UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escuela Técnica Superior de Ingeniería Informática

Universitat Politècnica de València

Modelo de red segura en una PYME

Proyecto Final de Carrera

Ingeniería Informática

Autor: Hèctor Rodríguez i Santonja

Director: Lourdes Peñalver Herrero

29.08.2015

DEDICATORIA

A l'àvia Teresa, per fer-me estimar tot allò que estime avui.

Tabla de contenidos

1. INTRODUCCIÓN

1.1. Resumen

Desde el principio de la era digital, la informática ha contribuido en gran medida a la evolución y revolución en el ámbito empresarial, teniendo un papel fundamental en estos procesos. Las ventajas que aporta, así como las comodidades son innumerables: control de maquinaria, sistemas 24x7, software de gestión, comunicación global, servicios web, etc. No obstante, toda esta evolución tecnológica lleva consigo un nuevo paradigma, la seguridad informática y como está afecta directamente a la empresa.

Ante este nuevo escenario, es necesario hacer hincapié en la seguridad de la plataforma informática, tanto a nivel hardware como software. El objetivo de la seguridad informática no es otro que asegurar que los recursos de un sistema se utilizan según su fin inicial, y que tan sólo las personas designadas para ello, pueden manipular o acceder a dicha información. Para ello, es necesario conocer una gran variedad de campos en la seguridad informática: seguridad en la *LAN/WAN*, Programación segura, Desarrollo de aplicaciones seguras, *SQL Injection*, *DNS Spoofing, XSS, Hijacking, Spoofing, MITM*, seguridad física del entorno y una larga lista. Por otra parte, están las leyes y estándares que las empresas deben y deberían cumplir para el correcto funcionamiento de la misma:

En concreto, en este PFC se ha desarrollado y explicado una rama de la informática de todas las, la seguridad en la *LAN/WAN*. Los objetivos de este proyecto son los siguientes:

- Alta disponibilidad de los servicios críticos
- Facilitar la escalabilidad de la *LAN*
- Optimización de tráfico
- Mejora de la Calidad del Servicio
- Homogeneización
- Mejora de la seguridad
- Concienciación a todos los usuarios de la importancia de la seguridad en el ámbito de la informática, así como las posibles consecuencias de una brecha en la seguridad

1.2. Motivación

Basándome en mis conocimientos previos, adquiridos a lo largo de mis estudios académicos junto con la experiencia profesional, la motivación de este PFC surge de la idea de estudiar y diseñar un modelo de red seguro adaptable a cualquier empresa dependiendo del número de usuarios, así como una serie de pautas a aplicar para garantizar la seguridad en la empresa. Por otra parte, también he podido investigar acerca de la normativa vigente en materia de seguridad para las PYME y cuáles son los principales errores de estas en materia de seguridad.

1.3. Objetivos

- Garantizar la disponibilidad del servicio -> todos los bloques excepto el bloque *DMZ* disponen de dos o más elementos hardware que garantizan una alta disponibilidad durante la producción. Además, no tan solo los elementos hardware están redundados, sino que las interconexiones entre los elementos también lo están.
- Facilitar la escalabilidad -> con la topología de red implementada, se asegura una escalabilidad fácil y controlada, puesto que en caso de necesitar ampliar en un switch el bloque, bastaría con introducirlo dentro del anillo ya formado, asegurando una alta disponibilidad y fácil configuración.
- Mejorar la seguridad -> la implementación de dos *Firewalls* así como la separación de las distintas redes en *VLAN* proporcionan una gran capa de seguridad en la red, haciendo más difícil poder realizar cualquier ataque con éxito.
- Facilitar la gestión y el mantenimiento -> tener identificados los bloques por *VLAN* así como una configuración estándar en los switch, asegura las tareas de gestión y mantenimiento de la red.

2. SEGURIDAD INFORMÁTICA

2.1. Introducción

Gracias a la tecnología actual, hoy en día se dispone de multitud de información al alcance de cualquiera, de una manera rápida y sencilla. La manera en la que se obtiene y trata la información es radicalmente distinta a como era hace unos años, donde el papel y máquina de escribir, o en su defecto bolígrafo, eran los principales generadores de información y los archivadores la fuente donde buscar. En la época actual, con unos simples *click* se puede obtener más cantidad de información en unos segundos que toda la información almacenada durante décadas.

Al igual que antaño, la principal preocupación en cuanto a la conservación de la información era que se produjese un incendio o una inundación que provocara la pérdida total de esta, hoy en día la preocupación es otra. Existen multitud de sistemas de copia de seguridad que evitan que la información se pierda, *backup* en local, *backup* en la nube, sistemas de almacenamiento compactos, etc. Además de la conservación de la información, hay otro factor a tener en cuenta: la integridad. Es necesario proteger la información de: quien puede acceder, como y cuando.

Un sistema seguro sería aquel que no interactuara con ningún otro, sin conexión a ninguna red, y aun así y todo, tendríamos que preocuparnos de la seguridad física del sistema. No obstante es imposible imaginar un sistema de estas características, puesto que la información ha de ser accesible, bien por los usuarios que la necesiten en la empresa, porqué es pública, o cualquier otra razón.

2.2. Definición seguridad informática

Se entiende por seguridad informática a aquel proceso en el cual se protege, con el máximo grado de eficacia posible, los activos importantes para la empresa. Estos activos normalmente son software (archivos, código fuente, etc) pero también pueden ser hardware o todo aquel material que contenga información de carácter privado. Se puede decir que el concepto de seguridad informática, es aquel que se encarga de proporcionar protección a los sistemas informáticos y la información que contiene.

En este punto, y antes de proseguir con el proyecto, es importante que queden claros dos conceptos relacionados con la seguridad informática:

- **No existe ningún sistema seguro al 100%**
- **Un sistema informático es tan seguro como su eslabón más débil**

2.3. Conceptos básicos

Puesto que es imposible un sistema seguro al 100%, hay una serie de requisitos que cualquier Sistema Informático debe de cumplir con el tratamiento de la información, estos requisitos son conocidos como la tríada CIA (***C****onfidentiality,* ***I****ntegrity y* ***A****vailability*) y son los pilares básicos de cualquier sistema seguro:

2.3.1.Disponibilidad

Cuando los datos pasan a formar parte del sistema, estos deben de almacenarse de manera segura y estar disponibles en cualquier momento para aquel usuario, proceso o aplicación autorizado del sistema que los necesite. El objetivo pues es tratar de que los datos estén siempre disponibles de una manera transparente, sea cual sea la situación del sistema.

2.3.2.Integridad

Quien vaya a utilizar los datos necesita que estos no estén comprometidos o corruptos, estar trabajando en la versión más actual de ellos, en resumen tratar con la información más exacta posible. Para ello se debe asegurar que tan solo las personas/aplicaciones/procesos autorizados pueden acceder a dicha información y modificarla, registrando cada modificación realizada, de tal manera que se sepa en cada momento quien y cuando ha modificado algo.

2.3.3.Confidencialidad

Nadie con el suficiente nivel de privilegio puede acceder a la información y compartirla. Se debe asegurar el acceso a la información a las personas con nivel suficiente. Esta medida no solo se refiere a permisos en los ficheros, también contempla robo de información a través de dispositivos extraíbles, miradas, etc.

Además, existen otros dos conceptos necesarios de explicar: son la autenticación y el no rechazo:

2.3.4.Autentificación

Es necesario que en una comunicación, el receptor de un mensaje esté seguro de que el emisor del mensaje es quien dice ser y no ha habido una modificación previa a la recepción. Para ello se utilizan métodos de autenticación.

2.3.5.No rechazo

Estandarizado en la ISO-7498-2, esta norma permite que un determinado miembro de una comunicación (emisor, receptor o ambos) no pueda negar el envío o recepción de una comunicación.

El grado de implantación que tienen los sistemas informáticos hoy en día en una empresa, así como la gran cantidad de dispositivos que tienen la capacidad de conectarse a la red, ha generado un notable incremento en el número de ataques que se reciben, con diversos fines: denegación de servicio, robo de información, etc. Es por ello que es necesario entender que es un ataque informático y que tipos de ataques existen.

2.4. Ataque informático

Se entiende como ataque informático aquel proceso o método causado e intencionado, con el fin de realizar un daño o problema a un objetivo en concreto. Dicho ataque es posible a través de una vulnerabilidad o punto débil del sistema.

Por poner un ejemplo, en una PYME de unos 10 trabajadores es común encontrar entre 10-150 equipos conectados a la *LAN*. Cada una de estas máquinas es un posible punto de fallo en la seguridad de la red. Además, hay que tener en cuenta el alcance de las redes inalámbricas y los dispositivos móviles que se conectan a ella, por lo que en unos años los posibles objetivos vulnerables se han disparado respecto al pasado. Con esta cifra de posibles objetivos, no es de

extrañar que en los últimos años se haya producido un notable incremento de ataques y robo de información, utilizando equipos desde fuera de la *LAN* y equipos comprometidos en el interior de la *LAN*.

2.5. Anatomía de un ataque informático

Un ataque informático, suele seguir, una serie de fase. Es importante conocer dichas fases puesto que nos proporcionará conocimientos para reconocerlo antes de que pueda llevarse a cabo con éxito.

2.5.1. Fase 1 – Reconocimiento

El objetivo no es más que obtener información acerca del objetivo sobre el que se pretende realizar un ataque. Las herramientas utilizadas en esta etapa varían desde ataques de Ingeniería Social, hasta simples consultas en buscadores, pasando por técnicas de sniffing.

2.5.2. Fase 2 – Exploración

Una vez obtenida información básica del objetivo, hay que trabajar esta información con el fin de obtener información del sistema a atacar: datos de usuario, direcciones IP, topología, etc. Para ello las herramientas utilizadas aquí son de un nivel de complejidad mayor que en la anterior fase, se suelen utilizar herramientas de escaneo como *NMAP*, escaneos de vulnerabilidades, etc.

2.5.3. Fase 3 - Obtención de acceso

En esta fase se explotan aquellas vulnerabilidades detectadas en el sistema, los ataques varían desde ataques *DDoS, MiM*, ataques de fuerza bruta, etc.

2.5.4. Fase 4 - Mantener el acceso

Una vez dentro del sistema, el objetivo no es otro que asegurarse poder acceder siempre que se desee, utilizando troyanos o backdoors.

2.5.5.Fase 5 - Borrado de rastros

Para evitar la detección de la intrusión, o para eliminar pruebas del ataque, se realiza un borrado de todo aquello que puede ser útil a la hora de obtener información. Se eliminan los *LOG* de los distintos sistemas de defensa.

2.6. Tipos de ataques informáticos

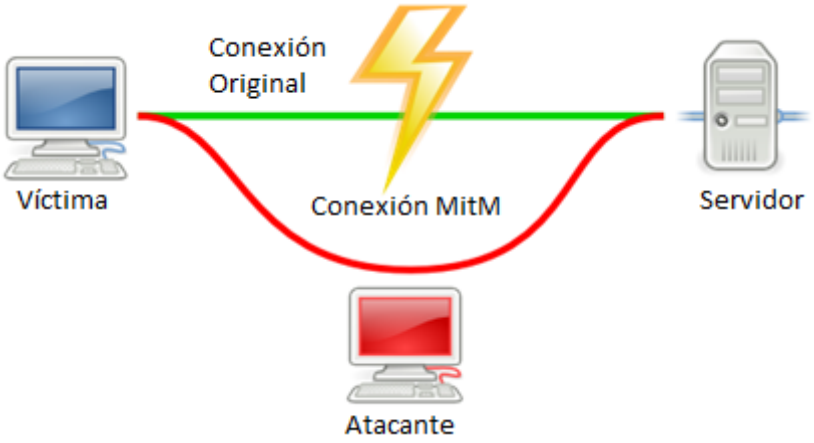
De entre la multitud de tipos de ataque informático que hay, se han seleccionados una pequeña variedad relacionada con la temática del PFC.

2.6.1.Man in the middle

Un ataque *Man in the Middle* es aquel que permite al atacante leer y modificar el mensaje original sin que ninguna de las dos partes tenga conocimiento de que dicha comunicación ha sido alterada. Hay muchos ataques *MITM*: *ARP Spoofing, DNS Spoofing, DHCP Spoofing, Port Stealing*, etc. En concreto, vamos a explicar el ataque *MITM* basado en el protocolo *ARP*.

En una comunicación normal, un usuario envía el paquete al switch/router y esté reenvía el paquete al destino en concreto. ¿Cómo sabe el switch/router cuál es el destino? Por las tablas *ARP*.

Las tablas *ARP* (Address Resolution Protocol) son las encargadas de asignar una IP a una *MAC* conocida, de tal manera que cuando llega un paquete con una *MAC* destino, el switch/router tan sólo tiene que comprobar esa *MAC* con que IP se corresponde y enviarla por el camino que corresponda. El atacante, en un ataque *MITM* lo que hace es engañar al origen/destino haciéndose pasar por el switch/router de tal manera que todos los paquetes pasan por el primero, y ahí es cuando puede ver o modificar el mensaje.



2.6.2.Ataque 0day

Un ataque 0day o día cero es aquel en el que se aprovecha una vulnerabilidad desconocida por los usuarios y fabricantes. Este tipo de ataques se solucionan con parches de actualización por parte de los fabricantes/desarrolladores, no obstante, son difíciles de prever y contener puesto que carecemos de información acerca de la vulnerabilidad usada.

2.6.3.Ataque DDoS

Conocidos como ataque de denegación de servicio, este tipo de ataques utiliza uno o varios equipos (pueden ser hasta miles) con el fin de que un servicio o recurso quede inaccesible tras colapsarse por una sobrecarga.

2.6.4.Fuerza bruta

Un ataque de fuerza bruta es aquel que consigue acceso a un sistema tras probar todas las combinaciones posibles de usuario/contraseña hasta conseguir una combinación válida.

2.6.5.Ingeniería social

Entendemos por ingeniería social al arte de conseguir información a través de la manipulación de las personas mediante engaños o persuasión y aprovechando la buena voluntad, ingenuidad o confianza del usuario. Esta técnica consigue su objetivo basándose en la premisa que el usuario es el eslabón más débil. Este tipo de ataques son muy difíciles de detectar y prever, puesto que se aprovechan del componente psicológico fruto de la confianza del usuario. Hay multitud de casos documentados de

estos ataques: el compañero que llama trabajando desde casa y necesita que se resetee el password, la necesidad de conectar un USB para imprimir un documento, etc.

3. LA SEGURIDAD EN UNA PYME

3.1. Introducción

Las redes, los sistemas informáticos, y la seguridad de la información son tan importantes como el propio producto de la empresa. Es por ello que la inversión en este campo es de capital importancia para una PYME, desde aspectos legales a comerciales, pasando por la ventaja en la competencia.

De todos los campos relacionados con la seguridad de la información que existen, este capítulo se centra en tres de ellos: el marco jurídico que engloba a una empresa, estándares aplicados al TI y la infraestructura de red.

En primer lugar está el marco jurídico. Hoy en día existen una serie de requerimientos legales, reguladores y estatuarios que obligan a la empresa a establecer una serie de medidas y controles con el fin de proteger los datos de carácter sensible.

Posteriormente encontramos una serie de estándares, que aseguran un a interoperabilidad y una calidad en la interacción de millones de componentes informáticos. Existen muchos tipos con funcionalidades y capacidades distintas, más adelante se detalla con mayor precisión aquellos relacionados con el ámbito en la seguridad de la información.

Y por último, y eje de este proyecto, el modelo de red o networking de una empresa. La velocidad a la que crecen los dispositivos con capacidad de interconexión es en muchas ocasiones una problemática para la empresa. Son muchos los casos en los que no se dispone de electrónica suficiente para abastecer dicho consumo, o no hay un esquema de red que permita crecer de manera controlada y homogeneizada, con las prestaciones que esto último significa. Puesto que se trata del tema más extenso, se describirá con mayor detalle en el siguiente capítulo.

3.2. Leyes Españolas

3.2.1.LOPD

LOPD o Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal. Vigente desde el año 2000 y según su definición oficial: es una ley que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. El objetivo de la misma es regular el tratamiento que se da a los datos de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

3.2.2. *LSSI*

Se trata de la Ley encargada de regularizar el comercio electrónico, con el fin de dotar al usuario de mayor protección y seguridad. Afecta a todas las personas físicas o jurídicas que presten algún servicio a través de una página web. Dicha ley obliga, entre otros puntos, a notificar al correspondiente registro mercantil en el que se esté inscrito, el nombre del dominio que se utiliza para prestar el servicio, domicilio social, C.I.F, datos de inscripción mercantil, etc.

3.3. Estándares

3.3.1. ISO/IEC 27001

Estándar internacional diseñado con la intención de proporcionar un modelo el cual permita implementar, operar, monitorizar, revisar y mantener un Sistema de Seguridad de la información. Para una organización, la implementación de la ISO/IEC 27001 supone un paso de calidad en lo que respecta a su trabajo. A la hora de implementarla, los objetivos, tamaño y estructura de la organización, marcará la rigurosidad de las medidas a aplicar.

3.3.2. ISO/IEC 27002

Se trata de una norma con carácter internacional en la cual se ofrecen consejos y recomendaciones de cara a la gestión de la seguridad de la información. Está dirigida a los responsables de mantener la seguridad en una organización. El objetivo de la misma es disponer de una base a través de la cual implementar normas de seguridad en una empresa sea un proceso sencillo, eficaz y práctico.

3.3.3. COBITs

Es un marco aceptado internacionalmente para el control de la información. El COBIT determina un conjunto de buenas prácticas para la eficacia, calidad y seguridad en las TI de una organización, siendo necesarias para alinear TI con el negocio.

3.3.4. *ITIL v3*

Se trata de un conjunto de buenas prácticas y no de un estándar, el cual tiene como finalidad facilitar la entrega de servicios de las TI. El *ITIL* comprende un extenso conjunto de prácticas y procedimientos de gestión, diseñados para ayudar a las organizaciones a lograr una calidad y eficiencia en las operaciones de TI. El origen del nombre de *ITIL* se corresponde por un conjunto de 30 libros dedicados a prácticas de gestión en las TI

3.3.5. *PRINCE 2*

Corresponde a una metodología de gestión de proyectos, la cual cubre todo el ciclo de vida de un proyecto a través de lo que se conoce como temáticas, los siguientes aspectos: la Calidad, el Cambio, la estructura de roles del proyecto (Organización), los planes (Cuánto, Cómo, Cuando), el Riesgo y el Progreso del proyecto.

3.4. Certificaciones recomendadas

3.4.1. CCNA

Certificación de la compañía CISCO, y que se entrega a los estudiantes que han aprobado el examen correspondiente. Esta certificación reconoce la habilidad para instalar, configurar y trabajar sobre dispositivos como routers y switch, redes *LAN* y *WAN*, así como distintos protocolos de red.

3.4.2. *CCNSP*

De un grado superior al *CCNA*, el *CCNP* certifica que, aquellos que han aprobado el examen, son capaces de implementar tecnologías apropiadas para crear redes escalables mediante routers, redes multicapa utilizando switch, mejorar los flujos de tráfico de datos y redundancia, así como mejorar la seguridad de las *LAN/WAN*, creación de Intranets, etc. En resumen, se trata de una certificación más completa que el *CCNA*

3.5. Errores típicos en una PYME

- No dar valor a la información o sistemas propios
- La seguridad es sólo cosa de informáticos
- Un antivirus y un *Firewall* son suficientes
- La seguridad como producto y no como proceso
- Falta de confidencialidad
- Cláusula de confidencialidad
- LOPD y su cumplimiento
- Servicios publicados
- Mantenimiento de la red

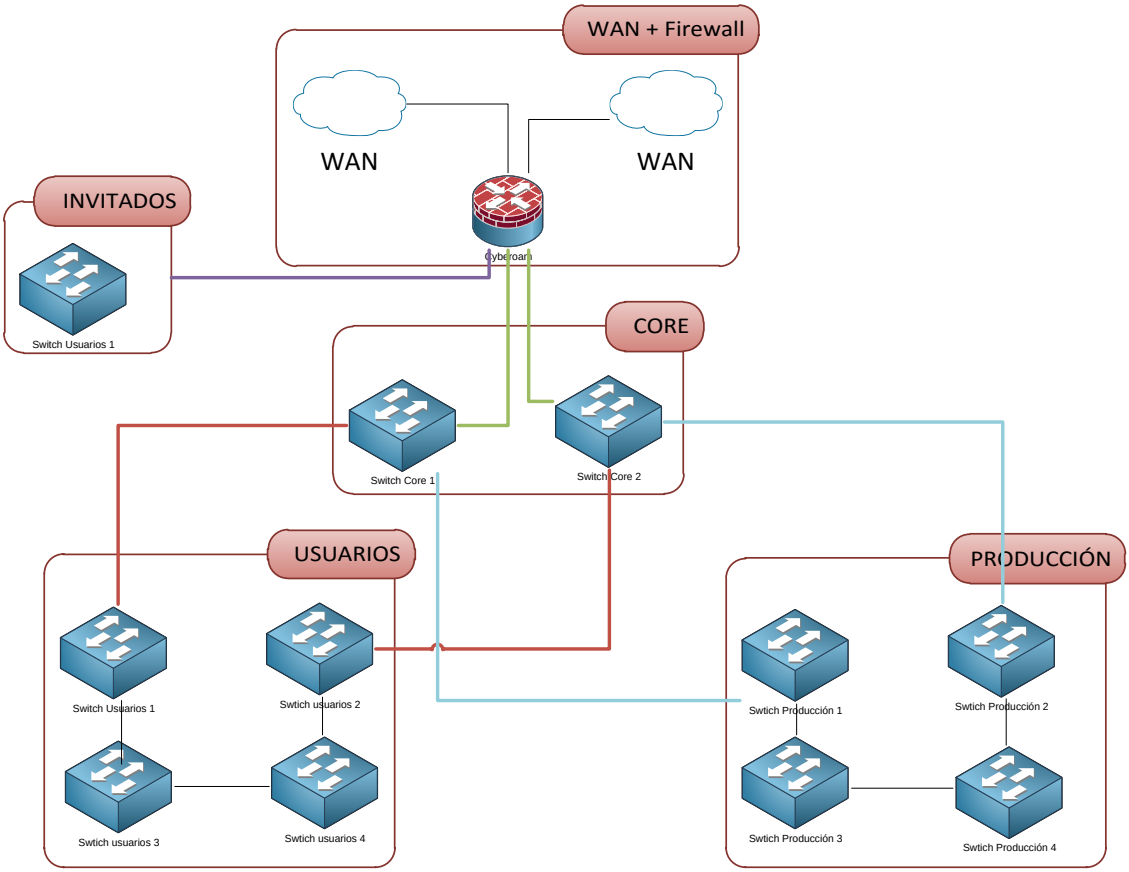
4. MODELO DE RED

4.1. Introducción

El objetivo principal de este modelo de red es el de normalizar a nivel físico la forma de interconectar los dispositivos de red así como dotar de una capa extra de seguridad a la red. El modelo de red propuesto consta de una estructura dividida en bloques funcionales, segmentados cada uno de ellos a nivel 3 del resto de bloques. Los bloques propuestos son:

1. *WAN+Firewall*
2. Producción
3. Usuarios
4. *DMZ*

Esta estructura de bloques se puede apreciar en la siguiente ilustración:



En las páginas siguientes se irán analizando uno por uno los diferentes bloques de los que consta el diseño de este modelo de red, así como la configuración de los equipos.

5. BLOQUE *WAN+FIREWALL*

5.1. Descripción

Este bloque consta de dos *Firewalls* Cyberoam en clúster HA configurados como activo-activo con puertos Gigabith Ethernet. Sirve para conectar a la *WAN* así como establecer túneles *VPN* con otras posibles sedes, labores de gestor de paquetes, filtrado web y de aplicaciones, restricciones por usuarios y QoS, IPS, gestor de *LOG*, etc. Además, los *Firewall* son los que realizaran las labores de capa 3 en la *LAN*.

Para efectuar dicha conexión, se sugieren las siguientes *VLAN*s:

- *DMZ* (*VLAN* 15): Conexión con la zona *DMZ*
- Servidores (*VLAN*20): Conexión con el bloque de producción
- Usuarios (*VLAN* 25): Conexión con el bloque de usuarios
- Invitados (*VLAN* 30): Invitados

En cuanto a las labores de *Firewall*, se realizará una configuración de seguridad que abarque reglas de *Firewall*, filtrado Web, filtrado de Aplicaciones, Antivirus y análisis tráfico. El esquema lógico de este bloque sería el siguiente:

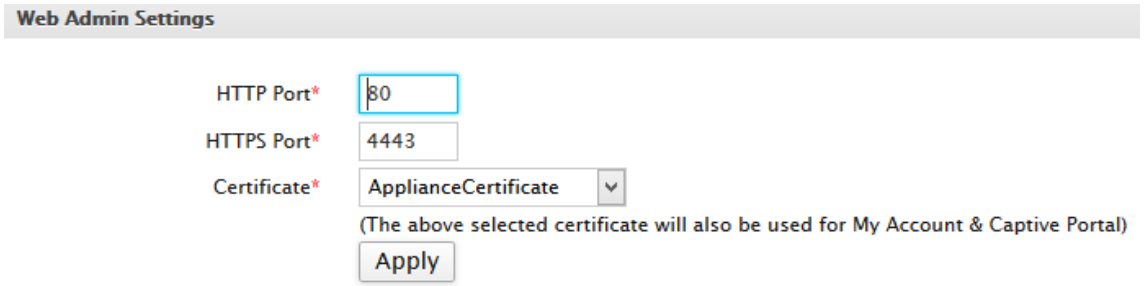
5.2. Cyberoam *Firewall*

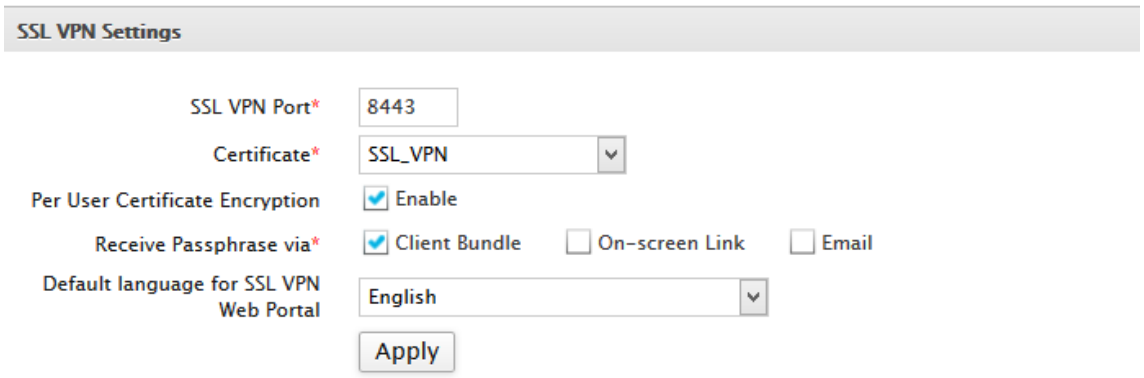
Se ha elegido la marca Cyberoam en cuanto al apartado de seguridad perimetral (*Firewall*). En los entornos actuales de red, junto con el aumento de número de usuarios, se ha producido una desperimetrizacion de las redes. Este factor junto con el aumento de usuarios y dispositivos de red, aplicaciones, etc. está provocando que las empresas pierdan el control sobre la seguridad de sus redes. En el entorno de red propuesto, se dispone de un clúster de *Firewalls* Cyberoam en Alta disponibilidad, funcionando de manera Activo-Activo y haciendo labores de L3. Cyberoam se trata de un *Firewall* con tecnología basada en Capa 8. El modelo utilizado es un Cyberoam CR25iNG

5.3. Configuración básica

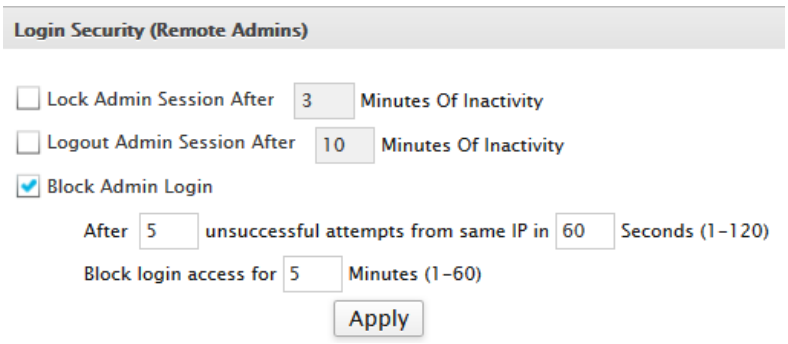
Dada la gran cantidad de parámetros que se permiten configurar, tan sólo se mostrará la configuración básica en lo referente a accesibilidad.

En cuanto a la accesibilidad, el Cyberoam queda configurado con el puerto 80 para el protocolo *HTTP* y con el puerto 443 para el protocolo *HTTPS*. En cuanto al portal cautivo para la *VPN*, el puerto utilizado será el 8443.



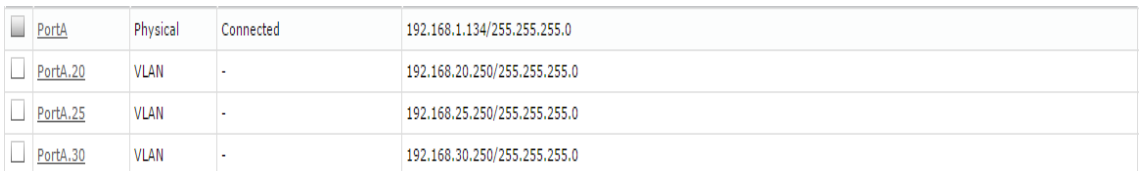


En lo que respecta a bloqueo por intentos fallidos, con el fin de evitar ataques de fuerza bruta se ha configurado la política de bloquear una IP durante 5 minutos si esta intenta acceder erróneamente 5 veces en 60 segundos.



5.4. Configuración Interfaces

El puerto A se ha utilizado en el Cyberoam para conectarlo a la *LAN*. En esta interfaz están configuradas las siguientes IP. Se puede observar como el Cyberoam dispone de una IP en la red 1, y el resto de IP en las *VLAN* correspondientes a los bloques descritos anteriormente.



☐	PortA	Physical	Connected	192.168.1.134/255.255.255.0
☐	PortA.20	VLAN	-	192.168.20.250/255.255.255.0
☐	PortA.25	VLAN	-	192.168.25.250/255.255.255.0
☐	PortA.30	VLAN	-	192.168.30.250/255.255.255.0

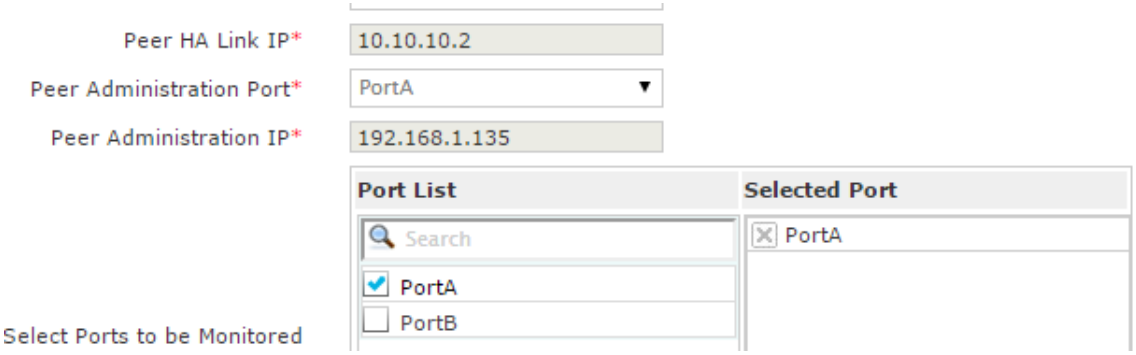
En cuanto al puerto B, se ha utilizado para la conexión contra la *WAN* (las IP públicas mostrada no se corresponden con las reales por motivos de seguridad).

☐	PortB	Physical	Connected	2.2.2.10/255.255.255.0
☐	PortB:0	Alias	-	2.2.2.11/255.255.255.0

El puerto C se ha utilizado para la zona *DMZ*:

☐	PortC	Physical	Connected	192.168.15.250/255.255.255.0

Para la configuración del, es la siguiente:



5.5. Reglas de *Firewall*

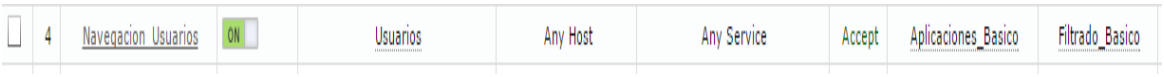
Puesto que el *Firewall* está dividido en interfaces, las reglas también están divididas en interfaces.

5.5.1.LAN -> WAN

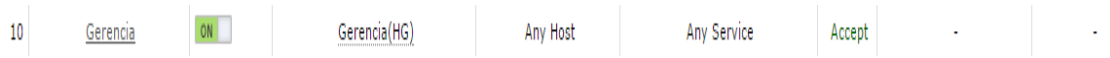
En esta primera regla, se habilita el tráfico *DNS* desde los equipos controladores de dominio a cualquier IP utilizando el servicio *DNS*. Esta regla se crea siguiendo las buenas prácticas de Cyberoam, en las cuales se recomienda que los controladores de dominio dispongan de una regla específica para dicha finalidad. Dependiendo de operadores y si se dispone de más de un *Gateway*, se debe dirigir el tráfico *DNS* por una *Gateway* u otro.

3	DNS	ON	Controladores_Dominio(HG)	Any Host	DNS	Accept

La siguiente regla se corresponde con la navegación de los usuarios de la red 192.168.25.0/24 hacia Internet. Esta regla tiene configurado el filtrado web así como el filtrado de aplicaciones. Creando esta regla específica se asegura que tan sólo los usuarios de la red 25 navegan por esta regla.



En ocasiones es necesario que exista una regla la cual no tenga aplicado ningún filtrado, ya sea de aplicaciones o web. Esta regla, tal y como se explica más adelante, si tiene aplicado el análisis antivirus. En el grupo de Gerencia se trata de un grupo de usuarios dentro de la red 25.



Al igual que en la regla de navegación usuarios, se han generado una regla que engloban la red de Producción y permite navegar a los equipos de la red. En esta ocasión si existe un filtrado web y de aplicaciones aplicado.

El Cyberoam tiene desplegado un servidor *DHCP* para la red de Invitados (explicado más adelante), como en los casos anteriores hay una regla que engloba dicha red, pero con algunas peculiaridades. En primer lugar, tan solo permite los servicios *DNS*, *HTTP*, HTTPS, *IMAP*, *POP3* y *SMTP*. Con esta medida se asegura que el equipo tan sólo pueda navegar a internet y utilizar el correo. Además, hay configurada una restricción QoS que limita el ancho de banda a 5 Mbps con tal de garantizar el tráfico para el resto de redes.

Por último, Cyberoam crea dos reglas que engloban a todos los equipos y todos los usuarios, siendo la opción por defecto permitir el tráfico. En la configuración actual, esta opción se ha cambiado y se han generado las reglas descritas anteriormente y que engloban por separado a las distintas redes, con el fin de evitar que cualquier equipo conectado a la red pueda navegar. Para ello, en la configuración de la regla está marcada la opción Drop.

	2	#LAN_WAN_LiveUserTraffic	ON	Any Host	Any Host	Any Service	Drop	User's Policy Applied	User's Policy Applied
	1	#LAN_WAN_AnyTraffic	ON	Any Host	Any Host	Any Service	Drop	-	-

Todas las reglas, tienen activado el análisis en tiempo real de paquetes *HTTP* y *FTP*.

5.5.2. *LAN -> LAN*

Con el fin de poder asegurar que los usuarios pueden trabajar correctamente, hay una regla que permite el tráfico de la red de usuarios a la red de producción, a aquellos servicios de aplicaciones que son necesarios. Dicha regla es la siguiente:

	LAN - LAN (Total 1)							
	16	LAN_LAN	ON	Usuarios	Produccion	Producción(SG)	Accept	

5.5.3. *DMZ -> WAN*

La regla que permite navegar desde la *DMZ* hacía la *WAN* tan solo engloba a un grupo de servidores (Servidores *DMZ*) y hacia el puerto B (puerto *WAN*). Lleva implementado el filtrado web y filtrado de aplicaciones.

	6	DMZ to WAN	ON	Servidores DMZ(HG)	#PortB	Any Service	Accept	Aplicaciones_Basico	Filtrado_Basico	-

5.5.4. *LAN -> DMZ*

De la *LAN* hacia la *DMZ* tan solo se permite el acceso por RDP e ICMP a un conjunto de ordenadores dentro del grupo Gestion_*DMZ*. Desde una *DMZ* no se debe poder acceder a la zona *LAN*, y en sentido inverso tan solo se debería permitir los servicios necesarios para la gestión de la misma. En este caso, la regla tiene habilitado el IPS para detectar posibles ataques desde dentro de la red.

	7	LAN to DMZ	ON	Gestion_DMZ(HG)	Servidores DMZ(HG)	PING , RDP	Accept

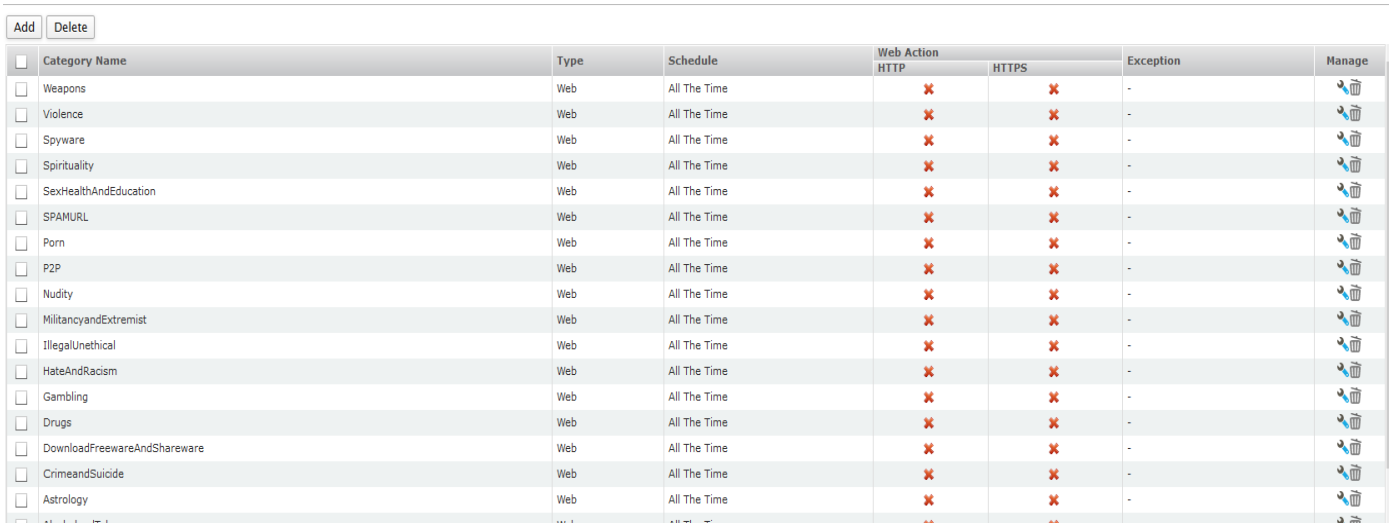
5.5.5. *WAN -> DMZ*

Las reglas creadas aquí son generadas automáticamente por el Cyberoam al crear los Virtual Host o NAT. Todas estas reglas tienen habilitado el IPS y permiten que el servicio publicado este accesible desde el exterior.

WAN - DMZ (Total 3)						
15	#Fichajes_Auto1	ON	Any Host	Fichajes	#Fichajes	Accept
13	#SAP Router_Auto1	ON	Any Host	SAP Router	#SAP Router	Accept
9	#Portal Web_Auto1	ON	Any Host	Portal Web	#Portal Web	Accept

5.6. Filtrado Web & Aplicaciones

Se ha optado por crear un filtrado Web básico de cara a la navegación de los usuarios, el cual restringe el acceso a Webs catalogadas dentro de la siguiente categoría.


Add Delete

Category Name	Type	Schedule	Web Action HTTP	Web Action HTTPS	Exception	Manage
Weapons	Web	All The Time	✖	✖	-	
Violence	Web	All The Time	✖	✖	-	
Spyware	Web	All The Time	✖	✖	-	
Spirituality	Web	All The Time	✖	✖	-	
SexHealthAndEducation	Web	All The Time	✖	✖	-	
SPAMURL	Web	All The Time	✖	✖	-	
Porn	Web	All The Time	✖	✖	-	
P2P	Web	All The Time	✖	✖	-	
Nudity	Web	All The Time	✖	✖	-	
MilitancyandExtremist	Web	All The Time	✖	✖	-	
IllegalUnethical	Web	All The Time	✖	✖	-	
HateAndRacism	Web	All The Time	✖	✖	-	
Gambling	Web	All The Time	✖	✖	-	
Drugs	Web	All The Time	✖	✖	-	
DownloadFreewareAndShareware	Web	All The Time	✖	✖	-	
CrimeandSuicide	Web	All The Time	✖	✖	-	
Astrology	Web	All The Time	✖	✖	-	

En caso de que un usuario trate de acceder a una página web catalogada dentro de las anteriores, el PopUp que verá es el siguiente. Con esta medida se evita que el usuario pueda acceder a sitios peligrosos o catalogados como no productivos por parte de la empresa.

Por otra parte, el filtrado de aplicaciones permite bloquear aplicaciones por protocolo, siendo esto muy útil para evitar túneles *VPN* o *SSH* desde dentro de la empresa, descargas *P2P*, etc. En este caso el usuario no verá ninguna imagen, sino que la conexión se cortará directamente.

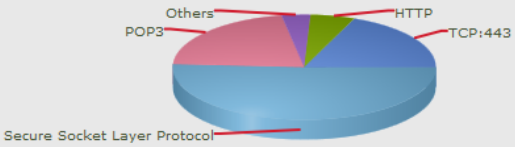
Application	Application Filter Criteria	Schedule	Action	Manage
Kongshare Proxy, HTTPort Proxy, Netevader Proxy, Avoidr Web Proxy, CyberGhost VPN Proxy, Proxyway Proxy, Proxy Switcher Proxy, Njutrino Proxy, K Proxy, Proxycap Proxy, Spinmyass Proxy, Camoproxy Proxy, Circumventor Proxy, Idhide Proxy, Lok5 Proxy, Your-Freedom Proxy, SOCK4 Proxy, Wallcooler VPN Proxy, Proxeasy Proxy, Tor2Web Proxy, Vpntunnel Proxy, MiddleSurf Proxy, RemoboVPN Proxy, Privitize VPN Proxy, Redirection Web-Proxy, Surrogofier Proxy, Proxifier Proxy, HTTP Tunnel Proxy, Asproxy Web Proxy, Cocoon, RealTunnel Proxy, Aniscartujo Web Proxy, Proximize Proxy, Securitykiss Proxy, Hamachi VPN Streaming, Air Proxy, Dtunnel Proxy, Bypassfw Proxy, Globosurf Proxy, JAP Proxy, AOL Desktop, SumRando, PD Proxy, Hide-Your-IP Proxy, Invisible Surfing Proxy, Kproxyagent Proxy, Zelune Proxy, Hide-My-IP Proxy, Proxyfree Web Proxy, VPNMakers Proxy, Tunnelbear Proxy Data, Suresome Proxy, Hide-IP Browser Proxy, Ultrasurf Proxy, Classroom Spy, Operamini Proxy, Sslpro.org Proxy, CProxy Proxy, I2P Proxy, Pingfu Proxy, Hotspotshield Proxy, Nateon Proxy, Mega Proxy, SOCK5 Proxy, Divavu Proxy, Kepard Proxy, Ztunnel Proxy, VPNium Proxy, 4everproxy Proxy, Spotflux Proxy, Proxify-Tray Proxy, Freegate Proxy, Proxy-service.de Proxy, Meebo Repeater Proxy, RPC over HTTP Proxy, FreeU Proxy, CyberghostVPN Web Proxy, OneClickVPN Proxy, My-Addr(SSL) Proxy, Vpndirect Proxy, Mysslproxy Proxy, Hopster Proxy, Skydur Proxy, Fly Proxy, HOS Proxy, Dynapass Proxy, Proxeasy Web Proxy, Ctunnel Proxy, WebFreer Proxy, Real-Hide IP Proxy, Telex, Expatshield Proxy, CoralCDN Proxy, PingTunnel Proxy, Socks2HTTP Proxy, Packetix Proxy, Simurgh Proxy, Ghostsurf Proxy, Puff Proxy, Auto-Hide IP Proxy, SSlunblock Proxy, Reduh Proxy, Toonel, Btunnel Proxy, ProXPN Proxy, Glype Proxy, Manual Proxy Surfing, Vtunnel Proxy, Rxproxy Proxy, Gbridge VPN Proxy, Vedivi-VPN Proxy, ZenMate, VNN-VPN Proxy, Max-Anonysurf Proxy, Frozenway Proxy, PHProxy, Tunnelbear Proxy Login, Gtunnel Proxy, Gapp Proxy, Psiphon Proxy, Sslbrowser Proxy, WiFree Proxy, TOR Proxy, ItsHidden Proxy, HTTP-Tunnel Proxy, ShadeYouVPN, Easy-Hide IP Proxy, IP-Shield Proxy, Justproxy Proxy, Launchwebs Proxy, Proxmachine Proxy, Hiddenvillage Proxy, FreeVPN Proxy	**Category** = Proxy and Tunnel	All the Time	Deny	
Manolito P2P Search, Piolet FileTransfer P2P, NapMX Retrieve P2P, Freenet P2P, Imesh P2P, Stealthnet P2P, Bearshare P2P, Ants IRC Connect P2P, Gnutella P2P, DirectConnect P2P, Manolito P2P Download, Phex P2P, QQ Download P2P, DC++ Hub List P2P, Kugoo Playlist P2P, Piolet Initialization P2P, GoBoogy Login P2P, DC++ Connect P2P, Klite Initiation P2P, Ares P2P, Manolito P2P Connect, MP3 Rocket Download, Soulseek Retrieving P2P, Winny P2P, Soul Attempt P2P, VeryCD, Pando P2P, Morpheus P2P, Shareaza P2P, DC++ Download P2P, WinMX P2P, Ants Initialization P2P, Ants P2P, Tixati P2P, Miro P2P, Torrent Clients P2P, Mute P2P, Peercast P2P, Manolito P2P GetServer List, 100BAO P2P, SoMud, Soulseek Download P2P, eMule P2P, Apple-Juice P2P, Vuze P2P, Flashget P2P, Napster P2P, Fileguri P2P	**Category** = P2P	All the Time	Deny	
TrialMadness Facebook Game, World Of Warcraft Game, Hyves Games, iPlay Website, Party Poker Website, Sina Games, Steam, WildOnes Facebook Game, Kongregate Game, Blokus Game, Necromanthus Game, JungleJewels Facebook Game, Call Of Duty 4 Game, Ace2Three Game, Yoville Facebook Game, Runesofmagic Game, Scramble Facebook Game, Pogo Website, Khanwars Game, Popcap Website, FrontierVille-Facebook Games, Ragnarokonline Game, Gamespy Game, MyTribe Facebook Game, Flashgames247 Game, TypingManiac Facebook Game, NightClubCity Facebook Game, PoolMaster Facebook Game, Facebook Games, Shockwave, AIM Games, Shockwave Game Website, Quake Halflife Game, Allslotscasino Game, Bored Website, Poker-Facebook Games, Doof Game, Winamax Game, Team-Fortress2 Game, PremierFootball Facebook Game, Chosenspace Game, Freeonlinegames Website, Minecraft Games, Windows Live Games, Y8 Game, Mail.ru Games, 51.COM Games, PetSociety-Facebook Games, Poker Stars Website, Metin Game, MillionaireCity-Facebook Games, Gamehouse Website, Ibibo Game, JewelPuzzle Facebook Game, Bejeweled-Facebook Games, Armor Games, Freeridegames Website, Xbox LIVE, Bomberclone Game, Bigfishgames Website, MobWars Facebook Game, Wordfeud Game, Battle-Net, Yahoo game, MindJolt-Facebook Games, Addicting Game, Bet365 Game, Sploder Game, JinWuTuan Game, Baidu.Hi Games, Mafia Wars-Facebook Games, Godgame, Omerta, EA.FIFA Game, FarmVille-Facebook Games, Hattrick Game, Evony Game, Doom3 Game, TreasureIsle-Facebook Games, Bigpoint Game, Roblox Game Play, Hangame, Playstation Network, Miniclip Games, Zango Website, Pokerstars Online Game, Zynga Game, CafeWorld-Facebook Games	**Category** = Gaming	All the Time	Deny	
MP3 File Download, AIM File Transfer, Filer.cx File Transfer, Hipfile Upload, Bayfiles Upload, Crocko Upload, SugarSync FileTransfer, Tortoise SVN, Okurin File Transfer, FileRio Upload, Filecloud.io File Transfer, Yahoo Webmail File Attach, Yahoo Messenger File Transfer, Fotki Media Upload, Multi Thread File Transfer, Justcloud File Transfer, NakidoFlag File Transfer, Rapidgator Upload, Hotfile Upload, HTTP Resume FileTransfer, Avaya Conference FileTransfer, Bitshare Upload, Egnyte File Transfer, Axifile File Transfer, Bonpoo File Transfer, Yahoo Messenger File Receive, Windows Live IM FileTransfer, File.host File Transfer, Filedropper File Transfer, iCloud, Fileserver File Transfer, Turbobit Upload, Sendspace Upload, Scribd File Transfer, Hotmail Webmail File Attach, Embedupload File Transfer, 1Fichier Upload, QQ Messenger File Transfer, Google Drive File Download, Gigaup File Transfer, TwitVid Upload/Download, IP Messenger FileTransfer, Putlocker Upload, Issuu File Transfer, Uploading File Transfer, Mendeley Desktop, Uptobox Download, EXE File Download, 2shared Upload, Meebo Messenger FileTransfer, SkyDrive File Upload, Google Drive File Upload, Minus Upload, Timbuktu FileTransfer, RAR File Download, Netload File Transfer, Gtalk Messenger FileTransfer, TrendMicro SafeSync, JDownloader, Webex File Transfer, Cubby File transfer, Bigupload File Transfer, Megashares Upload, Uptobox Upload, 4shared File Transfer, UbuntuOne FileTransfer, TwitPic Upload/Download, TeamViewer FileTransfer, SendMyWay Upload, Zshare Upload, SkyDrive File Download, Divshare File Transfer, Docstoc File Transfer, Serv-U RemoteAccess FileTransfer, Last.fm Free Downloads, ZIP File Download	**Category** = File Transfer	All the Time	Deny	

5.7. Cyberoam iView

Una de las características por las que se ha elegido esta marca es la funcionalidad de reportes, que permite generar informes completos sin necesidad de adquirir elementos HW aparte, así como la potencia de los informes. Con estos informes se facilita la labor al administrador del sistema de cara a saber por dónde se dirige su tráfico, protocolos utilizados, navegación de usuarios, etc.

En la siguiente captura, se puede observar que protocolos y el porcentaje de utilización respecto al tráfico total de la salida hacia Internet.

Top Applications

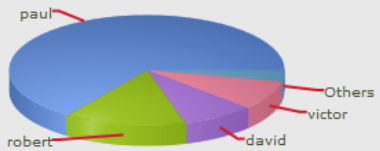


Application/Proto:Port	Category	Risk	Bytes	Percent
TCP:443	N/A	N/A	151.92 MB	18.61 %
HTTP	General Internet	4	45.68 MB	5.6 %
Others	N/A	N/A	29.89 MB	3.66 %
POP3	Infrastructure	1	173.23 MB	21.22 %
Secure Socket Layer Prot...	Infrastructure	1	415.59 MB	50.91 %

View All

Tal y como se ha comentado anteriormente, otra de las funcionalidades es la de obtener mayor información acerca de la navegación de usuarios.

Top Users

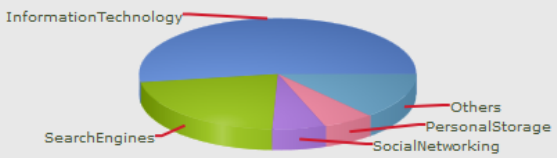


User	Bytes	Percent
paul	530.88 MB	65.03 %
robert	118.71 MB	14.54 %
david	70.39 MB	8.62 %
victor	69.55 MB	8.52 %
Others	26.79 MB	3.28 %

View All

Por último, otra de las características interesantes de cara a catalogar el tráfico, es el porcentaje de utilización según la categorización del mismo.

Top Web Categories



Category	Hits	Percent
InformationTechnology	157	52.33 %
SearchEngines	66	22 %
SocialNetworking	19	6.33 %
PersonalStorage	18	6 %
Others	40	13.33 %

View All

6. BLOQUE CORE

6.1. Descripción

Este bloque consta de dos switch HP ProCurve 2530 con 24 puertos de GigabitEthernet.

6.2. Funcionalidad

Este bloque sirve de unión entre todos los demás bloques del modelo de red, y su misión es conmutar paquetes entre los distintos bloques lo más rápidamente posible.

6.3. VLAN's

En el bloque de switch de core se han configurado las siguientes *VLAN* con el fin de realizar una configuración segura de red y segmentarla.

- *VLAN* 1 -> por defecto, utilizada para realizar el trunk con el otro switch de core.
- *VLAN* 5 -> utilizada para los puertos que conectan el switch con el puerto *WAN* del Cyberoam así como el puerto desde el router del proveedor. Con esta medida se otorga una protección extra de seguridad al tráfico.
- *VLAN* 15 -> Conexión con el bloque *DMZ*
- *VLAN*20 -> Conexión con el bloque de producción e IP del switch
- *VLAN* 25 -> Conexión con el bloque de usuarios
- *VLAN* 30 -> Conexión con el *DHCP* del Cyberoam

6.4. Configuración

A continuación, se detalla la configuración de los switch de core, desglosada con el fin de explicar más detalladamente.

En este primer bloque se muestra el nombre del switch así como la configuración de los trunk que enlazaran con los distintos bloques así como entre los switch de core.

```
; hpStack_WB Configuration Editor; Created on release #WB.15.16.0004
; Ver #06:0c.fc.f3.ff.35.0d:c2
   hostname "score-xx"
trunk 1/23-1/24 trk1 trunk
trunk 1/17-1/18 trk2 trunk
trunk 1/15-1/16 trk3 trunk
```

En el siguiente bloque se realiza la configuración de *NTP* para el switch contra un servidor público de *NTP* con el fin de tener siempre el switch con el tiempo actual.

```
timesync sntp
sntp unicast
sntp 30
sntp server priority 1 176.31.53.99
time timezone 60
```

En el siguiente bloque se realiza la configuración de *NTP* para el switch contra un servidor público de *NTP* con el fin de tener siempre el switch con el tiempo actual.

La puerta de enlace por defecto es la siguiente:

```
ip default-Gateway 192.168.20.250
```

En cuanto a la configuración de *VLAN*, es la siguiente. En primer lugar está la *VLAN* 1, la *VLAN* por defecto, en la cual está el puerto 19 y el Trk1 como untagged o acceso. El puerto 19 sirve de conexión entre el switch y el puerto *LAN* de nuestro *Firewall*. El Trk1 es el trunk que utilizamos para unir un switch con otro.

```
VLAN 1
name "Default"
untagged 1/19,Trk1
no ip address
exit
```

La *VLAN* 5 se utiliza para securizar la conexión contra la *WAN* del proveedor. En esta *VLAN* están como acceso los puertos 21 y 22, siendo el primero el puerto que conecta contra el Cyberoam y el segundo el puerto que conecta contra el router del proveedor. Además, se pasa como tagged o trunk la *VLAN*5 por el trunk de conexión con el otro swtich.

```
VLAN 5
name "WAN"
untagged 1/21-1/22
tagged Trk1
no ip address
exit
```

La *VLAN*20, la de producción, es la que se utilizará en todos los dispositivos para darles una IP de gestión. Además, también se utilizará para conectar con el bloque de producción.

VLAN 20
name "producción"
untagged Trk2
tagged Trk1
ip address 192.168.20.235 255.255.255.0
exit

La *VLAN*25 o de usuarios esta pasada por el Trk3 como untagged y como tagged en el trunk de enlace con el otro switch.

VLAN 25
name "usuarios"
untagged Trk3
tagged Trk1
no ip address
exit

En lo que respecta a la configuración de Spanning Tree, el protocolo utilizado es el rapid spaning tree. Se ha descartado el MSTP por la complejidad de este y el tamaño de la red. Los trunk tienen configurada por defecto la prioridad 4 en el spaning tree. En cuanto al dispositivo, el switch de core principal tendrá una prioridad de *STP* de 4 respecto a una prioridad de 6 que tendrá el switch core secundario.

spanning-tree
no spanning-tree Trk1 auto-edge-port
spanning-tree Trk1 priority 4
no spanning-tree Trk2 auto-edge-port
spanning-tree Trk2 priority 4
no spanning-tree Trk3 auto-edge-port
spanning-tree Trk3 priority 4
spanning-tree priority 4 force-version rstp-operation

En cuanto a la configuración de *VLAN*, es la siguiente. En primer lugar está la *VLAN* 1, la *VLAN* por defecto, en la cual está el puerto 19 y el Trk1 como untagged o acceso. El puerto 19 sirve de conexión entre el switch y el puerto *LAN* de nuestro *Firewall*. El Trk1 es el trunk que utilizamos para unir un switch con otro.

El resto de configuración es la configuración por defecto del switch así como los password del dispositivo.

no tftp server
no autorun

no dhcp config-file-update
no dhcp image-file-update
password manager

La configuración de puertos quedaría de la siguiente manera:

swcore01													
1	3	5	7	9	11	13	15	17	19	21	23	21	23
							Usuarios	Prod	A CYBEROAM	B Cyberoam	trk1		
							Usuarios	Prod	C CYBEROAM	WAN	trk1		
2	4	6	8	10	12	14	16	18	20	22	24	21	24

swcore02													
1	3	5	7	9	11	13	15	17	19	21	23	21	23
							Usuarios	Prod	A CYBEROAM	B Cyberoam	trk1		
							Usuarios	Prod	C CYBEROAM		trk1		
2	4	6	8	10	12	14	16	18	20	22	24	21	24

score01													
1	3	5	7	9	11	13	15	17	19	21	23	21	23
							U25	U20	U1	U5	U1, T5, 20, 25, 30		
							U25	U20	U 15	U5	U1, T5, 20, 25, 30		
2	4	6	8	10	12	14	16	18	20	22	24	21	24

score02													
1	3	5	7	9	11	13	15	17	19	21	23	21	23
							U25	U20	U1	U5	U1, T5, 20, 25, 30		
							U25	U20	U 15	U5	U1, T5, 20, 25, 30		
2	4	6	8	10	12	14	16	18	20	22	24	21	24

7. BLOQUE PRODUCCIÓN

7.1. Descripción

Este bloque de producción consta de dos switch con puerto de GigabitEthernet Cisco W2960 24S.

7.2. Funcionalidad

Sirve para tener controlado y asilado de la red de usuarios todos aquellos dispositivos destinados a la producción de la red de usuarios.

7.3. Configuración

La configuración de los bloques de producción es más sencilla que de los switch de Core, se desglosa a continuación:

La primera parte de la configuración consiste en los parámetros básicos del sistema operativo del switch cisco (iOS) así como la configuración de password del dispositivo y el nombre del mismo.

```
service timestamps debug datetime msec
service timestamps log datetime msec
hostname swprod-xx
boot-start-marker
boot-end-marker
enable secret 0 cisco
username cisco privilege 15 secret 0 cisco
aaa session-id common
clock timezone MET 1
clock summer-time MET recurring last Sun Mar 2:00 last Sun Oct 3:00
system mtu routing 1500
vtp mode transparent
no ip source-route
no ip domain-lookup
```

El siguiente bloque de configuración se corresponde al *STP* así como la prioridad que tiene. El protocolo es el mismo que en los switch de core y la prioridad es inferior para no entrar en conflicto.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree VLAN 1,20 priority 32768
```

VLAN internal allocation policy ascending

En cuanto al acceso de los puertos, en el caso de los switch de producción todos los puertos están configurados con la *VLAN*20 excepto los 4 últimos puertos utilizados para enlazar con los otros switch del bloque y con los switch de core.

```
VLAN 1
name Defecto
!
VLAN 20
name PRODUCCION
!
interface range GigabitEthernet 0/1-44
switchport mode access
switchport acces VLAN 20
spanning-tree portfast
!
interface port-channel 1
interface gigabitethernet 1/45
channel-group 1 mode on
interface gigabitethernet 1/47
channel-group 1 mode on
!
interface port-channel 1
switchport trunk encapsulation dot1q
switchport trunk allowed VLAN 1,20
switchport mode trunk
!
interface port-channel 2
interface gigabitethernet 1/46
channel-group 1 mode on
interface gigabitethernet 1/48
channel-group 2 mode on
!
interface port-channel 2
switchport trunk encapsulation dot1q
switchport trunk allowed VLAN 1,20
switchport mode trunk
```

Tal y como se ha indicado anteriormente, la gestión del switch estará en la *VLAN*20, por lo que la configuración es la siguiente:

```
interface VLAN20
ip address 192.168.20.XXX 255.255.255.0
no ip route-cache
no shutdown
ip default-Gateway 192.168.20.250
```

El bloque final es la configuración del *SNMP* así como los password de acceso a través de consola y la configuración del *NTP*

```
no ip HTTP server
no ip HTTP secure-server
SNMP-server community public RO
SNMP-server community private RW
tacacs-server directed-request
!
line con 0
password 0 cisco
line vty 0 4
password 0 cisco
transport input telnet
line vty 5 15
password 0 cisco
transport input telnet
!
NTP clock-period 36028840
NTP server 138.100.62.8
end
```

La configuración de los puertos quedaría de la siguiente manera:

swprod01																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
															Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Trk1	Trk2
															Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Dispositivo	Trk1	Trk2
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	3	4

swprod01																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
													U20	U20	U20	U20	U20	U20	U20	U20	U20	U20	U20	U1, T,20	U1, T,20
													U20	U20	U20	U20	U20	U20	U20	U20	U20	U20	U20	U1, T,20	U1, T,20
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	3	4

8. BLOQUE USUARIOS

8.1. Descripción

Este bloque de usuarios consta de dos switch con puerto de GigabitEthernet Cisco W2960 24S.

8.2. Funcionalidad

La función de este bloque es dar acceso a los puestos de usuario final de la red así como disponer de un acceso WiFi o cableado para los invitados.

8.3. Configuración

La configuración de los bloques de usuario es igual de sencilla que el bloque anterior:

```
service timestamps debug datetime msec
service timestamps log datetime msec
hostname swusua-xx
boot-start-marker
boot-end-marker
enable secret 0 cisco
username cisco privilege 15 secret 0 cisco
aaa session-id common
clock timezone MET 1
clock summer-time MET recurring last Sun Mar 2:00 last Sun Oct 3:00
system mtu routing 1500
vtp mode transparent
no ip source-route
no ip domain-lookup
```

El siguiente bloque de configuración se corresponde al *STP* así como la prioridad que tiene. El protocolo es el mismo que en los switch de core y la prioridad es inferior para no entrar en conflicto.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree VLAN 1,25,30 priority 32768
VLAN internal allocation policy ascending
```

En cuanto al acceso de los puertos, en el caso de los switch de producción todos los puertos están configurados con la *VLAN* 25 excepto los 4 últimos puertos utilizados para enlazar con los otros switch del bloque y con los switch de core.

```
VLAN 1
name Defecto
!
VLAN 25
name USUARIO
!
VLAN 30
name USUARIO
!
interface range GigabitEthernet 0/1-2
switchport mode access
switchport acces VLAN 30
spanning-tree portfast
!
interface range GigabitEthernet 0/3-44
switchport mode access
switchport acces VLAN 25
spanning-tree portfast
!
interface port-channel 1
interface gigabitethernet 1/45
channel-group 1 mode on
interface gigabitethernet 1/47
channel-group 1 mode on
!
interface port-channel 1
switchport trunk encapsulation dot1q
switchport trunk allowed VLAN 1,25,30
switchport mode trunk
!
interface port-channel 2
interface gigabitethernet 1/46
channel-group 2 mode on
interface gigabitethernet 1/48
channel-group 2 mode on
!
interface port-channel 2
switchport trunk encapsulation dot1q
switchport trunk allowed VLAN 1,25,30
switchport mode trunk
```

Tal y como se ha indicado anteriormente, la gestión del switch estará en la *VLAN*20, por lo que la configuración es la siguiente:

```
interface VLAN25
ip address 192.168.25.XXX 255.255.255.0
no ip route-cache
no shutdown
ip default-Gateway 192.168.25.250
```

El bloque final es la configuración del *SNMP* así como los password de acceso a través de consola y la configuración del *NTP*

```
no ip HTTP server
no ip HTTP secure-server
SNMP-server community public RO
SNMP-server community private RW
tacacs-server directed-request
!
line con 0
password 0 cisco
line vty 0 4
password 0 cisco
transport input telnet
line vty 5 15
password 0 cisco
transport input telnet
!
NTP clock-period 36028840
NTP server 138.100.62.8
end
```

En cuanto a la configuración final, quedaría de la siguiente manera:

swusua01																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
AP															Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Trk1	Trk2
															Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Usuario	Trk1	Trk2
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	3	4

swusua01																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
U30	U30												U25	U25	U25	U25	U25	U25	U25	U25	U25	U25	U25	U1, T,25	U1, T,25
													U25	U25	U25	U25	U25	U25	U25	U25	U25	U25	U25	U1, T,25	U1, T,25
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	3	4

9. BLOQUE *DMZ*

9.1. Descripción

Este bloque de *DMZ* consta de un único switch con puertos de GigabitEthernet Cisco W2960 24S.

9.2. Funcionalidad

La finalidad de este switch será conectar los puertos de aquellas máquinas que se quieran aislar físicamente de la red de producción y usuarios.

9.3. Configuración

La configuración del bloque *DMZ* no es muy distinta del resto de bloques:

```
service timestamps debug datetime msec
service timestamps log datetime msec
hostname swDMZ-xx
boot-start-marker
boot-end-marker
enable secret 0 cisco
username cisco privilege 15 secret 0 cisco
aaa session-id common
clock timezone MET 1
clock summer-time MET recurring last Sun Mar 2:00 last Sun Oct 3:00
system mtu routing 1500
vtp mode transparent
no ip source-route
no ip domain-lookup
```

El siguiente bloque de configuración se corresponde al *STP* así como la prioridad que tiene. El protocolo es el mismo que en los switch de core y la prioridad es inferior para no entrar en conflicto.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree VLAN 1,15 priority 32768
VLAN internal allocation policy ascending
```

En cuanto al acceso de los puertos, en el caso del switch *DMZ* todos los puertos están configurados con la *VLAN* 15.

```
VLAN 1
name Defecto
!
VLAN 15
name DMZ
!
interface range GigabitEthernet 0/1-24
switchport mode access
switchport acces VLAN 15
spanning-tree portfast
!
interface port-channel 1
interface gigabitethernet 1/25
channel-group 1 mode on
interface gigabitethernet 1/27
channel-group 1 mode on
!
interface port-channel 1
switchport trunk encapsulation dot1q
switchport trunk allowed VLAN 15
switchport mode trunk
!
interface port-channel 2
interface gigabitethernet 1/26
channel-group 2 mode on
interface gigabitethernet 1/28
channel-group 2 mode on
!
interface port-channel 2
switchport trunk encapsulation dot1q
switchport trunk allowed VLAN 15
switchport mode trunk
```

Tal y como se ha indicado anteriormente, la gestión del switch estará en la *VLAN*15, por lo que la configuración es la siguiente:

```
interface VLAN15
ip address 192.168.15.XXX 255.255.255.0
no ip route-cache
no shutdown
ip default-Gateway 192.168.15.250
```

El bloque final es la configuración del *SNMP* así como los password de acceso a través de consola y la configuración del *NTP*

```
no ip HTTP server
no ip HTTP secure-server
SNMP-server community public RO
SNMP-server community private RW
tacacs-server directed-request
!
line con 0
password 0 cisco
line vty 0 4
password 0 cisco
transport input telnet
line vty 5 15
password 0 cisco
transport input telnet
!
NTP clock-period 36028840
NTP server 138.100.62.8
end
```

La configuración final del switch sería la siguiente:

swDMZ01													
1	2	3	4	5	6	7	8	9	10	11	12	25	26
						DMZ	DMZ	DMZ	DMZ	DMZ	DMZ	Trk1	Trk2
						DMZ	DMZ	DMZ	DMZ	DMZ	DMZ	Trk1	Trk2
13	14	15	16	17	18	19	20	21	22	23	24	27	28

swDMZ01													
1	2	3	4	5	6	7	8	9	10	11	12	25	26
U15	U15	U15	U15	U15	U15	U15	U15	U15	U15	U15	U15	U1, T,15	U1, T,15
U15	U15	U15	U15	U15	U15	U15	U15	U15	U15	U15	U15	U1, T,15	U1, T,15
13	14	15	16	17	18	19	20	21	22	23	24	27	28

10. SERVIDOR *DHCP*

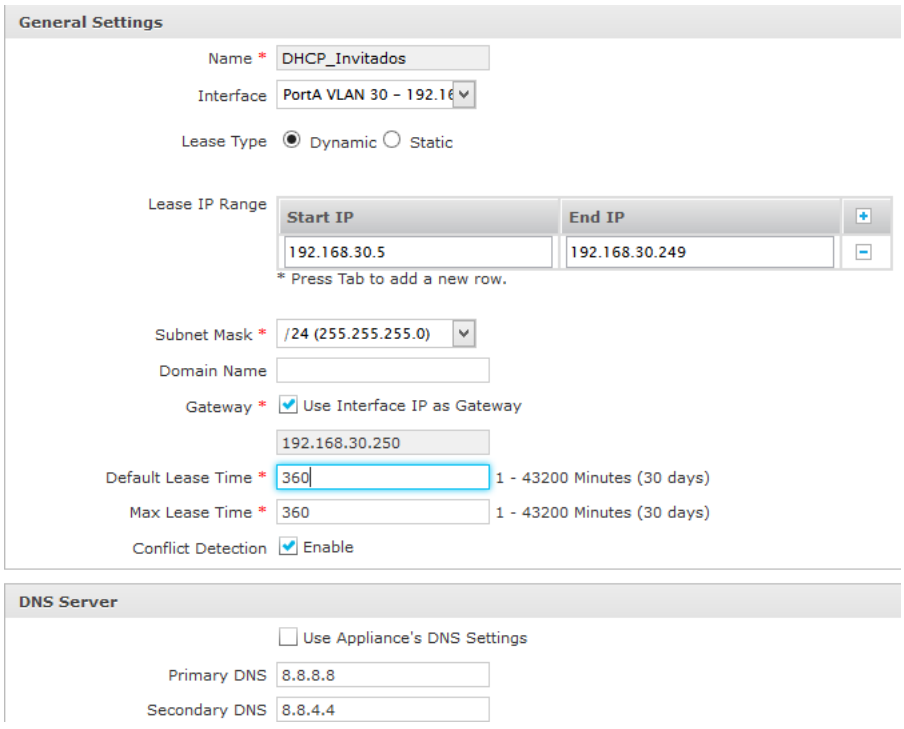
10.1. Descripción

Se ha incluido un servidor *DHCP* aprovechando la funcionalidad que ofrece el Cyberoam, de tal manera que se ha podido generar una red distinta para aquellos usuarios invitados, los cuales podrán navegar y recibir correo sin tener acceso a ningún otro equipo de la red.

10.2. Servidor *DHCP*

La configuración básica del servidor *DHCP* es la siguiente:

En cuanto a la configuración, es la siguiente:



Con la configuración del servidor, se dota a la empresa de una medida rápida y fácil de seguridad, además el *Lease* configurado asegura que el listado de direcciones IP no se acaban puesto que el Tiempo Máximo de concesión es de unas 6 horas. Para poder facilitar el *DHCP* a los equipos, se ha configurado en los puertos de los switch de acceso dos puertos en la *VLAN* 30.

Bien conectando un equipo directamente a la roseta indicada, o con la opción más fácil, configurando un punto de acceso, los usuarios dispondrán invitados dispondrán de una IP de manera automática.

10.3. Configuración de los puertos

Tal y como se ha comentado en el punto anterior, hay dos puertos configurados con la *VLAN* 30 de tal manera que en caso de conectar un equipo a la toma, y siempre y cuando la configuración de re de dicho equipo esté en *DHCP*, este recibirá automáticamente una IP libre del servidor *DHCP* del Cyberoam. Para ello es necesario configurar el puerto, dentro del bloque de usuarios, de la siguiente manera:

```
interface range GigabitEthernet 0/1-2
switchport mode access
switchport acces VLAN 30
spanning-tree portfast
```

En caso de necesitar más puertos, la solución pasaría por replicar dicha configuración en el puerto necesario.

11.VALORACIÓN ECONÓMICA

La oferta económica de un proyecto de tal calibre sería la adjunta en la imagen anterior, en ella están incluidos tanto el hardware necesario (*Firewall*, bloque core, bloque producción, bloque usuario, bloque *DMZ*) así como los servicios necesarios para realizar dicha instalación. Cabe tener en cuenta, que dicho presupuesto está basado en presupuestos parecidos ofrecidos a clientes, por lo que es posible que el precio mostrado no sea el precio de mercado al estar sujetos a posibles descuentos comerciales.

Producto	Cantidad	Descrpición	Total Neto
Cyberam	2	- Cyberoam 25 iNG para 50 usuarios como máximo, incluyendo los siguientes servicios: - Firewall - Antivirus - Application Filter - Web Filter - IPS - Reporting - L3 en la red - QoS - 3 años de suscripcion - 3 años de soporte 8*5	2.125,78 €
HP	2	- HP 2920-24G Swtich 10/100/1000 + 4 x GigaBit SFTP - Soporte HP Foundation Care Next Business Day 5 años	2.731,24 €
Cisco	5	- Cisco 2960-24s Swtich 10/100/1000 + 4 x GigaBit SFTP - Soporte Cisco Next Business Day 5 años - 2 para bloque producción - 2 bloque usuarios - 1 bloque DMZ	5346,58
Empresa proveedora	3	Servicios profesionales acorde al proyecto de sustitución y mejora de la infraestructura de la Pyme, con un total de 3 jornadas - Fase Análisis - Fase Ejecución - Fase Implementación - Fase Troubleshooting - Documentación	1.985,54 €
Total			**22.392,74 €**

12.CONCLUSIÓN

Las conclusiones que se pueden aportar acerca de **Modelo de red segura en una PYME** son las siguientes:

1. Se ha logrado definir con éxito, una base sobre la seguridad informática y las implicaciones que tiene en el entorno productivo actual.
2. Se ha sido capaz de dar una definición aproximada referente a algunos términos sobre la seguridad informática, sin utilizar un lenguaje 100% técnico, haciendo sencilla la explicación deseada.
3. El modelo de red se ha basado en un modelo escalable y fácilmente gestionable, que permita mantenerlo y crecer de una manera controlada y adecuada
4. Se ha garantizado una capa extra de seguridad con la separación de redes mediante las *VLAN*, sin una configuración extremadamente compleja y difícil de mantener
5. La implementación de políticas de QoS, filtrado Web y de aplicaciones, etc permite aportar un mayor control y seguridad, así como una buena experiencia de navegación, tanto al administrador de la red como a los usuarios.
6. Se ha añadido una valoración económica con equipamiento y precios basados en el mercado actual, que permite hacerse una idea de cuánto costaría realizar una inversión de este tipo y que equipamiento dispondrían con este, así como la inversión en horas necesaria.

13.BIBLIOGRAFÍA

Alonso, C. (s.f.). *El Lado del Mal*. Obtenido de www.elladodelmal.com

Benet, M. (29 de Mayo de 2013). *Security Art Work*. Obtenido de Security Art Work: http://www.securityartwork.es/2013/05/29/los-10-errores-tipicos-de-una-pyme-en-materia-de-seguridad/

Bermejo, I. T. (s.f.). *Fundacion Dedalo*. Obtenido de Fundacion Dedalo: http://www.fundaciondedalo.org/archivos/ACTIVIDADES/SSI08/TalleresHerramSegPYME.pdf

Garcia, M. I. (Octubre de 2008). *Adminso*. Obtenido de Adminso: http://www.adminso.es/images/1/1d/PFC_marisa.pdf

Garcia-Sabater, J. P. (11 de Enero de 2008). *Mi Official Site* . Obtenido de Mi Official Site : http://jpgarcia.webs.upv.es/?page_id=34

Kevin D. Mitnick, W. L. (2007). *El arte de la intrusión.* Ra-Ma.

Mena, E. (6 de Julio de 2013). *Sugerencias para la memoria de PFCs, TFMs, y Tesis Doctorales*. Obtenido de Sugerencias para la memoria de PFCs, TFMs, y Tesis Doctorales: http://eolo.cps.unizar.es/docencia/PFC/Sugerencias-Documentacion.pdf

Mieres, J. (Enero de 2009). *Evil Fingers*. Obtenido de Evil Fingers: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Molina, J. (12 de Enero de 2012). *La neutralidad de red*. Obtenido de La neutralidad de red: http://laneutralidaddered.blogspot.com.es/2012/01/pfc-la-neutralidad-de-red-gestion-de.html?m=1

Moya, J. M. (2005). *Seguridad en Redes y Sistemas Informáticos.* Paraninfo.

Nuñez, A. A. (14 de Junio de 2014). *Seguridad Informática "A lo Jabalí"*. Obtenido de Seguridad Informática "A lo Jabalí": http://www.seguridadjabali.com/2014/06/seguridad-informatica-definicion.html

Opentia. (29 de Enero de 2007). Obtenido de Opentia: http://people.ffii.org/~abarrio/estandares/OPENTIA-estudio-TiposDeEstandares-20070129.pdf

Pérez, A. (13 de Junio de 2013). *LOPD, LSSI e Email Marketing, lo mínimo que deberías conocer*. Obtenido de LOPD, LSSI e Email Marketing, lo mínimo que deberías conocer: http://www.teenvio.com/es/consejos/lopd-lssi-email-marketing/

Plaza, J. J. (Septiembre de 2005). *Departament d'Enginyeria Informàtica i Matemàtiques*. Obtenido de Departament d'Enginyeria Informàtica i Matemàtiques: https://deim.urv.cat/~pfc/docs/pfc307/d1126605824.pdf

Pol. (19 de Febrero de 2009). *Kaos Klub*. Obtenido de Kaos Klub: http://www.kaosklub.com/recursos-y-consejos-para-hacer-el-pfc-proyecto-final-de-carrera/

Ramírez, J. C. (Agosto de 2008). *Instituto de Investigación Tecnológica*. Obtenido de Instituto de Investigación Tecnológica: http://www.iit.upcomillas.es/pfc/resumenes/48ca15671b800.pdf