VNIVERSITAT DE VALÈNCIA

Escola Tècnica Superior d'Enginyeria

Proyecto Final de Carrera

ESTUDIO Y EVALUACIÓN DE NUEVAS HERRAMIENTAS DE SEGURIDAD APLICADAS A UNA EMPRESA PÚBLICA

Autor:
D. Ignacio Cantó Salinas

Tutor:
D. Santiago Felici Castell
Director:
D. Ángel Alonso Parrizas

Burjassot, Mayo de 2008

Agradecimientos

A mis padres por tantas cosas, que es imposible escribirlas.

A mis hermanos que como mis padres, menos la vida, me lo han dado todo.

A Mati por estar ahí siempre, te quiero.

A mi tía Maritere.

A toda mi familia.

A mis amigos de la Universidad, por los grandes momentos que hemos pasado juntos y los que nos quedan.

A la Generalitat Valenciana, por haberme permitido utilizar sus equipos y recursos, en especial a Marlen.

A Enrique, compañero y siempre seguro mitigador de dudas.

Finalmente a Santi y a Ángel por haber hecho posible que este proyecto viera la luz.

Gracias a todos.

Índice general

Índice de figuras

Índice de tablas

Resumen

En el presente proyecto se abordará la problemática generada en la Generalitat Valenciana (GVA) a raíz del final de servicio de mantenimiento del concentrador de túneles VPN, concretamente el Cisco VPN3060.

Cuando se tuvo conocimiento del final del servicio de mantenimiento y actualización se planteó forzosamente su sustitución, no porque no diera el servicio que se le demandaba, sino porque la GVA en su política de seguridad no permite que hayan equipos sin mantenimiento.

Tras plantearnos los objetivos del presente proyecto pasaremos a explicar de modo breve las tecnologías sobre las que luego habremos de tomar decisiones.

Una vez conozcamos cómo es la red corporativa de la GVA, cómo funciona en ella el servicio VPN (Virtual Private Network), cuáles son nuestras necesidades y de qué tecnologías disponemos, podremos definir lo que serán los requisitos del sistema futuro. Estos requisitos los obtendremos haciendo un análisis comparativo justificado de las opciones tecnológicas de las que se dispone.

Se implementará el nuevo sistema y una vez en producción, con datos, se verá como las decisiones tomadas fueron las adecuadas. Veremos punto por punto cómo la migración ha sido llevada a cabo de tal manera que se han mejorado todas las facetas del servicio, tanto por parte del usuario como de sus administradores.

Acabaremos viendo cuál ha sido el coste total del proyecto y listaremos una serie de futuras acciones que podrían complementarlo.

Capítulo 1.
Introducción

Con el paso del tiempo las empresas han visto la necesidad de que las redes de área local superen la barrera de lo local permitiendo la conectividad de su personal y oficinas en otros edificios, ciudades, comunidades autónomas e incluso países.

Antes se usaban líneas dedicadas que resultaban ser carísimas y críticas. Con la aparición de internet, las empresas, centros de formación, organizaciones de todo tipo e incluso usuarios particulares tienen la posibilidad de crear una Red Privada Virtual (VPN) que permita la conexión entre diferentes ubicaciones salvando la distancia entre ellas.

Entendemos por VPN la interconexión de un conjunto de ordenadores haciendo uso de una infraestructura pública (como internet, red ATM o Frame Relay), normalmente compartida, para simular una infraestructura dedicada o privada.

Las VPNs utilizan protocolos especiales de seguridad que permiten obtener acceso a servicios de carácter privado, únicamente a personal autorizado, de una empresa, centros de formación, organizaciones, etc. Debido al uso de redes públicas, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados. En el traslado a través de internet la autenticación y la encriptación son cuestiones críticas para asegurar la confidencialidad e integridad de los datos transmitidos.

Cuando un usuario se conecta vía internet, la configuración de la VPN le permite conectarse a la red privada del organismo con el que colabora y acceder a los recursos disponibles de la misma como si estuviera tranquilamente sentado en su oficina sufriendo las limitaciones asociadas a la capacidad del servidor de túneles y, si accede a destinos ubicados fuera de la red local de su empresa sufrirá también las limitaciones que le imponga la conexión a internet que tenga su empresa.

1.1 Problemática

El VPN corporativo de la Generalitat Valenciana (GVA) ofrece un servicio de conexión segura a la Red Corporativa (RC) desde el exterior. Gracias a este servicio conseguimos que el personal de la GVA que quiera acceder a la RC de manera remota pueda hacerlo de forma que el tráfico de datos vaya siempre cifrado fuera de nuestra red, hasta el punto final de cliente, impidiendo que pueda escucharse en puntos intermedios. Así mismo, se utiliza para proporcionar acceso a empresas externas que

ofrecen un servicio de mantenimiento y monitorización de los distintos servidores y aplicaciones dentro de la GVA.

El acceso a la RC de la GVA a través de este servicio se realiza siempre de manera personal, utilizando los certificados digitales de la Autoridad de Certificación de la Comunidad Valenciana (ACCV). El certificado digital permite asegurar inmediatamente las transacciones en línea, con su servicio de autenticación, confidencialidad de mensajes y garantía que la información transmitida es recibida exactamente como fue enviada. Todos los accesos son registrados y guardados en un servidor con la hora y el día, permitiendo poder exigir responsabilidades en caso de uso indebido.

Actualmente hay más de 1.300 usuarios dados de alta en este servicio y cada mes se realizan entre 60 y 80 nuevas altas. Diariamente se realizan entre 300 y 400 accesos a la RC utilizando este sistema, y durante el horario laboral se mantienen constantes entre 80 y 100 usuarios concurrentes.

Cisco, el fabricante del concentrador VPN 3060 que se usaba anteriormente, anunció ya hace tiempo la desaparición del mercado de este producto. Desde Noviembre de 2006 Cisco no desarrollaba, reparaba, mantenía o realizaba pruebas de este producto. No se podrá realizar ningún tipo de contrato de servicio relacionado con este producto a partir de agosto de 2008. Además, todos los servicios de soporte desaparecerán en Noviembre de 2008, considerando a partir de esa fecha el producto como obsoleto.

Los sustitutos de los VPN 3000 de Cisco, son los Cisco ASA 5500 que poseen la doble funcionalidad de cortafuegos y concentradores VPN. Es precisamente la dualidad cortafuegos/concentrador VPN la que ha hecho que este sustituto natural del equipo que había hasta ahora no fuera valorado, ya que la política de la GVA es el uso de máquinas exclusivas dedicadas para los servicios que se ofrecen. El hecho de que el ASA 5500 también sea cortafuegos hace que el producto se encarezca y que su procesador no esté dedicado en exclusiva a las labores de creación de túneles VPN. En definitiva, por un precio inferior podemos encontrar máquinas de otras marcas que hagan de concentradores VPN exclusivamente.

La inminente desaparición del mercado del concentrador VPN 3060 hacía necesaria la búsqueda de otro sistema que permitiera a la GVA poder ofrecer el mismo servicio e incluso realizar mejoras e incluir nuevas funcionalidades. En el último año, con la integración de la GVA en la Red Interadministrativa de los Ministerios (SARA), la demanda de accesos a los distintos servicios que ofrece esta red interadministrativa ha crecido en gran medida. El perfil de los usuarios que reclaman estos servicios, lejos de ser técnico, dificulta la utilización del típico *software* de cliente VPN.

En base al informe de la consultoría Gartner **[Apéndice A]** que recomienda como punteros en este terreno a Juniper y Aventail se pidió a ambas empresas que hicieran sendas presentaciones de sus productos y que permitieran a la GVA las pruebas con las respectivas máquinas.

1.2 Motivación

Mi labor como becario en la GVA consiste en una participación activa en la administración de los sistemas de seguridad y mantenimiento de la RC. Concentrador VPN, cortafuegos, balanceadores de carga, servidores DNS, gestores de tráfico, etc. son varias de las tecnologías de uso diario.

En este proceso de aprendizaje surge la oportunidad de participar en la implantación de un nuevo concentrador VPN, lo que me ha dado la ocasión de poder justificar y documentar todo el cambio además de configurar los nuevos equipos.

1.3 Objetivos

El objetivo de este trabajo es llevar a cabo y documentar la migración del servicio del concentrador Cisco VPN3060 a uno nuevo, concretamente el Juniper SA 4000. Al final de este proceso el sistema quedará en proceso de producción. Los pasos a seguir para conseguir este objetivo serán:

- ✓ Análisis de la tecnología anterior utilizada y su configuración.
- ✓ Análisis de la problemática asociada a ella.
- ✓ Análisis de las posibles alternativas tecnológicas.
- ✓ Establecimiento de requisitos, diseño del nuevo sistema.
- ✓ Elección de la nueva máquina.
- ✓ Implementación del nuevo sistema
- ✓ Puesta en producción del nuevo sistema.
- ✓ Análisis del nuevo sistema. Comprobación de las mejoras.
- ✓ Documentación la migración.

Es fundamental el llevar a cabo la migración de modo trasparente para el usuario y sin la interrupción del servicio.

1.4 Resumen

La conexión VPN a la RC de la GVA es un servicio fundamental. El concentrador de túneles que se venía usando hasta ahora ha sido declarado como obsoleto.

Hay que hacer un estudio de las tecnologías existentes a día de hoy para establecer unos requisitos y de las máquinas dedicadas de las que se dispone en el mercado para buscar un sustituto al declarado como obsoleto. Una vez tengamos los requisitos y sepamos la máquina sustituta habremos de configurarla y ponerla en producción, todo ello de forma trasparente para el usuario.

Capítulo 2.
Estado del Arte

A lo largo del presente capítulo se hará una introducción teórica de los conceptos que usaremos en el presente y en capítulos posteriores para poder entender en qué se basa la tecnología para crear Redes Privadas Virtuales (VPNs) seguras y confiables. También para poder entender el por qué de las decisiones que se tomaron en su día para la elección del nuevo concentrador de túneles VPN.

Primero se explicarán los distintos tipos de autenticación existentes, basadas en RADIUS (Remote Authentication Dial-In User Service) o basadas en LDAP (Lightweight Directory Access Protocolo). La primera de ellas es la que se utilizaba en el modelo anterior de concentrador de túneles (Cisco VPN 3060), concretamente FreeRADIUS y la segunda es la que se utiliza en el nuevo Juniper, en concreto OpenLDAP.

Una vez hayamos demostrado a nuestro interlocutor que somos quienes decimos ser y él haya hecho lo propio (autenticación mutua), tendremos que proteger la información que vayamos a intercambiar. Para eso, para cifrar la información intercambiada, usaremos cifrado de clave pública o asimétrico (lento) para intercambiar las claves de sesión y cifrado de clave privada o simétrico (rápido) para el intercambio de la información dentro de la sesión.

Además de garantizar la confidencialidad de la comunicación, es necesario garantizar la integridad de los datos intercambiados, así, se explicarán las diferentes posibles implementaciones criptográficas de las que tanto el antiguo concentrador VPN como el nuevo hacen uso. Se hablará de los algoritmos MD5 (Message-Digest Algorithm 5) y SHA (Secure Hash Algorithm).

Todas estas tecnologías criptográficas y de autenticación se integran en los protocolos de red seguros, en lo que se basan las tecnologías VPN, por lo que se hará un estudio profundo de las diferentes tecnologías de VPN que son: IPSec (Internet Protocol Security) y SSL (Secure Sockets Layer).

La soluciones VPN puede hacer uso de certificados digitales, tanto en la parte sevidora como en la cliente. De los certificados digitales y de otros conceptos importantes, como las Infraestructura de Clave Pública (PKI), hablaremos en el apartado siguiente. La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar

digitalmente información, garantizar el no repudio de un envío y otros usos. Describiremos una serie de conceptos asociados a ella que nos servirán para tomar decisiones de configuración de los nuevos equipos, en el caso de la Lista de Certificados Revocados (CRL), o para describir el funcionamiento del sistema de la GVA a través de su Autoridad de Certificación (AC) que es la ACCV.

Veremos a continuación un par de casos particulares de certificados digitales como son el DNI electrónico y la firma digital.

Con los conceptos relativos a las PKIs claros y habiendo visto el par de ejemplos de certificados digitales anteriormente, pasaremos a describir exhaustivamente la ACCV como PKI necesaria para la ejecución del servicio VPN de la GVA.

Finalmente y para terminar el capítulo se verán las distintas opciones de las que se dispone para la creación de túneles VPN, desde la aplicación *software* a el uso de máquinas altamente especializadas. De éstas últimas se verán tres modelos.

2.1 Métodos de autenticación

Existen dos modelos de autenticación uno descentralizado y otro centralizado. En el modelo descentralizado, cada servicio de la red maneja sus claves de forma independiente, por ejemplo los usuarios de Oracle, los usuarios de un cortafuegos, los administradores de un sitio Web, cada una de estas aplicaciones maneja por separado sus claves y las mismas no son compartidas.

En la autenticación centralizada los usuarios y sus claves se ubican en un repositorio central, las diferentes aplicaciones se configuran para identificar este lugar y hacer la autenticación contra el repositorio. Para nuestro caso las claves estarán ubicadas dentro de un servidor de directorio LDAP o serán accedidas mediante el protocolo RADIUS, pero en general podrían estar almacenadas en un archivo de texto plano o en una base de datos relacional entre otros métodos de almacenamiento de información.

En el concentrador CiscoVPN se utilizaba RADIUS como medio para autenticar a los usuarios que habían solicitado el servicio y habían sido dados de alta en el mismo. En el concentrador Juniper lo que se usa es LDAP con el mismo objetivo.

2.1.1 Protocolo RADIUS

RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación, autorización y manejo de cuentas de usuario

originalmente desarrollado por Livingston Enterprises y publicado en 1997 como los RFC 2058 y 2059 **[RFC]**. Es utilizado para administrar el acceso remoto y la movilidad IP, como ocurre en servicios de acceso por modem, DSL (Digital Subscriber Line), servicios inalámbricos 802.11 o servicios de VoIP (Voice over IP). Este protocolo trabaja a través del puerto 1812 por UDP (User Datagram Protocol).

RADIUS permite la administración centralizada de la autenticación de los datos, tales como nombres de usuario y contraseñas. Puede aumentar significativamente la seguridad al permitir la centralización de la administración de contraseñas. Por supuesto, la otra cara de ese argumento es que una vez que obtengamos el control del servidor, lo tenemos todo. Utiliza el algoritmo de integridad MD5 para la contraseña de seguridad de *hashing*[1].

Cuando se realiza la conexión con un ISP (Proveedor de Servicios de Internet) mediante módem, DSL, cablemódem, Ethernet o Wi-Fi (Wireless-Fidelity), se envía una información que generalmente es un nombre de usuario y una contraseña. Antes de que el acceso a la red sea concedido, esta información es procesada por un dispositivo NAS (Network Access Server) a través del protocolo PPP (Point-to-Point Protocol) siendo posteriormente validada por un servidor RADIUS a través del protocolo correspondiente valiéndose de diversos esquemas de autenticación, como PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol) o EAP (Extensible Authentication Protocol)

Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, los datos se pueden utilizar con propósitos estadísticos o simplemente para tener un control del uso que hacen los usuarios del sistema. Estos datos son guardados en un archivo que se suele ser llamado *log.* A continuación podemos ver un pequeño fragmento de este archivo para un usuario en particular,

15950 03/27/2008 16:28:44.580 SEV=5 IKE/79 RPT=41804 89.23.222.223
Group (PFC)
Validation of certificate successful
(CN=JOSE IGNACIO FERRERO SANZ - NIF:25557759G, SN=B9D4F3AA0415D8)

El certificado del usuario es correcto.

15953 03/27/2008 16:28:44.930 SEV=4 IKE/52 RPT=38096 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G) authenticated.

[1] La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos sobre los que se calcula, MD5 en este caso.

La autenticación del usuario es correcta.

15955 03/27/2008 16:28:45.070 SEV=5 IKE/184 RPT=37275 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
Client Type: WinNT
Client Application Version: 4.8.02.0010

Aplicación Cliente del servicio VPN y sistema operativo sobre el que está corriendo.

15960 03/27/2008 16:28:46.020 SEV=5 IKE/25 RPT=39420 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
Received remote Proxy Host data in ID Payload:
Address 172.31.3.52, Protocol 0, Port 0

IP del usuario que accede al servicio.

16004 03/27/2008 16:32:54.550 SEV=4 AUTH/28 RPT=37680 89.23.222.223
User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G) Group (PFC) disconnected:
Session Type: IPSec/NAT-T
Duration: 0:04:08
Bytes xmt: 73072
Bytes rcv: 49224
Reason: User Requested

Duración de la sesión, tráfico que ha habido y motivo de la desconexión.

Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP (Simple Network Management Protocol) para monitorizar remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes).

FreeRADIUS [Free]: proyecto iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg (quien colaboró anteriormente en el desarrollo de Cistron RADIUS), es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que lo componen. Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios.

FreeRADIUS inició como un proyecto de servidor RADIUS que permitiera una mayor colaboración de la comunidad y que pudiera cubrir las necesidades que otros servidores RADIUS no podían. Actualmente incluye soporte para LDAP, SQL (Structured Query Language) y otras bases de datos, así como EAP y PAP. Actualmente incluye soporte para todos los protocolos comunes de autenticación y bases de datos.

Era el usado en el concentrador Cisco 3060.

2.1.2 Protocolo LDAP

LDAP (Lightweight Directory Access Protocolo) no se trata de un sistema de almacenamiento como muchas veces se piensa. Se trata de un protocolo de comunicación para acceder y modificar información almacenada en un servicio de directorio jerárquico distribuido, conocido normalmente como directorio LDAP.

Un servicio de directorio es una aplicación software o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos. El directorio es una clase especial de base de datos que contiene información estructurada en forma de árbol.

El objetivo de LDAP es acceder a depósitos de información referente a usuarios, contraseñas y otras entidades en un entorno de red, ofreciendo una amplia capacidad de filtrado sobre la información que está siendo solicitada.

¿Es el directorio LDAP una base de datos? Sí, lo es, pero no se trata de una base de datos relacional como pueda ser Oracle o MySQL. Como se ha dicho se trata de un directorio como pueda serlo el que guarda las fichas de los libros en una biblioteca. Al tratarse de un directorio está totalmente jerarquizado y está optimizado para muchas lecturas simultáneas y de pequeño volumen. Aunque se puede guardar lo que se quiera, está pensado para almacenar datos de poco tamaño (email, teléfono, dirección, permisos, habitualmente almacena la información de usuario y contraseña) y, a su vez, no está optimizado para que haya muchas modificaciones, pensemos que, por ejemplo la dirección de correo electrónico no es algo que se modifique con mucha frecuencia.

LDAP también es capaz de replicar su información a otros puntos en la red. Esto facilita la disipación de información a diversos puntos.

Directorios LDAP

Algunas de las implementaciones del servidor LDAP o directorio LDAP son las siguientes:

- Apache Directory Server : es un servidor basado en LDAP que centraliza configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas, así como información de control de acceso dentro de un sistema operativo independiente de la plataforma. Forma un repositorio central para la infraestructura de manejo de identidad. Apache Directory Server simplifica el manejo de

usuarios eliminando la redundancia de datos y automatizando su mantenimiento.

- Novell eDirectory: También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos que representa cada servidor, computadora, impresora, servicio, personas, etc. entre los cuales se crean permisos para el control de acceso por medio de herencia.
  La ventaja de esta implementación es que corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo
- Active Directory: es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración. Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAPv3 lo que permite integrar otros sistemas que soporten el protocolo.
  En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.
- OpenLDAP **[OLdap]**: Será el que utilicemos en el Juniper Networks SA 4000 SSL VPN. Se trata de una implementación libre del protocolo, que soporta múltiples esquemas, por lo que puede utilizarse para conectarse a cualquier otro LDAP.
  OpenLDAP tiene cuatro componentes principales:
  - Slapd: demonio LDAP autónomo.
  - Slurpd: demonio de replicación de actualizaciones LDAP autónomo.
  - Rutinas de biblioteca de soporte del protocolo LDAP.
  - Utilidades, herramientas y clientes.

2.2 Cifrado de la información

2.2.1 Aspectos generales

El concepto de seguridad en redes cubre distintos aspectos:

- La integridad: garantía de que los datos que conforman una cierta información no han sido modificados por un tercero. La medida de seguridad que se usará será la firma digital.
- Confidencialidad: la información nunca debe de poder ser accedida por terceros. La medida de seguridad utilizada será el cifrado o encriptación.
- Disponibilidad: se debe de poder tener acceso a la información siempre que se necesite.

- Autenticación: los dos extremos de una comunicación deben identificarse convenientemente entre sí. Se usarán los certificados digitales como medida de seguridad.
- No repudio: poder demostrar fehacientemente que una entidad o usuario participó en una transacción concreta. La medida de seguridad que se usará será la firma digital.

El cifrado moderno se divide actualmente en cifrado de **clave privada** y cifrado de **clave pública**:

- En el cifrado de **clave privada** o simétrico, las claves de cifrado y descifrado son la misma (o bien se deriva de forma directa una de la otra), debiendo mantenerse en secreto dicha clave. Como ejemplo tenemos: DES (Data Encryption Standar), DES triple, IDEA (International Data Encryption Algorithm) y AES (Advanced Encryption Estándar). El cifrado de clave privada es más rápido que el de clave pública por tanto se utiliza generalmente en el intercambio de información dentro de una sesión. Estas claves también son conocidas como claves de sesión o de cifrado simétricas ya que en ambos extremos se posee la misma clave.

- En el cifrado de **clave pública** las claves de cifrado y descifrado son independientes no derivándose una de la otra, por lo cual puede hacerse pública la clave de cifrado siempre que se mantenga en secreto la clave de descifrado. Como ejemplo tenemos el cifrado RSA (Rivest, Shamir, Adleman) y DSA (Digital Signature Algorithm). El cifrado de clave pública es más lento y por tanto se utiliza para intercambiar las claves de sesión. Como este algoritmo utiliza dos claves diferentes, una privada y otra pública, el cifrado se conoce como cifrado asimétrico.

2.2.2 Algoritmos de clave privada y pública

El criptoanálisis es la ciencia que se encarga de descifrar los mensajes mientras que la criptografía busca métodos más seguros de cifrado. Podemos clasificar la criptografía en dos grupos:

- La clásica: que usa cifrados rudimentarios basados en sustitución y trasposición.
- La moderna: que usa cifrados basados en algoritmos parametrizados en base a claves.

2.2.2.1 Algoritmos de clave privada: DES, DES triple, IDEA y AES

Cifrado DES (Data Encryption Standar).

Desarrollado por IBM (International Business Machines) a principios de la década de los 70 a partir de otro algoritmo conocido como Lucifer que utilizaba claves de 112 bits y que fueron reducidas a 56 bits (por orden de la Agencia de Seguridad Americana, NSA) en el algoritmo DES. Se diseñó de forma que no pudiera ser descifrado por criptoanálisis, pero sí que puede ser descifrado probando todas las claves posibles, asumiendo que se cuenta con el hardware adecuado. Una de las partes positivas de DES es que podemos descifrar los mensajes utilizando el mismo algoritmo que utilizamos para cifrar. La única diferencia consiste en el orden en que se aplican las subclaves dado que en el descifrado se utilizan en orden inverso.

Aunque en un principio el DES parecía inviolable, dos investigadores de criptografía de Standford diseñaron en 1977 una máquina para violar el DES y estimaron que podría construirse por unos 20 millones de dólares. Dado un trozo pequeño de texto normal y el texto cifrado correspondiente, esta máquina podría encontrar la clave mediante una búsqueda exhaustiva del espacio de claves de 2^{56} en menos de un día.

La conclusión que se puede obtener de estos argumentos es que el DES no es seguro.

Cifrado DES triple.

El cifrado realizado con el algoritmo DES es descifrable mediante diversos tipo de ataques de fuerza bruta, hecho que corroboró IBM en su artículo de 1994, indicando de forma explícita que la NSA decidió que así fuera con el fin de poder desencriptar los mensajes que deseara.

Parece, por tanto, que el cifrado con el algoritmo DES no es seguro. Sin embargo, el cifrado triple con el algoritmo DES es otro asunto. La clave utilizada por Triple DES es de 128 bits (112 de clave y 16 de paridad), es decir, dos claves de 64 bits (56 de clave y 8 de paridad) de los utilizados en DES. El motivo de utilizar este de tipo de clave es la compatibilidad con DES. Si la clave utilizada es el conjunto de dos claves DES iguales, el resultado será el mismo para DES y para Triple DES.

Cifrado IDEA (International Data Encryption Algorithm)

Después de comprobar la debilidad del algoritmo DES en su forma simple, diversos trabajos propusieron nuevos métodos de cifrados de bloques (Blowfish, Crab, Feal, Khafre, Loki91, Newdes, RedocII, Safer K64). Sin embargo el más interesante e importante de los cifrados posteriores al algoritmo DES es el algoritmo IDEA.

El algoritmo IDEA es un algoritmo de clave privada que fue diseñado por dos investigadores en Suiza. Usa una clave de 128 bits, lo que lo hará inmune durante décadas a los ataques de la fuerza bruta. No hay ninguna técnica o máquina conocida actualmente que se crea que puede descifrar el algoritmo IDEA.

Cifrado AES (Advanced Encryption Estándar) o Rijndael.

Es considerado el sucesor de DES. Este algoritmo se adoptó oficialmente en octubre del 2000 como nuevo estándar avanzado de

cifrado por el NIST (National Institute for Standards and Technology) para su empleo en aplicaciones criptográficas.

Sus autores son dos, los belgas Joan Daemen y Vincent Rijmen, de ahí su nombre Rijndael. Tiene como peculiaridad que todo el proceso de selección, revisión y estudio se efectuó de forma pública y abierta por lo que toda la comunidad criptográfica mundial ha participado en su análisis, lo cual convierte a Rijndael en un algoritmo perfectamente digno de la confianza de todos.

AES es un sistema de cifrado por bloques, diseñado para manejar longitudes de clave variables, comprendidas entre los 128 y los 256 bits.

2.2.2.2 Algoritmo de clave pública: RSA

Los métodos de cifrado de clave pública, también son conocidos como de clave asimétrica, porque son algoritmos que se basan en un par de claves: una pública que dispone todo el mundo y una clave asociada a dicha clave pública, que es privada y que guarda el usuario encarecidamente.

Históricamente el problema de distribución de claves siempre ha sido la parte débil de la mayoría de criptosistemas. Sin importar lo robusto que sea el criptosistema si un intruso puede robar la clave el sistema no vale nada.

En 1976, dos investigadores de la Universidad de Stanford (Diffie y Hellman) propusieron una clase nueva de criptosistema en el que las claves de cifrado y descifrado eran diferentes y la clave de descifrado no podía derivarse de la clave de cifrado. En su propuesta, el algoritmo de cifrado (con clave), E, y el algoritmo de descifrado (con clave), D, tenían que cumplir los tres requisitos siguientes:

1. D(E(P))=P.

2. Es excesivamente difícil deducir D de E.

3. E no puede descifrarse mediante un ataque de texto normal seleccionado.

El método funciona como sigue: una persona A que quiera recibir mensajes secretos primero diseña dos algoritmos E y D que cumplan los requisitos anteriores. El algoritmo de cifrado y la clave, E_A de cifrado, se hacen públicos, de ahí el nombre de criptografía de clave pública. Esto podría hacerse poniéndolos en un archivo accesible a cualquiera que quiera leerlo. A publica también el algoritmo de descifrado pero mantiene secreta la clave de descifrado D_A. Por tanto E_A es pública, pero D_A es secreta.

Viendo la figura 2.1 veamos si podemos resolver el problema de establecer un canal seguro entre A y B que nunca han tenido contacto previo.

Se supone que tanto la clave de cifrado de A, E_A, como la clave de cifrado de B, E_B, están en un archivo de lectura pública.

Ahora, A toma su primer mensaje P, calcula $E_B(P)$ y lo envía a B.

B entonces lo descifra aplicando su clave secreta D_B (es decir, calcula $D_B(E_B(P))=P$).

Nadie más puede leer el mensaje cifrado, $E_B(P)$, porque se supone que el sistema de cifrado es robusto y porque es demasiado difícil derivar D_B de la E_B públicamente conocida.

A y B ahora pueden comunicarse con seguridad.

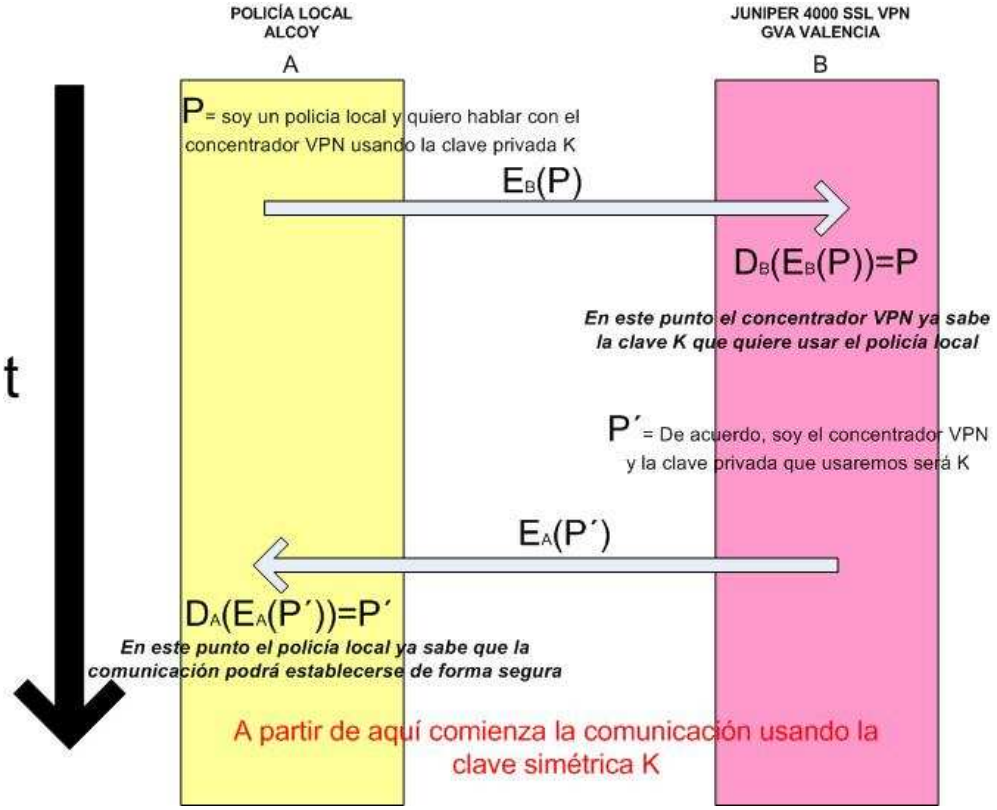


Figura 2.1: Establecimiento de un canal de comunicación seguro entre dos interlocutores.

La única dificultad del método anterior estriba en que necesitamos encontrar algoritmos que realmente satisfagan los tres requisitos. Debido a las ventajas potenciales de la criptografía de clave pública muchos investigadores están trabajando en este tema y ya se han publicado algunos algoritmos.

Cifrado RSA (Rivest, Shamir, Adleman).

Un buen método fue descubierto por un grupo del Instituto Tecnológico de Massachusetts (MIT) y es conocido como RSA. Su método se basa en:

- Buscar dos números primos lo suficientemente grandes: **p** y **q** con p≠q (de entre 100 y 300 dígitos).

- Se obtiene **n**=p×q y **z**=(p-1)×(q-1).

- Seleccionamos un número **d** sin ningún factor común con z (primo con respecto a z).

- Encontrar **e** tal que e×d= 1 mod z

Con estos parámetros calculados por adelantado estamos listos para comenzar el cifrado. Dividimos el texto normal (considerado como una cadena de bits) en bloques para que cada mensaje de texto normal, P, caiga en el intervalo 0<P<n. Esto puede hacerse agrupando el texto normal en bloques de k bits, donde k es el entero más grande para el que 2^k<n es verdad.

Para cifrar un mensaje, P, calculamos $C=P^e$(mod n). Para descifrar C, calculamos $P=C^d$(mod n). Puede demostrarse que, para todos los P del intervalo especificado, las funciones de cifrado y descifrado son inversas. Para ejecutar el cifrado se necesitan e y n. Para llevar a cabo el descifrado se requieren d y n. Por tanto, la clave pública consiste en el par (e,n) y la clave privada consiste en (d,n).

La seguridad del método se basa en la dificultad de factorizar números grandes. Si en algún momento los ordenadores son capaces entonces, simplemente se puede escoger un p y un q todavía más grandes.

2.2.3 Algoritmos de comprobación de integridad: MD5 y SHA-1

La comprobación de la integridad se refiere comprobación de la corrección y completitud de los datos que han sido enviados. Los algoritmos que se suelen utilizar para realizar la comprobación de la integridad de ficheros binarios son el MD5 y el SHA.

MD5 (Message-Digest Algorithm 5)

Diseñado por el profesor Ronald Rivest del MIT. Fue desarrollado en 1991 como reemplazo del algoritmo MD4. A pesar de su amplia difusión actual la sucesión de problemas de seguridad detectados, desde que en 1996 Hans Dobbertin anunciase una colisión de *hash,* plantean una serie de dudas acerca de su uso futuro.

SHA-1 (Secure Hash Algorithm)

Desarrollado como parte del Secure Hash Standard (SHS) y el Digital Signature Standard (DSS) por la NSA. Aparentemente se trata de

un algoritmo seguro y sin fisuras, al menos por ahora. La primera versión, conocida como SHA, fue mejorada como protección ante un tipo de ataque que nunca fue revelado. Los principios subyacentes al SHA-1 son similares a los del MD4 de Rivest. A falta de ataques ulteriores se le puede considerar seguro.

El funcionamiento de ambos (MD5 y SHA-1) de modo muy básico consiste en comparar una suma publicada con la suma de comprobación del archivo descargado. Así un usuario puede tener la confianza suficiente de que el archivo es igual que el publicado por los desarrolladores. Esto protege al usuario contra los virus que algún otro usuario malicioso pudiera incluir en el software. La comprobación de un archivo descargado contra su suma MD5/SHA-1 no detecta solamente los archivos alterados de una manera maliciosa, también reconoce una descarga corrupta o incompleta.

2.3 Tecnologías de cifrado de comunicaciones

La red de computadores Arpanet (Advanced Research Projects Agency NETwork), madre de la internet que conocemos ahora, no fue diseñada teniendo en cuenta la seguridad. Entre otras razones porque en aquellos tiempos las amenazas eran muy reducidas y aprovechar las vulnerabilidades existentes era mucho más complejo, condicionado porque el acceso a esta red sólo estaba al alcance de muy pocas universidades, centros de investigación, departamentos militares, etc.

Con el desarrollo de Internet y la presencia en estos últimos años de cualquier compañía o usuario final la panorámica ha cambiado radicalmente así como las necesidades, siendo ahora la seguridad en las comunicaciones una necesidad vital. También, el desarrollo de nuevas oportunidades de negocio y de transacciones mediante las comunicaciones está siendo un catalizador para que la seguridad se tenga en cuenta en la internet moderna. Ahora la mayoría de las comunicaciones donde hay información sensible o donde se quiere garantizar que el emisor o receptor es quien dice ser, debe de perseguir los objetivos de Confidencialidad, Integridad y Autenticidad

Con bastante frecuencia cuando se establecen túneles VPN, además de la integración de las direcciones de red, se plantea un requerimiento desde el punto de vista de la seguridad, dado que los datagramas viajan por una infraestructura pública en la que la información puede ser capturada y/o modificada por usuarios externos. Por este motivo la constitución de túneles VPN viene acompañada a menudo de un requerimiento de seguridad, constituyendo lo que podríamos denominar VPN seguras.

Figura 2.2: Capas del modelo OSI.

El problema de una comunicación segura a través de una red se resuelve normalmente a nivel de enlace, a nivel de red o a nivel de aplicación del modelo de la Organización Internacional para la Estandarización (OSI):

Nivel de enlace: La seguridad a nivel de enlace se implementa en los dispositivos que se conectan al medio de transmisión, por ejemplo dos *routers* que se comunican mediante una línea punto a punto. En este caso los mecanismos de seguridad se pueden aplicar de forma transparente al protocolo utilizado a nivel de red. Sin embargo en una red grande requiere encriptar y desencriptar la información en cada salto que da el paquete; aun en el caso de utilizar dispositivos que realicen esta tarea por *hardware* el retardo que esto puede introducir cuando el número de saltos es elevado puede hacer inviable el uso de aplicaciones en tiempo real que requieren cierto nivel de Calidad de Servicio[2]. Además implementar seguridad a nivel de enlace requiere controlar la infraestructura de la red, cosa que no es factible cuando se utilizan los servicios de un operador o ISP.

Nivel de red: Esta es la aproximación adoptada por los estándares IPSec. En este caso la seguridad se limita al protocolo IP y otros protocolos sólo podrán aprovecharla si se encapsulan previamente en paquetes IP. La seguridad a nivel de red puede aplicarla el usuario de forma transparente al proveedor del servicio y encaja de forma muy adecuada con el concepto de VPNs pudiendo crear lo que denominamos VPN seguras.

Nivel de aplicación: esta es la aproximación que adopta SSL. El principal inconveniente de abordar la seguridad a nivel de aplicación estriba precisamente en la necesidad de incorporar funcionalidades

[2] Calidad de Servicio: son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado.

similares en cada uno de los protocolos del nivel de aplicación que deban utilizarlas, replicando así gran cantidad de tareas en diferentes partes de código.

La ventaja es que la seguridad se puede desarrollar de forma selectiva, aplicándola únicamente en el intercambio de información confidencial o importante. Además, al aplicarse los mecanismos de encriptado o validación de la información en el nivel más alto posible el nivel de seguridad obtenido es máximo ya que se reduce el riesgo de que la información pueda ser interceptada o modificada por otros usuarios o procesos distintos del destinatario de ésta.

La cuestión que nos ocupará será decidir si se usa un concentrador VPN que trabaje con la tecnología IPSec o uno que trabaje con la tecnología SSL. Existe también la tecnología PPTP (Point to Point Tunneling Protocol) pero no la estudiaremos porque al ser al ser propietaria de Microsoft no nos sirve para los objetivos buscados en este proyecto además de que, junto con la tecnología L2TP (Layer 2 Tunneling Protocol) ninguna de las dos son protocolos de seguridad IP tan buenos como IPSec o SSL.

Pasaremos a hacer un análisis de las dos tecnologías para cuando redactemos lo requisitos del sistema poder elegir entre una u otra.

2.3.1 Tecnología IPSec

IPSec (Internet Protocol Security), es la seguridad para IP. El protocolo IP, en sus orígenes, no fue diseñado teniendo en cuenta la seguridad. Es por ello que es muy fácil realizar ataques a nivel IP como el *spoofing* (ataques falseando la dirección origen), ataques para capturar el tráfico y vulnerar la confidencialidad, ataques de *hijacking* (robo de sesión), o ataques de repetición dando como resultado una denegación de servicio[3].

El protocolo IP en su versión 4 no integra IPSec de manera nativa pero es posible añadir esta capa. IP en su versión 6 sí incorpora IPSec por lo que no es necesario añadir ningún soporte al núcleo del sistema operativo que quiera hacer uso de IPSec.

IPSec fue el primer gran esfuerzo para desarrollar un estándar de seguridad para redes.

Básicamente IPSec permite garantizar la confidencialidad de las comunicaciones, la integridad de los mensajes enviados y la autenticidad del emisor y receptor de los mensajes.

Los protocolos de IPSec actúan en la capa de red (Fig.2.2).

Otros protocolos de seguridad para Internet de uso extendido, Transport Layer Security (TLS) y Secure Shell (SSH) operan de la capa

[3] Denegación de servicio: ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

de transporte. Esto hace que IPSec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo Protocolo de Control de Transmisión (TCP) y UDP, los protocolos de capa de transporte más usados.

IPSec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPSec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código

Las **funcionalidades** de IPSec son:

- Autentication Header (AH): garantiza que el datagrama fue enviado por el remitente y que no ha sido alterado durante su viaje.
- Encapsulating Security Payload (ESP): garantiza que el contenido no pueda ser examinado por terceros (o que si lo es, no pueda ser interpretado). Opcionalmente puede incluir la función de AH de autentificación.

Tanto AH como ESP definen una cabecera IPSec incluida en el paquete a enviar.

- Internet Security Association and Key Management Protocol (ISAKMP): es un entorno que permite un mecanismo seguro (manual y automático) de intercambio de formatos de paquete y claves utilizadas en las tareas de encriptado y autentificación de AH y ESP. Incluye a IKE (Internet Key Exchange). Utiliza Diffie-Hellman.
- Security Association (SA): conjunto de políticas y claves para establecer y proteger una conexión.

Los modos de **funcionamiento** son:

- Modo transporte: comunicación segura extremo a extremo. Requiere implementación de IPSec en ambas *hosts*. No se cifra la cabecera IP.
- Modo túnel: comunicación segura entre *routers* únicamente que ejecutan pasarelas de seguridad. Permite incorporar IPSec sin tener que modificar los *hosts*. A los paquetes se añade otra cabecera. Se integra cómodamente con VPNs.

El proceso de comunicación de dos equipos (A y B) sería el siguiente:

1. La unidad de IPSec en el equipo A comprueba la lista de filtro IP en la directiva activa para buscar la correspondencia con la dirección o el tipo de tráfico de los paquetes de salida.
2. La unidad de IPSec notifica a ISAKMP para iniciar las negociaciones de seguridad con el equipo B.
3. El servicio ISAKMP en el equipo B recibe una solicitud de negociaciones de seguridad.
4. Los dos equipos realizan un intercambio de clave, establecen un ISAKMP y una clave secreta compartida.

5. Los dos equipos negocian el nivel de seguridad para la transmisión de información, establecen un par de IPSec SA y las claves para asegurar los paquetes IP.
6. Al utilizar la IPSec SA y clave de salida, la unidad de IPSec en el equipo A firma los paquetes por integridad y cifra los paquetes si se ha negociado la confidencialidad.
7. La unidad IPSec en el equipo A transfiere los paquetes al tipo de conexión apropiado para la transmisión al equipo B.
8. El equipo B recibe los paquetes asegurados y los transfiere a la unidad de IPSec.
9. Al utilizar la SA y la clave de salida, la unidad de IPSec en el equipo B comprueba la firma de integridad y descifra los paquetes.
10. La unidad de IPSec en el equipo B transfiere los paquetes descifrados a la unidad TCP/IP que los transfiere a la aplicación de recepción.

2.3.2 Tecnología SSL

SSL (Secure Sockets Layer) fue desarrollado por la compañía Netscape Comunications Corporation, la creadora del navegador Netscape Navigator.

Si IPSec intenta alcanzar seguridad en la propia red, SSL lo hace al nivel de la aplicación.

Los protocolos de Internet, como el protocolo HyperText Transfer Protocol (HTTP) que permite ver webs, el protocolo para la transmisión de ficheros File Transfer Protocol (FTP), o el protocolo de acceso remoto a los sistemas TELecommunication NETwork (Telnet), son protocolos que no garantizan Confidencialidad, Integridad ni Autenticidad. Es por esta razón por la que se ha desarrollado una capa intermedia, SSL, que permite añadir seguridad a los protocolos que por su naturaleza no son seguros. Por ejemplo, el protocolo HTTPS es básicamente el protocolo HTTP pero con la capa SSL que añade la seguridad. Eso es aplicable para cualquier protocolo, Post Office Protocol (POP3), Internet Message Access Protocol (IMAP),….. Otro ejemplo de protocolo que usa SSL es el protocolo SSH para el acceso remoto a los sistemas y para poder crear túneles entre máquinas y aplicaciones.

La capa SSL se ubica en el modelo OSI en la capa de sesión.

SSL corre en el espacio del usuario simplificando enormemente la implementación y la administración. Ya no hay la necesidad de instalar ningún *software* cliente como ocurría en el concentrador Cisco.

Cuando el cliente pide al servidor seguro una comunicación segura el servidor abre un puerto cifrado gestionado por un software llamado Protocolo SSL Record situado encima de TCP. Será el software de alto nivel, Protocolo SSL Handshake, quien utilice el Protocolo SSL Record y el puerto abierto para comunicarse de forma segura con el cliente.

El **Protocolo SSL Handshake**

Durante el protocolo SSL Handshake el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes seis fases (de manera muy resumida):

1. La fase Hola, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación.
2. La fase de intercambio de claves, en la que intercambia información sobre las claves de modo que, al final, ambas partes comparten una clave maestra.
3. La fase de producción de clave de sesión, que será la usada para cifrar los datos intercambiados.
4. La fase de verificación del servidor, presente sólo cuando se usa RSA como algoritmo de intercambio de claves y que sirve para que el cliente autentique al servidor.
5. La fase de autenticación del cliente, en la que el servidor solicita al cliente un certificado (si es necesaria la autenticación de cliente).
6. Por último la fase de fin, que indica que ya se puede comenzar la sesión segura.

El **Protocolo SSL Record**

El Protocolo SSL Record especifica la forma de encapsular los datos transmitidos y recibidos. La porción de datos del protocolo tiene tres componentes:

- MAC-DATA: el código de autenticación del mensaje.
- ACTUAL-DATA: los datos de aplicación a transmitir.
- PADDING-DATA: los datos requeridos para rellenar el mensaje cuando se usa cifrado en bloque.

Teniendo en cuenta los tres pilares de la seguridad en los sistemas de información (Confidencialidad, Integridad y Autenticidad), SSL garantizaría la Confidencialidad e Integridad, es decir, evitaría que terceras personas tuvieran acceso a la información que viaja por la red entre dos puntos y que los mensajes que son intercambiados no sean alterados. A su vez añadiría una tercera variable, la Autenticación, es decir, que el cliente garantiza que el servidor es quien dice ser. Para todas estas garantías es necesario que el servidor disponga de un certificado.

Opcionalmente es posible que el servidor autentique al cliente de tal manera que el servidor garantice que el cliente es quien dice ser por lo que entra en juego un segundo certificado: el certificado de cliente.

2.4 Infraestructura de clave pública

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío y otros usos.

Para entender el sistema PKI hemos de familiarizarnos con una serie de conceptos relacionados con ella:

La **autoridad de certificación (AC)**: es una entidad de confianza que es reconocida y aceptada por todos e imposible de suplantar. Por regla general, por seguridad no se trabaja directamente con la AC, si no con un intermediario o Autoridad de Registro (AR). La AC de la GVA es la ACCV.

El **certificado digital**: es una archivo firmado con la clave privada de una AC que contiene: la identidad, la clave pública de dicha AC, atributos varios y un compendio de dicha información. En definitiva, es un vínculo entre una clave pública y una identidad de usuario, que se consigue mediante una firma digital por una tercera parte o AC que hace pública su clave pública en la que todos confían.

Existen diferentes tipos de certificado digital **[BOE 2]**, en función de la información que contiene cada uno y a nombre de quién se emite el certificado:

- Certificado personal, emitidos exclusivamente a personas físicas.
- Certificado de pertenencia a empresa, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- Certificado de representante, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- Certificado de persona jurídica, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- Certificado de atributo, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal. (p.ej. Médico, Director, Casado, Apoderado de..., etc.).

Además existen otros tipos de certificado digital utilizados en entornos más técnicos:

- Certificado de servidor seguro, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.

- Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

El **certificado raíz**: es un certificado emitido de la AC para sí misma con su clave pública para comprobar certificados emitidos por ella. Se suele instalar previamente dicho certificado en el navegador para poder utilizar los certificados de dicha AC. Los navegadores llevan por defecto muchos de ellos.

La **autoridad de registro**: que identifica de forma inequívoca al solicitante de un certificado y suministra a la AC los datos verificados para que pueda emitirlo.

Los **repositorios**: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de certificados revocados.

Lista de certificados revocados (CRL): es una lista donde se recogen todos los certificados de la AC dados de baja por caducidad aún estando temporalmente vigentes por problemas varios (como que se haya hecho pública la clave privada de un usuario) y ,por tanto, cualquier firma emitida con posterioridad a la revocación no tiene validez. Este documento también es firmado por la propia AC. La alternativa a esta lista es OCSP (Online Certificate Status Protocol) que lo que hace es ejecutar una consulta online de los certificados que han sido revocados.

Figura 2.3: Infraestructura de clave pública

Podríamos resumir este apartado de este modo: ¿cómo podemos estar seguros de que la clave pública de un usuario, que hemos encontrado por ejemplo en un directorio o una página web corresponde realmente a ese individuo y no ha sido falsificada por otro? ¿Cómo fiarnos de esa clave pública antes de confiarle algún secreto nuestro?

Viendo la figura 2.3, la solución consiste en recurrir a una tercera parte confiable, erigida en la figura de una AC. La función básica de una AC reside en verificar la identidad de los solicitantes de certificados, crear los certificados y publicar las CRLs cuando éstos son inutilizados. El certificado contiene de forma estructurada información acerca de la identidad de su titular, su clave pública y la AC que lo emitió. Actualmente, el estándar al uso es el X.509.v3 **[Uit]**.

2.4.1 La firma digital

A nivel autonómico la regulación de la firma electrónica se describe en el Decreto 87/2002 **[DOCV 1]**, en este decreto se definen las directrices de uso de la firma digital en la GVA.

En España existe la Ley 59/2003 **[BOE 2]**, esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación, define cuatro tipos de firma:

- Simple: incluye un método de identificar al firmante
- Avanzada: además de identificar al firmante permite garantizar la integridad del documento. Se emplean técnicas de infraestructura de clave pública.
- Reconocida: es la firma avanzada ejecutada con un DSCF (Dispositivo Seguro de Creación de Firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante).
- Avanzada Certificada: firma igual que la avanzada en la que el certificante queda también acreditado.

En resumen, con la firma digital podemos asegurar la autenticación, la integridad y el no repudio. La clave estriba en pedir obligatoriamente un acuse de recibo.

Los requisitos que debe de cumplir son: debe ser fácil de generar, irrevocable, única, fácil de autenticar y depender tanto del mensaje como del autor.

La firma digital de un documento es el resultado de aplicar una función *hash* a su contenido y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica. El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos

mencionar: la vigencia del certificado digital del firmante, la revocación del certificado digital del firmante y la inclusión de sello de tiempo.

Cuando la entrada es un documento el resultado de la función es un número que identifica casi inequívocamente al texto. Si se adjunta este número al texto el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido.

Como en el caso de la criptografía podríamos usar una clave secreta o una pública. Para el caso de la clave secreta un enfoque sería tener una autoridad central X que sepa todo y en quien todos confíen. De este modo cada usuario escogería una clave secreta y la llevaría personalmente a la autoridad central X.

Por tanto sólo el usuario y X conocen la clave secreta del usuario. Además X lee todos los mensajes firmados. Por ello los candidatos más lógicos para operar el servidor X son el gobierno, los bancos, etc. Pero estas organizaciones no tiene porqué inspirar confianza completa a todos los ciudadanos.

2.4.2 El DNI electrónico (DNIe)

El DNIe **[DNIe]** ha adoptado la PKI.

El marco legal del DNIe lo encontramos a nivel europeo en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo **[EU 1]** y a nivel nacional en el Real Decreto 1553/2005 **[BOE 3]**, por el que se regula documento nacional de identidad y sus certificados de firma electrónica.

La Comisión Europea encargada del seguimiento de esta Directiva en su última reunión en Lisboa tomó una serie de acuerdos, los dos más importantes fueron:

- en 2010, la identidad-e y la contratación-e tendrán que ser completamente interoperables
- en 2009 todos los ciudadanos deberán poder hacer cualquier registro de manera electrónica y desde cualquier punto

Esto obliga a todas las Administraciones Públicas (AAPP) a facilitar a los ciudadanos cualquier tipo de servicio electrónico de una forma rápida y eficaz.

En la medida que el DNIe vaya sustituyendo al DNI tradicional y se implanten las nuevas aplicaciones, podremos utilizarlo para:

- Realizar compras firmadas a través de Internet.
- Hacer trámites completos con las AAPP a cualquier hora y sin tener que desplazarse ni hacer colas.
- Realizar transacciones seguras con entidades bancarias.
- Acceder al edificio donde trabajamos.
- Utilizar de forma segura nuestro ordenador personal.

- Participar en una conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser.

Figura 2.4: El DNIe [DNIe].

El DNIe es una oportunidad para acelerar la implantación de la Sociedad de la Información en España y situarnos entre los países más avanzados del mundo en la utilización de las tecnologías de la información y de las comunicaciones, lo que, sin duda, redundará en beneficio de todos los ciudadanos.

2.5 Autoridades de certificación: la ACCV

La AC, por sí misma o mediante la intervención de una AR, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la AC utilizando su clave privada. La AC es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública. La confianza de los usuarios en la AC es importante para el funcionamiento del servicio y justifica la filosofía de su empleo, pero no existe un procedimiento normalizado para demostrar que una AC merece dicha confianza.

ACCV.

La Autoridad de Certificación de la Comunidad Valenciana es el Ente Prestador de Servicios de Certificación Electrónica de la Comunidad Valenciana, constituido mediante la Ley 14/2005, de 23 de diciembre, de la GVA **[DOCV 2]**.

La ACCV **[ACCV]** proporciona a los ciudadanos, las empresas y las AAPP los mecanismos de identificación telemática segura en los trámites administrativos a través de Internet: los certificados digitales y las tecnologías asociadas.

Los certificados emitidos y el resto de servicios que la ACCV presta se ajustan a lo establecido en la Ley 59/2003 de firma electrónica **[BOE 2]**, por lo que la ACCV goza de amplio reconocimiento en todas las AAPP. Además, con los certificados digitales reconocidos expedidos por la ACCV se puede generar firma electrónica reconocida.

Los ciudadanos que deseen solicitar un certificado digital en soporte *software* deben dirigirse a cualquiera de los Puntos de Registro de Usuario de la ACCV (PRU) que existen en la Comunidad Valenciana. La emisión del certificado digital es presencial y dura entre 5 y 10 minutos desde el momento de la solicitud.

Los tipos de certificados que emite la ACCV son:

- Los certificados reconocidos en soporte software para ciudadanos (para personas físicas) se proporcionan en soporte disquete**,** se pueden utilizar para:
  - Firmar y cifrar mensajes de correo electrónico seguro.
  - La identificación de usuarios ante servicios telemáticos: Oficina Virtual de la Agencia Tributaria, Oficina Virtual de la Seguridad Social, Oficina Virtual del Catastro y en el caso que nos ocupa validar a los usuarios del servicio VPN, etc.
    También la firma electrónica y el cifrado de documentos en estas aplicaciones.

- Los certificados reconocidos de entidad (personas jurídicas) se proporcionan en tarjeta criptográfica (Figura 2.5), se pueden utilizar para:
  - Firmar y cifrar mensajes de correo electrónico seguro.
  - La identificación de entidades ante servicios telemáticos: Oficina Virtual de la Agencia Tributaria, Oficina Virtual de la Seguridad Social, Oficina Virtual del Catastro, etc. También la firma electrónica y el cifrado de documentos en estas aplicaciones.
    Hay que destacar el acceso al servicio VPN de la GVA por parte de una persona jurídica no está permitido.

Figura 2.5: Tarjeta criptográfica ACCV [ACCV].

- Los certificados no personales para otros usos, que se pueden utilizar para:

- Certificados para servidor con soporte SSL: son certificados que permiten identificar en internet y de forma fiable a los servidores web que establecen comunicaciones seguras mediante el protocolo SSL. Se pueden identificar porque se accede a ellos a través de direcciones del tipo https://. Su emisión y uso está sujeta a la Política de Certificación de Certificados para servidores con soporte SSL **[POL 1]**.
- Certificados para servidores de VPN: son certificados que permiten identificar en internet y de forma fiable a los servidores que establecen conexiones seguras vía VPN. Su emisión y uso está sujeta a la Política de Certificación de Certificados para servidores de VPN **[POL 2]**.
- Certificados de aplicación: son certificados que nos permiten recibir información firmada desde una aplicación y comprobar su integridad. Su emisión y uso está sujeta a la Política de Certificación de Certificados de aplicación **[POL 3]**.
- Certificados para firma de código: nos aseguran que el código que ejecutamos ha sido firmado por quien lo ha desarrollado y no es malicioso. Su emisión y uso está sujeta a la Política de Certificación de Certificados para firma de código **[POL 4]**.

- Los certificados de inicio de sesión en Windows.

2.6 Soluciones VPN *software* y *hardware*

Para acceder de modo remoto por VPN a una red son dos las opciones de las que disponemos:

- Podemos hacerlo utilizando un *software* que corra en un ordenador de propósito general, que, como una más de sus aplicaciones tenga una que haga de concentrador VPN; como ejemplos tendríamos OpenVpn **[OVpn]** o incluso el propio WindowsXP que posee este *software* implementado.

- Podemos comprar máquinas en las que la arquitectura del hardware está específicamente diseñada e implementada para la optimización de estas aplicaciones que además son las únicas que corren en esos equipos e incluso cuentan con ASIC (Circuito Integrado para Aplicaciones Específicas) que son circuitos integrados hechos a la medida para un uso en particular, lo que hace que se optimicen los recursos y tiempos de respuesta. Estas máquinas reciben el nombre de

appliances; Cisco, NetGear, Juniper, Aventail son varias de las marcas comerciales que las ofrecen.

El volumen de conexiones VPN de la GVA con más de más de 1.300 usuarios dados de alta en el servicio, del orden de 100 nuevas altas mensuales, entre 300 y 400 accesos diarios y unos 90 usuarios concurrentes, hacen obligatorio el uso de *appliances* para poder dar este servicio.

2.6.1 Implementación *software* de VPN: WindowsXP, OpenVpn

Existen un gran número de aplicaciones que pueden dar este servicio: iPIG, OpenVPN, WallCooler, KVpnc. Se hará una descripción somera de WindowsXP y OpenVpn, debido a que son las dos más utilizadas, una como *software* de pago y la otra como *software* de libre distribución.

WindowsXP: incluye la funcionalidad VPN que le permite ser configurado como servidor de conexiones entrantes **[WXP]**, pudiendo atender conexiones entrantes desde una conexión como es internet o bien desde una llamada telefónica a un módem analógico.

Como cliente de conexión en el equipo que se conecta a un Windows XP configurado para recibir conexiones entrantes, puede actuar una versión de Windows 95 o superior. Por supuesto que no es compatible con otros sistemas operativos.

En cualquier caso, al tratarse de un mini-servidor, está limitado a una sola conexión entrante, sólo es capaz de usar el protocolo PPTP para la conexión entrante, tampoco incluye funcionalidad de servicio Domain Name System (DNS), ni el Windows Internet Naming Service (WINS), con lo que su capacidad de servidor VPN para dar servicio a una red privada es totalmente reducida, estando orientado su uso a dar servicio a los recursos compartidos del propio equipo con Windows XP.

En definitiva, esta funcionalidad que ofrece Windows no es una solución profesional para conectar a una red a varios usuarios. Simplemente nos permite conectarnos a nuestro ordenador remotamente de forma segura.

OpenVpn: la gran ventaja de esta aplicación es que es de libre distribución. Se apoya sobre la tecnología SSL. La tecnología SSL, como se ha visto con anterioridad, corre en el espacio del usuario simplificando su implementación y administración. Es muy portable y no necesita modificaciones del núcleo del sistema operativo, además encaja muy bien con la asignación dinámica de direcciones.

Los sistemas operativos sobre los que puede funcionar son, entre muchos otros: Linux, Windows 2000/XP y siguientes, OpenBSD, FreeBSD, NetBSD, Mac OS X, Solaris, etc. Puede soportar miles de

usuarios. En definitiva, al ser multiplataforma es netamente superior a implementar un servidor VPN sobre Windows.

2.6.2 Soluciones hardware, concentradores VPN de Cisco, Aventail y Juniper.

Las marcas que ofrecen el servicio de *appliances* para VPN son varias. Se hará una descripción sucinta de las características de cada una de estas tres ya que en capítulos posteriores veremos a fondo la tecnología e información utilizada por los equipos. Su elección ha sido debida a que: Cisco es la que se utilizaba hasta ahora para dar el servicio y Aventail y Juniper son las dos opciones, en base al informe Gartner **[Apéndice A]**, barajadas para la implantación del nuevo servicio VPN.

Cisco: el modelo que concretamente se estaba utilizando en la GVA era el 3060, soporta hasta 5.000 conexiones IPSec concurrentes con un ancho de banda de hasta 100 Mbps. En cuanto al número de interfaces, este modelo tiene tres 10/100BASE-T Ethernet **[Data 1]**. Este modelo también tenía la posibilidad de usar la tecnología SSL pero para nada estaba optimizado. El número de clientes simultáneos era de 500 y además se ralentizaba la máquina y daba problemas con el uso de certificados.

Figura 2.6: Cisco VPN Concentrator 3060.

Aventail: el modelo que se evaluó para una posible adquisición fue el Sonicwall Aventail EX 2500. El número de usuarios varía para este modelo dependiendo de la licencia que se adquiera, pudiendo optarse entre 5, 50, 100, 250, 500, 1000 ó 2000 con un ancho de banda de hasta 1000Mbps. Tiene seis interfaces 10/100/1000BASE-T Ethernet **[Data 2]**.

Figura 2.7: Sonicwall Aventail EX 2500.

Juniper: el modelo que finalmente se ha adquirido es el Juniper Networks SA 4000 SSL VPN. El número de usuarios concurrentes, al igual que en el Aventail, puede variar según la licencia que adquiramos.

En este caso podríamos elegir entre 50, 100, 250, 500 ó 1000 con un ancho de banda de hasta 1000Mbps. Tiene dos interfaces 10/100/1000BASE-T Ethernet **[Data 3]**.

Figura 2.8: Juniper Networks SA 4000 SSL VPN.

2.7 Resumen

A lo largo del presente capítulo se ha visto una introducción teórica de los conceptos que serán usados en capítulos posteriores y ejemplos de ellos.

Se han repasado los distintos tipos de autenticación existentes (RADIUS y LDAP). Hemos hablado del cifrado de la información con el cifrado simétrico y el asimétrico; también hemos visto cómo esa información debe de ser verificada.

Posteriormente hemos conocido las dos grandes alternativas tecnológicas para el cifrado de las comunicaciones (IPSEC y SSL).

Hemos conocido lo que son las PKIs viendo ejemplos, tanto de las partes que las componen (AC, CR, CRL, etc.), como de ellas mismas (ACCV).

Finalmente también hemos conocido cuáles son los posibles sustitutos del equipo físico que debemos de migrar.

Capítulo 3.
Análisis del sistema y elaboración de requisitos

En este capítulo se verá cómo es la Red Corporativa (RC) de la Generalitat Valenciana (GVA) y cuál es el recorrido de una conexión VPN (Virtual Private Network) en la RC. Enunciaremos cuáles son los requisitos de nuestro sistema en base a unas decisiones tecnológicas. Veremos el sistema que quedó obsoleto en qué tipo de tecnología se apoyaba y se planteará el nuevo sistema implantado, viendo las diferencias con el anterior y las ventajas obtenidas. Será en el siguiente capítulo donde se verá la configuración del nuevo sistema al completo.

3.1 Red distribuida de la GVA

La RC de la GVA tiene un parque muy elevado de equipos, ya no solo simples ordenadores personales para sus trabajadores, sino que junto con éstos, podemos encontrar equipos de red (por motivos de seguridad y debido a la criticidad de los servicios la mayor parte de ellos redundados) como son: cortafuegos, balanceadores de carga, gestores de tráfico, servidores de dominio, servidores web, enrutadores, etc. En definitiva se trata de una vasta red.

A continuación se hará una descripción de la parte de la RC que está involucrada en el servicio VPN. Se hará una descripción por partes para finalmente poder tener y comprender una visión total. Por razones de seguridad se han omitido datos de componentes *hardware* y los direccionamientos IP son ficticios.

En la figura 3.1 se puede ver como la GVA dispone de dos Proveedores de Servicios de Internet (ISP) a fin de poder garantizar la conectividad de sus servicios ante un eventual caída de uno de ellos.

En sentido de salida la RC está balanceada, es decir, cuando un usuario sale a internet no siempre lo hace a través del mismo ISP, puede optar por uno u otro dependiendo de estos balanceadores. Consecuentemente los servicios que se publican para el exterior desde la GVA tienen un doble resolución DNS (Domain Name System) ya que cada ISP posee su propio direccionamiento IP.

En sentido de entrada a la RC, todas las conexiones pasan obligatoriamente por el cortafuego A donde son filtradas.

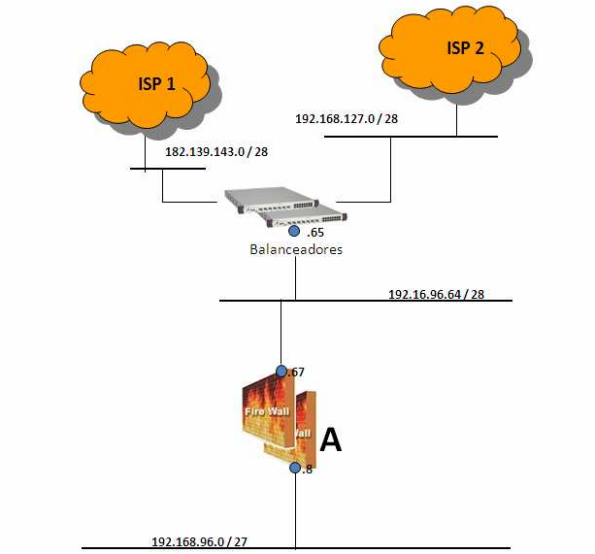


Figura 3.1. ISPs de la RC de la GVA.

Antes de pasar a la explicación de la parte de la RC de la figura 3.2 se aclararán unos de conceptos.

Una DMZ (DeMilitarizaded Zone) es una red local que se ubica entre la red interna de una organización y una red externa, generalmente internet, como podemos ver en la figura 3.2. Las DMZs de la RC de la GVA se encuentran entre internet, que estaría en la parte de arriba de la figura y la red interna que estaría en la parte de abajo.

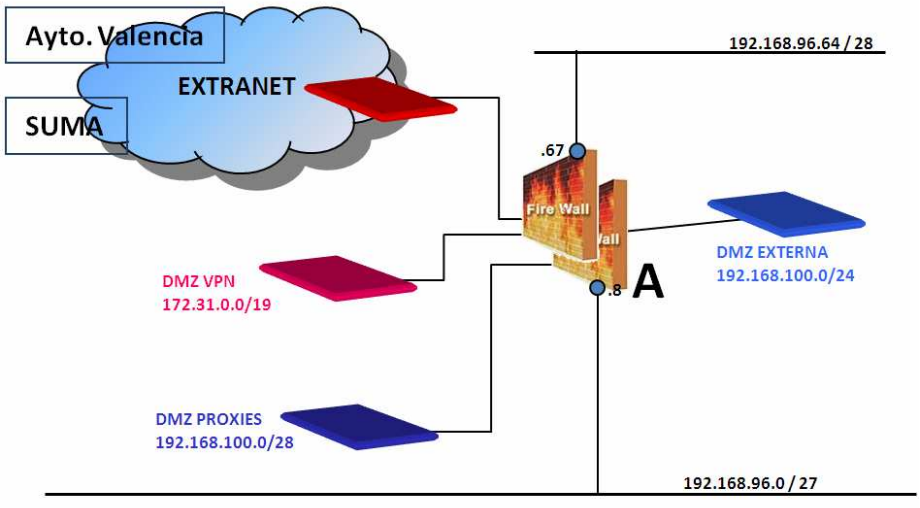


Figura 3.2: DMZs y Extranet de la RC de la GVA.

Se han definido diferentes DMZs que ofrecen distintos servicios para dar un alto grado de modularidad a la RC que la haga más fácilmente

manejable, ampliable, etc. El cortafuego A controlará el acceso a cada una de ellas.

Los *Proxies* son unos servidores cuya función es tener en su memoria las páginas accedidas por parte de los usuarios del sistema con lo que el tiempo de consulta de algunas de ellas mejora sustancialmente. El usuario no tiene que salir a internet a consultarlas ya que se encuentran almacenadas y actualizadas en estos servidores.

La *DMZ Proxies* es la subred donde está el conjunto de servidores Proxies. A esta acceden los trabajadores de la GVA.

La *DMZ Externa* es la que aloja todos los servicios que se hacen públicos a internet como son por ejemplo http://www.gva.es o http://www.san.gva.es. A esta DMZ entran tanto los trabajadores de la GVA como el público en general desde internet.

La *DMZ VPN* es la subred donde están los concentradores VPN.

Colgando del cortafuego A también tenemos lo que se ha llamado extranet. Esta extranet está formada por líneas punto a punto (ONO, Telefónica, etc.) que unen a varias instituciones con la GVA, por ejemplo el Ayuntamiento de Valencia o el SUMA, del cual se hablará a continuación.

La extranet ha surgido como producto de la necesidad de conexiones múltiples constantes con la GVA por parte de estas instituciones. Ello no es óbice para que estas instituciones puedan, caso de ser necesario, usar como método alternativo de conexión el servicio VPN.

El acceso interadministrativo es vital para que los servicios públicos puedan ofrecer una atención adecuada a los ciudadanos. Las infraestructuras comunes en las Administraciones Públicas (AAPP) son fundamentales. La primera de las infraestructuras comunes ha sido la que se ha denominado red SARA que son las siglas de Sistema de Aplicaciones y Redes para las Administraciones.

En la figura 3.3 podemos ver como del cortafuego B cuelgan la DMZ Interna y la red SARA.

SARA es una red privada que une a todos los departamentos y Ministerios de la Administración General del Estado y Comunidades Autónomas de forma segura a la que sólo tiene acceso, de manera controlada, los organismos públicos. El objetivo final de esta red es que se convierta en la columna vertebral de todas las comunicaciones entre administraciones en España.

Entre otros departamentos de la Administración General del Estado la GVA facilita la conexión a la DGT (Dirección General de Tráfico) por parte de las Policías Locales de los distintos ayuntamientos y también la conexión con la Agencia Tributaria por parte de, por ejemplo, el SUMA **[Suma]** que es un organismo autónomo creado por la Diputación Provincial de Alicante cuya misión es gestionar y recaudar los tributos municipales de los Ayuntamientos de la provincia de Alicante.

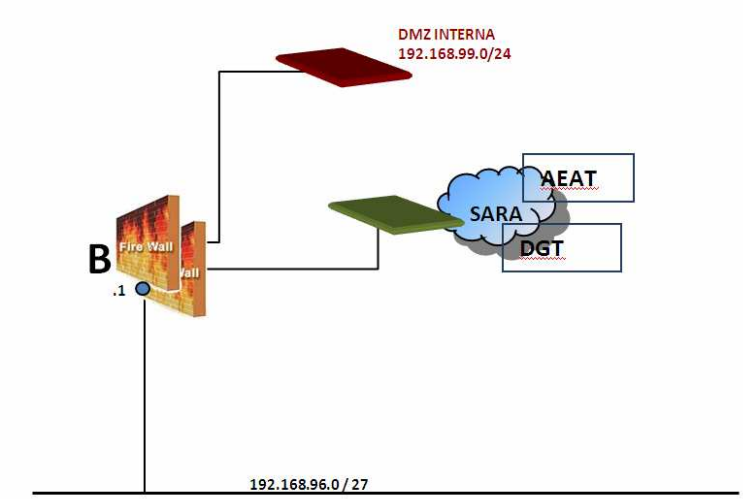


Figura 3.3 DMZ interna y acceso SARA por la RC.

Tanto Policías Locales como el SUMA han de comunicarse vía GVA con la Administración General del Estado. Los primeros lo harán usando el servicio VPN; el segundo lo hará mediante las líneas punto a punto directamente como si formara parte de la RC de la GVA.

También cuelga de este cortafuego B la *DMZ Interna*, que está formada por el conjunto de servidores que albergan los servicios internos a los que tienen acceso únicamente los trabajadores de la GVA, como por ejemplo http://portaldelfuncionari.gva.es. Estos servicios no tienen acceso desde la internet.

Finalmente y para terminar esta explicación por partes de la RC vemos en la figura 3.4 la nube que representa la propia red IP que componen todos los trabajadores de la GVA.

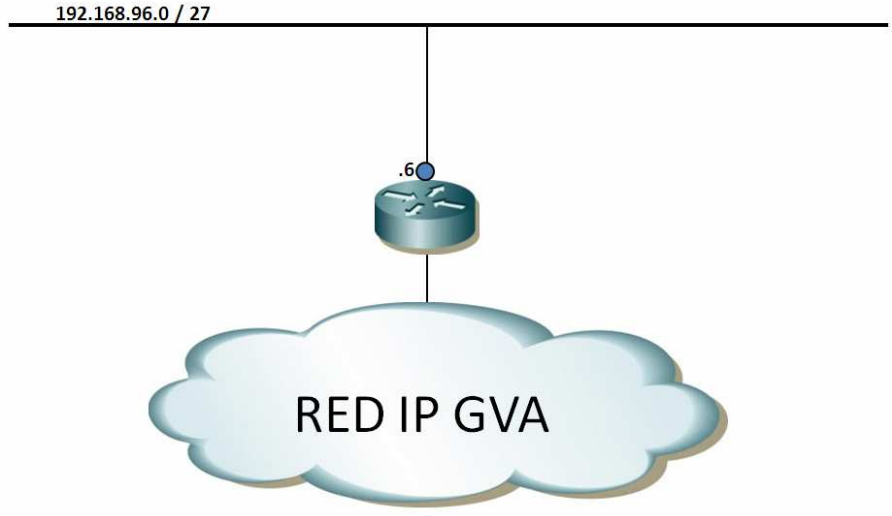


Figura 3.4: Red IP de la RC.

Una vez explicada la RC de la GVA por partes, veamos en la figura3.5 una visión general.

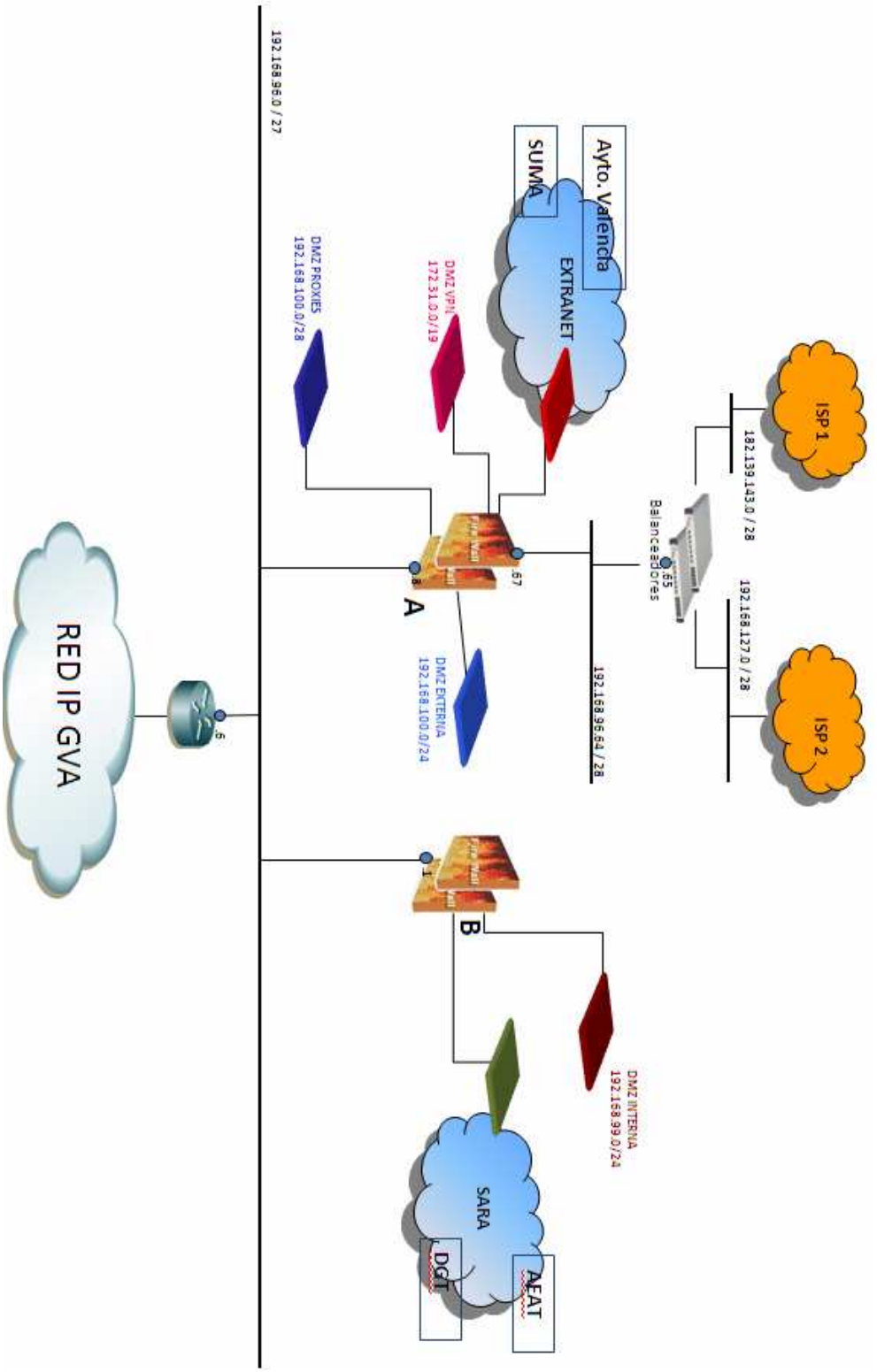


Figura 3.5: Red Corporativa de la GVA.

3.2 Acceso al servicio VPN

El VPN Corporativo de la GVA ofrece un servicio de conexión segura a la RC desde el exterior.

Gracias a este servicio se consigue que el personal de la GVA que quiera acceder a la RC de manera remota pueda hacerlo de forma que el tráfico de datos vaya siempre cifrado fuera de nuestra red hasta el punto final de cliente, impidiendo que pueda escucharse en puntos intermedios.

Así mismo se utiliza para proporcionar acceso a empresas externas que ofrecen un servicio de mantenimiento y monitorización de los distintos servidores y aplicaciones dentro de la GVA.

Otro caso de usuario que, sin ser personal de la GVA utiliza el servicio VPN, es el de los policías locales de las distintas poblaciones de la Comunidad Valenciana para los cuales la GVA actúa de pasarela para que ellos puedan acceder a la página web de la DGT.

Cuando un usuario se conecta vía internet, la configuración de VPN le permite conectarse a la red privada del organismo con el que colabora y acceder a los recursos disponibles de la misma como si estuviera tranquilamente sentado en su puesto de trabajo sufriendo las limitaciones asociadas a la capacidad del servidor de túneles y, si accede a destinos ubicados fuera de la red local de su empresa sufrirá también las limitaciones que le imponga la conexión a internet que tenga su empresa.

El acceso a la RC de la GVA a través de este servicio se realiza siempre de manera personal utilizando los certificados digitales de la ACCV. Todos los accesos son registrados y guardados en un servidor con la hora y el día, permitiendo poder exigir responsabilidades en caso de uso indebido.

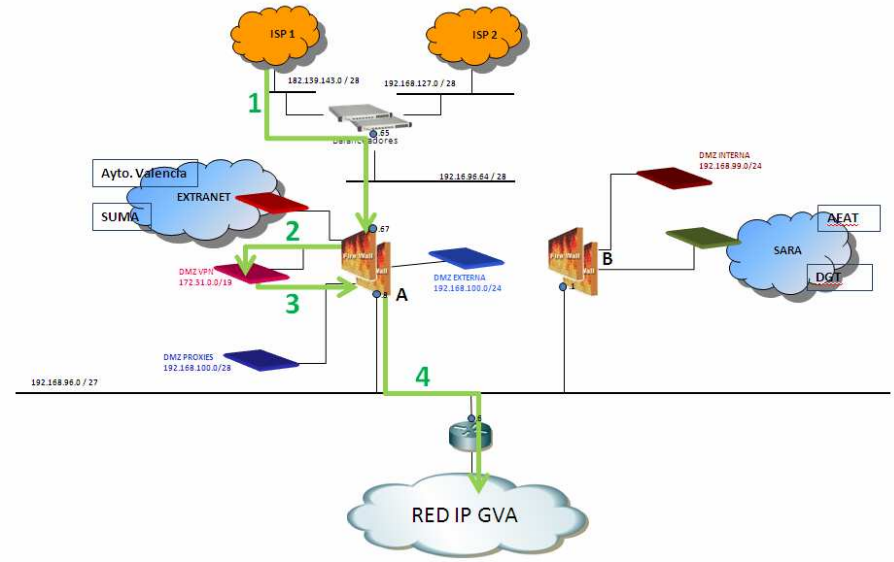


Figura 3.6: Recorrido de una conexión VPN en la RC de la GVA.

El recorrido de una conexión para establecer una VPN con la RC de la GVA (Figura 3.6) sería el siguiente:

1. El usuario entraría desde la internet a la RC a través de uno de los dos ISPs que posee la GVA. Atravesaría los balanceadores y en el cortafuego A pasaría el primer filtrado de seguridad.
2. Del cortafuego A llegaría al concentrador de túneles VPN donde adquiriría su perfil específico de usuario.
3. Nuevamente pasaría por el cortafuego A volviendo a ser filtrado arreglo a su perfil.
4. El usuario ya se encuentra en la RC de la GVA como si estuviera sentado en su puesto de trabajo.

Los trabajadores usuales de la GVA no encuentran diferencia alguna a estar en su oficina o en su casa conectados al servicio VPN.

En el caso de, por ejemplo, los policías locales que no son trabajadores GVA lo que ocurre es que cuando el concentrador VPN asigna su perfil, únicamente permite a la IP con la que el policía entra atravesar el cortafuegos B y llegar a la red SARA. Cualquier otro intento de navegar dentro de la RC de la GVA es rechazado.

3.3 Análisis de requisitos del servicio a implantar.

Veremos en este apartado en qué se han basado y cuáles han sido las elecciones tecnológicas que pasarán a ser los requisitos del nuevo sistema.

Las decisiones que debemos tomar son:

- método de autenticación a usar: RADIUS o LDAP.
- tecnología del cifrado de comunicaciones: IPSec o SSL.
- modo de obtención de los certificados revocados: CRL u OCSP.
- solución *hardware*: Aventail EX2500 o Juniper SA 4000.

3.3.1 Método de autenticación

RADIUS (Remote Authentication Dial-In User Service) y LDAP (Lightweight Directory Access Protocolo) pueden ser los métodos implantados en el nuevo equipo para autenticarse.

Hasta ahora se venía utilizando RADIUS. El motivo principal era porque a través del fichero *users*.*txt* se acababan de ajustar los perfiles de los usuarios además de que se generaba un fichero con todos los *logs* que había habido. Con los nuevos equipos la necesidad de usar *users*.txt

desaparece y también el tema de los *logs* está ya integrado en el propio equipo.

Como LDAP es más eficiente en las búsquedas, es decir, es considerablemente más rápido, nos decantaremos por este protocolo. El trabajo de recoger estadísticas y demás datos recaerá en el nuevo dispositivo que ya está preparado.

3.3.2 Tecnología del cifrado de comunicaciones.

Veamos a continuación como, teniendo las dos posibilidades a nuestro alcance en el nuevo concentrador y teniendo la experiencia de haber hecho uso de IPSec (Internet Protocol Security) en el concentrador antiguo de Cisco, debemos de elegir SSL (Secure Sockets Layer) como la tecnología a utilizar después de elaborar una tabla de pros y contras.

Si IPSec intenta alcanzar seguridad en la propia red, SSL lo hace al nivel de la aplicación.

SSL usa la tecnología embebida en los navegadores web para conectarse de modo seguro. Lo que a priori en una gran ventaja también puede ser a su vez el problema más crítico, ya que supone que un dispositivo (ordenador, PDA, teléfono inteligente, etc.) en cualquier parte del mundo pueden conectarse. Evidentemente esto aumenta la productividad pero, también es obvio, que nuestra red queda expuesta a un sinfín de dispositivos de los cuales desconocemos su seguridad y de los que debemos de protegernos.

IPSec tiene el problema de la necesidad de instalación de un cliente en el ordenador en el que nos vayamos a conectar (con el consiguiente mantenimiento técnico que dada la magnitud de esta la RC de la GVA podría llegar a ser intratable). El usuario está atado a esa máquina. Por el contrario, la seguridad es mayor.

Las enumeradas anteriormente podrían ser, a priori, las diferencias fundamentales de las dos tecnologías. Existen otras (Tabla. 3.1), que pueden servirnos para definirnos por un protocolo u otro en base a ciertos criterios.

Se evaluará a continuación, para las necesidades particulares de la GVA, las características que componen la tabla 3.1.

Control de accesos: el número de conexiones efímeras o puestos móviles es mucho mayor que el de conexiones permanentes, la mayor parte del personal trabaja en dependencias de la GVA sin utilizar el servicio VPN, por lo que en este punto se elegiría SSL.

		SSL	IPSec
Control de Accesos	Conexiones permanentes		✓
	Conexiones efímeras o puestos móviles	✓	
	Ambos tipos de acceso	✓	✓
Usuarios	Todos los usuarios son empleados de la compañía		✓
	No todos los usuarios son empleados de la compañía	✓	
	No todos los usuarios son empleados de la compañía y, además, algunos trabajan con sus propios sistemas	✓	✓
Software Cliente	Todos los usuarios han de tener acceso a todos los recursos de la red		✓
	Deseamos controlar el acceso a determinadas aplicaciones	✓	
	Necesitamos niveles variables de control de acceso en las diferentes aplicaciones	✓	✓
Confidencialidad y Autenticidad	Precisamos de un alto nivel de seguridad en el cifrado y autenticación		✓
	La confidencialidad y autenticidad no son especialmente críticas en nuestros sistemas	✓	
	Precisamos de niveles moderados de confidencialidad e integridad	✓	
Criticidad de los recursos accedidos	Alta		✓
	Moderada	✓	
	Variable	✓	✓
Criticidad de las funciones realizadas	Alta		✓
	Moderada	✓	
	Variable	✓	✓
Nivel técnico de los usuarios	Entre moderado y alto		✓
	Entre moderado y bajo	✓	
Implantación, flexibilidad y escalabidad	Deseamos una implantación rápida y facilidad de mantenimiento	✓	
	Deseamos flexibilidad en las modificaciones futuras		✓
	Ambas consideraciones son importantes	✓	✓

Tabla 3.1: Elección de IPSec o SSL según las características de la red.

Usuarios: no todos los usuarios son de la GVA. El servicio VPN es utilizado, además de por personal propio desplazado, por policías locales y empresas que trabajan para la Generalitat. La elección sería SSL.

Software cliente: si bien unos pocos sí, en general, los usuarios de la VPN no han de tener acceso a todos los recursos de la red. Esto, aparte de poder ser modelado desde el software asociado a la *appliance* (como veremos luego), también puede ser controlado con el uso de permisos en los cortafuegos. En consecuencia una vez más SSL.

Confidencialidad y autenticidad: el tipo de información tratada por la GVA en los servicios accedidos por este servicio VPN, de acuerdo con el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal **[BOE 1]** no son de nivel alto, por lo que se usaría la tecnología SSL.

Criticidad de los recursos accedidos: los recursos accedidos por VPN nos son críticos. Se utilizan en su mayor parte como pasarela para otras webs o para el desarrollo de aplicaciones en pruebas. Se elegiría SSL.

Criticidad de las funciones realizadas: no son críticas debido al tipo de usuario de la VPN. SSL otra vez.

Nivel técnico de los usuarios: el nivel técnico de los usuarios en abrumadora mayoría es bajo. La facilidad de acceder de modo seguro, vía SSL, mediante un explorador web a una aplicación es una ventaja incomparable a tener que instalar un cliente VPN en cada uno de las computadoras de los usuarios. Se usaría SSL.

Implantación, flexibilidad y escalabilidad: en este caso pesa bastante más la implantación rápida y el fácil mantenimiento al tratarse de una red de gran tamaño. Las modificaciones futuras pese a no ser flexibles serán realizadas por personal altamente especializado con lo que el problema se minimiza. SSL sería la elección.

La conclusión es obvia: debemos utilizar tecnología SSL.

Para las necesidades que se buscan cubrir, la mejor opción es la utilización de concentradores SSL VPN. Estos dispositivos no sólo permiten realizar las antiguas funciones del concentrador VPN 3060 de Cisco, sino que mejoran sustancialmente la usabilidad del sistema, ya que permite la utilización de diversos métodos de acceso aparte del tradicional software de cliente VPN.

Los nuevos equipos permitirán ofrecer un acceso mucho más sencillo a través de navegador web, sin renunciar a la seguridad que nos ofrece la encriptación y la utilización de certificados digitales.

3.3.3 Modo de obtención de los certificados revocados.

Cuando un tercero desea comprobar la validez de un certificado debe descargar una CRL (Lista de Certificado Revocados) actualizada desde los servidores de la misma AC (Autoridad de Certificación) que emitió el certificado en cuestión. A continuación comprueba la autenticidad de la lista gracias a la firma digital de la AC. Después debe comprobar que el número de serie del certificado cuestionado está en la lista. En caso afirmativo, no se debe aceptar el certificado como válido.

Estrictamente hablando, no es necesario descargar una CRL cada vez que se verifica un certificado. Solamente es necesario cuando no se dispone de la CRL de una entidad de certificación concreta o cuando dicha lista tiene una cierta antigüedad que aconseja su renovación.

La única ventaja de las CRL es que se pueden consultar sin necesidad de una conexión de datos permanente con cada AC. Basta establecer dicha conexión con cierta periodicidad para descargar las CRLs actualizadas.

Sin embargo, las desventajas de las CRLs son varias:

- ✓ El contenido de las CRL puede considerarse información sensible, análogamente a la lista de morosos de un banco.
- ✓ La búsqueda en la CRL es de modo secuencial. Los registros que se encuentran al principio de la lista no son problemáticos. La desventaja aparece cuando estos registros buscados están al final de la CRL. Entonces el tiempo de búsqueda se hace crítico.
- ✓ Existe el peligro de que un certificado haya sido revocado, pero no aparezca en la CRL del tercero que comprueba su validez. Esto se debe a que la CRL utilizada podría no estar actualizada.
- ✓ Si existe responsabilidad legal por el uso de un certificado revocado, no hay forma de demostrar quién es el culpable: el tercero por no comprobar la validez, o la AC por no incluirlo en la CRL a tiempo.
- ✓ Las CRL crecen en tamaño, resultando ineficientes para su tratamiento directo. Uno de los problemas que se encuentra en el Cisco VPN3060 es precisamente este, el tamaño de la CRL es superior al del buffer de datos dedicado que hay en el dispositivo. En la actualidad el tamaño de la CRL de la ACCV es de 1,5 MB, por contra el tamaño del buffer en el *hardware* dedicado es de 1MB.

La única alternativa a las CRLs es utilizar un protocolo de consulta en línea que aporte información al momento sobre cada certificado en concreto. Este protocolo se denomina OCSP (Online Certificate Status Protocol).

La naturaleza de las peticiones y respuestas de OCSP hace que a los servidores OCSP se les conozca como OCSP *responders*.

OCSP fue creado para solventar las deficiencias de las CRLs.

Sus ventajas respecto a estas son:

- ✓ puede proporcionar una información más adecuada y reciente del estado de revocación de un certificado.
- ✓ elimina la necesidad de que los clientes tengan que obtener y procesar las CRLs, ahorrando de este modo tráfico de red y procesado por parte del cliente.
- ✓ la búsqueda de información en OCSP está optimizada de modo que ofrece tiempos de respuesta mucho mejores.
- ✓ el consumo medio de ancho de banda para la consulta por usuario es menor.

OCSP soporta el encadenamiento de confianza de las peticiones OCSP entre los *responders*. Esto permite que los clientes se comuniquen con un *responder* de confianza para lanzar una petición a una AC alternativa dentro de la misma Infraestructura de Clave Pública (PKI).

Una consulta por el estado de un certificado sobre una CRL debe recorrerla completa secuencialmente para decir si es válido o no. Un OCSP *responder* en el fondo usa un motor de base de datos para consultar el estado del certificado solicitado, con todas las ventajas y estructura para facilitar las consultas. Esto se manifiesta aún más cuando el tamaño de la CRL es muy grande.

Es obvio que debemos de elegir OCSP como el modo de obtener los certificados revocados. El número de ventajas sobre CRL es abrumador.

3.3.4 Solución *hardware*

En base al informe de la consultoría Gartner **[Apéndice A]** que recomienda como punteros en este terreno a Juniper y Aventail se pidió a ambas empresas que hicieran sendas presentaciones de sus productos y que permitieran a la GVA las pruebas con las máquinas.

En la tabla 3.2 se han expuesto las características principales tanto de las nuevas alternativas como del antiguo concentrador. El objetivo de mostrar las del antiguo es para poder ver el salto tecnológico que se ha llevado a cabo.

Como se puede observar en la tabla 3.2, las diferencias entre Aventail EX2500 y Juniper SA 4000 son mínimas.

Después de haber estado configurando e integrando ambos sistemas dentro de nuestro entorno de trabajo pensamos que la que mejor se adaptaba a nuestras necesidades era la oferta de Juniper. La razón fundamental se basaba en la alta compatibilidad con nuestros

sistemas de autorización de certificados digitales. Además de: el interfaz más amigable que éste presenta, el tipo de servicio de mantenimiento ofertado por la marca y su precio.

	Cisco VPN3060	Aventail EX2500	Juniper SA 4000
Usuarios concurrentes SSL	500	2000	2000
***Clúster*[4]**	----------	8	6
Memoria sistema	512MB	2 GB	2 GB
Ancho de banda	100 MB	1 GB	1 GB
Tiempo medio entre fallos	--------	100.000 horas	65.000 horas
Encriptación	DES, DES3, AES, MD5, SHA	DES, DES3, RC4, AES, MD5, SHA	DES, DES3, RC4, AES, MD5, SHA
Certificados Revocados	CRL	CRL OSCP	CRL OCSP
Servicio de directorio	Microsoft AD LDAP RADIUS	Microsoft AD LDAP RADIUS	Microsoft AD LDAP RADIUS

Tabla 3.2. Comparación de las características más importantes de los tres concentradores VPN.

3.4 Características del equipo a migrar: Cisco VPN 3060

El servicio VPN hasta ahora era ofrecido por el concentrador VPN 3060 de Cisco. En el **Apéndice B** se puede consultar cómo era su configuración y la problemática asociada tanto a la tecnología utilizada como al propio equipo. A continuación veremos un extracto de los puntos más importantes que ayudaran a comprender la transición de un equipo a otro y las ventajas que se han obtenido con la migración.

3.4.1 Proceso de alta en el servicio

El proceso de alta en el servicio involucra al usuario y al administrador. El primero deberá instalar el cliente y los certificados (tanto el suyo propio, CP, como los de la ACCV, CACCV) en su equipo. El

[4] *Cluster*: conjunto de máquinas comportándose como si fueran una única.

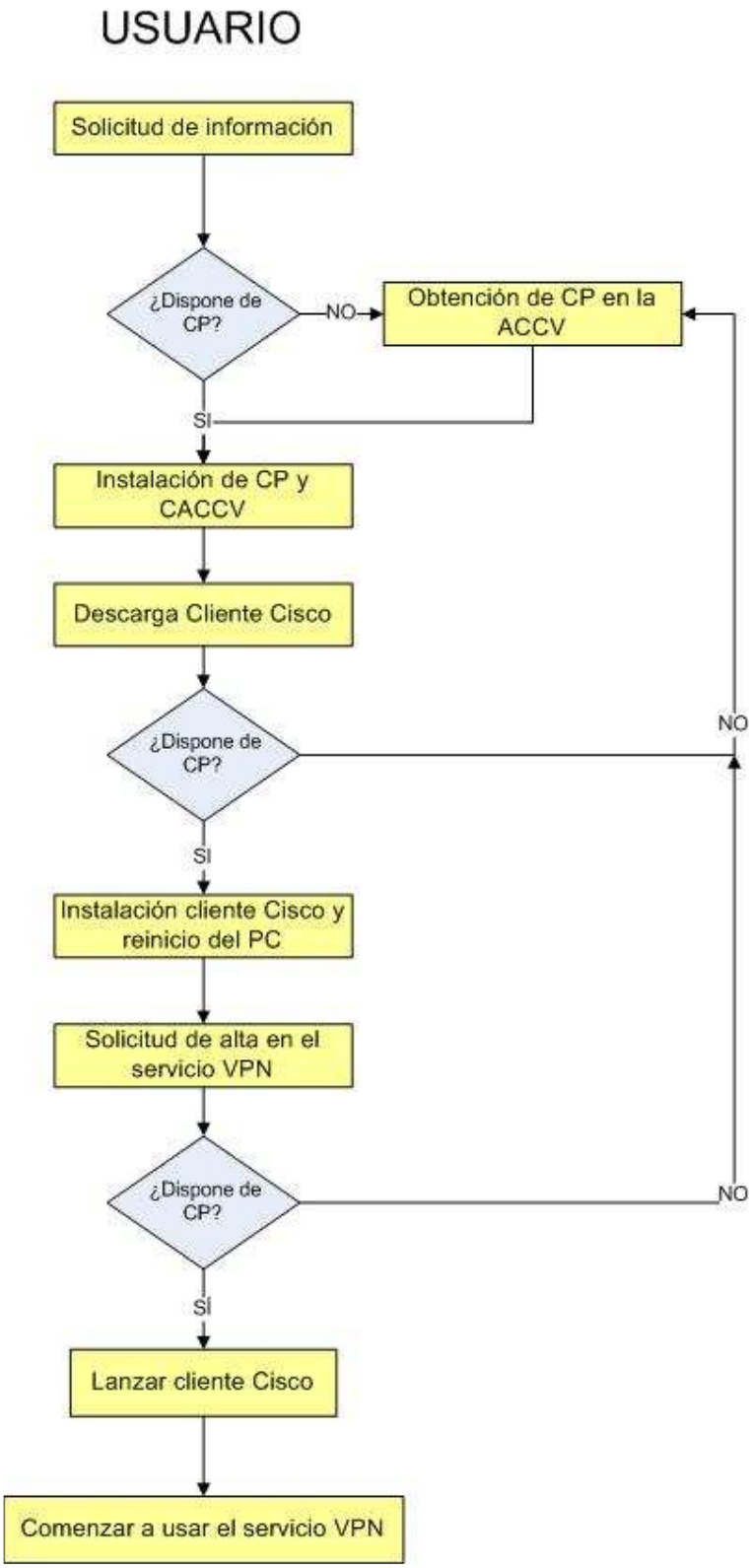


Figura 3.7: Diagrama de flujo de los pasos necesarios a seguir por parte del usuario para el uso del servicio VPN en el equipo a migrar.

segundo dará de alta al usuario en el servicio y si fuera necesario al grupo al cual pertenece ese usuario.

Cuando se habla de CP se entiende que es el certificado expedido por la ACCV.

Veamos unos diagramas de flujo para ver el proceso seguido por el usuario que quiere comenzar a usar el servicio (Fig. 3.7) y la labor desarrollada por parte del administrador del servicio VPN para dar de alta a este usuario (Fig. 3.8). Posteriormente utilizaremos estos diagramas para poder comparar el nuevo dispositivo.

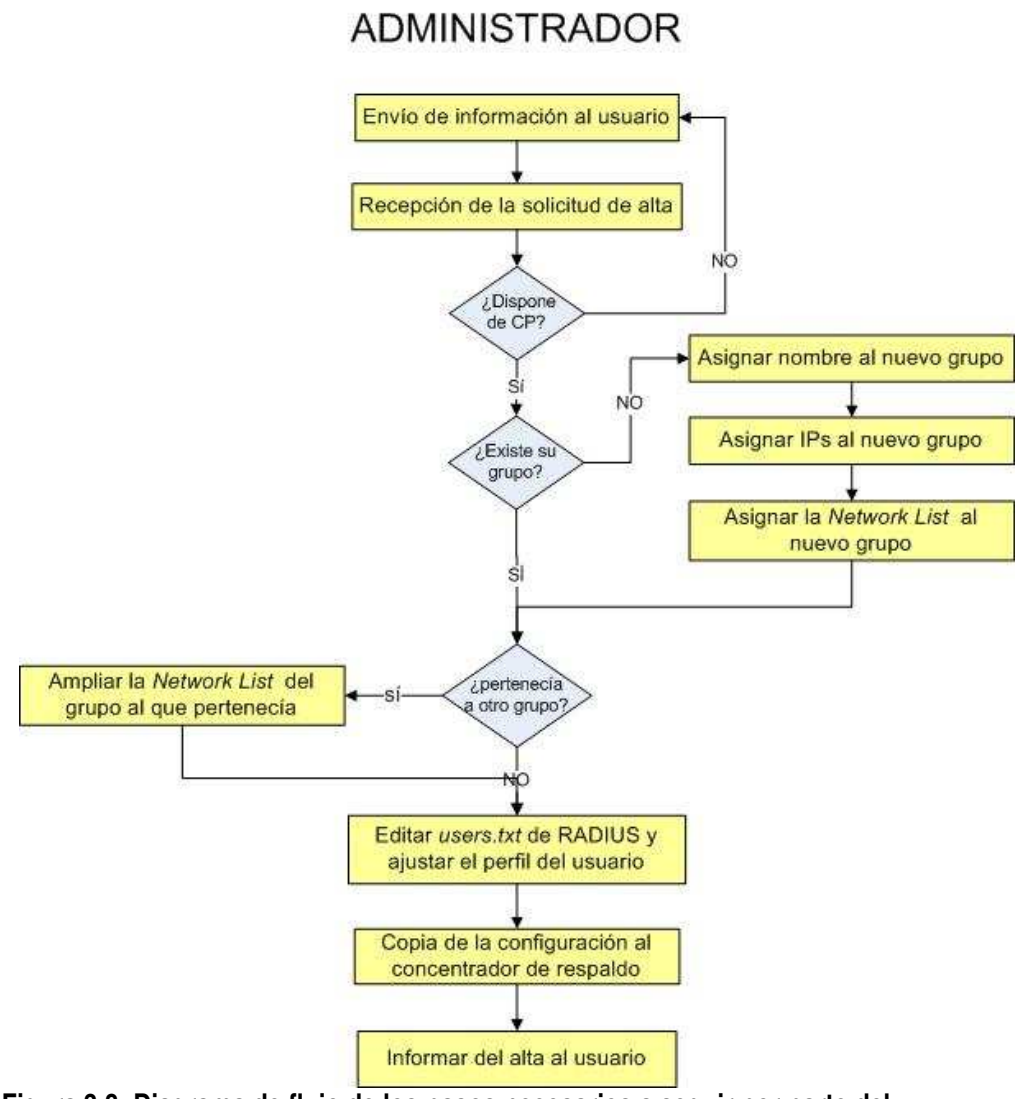


Figura 3.8: Diagrama de flujo de los pasos necesarios a seguir por parte del administrador para dar de alta a un nuevo usuario en el equipo a migrar.

Como vemos en la figura 3.7 el usuario, para poder descargarse el cliente de Cisco, necesita tener su certificado. Se puede ver todo el proceso con los pasos a seguir por parte del usuario de manera detallada en el **Apartado B.1.1.**

En la figura 3.8 vemos los pasos seguidos por parte del administrador del servicio VPN para dar de alta a un nuevo usuario.

Podemos ver en detalle todo el procedimiento en el **Apartado B.1.2.** Comentar únicamente que es con la edición del fichero *users*.txt de RADIUS como se consigue terminar de ajustar el perfil del usuario asignándole su grupo, IP, etc. La *Network List* son las IPs a las que el grupo en cuestión puede tener acceso.

3.4.2 Proceso seguido en el concentrador

Veamos a continuación cuando llega una petición al concentrador VPN de Cisco cuáles son los pasos que se siguen.

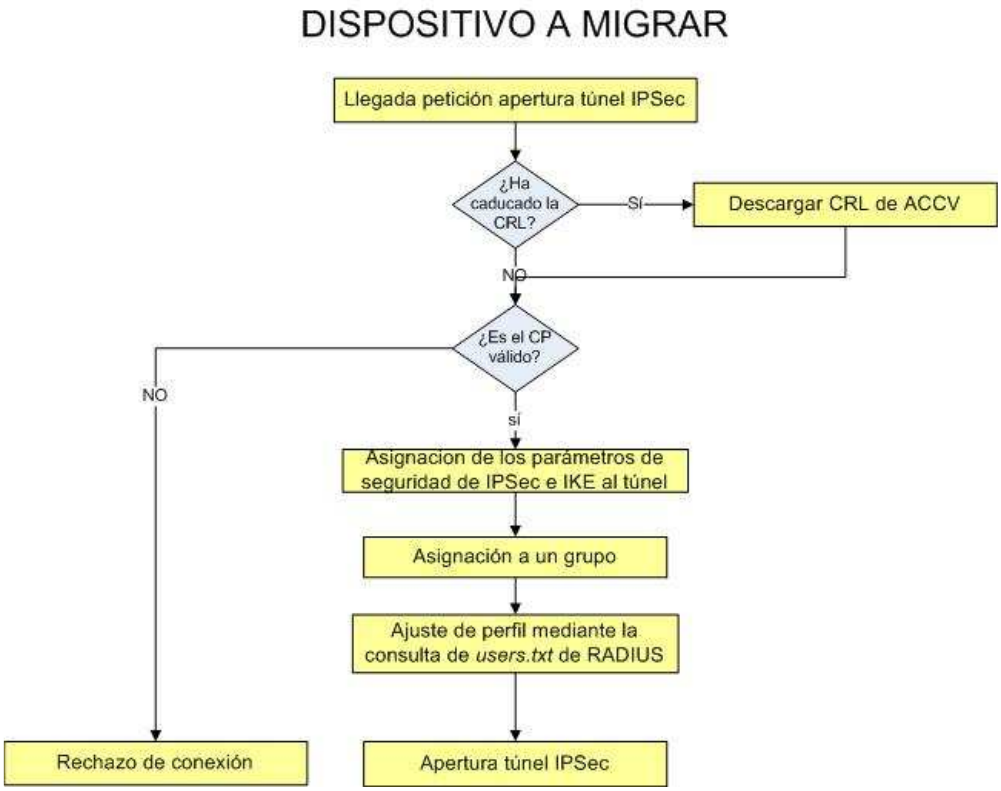


Figura 3.9: Diagrama de flujo de los pasos realizados por el equipo a migrar para la apertura de un túnel IPSec.

Como vemos en la figura 3.9 puede darse el caso de que a un usuario cuyo certificado haya sido revocado se le permita entrar en el sistema porque la CRL no haya sido actualizada. Éste junto con otros problemas son comentados a continuación y estudiados de modo más exhaustivo en el **Apéndice B**.

3.4.3 Problemas del equipo

Los problemas a los que avocaba el uso del Cisco eran de diverso orden:

- Problemas con el cliente: a nivel de instalación (creados por la inexperiencia del usuario o por el sistema operativo usado) y a nivel del cierre de la sesión de usuario.
- Problemas con el tamaño de la Lista de Certificados Revocados (CRL) que no cabían en la memoria del dispositivo.
- Problemas con la creación de los grupos a los que pertenecen los usuarios ya que un usuario puede pertenecer a más de un grupo haciendo muy costoso el ajuste de su perfil.
- El manejo del *log* de RADIUS es muy costoso, si queremos filtrar algún tipo de información lo hemos de hacer de modo manual o hacernos nuestros propios scripts.[5]
- Problemas a la hora de copiar la configuración del equipo activo al de *backup,* El proceso se hace de forma manual.
- Y cómo no, el problema principal y que ha llevado a la migración del servicio VPN y a la postre a la creación del presente proyecto final de carrera, la descatalogación del equipo y la suspensión de su mantenimiento.

3.5 Características de la solución a integrar: Juniper SA4000

El nuevo concentrador de túneles VPN puesto en funcionamiento en la RC de la GVA ha sido el Juniper Networks SA 4000 SSL VPN. En el Capítulo 4 y en Anexo D se verá con detalle la configuración del sistema. En el presente apartado se verá un extracto de los puntos más importantes ya vistos en el apartado anterior para el dispositivo de Cisco para así, finalmente, poder compararlos a ambos.

3.5.1 Proceso de alta en el servicio

El proceso de alta en el servicio involucra al usuario y al administrador. En eso no encontraremos diferencia con el anterior dispositivo; lo que marcará una diferencia notable será el cómo. El objeto final de este proceso de alta es que el usuario pueda hacer uso del servicio.

[5] *Script*: conjunto de instrucciones que permiten la automatización de tareas.

3.5.1.1 Por parte del usuario

Después de solicitar la información al servicio de comunicaciones de la GVA, el usuario deberá instalar los certificados (CP y CACCV) en su equipo y pedir el alta en el servicio.

Desde el servicio de comunicaciones se le indicará la URL (Uniform Resource Locator) que debe de introducir en su navegador para hacer uso del servicio.

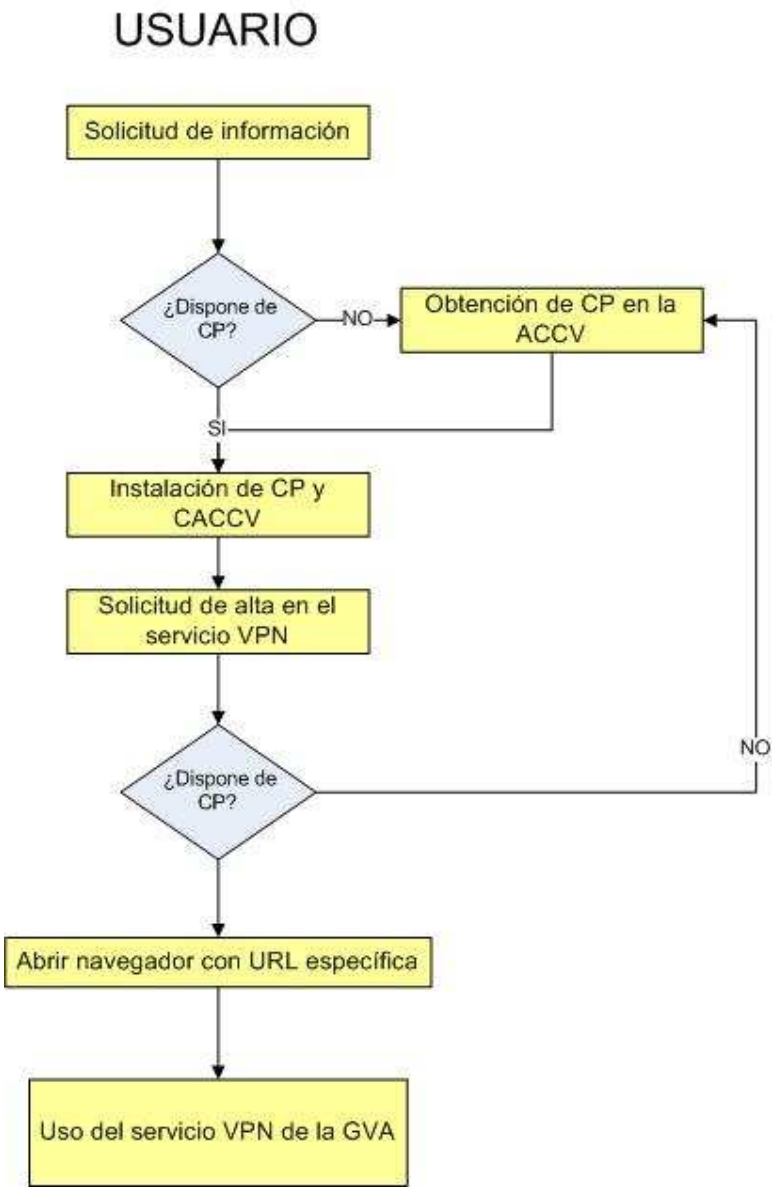


Figura 3.10: Diagrama de flujo de los pasos necesarios a seguir por parte del usuario para el uso del servicio VPN en el equipo a integrar.

Puede verse en la figura 3.10 el proceso seguido por el usuario que quiere comenzar a usar el servicio VPN.

3.5.1.2 Por parte del administrador

Como vemos en la figura 3.11 el administrador una vez recibe la petición de alta en el servicio comprueba que el usuario tiene CP y en el LDAP lo añade al grupo. Si es necesario crea primero el grupo.

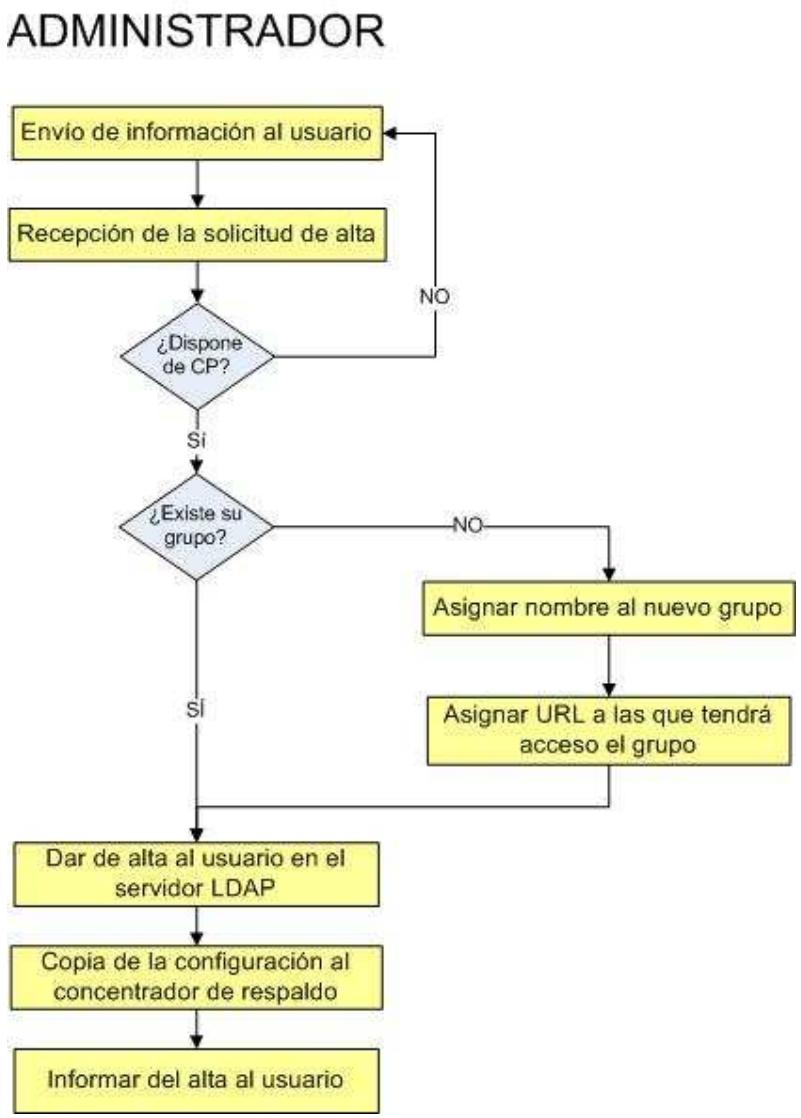


Figura 3.11: Diagrama de flujo de los pasos necesarios a seguir por parte del administrador para dar de alta a un nuevo usuario en el equipo a integrar.

Los usuarios se añaden a los grupos en el servidor LDAP; la configuración del concentrador no se toca para nada.

Si hay que crear un grupo nuevo eso sí se hace en el concentrador.

3.5.2 Proceso seguido en el concentrador

Podemos ver el diagrama de flujo en la figura 3.12. Cuando llega una petición el concentrador comprueba que el certificado es válido haciendo una consulta OCSP.

A continuación se hace una consulta LDAP que devuelve el grupo al que pertenece el usuario. El concentrador asigna el perfil de ese grupo y abre el túnel SSL.

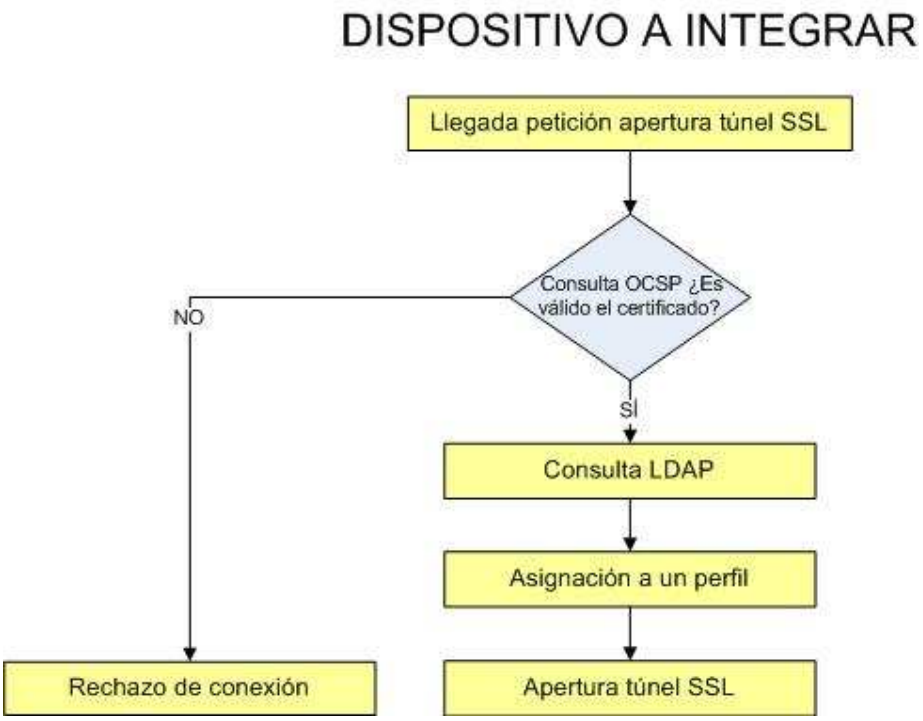


Figura 3.12: Diagrama de flujo de los pasos realizados por el equipo a integrar para la apertura de un túnel SSL.

3.6 Consecuencias de la migración

Veremos a continuación como el nuevo dispositivo ha reducido considerablemente el número de tareas a realizar por parte del usuario, del administrador y del concentrador. Además se han resuelto todos los problemas que teníamos, algunos de ellos eran críticos, como el de las CRLs.

3.6.1 Ventajas en el proceso de alta por parte del usuario

Comparando las figuras 3.7 con la figura 3.10 se puede observar cómo ha desaparecido del diagrama de flujo todo lo que tiene que ver con el cliente:

- ✓ verificación de que el usuario tiene el CP para descargárselo.
- ✓ instalación del mismo, con un significativo ahorro en la cantidad de recursos de personal que acarrea una incorrecta instalación.
- ✓ reinicio del ordenador del usuario.

Sólo en este primer punto el ahorro de esfuerzo de trabajo ya compensa toda la inversión realizada. Se verá a continuación una tabla comparativa (Tabla 3.3) del tiempo dedicado a subsanar problemas de instalación del cliente en cada uno de los dispositivos.

Obviamente las llamadas realizadas por problemas con el Juniper no se refieren a la instalación de ningún cliente sino a problemas mínimos de comprensión de las indicaciones mandadas desde el servicio de comunicaciones respecto a la apertura del navegador con una URL específica.

	Cisco VPN3060	**Juniper SA 4000**	**% de mejora**
Nivel 1	650 min./mes	25 min./mes	**96%**
Nivel 2	130 min./mes	10 min./mes	**92%**

Tabla 3.3: Tiempo utilizado por el servicio de atención telefónica y los administradores del sistema en resolver problemas generados por el cliente en cada dispositivo.

Existen dos niveles de atención telefónica:

- Nivel 1, que es el formado por los trabajadores del centro de atención telefónica que atienden las incidencias en primera instancia tratando de resolverlas siguiendo unos procedimientos estandarizados en un manual.
- Nivel 2, si los trabajadores del Nivel 1 no han sido capaces de resolver el problema aplicando el procedimiento establecido, la incidencia pasa a este nivel que está formado por los propios administradores del sistema.

Como vemos en la tabla hay un ahorro de tiempo usado en atender incidencias de este tipo del 96% en el Nivel 1 y del 92% en el Nivel 2.

Los vistos hasta ahora son beneficios que dependiendo del usuario redundan en los administradores. Uno que sí que es directo para los primeros es que, a partir de ahora, el usuario ya no tiene que ejecutar la aplicación cliente, sino que simplemente abrirá su navegador y tecleará la URL que le digan los administradores.

3.6.2 Ventajas en el proceso de alta por parte del administrador

Comparando la figura 3.8 con la figura 3.11 podemos ver como la parte inicial es igual en cuanto a la comprobación por parte del administrador de que el peticionario dispone de CP.

Las diferencias comienzan cuando el usuario pertenece a más de un grupo. Entonces en el equipo a migrar hay que ampliar la Network List del grupo al que ya pertenecía el usuario y ajustar el perfil mediante la edición de users.txt de RADIUS. En el equipo a integrar que un usuario pertenezca a más de un grupo no supone ningún tipo de problema; se le añade a tantos grupos como pertenezca en LDAP y en el concentrador se crea el recurso.

Otra diferencia, si cabe, aún más importante que la anterior es que en el nuevo concentrador la copia de la configuración sobre el concentrador de respaldo es prácticamente automática.

En la tabla 3.4 podemos ver una comparación de los distintos tiempos aproximados.

	Cisco VPN3060	**Juniper SA 4000**
Añadir usuario a un grupo por primera vez	3 min.	2 min
Añadir usuario a un segundo grupo	8 min.	2 min
Copiar la configuración en el concentrador de respaldo	3 min.	0,5 min
TOTALES	**14 min. -- 6 min.**	**4,5 min. -- 2,5 min.**
	% de mejora	**68% --------- 59%**

Tabla 3.4: Tiempos medios utilizados por el administrador del sistema en los dos concentradores cuando se añade un usuario a un grupo por primera vez y cuando se añade a un segundo grupo.

Analizando la tabla por partes observamos como la reducción mayor de tiempos ha sido la obtenida en el volcado de la configuración en el concentrador de respaldo con un 83%.

A continuación la segunda mejora mayor ha sido la de añadir a un segundo grupo a un usuario con un 75%.

En añadir a un usuario por primera vez a un grupo se ha ahorrado un 33%.

Cuando el administrador hace algún cambio obligatoriamente ha de volcar la nueva configuración en el concentrador de respaldo y es ahí, suma de los tiempos, donde el ahorro obtenido se hace más evidente.

Hemos logrado reducir el tiempo de añadir a un usuario a un grupo a un poco menos de la mitad, siendo éste el caso aproximadamente del 90% de las solicitudes que se gestionan.

El tiempo de añadir a un usuario a un segundo grupo ha descendido en poco más de 2/3 lo que es un ahorro muy considerable.

3.6.3 Ventajas en el proceso seguido por el equipo

Comparando la figura 3.9 con la figura 3.12 observamos varias diferencias.

La consulta de los certificados revocados ya no se hace sobre una CRL habiéndola actualizado si ha sido necesario, sino mediante una consulta OCSP. El tamaño actual de la CRL de la ACCV es de unos 1500 KB; el tamaño de una consulta OCSP es de unos 30 KB.

Si se considera que se usa una CRL almacenada por un tiempo para ser consultada contra el ancho de banda (BW) que se usa por cada consulta a través de OCSP, existe una diferencia de uso de BW que crece mientras aumenta el número de validaciones por día que debe responder la AC. Con CRL el BW usado sigue una curva logarítmica por el hecho de que aunque aumenten las consultas diarias, estas se hacen a la CRL almacenada. En cambio, con OCSP, si las consultas aumentan necesariamente aumenta el BW usado por lo que la curva resultante es exponencial. Debido a esto, el tiempo de validación, a pesar de seguir la misma curva, al aumentar las validaciones por día usando CRL, el tiempo "límite" es menor al que se obtiene si se usa OCSP.

Claro que esto sería suponiendo que actualizamos la CRL únicamente una vez al día. Pero esa situación no corresponde con las necesidades de la GVA. Por motivos de seguridad la CRL debería de ser descargada como mínimo cada 30 minutos.

Veamos en la tabla 3.5 el ahorro en el consumo de BW que supone el uso de OCSP en vez de descargar la CRL. Vamos a suponer que de los 300 accesos de media que tiene al día el servicio VPN el 80% se da en horario laboral que sería de las 8:00h a las 20:00h.

Tenemos pues 240 validaciones haciendo uso de la CRL en 12 horas; como la CRL se actualiza cada 30 minutos, suponiendo una distribución homogénea de estas validaciones, obtendremos que cada vez que se descarga la CRL en el concentrador se comprueba la validez del certificado de 10 usuarios. La conexión de la GVA tiene una media de 150K/seg.

	CRL	OCSP
Consumo de BW por usuario validado	1500KB/ 150KB= 10seg 10seg./10user= **1 seg.**	30KB/150KB = **0,2 seg**.
	Porcentaje de mejora	**80%**

Tabla 3.5: Consumo de BW por usuario validado usando CRL u OCSP.

Recordemos que esta, entre otras, era una de las ventajas que aportaba el uso de OCSP expuestas en la del Capítulo 3 cuando analizábamos los requisitos que se exigirían al nuevo sistema.

La segunda diferencia es que ya no hemos de terminar de ajustar el perfil de cada usuario con el archivo *users.txt*. Ahora la consulta del LDAP nos devuelve directamente el perfil correcto del usuario.

3.6.4 Solución a los problemas planteados en el equipo a migrar

En los puntos anteriores hemos visto las ventajas que hemos obtenido con la migración del servicio comparando las acciones llevadas a cabo por usuario, administrador y dispositivo.

También planteamos en su momento unos problemas que, en parte, han sido resueltos al enumerar estas ventajas nombradas con anterioridad. Los repasaremos a continuación.

El problema de la instalación del cliente de Cisco ha desaparecido por completo. El nuevo dispositivo no necesita de la instalación de ningún tipo de cliente con lo que el problema no existe. También se ha ganado el tiempo que pasaba desde que la aplicación cliente era abierta hasta que finalmente se cerraba el túnel VPN.

Poco más o menos ocurre con el tema de las CRLs, ahora el nuevo dispositivo ha adoptado OCSP. Ya no hay que descargar ningún tipo de información; la información no debe de ser almacenada en el dispositivo luego tampoco tenemos ya problema de tamaño de buffer y para rematar, no hay ningún peligro de que la información esté obsoleta. La consulta en línea nos ha quitado todos estos problemas.

En cuanto a los grupos a los que pertenecen los usuarios ya no habremos de ampliar su *network list* para luego restringir sus derechos editando el *users.txt* de RADIUS. Cuando el usuario entre en el sistema se le asignará un perfil específico, independientemente de a cuantos grupos pertenezca y sin tener que alterar ninguno de ellos por el hecho de que un usuario pertenezca a varios.

Los *logs* del sistema son mucho más amigables que en el dispositivo anterior, la información ya no es volcada sin más en un archivo; ahora las consultas son más fáciles.

La configuración del dispositivo que está funcionando al de respaldo ya no es una tediosa tarea. Simplemente apretando un botón en la aplicación del nuevo dispositivo la configuración es copiada automáticamente.

Además la copia de la configuración del equipo se puede automatizar, de tal modo que es la propia máquina la que envía a un servidor externo, de nuestra elección, su configuración cada intervalo de tiempo que nosotros decidamos.

Evidentemente el problema de la descatalogación del nuevo equipo no está todavía en el horizonte y para aquel entonces existirá una nueva tecnología que aún mejore y haga más fácil la administración de los dispositivos.

3.7 Resumen

En este capítulo hemos conocido cómo está estructurada la RC de la GVA y cuál es el recorrido de una conexión VPN.

Hemos razonado el porqué de las elecciones de cada una de las tecnologías posibles; estas elecciones han pasado a ser los requisitos que se implementaran en el nuevo sistema.

Para poder comprobar que la migración ha mejorado lo que existía hasta ahora hemos presentado de modo básico cómo estaba configurado el equipo a migrar y de qué manera se realizaban las tareas.

Se ha mostrado cómo se hacen ahora esas tareas en el nuevo concentrador y, finalmente, se ha demostrado fehacientemente como la migración sólo ha traído beneficios al sistema.

Capítulo 4.
Implementación del nuevo servicio VPN

El proceso seguido fue el siguiente:

- lo primero en ser instalado y configurado fue el servidor LDAP (Lightweight Directory Access Protocolo) sobre la máquina Sunfire.
- a continuación se configuró el nuevo concentrador de túneles SSL VPN Juniper.
- se acabó realizando las tareas necesarias para que el servicio pudiera ser utilizado en la Red Corporativa (RC).

4.1 Instalación del servidor LDAP

El servidor LDAP fue instalado sobre un par de máquinas Sun, concretamente Sunfire V120 **[SunV120]**. El sistema operativo que se instaló en estas máquinas fue Solaris 10 **[Sol10]**.

Estos dos servidores trabajan con un balanceo activo/pasivo para garantizar la disponibilidad, a su vez, sus discos están formando un RAID1.

La información que se guarda en un directorio está formada por entradas; cada entrada es un conjunto de atributos que se identifica unívocamente a través de un Distinguished Name (DN). Cada uno de estos atributos es de un tipo concreto y puede tener uno o varios valores. Estos atributos suelen ser nemónicos como por ejemplo *cn* (*common name*) o *mail* que indicaría el nombre o email de una entrada en el directorio.

La información se almacena en el directorio en forma de árbol jerárquico, en nuestro caso utilizando la jerarquía de internet para definir la estructura del directorio LDAP. Así, la raíz será **es**, un hijo, **accv** y dentro de este los diversos usuarios que pudiera tener (Figura 4.1).

LDAP posee un atributo, *objectClass*, que permite definir qué datos van a ser obligatorios y cuáles opcionales a través de los esquemas (*schemas*). O sea, los esquemas van a ser como definiciones de los datos que va a contener el directorio. OpenLDAP incluye varios esquemas, pero

podremos añadir o modificar los ya existentes para cumplir con nuestras necesidades.

El acceso a la información del directorio se hace a través de los DN; los DN son únicos. Por ejemplo, para el ejemplo de accv, imaginemos que tenemos un usuario que tiene de ***uid*** user1. Su DN sería:

dn: uid=**user1**, cn=**ciudadano**, dc=**accv**, dc=**es**

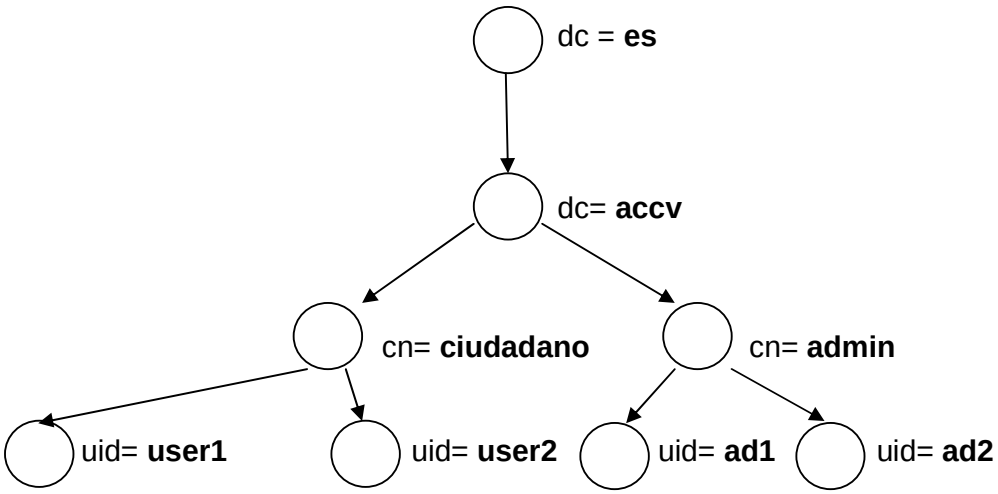


Figura 4.1 Árbol del directorio LDAP para el servicio de autenticación implementado en la GVA.

OpenLDAP permite, además, definir ACL (Access Control Lists) para el acceso a los datos, aparte de que permite transmitir los datos sobre una capa segura como OpenSSL. Así mismo, OpenLDAP permite la replicación de los datos entre varios servidores OpenLDAP. Para descongestionar los servidores nosotros utilizaremos un único servidor.

Una vez se tiene clara la estructura que tendrá nuestro directorio LDAP podemos comenzar a configurar el fichero **Apéndice C**. Terminada esta configuración podemos pasar a añadir los datos al directorio; todo el intercambio de datos con LDAP se hace con unos ficheros con un formato especial. El detalle de cómo añadimos los datos también puede ser visto en el Apéndice C.

Para ahorrar tiempo de configuración se ha hecho un *script* que transforma los usuarios de Radius en usuarios de LDAP. Concretamente el *script* va leyendo el fichero *users*.txt y transformándolo en el fichero *.ldif* que, como se explica en el Apéndice C, es el que usamos para añadir la información a nuestro servidor LDAP.

4.2 Configuración del nuevo equipo

Por motivos de seguridad y para alcanzar la alta disponibilidad del servicio VPN, las máquinas Juniper forman un *clúster* en modo activo pasivo.

Tiene una IP física cada uno y una virtual conjuntamente que es la que se publica para el servicio. Cuando el activo cae, instantáneamente, el pasivo pasa a ser el activo de modo transparente para los usuarios. Los que estuvieran conectados no pierden el servicio ni han de volver a autenticarse; la máquina de respaldo está funcionando en paralelo a la activa.

Comenzaremos a configurar el equipo. Como veremos los conceptos que usa Juniper se alejan bastante de la visión del de Cisco.

La aplicación que maneja al Juniper se llama IVE (Instant Virtual Extranet).

Este apartado no pretende ser un manual [**Manual**]. Repasaremos los pasos seguidos para la configuración del dispositivo. Las capturas con las partes más importantes de la configuración (obviamente sería inviable mostrarlas todas) se pueden consultar en el **Apéndice D**.

Comenzamos instalando las licencias que hemos adquirido: *clúster* para dos equipos compartiendo 250 usuarios concurrentes, ampliación de funcionalidades en el IVE, etc.

A continuación le asignamos una IP al concentrador indicando cuál de los dos que forman el *clúster* es el que funciona como Maestro. Le damos también las IPs de los que serán sus servidores de dominio y su puerta de enlace. Le indicamos el servidor al que se enviará la copia de seguridad de su configuración y el intervalo de tiempo que queremos que utilice para llevar a cabo la tarea.

Tenemos que instalar el certificado propio del concentrador. Añadimos las Autoridades de Certificación (AC) en las que confiamos y le decimos que use OCSP (Online Certificate Status Protocol) como método para comprobar si los certificados de los usuarios son válidos.

Introducimos la IP de nuestro servidor LDAP, la de su respaldo y le decimos que es lo que tiene que comprobar cuando haga la consulta.

Llegados a este punto podemos comenzar a configurar las partes principales de nuestro servicio VPN, como son:

- Definición de los distintos **roles de usuario** que tendremos.
- Definición de los distintos **perfiles de recurso**.
- Definición de los **dominios de autenticación**.
- Definición de una **política de inicio de sesión**.

A cada **rol de usuario** le asignamos un nombre y le decimos el tipo de acceso al que tendrá permiso, podemos elegir dar accesos a: web, archivos, telnet, etc.

Pasamos a crear un **perfil de recurso**, que es un conjunto de opciones de configuración que contiene:

- política del recurso: que especifica los recursos a los que se aplicarán las políticas (como URLs, servidores, archivos) y si el IVE ha de ejecutar alguna acción.
- asignación a roles de ese recurso.
- marcadores que darán acceso al recurso.

Un **dominio de autenticación** es un conjunto de recursos de autenticación que incluye:

- Un servidor de autenticación que verifica la identidad del usuario (LDAP en nuestro caso). El IVE reenvía las credenciales enviadas desde la página de inicio de sesión a nuestro servidor de autenticación LDAP.
- Una política de autenticación que especifica qué requisitos de seguridad del dominio de autenticación deberán cumplirse para que el IVE reenvíe las credenciales a nuestro LDAP.
- Reglas de mapeo de roles que son las condiciones que un usuario debe de satisfacer para que el IVE asigne al usuario uno o más roles. Estas condiciones se basan en la información devuelta por el nombre de usuario de la persona o los atributos del certificado.

Una **política de inicio de sesión** es una regla del sistema que especifica:

- La URL en la que el usurario puede iniciar una sesión en el IVE. Por ejemplo, http://ive/PFC.
- Una página de inicio de sesión que mostrar al usuario.
- Si el usuario debe o no escribir o seleccionar un dominio de autenticación al que el IVE envíe las credenciales.
- los dominios de autenticación a los que la política es aplicable.

Habiendo seguido todos los pasos expuestos con anterioridad el concentrador queda configurado para su uso.

En la figura 4.2 podemos ver cómo encajan todas las partes vistas en el presente apartado. Hagamos un repaso de todas ellas:

1. El usuario teclea en su navegador la dirección URL que le haya facilitado el servicio de comunicaciones para poder hacer uso del servicio VPN de la GVA.
2. El IVE evalúa las políticas de inicio de sesión hasta que la URL que ha introducido el usuario coincide con los que el IVE

posee y muestra la usuario una pantalla de autenticación. Si no coincide, la conexión es rechazada.

Figura 4.2: Participación de cada una de las partes del nuevo servicio VPN en la creación de un túnel SSL.

3. El usuario se autentica con el certificado que le ha suministrado la ACCV.
4. El IVE reenvía el certificado de usuario al servidor LDAP que en caso de ser correcto devuelve al IVE una serie de atributos que servirán para mapear al usuario en un determinado grupo o grupos.
5. El IVE evalúa la información que le ha devuelto el servidor LDAP y asigna al usuario a un grupo o grupos.
6. El usuario solicita un recurso.
7. El IVE evalúa los perfiles de recurso y políticas asociadas a ese usuario.
8. El IVE actúa como intermediario entre el usuario y el servidor/recurso al que éste quiere acceder.
9. El usuario accede a los recursos o servidor de aplicaciones que solicita hasta que la sesión es finalizada por él mismo o por el IVE.

4.3 Configuración adicional de los servicios de red

Más allá de las obvias tareas de configuración del equipo y del servidor LDAP, cualquier cambio en la RC de la GVA lleva una serie de tareas complementarias asociadas necesarias para la puesta en marcha del servicio.

Cada vez que se añade un servicio a la RC hay que publicarlo. Como se comentó en el capítulo anterior la RC de la GVA dispone de dos ISP por lo tanto, se han tenido que dar de alta en los servidores DNS las IPs del nuevo concentrador.

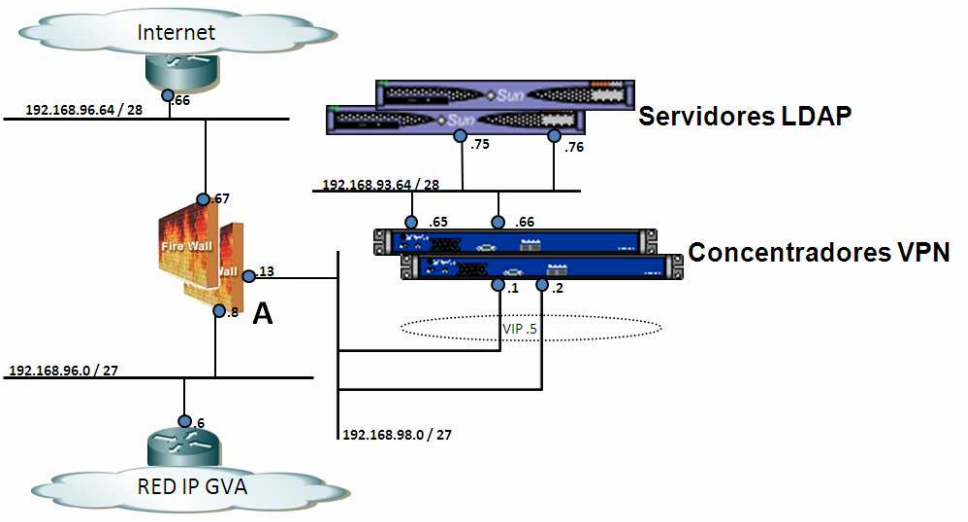


Figura 4.3: Detalle de la topología del servicio VPN de la GVA.

También se ha tenido que dar los permisos pertinentes en los cortafuegos para que las conexiones puedan cruzarlos y entrar en la RC. El servidor LDAP también deberá ser dado de alta en los cortafuego para que las conexiones puedan entrar y salir de él.

4.4 Resumen

En este capítulo hemos visto los pasos que se siguieron para dejar el servicio en funcionamiento.

Primero se instaló y configuró el servidor LDAP; a continuación se configuró el concentrador de túneles y se terminó realizando las tareas necesarias para que el servicio pudiera ser utilizado en la RC.

Capítulo 5. Resultados y Conclusiones

5.1Revisión de objetivos

Lo primero que haremos en este capítulo es valorar en qué medida se han cubierto los objetivos iniciales de este proyecto:

- Se ha analizado la tecnología de la que se disponía hasta ahora.
- Se han visto las alternativas tecnológicas de las que se disponía, tanto nuevas como las ya utilizadas.
- De entre los dispositivos actuales se ha elegido el que mejor se ajustaba a las necesidades de la GVA (Generalitat Valenciana).
- Se ha diseñado la nueva configuración.
- Se ha configurado y puesto en producción el nuevo dispositivo.
- Se ha documentado la migración del servicio con la redacción del presente proyecto.
- Se ha instaurado el nuevo sistema de modo trasparente para los usuarios.

5.2 Conclusiones

La finalidad principal de este proyecto era que el servicio de acceso remoto a la Red Corporativa (RC) de la GVA fuera actualizado de modo trasparente para sus usuarios, sin causarles molestias ni pérdidas del servicio.

Otro de los objetivos importantes era que el cambio aportara el mayor número de beneficios al funcionamiento de todo el sistema.

Las ventajas obtenidas con la nueva tecnología han redundado en un aprovechamiento mayor del tiempo de trabajo de los administradores del sistema en otras de sus labores, ya que el número de horas invertidas en la atención de incidencias generadas por problemas con el cliente ha

desaparecido casi en su totalidad. Y no sólo del tiempo de trabajo de estos trabajadores sino también el de los de atención primaria que se encuentran en el centro de atención telefónica.

Dando de alta a los nuevos usuarios en el servicio el tiempo también ha disminuido muy considerablemente, al igual que lo ha hecho en el usado para volcar la configuración de un concentrador al de respaldo.

El consumo de BW también ha disminuido.

5.3 Trabajo futuro

Varias son las tareas que vendrían a completar el proceso de migración.

Entre ellas se encuentra la actualización de los manuales de instalación del servicio para los usuarios. Hasta ahora el usuario final debía de instalar los certificados y el cliente, con la nueva tecnología el usuario, ya no tendrá que descargarse ni instalar el cliente; sólo tendrá que teclear un URL en su navegador.

También existe un documento utilizado por los técnicos de atención telefónica (Nivel 1) de la GVA que deberá de ser actualizado convenientemente en el mismo sentido.

Todos los servicios son monitorizados para poder detectar y localizar fallos en el sistema, caídas, etc. También para poder extraer estadísticas de las que poder sacar conclusiones. Por lo tanto, deberemos de añadir a nuestro sistema de monitorización (concretamente CACTI) las nuevas máquinas (concentradores y servidores LDAP).

Dar de alta las nuevas máquinas (características técnicas y físicas) en todos las bases de datos, esquemas de red, etc. en los que deben de constar. Informar a los distintos departamentos de su existencia para por ejemplo, tenerlas en cuenta cuando se lance la siguiente auditoría del sistema.

No podemos dejar de pensar en el trabajo propio del mantenimiento del servicio, como son: copias de seguridad, actualizaciones de aplicaciones y el obvio de añadir nuevos usuarios y grupos.

Y por supuesto, estar al tanto de las nuevas tecnologías y mejoras que puedan hacer que el sistema sea mejorado aún más.

5.4 Resumen

En este capítulo se han evaluado los resultados obtenidos en relación con los objetivos iniciales del proyecto. También se han planteado ciertas líneas de trabajo relacionadas con este proyecto que serían interesantes de desarrollar en un futuro. Estas líneas de actuación son importantes, pero no son críticas; se ha podido poner el servicio en producción sin que estuvieran completadas.

Capítulo 6.
Planificación temporal y presupuesto

6.1 Planificación temporal

El proyecto dispone de de un ingeniero que realizará todas las tareas en las que se divide el proyecto.

Hagamos una relación de las diferentes tareas que se han llevado a cabo durante la realización del proyecto.

- Documentación.
  - Búsqueda bibliográfica.
  - Revisión bibliográfica.

- Análisis de la arquitectura actual.
  - Tecnología utilizada.
  - Problemática.

- Análisis de los servicios a instalar.
  - Comparación de las dos tecnologías.
  - Elección tecnológica.
  - Comparación distintos equipos sustitutos.
  - Elección del nuevo dispositivo.

- Puesta en preproducción.
  - Instalación servidor LDAP.
  - Configuración del concentrador.

- Periodo de pruebas.

- Instalación física y puesta en marcha del equipo.
  - Configuración definitiva.
  - Configuración adicional de los servicios de red.
  - Puesta en producción.

- Periodo de funcionamiento del sistema.

- Evaluación de resultados.

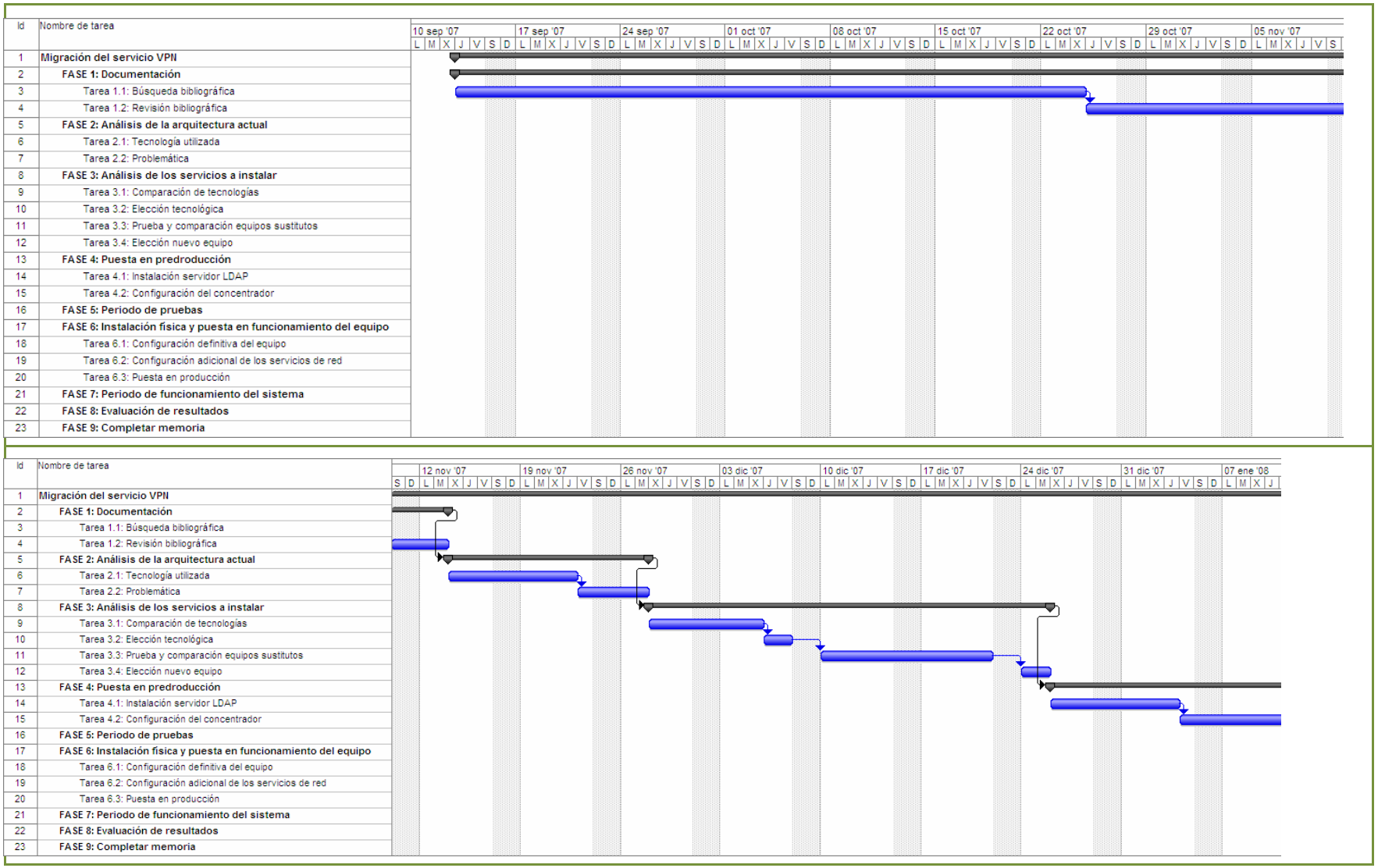
- Completar memoria.

En la tabla 6.1 podemos ver el orden y las dependencias temporales entre las tareas mencionadas anteriormente.

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Migración del servicio VPN**	**170 días**	**jue 13/09/07**	**mié 07/05/08**	
2	**FASE 1: Documentación**	**44 días**	**jue 13/09/07**	**mar 13/11/07**	
3	Tarea 1.1: Búsqueda bibliográfica	30 días	jue 13/09/07	mié 24/10/07	
4	Tarea 1.2: Revisión bibliográfica	14 días	jue 25/10/07	mar 13/11/07	3
5	**FASE 2: Análisis de la arquitectura actual**	**10 días**	**mié 14/11/07**	**mar 27/11/07**	**2**
6	Tarea 2.1: Tecnología utilizada	7 días	mié 14/11/07	jue 22/11/07	
7	Tarea 2.2: Problemática	3 días	vie 23/11/07	mar 27/11/07	6
8	**FASE 3: Análisis de los servicios a instalar**	**20 días**	**mié 28/11/07**	**mar 25/12/07**	**5**
9	Tarea 3.1: Comparación de tecnologías	6 días	mié 28/11/07	mié 05/12/07	
10	Tarea 3.2: Elección tecnológica	2 días	jue 06/12/07	vie 07/12/07	9
11	Tarea 3.3: Prueba y comparación equipos sustitutos	10 días	lun 10/12/07	vie 21/12/07	10
12	Tarea 3.4: Elección nuevo equipo	2 días	lun 24/12/07	mar 25/12/07	11
13	**FASE 4: Puesta en predroducción**	**17 días**	**mié 26/12/07**	**jue 17/01/08**	**8**
14	Tarea 4.1: Instalación servidor LDAP	7 días	mié 26/12/07	jue 03/01/08	
15	Tarea 4.2: Configuración del concentrador	10 días	vie 04/01/08	jue 17/01/08	14
16	**FASE 5: Periodo de pruebas**	9 días	vie 18/01/08	mié 30/01/08	13
17	**FASE 6: Instalación física y puesta en funcionamiento del equipo**	**15 días**	**jue 31/01/08**	**mié 20/02/08**	**16**
18	Tarea 6.1: Configuración definitiva del equipo	4 días	jue 31/01/08	mar 05/02/08	
19	Tarea 6.2: Configuración adicional de los servicios de red	8 días	mié 06/02/08	vie 15/02/08	18
20	Tarea 6.3: Puesta en producción	3 días	lun 18/02/08	mié 20/02/08	19
21	**FASE 7: Periodo de funcionamiento del sistema**	**22 días**	jue 21/02/08	vie 21/03/08	17
22	**FASE 8: Evaluación de resultados**	**10 días**	lun 24/03/08	vie 04/04/08	21
23	**FASE 9: Completar memoria**	**23 días**	lun 07/04/08	mié 07/05/08	22

Tabla 6.1: Orden y dependencias temporales de las tareas.

En la figura 6.1 vemos un diagrama de Gantt donde se muestra el coste temporal del proyecto, la duración de cada tarea y sus respectivas subtareas, así como las dependencias entre ellas.


Id
Nombre de tarea
1 Migración del servicio VPN
2 FASE 1: Documentación
3 Tarea 1.1: Búsqueda bibliográfica
4 Tarea 1.2: Revisión bibliográfica
5 FASE 2: Análisis de la arquitectura actual
6 Tarea 2.1: Tecnología utilizada
7 Tarea 2.2: Problemática
8 FASE 3: Análisis de los servicios a instalar
9 Tarea 3.1: Comparación de tecnologías
10 Tarea 3.2: Elección tecnológica
11 Tarea 3.3: Prueba y comparación equipos sustitutos
12 Tarea 3.4: Elección nuevo equipo
13 FASE 4: Puesta en predroducción
14 Tarea 4.1: Instalación servidor LDAP
15 Tarea 4.2: Configuración del concentrador
16 FASE 5: Periodo de pruebas
17 FASE 6: Instalación física y puesta en funcionamiento del equipo
18 Tarea 6.1: Configuración definitiva del equipo
19 Tarea 6.2: Configuración adicional de los servicios de red
20 Tarea 6.3: Puesta en producción
21 FASE 7: Periodo de funcionamiento del sistema
22 FASE 8: Evaluación de resultados
23 FASE 9: Completar memoria
10 sep '07
17 sep '07
24 sep '07
01 oct '07
08 oct '07
15 oct '07
22 oct '07
29 oct '07
05 nov '07
12 nov '07
19 nov '07
26 nov '07
03 dic '07
10 dic '07
17 dic '07
24 dic '07
31 dic '07
07 ene '08

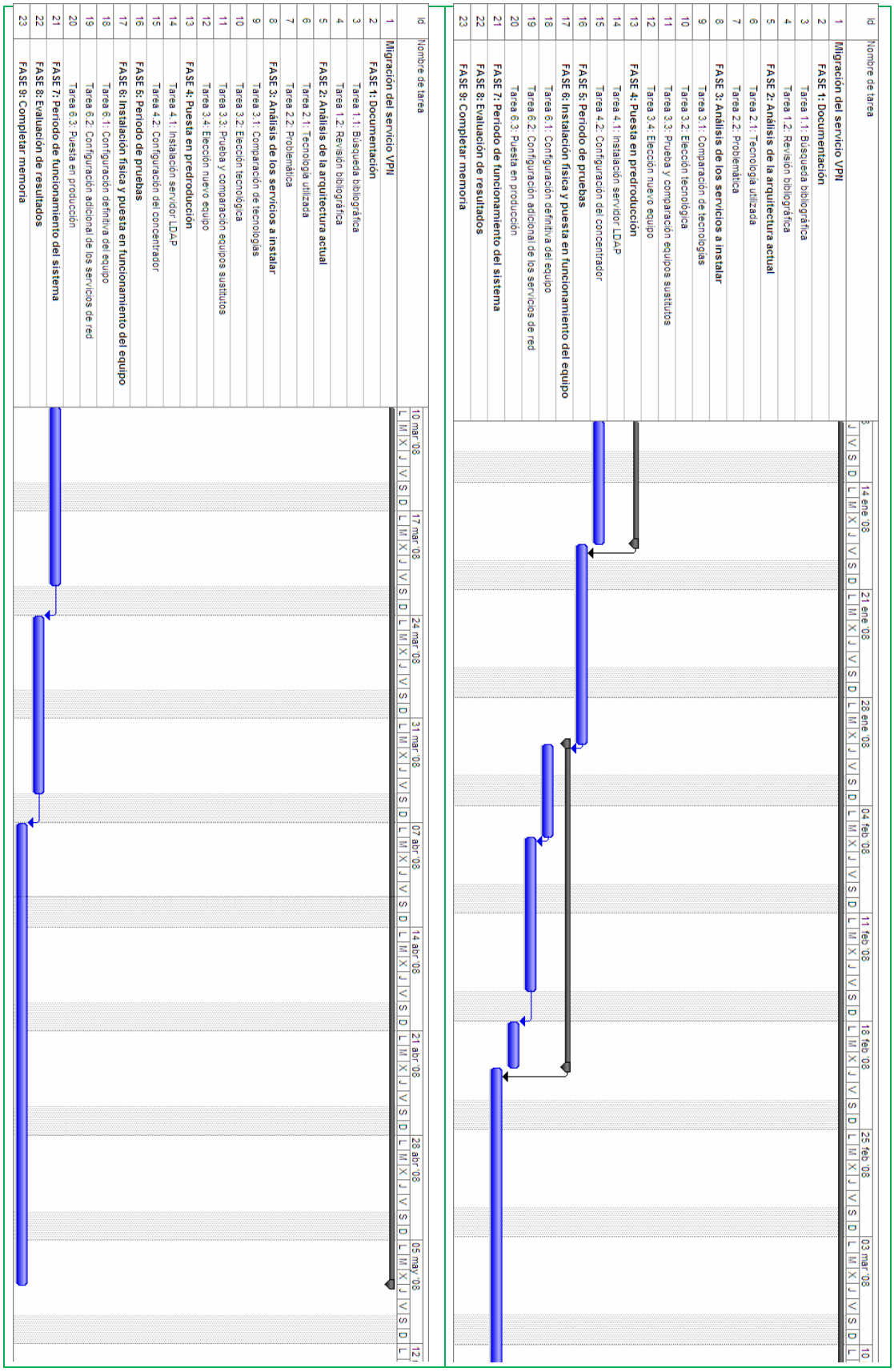


Figura 6.1: Diagrama de Gantt del proyecto.

6.2 Costes y presupuesto

Una vez calculado el coste temporal del proyecto vamos a calcular el coste económico que éste supondría.

El coste económico del proyecto vendrá asociado a dos conceptos:

- Coste material: este concepto incluye los costes tocantes a material *software* y *hardware* del que se dispone en la GVA, que va siendo amortizado. Para los dos supondremos una vida útil de 2 años.
  Aparte hemos de añadir el coste del propio concentrador que se va a adquirir, su software asociado y el mantenimiento propio de la marca. Además de un par de máquinas Sun donde se instalará el servidor LDAP (Activo/*Backup*).

- Coste humano: este concepto incluye las cuantías asociadas a recursos humanos. El coste de un recurso de este tipo viene dado por la experiencia del mismo y su cualificación profesional. En el caso que nos ocupa son las horas trabajadas por el Ingeniero que ha trabajado en el proyecto.

Para el cálculo de las cantidades imputables de amortización de equipos y software del proyecto hemos considerado que un año tiene 1595,4 horas de trabajo **[Ine]**, de este modo la amortización de:

- PC Intel Core 2 CPU a 1.4 GHz, RAM de 2 GB es de 1.200€/3.191 horas = 0,31 €/h.
- Sunfire V120, 2GB de RAM es de 980€/3191 horas = 0,31€/h.
- Sistema Operativo Windows XP Professional, es de: 120€/3191 horas =0,04 €/h.
- MS Office 2007 es de 140€/3191 horas= 0,04 €/h.
- MS Visio 2007 es de 110€/3191 horas= 0,03 €/h.
- MS Project 2007 es de 110€/3191 horas= 0,03 €/h.

Se ha considerado una jornada de 8 horas diarias de trabajo; por lo tanto, los 170 días que tiene de duración el proyecto hacen un total de 1.360 horas de trabajo.

Costes del Proyecto				
A. COSTES DE PERSONAL				
	CANTIDAD	**HORAS**	**COSTE/HR**	**COSTE**
Ingeniero	1	1360	30,00	40.800,00
			Subtotal A	**40.800,00**
B. COSTES MATERIAL				
B.1 HARDWARE	**CANTIDAD**	**HORAS**	**COSTE/HR**	**COSTE**
PC Pentium	1	1360	0,31	421,60
Sunfire v120	2	1360	0,31	843,20
B.2 SOFTWARE				
Windows XP	1	1360	0,04	54,40
M.S. Office 2007	1	1360	0,04	54,40
M.S. Visio 2007	1	1360	0,03	40,80
M.S. Project	1	1360	0,03	40,80
B.3 CONCENTRADOR	**CANTIDAD**		**COSTE Uni.**	**COSTE**
Juniper SA4000	2		3.600,00	7.200,00
Licencia para 250 users concurrentes	1		15.430,00	15.430,00
Licencia para compartir 250 users en *cluster*	1		9.770,00	9.770,00
Aplicaciones de seguridad y administración	1		4.640,00	4.640,00
Mantenimiento y soporte técnico Anual	1		7.825,00	7.825,00
			Subtotal B	**45.395,40**
1.C OTROS GASTOS				
	CANTIDAD		**COSTE Uni.**	**COSTE**
Viajes	1		110,00	110,00
			Subtotal C	110,00
			TOTAL	**86.305,40**

Tabla 6.2: Coste del Proyecto.

Los viajes son el traslado del ingeniero al centro de procesos de datos para la instalación física del concentrador y del servidor LDAP.

La parte de *software* que tiene que ver con las máquinas Sun no ha sido tenida en cuenta porque tanto el sistema operativo (Solaris 10) como el servidor LDAP (OpenLDAP) son de libre distribución.

6.3 Resumen

En el presente capítulo hemos hecho una planificación temporal de las tareas necesarias para la consecución del proyecto así como los costes hardware y software asociados al mismo.

El proyecto dispone de un ingeniero que será quien realizará todas las tareas.

Apéndice A
El informe Gartner

La Consultora Gartner es la empresa de consultoría tecnológica de mayor prestigio a nivel internacional.

En diciembre de 2006 publicó un informe **[Gart]** acerca de los servicios SSL VPN. La Figura A.1 muestra los resultados de este informe.

Ability to execute es en el eje de las ordenadas el criterio de evaluación. Este criterio, a grandes rasgos, hace referencia a la efectividad de las empresas para tener su producto vendido, instalado y en funcionamiento en casa del cliente. También se evalúa la relación producto/servicio, la experiencia de los clientes y el poder de cuota de mercado de las empresas.

En el eje de las abscisas encontramos ***Completeness of visión***, este criterio de evaluación hace referencia a cómo la empresa plantea la estrategia de ventas, estrategia de mercado, la estrategia del producto, el modelo de negocio y por supuesto la innovación de la mano de la investigación y el desarrollo.

En cuanto a la pertenencia a un cuadrante u otro, de forma muy resumida, los ***Leaders*** son aquellos que destacan en todos los criterios de visión y ejecución, para mantenerse en este cuadrante estas empresas tienen que ser entre otras cosas líderes en ventas y destacar en acceso móvil y seguridad. Según Gartner "Los líderes son capaces de equilibrar esfuerzo y progreso en todos los aspectos relacionados con visión y ejecución. Sus acciones elevan el listón competitivo para todos los productos del mercado, y son capaces de cambiar el curso de la industria. Para mantenerse en el cuadrante de líderes, los proveedores deben sobresalir en el acceso y protección en movilidad, así como dominar en el aspecto comercial".

Los ***Challengers*** tienen productos sólidos que resuelven las necesidades básicas del mercado con unas fuertes ventas. Son buenos ganando contratos pero compiten en un sector limitado. Son eficientes para problemas específicos, en general se les considera la alternativa conservadora y segura de los *Niche players*.

Los ***Visionaries*** invierten en la tecnología del futuro, la de la siguiente generación, dando a sus clientes un rápido acceso a esta tecnología futura. Pueden influir en el desarrollo de la tecnología en el mercado pero carecen de la *ability to execute* que les haga mejores estrategas que *challengers* o *leaders.*

Los ***Niche players*** ofrecen soluciones para los necesidades típicas de los usuarios. Responden a los cambios en el mercado, no son

capaces de cambiar el curso de la industria. Sirven a clientes conservadores más eficientemente que los *leaders*. Estos clientes buscan estabilidad y centrarse en unas pocas e importantes características.

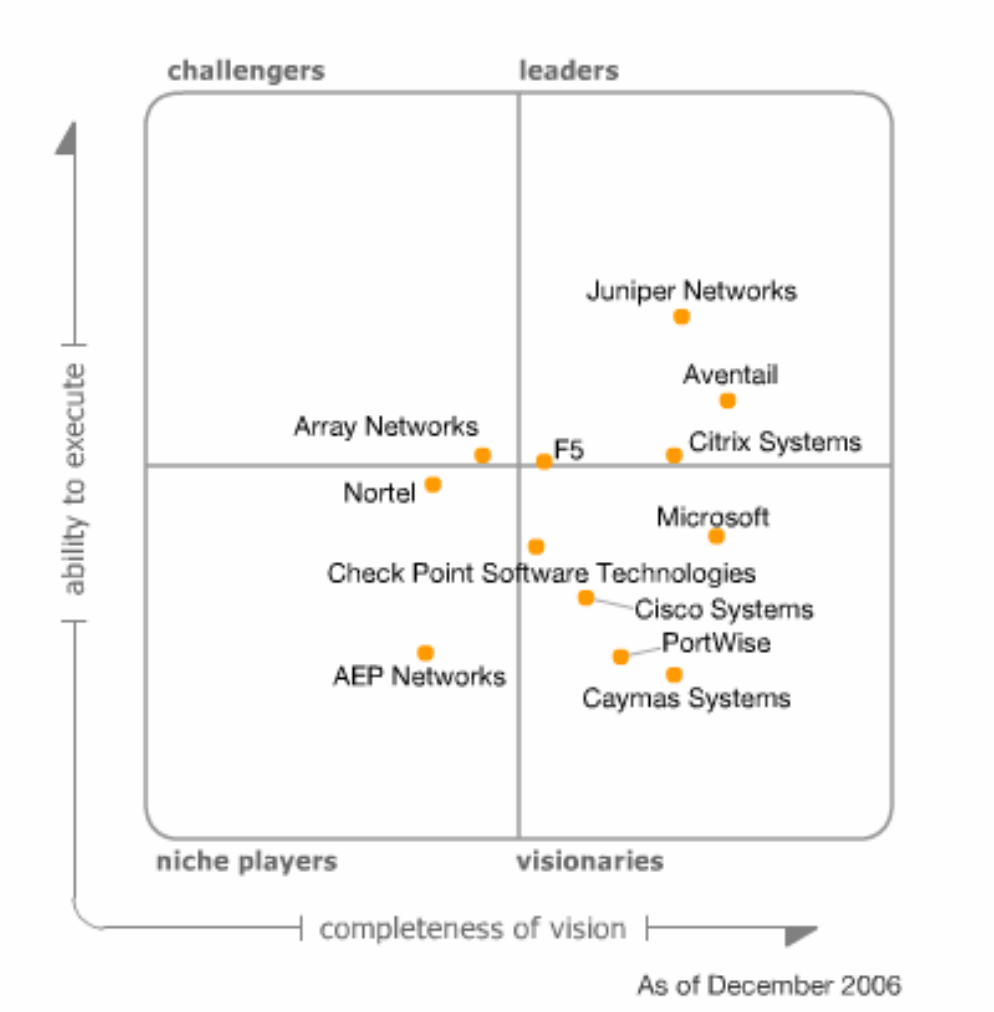


Figura A.1: Informe Gartner [Gart].

En base al informe de la consultoría Gartner que recomienda como punteros en este terreno a Juniper y Aventail se pidió a ambas empresas que hicieran sendas presentaciones de sus productos y que permitieran a la GVA las pruebas con las máquinas.

Después de haber estado configurando e integrando ambos sistemas dentro de nuestro entorno de trabajo pensamos que la que mejor se adaptaba a nuestras necesidades era la oferta de Juniper. La razón fundamental se basaba en la alta compatibilidad con nuestros sistemas de autorización de certificados digitales.

Apéndice B
Configuración del Cisco VPN 3060

Es la máquina usada hasta ahora. Se verá una pequeña descripción tanto de su configuración como de los pasos a dar por parte tanto del usuario como del administrador para poder dar un alta en el servicio.

Se expondrá también la problemática asociada tanto a nivel tecnológico, como pueda ser el límite físico del buffer donde se aloja la Lista de Certificados Revocados (CRL), como a nivel de mantenimiento e instalación

B.1 Proceso de alta en el servicio

Veamos como el alta de un usuario en el servicio implica tanto al administrador como al propio usuario. Ambos deberán de llevar a cabo una serie de tareas.

B.1.1 Por parte del usuario

Cuando un usuario quiere comenzar a usar el servicio de Virtual Private Network (VPN) el servicio de comunicaciones le informa de los pasos a seguir que son los siguientes:

1. Obtención del certificado digital expedido por la Autoridad de Certificación de la Comunidad Valenciana (ACCV) e instalación del mismo en el ordenador desde el que se vaya a cerrar el túnel VPN.

   En ese equipo además del certificado del usuario que vaya a usar el servicio también habrán de instalarse los certificados propios de la ACCV.
2. Una vez instalados los certificados (personal y ACCV) en el ordenador, el nuevo usuario necesitará descargar e instalar el software de conexión VPN. El llamado cliente VPN. La versión actual del cliente es la v.4.8.01.0300
3. A continuación debe de rellenar el formulario de “Solicitud de Alta” y enviarlo al servicio de comunicaciones de la GVA.
4. Una vez confirmada el alta en el servicio el usuario puede comenzar a hacer uso del mismo.

B.1.2 Por parte de los administradores

La asignación de los distintos usuarios a un grupo u otro tiene dos niveles:

- Un primer nivel donde se comprueba que el usuario que está accediendo posee el certificado de la ACCV pasando a formar parte del grupo de usuarios con certificado ACCV.
- Un segundo nivel en el que, cumpliendo el anterior requisito, le será asignado su grupo definitivo.

En el siguiente fragmento de código del *log* de RADIUS podemos observar estos dos niveles y el detalle de los requisitos que se cumplen en cada nivel. También podemos ver otro tipo de información que guarda el fichero:

15950 03/27/2008 16:28:44.580 SEV=5 IKE/79 RPT=41804 89.23.222.223
Group (PFC)
Validation of certificate successful
(CN=JOSE IGNACIO FERRERO SANZ - NIF:25557759G, SN=B9D4F3AA0415D8)

15953 03/27/2008 16:28:44.930 SEV=4 IKE/52 RPT=38096 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G) authenticated.

15955 03/27/2008 16:28:45.070 SEV=5 IKE/184 RPT=37275 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
Client Type: WinNT
Client Application Version: 4.8.02.0010

15957 03/27/2008 16:28:46.010 SEV=4 IKE/119 RPT=37567 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
PHASE 1 COMPLETED

15960 03/27/2008 16:28:46.020 SEV=5 IKE/25 RPT=39420 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
Received remote Proxy Host data in ID Payload:
Address 172.31.3.52, Protocol 0, Port 0

15966 03/27/2008 16:28:46.020 SEV=5 IKE/66 RPT=40829 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
IKE Remote Peer configured for SA: VPN_Con_Certificado

15970 03/27/2008 16:28:46.100 SEV=4 IKE/173 RPT=34246 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
NAT-Traversal successfully negotiated!
IPSec traffic will be encapsulated to pass through NAT devices.

15976 03/27/2008 16:28:46.100 SEV=4 IKE/120 RPT=44513 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)

PHASE 2 COMPLETED
15999 03/27/2008 16:32:54.530 SEV=5 IKE/50 RPT=35502 89.23.222.223
Group (PFC) User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G)
Connection terminated for peer JOSE IGNACIO FERRERO SANZ - NIF:25557759G.
Reason: Peer Terminate

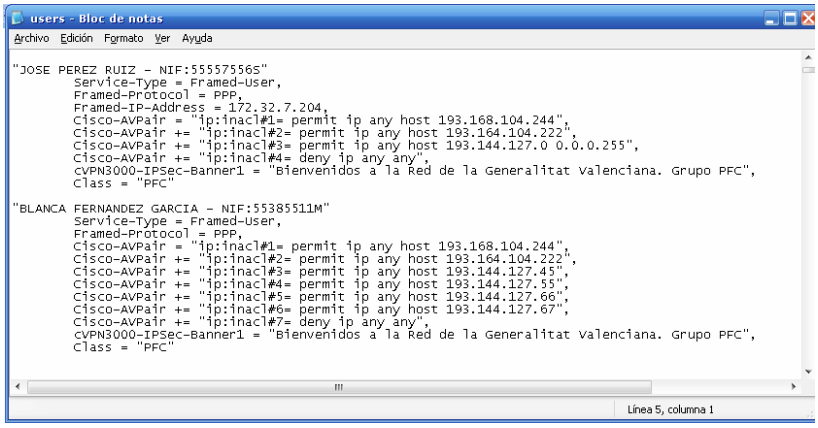
16004 03/27/2008 16:32:54.550 SEV=4 AUTH/28 RPT=37680 89.23.222.223
User (JOSE IGNACIO FERRERO SANZ - NIF:25557759G) Group (PFC) disconnected:
Session Type: IPSec/NAT-T
Duration: 0:04:08
Bytes xmt: 73072
Bytes rcv: 49224
Reason: User Requested

Creación de grupos

Los pasos más importantes en la creación de los grupos que darán a posteriori los permisos para los distintos accesos son:

1. Creación del grupo nuevo.
2. Asignación de un rango de direcciones IP a ese grupo (*pool*).
3. Creación de la *Network List*[6] asociada a ese grupo.
4. Elección del cifrado de la información.
5. Finalmente mediante la edición del fichero users.txt de RADIUS se intenta ajustar el perfil del usuario.

Lo primero que se han de plantear los administradores del sistema de acceso VPN es si el usuario que demanda el servicio mediante el formulario posee realmente el certificado digital expedido por la ACCV. Aunque los futuros usuarios del servicio reciben información detallada del proceso de alta el caso de los que demandan el acceso al servicio sin el preceptivo certificado no es una situación anormal. Esta comprobación se lleva a cabo consultando la base de datos de la ACCV en busca de ese usuario.



[6] *Network List*: es el listado de direcciones IP a las que puede acceder un grupo.

Figura B.1: Contenido de users.txt de RADIUS.

En caso afirmativo hay que analizar de qué tipo de usuario se trata. Si es un usuario de un grupo ya existente cabe la posibilidad de que el grupo en cuestión use IPs dentro de un rango específico de modo dinámico o que también usando IPs dentro de un rango estas sean asignadas unívocamente. Como se puede ver en la figura B.1 se configura el archivo users.txt de RADIUS del modo pertinente.

Evidentemente estas acciones llevan asociadas unas comprobaciones de tamaño de los *pools*[7] de direcciones IP para evitar su desbordamiento.

En la figura B.1 se puede ver como el usuario Blanca Fernández tiene una asignación de IP dinámica (de entre las del *pool* de su grupo).

En cambio, José Pérez tiene una IP fija del *pool* de su grupo. El resto del contenido del archivo *users.txt* irá siendo comentado a lo largo de este capítulo.

En la figura B.2 podemos ver como se asigna un rango (pool) de direcciones a un grupo.

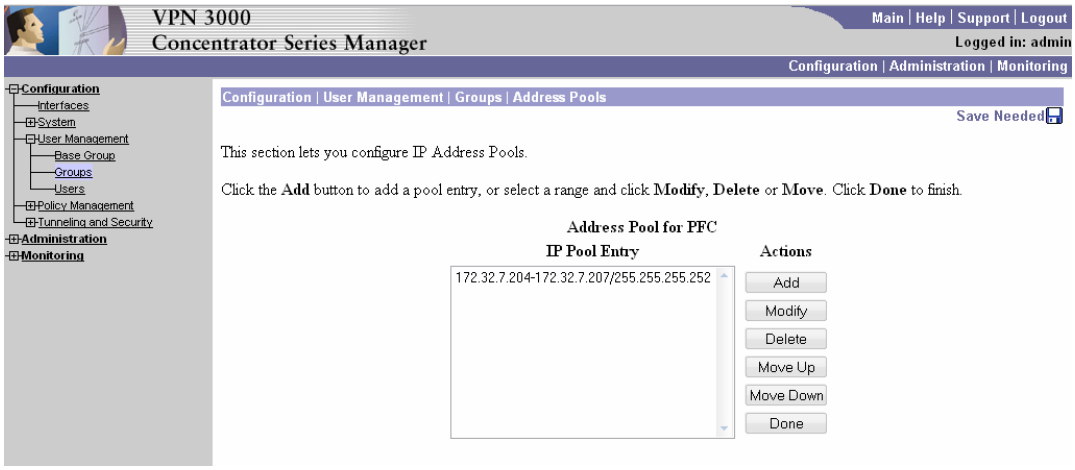


Figura B.2: Asignación de un *pool* de direcciones a un grupo en el concentrador Cisco.

En el caso de que no exista el grupo al que debe de pertenecer el nuevo usuario habrá de ser creado siguiendo los siguientes pasos:

1. Asignar un rango de direcciones IP al nuevo grupo. Figura B.2.

2. Dar los direccionamientos IP a los que podrá acceder este grupo (*Network List*). En la figura B.3 se pude observar como se ha creado una *Network List* con tres direcciones IP. Se usa

[7] *Pool* de direcciones: rango de direcciones asignadas previamente para un grupo.

wildcard[8]. En la figura vemos como esta *Network List* da acceso al grupo PFC a dos direcciones únicas que son la 193.168.104.244 y la 193.168.104.222 y al rango de direcciones de la 193.144.127.0 a la 193.144.127.255.

Figura B.3: Elección del cifrado de la información para la comunicación en el concentrador Cisco.

3. El tipo de cifrado lo seleccionamos de una serie de opciones que nos da el concentrador Cisco como se vio en el Estado del Arte. En la figura B.3 vemos como la Seguridad Asociada a IPSec es el grupo VPN_Con_Certificado además de exigir la validación con certificado.
   En la figura B.4 podemos observar cuáles son los algoritmos de certificado que componen el perfil de VPN_Con_Certificado, tanto para IPSec como para IKE.

En la figura B.3 se ve como la Seguridad Asociada a IPSec es el grupo VPN_Con_Certificado, además de exigir la validación con certificado.

[8] *Wildcard*: Las máscaras de *wildcard* usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas.

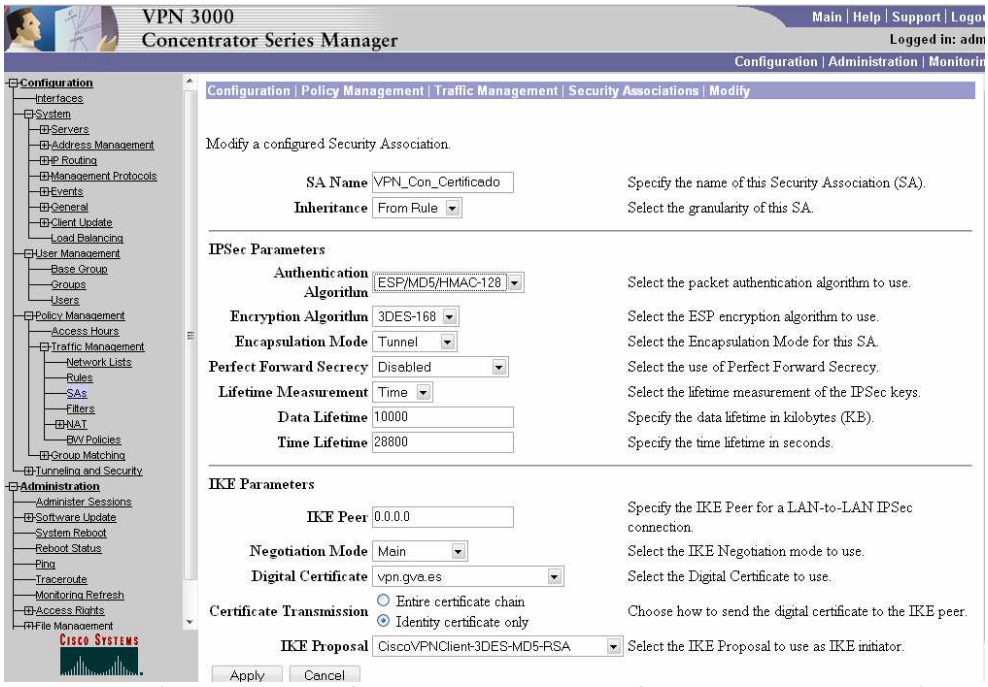


Figura B.4: Contenido de la Seguridad Asociada a IPSec en el concentrador Cisco.

Se puede ver el contenido del tipo Seguridad Asociada a IPSec a nivel del propio IPSec y de los parámetros para IKE.

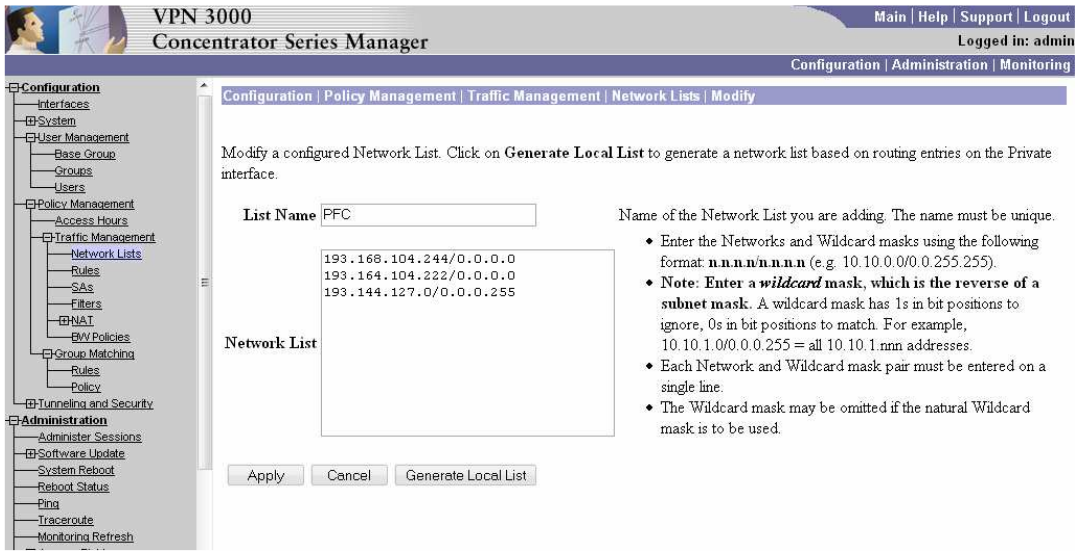


Figura B.5: Creación de Network List para un grupo en el concentrador Cisco.

1. Mediante la edición individualizada de cada usuario en *users.txt* configurar el tipo de acceso al servicio. Podemos ver un ejemplo en el apartado C1.2.

Llegados a este punto ya podemos crear el grupo propiamente dicho y darle las características que le hemos preparado.

En la figura B.6 vemos como bautizamos al nuevo grupo. En este caso de ejemplo el nombre elegido es PFC. A la derecha hay un botón con el que editaremos el *pool* de direcciones asociado al grupo como se ha visto en la figura B.2.

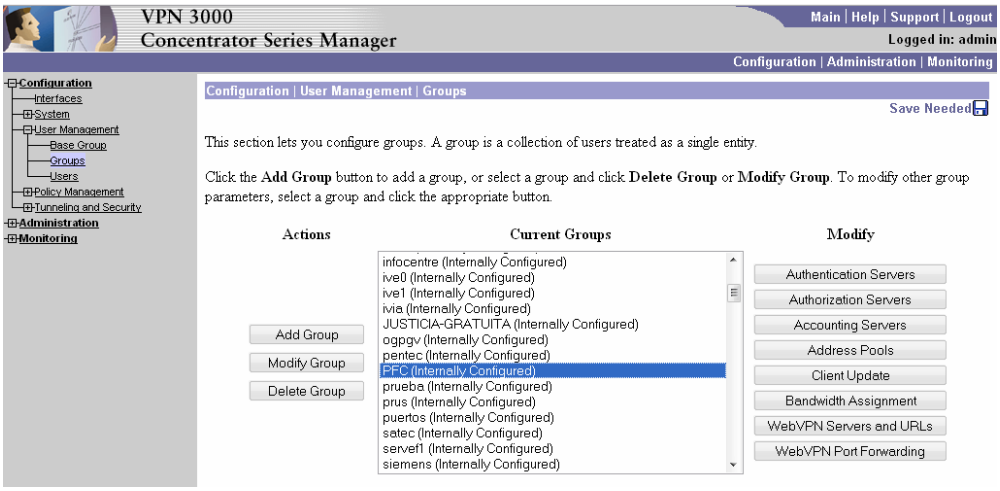


Figura B.6: Asignación de nombre al nuevo grupo en el concentrador Cisco.

Pasamos a editar las características generales del grupo PFC. En la figura B.7 podemos ver como se le dice cuáles serán sus servidores DNS y el protocolo que usarán que como ya es sabido será el IPSec.

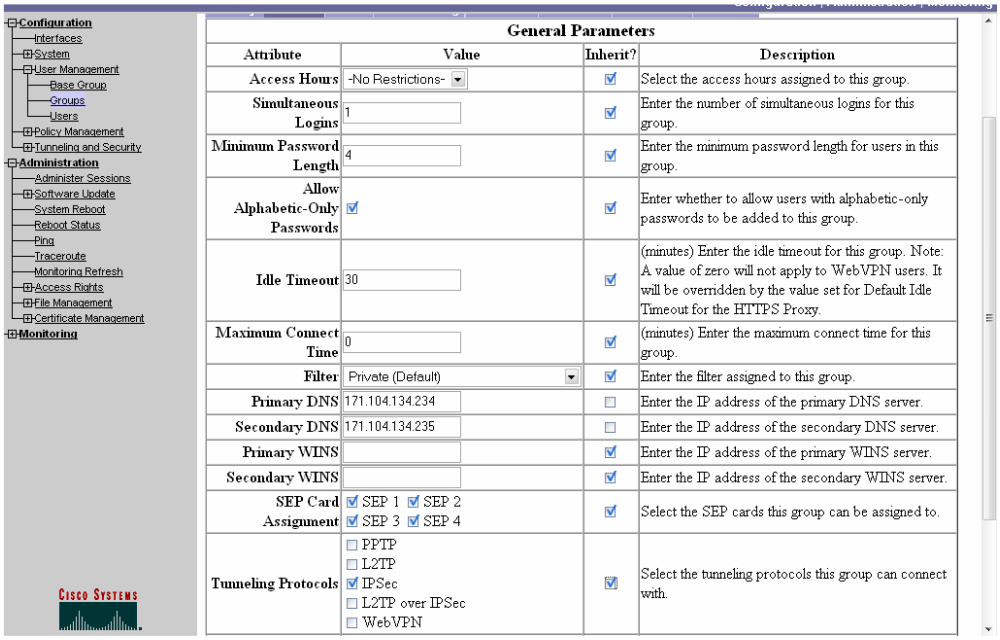


Figura B.7: Asignación de parámetros generales a un grupo.

Le decimos que el grupo sólo tunelizará las direcciones IP que hayan en su *Network List.*

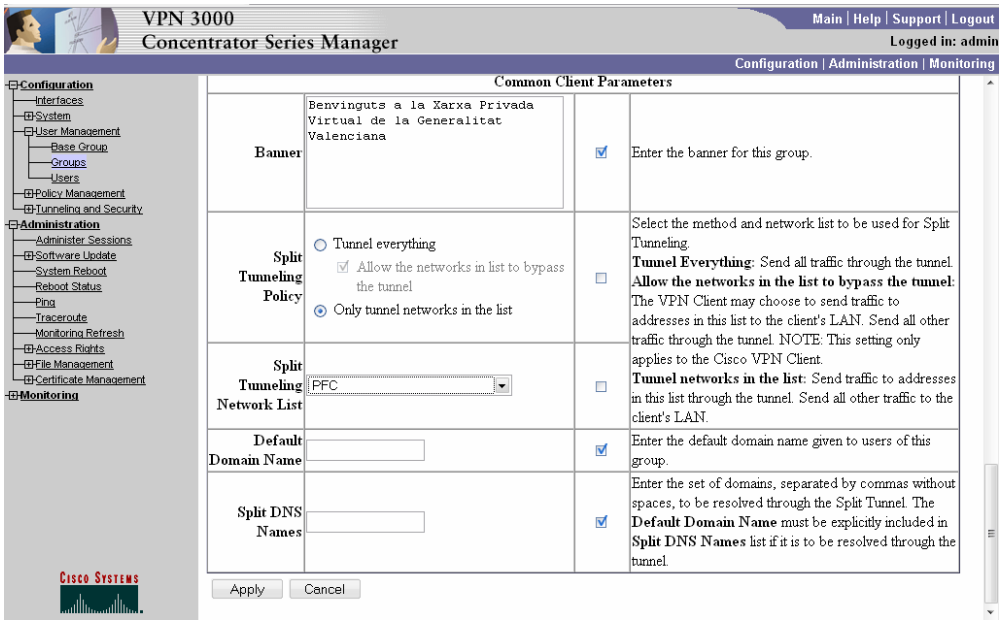


Figura B.8: Elección de la *Network List* para un grupo en el concentrador Cisco.

Retomando lo que se decía principio de este subapartado, con esta configuración le diremos al Cisco que use el servidor RADIUS como servidor de autenticación (Figura B.9) y será él quien nos devuelva el nombre definitivo del grupo al que pertenece el usuario.

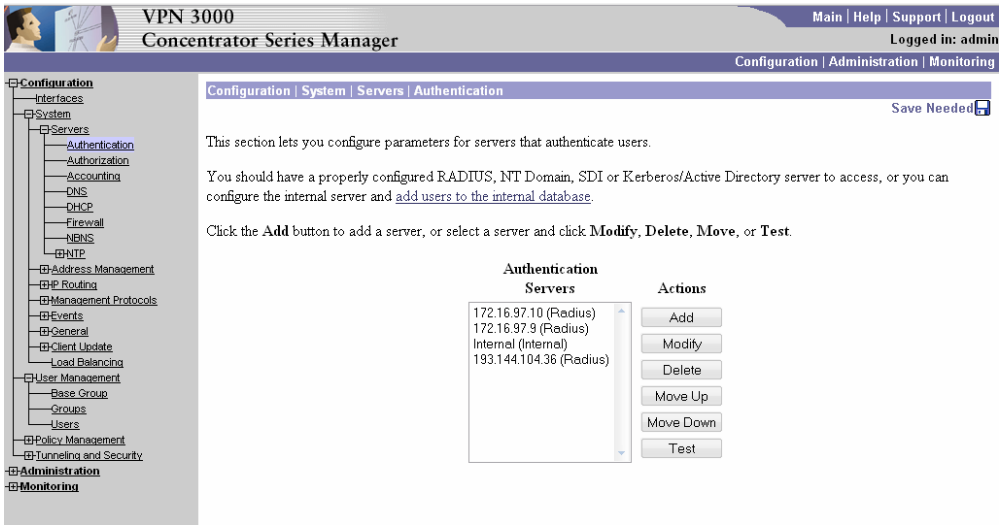


Figura B.9: Designación de RADIUS como servidor de autenticación en el concentrador Cisco.

B.2 Problemas con el cliente Cisco

Varios son los problemas que da el cliente VPN de Cisco. Actualmente está en uso la versión 4.8.01.0300

El primero y principal es el de la propia instalación del mismo. Aunque a los futuros usuarios del servicio se les da un exhaustivo documento para la configuración del mismo, el bajo o nulo conocimiento informático básico de algunos de estos usuarios VPN hace que esta tarea sea complicada haciendo que la GVA gaste unos recursos en esta actividad sin poder aplicarlos en otras vertientes.

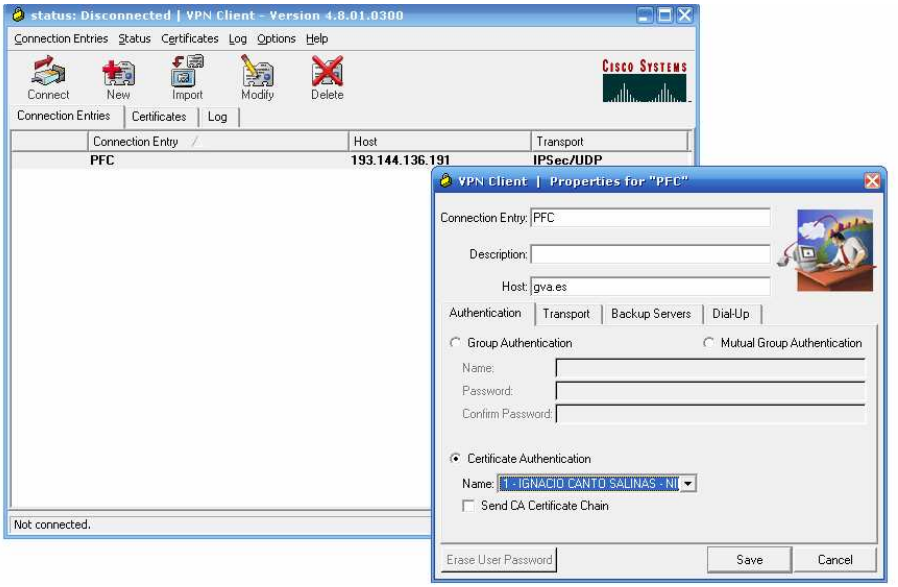


Figura B.10: Cliente VPN Cisco.

Otro de los problemas que se ha detectado es que, cuando uno de los usuarios deja de usar el cliente su sesión queda abierta más allá de que la aplicación Cliente sea cerrada con el peligro que supone que otro usuario de ese mismo equipo pueda suplantar la personalidad del usuario anterior. Para resolver este problema no queda otra solución que matar el proceso cliente desde el Administrador de Tareas del propio Windows.

La proliferación de distintos sistemas operativos hace que no todos los usuarios dispongan de un sistema operativo Windows en su ordenador. Este es otro de los problemas con los que se encuentra el cliente de Cisco; al estar seriamente atado a los sistemas Windows hace que el intento de su uso en otros sistemas operativos sea bastante conflictivo y cuanto menos hace muy complicada su configuración. Hay que parchear el núcleo del sistema operativo lo que, evidentemente, no es tarea fácil y menos aún para usuarios del tipo con los que se trata en la GVA para los cuales es misión imposible.

B.3 Problemas con las CLRs

La lista de certificados revocados es una lista donde se recogen todos los certificados de la AC dados de baja por caducidad aún estando temporalmente vigentes por problemas varios y por tanto cualquier firma emitida con posterioridad a la revocación no tiene validez o los revocados. Este documento también es firmado por la propia AC.

Cuando un tercero desea comprobar la validez de un certificado debe descargar una CRL actualizada desde los servidores de la misma AC que emitió el certificado en cuestión. A continuación comprueba la autenticidad de la lista gracias a la firma digital de la AC. Después debe comprobar que el número de serie del certificado cuestionado está en la lista. En caso afirmativo no se debe aceptar el certificado como válido.

Estrictamente hablando no es necesario descargar una CRL cada vez que se verifica un certificado. Solamente es necesario cuando no se dispone de la CRL de una entidad de certificación concreta y cuando dicha lista tiene una cierta antigüedad que aconseja su renovación.

La única ventaja de las CRL es que se pueden consultar sin necesidad de una conexión de datos permanente con cada AC. Basta establecer dicha conexión con cierta periodicidad para descargar las CRL actualizadas.

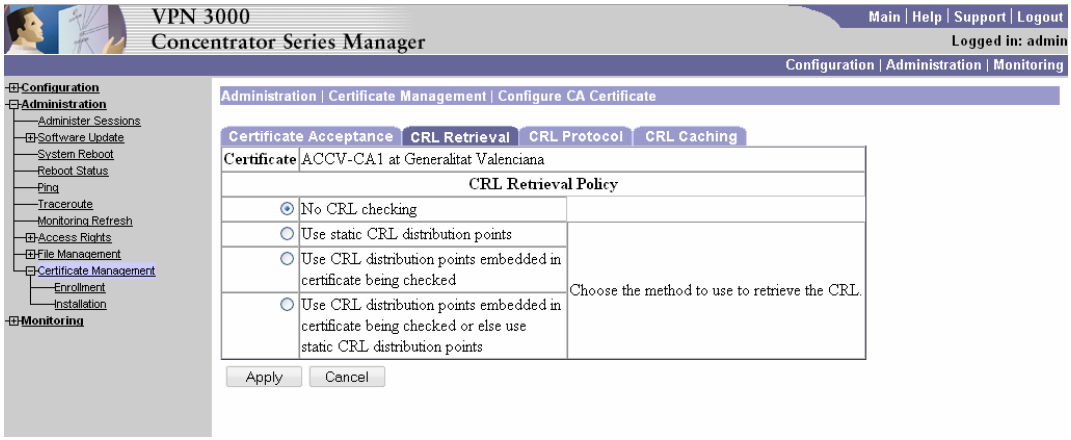


Figura B.11: Configuración del tipo de obtención de la CRL en el concentrador Cisco.

La búsqueda en la CRL es de modo secuencial. Si el registro buscado está al principio de la lista el tiempo de búsqueda es mínimo pero, si el registro está en la parte final de la lista el tiempo de consulta es considerable.

El problema que existe en el Cisco VPN 3060 es que a día de hoy los tamaños de las CRLs son tales que no caben en el buffer reservado para ellas en el dispositivo; el tamaño actual de la CRL de la ACCV es de 1.5MB y el tamaño del buffer es de 1MB.

B.4 Problemas con los grupos

El tema de los grupos es un tanto delicado. Para la administración del servicio se crean una serie de grupos a los que pertenecen unos usuarios. Conviene recordar que cuando se habla de grupos nos referimos a unos usuarios con permisos para acceder a una serie de máquinas (*network list*). Al ser una visión más general el caso de los grupos conlleva una serie de problemáticas:

- ✓ Podemos encontrarnos el caso de que trabajadores de una misma empresa, perteneciendo al mismo grupo, no accedan al mismo número de servicios o máquinas, es decir, pueden tener una serie de máquinas en común en su *network list* pero otras que no sean accedidas más que por un número reducido de usuarios de ese grupo.
- ✓ También puede darse el caso de usuario pertenezca a más de un grupo.

Una solución sería crear un grupo nuevo para este usuario, pero claro, esta solución no es nada práctica y conlleva un esfuerzo extra por parte de los administradores del sistema que no es asumible.

La solución de este problema no es otra que la necesidad por parte del administrador del sistema de ampliar uno de los grupos con el *network list* del otro grupo para que este usuario pueda tener acceso, tanto a las máquinas y servicios de un grupo, como de otro.

Es a nivel individual y mediante el contenido del fichero users.txt de RADIUS donde se acaban de dar los permisos necesarios a cada usuario, es decir, donde se darán los permisos finales para que dentro de su *network list* el usuario en particular pueda acceder a unas máquinas determinadas.

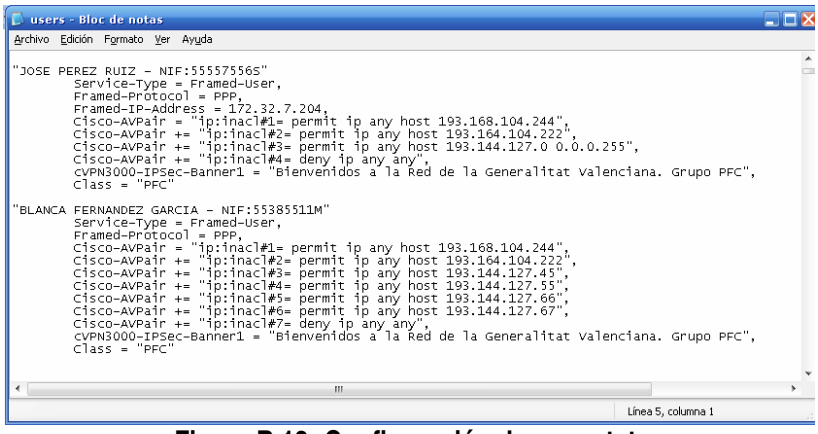


Figura B.12: Configuración de users.txt.

En la Figura B.12 se puede observar como el usuario Jose Pérez tiene acceso a toda la *network list* de su grupo. En cambio Blanca Fernández sólo tiene acceso a las dos primeras máquinas de la network list y de toda la red 193.144.127.0/24 únicamente a cuatro de ellas.

Modelar cada usuario editando su perfil en el archivo users.txt es una tarea ardua y pesada. El número de usuarios del servicio VPN no deja de crecer y sólo esta tarea podría ocupar el horario casi completo de un trabajador del servicio de comunicaciones. En la medida de lo posible debe de ser automatizado o simplificado al máximo.

B.5 Problema de alta disponibilidad, copia configuración

Cuando se actualiza la configuración del equipo (se da de alta un usuario, un grupo, etc.) existe un problema importante y es que no se puede volcar la información sobre el equipo de respaldo de modo inmediato y seguro. Obligatoriamente se ha de seguir un procedimiento de copia manual con el riesgo y consumo de recurso que ello conlleva.

B.6 El problema del final de vida del equipo

Este ha sido el problema que ha originado el cambio de equipo, tecnología y a la postre el presente proyecto final de carrera.

Apéndice C
Configuración del servidor LDAP

Uno de los requisitos de la implantación del nuevo dispositivo es la instalación de un servidor LDAP. La estructura del mismo la hemos visto en el Capítulo 4. Veamos a continuación la implementación en detalle.

Una vez descargada la última versión del LDAP de *http://www.OpenLDAP.org/software/download/* la descomprimimos, compilamos e instalamos siguiendo el proceso habitual en los sistemas Unix

Procedemos ahora a configurar el fichero de configuracion del OpenLDAP, que es */usr/local/etc/OpenLDAP/slapd.conf*. Este fichero está estructurado en dos partes: una primera con las opciones globales del OpenLDAP y otra con las definiciones de cada directorio que queramos tener.

```
#inclusión de los esquemas de los que hemos hablado con
anterioridad en el Capítulo 4
include         /usr/local/etc/OpenLDAP/schema/core.schema
include         /usr/local/etc/OpenLDAP/schema/cosine.schema

#Los siguientes valores indican la ruta de los pid y los
argumentos
pidfile         /var/run/slapd.pid
argsfile        /var/run/slapd.args

# permisos para nuestra base de datos
access to attr=userpassword
    by self write
    by * read

access to *
    by self write
    by dn=".+" read
    by * read


#Aquí comienza la definición de los directorios.
# Con esto definimos, a parte del inicio de la configuración de la
#base de datos, el tipo de base de datos que queremos usar. Lo
normal #es usar ldbm, pero otras opciones son passwd y shell.
database ldbm
```

```
# Sufijo o raíz del directorio. Es el nodo raiz superior
# de nuestro directorio ldap es decir accv.es
suffix "dc=accv, dc=es"

# Definimos el DN del administrador
rootdn "cn=administrador, dc=accv, dc=es"

# contraseña del administrador de LDAP, normalmente encriptada.
rootpw secret

# Aqui es donde se guardarán los datos del directorio
directory /var/lib/ldap
```

Llegados a este punto podemos lanzar el demonio del servidor LDAP.

Sólo nos resta comenzar a añadir datos al directorio. Todo el intercambio de datos con LDAP se hace con unos ficheros con un formato especial. Este formato es el LDIF (LDAP interchange format). Llamaremos al fichero *pfc* y tendrá la extensión *.ldif*.

```
####################################
dn: dc=accv,dc=es
objectclass: dcObject
objectclass: organizacion
o: accv

dn: cn=administrador,dc=accv,dc=es
objectclass: organizationalRole
cn: administrador
####################################
```

Lo añadiremos al directorio con el comando siguiente que nos pedirá la clave del administrador:

```
$ ldapadd -x -D "cn= administrador,dc=accv,dc=es" -W -f pfc.ldif
```

Una vez hecho esto ya podemos añadir el resto de datos al LDAP.

Como se ha comentado en el Capítulo 4 se ha hecho un *script* que nos transforma los usuarios de Radius en ficheros *.ldif* para poder ir añadiendo datos a nuestro nuevo LDAP del modo más automatizado posible y poder reutilizar la información que ya teníamos de Radius en el nuevo LDAP. El código del script no se muestra por motivos de seguridad.

Apéndice D
Configuración del Juniper SA4000

Comenzaremos a configurar el equipo. Los conceptos que usa Juniper se alejan bastante de la concepción del Cisco. La aplicación que maneja el dispositivo se llama IVE (Instant Virtual Extranet).

Este apartado no pretende ser un manual [**Manual**], sino una explicación de cómo se ha configurado el equipo.

Veremos a continuación:

- Definición del rol de usuario.
- Definición de los perfiles de recurso.
- Definición del servidor de autenticación. LDAP en nuestro caso.
- Definición de un dominio de autenticación.
- Definición de una política de inicio de sesión.

D.1 Definición del rol de usuario

En la figura D.1 vemos como se define el rol de usuario. Le asignamos un nombre y le decimos el tipo de acceso al que tendrá permiso; podemos elegir dar accesos a: web, archivos, telnet, etc. Cada uno de estos accesos se administra desde las pestañas que hay a continuación de la de *General.* En este caso editaremos la de *Web* que es el permiso que le vamos a dar a este usuario.

En la figura D.2 vemos como autorizamos al usuario a que escriba en la barra de direcciones de la aplicación.

Llegados a este punto ya hemos definido un rol de usuario que, recordemos, podrá únicamente de momento navegar por la web.

A continuación cuando creemos un perfil de recurso se lo podremos aplicar a este rol de usuario, también podremos asignar usuarios a este rol mediante reglas de mapeo que veremos en los dominios de autenticación.

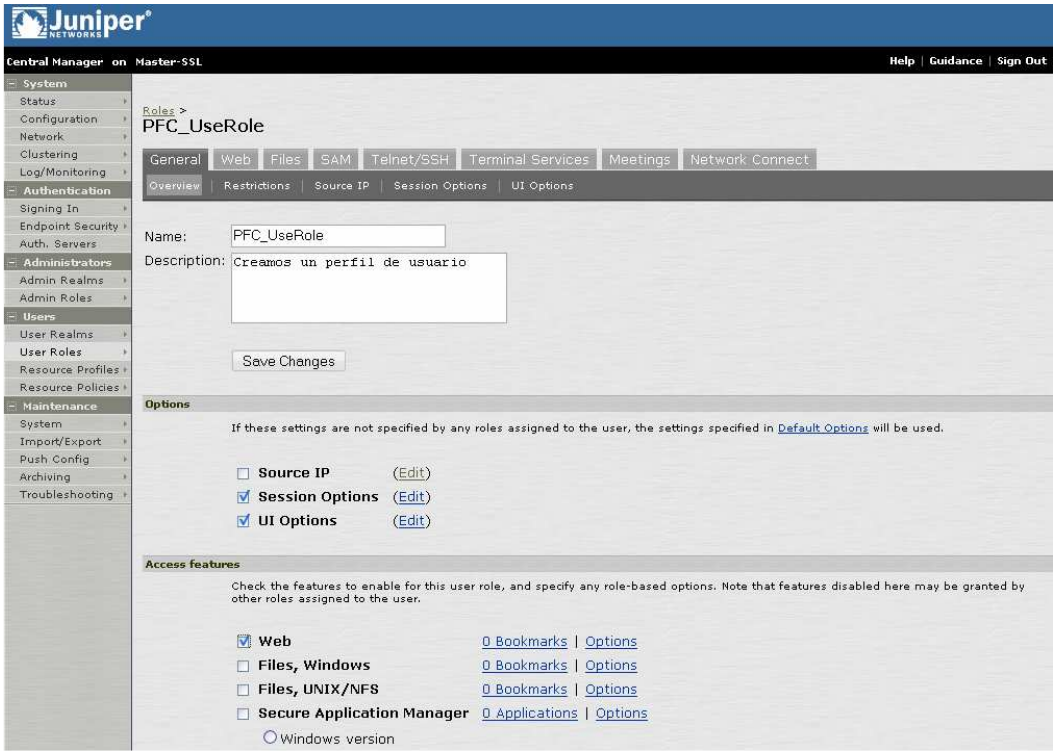


Figura D.1: Definición del rol de usuario en el concentrador Juniper.

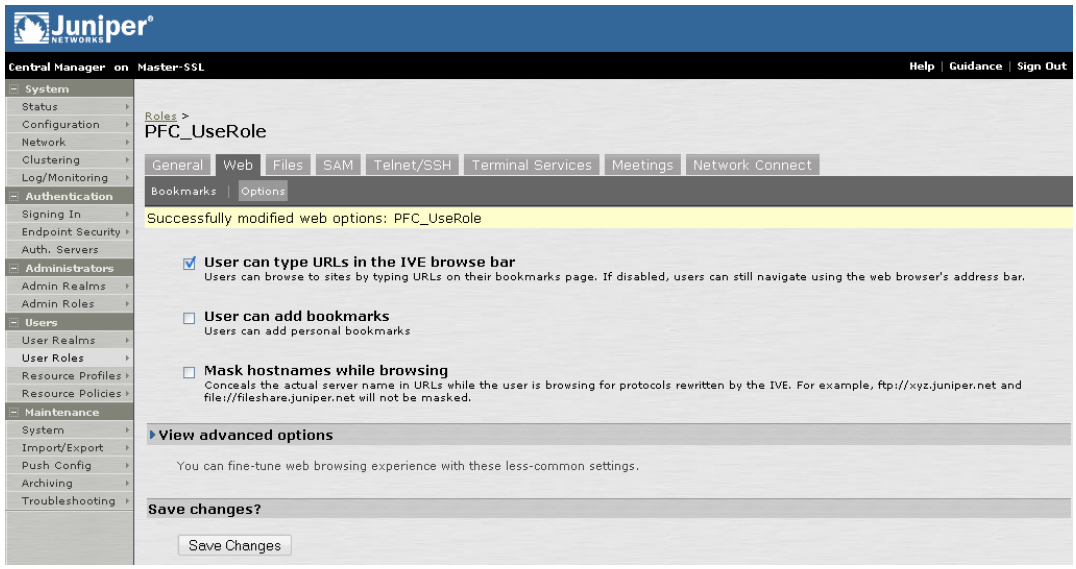


Figura D.2: Autorizaciones otorgadas al rol de usurio en el concentrador Juniper.

D.2 Definición del perfil de recurso

Pasemos a crear un perfil de recurso. Un perfil de recursos es un conjunto de opciones de configuración que contiene:

- política del recurso: que especifica los recursos a los que se aplicarán las políticas (como URLs, servidores, archivos) y si el IVE ha de ejecutar alguna acción.
- asignación de roles.
- marcadores que darán acceso al recurso

Podemos ver en la figura D.3 como le damos el nombre PFC_ Perfil_de_recurso al perfil y que el marcador es http://www.gva.es. Más abajo vemos como se pude editar la política del recurso. De hecho lo que hacemos es editarla y denegar el acceso a esa URL.

En la pestaña de Roles (figura D.4) será donde asignemos a un rol ese recurso.

Ya hemos configurado el perfil de recurso PFC_perfil_de_recurso. Hay que hacer notar que aunque IVE tiene una política de recurso que permite el acceso web, cuando un usuario sea mapeado al PFC_userRole que hemos creado, antes se le aplicará la política del recurso que se le ha asignado porque ésta tiene más precedencia que la que viene con el IVE por defecto.

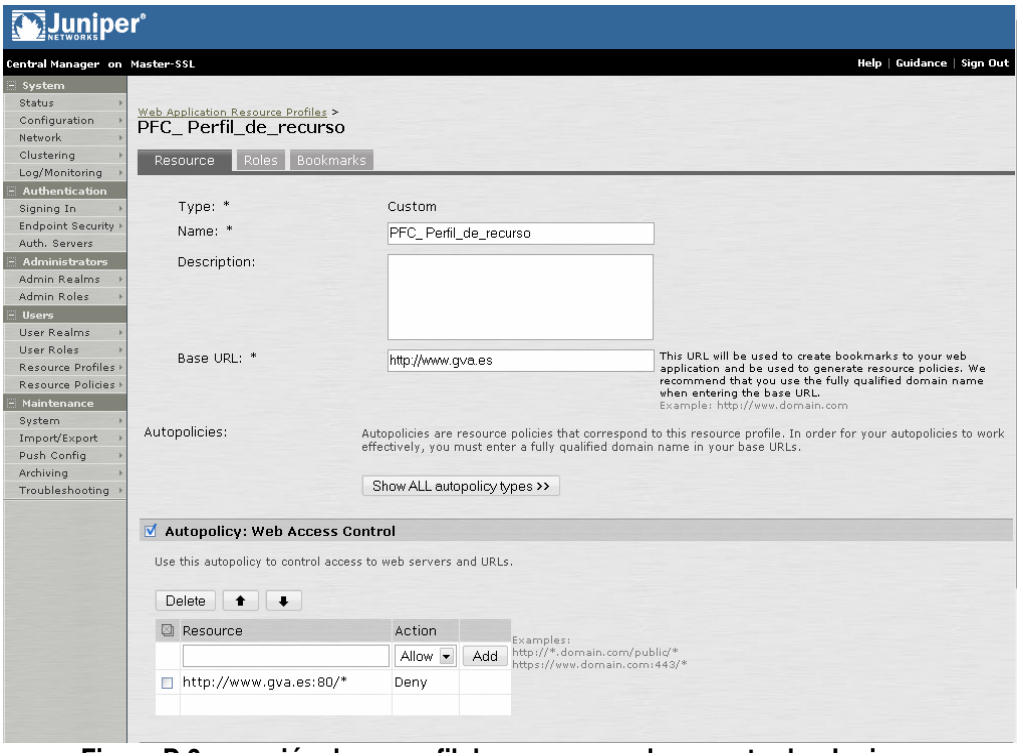


Figura D.3: creación de un perfil de recurso en el concentrador Juniper.

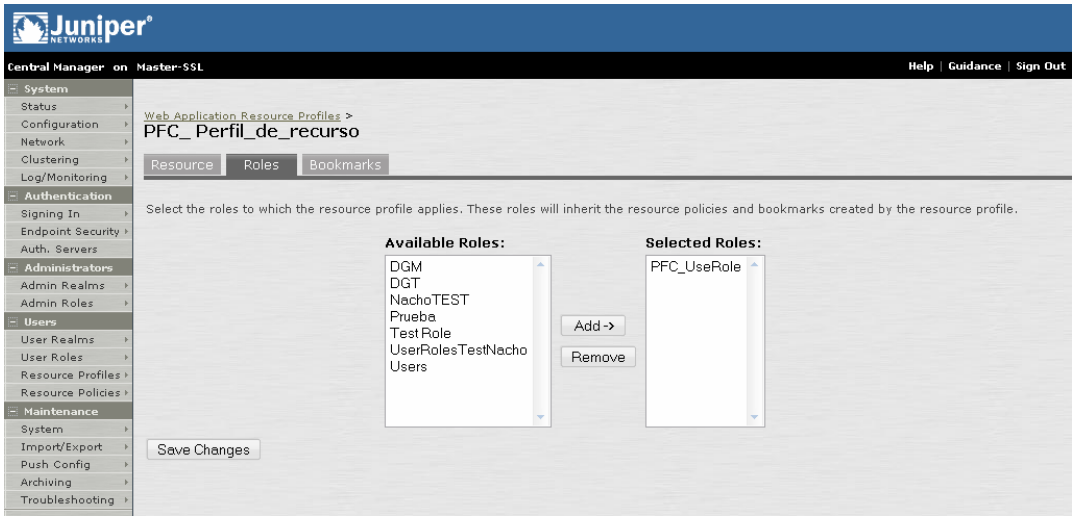


Figura D.4: asiganción de un rol de usuario a un recurso en el concentrador Juniper.

D.3 Definición de un servidor de autenticación, LDAP

Vamos a configurar nuestro servidor LDAP en el IVE, figura D5

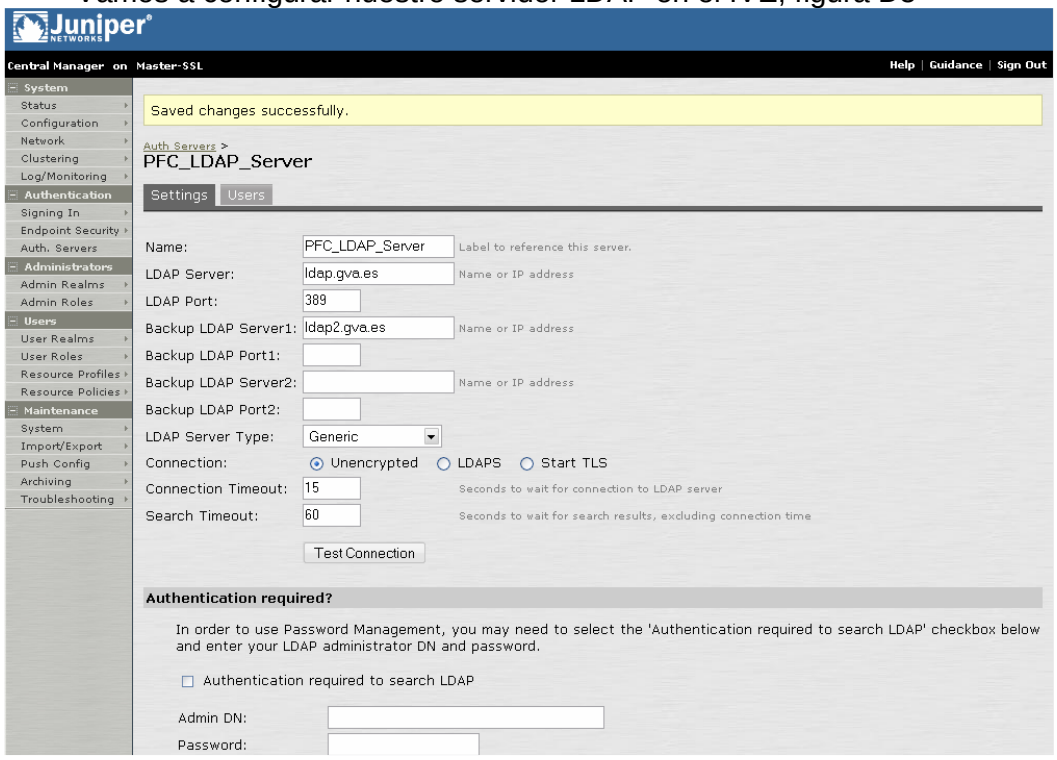


Figura D.5: configuración del servidor LDAP en el concentrador Juniper.

Ya hemos creado el un servidor de autenticación. Ahora los usuarios de ese servidor pueden entrar en el dominio de autenticación que usa PFC_LDAP_Server como servidor de autenticación.

D.4 Definición de un dominio de autenticación

Un dominio de autenticación es un conjunto de recursos de autenticación que incluye:

- Un servidor de autenticación que verifica la identidad del usuario (LDAP en nuestro caso). El IVE reenvía las credenciales enviadas desde la página de inicio de sesión a nuestro servidor de autenticación LDAP.
- Una política de autenticación que especifica qué requisitos de seguridad del dominio de autenticación deberán cumplirse para que el IVE reenvíe las credenciales a nuestro LDAP.
- Reglas de mapeo de roles que son las condiciones que un usuario debe de satisfacer para que el IVE asigne al usuario uno o más roles. Estas condiciones se basan en la información devuelta por el nombre de usuario de la persona o los atributos del certificado.

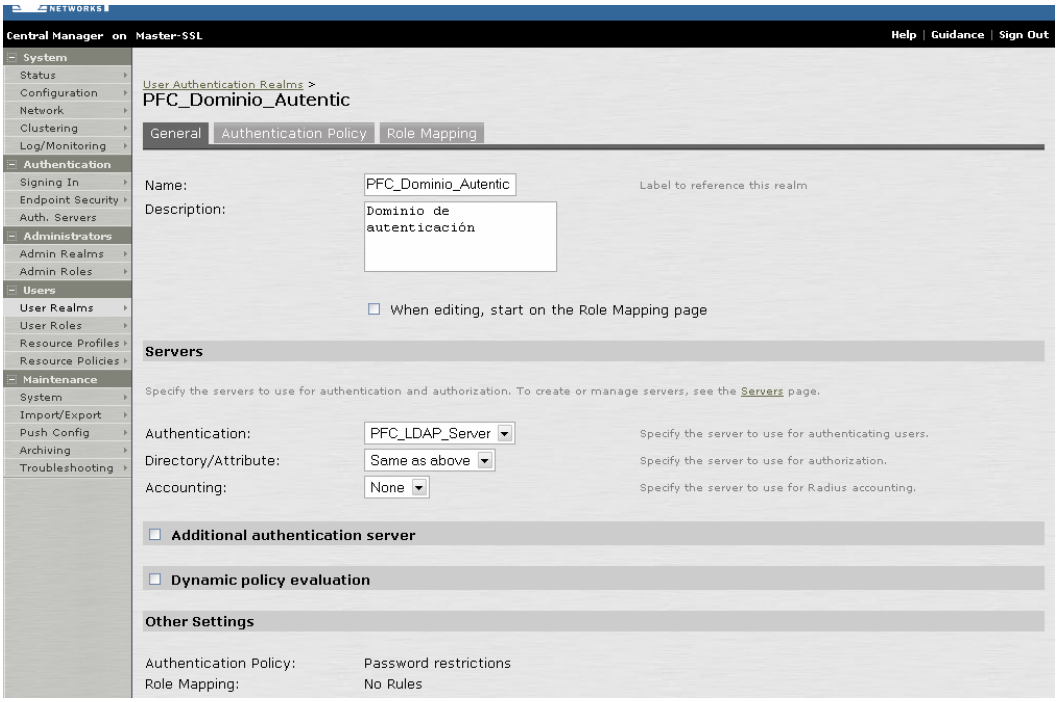


Figura D.6: creación de un dominio de autenticación en el concentrador Juniper.

Le asignamos el servidor de autenticación que hemos dado de alta y en la pestaña del mapeo de reglas configuramos la regla para mapear.

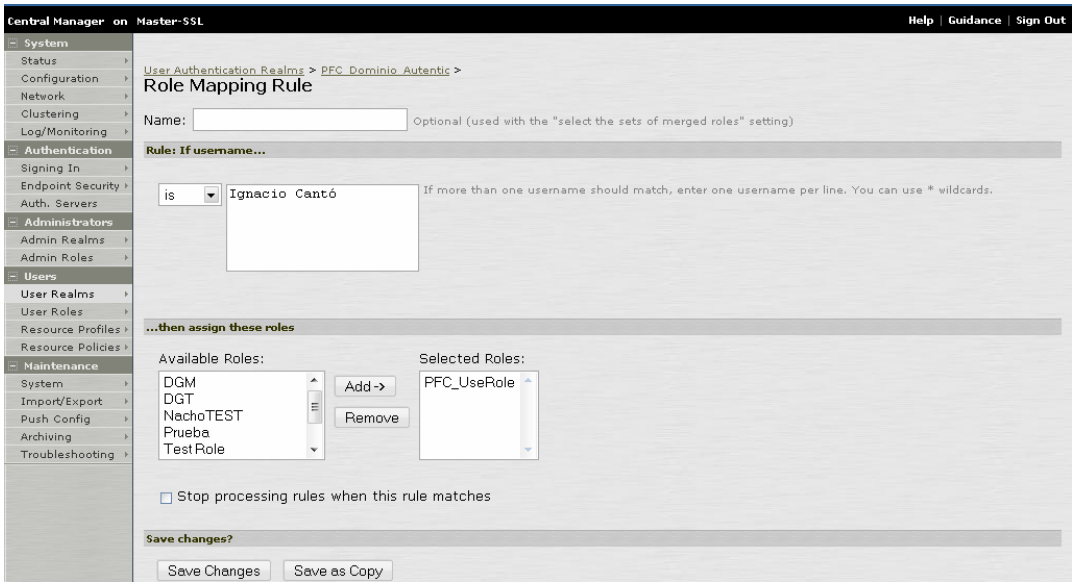


Figura D.7: regla de mapeo de rol en el concentrador Juniper.

D.5 Definición de una política de inicio de sesión

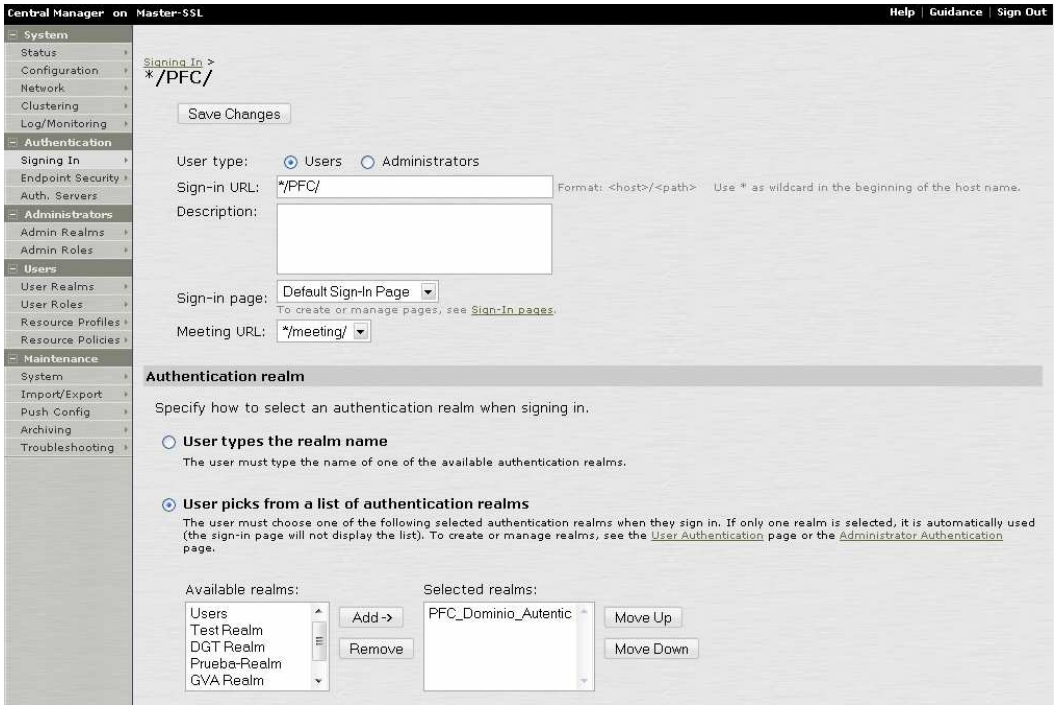


Figura D.8: definición de una política de inicio de sesión en el concentrador Juniper.

Una política de inicio de sesión es una regla del sistema que especifica:

- La URL en la que el usurario puede iniciar una sesión en el IVE.
- Una página de inicio de sesión que mostrar al usuario.
- Si el usuario debe o no escribir o seleccionar un dominio de autenticación al que el IVE envíe las credenciales.
- los dominios de autenticación a los que la política es aplicable.

.

Apéndice E
Contenido CD

- Memoria.
- Manual de configuración del Juniper Networks SA 4000 SSL.
- Fichas técnicas de: Cisco VPN Concentrator 3060, Sonicwall Aventail EX 2500 y Juniper Networks SA 4000 SSL.
- Bibliografía.
- Tabla *Excel* del coste del proyecto.
- Archivo de *MS Project* con las distintas fases del proyecto.

Glosario

AAPP Administraciones Públicas.

AC Certification Authority (Autoridad de Certificación).

ACCV Autoridad de Certificación de la Comunidad Valenciana.

AES Advanced Encryption Standar (Estándar avanzado de encriptación).

AH Autentication Header (Cabecera de autenticación).

ARPANET Advanced Research Projects Agency NETwork.

ASIC Application Specific Integrated Circuit (Circuito integrado para aplicaciones específicas).

ATM Asynchronous Transfer Mode (Modo de Transferencia Asíncrona).

BW BandWidth (Ancho de banda).

CHAP Challenge Handshake Authentication Protocol (Protocolo de autenticación basado en el Handshake).

CIA Confidencialidad, Integridad y Disponibilidad.

CRL Certificate Revocation List (Lista de certificados revocados).

DES Data Encryption Standar (Estándard para la encriptación de datos).

DES triple Data Encryption Standar triple Estándard para la encriptación de datos triple).

DGT Dirección General de Tráfico.

DMZ DeMilitarizaded Zone.

DNS Domain Name System (Base de datos con nombres de dominio).

DSA Digital Signature Algorithm (Algoritmo de firma digital).

DSCF (dispositivo seguro de creación de firma).

DSL Digital Subscriber Line (Línea de abonado digital).

DSS Digital Signature Standard (Estándar de firma digital).

EAP Extensible Authentication Protocol (Protocolo de autenticación ampliable).

ESP Encapsulating Security Payload (Encapsulado de carga segura).

FTP File Transfer Protocol (Protocolo de transferencia de archivos).

GVA Generalidad Valenciana.

HTTP HyperText Transfer Protocol (Protocolo de transferencia de hipertexto).

IDEA International Data Encryption Algorithm (Algoritmo internacional de encriptación de datos).

IKE Internet Key Exchange (Intercambio de claves en internet).

IVE Instant Virtual Extranet (Interfaz gráfica del concentrador Juniper).

IMAP Internet Message Access Protocol (Protocolo de acceso a mensajes electrónicos).

IPSEC Internet Protocol Security (Protocolo de seguridad de internet).

ISAKMP Internet Security Association and Key Management Protocol (Protocolo de seguridad asociada y de manejo de clave).

ISP Internet Service Provider (Proveedor de servicios de internet).

LDAP Lightweight Directory Access Protocol (Protocolo ligero de acceso a directorio).

LDIF LDAP interchange format. (fichero de intercambio de datos en LDAP)

L2TP Layer 2 Tunneling Protocol.

MD5 Message Digest Algorithm 5 (Algoritmo de resumen del mensaje 5)

MIT Massachusetts Institute of Technology (Instituto tecnológico de Massachusetts).

NAS Network Access Server (Servidor de acceso a la red).

NIST National Institute for Standards and Technology (Instituto americano para la estandarización y la tecnología).

NSA National Security Agency (Agencia de seguridad americana).

OCSP Online Certificate Status Protocol (Estado de los certificados consultable en línea).

OSI International Organization for Standardization (Organización internacional para la estandarización).

PAP Password Authentication Protocol (Protocolo de autenticación de clave de acceso).

POP3 Post Office Protocol (Protocolo para el envío de correo).

PPP Point to Point Protocol (Protocolo punto a punto).

PPTP Point to Point Tunneling Protocol (Protocolo de tunelización punto a punto).

PRU Puntos de Registro de Usuario de la ACCV.

RADIUS Remote Authentication Dial-In User Service (Servicio de autenticación remoto).

RC Red Corporativa.

RSA Rivest, Shamir, Adleman.

SA Security Association (Seguridad asociada).

SARA Sistema de Aplicaciones y Redes para las Administraciones.

SHA Secure Hash Algorithm (Algoritmo Hash Seguro).

SHS Secure Hash Standard (Estándar hash seguro).

SNMP Simple Network Management Protocol (Protocolo simple de administración de red).

SQL Structured Query Language (Lenguaje de consulta estructurado).

SSH Secure Shell (Protocolo de acceso remoto).

SSL Secure sockets Layer (Seguridad de la capa de transporte).

TCP Transmission Control Protocol (Protocolo de control de transmisión).

Telnet TELecommunication NETwork (Protocolo de acceso remoto).

TLS Transport Layer Security (Seguridad de la capa de transporte).

UDP User Datagram Protocol (Protocolo de intercambio de datagramas).

UIT Unión Internacional de Telecomunicaciones.

UIT-T Órgano permanente de la UIT para la normalización.

URL Uniform Resource Locator (Localizador uniforme de recurso).

VoIP Voice over IP (Voz sobre IP).

VPN Virtual Private NEtwork (Red privada virtual).

WIFI WIreless-FIdelity (Estándares para redes inalámbricas).

WINS Windows Internet Naming Service (Servidor de nombres de Windows).

Bibliografía

[ACCV] *ACCV*
http://www.accv.es (Activa a 1 de mayo 2008).

[BOE 1] *Real Decreto 994/1999 Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.* BOE núm. 151, viernes 25 junio de 1999.
http://www.boe.es/boe/dias/1999/06/25/pdfs/A24241-24245.pdf
(Copia en CD, activa a 1 de mayo 2008).

[BOE 2] *Ley 59/2003 de Firma Electrónica.* BOE núm. 304, sábado 20 diciembre de 2003.
http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf
(Copia en CD, activa a 1 de mayo 2008).

[BOE 3] *Real Decreto 1553/2005 Regulación de la expedición del documento nacional de identidad y sus certificados de firma electrónica.* BOE núm. 307, sábado 24 de diciembre de 2005.
http://www.boe.es/boe/dias/2005/12/24/pdfs/A42090-42093.pdf
(Copia en CD, activa a 1 de mayo 2008).

[Cisco] *Cisco Systems*
http://www.cisco.com (Activa a 1 de mayo 2008).

[Data 1] *Ficha técnica Cisco VPN3060*
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5743/ps5749/ps2284/product_data_sheet09186a00801d3b56.pdf
(Copia en CD, activa a 1 de mayo 2008).

[Data 2] *Ficha técnica Sonicwall Aventail EX2500*
http://www.sonicwall.com/downloads/DS_Eclass_SSL_VPN_US.PDF
(Copia en CD, activa a 1 de mayo 2008).

[Data 3] *Ficha técnica Juniper Networks SA 4000 VPN SSL*
http://www.juniper.net/products/ssl/dsheet/100125.pdf
(Copia en CD, activa a 1 de mayo 2008).

[Dawson, 2002] Christian W. Dawson, Gregorio Martín. *El proyecto fin de carrera en ingeniería informática: una guía para el estudiante*. 1.ªEdición, Prentice Hall Madrid 2002.

[Dkpd] *Dokupedia*
http://es.dokupedia.org/index.php (Activa a 1 de mayo 2008).

[DNIe] *El DNI electrónico*

www.dnielectronico.es (Activa a 1 de mayo 2008).

[DOCV 1] *Decret 87/2002 del Govern Valencià, Regulació de la utilització de la firma electrònica avançada en la Generalitat Valenciana.* DOCV núm. 4265, jueves 6 de junio de 2002.
http://www.docv.gva.es/portal/portal/2002/06/06/pdf/2002_X6056.pdf
(Copia en CD, activa a 1 de mayo 2008).

[DOCV 2] *Ley 14/2005 de 23 de diciembre, de medidas fiscales, de gestión administrativa y financiera y de organización de la Generalitat Valenciana*. DOCV 5166, viernes 30 de diciembre de 2005
http://www.docv.gva.es/portal/portal/2005/12/30/pdf/2005_14571.pdf
(Copia en CD, activa a 1 de mayo 2008).

[Domingo, 2005] Alberto Domingo Ajenjo. *Dirección y gestión de proyectos: un enfoque práctico. X edición* Ra-Ma Madrid 2005.

[EU 1] *Directiva 1999/93/CE del Parlamento Europeo y del Consejo, Establecimiento de un marco comunitario para la firma electrónica.*
http://www.cert.fnmt.es/legsoporte/directiva.PDF
(Copia en CD, activa a 1 de mayo 2008).

[Free] *FreeRADIUS*
http://freeRADIUS.org// (Activa a 1 de mayo 2008).

[Gart] *Informe Gartner*
http://mediaproducts.gartner.com/reprints/juniper/vol2/article3/article3.html (Copia en CD, activa a 1 de mayo 2008).

[Ine] *Encuesta sobre el tiempo de trabajo en el año 2000.*
http://banners.noticiasdot.com/termometro/boletines/docs/paises/europa/espana/ine/2003/ine_horastrabajo2002.pdf
(Copia en CD, activa a 1 de mayo 2008).

[IPSec] *IPSec*
http://www.ccs.neu.edu/home/fell/COM1621/1621ppt/Overview_of_IPSec.ppt (Copia en CD, activa a 1 de mayo 2008).

[IPSecVsSSL 1] *VPN SSL vs IPSec*
http://www.thegreenbow.com/IPSecssl.html (Copia en CD, activa a 1 de mayo 2008).

[IPSecVsSSL 2] *VPN's: IPSec vs SSL*
http://netsecurity.about.com/cs/generalsecurity/a/aa111703.htm
(Copia en CD, activa a 1 de mayo 2008).

[IPSecVsSSL 3] *When is SSL VPN a better choice than IPSec VPN?*
http://www.watchguard.com/products/ssl_IPSec.asp
(Copia en CD, activa a 1 de mayo 2008).

[Macro] *MACROLAN*
http://www.empresas.telefonica.es/catalogoTEE/comunicacionesprivadas/datos/redes_privadas/macrolan/ (Activa a 1 de mayo 2008).

[Manual] *Manual del Juniper Networks SA 4000 VPN SSL*
http://www.juniper.net/techpubs/software/ive/6.x/admin/6.0-IVEAdminGuide.pdf (Copia en CD, activa a 1 de mayo 2008).

[MS] *Microsoft*
http://www.microsoft.com (Activa a 1 de mayo 2008).

[OLdap] *OpenLDAP*
http://www.OpenLDAP.org/ (Activa a 1 de mayo 2008).

[OVpn] *OpenVpn*
http://openvpn.net/ (Activa a 1 de mayo 2008).

[POL 1] *Política de Certificación de Certificados para servidores de VPN de la GVA.*
http://www.accv.es/pdf-politicas/PKIGVA-CP-08V1.0-c.pdf
(Copia en CD, activa a 1 de mayo 2008).

[POL 2] *Política de Certificación de Certificados para servidores con soporte SSL de la GVA.*
http://www.accv.es/pdf-politicas/PKIGVA-CP-03V1.1-c.pdf
(Copia en CD, activa a 1 de mayo 2008).

[POL 3] *Política de Certificación de Certificados de aplicación de la GVA.*
http://www.accv.es/pdf-politicas/PKIGVA-CP-05V2.0-c.pdf
(Copia en CD, activa a 1 de mayo 2008).

[POL 4] *Política de Certificación de Certificados para firma de código de la GVA*.
http://www.accv.es/pdf-politicas/PKIGVA-CP-04V1.1-c.pdf
(Copia en CD, activa a 1 de mayo 2008).

[Redes] *Apuntes de Redes de Computadores*. Rogelio Montañana. Universidad de Valencia.
http://www.uv.es/~montanan/redes (Activa a 1 de mayo 2008).

[RFC] *Página de los editores de RFC*
http://www.rfc-editor.org/ (Activa a 1 de mayo 2008).

[Sol10] *Manual de instalación de Solaris 10.*
http://dlc.sun.com/pdf/819-0310/819-0310.pdf
(Copia en CD, activa a 1 de mayo 2008).

[Suma] *SUMA*
http://www.suma.es/ (Activa a 1 de mayo 2008).

[SunV120] *Guía usuario Sunfire V120.*
www.compsci.wm.edu/SciClone/documentation/hardware/Sun/V120/v120_UserGuide.pdf (Copia en CD, activa a 1 de mayo 2008).

[Uit] *UIT-T*
http://www.itu.int/ITUTELECOM/index-es.html (Activa a 1 de mayo 2008).

[VPN] *Qué es y cómo crear una VPN.*
http://www.configurarequipos.com/doc499.html (Copia en CD, activa a 1 de mayo 2008).

[VPNeIPSec] *VPN e IPSec*
http://www.criptored.upm.es/guiateoria/gt_m445c.htm (Copia en CD, activa a 1 de mayo 2008).

[Wiki] *Wikipedia la enciclopedia libre*
http://www.wikipedia.es (Activa a 1 de mayo 2008).

[Windows] *Manual de Windows.*
http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/ch10s02.html (Activa a 1 de mayo 2008).

[Word] *Diccionario Inglés*
http://www.wordreference.es (Activa a 1 de mayo 2008).

[WXP] *Conexión VPN en Windows XP*
http://www.raulserrano.net/archivo/2003/12/conexion-vpn-en-windows-xp/ (Activa a 1 de mayo 2008).