍDA CPD EXTENDIDO

En el caso de caída de un servicio alojado en un *CPD* estándar, el mecanismo de conmutación explicado anteriormente hará que tengamos el servicio disponible en el *CPD* extendido. Una vez activo, tenemos varias posibilidades de gestionar el entorno extendido de varias formas.

La primera forma es que, dentro del propio *CPD* extendido, siguiéramos las mismas directivas que se han seguido en los *CPD* estándar ya que en este caso, podemos indicar en la configuración de servidores *DNS* y balanceadores que la granja de *backup* está replicada y en modo pasivo en el otro *site*.

Esto es posible gracias, además de a la configuración de los servidores *DNS*, a la monitorización entre los miembros del mismo *cluster* de balanceadores. Estos miembros monitorizan el estado de todas las granjas y pueden tomar la decisión de conmutar a cualquier *site*.

La segunda forma de gestionar un servicio dentro del *CPD* extendido es ponerlo en modo activo-activo, es decir, dejar que ambos *sites* respondan a peticiones al mismo tiempo. En caso de caída una de las granjas asumiría todo el tráfico sin problemas ya que los recursos han sido dimensionados para ello.

Esta opción es posible gracias a que los 4 balanceadores del *CPD* extendido estarán formando un *cluster*, y por tanto todos los miembros del mismo son capaces de ver el estado de las sesiones del resto de granjas y servidores y repartir la carga a conveniencia.

MARIO ARENAS GARCÍA

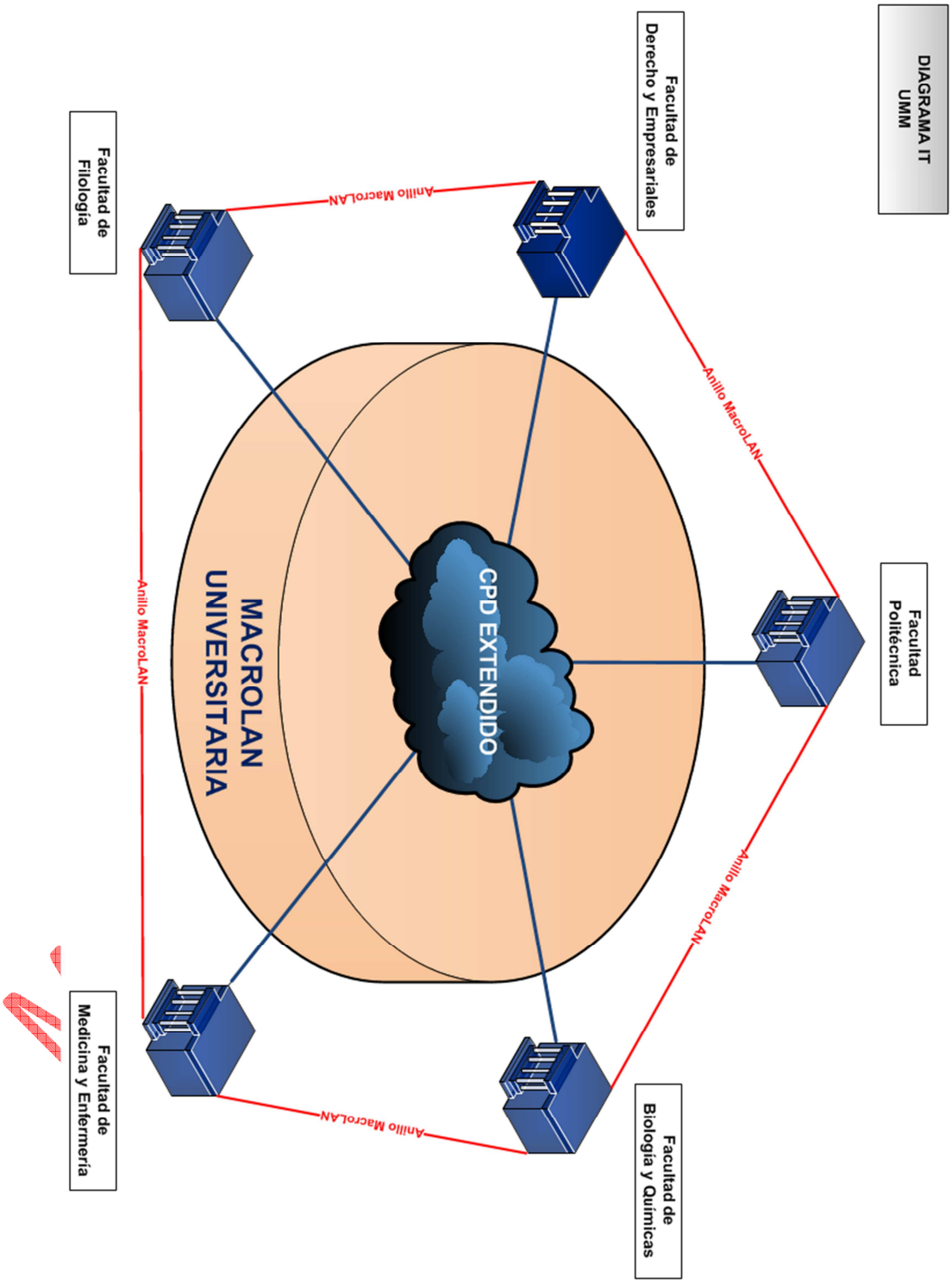
11. MAPAS DE RED

A continuación se adjuntan los diagramas de red de los que se habla durante todo el documento. Estos diagramas representan el conjunto de infraestructuras que se desplegarán durante el proyecto. En algunos casos estos diagramas no se refieren a infraestructuras físicas sino a topologías lógicas de funcionamiento.

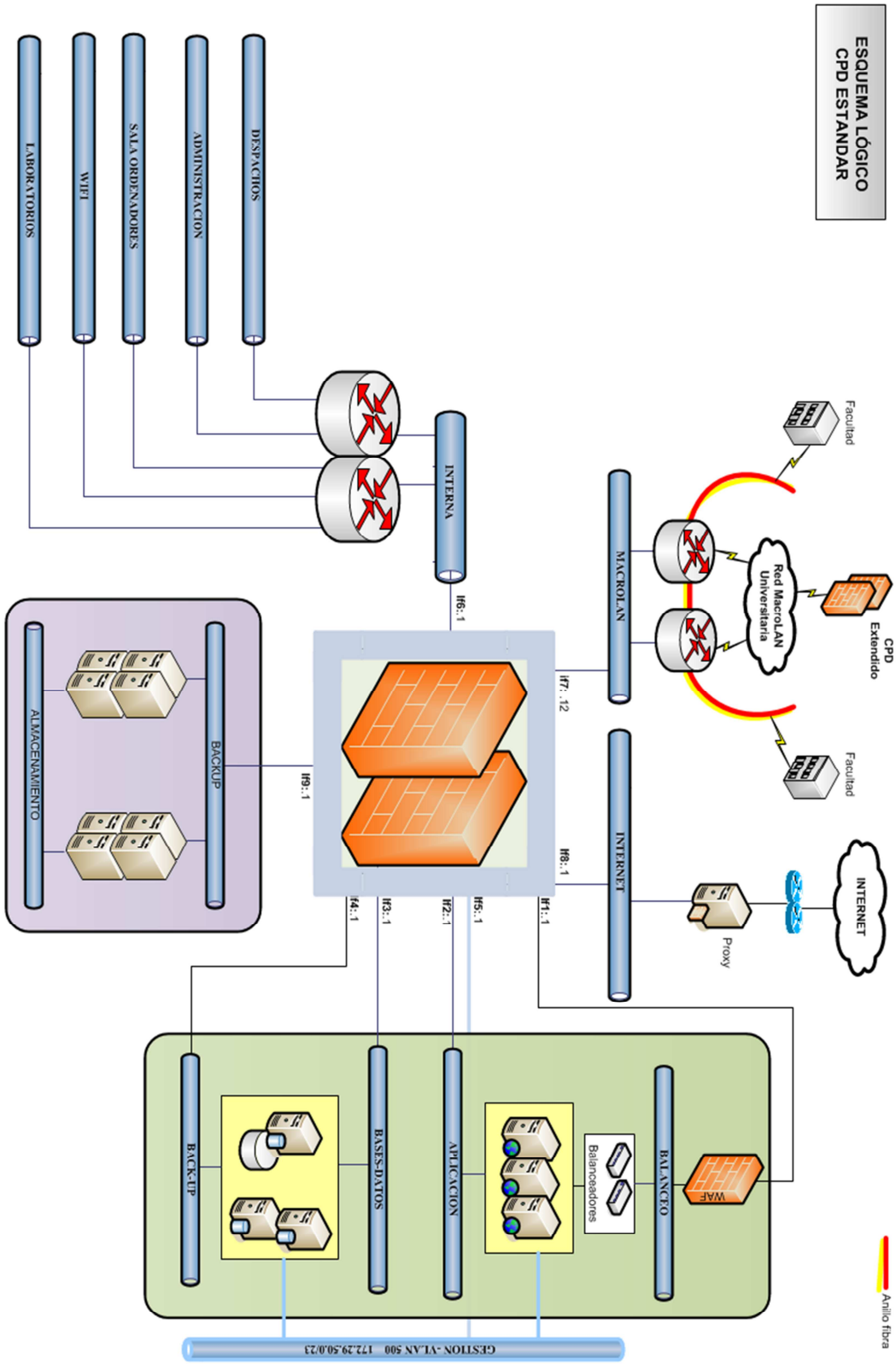
Aunque en los diagramas representan en cada caso simplemente las infraestructuras de cada parte de la red, en los apartados anteriores se ha especificado el funcionamiento y flujos de datos a través de las mismas. Esas especificaciones están desarrolladas sobre estos mismos diagramas.

MARIO ARENAS GARCÍA

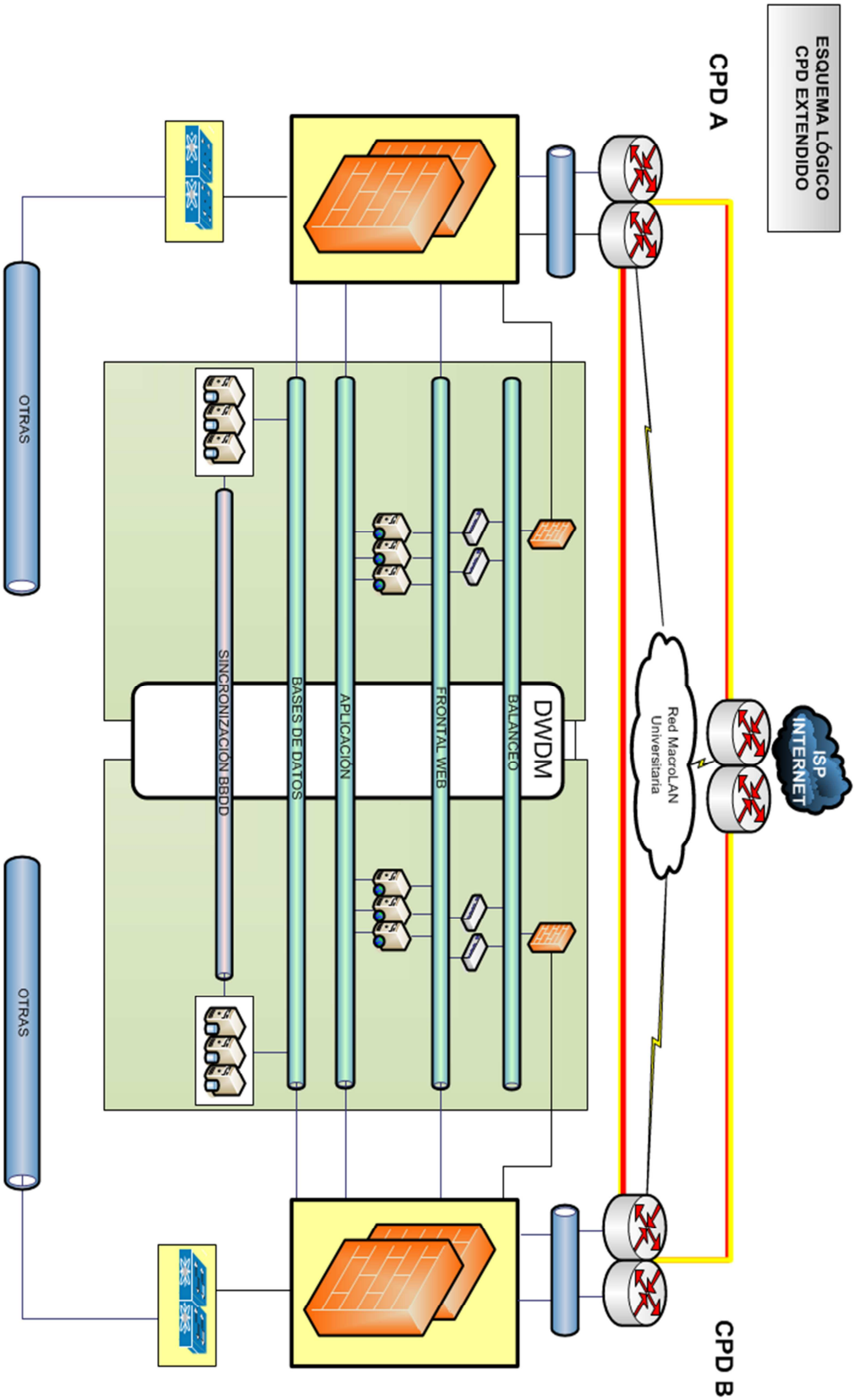
11.1. CAMPUS UNIVERSITARIO



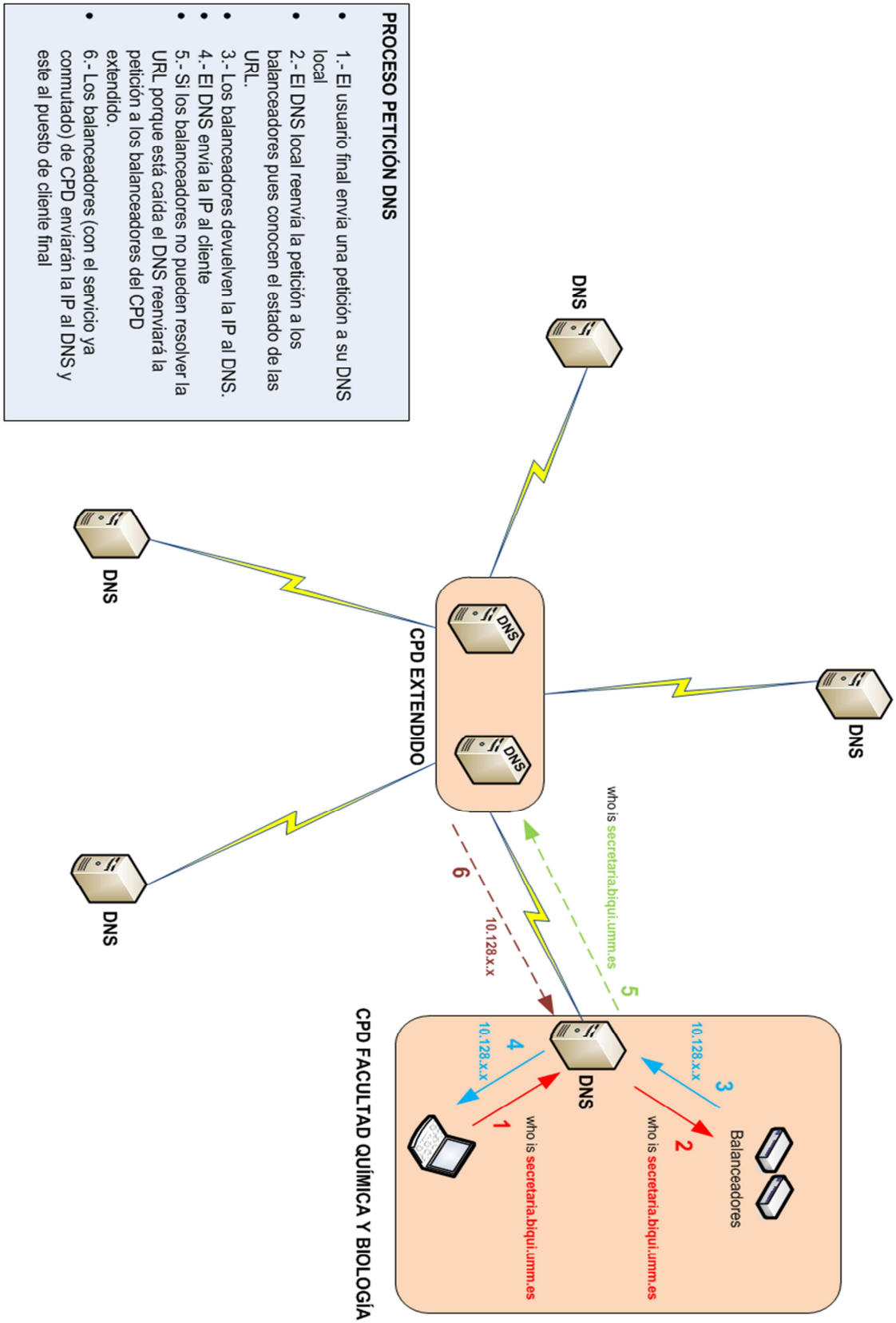
11.2. *CPD* ESTÁNDAR



11.3. *CPD* EXTENDIDO



11.4. BALANCEO GLOBAL *DNS*



12.ANEXOS

En los siguientes apartados se especificarán algunos datos que se han ido mencionando a lo largo del documento. En otros casos, los apartados servirán para ilustrar el funcionamiento de ciertos sistemas de los que haremos uso pero no son objetivo de este proyecto.

12.1. RED *MACROLAN*

La red *MacroLAN* es una red propietaria de Telefónica de ámbito nacional que permite conectar a las organizaciones con otras sedes de manera rápida, confiable, sin pérdidas cuyo ancho de banda está garantizado.

El acceso desde un equipo final de *MacroLAN* conecta la red interna de cliente con la red metropolitana. A esta zona de la red también se le conoce como *MetroLAN*, que no es más que la infraestructura *WAN* a nivel metropolitano.

En la red *MetroLAN* se utilizan protocolos de enrutamiento dinámica tales como *RIP* y *OSPF*, aunque este segundo está resultando el predominante durante estos últimos años. *RIP* fue el protocolo utilizado al principio para conectar las sedes de metropolitanas de los clientes.

Los equipos de cliente final (*EDC*), se conectan a otro equipo agregador, cuya misión es concentrar el tráfico de los clientes finales y así hacer posible la comunicación de las sedes de los clientes en conexiones metropolitanas.

A su vez, los equipos agregadores se conectan a equipos de frontera de la red nacional llamados *PE*. Estos *PE* son los encargados de multiplexar dichas conexiones y encaminar el tráfico desde la red metropolitana a la red nacional.

Estos equipos por su parte implementan de cara a la red nacional, *MPLS* como protocolo de enrutamiento dinámico para la *WAN*. Además, hay una serie de equipos que se utilizan para llevar el control de la red nacional y tener conocimiento de la topología *MPLS*.

MARIO ARENAS GARCÍA

12.2. DIRECCIONAMIENTO

En el siguiente inventario de direccionamiento únicamente se han tenido en cuenta las redes principales de cada CPD. A saber: redes internas y redes de producción. No es de interés en este documento incluir el direccionamiento de interconexiones entre elementos.

Por otra parte, como podemos ver en el inventario, el direccionamiento del CPD extendido es el mismo que el de los CPD estándar. Esto es así porque en caso de migración, migraremos el direccionamiento completo de cada facultad. Lo único que cambian son las máscaras.

FACULTAD	RED	DIRECCIONAMIENTO	MÁSCARA
POLITÉCNICA	Despachos	172.16.1.0	24
	Administración	172.16.2.0	24
	WiFi	172.16.3.0	24
	Laboratorios	172.16.4.0	24
	Ordenadores	172.16.5.0	24
	Vlan - Frontales	10.128.1.0	24
	Vlan - Aplicación	10.128.6.0	24
	Vlan - BBDD	10.128.11.0	24
QUÍMICA Y BIOLOGÍA	Despachos	172.16.7.0	24
	Administración	172.16.8.0	24
	WiFi	172.16.9.0	24
	Laboratorios	172.16.10.0	24
	Ordenadores	172.16.11.0	24
	Vlan - Frontales	10.128.2.0	24
	Vlan - Aplicación	10.128.7.0	24
	Vlan - BBDD	10.128.12.0	24
MEDICINA Y ENFERMERÍA	Despachos	172.16.12.0	24
	Administración	172.16.13.0	24
	WiFi	172.16.14.0	24
	Laboratorios	172.16.15.0	24
	Ordenadores	172.16.16.0	24
	Vlan - Frontales	192.168.3.0	24
	Vlan - Aplicación	10.128.8.0	24
	Vlan - BBDD	10.128.13.0	24
FILOLOGÍA	Despachos	172.16.17.0	24
	Administración	172.16.18.0	24
	WiFi	172.16.19.0	24
	Laboratorios	172.16.20.0	24

ARENAS GARCÍA

	Ordenadores	172.16.21.0	24
	Vlan - Frontales	10.128.4.0	24
	Vlan - Aplicación	10.128.9.0	24
	Vlan - BBDD	10.128.14.0	24
DERECHO Y EMPRESARIALES	**Despachos**	172.16.22.0	24
	Administración	172.16.23.0	24
	WiFi	172.16.24.0	24
	Laboratorios	172.16.25.0	24
	Ordenadores	172.16.26.0	24
	Vlan - Frontales	10.128.5.0	24
	Vlan - Aplicación	10.128.10.0	24
	Vlan - BBDD	10.128.15.0	24

12.3. PRESUPUESTO

En el siguiente presupuesto se desglosan los precios totales de cada uno de los componentes software y hardware, incluyendo las licencias necesarias con un mantenimiento de 3 años.

Al mismo tiempo también se desglosan los tipos de perfiles necesarios para llevar todas estas tareas a cabo. Además, también se especifica el número de personas, cantidad de horas y la relación coste/perfil.

No se han tenido en cuenta gastos menores como por ejemplo: cables coaxiales, conversores, fibra óptica, etc…ya que faltan datos para poder calcular las cantidades correctas.

MARIO ARENAS GARCÍA

DESCRIPCIÓN	MODELO	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
Firewall Check Point	13800	2	62.500 €	125.000 €
Firewall Check Point	4800	10	21.000 €	210.000 €
Balanceador F5	4200	4	35.770 €	143.080 €
Balanceador F5	2200	10	16.950 €	169.500 €
Analizador SSL Blue Coat	SV1800	5	15.000 €	75.000 €
Analizador SSL Blue Coat	SV2800	2	25.000 €	50.000 €
Malware Analyzer Blue Coat	MAA S400-10	5	18.750 €	93.750 €
Malware Analyzer Blue Coat	MAA S500-10	2	33.975 €	67.950 €
Proxy AV Blue Coat	510	5	6.800 €	34.000 €
Proxy AV Blue Coat	1400	2	17.500 €	35.000 €
Switch Cisco Catalyst	2960	41	3.200 €	131.200 €
Switch Cisco Nexus	2000	18	4.800 €	86.400 €
Switch Cisco Nexus	5000	14	45.000 €	630.000 €
Cabina almacenamiento Dell	R730xd	5	8.550 €	42.750 €
Cabina almacenamiento Dell	MD1400/20	4	21.100 €	84.400 €
Cabina Procesamiento Dell	FX2	20	47.850 €	957.000 €
Cabina Procesamiento Dell	R720D	10	6.200 €	62.000 €
SecureSphere Imperva	X2500	5	22.000 €	110.000 €
SecureSphere Imperva	X4500	2	52.000 €	104.000 €
Veeam Backup & Replication	v8	500	125 €	62.500 €
Antivirus de usuario	EndPoint Protection Advanced	800	38 €	30.400 €

TOTAL	3.303.930 €

PERFIL	TAREA	PERSONAS ASIGNADAS	COSTE HORA	HORAS	SUBTOTAL
Ingeniero seguridad	Diseño seguridad	1	60 €	150	9.000 €
Ingeniero comunicaciones	Diseño comunicaciones	1	60 €	150	9.000 €
Ingeniero sistemas	Diseño sistemas	1	60 €	150	9.000 €
Consultor seguridad	Apoyo diseño y configuración	1	40 €	250	10.000 €
Consultor comunicaciones	Apoyo diseño y configuración	1	40 €	250	10.000 €
Consultor sistemas	Apoyo diseño y configuración	1	40 €	250	10.000 €
Administrador seguridad	Ejecución de tareas	2	20 €	120	4.800 €
Administrador comunicaciones	Ejecución de tareas	2	20 €	120	4.800 €
Administrador sistemas	Ejecución de tareas	2	20 €	120	4.800 €
Jefe de proyecto	Supervisión de proyecto	1	45 €	400	18.000 €

TOTAL	89.400 €

Teniendo en cuenta que el entorno, el cliente y el montante total del proyecto, será difícil de justificar este gasto a no ser que desde la dirección de la universidad contemplen un plan de crecimiento grande.

Sería posible reducir el coste del proyecto reduciendo las funcionalidades de ciertos sistemas, contingencias, licencias, etc…pero, según la dirección, todos estos servicios son necesarios.

Desde este punto de vista, y solo si se tiene en cuenta un crecimiento grande, el proyecto estaría justificado desde el punto de vista económico. En caso contrario, habría que hacer un replanteamiento.

12.4. PRESENTACIÓN

La presentación consta de un documento en formato *.ppt* e ilustra a grandes rasgos, cuales son las necesidades del proyecto, estado actual de la infraestructura *IT*, cómo se ha diseñado y cuál es su funcionamiento.

12.5. BIBLIOGRAFÍA

A continuación se especifican los enlaces que se han ido utilizando a lo largo del desarrollo del proyecto para poder apoyarme en documentación contrastada y precisa tanto de aspectos técnicos o informativos:

- www.f5.com
- www.checkpoint.com
- www.bluecoat.com
- www.imperva.com
- www.barracuda.com
- www.fortinet.com
- www.dell.com
- www.hp.com
- www.paloalto.com
- www.juniper.com
- www.enterasys.com
- www.radware.com
- www.a10networks.com
- www.infoblox.com
- www.cisco.com
- www.fortinet.com
- www.mcafee.com
- www.veeam.com
- http://www.zerodayinitiative.com/
- http://es.wikipedia.org/wiki/Agregaci%C3%B3n_de_enlaces
- http://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html
- http://en.wikipedia.org/wiki/Routing
- http://www.pello.info/filez/firewall/iptables.html
- http://www.f5.com/it-management/solutions/global-load-balancing/overview/

MARIO ARENAS GARCÍA

- http://blog.aodbc.es/2012/05/21/introduccion-a-gslb-global-site-load-balance/
- http://es.wikipedia.org/wiki/Cableado_estructurado
- http://es.wikipedia.org/wiki/Modelo_OSI
- http://www.taringa.net/posts/ciencia-educacion/17185634/Modelo-tcp-ip-Informatica-Redes.html
- http://www.tirea.es/Menu/Entidades-Aseguradoras/Diversos/Redes-y-Correo/Acceso/MicroLan.aspx
- http://www.movistar.es/empresas/para-tu-oficina/redes/ficha/empresas-macrolan-vpn

12.6. CONCLUSIONES

En este apartado tenemos varias lecturas posibles. Podemos abordar las conclusiones desde un punto de vista técnico, viabilidad del proyecto, complejidad del proyecto, etc…en cualquiera de los casos estaríamos haciendo un análisis parcial.

Por tanto, lo más completo para exponer las conclusiones del proyecto es hacer una reflexión sobre los puntos clave que son aquellos que resultan cruciales a la hora de abordarlo. En consecuencia, lo primero que tendremos que hacer es comentar esos aspectos.

En este sentido, podrían identificarse los siguientes elementos claves de este proyecto:

- Alta disponibilidad: este es uno de los factores más importantes, desde el punto de vista técnico, del proyecto. Dadas las exigencias de la dirección de la universidad, y tal y como se ha detallado en el desarrollo del proyecto, se ha llevado una alta disponibilidad flexible, dinámica y rápida cumpliendo con tales exigencias.
- Extensión de infraestructuras: este factor clave dentro de la infraestructura IT de la universidad, se ha resuelto mediante la implantación de dos CPD trabajando en conjunto de forma síncrona. Es una solución que cumple con creces las expectativas iniciales, por lo que se considera que este punto ha sido satisfecho de forma eficiente.
- Viabilidad económica: este es, sin duda, el punto más débil del proyecto. Debido a que se trata de un entorno mediano, quizá no esté justificado un gasto tan elevado si pretendemos dar

MARIO ARENAS GARCÍA

cobertura a las necesidades actuales. Como parece ser que se espera un crecimiento exponencial, podemos asegurar que está justificado ya que es una inversión a largo plazo (mínimo 3 años).

- Entorno: la solución propuesta no suele ser propia de este tipo de entornos, más bien se trata una infraestructura con la que contaría una gran empresa o bien una organización cuya necesidad de mecanismos de alta disponibilidad sea crucial (como por ejemplo en un sistema sanitario o bancario). En cualquier caso, el desarrollo queda adecuado para este entorno.

Por último, únicamente comentar que, aunque el tiempo de ejecución del proyecto ha tenido que verse ajustado a los tiempos dados. Esos tiempos no se ajustan a la realidad ya que un proyecto de esta envergadura se desarrolla a lo largo de meses o años.

MARIO ARENAS GARCÍA