Universidad de Alcalá
Escuela Politécnica Superior

Grado en Ingeniería Informática

Trabajo Fin de Grado

Implantación, creación de un laboratorio de pruebas y casos prácticos para la herramienta CheckPoint DLP-1 2571

Autor: Daniel Martín Santos

Tutor: Luis de Marcos Ortega

2013

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

Grado en Ingeniería Informática

Trabajo Fin de Grado

Implantación, creación de un laboratorio de pruebas y casos prácticos para la herramienta CheckPoint DLP-1 2571

Autor: Daniel Martín Santos

Director: Luis de Marcos Ortega

TRIBUNAL:

Presidente:

Vocal 1:

Vocal 2:

CALIFICACIÓN: ……

FECHA: ……..……

A mi padre,

porque, desde el cielo, sé que está orgulloso

A Sara,

por disfrutar y luchar a mi lado

Agradecimientos

A mi madre, por el día a día, creer plenamente y apoyarme en todo lo que hago y darme los medios para conseguir mis metas.

A mi hermana, por confiar en mí y apoyarme cuando lo necesito.

A Manuel Sánchez Rubio, por ser mi guía en el trabajo y enseñarme tantas cosas que no están en los libros.

A Jesús, José Luis y Sara, por tantas horas de esfuerzo realizado codo con codo pero siempre divertidas.

A Sara, por recorrer conmigo éste y tantos caminos que nos depara la vida.

Índice general

Índice de ilustraciones

Índice de tablas

Resumen

La prevención de pérdida de datos, o Data Loss Prevention (DLP), es un término que resume un enfoque de gestión de la seguridad de la información sensible de las empresas.

DLP-1 2571 es una herramienta de Data Loss Prevention creada por Check Point para organizaciones que pretende detectar y prevenir el envío voluntario o involuntario de información confidencial de la organización de una forma cómoda, eficaz y sin ralentización de las comunicaciones.

En éste trabajo de fin de grado describiremos las funcionalidades y veremos casos prácticos, o pruebas, de los módulos de software que Check Point pone a nuestra disposición en ésta herramienta de DLP. Estos módulos ofrecen al administrador de la red un interfaz sencillo y amigable para definir las reglas de restricción, observar el tráfico de datos, obtener estadísticas, etc.

Palabras clave

Data Loss Prevention, DLP, CheckPoint, implantación, laboratorio, pruebas.

Abstract

Data Loss Prevention (DLP) is a term which summarizes the security management of sensitive information in companies.

DLP-1 2571 is a tool, created by Check Point to manage the Data Loss Prevention in organizations, which aims detect and prevent intentional or unintentional sending of confidential information of the organization. All these advantages are achieved with an easy management and without communications slowdown.

In this degree final project we will describe module functionalities and we will show you case studies and functionality tests of the software modules that Check Point makes available for us in this DLP tool. These modules allow to the network administrator a simple and friendly interface to define restriction policies, to monitor data traffic, to obtain statistics and so on.

Keywords

Data Loss Prevention, DLP, CheckPoint, deployment, laboratory, tests.

Resumen extendido

A continuación se va a resumir con más detalle la estructura que veremos en este trabajo fin de grado con descripciones detalladas de cada una de las partes que lo componen. También se van a establecer unos objetivos que pretendemos conseguir con este trabajo y el alcance del mismo para futuras ampliaciones del mismo.

- **Descripción**

El resultado principal del desarrollo de este trabajo de fin de grado será una memoria detallada en la que encontraremos los siguientes tres grandes bloques:

BLOQUE 1: Bases del Data Loss Prevention

Se describirá una serie de conceptos teóricos que se deben tener claros a la hora de la lectura de éste trabajo fin de grado para una correcta compresión del mismo. Entre otros, recordaremos algunos fundamentos de redes de computadores relacionados con protocolos, modelo OSI y TCP/IP, sistemas de gestión de la seguridad de la información, firewalls, proxies, etc.

En este bloque también se hará una descripción profunda de qué es el Data Loss Prevention y un breve análisis de la herramienta de Check Point DLP-1 2571 así como de los módulos de software necesarios para la gestión de la misma.

Para completar el conocimiento de las funcionalidades de la herramienta de una manera extensa se recomienda la lectura de *TFG de Sara Carral Ramos 'Análisis, funcionalidades y propuestas de implantación de la herramienta CheckPoint DLP-1 2571'* [2].

BLOQUE 2: Elección de escenario y montaje de un laboratorio de pruebas

En este bloque se hará una elección de un escenario apropiado para el montaje de un laboratorio de pruebas. Este escenario será escogido de una lista de propuestas posibles descritas a fondo en el *TFG de Sara Carral Ramos 'Análisis, funcionalidades y propuestas de implantación de la herramienta CheckPoint DLP-1 2571'* [2]. Se describirán los motivos por los cuales hemos escogido uno de ellos en concreto para llevar a cabo las pruebas.

Por último, en este bloque se especificará también el procedimiento paso a paso llevado a cabo para la creación de un laboratorio de pruebas que utilizaremos en el siguiente bloque, así como el material necesario para llevar a cabo las mismas.

BLOQUE 3: Casos prácticos

Este último gran apartado describirá cada una de las pruebas llevadas a cabo documentadas con amplias descripciones y pantallazos. Se contrastará su utilidad con una serie de hipotéticos casos reales con el fin de demostrar en qué situaciones es útil implementar algo parecido en las empresas de hoy en día.

En la resolución de cada uno de los bloques anteriores se generarán una serie de contenidos electrónicos que se adjuntarán con la entrega de este trabajo ya que pueden ser útiles para el montaje de laboratorios futuros.

Los medios que utilizaremos dependerán del número de máquinas que queramos establecer como clientes en el laboratorio. No obstante, tendremos como mínimo un número de 3 PCs necesarios para albergar los elementos de red que aparecerán en las pruebas así como un switch, un router y el UTM-1 de la herramienta DLP-1 2571.

Además se utilizarán otros medios como una conexión a Internet para búsqueda de información y un PC personal donde albergar todo el material y donde realizar la documentación de las distintas partes del TFG.

Por último serán estrictamente necesarias las herramientas software de Check Point, el sistema operativo propietario de Check Point, Secure Platform R75.40 y herramientas de software libre para simular servicios de Internet, como por ejemplo Filezilla (para servidores FTP) o XAMPP (para servidores web).

- ## Objetivo

El propósito principal de éste trabajo de fin de grado está orientado tanto a un aprendizaje personal de la materia, así como una primera aproximación a un mundo de control de información en las empresas para evitar fugas de datos, que actualmente está en expansión.

Se puede fijar como principal objetivo el conocimiento a fondo de la herramienta de Data Loss Prevention así como del uso de cada uno de sus módulos. La capacidad de instalación de una herramienta desconocida y el montaje de un laboratorio de pruebas puede ser un objetivo secundario a alcanzar debido al reto personal que ello supone.

Una vez realizado el montaje del laboratorio de pruebas, y destacando el material generado en la creación del mismo, la fácil reproducción del mismo laboratorio en el futuro dará la posibilidad de probar la herramienta a quien lo desee, tanto a alumnos como a profesores que quizá quieran experimentar con ella antes de sus clases.

- ## Alcance

El escenario propuesto e implementado en el laboratorio de pruebas puede servir como base para la implementación de un sistema DLP en cualquier organización interesada en dotar a su empresa de un sistema de estas características. Por ello el material generado por la realización de este trabajo es clave para los primeros pasos de cualquier administrador de un sistema DLP.

De la misma manera, puede servir de punto de partida para futuros alumnos que quieran profundizar más en el desarrollo de este trabajo fin de grado con, por ejemplo, la creación de material docente como transparencias, enunciados de prácticas, resoluciones, etc.

BLOQUE 1:
Bases del Data Loss Prevention

A continuación se van a describir una serie de conceptos que conviene tener claros para la correcta comprensión de este trabajo fin de grado y que, en su mayoría, están relacionados con los principios fundamentales de las redes de computadores, sistemas de cortafuegos, proxies, una amplia descripción de qué es el Data Loss Prevention, etc.

Finalmente se hará una descripción de la herramienta que se va a utilizar para las pruebas así como de cada uno de sus módulos.

1.1. Fundamentos de redes de computadores

En esta última década la necesidad de conectar dispositivos tecnológicos, y más concretamente ordenadores, ha crecido de manera exponencial, lo que ha provocado un crecimiento proporcional del desarrollo de las redes de computadores.

Podemos definir red de computadores como un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones.

De esta manera ponen al alcance de los usuarios de las mismas un amplio abanico de funcionalidades como compartir ficheros, impresoras y otros recursos,

enviar correos electrónicos, ejecutar programas de forma remota en otros ordenadores, búsqueda de todo tipo de información, etc.

En lo referente a las empresas, las conexiones por red permiten sus empleados colaborar entre sí y con empleados de otros lugares u otras empresas repartidos por todo el mundo. Posibilitan así el contacto, de forma innovadora, entre personas pertenecientes a una misma oficina o de cualquier punto geográfico. Si la empresa está conectada por una red, nadie está lejos de nadie.

1.1.1. Componentes básicos de las redes de computadores

Una vez hemos comprendido lo que es una red de computadores, veamos cuáles son sus componentes básicos.

- **Software:** Incluye tanto el sistema operativo de red (en términos generales cualquier sistema operativo, como Linux o Windows, da soporte a redes) así como software específico de aplicación.
  Gracias al software, nos es posible realizar tareas específicas de manera fácil para nosotros

- **Hardware:** Este grupo lo forman todos aquellos elementos o dispositivos físicos que permiten formar redes. Por ejemplo dispositivos de usuarios finales (PC, móviles, impresoras, televisiones, etc.), servidores, tarjetas de red, routers, switches, hubs, puntos de acceso inalámbricos, cables, etc. En este caso nos centraremos en los conceptos de:

  - **Dispositivos de usuario final:** Son dispositivos tales como PCs, móviles, impresoras, televisiones, lectores de CD, etc.

Ilustración 1: Dispositivos de usuario finales

- **Dispositivos de red:** Son los dispositivos que usaremos para que sea posible una comunicación de red. Según las necesidades se deben seleccionar los elementos adecuados para poder completar el sistema y que pueda existir una comunicación entre ellos.
  Entre los dispositivos más habituales nos encontramos con puntos de acceso inalámbricos, router, switch o bridge. A continuación definiremos algunos de los más comunes.

  - **Routers**: Un router, también conocido como enrutador de paquetes es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI (que explicaremos más adelante).
    Su función principal es enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

Ilustración 2: Router WiFi

  - **Switch**: Dispositivo que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI. Este dispositivo interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro.
    Su empleo es muy común cuando existe el propósito de conectar múltiples redes entre sí para que funcionen como una sola.

Ilustración 3: Switch

- **Tarjetas de red:** Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red, o NIC (Network Card Interface), con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo a esos datos a un formato que pueda ser transmitido por el medio (bits, ceros y unos). Este componente es muy importante para que se pueda establecer una comunicación a través de la red.

Ilustración 4: Tarjeta de red

- **Protocolos de redes:** Modelos o estándares que determinan un conjunto de reglas que serán usadas por los dispositivos de red para comunicarse entre ellos intercambiando mensajes a través de una red. En el siguiente apartado nos centraremos en dos grandes modelos de protocolos de red.

1.1.1.1. Protocolos de red

En este apartado explicaremos más en profundidad lo que son los protocolos de red y nos centraremos en dos de sus modelos más importantes.

Los protocolos son reglas de comunicación que permiten a dispositivos que manejan lenguajes diferentes, y que de otra manera serían incompatibles, llevar a cabo tarea comunes con éxito y para un mismo fin.

Para lograr mantener esas conexiones con éxito deben especificarse una serie de propiedades:

- Detección de la conexión física y existencia de puntos finales o nodos.
- Negociación de varias características de la conexión.
- Inicialización y finalización de mensajes.
- Formateo de mensajes.
- Corrección de errores.
- Detección y tratamiento de posibles pérdidas de conexiones.
- Terminación de conexiones.

Existen una gran variedad de protocolos y estándares, pero nosotros nos centraremos en los 2 más importantes:

- **Modelo OSI:** modelo estándar y marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.
- **Modelo TCP/IP:** el modelo más utilizado a nivel mundial, tanto en la comunicaciones a nivel global como local.

1.1.1.2. Modelo OSI

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), también llamado OSI (Open System Interconnection) es el modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización (**ISO**) en el año 1984.

Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

- **Estructura multinivel:** Modelo basado en una estructura multinivel con la idea de que cada nivel se encargue de resolver una parte del problema de comunicación. Cada nivel ejecuta funciones específicas.
  El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otros ordenadores, pero debe hacerlo enviando un mensaje a través de los niveles inferiores de su mismo ordenador. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

- **Puntos de acceso:** Existen interfaces llamadas “puntos de acceso” a los servicios entre cada uno de los diferentes niveles que componen este modelo.

- **Dependencias entre niveles:** Cada nivel depende del nivel inferior y el superior.

- **Encabezados:** En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que exista comunicación coherente entre capas iguales de ordenadores diferentes (emisor y receptor). Cualquiera de los niveles puede incorporar un encabezado al mensaje.

- **Unidades de información:** En cada nivel, la unidad de información tiene diferente nombre y estructura, siendo siete los niveles de los que se compone y que se detallarán a continuación.

Como se ha comentado más arriba, este modelo está dividido en capas. Esto proporciona una serie de ventajas que son las siguientes:

- Dividir la comunicación de red en partes más pequeñas y sencillas simplificando el tratamiento de errores.

- Normalizar los componentes de red para permitir el desarrollo y soporte de los pro-ductos de diferentes fabricantes.

- Permitir a los distintos tipos de software y hardware de red comunicarse entre sí.

- Aislar y tratar de manera independiente los cambios por cada capa para permitir un desarrollo más veloz.

- Simplificar el aprendizaje dividiendo en partes más pequeñas la comunicación de red.

De tal modo, mostramos a continuación la distribución en forma de pila de las siete capas que forman este modelo.

Ilustración 5: Distribución modelo OSI

A continuación detallaremos cada una de las siete capas de las que está compuesto el modelo OSI.

- **Capa 1: Capa física.** La capa física controla el medio de transporte mediante la definición de las características eléctricas y mecánicas del medio que lleva la señal. Pertenecen a esta capa el cable de par trenzado, el cable de fibra óptica, el cable coaxial y las líneas serie.

- **Capa 2: Capa de enlace.** Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo.

- **Capa 3: Capa de red.** El servicio básico del nivel de red es proporcionar transferencia de datos transparente entre entidades de transporte. Es decir, libera al nivel de transporte de la necesidad de conocer el funcionamiento interno de la subred.

  Entre sus principales funciones se encuentran el encaminamiento y el control de la congestión.

- **Capa 4: Capa de transporte.** Es el primer nivel que lleva a cabo comunicación extremo - extremo, condición que se mantiene en los niveles superiores a él. Su objetivo es proporcionar mecanismos que garanticen que el intercambio de datos entre procesos de distintos sistemas se lleve a cabo de forma fiable. El nivel de transporte debe asegurar que los paquetes de datos se entregan libres de error, ordenados y sin pérdidas ni duplicados.

- **Capa 5: Capa de sesión.** El nivel de sesión proporciona los mecanismos para controlar el diálogo entre aplicaciones. Como mínimo el nivel de sesión proporciona un medio para que dos procesos de aplicación puedan establecer y utilizar una conexión, llamada sesión.

- **Capa 6: Capa de presentación.** El objetivo es encargarse de la representación de la información de manera que, aunque distintos equipos puedan tener diferentes representaciones internas de caracteres, los datos lleguen de manera reconocible.

- **Capa 7: Capa de aplicación.** El nivel de aplicación proporciona un medio a los procesos de aplicación para acceder al entorno OSI. Contiene funciones de gestión y mecanismos útiles para soportar aplicaciones distribuidas. Ejemplos de protocolos a este nivel son los de transferencia de ficheros y correo electrónico.

Por tanto, cuando se produzca un intercambio de datos entre un emisor y un receptor este modelo actuará de la siguiente forma.

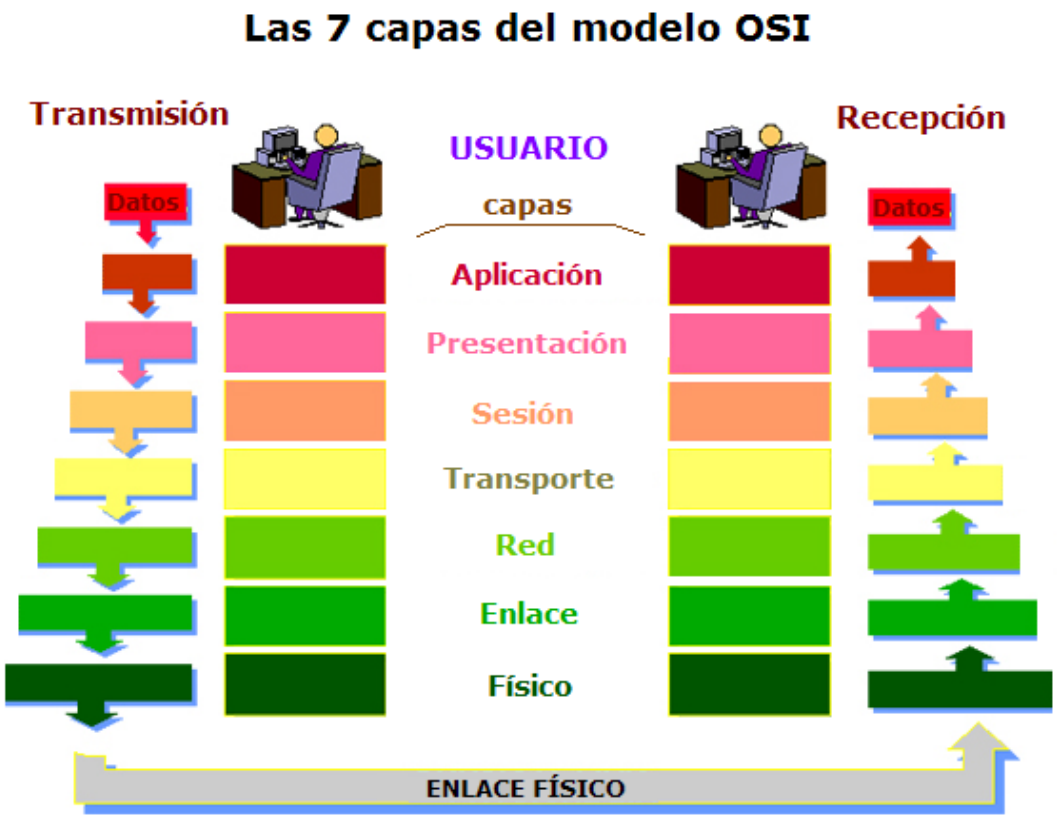

Ilustración 6: Intercambio de datos modelo OSI

1.1.1.3. Modelo TCP/IP

El modelo TCP/IP es un modelo de descripción de protocolos de red creado en la década de 1965 por DARPA, una agencia del Departamento de Defensa de los Estados Unidos y que posteriormente evolucionó en ARPANET.

Contrariamente a otras tecnologías de red propietarias, TCP/IP ha sido desarrollado como una norma abierta. Esto quiere decir que cualquiera puede utilizar este modelo. TCP/IP, describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. También provee conectividad extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, encaminados y recibidos por el destinatario.

Todo esto se engloba en el fin de conseguir un intercambio fiable de datos entre dos equipos, y para esto, se requiere de un gran esfuerzo y de un Software de comunicaciones bastante complejo.

Este modelo también se divide en diferentes capas de abstracción, las cuales están perfectamente jerarquizadas y cada una se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

A pesar de que algunas capas del modelo TCP/IP tengan el mismo nombre que las capas del modelo OSI, éstas no son las mismas. La capa aplicación por ejemplo garantiza diferentes funciones en cada modelo.

Ilustración 7: Modelo TCP/IP

Con lo cual podemos observar las diferencias entre modelo **OSI** y modelo **TCP/IP**.

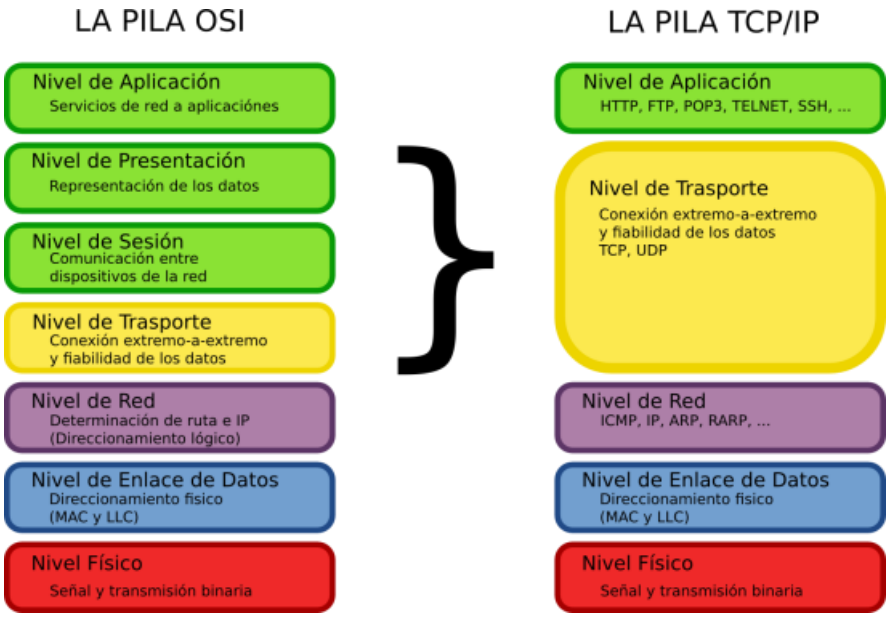

Ilustración 8: Diferencias entre modelo OSI y TCP/IP

En este modelo, nos encontramos con 4 capas bien definidas que se detallan a continuación.

- **Capa 1: Capa de acceso a la red.** Capa que engloba realmente las funciones de la capa física y la capa de enlace de datos equivalente al modelo **OSI**. Es responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. Pertenecen a esta capa los protocolos PPP y ARP.

- **Capa 2: Capa de Internet.** Podemos decir que esta capa es el "corazón" de la red, cumple el mismo papel que la capa de red del modelo **OSI**. Se encarga de encaminar los paquetes de la forma más conveniente para que lleguen a su destino y a la vez evitar que se produzcan situaciones de congestión en cualquiera de los nodos intermedios. Maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de enrutamiento para poder dirigirlos al lugar correspondiente. Pertenecen a esta capa los protocolos IP, ARP, ICMP y ARP.

- **Capa 3: Capa de transporte.** Su función es la misma que su equivalente en el modelo OSI, permitir la comunicación de extremo a extremo en la red, así como proporcionar comunicación punto a punto y regular el flujo de la red. Pertenecen a esta capa los protocolos TCP y UDP.

- **Capa 4: Capa de aplicación.** Esta capa realiza las funciones que equivalen a las capas de sesión, presentación y aplicación del modelo OSI. Los usuarios llaman a una aplicación que acceda a servicios disponibles a través de la red de redes TCP/IP y cada programa de aplicación selecciona el tipo de transporte necesario en ese momento. En esta capa tenemos todos los protocolos de alto nivel que se utilizan para ofrecer servicios a los usuarios, tales como, FTP, HTTP o DNS.

1.1.2. Sistema de gestión de la seguridad de la información

Un Sistema de Gestión de la seguridad de la Información (SGSI) es, como el propio nombre indica, un conjunto de políticas de administración de la información. El

término es utilizado principalmente por la ISO/IEC 27001. Este término se denomina en inglés “Information Security Management System" (ISMS).

El concepto clave de un SGSI es que una organización debe realizar el diseño, la implantación y el mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

La herramienta que se utiliza para la realización de este trabajo es precisamente una de las piezas que se utilizan para lograr éste cometido. Podríamos afirmar que el término Data Loss Prevention está íntimamente relacionado con el concepto SGSI.

1.1.3. Cortafuegos o Firewalls

Los cortafuegos, o mejor conocidos como firewalls, son una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, otra pieza más de un sistema de gestión de la seguridad de la información.

Se trata de un dispositivo, o conjunto de dispositivos, configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware, software, o una combinación de ambos. Éstos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente redes de corporaciones internas, más conocidas como intranets.

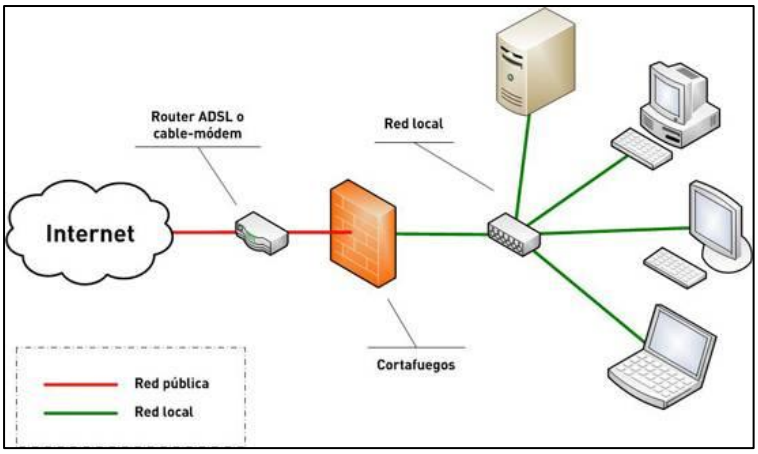

Ilustración 9: Ubicación más frecuente de un firewall

Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados, también conocidos como políticas. También es frecuente conectar al cortafuegos a una tercera red, llamada "zona desmilitarizada" o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo de los que un firewall nos puede proteger.

1.1.4. Servidor Proxy

La finalidad más habitual de un servidor proxy consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc. Esta función de servidor proxy puede ser realizada por un programa (en forma de software) o dispositivo (en forma de hardware).

Ilustración 10: Proxy BlueCoat SG800 Series

Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: proporcionar caché, control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, etc.

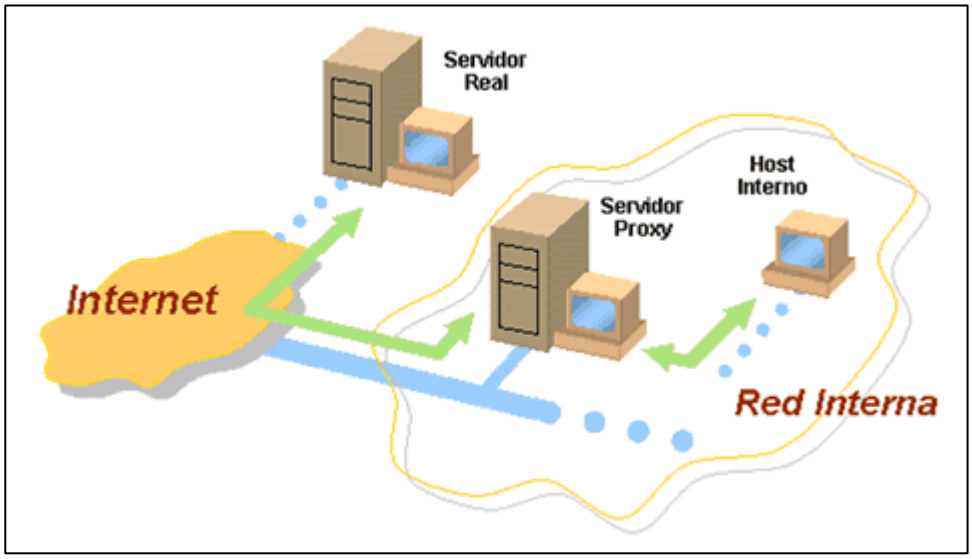

Ilustración 9: Funcionamiento de un proxy

1.1.4.1. Usos más comunes de servidores proxy

Un servidor proxy dispone de diferentes características o funciones para gestionar el tráfico de información. Entre ellas podemos encontrar:

- Filtrado de contenido, mediante BBDD que se han ido recopilando con el tiempo y que permiten a los proveedores dar un valor añadido a sus productos.
- Cache de contenido, para mejorar el rendimiento del uso del ancho de banda.
- Función de router, estos dispositivos pueden actuar como un router cualquiera.
- Proxy Inverso, usado delante de los servidores web y servidores de aplicaciones para liberar de carga a los servidores y proporcionar una capa de seguridad a los mismos.
- Seguridad, estos dispositivos pueden aplicar una capa de autenticación y autorización mediante el uso de fuentes de usuarios para gestionar el acceso a los recursos de una empresa o de Internet.

- Anonimato, acceder de manera anónima a los sitios web ocultando la ip origen, etc.

Existen dos maneras básicas de funcionamiento de un proxy diferenciadas por la configuración que el cliente debe realizar para la correcta comunicación con el mismo:

- Proxy transparente: El Proxy intercepta la comunicación normal de red sin la necesidad de ninguna configuración especial en el cliente.

  Suele estar situado entre los clientes e Internet en entornos empresariales para forzar el uso de políticas de seguridad con un coste mínimo de administración por parte de los departamentos de TI.

  Además permite que los usuarios no tengan, de manera inmediata y fácil, conocimiento de su existencia. Los proxies transparentes también son utilizados por los proveedores de Internet (Internet Service Provider o ISP) para conseguir un ahorro de ancho de banda, utilizando el cacheo de datos, y así mejorar los tiempos de respuesta de los clientes. Este tipo de funcionalidad se suele implementar normalmente en países donde el ancho de banda disponible es limitado y caro como por ejemplo en islas.

- Proxy explícito: Al contrario que la implementación de Proxy Transparente los clientes deben ser configurados explícitamente para poder comunicarse normalmente con la red.

  Esto inicialmente supone un sobre coste aunque existen alternativas que facilitan la configuración automática de proxies explícitos como la descarga automática de la configuración desde un servidor Web, a través de un fichero PAC (Proxy Auto-Configuration), la auto detección de la configuración del proxy, etc.

1.1.5. Unified Threat Management (UTM)

El término Unified Threat Management (en castellano Gestión Unificada de Amenazas) fue utilizado por primera vez en 2004 para describir a los cortafuegos de red que engloban múltiples funcionalidades, trabajando a nivel de capa de aplicación, en una misma máquina.

Entre otras, algunas de las funcionalidades más comunes que son capaces de implementar los UTM son:

- Análisis de tráfico UDP.
- Creación de VPNs.
- Control Antispam.
- Control Antiphishing.
- Control Antispyware.
- Filtrado de contenidos de sitios web, FTPs, correo electrónico, etc.
- Antivirus.
- Detección y Prevención de Intrusos (IDS/IPS).

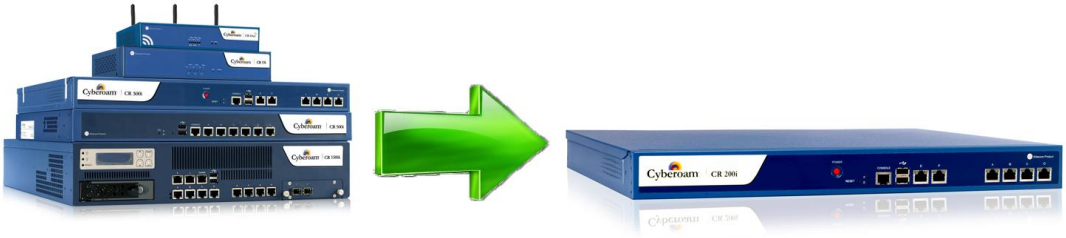

Ilustración 10: Evolución a UTMs

Este tipo de firewalls de red pueden trabajar de dos modos según su tipo de funcionamiento:

- Modo proxy: hacen uso de proxies para procesar y redirigir todo el tráfico interno.

- Modo Transparente: no redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones hardware.

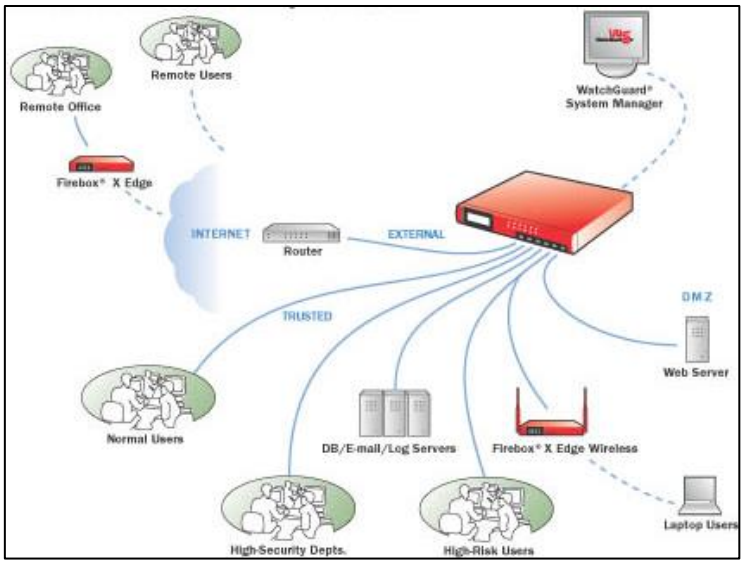

Ilustración 11: Funcionamiento de un sistema UTM

Para toda empresa es importante hacer un análisis de ventajas y desventajas antes de tomar la decisión de implantar un sistema de este tipo en sus instalaciones. A grandes rasgos las principales ventajas que encontramos son las siguientes:

- Sustitución de varios sistemas independientes por uno único.
- Mayor facilidad de configuración respecto a grandes grupos de sistemas independientes.
- Mejor efectividad en la gestión de la red.
- Bajo coste de implantación del mismo.

Por el contrario, también detectamos una serie de desventajas a la hora de implantar un sistema UTM en una empresa:

- Se crea un punto único de fallo, es decir, si falla este sistema la organización queda desprotegida totalmente.
- Crea un punto de cuello de botella, lo que puede perjudicar a empresas de gran tamaño.
- Tiene un coste fijo periódico.

1.2. Tipos principales de Servidores

Hablando en términos informáticos, un servidor es un nodo que forma parte de una red y que pone a disposición uno o varios servicios a otros nodos de red llamados clientes.

Generalmente se trata de una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Los servicios más habituales son la gestión de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un ordenador, y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. En ciertas ocasiones, dependiendo de la utilidad que vayamos a darle, un mismo ordenador puede cumplir simultáneamente las funciones de cliente y servidor.

Al contrario de lo que mucha gente puede pensar, un servidor no es necesariamente una máquina de última generación de grandes proporciones ni es necesariamente un superordenador. Un servidor puede ser desde un ordenador antiguo, hasta una máquina sumamente potente (como lo son en general los servidores web, bases de datos grandes, procesadores especiales, etc.). Todo esto depende del uso que se le dé al servidor.

Ilustración 13: Cuarto de servidores

Ilustración 12: PC servidor y estación de trabajo

No obstante, dependiendo de la carga general que vaya a recibir el servidor pueden ser de dos tipos:

- **Servidores dedicados:** Son aquellos que dedican toda su potencia a atender todas las solicitudes de procesamiento de los clientes.

- **Servidores no dedicados:** Son aquellos que no dedican toda su potencia a las peticiones recibidas, sino que también se suelen utilizar como estaciones de trabajo al procesar también solicitudes de un usuario local

A continuación vamos a ver con más detenimiento las funciones de los servidores generalmente más utilizados y que utilizaremos en las pruebas que veremos en las siguientes páginas de este trabajo fin de grado: Servidores de correo electrónico, servidores FTP y servidores web.

1.2.1. Servidores de Correo electrónico

Un servidor de correo es una aplicación de red ubicada en un servidor en Internet (o en una red local, aunque es menos frecuente), cuya función es muy similar al correo postal tradicional. La diferencia es que, en este caso, lo que se maneja son los correos electrónicos (mundialmente conocidos como e-mails), a los que se les hace circular a través de redes de transmisión de datos hasta llegar a su destino en unos pocos segundos. De una forma similar al correo postal, en el correo electrónico se puede adjuntar todo tipo de información (extensos informes, fotos, grabaciones de vídeo o voz, etc.) eso sí en formato electrónico.

Ilustración 14: Principales servidores de correo

Esto nos proporciona una serie de ventajas con respecto al correo postal tradicional:

- El coste del envío de un correo electrónico es nulo, tan sólo es necesario poseer una conexión a Internet y estar registrado en un servidor de correo que te proporcione una cuenta única a la cual destinar los e-mails y con la cual acceder a tu bandeja de entrada.
- El tamaño de los documentos, en general, pueden ocupar bastante capacidad (las limitaciones las establecen los propios servidores). Lo suficiente como para poder enviar documentos de texto de miles de páginas, cientos de fotos y varios archivos de audio y vídeo.
- El tiempo de entrega del e-mail es prácticamente instantáneo, por lo que no tendremos que esperar largos días para recibir ciertas noticias urgentes.
- Cada día más empresas se comunican con sus clientes, envían facturas, recibos, etc. a través de correo electrónico por lo que se genera un ahorro importante

en material de oficina (papel, impresora, etc.) y además se contribuye a evitar la tala de árboles para la generación de papel.

A nivel internacional hay una serie de compañías que han puesto a nuestra disposición una serie de servicios entre los que se encuentra el correo electrónico. Entre otras hemos de destacar los dominios más utilizados como Gmail (de la compañía Google), Hotmail (de Microsoft), Yahoo! Mail, AOL Mail, GMX Mail, etc.

Además cualquiera de nosotros podríamos implementar un servidor de correo electrónico a nivel local con diversos programas cuya finalidad es proporcionar la infraestructura para ello. Entre otros se encuentra ArGoSoft Mail Server, que será el que utilicemos para montar nuestro propio servidor de correo.

1.2.2. Servidores FTP

FTP (File Transfer Protocol, "Protocolo de Transferencia de Archivos") es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un equipo servidor para descargar archivos desde él o para enviarle archivos y almacenarlos, independientemente del sistema operativo utilizado en cada equipo.

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes como LAN, WAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores y ordenadores.

Por lo general, los programas servidores FTP no suelen encontrarse en los ordenadores personales, por lo que un usuario normalmente utilizará el FTP para conectarse remotamente a uno y así intercambiar información con él.

Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento web, en el que sus clientes utilizan el servicio para subir sus páginas web y sus archivos correspondientes, o como servidor de backup (copias de seguridad) de los archivos importantes que pueda tener una empresa.

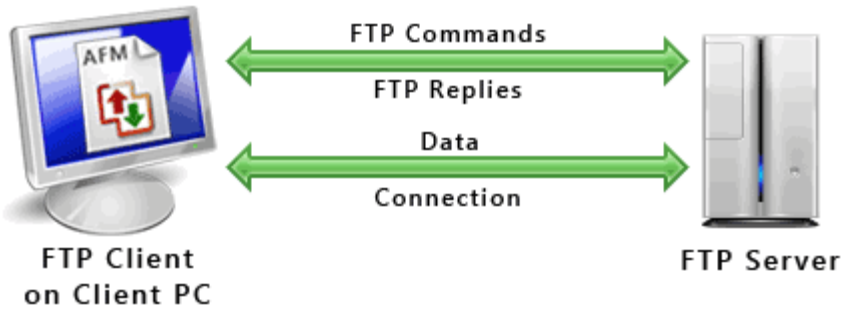

Ilustración 15: Flujo de datos FTP

Además existe una variación del protocolo para que los datos se transmitan cifrados, como el SFTP (Secure File Transfer Protocol).

El sistema más utilizado como servidor local de FTP es FileZilla Server, el cual nos permite instaurar un servidor FTP de una manera fácil y eficaz.

1.2.3. Servidores WEB

Un servidor web o servidor HTTP es un programa informático que procesa una aplicación del lado del servidor realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente. El código recibido por el cliente suele ser compilado y ejecutado por un navegador web. Para la transmisión de todos estos datos suele utilizarse algún protocolo. Generalmente se utiliza el protocolo HTTP para estas comunicaciones, perteneciente a la capa de aplicación del modelo OSI.

El Servidor web se ejecuta en un ordenador manteniéndose a la espera de peticiones por parte de un cliente (un navegador web) y que responde a estas peticiones adecuadamente, mediante una página web que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún error.

A modo de ejemplo, al teclear cualquier dirección válida en nuestro navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página. El cliente, una vez recibido el código, lo interpreta y lo exhibe en pantalla.

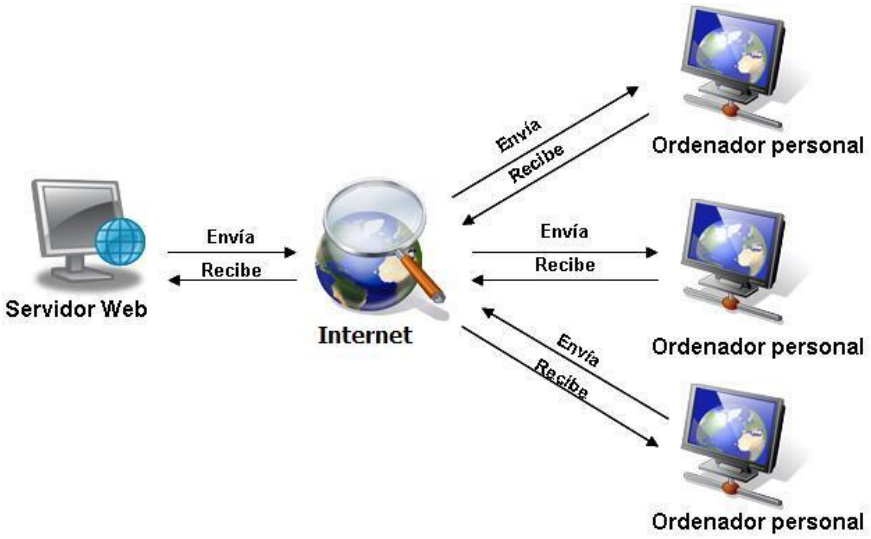

Ilustración 16: Flujo de una petición web

Como vemos con este ejemplo, el cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página. El servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Además de la transferencia de código HTML, los Servidores web pueden entregar aplicaciones web. Éstas son porciones de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- **Aplicaciones en el lado del cliente:** el cliente web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java "applets" o Javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Comúnmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje javascript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins.
- **Aplicaciones en el lado del servidor:** el servidor web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor muchas veces suelen ser la mejor opción para realizar aplicaciones web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad añadida, como sí ocurre en el caso de querer ejecutar aplicaciones javascript o java. Así pues, cualquier cliente dotado de un navegador web básico puede utilizar este tipo de aplicaciones.

Uno de los servidores web más extensamente utilizado es el Servidor Web APACHE. Es el que utilizaremos más adelante para el alojamiento de una web de pruebas.

1.3. Tipos principales de Clientes

El cliente es una aplicación informática o un ordenador que consume un servicio remoto de otro equipo conocido como servidor. Normalmente se utiliza una red de telecomunicaciones.

El término se usó inicialmente para los llamados terminales tontos, dispositivos que no eran capaces de ejecutar programas por sí mismos, pero podían conectarse e interactuar con equipos remotos por medio de una red y dejar que éste realizase todas las operaciones requeridas, mostrando luego los resultados al usuario. Se utilizaban sobre todo porque su coste en esos momentos era mucho menor que el de un ordenador. Estos terminales tontos eran clientes de un equipo mainframe por medio del tiempo compartido.

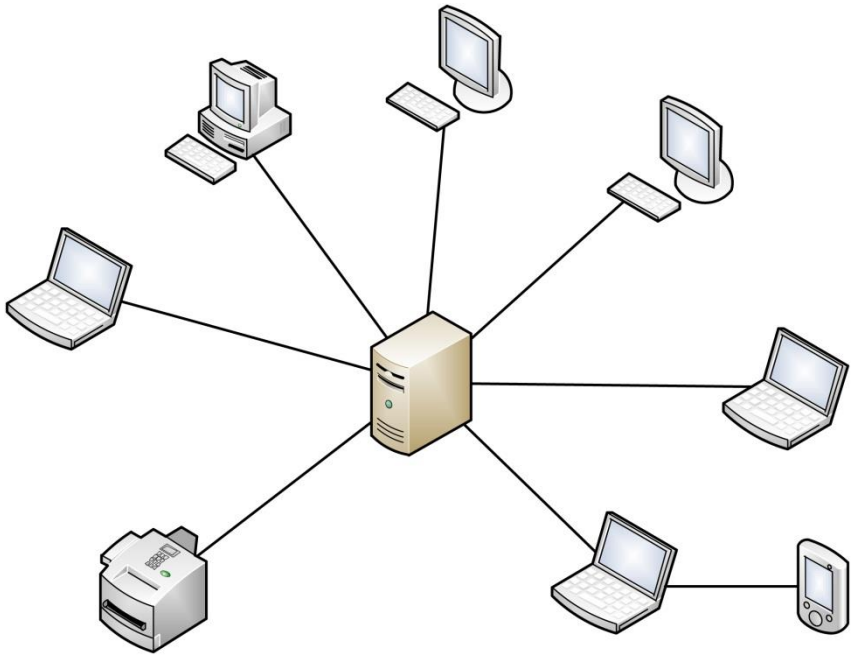

Ilustración 17: Arquitectura Cliente-Servidor

Actualmente se suele utilizar para referirse a programas que requieren específicamente una conexión a otro programa, al que también se denomina servidor y que suele estar en otra máquina. Ya no se utilizan por criterios de coste, sino para obtener datos externos (por ejemplo páginas web, información bursátil o bases de datos), interactuar con otros usuarios a través de un gestor central (como por ejemplo los protocolos BitTorrent o IRC), compartir información con otros usuarios (servidores de archivos y otras aplicaciones) o utilizar recursos de los que no se dispone en la máquina local (por ejemplo impresión).

Uno de los clientes más utilizados, sobre todo por su versatilidad, es el navegador web. Muchos servidores son capaces de ofrecer sus servicios a través de un navegador web en lugar de requerir la instalación de un programa específico.

A continuación vamos a ver con más detenimiento las funciones de los clientes generalmente más utilizados y que utilizaremos en las pruebas que veremos en las siguientes páginas de este trabajo fin de grado: Clientes de correo electrónico, clientes FTP y clientes web.

1.3.1. Clientes de Correo electrónico

Un cliente de correo electrónico es un programa de ordenador usado para leer y enviar mensajes de correo electrónico.

Originalmente, los clientes de correo electrónico fueron pensados para ser programas simples para leer los mensajes del correo de usuario. Los clientes de correo más modernos deben soportar protocolos como POP3 e Internet Message Access Protocol (IMAP) para comunicarse con un agente de transferencia de correo remoto localizado en la máquina de proveedores de correo electrónico.

IMAP está optimizado para almacenar correos electrónicos en el servidor, mientras que el protocolo POP3 asume generalmente que los mensajes de correo electrónico se descargan al cliente. La gran mayoría de clientes de correo electrónico emplean el Protocolo de Transferencia Simple de Correo (Simple Mail Transfer Protocol o SMTP) para enviar los mensajes de correo electrónico.

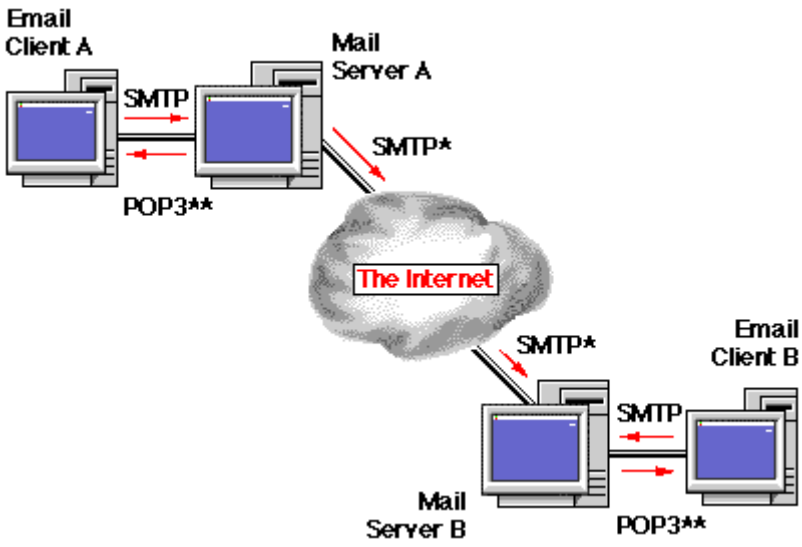

Ilustración 18: Flujo de datos de correo electrónico

A parte de los clientes de correo nombrados hasta aquí existen también programas de correo electrónicos basados en la Web, denominados Webmail o correo web.

Un correo web es un cliente de correo electrónico, que provee una interfaz web por la que acceder al correo electrónico. El correo web permite listar, desplegar y borrar vía un navegador web los correos almacenados en el servidor remoto. Los correos pueden ser consultados posteriormente desde otro computador conectado a Internet y que disponga de un navegador web.

Los clientes de correo electrónico no basados en la web y más utilizados son Mozilla Thunderbird, Microsoft Outlook, Foxmail, etc.

Por otro lado hemos de destacar los clientes web más utilizados como Gmail, Hotmail, Yahoo! Mail, AOL Mail, GMX Mail, etc.

Ilustración 19: Clientes de correo electrónico

1.3.2. Clientes FTP

Un cliente FTP emplea el protocolo FTP para conectarse a un servidor FTP para transferir archivos.

Algunos clientes de FTP básicos vienen integrados en los sistemas operativos, incluyendo Windows, DOS, Linux y Unix. Sin embargo, hay disponibles clientes con más funcionalidades, habitualmente en forma de freeware para Windows y como software libre para sistemas de tipo Unix. La mayoría de los navegadores recientes también llevan integrados clientes FTP, aunque un cliente FTP trabajará mejor para FTP privadas que un navegador.

Para utilizar un cliente FTP, se necesita conocer el nombre del archivo, el ordenador en que reside (servidor, en el caso de descarga de archivos), el ordenador al que se quiere transferir el archivo (en caso de querer subirlo nosotros al servidor), y la carpeta en la que se encuentra.

Los servidores FTP anónimos ofrecen sus servicios libremente a todos los usuarios, permiten acceder a sus archivos sin necesidad de tener un USER ID o una cuenta de usuario. Es la manera más cómoda fuera del servicio web de permitir que todo el mundo tenga acceso a cierta información sin que para ello el administrador de un sistema tenga que crear una cuenta para cada usuario.

Si un servidor posee servicio “FTP anonymous” solamente con teclear la palabra anonymous, cuando pregunte por tu usuario tendrás acceso a ese sistema. No se necesita ninguna contraseña preestablecida, aunque tendrás que introducir una sólo para ese momento, normalmente se suele utilizar la dirección de correo electrónico propia. Solamente con eso se consigue acceso a los archivos del FTP, aunque con menos privilegios que un usuario normal. Normalmente solo podrás leer y copiar los archivos que sean públicos.

Si se desea tener privilegios de acceso a cualquier parte del sistema de archivos del servidor FTP, de modificación de archivos existentes, y de posibilidad de subir nuestros propios archivos, generalmente se suele realizar mediante una cuenta de usuario. En el servidor se guarda la información de las distintas cuentas de usuario que pueden acceder a él, de manera que para iniciar una sesión FTP debemos introducir una autentificación (login) y una contraseña (password) que nos identifique unívocamente.

FTP admite dos modos de conexión del cliente: Activo y Pasivo. En ambos modos el cliente establece una conexión con el servidor mediante el puerto 21, que establece el canal de control. Veamos con algo más de detalle el funcionamiento de ambos:

- **Modo activo:** el cliente manda un comando PORT al servidor por el canal de control indicándole el número de puerto por el que el cliente establecerá la conexión de datos, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados.

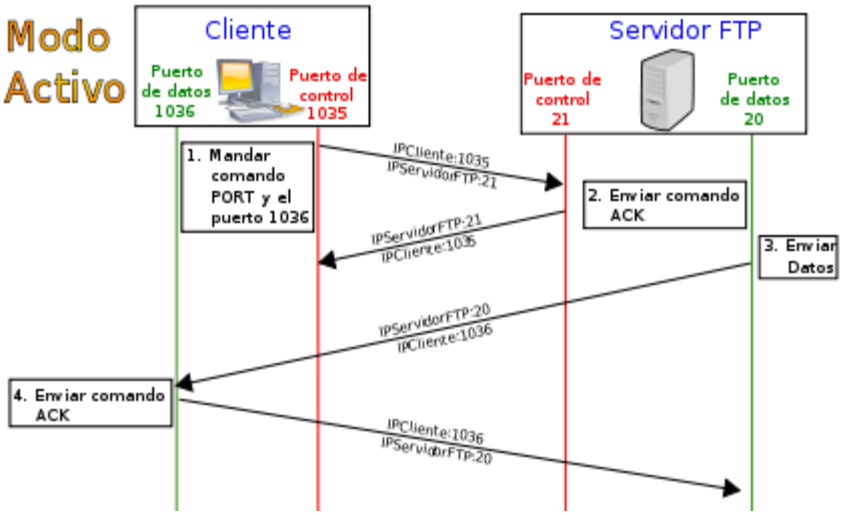

Ilustración 20: Modo activo FTP

Lo anterior tiene un grave problema de seguridad, y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024, con los problemas que ello implica si tenemos el equipo conectado a una red insegura como Internet.

- **Modo pasivo:** Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control el puerto (mayor a 1023) del servidor al que debe conectarse el cliente. El cliente inicia una conexión desde el puerto siguiente al puerto de control hacia el puerto del servidor especificado anteriormente.

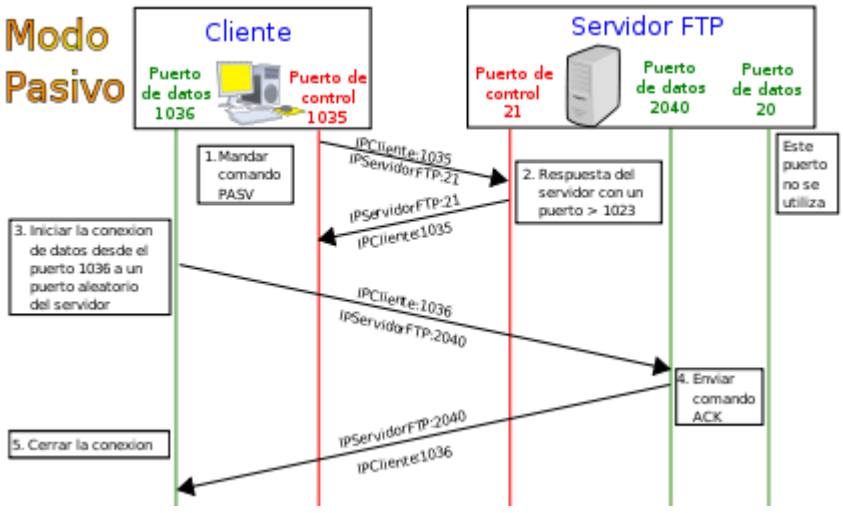

Ilustración 21: Modo pasivo FTP

Antes de cada nueva transferencia tanto en el modo Activo como en el Pasivo, el cliente debe enviar otra vez un comando de control (PORT o PASV, según el

modo en el que se haya conectado). El servidor recibirá esa conexión de datos en un nuevo puerto aleatorio.

1.3.3. Clientes WEB

El cliente web tendrá la posibilidad de poder realizar peticiones y navegar por la web a través de un navegador web. Estas peticiones son bidireccionales entre el cliente y el servidor, por lo que es obvio que utiliza una arquitectura cliente-servidor.

Generalmente para la transmisión e intercambio de datos entre cliente y servidor se utiliza el protocolo HTTP (perteneciente a la capa de aplicación) para la web pero también se puede utilizar una modificación de este, el protocolo HTTPS. Este último lo utilizan algunos servidores web en páginas con información crítica, con el fin de asegurar al cliente una conexión segura sin riesgos.

Como se ha comentado antes en el apartado de servidor web, el cliente desde el navegador, será el encargado de interpretar código HTML que reciba por parte del servidor.

Los navegadores web nos dan soporte para servicios FTP, administrar el correo electrónico, etc. Existe una gran variedad de navegadores web, pero los más utilizados actualmente son: Internet Explorer, Mozilla Firefox, Google Chrome y Safari.

Ilustración 22: Clientes web más utilizados

1.4. Data Loss Prevention

La creciente evolución de la tecnología, hace que la protección de la información, independiente del medio donde se tenga almacenada o por la cual sea transportada, requiera de niveles más complejos y eficientes para prevenir el robo y uso indebido de los datos.

Las empresas hoy día enfrentan graves consecuencias, debido a las malas prácticas de sus empleados frente a los datos corporativos, lo que pone en riesgo la información confidencial y propietaria de las organizaciones. En este sentido, los dispositivos portátiles y de almacenaje extraíbles, representan una serie amenaza, convirtiéndose en elementos claves a tener en cuenta en el panorama de seguridad actual.

La información se mueve más allá del perímetro empresarial y la capacidad de almacenamiento crece mientras que el tamaño de los dispositivos es cada vez menor. Cualquier persona con un dispositivo removible, puede descargar datos sensitivos y exponer información de alto valor para una empresa. Además estos elementos representan uno de los vectores potenciales de ataque para la propagación de códigos maliciosos diseñados para el robo de información.

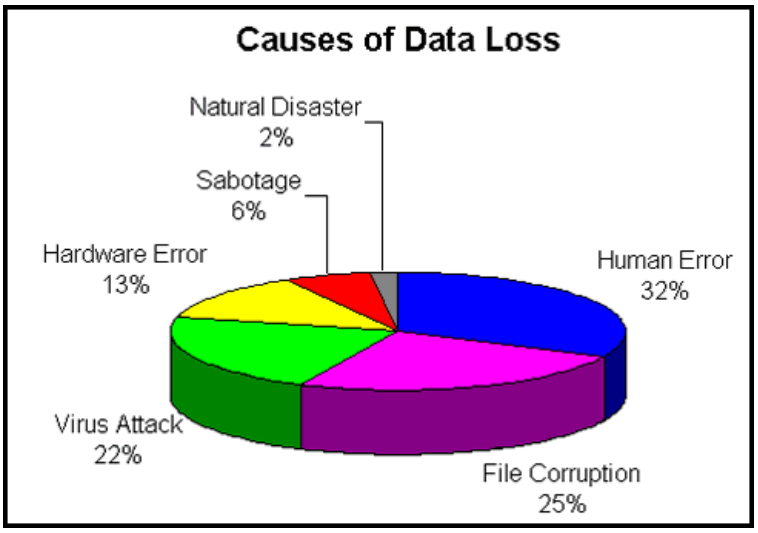

Ilustración 23: Causas de la pérdida de datos

La cuestión es que el "ecosistema" adquiere una complejidad que obliga a los administradores de IT a asumir este desafío con la ayuda de soluciones que permitan proteger su información a través de gestión y control eficiente. Esa tecnología se denomina: Prevención de la pérdida de datos.

Prevención de la pérdida de datos o data loss prevention es, como muchos otros términos, un término de marketing para resumir un enfoque de gestión de la seguridad de la información con muchos años de vida. El data loss prevention se focaliza en analizar y entender los flujos de datos en una organización, la situación de los datos (en movimiento, en uso o almacenados), e implantar las medidas de seguridad necesarias para proteger su confidencialidad.

La tecnología DLP, no solo previene el robo de información sino que además la protege. DLP no debe verse como una opción, sino como una iniciativa crítica para proteger el activo más importante de una organización: La información confidencial y propietaria. Los daños y perjuicios que traen consigo la pérdida o robo de información son mucho mayores que los costes asociados a la implementación de tecnologías DLP.

Ilustración 24: Robo de información

El data loss prevention se entiende mejor pensando en distintos escenarios que afectan a la seguridad de la información de cualquier empresa que en la actualidad necesite proteger activos digitales como diseños, imágenes, planes, documentación sensible, etc. Esta metodología, podría utilizarse para evitar que empleados descontentos se llevaran información sin autorización de una organización imprimiéndola, en un dispositivo USB de almacenamiento (pendrive, disco externo...) o enviándola por Internet (mediante correo electrónico, redes sociales, sistemas de almacenamiento externo como FTPs, etc.).

Las soluciones de data loss prevention no solo permiten bloquear la impresión, el copiado de datos a dispositivos USB o el envío de datos por Internet, sino que permite controlar y monitorizar dichos flujos de datos: permitiendo la impresión, copiado o envío a determinados grupos de usuarios y registrando todas las impresiones, copias y envíos en un histórico.

La implantación de un sistema de este tipo no es trivial. Se requiere un trabajo inicial de análisis de los flujos de datos, clasificación de la información, análisis de

riesgos y configuración de sistemas. Sin embargo, con el inicio de un proyecto de este tipo, se pueden obtener resultados inmediatos que ayudan a prevenir daños mayores mientras se trabaja en una implantación global de una solución definitiva.

Antes de comenzar la implantación de un sistema DLP en una organización, considere los siguientes pasos sugeridos:

1. Analice la situación actual de su empresa y defina sus requerimientos DLP

   De esta manera es posible tener un panorama claro de las brechas que, en materia de seguridad de la información, afectan a la empresa y de acuerdo a ello implementar los controles DLP respectivos.

2. Asegure sus PCs y defina políticas claras de uso de los dispositivos portables y memorias USB

   

   Ilustración 25: USB protegido

   Aplique políticas de seguridad automáticamente para proteger los datos de forma anticipada y evitar que la información confidencial salga de la organización. Es necesario establecer políticas claras que definan el uso correcto de estos dispositivos tanto dentro como fuera de la organización y crear campañas de concienciación en los empleados sobre la importancia de respetar estas normativas.

3. Asegure su correo electrónico, los archivos y carpetas a través de encriptación

   Proteja su Información Confidencial a través de encriptación que le permitirá que únicamente las personas autorizadas, internas y externas, tengan acceso a ella.

4. Monitoree, encuentre, registre y haga cumplir las políticas de seguridad de su empresa

Las organizaciones pueden obtener un beneficio inmediato por el despliegue de un sistema integral de prevención de fuga de datos que puede supervisar y hacer cumplir una política de seguridad para los datos. Los administradores pueden simplemente establecer y configurar las políticas de seguridad con el objetivo primordial de tener el sistema protegido contra accidentes y fugas provocadas por usuarios malintencionados.

5. Realice una implementación por fases que garantice el éxito

Proteger los datos sensibles y propietarios es crucial para la mayoría de las empresas donde la Propiedad Intelectual y la información confidencial se correlacionan con el valor monetario de la compañía.

Ilustración 26: Eslogan DLP de Check Point

La característica fundamental de la tecnología DLP frente a otros servicios o productos de seguridad es su capacidad de entender los distintos protocolos y formatos de archivo e inspeccionar en el contenido de los datos que se usan, transmiten o almacenan, determinando si la acción que se está realizando cumple la política de seguridad de la organización, sin apenas retardo en las comunicaciones.

1.5. Conocimiento de la herramienta

En el siguiente apartado vamos a detallar la principal actividad de la empresa Check Point desde sus orígenes hasta la actualidad. También detallaremos las principales características de la herramienta DLP-1 2571 en cuanto a hardware y, una breve descripción de cada uno de los módulos software que componen la herramienta SmartConsole R75.40, para una mayor descripción de los mismos se recomienda la lectura de *TFG de Sara Carral Ramos 'Análisis, funcionalidades y propuestas de implantación de la herramienta CheckPoint DLP-1 2571'* [2].

1.5.1. Check Point

Check Point Software Technologies Ltd (http://www.checkpoint.com), es un proveedor a nivel global de soluciones de seguridad IT, líder mundial en seguridad en Internet. Conocido por sus productos Firewall y VPN, Check Point fue el pionero en la industria con el firewalls y su tecnología patentada de inspección del estado de la red. Hoy en día la compañía desarrolla, comercializa y soporta una amplia gama de software y hardware combinados en productos de que cubren todos los aspectos de seguridad de la tecnología de la información, incluyendo seguridad de red, seguridad en puntos finales, seguridad de datos y en la gestión de las mismas.

Ilustración 27: Logotipo Check Point

Fundada en 1993 en Ramat-Gan, Israel, Check Point cuenta hoy con aproximadamente 2.200 empleados en todo el mundo. Los Centros de desarrollo de la compañía se encuentran en Israel, California (ZoneAlarm), Suecia (ex centro de desarrollo de Protección de Datos) y en Bielorrusia. La empresa también tiene oficinas en los Estados Unidos, en Redwood City, California y en Dallas, Texas, así como en Canadá en Ottawa, Ontario.

Check Point ofrece a sus clientes una gran protección contra todo tipo de amenazas, reduce la complejidad que conlleva la seguridad al mismo tiempo que

ofrece una gran flexibilidad en la soluciones a sus clientes pudiendo personalizarlas para satisfacer completamente las necesidades de seguridad exactas de cualquier organización. Este gran proveedor es el único que ha ido más allá de la tecnología y ha definido la seguridad como un proceso de negocio.

Check Point combina de forma única la política, las personas y la aplicación generando una mayor protección de los activos de información y ayuda a las organizaciones a implementar un plan de seguridad que se alinea de manera total con las necesidades del negocio.

Podemos dividir los productos que ofrece Check Point en una serie de categorías que se detallan a continuación:

- **Security Gateway:** Es el negocio básico de Check Point. En esta categoría podemos encontrar tres grandes grupos que ofrecer al cliente:

    - **Security Appliances:** En estos dispositivos de seguridad se integran mecanismos Hardware que vienen preinstalados con la arquitectura Software Blade que genera una solución segura para el cliente. Estos dispositivos de seguridad pueden ofrecer servicios fiables a miles de empresas en todo el mundo.

    - **Security Software Blades:** Módulos de seguridad independientes y flexibles que se pueden combinar para generar una solución de seguridad personalizada.

    - **Virtualization Security:** Este tipo de solución se reduce a entornos virtuales.

- **Endpoint Security:** Agente de seguridad individual que combina firewall, antivirus, antispyware, cifrado completo del disco, cifrado

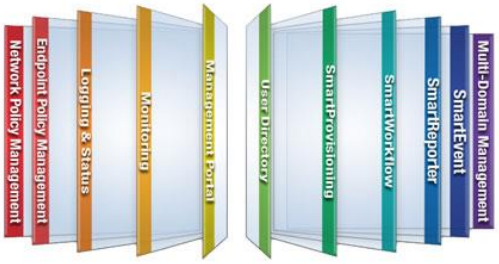

Ilustración 28: Logotipo Software Blade

de los medios de comunicación con protección de puertos, control de acceso a redes (NAC), control de programa y VPN en endpoint.

- **Gestión de la Seguridad:** Permite a los administradores gestionar eventos, establecer normas y aplicar protección a toda la infraestructura de seguridad desde una única interfaz.

La arquitectura Software Blade de Check Point brinda movilidad, flexibilidad y modularidad a sus clientes con una administración centralizada.

Esta arquitectura propietaria de Check Point permite que las empresas seleccionen la protección que más se adecúa a sus necesidades, creando gateways de seguridad a medida para diferentes entornos y sitios web, y gestionarlos de forma centralizada.

1.5.2. Herramienta DLP-1 2571

DLP-1 2571 es una potente herramienta de Data Loss Prevention creada por Check Point para organizaciones de aproximadamente 1.000 personas, en las que no interesa que se produzcan pérdidas de información en las comunicaciones.

La mejor solución para evitar las fugas involuntarias de datos consiste en aplicar una política corporativa automatizada que permita interceptar los datos protegidos antes de que abandonen la organización.

DLP-1 2571 identifica, controla y protege la transmisión de datos a través de la inspección de contenidos y el análisis de los parámetros de operación tales como origen, destino, objeto de datos y protocolo.

Esta herramienta va orientada a empresas que pretenden detectar y prevenir la transmisión no autorizada de información confidencial dentro de su organización de una forma eficaz y sin ralentizar las comunicaciones.

Ilustración 29: Foto DLP-1 2571

Esta herramienta tiene una serie de características técnicas y físicas que definiremos a continuación:

Tabla 1: Características técnicas

CARACTERÍSTICAS TÉCNICAS	
Tipo de dispositivo	Security Appliance
Dimensiones (mm)	443 x 381 x 44
Peso	6.5 kg
Voltaje	100 - 240V
Frecuencia	50 - 60Hz
Fuente de alimentación (max)	250W
Consumo de energía (max)	77.5W
Ámbito de funcionamiento	Temperatura: 5° - 40° C, Humedad: 10% - 85%, Altitud: 2.500 m
Normas de seguridad aceptadas	UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3AS/NZS 3548:1995; KN22KN61000-4 Series, TTA; IC-950; ROHS

Tabla 2: Características físicas

CARACTERÍSTICAS FÍSICAS	
Interfaces (RJ-45)	Interfaz de Gestión
	Interfaz de Consola
	Interfaz de Sincronización
	LAN x4
Puertos USB	x4
Disco Duro	500 GB x1
Display	Pantalla retroiluminada
	Controles de display x4
Otros	Botón de Reset
Protocolos Data Link	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de transporte	SMTP
Protocolo Remote Management	HTTP, FTP
Capacidad	Número máximo de usuarios: 1000

A continuación se van a destacar las mejoras introducidas en ésta versión de la solución (DLP-12571 + R75.40 Gaia + SmartConsole) con respecto a versiones anteriores:

- Mayor visibilidad y herramientas de administración:
    - Administración de estadísticas usando las herramientas SmartDashboard® y SmartView Monitor.
    - Los administradores pueden enviar o descartar el uso de correo electrónico con SmartView Tracker® y SmartEvent.

- Introducción de métodos para prevenir la exposición accidental de datos sensibles:

    - Ocultar los números de tarjetas de crédito, mostrando sólo los últimos 4 dígitos en los registros.

    - Permisos personalizables de administrador que dará más control sobre quién puede ver los datos de DLP.

- Mejoras en la aplicación de plantillas:

    - Nueva opción para ignorar las plantillas vacías durante la exploración.

    - Carga de forma dinámica muchas plantillas en un solo tipo de datos.

- Mejoras en correo electrónico y aplicaciones web:

    - Evita la pérdida de los datos de HTTP/S, de determinado tráfico como Gmail y Facebook.

    - Inspecciona mensajes de correo electrónico entre los usuarios internos y grupos de una organización.

    - Analiza TLS saliente (SMTPS) de correo electrónico cifrado mediante Check Point® de Microsoft Exchange Agent.

    - Inspección de los puertos HTTP/S no estándar.

- Mejora del rendimiento y disponibilidad:

    - Mejoras de rendimiento (velocidad de conexión y conexiones simultáneas).

    - DLP-1 2571 tiene modos tanto de autonomía como de plena disponibilidad.

- Posee distribución de carga.

- Se incluyen más de 500 tipos de datos definidos, ofreciendo la posibilidad de personalizar algunos de ellos según las necesidades del administrador.

- Notables mejoras en el lenguaje CPCode, el cual permite crear Scripts que definirán patrones de palabras a rastrear en las comunicaciones.

1.5.3. Módulos de Smart Console R75.40

A continuación se van a explicar las funcionalidades generales de cada uno de los módulos que compone la SmartConsole Application de Check Point.

- **SmartDashBoard**

SmartDashBoard es el programa principal para los administradores, mediante él se definen los Data Types y con ellos la política del DLP (conjunto de reglas). El sistema DLP-1 se encargará de revisar el tráfico de los clientes a través de cada una de las reglas definidas, con el fin de que no se incumpla la política de la organización (ver siguiente ilustración). Estas reglas son aplicables a navegación web, correo electrónico, etc.

Data Loss Prevention (DLP) Policy

Type to Search | Grouping: Category

Data	Source	Destination	Exceptions	Action	Track	Install On	Category
None (11)							
Palabras malsonantes	My Organization	Outside My Org	None	Prevent	Log	DLP Blades	None
Archivos con password	My Organization	Outside My Org	None	Prevent	Log	DLP Blades	None
Ejecutables	My Organization	Outside My Org	None	Prevent	Log	DLP Blades	None
Diccionario	My Organization	Outside My Org	None	Prevent	Log	DLP Blades	None
Informacion confidencial	My Organization	Outside My Org	None	Ask User	Log	DLP Blades	None
Imagenes	My Organization	Outside My Org	None	Ask User	Log	DLP Blades	None
Cuenta Bancaria	My Organization	Outside My Org	None	Inform User	Log	DLP Blades	None
Facturas	My Organization	Outside My Org	None	Ask User	Log	DLP Blades	None
DNI	My Organization	Outside My Org	None	Inform User	Log	DLP Blades	None
Numero de telefono	My Organization	Outside My Org	None	Detect	Log	DLP Blades	None
Nombres de Personalid...	My Organization	Outside My Org	None	Detect	Log	DLP Blades	None

Ilustración 30: Política de una empresa

- **SmartViewMonitor**

Esta sencilla herramienta de Check Point permite a los administradores configurar y supervisar los distintos aspectos de las actividades de la red. Muestra un cuadro completo de la red y el rendimiento de la seguridad, presentando una imagen visual de los cambios en las pasarelas (ver ilustración), túneles, usuarios remotos y actividades de seguridad.

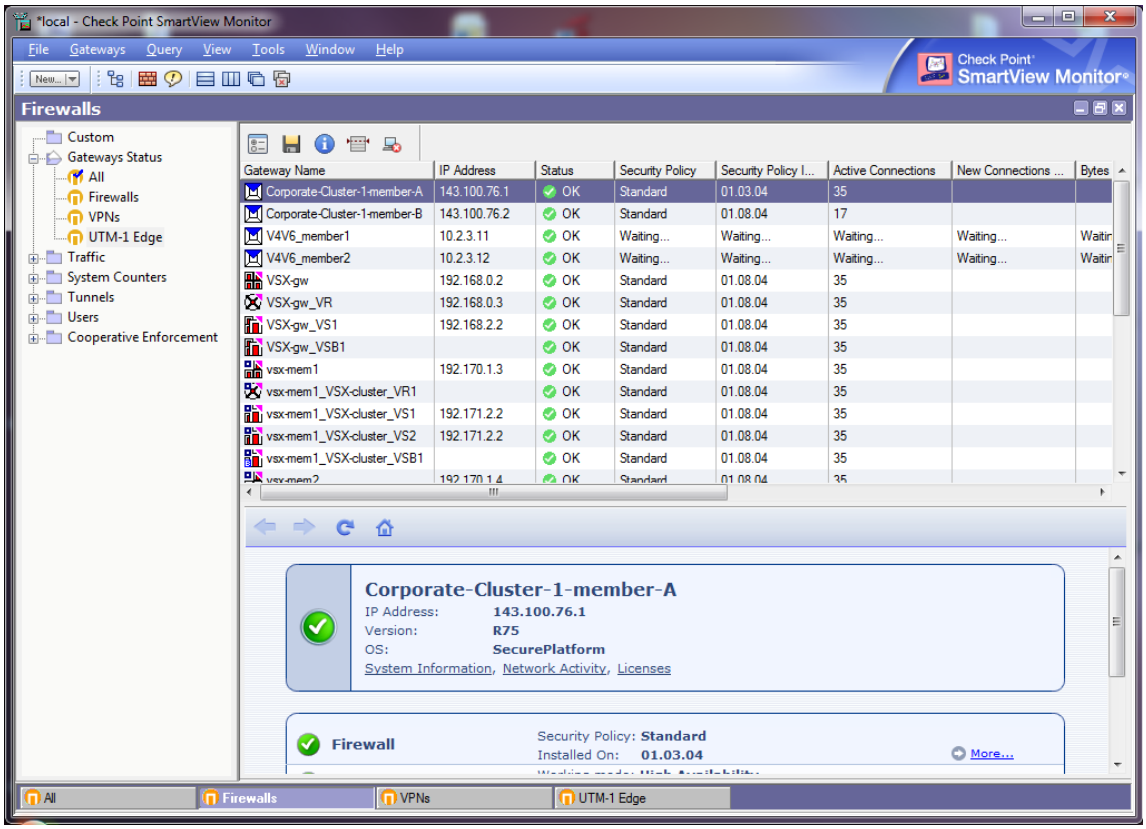

Ilustración 31: Estado de puertas de enlace

- **SmartViewTracker**

Otra de las herramientas de Check Point es SmartViewTracker, el cual proporciona la capacidad de recopilar información detallada sobre la actividad en la red en forma de gráficos, pudiendo analizar patrones de tráfico, problemas de redes y de seguridad.

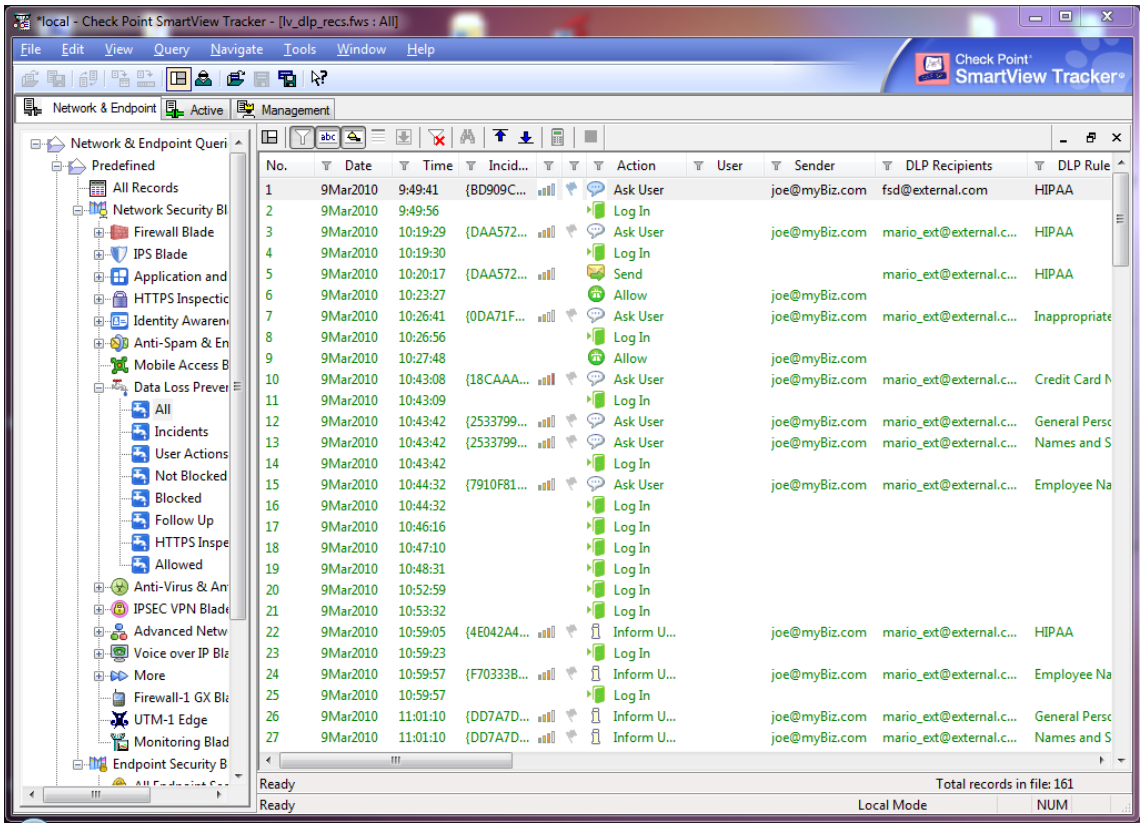

Ilustración 32: Seguimiento DLP de la red

El administrador suele utilizar SmartViewTracker para garantizar el buen funcionamiento de las máquinas dentro de su organización, pudiendo detectar problemas de seguridad en sus sistemas, recopilar información para propósitos legales o de auditorías, y generar informes. En casos de ataque o comportamiento sospechoso en la red, el administrador puede finalizar conexiones de manera temporal o definitiva para IPs específicas.

- **SmartEvent**

Una arquitectura de seguridad multicapa, consiste en proteger servidores, hosts y aplicaciones de actividades perjudiciales, generando una gran cantidad de logs difíciles de interpretar. SmartEvent® es una herramienta que permite gestionar estos logs (ya sea organizándolos por tipo, usuario involucrado en la incidencia, política incumplida, grado de importancia, tipo de acción, etc.), en forma de gráficos o

pequeñas tablas fácilmente configurables por el administrador en un entorno intuitivo y amigable.

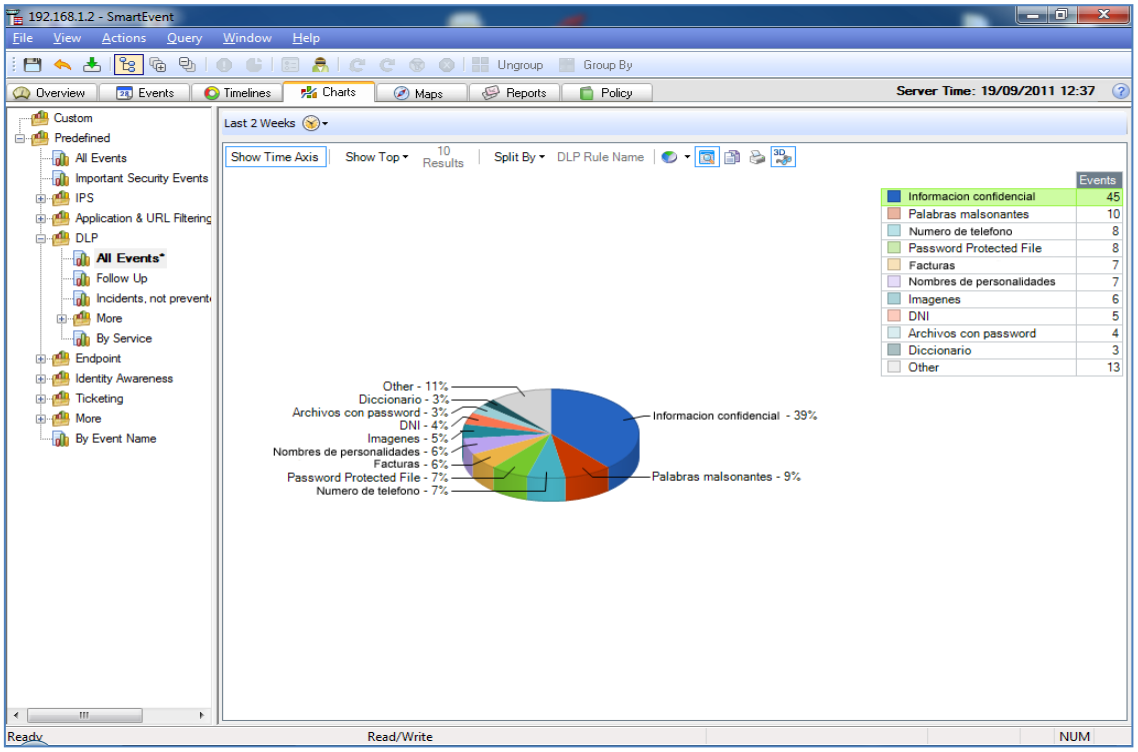

Ilustración 33: Gráfico de políticas incumplidas durante dos semanas

Ofrece un gran número de eventos predefinidos y fáciles de personalizar para conseguir un despliegue rápido de la información.

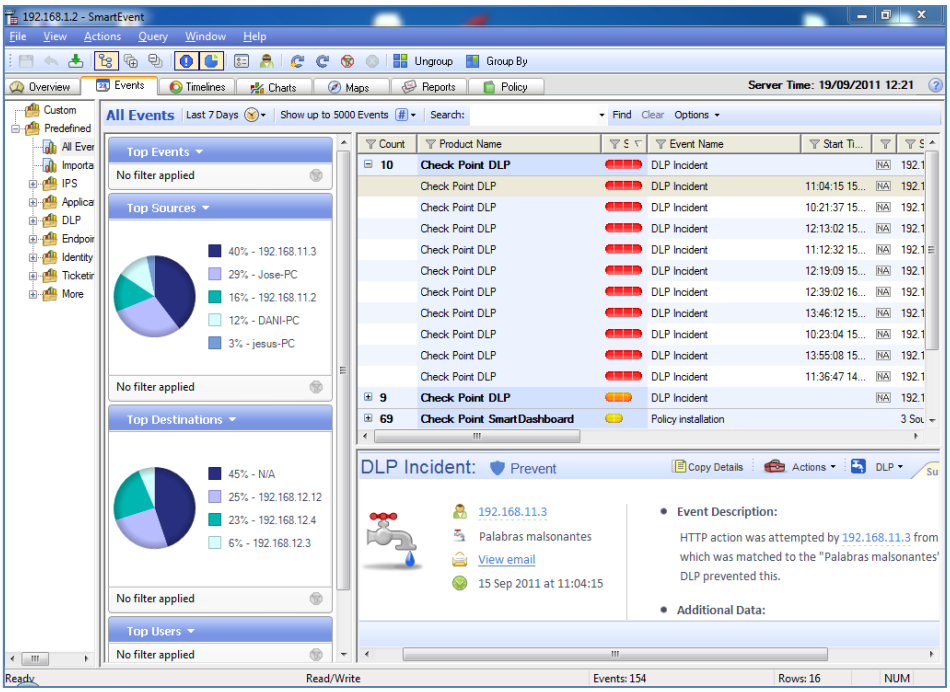

Ilustración 34: Listado de eventos de la última semana

SmartEvent no sólo minimiza la cantidad de datos que necesitan ser revisados, también prioriza amenazas en tiempo real.

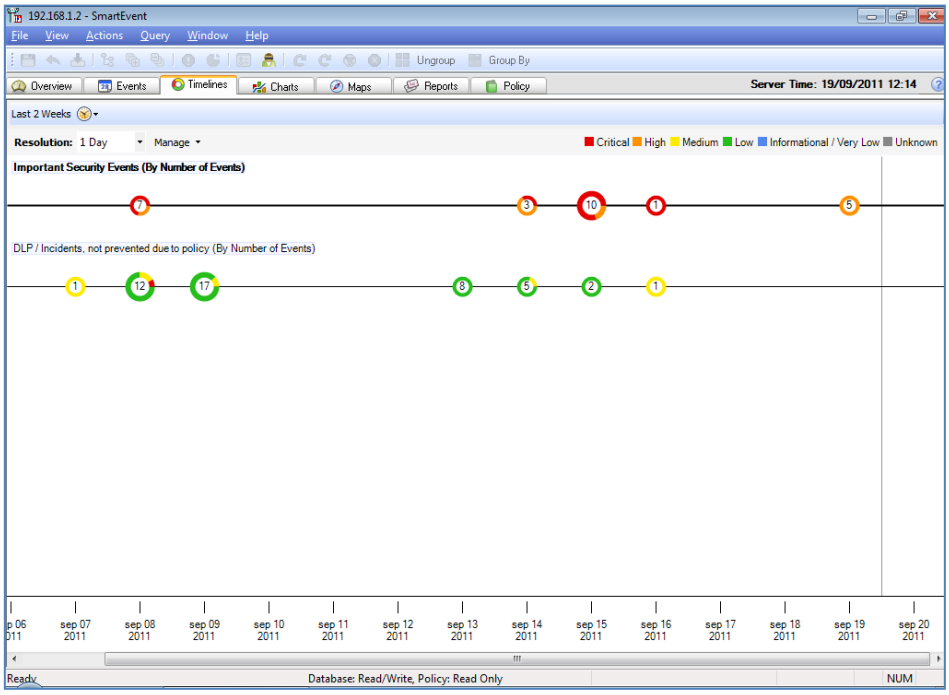

Ilustración 35: Gráfico temporal con número de incidencias y grado de importancia

Gracias a su arquitectura distribuida, *SmartEvent*® puede estar instalado en un único servidor, no obstante tiene la flexibilidad de repartir la carga de procesamiento y reducir la carga de la red. Los eventos que se generan son analizados y se les asigna un nivel de importancia. De ésta manera es posible detener el tráfico de datos en la puerta de enlace. Aparte de poder ver los incidentes en tiempo real, *SmartEvent*® proporciona un modo de auto aprendizaje de los patrones normales para una política y sugiere cambios en ella para evitar falsas alarmas.

- **SmartReporter**

SmartReporter es una solución fácil de usar para el análisis del tráfico y auditoría. Con esta herramienta podemos generar informes detallados o resumidos en el formato elegido (HTML o MHT) para todos los eventos registrados por Gateway Security Check Point, SecureClient e IPS.

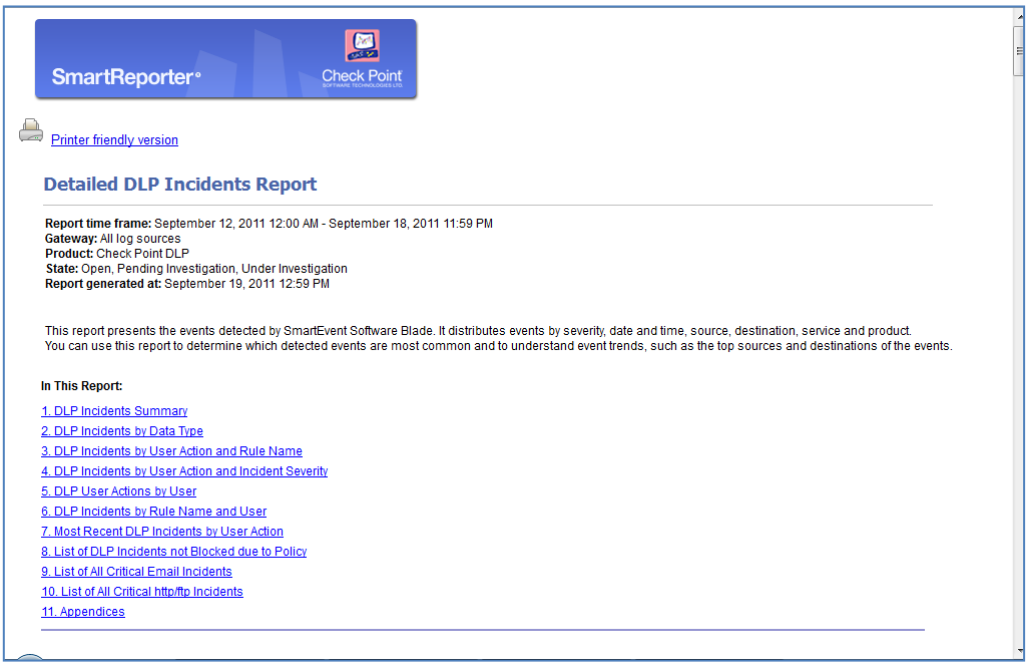

Ilustración 36: Ejemplo de encabezado de un informe

SmartReporter comprime los registros similares y escribe la lista comprimida de eventos en una base de datos relacional. Esta base de datos permite la generación rápida y eficiente de una amplia gama de informes, permitiendo elegir los plazos de

tiempo de los que se quiere extraer el informe (últimos 6 meses, última semana, un día específico, etc.).

Tenemos a nuestra disposición dos tipos de informes: estándar y express. Cada uno de ellos permitiéndonos cambiar opciones en la generación del informe tales como contenido del informe, formato de creación, filtros, horarios, etc.

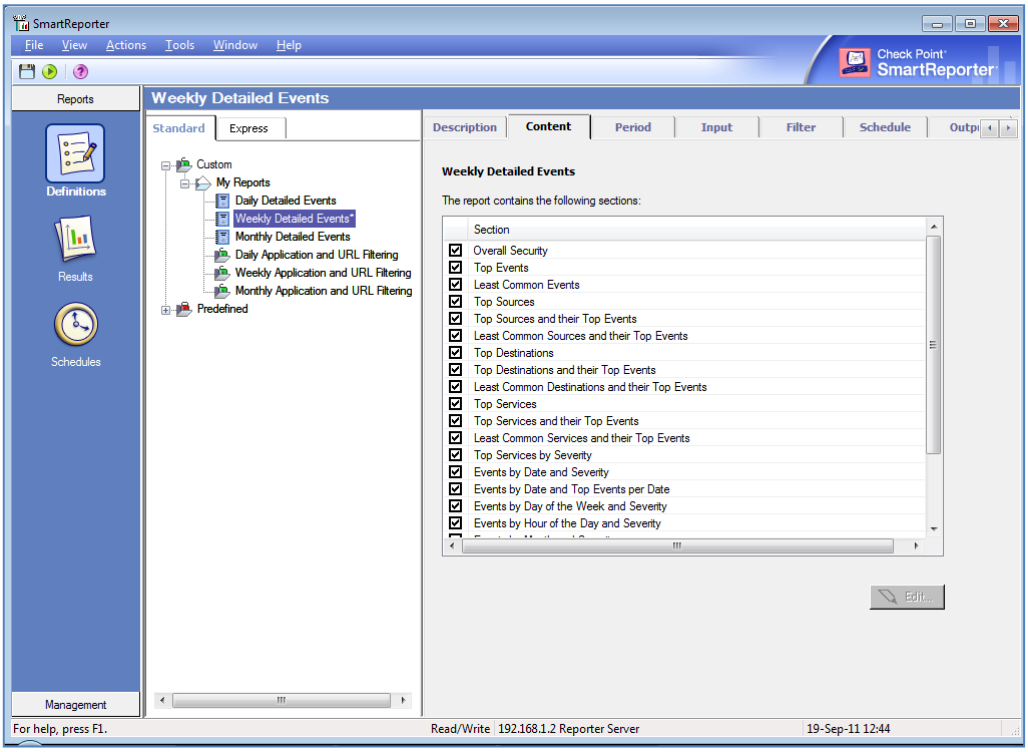

Ilustración 37: Opciones configurables del contenido de los informes

Los informes express se basan en datos recogidos por los contadores del sistema Check Point y por archivos de SmartView Monitor, a diferencia de los informes estándar que se basan en los log almacenados en las bases de datos. Además, esta herramienta se puede configurar para generar informes automáticamente en determinados horarios y fechas.

- **UserCheck**

UserCheck es la aplicación que informa al usuario de las acciones que quedan monitorizadas o bloqueadas, dependiendo del tipo de regla definida, mediante pop-up en su propio PC.

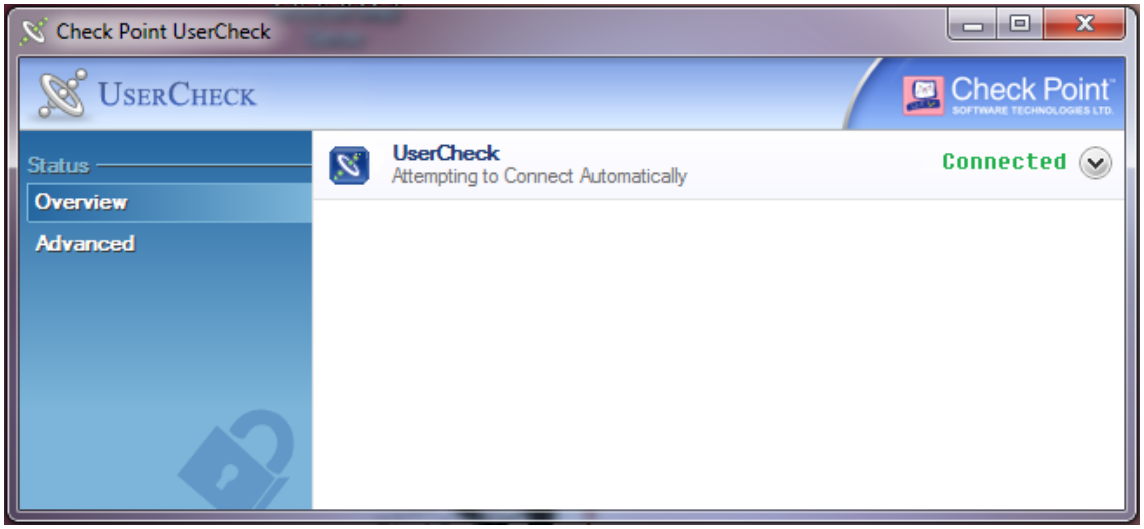

Ilustración 38: Estado de la conexión con el servidor DLP-1

- **SmartUpdate**

Con SmartUpdate vamos a tener facilidades para obtener ciertas actualizaciones software y licencias actualizadas a múltiples sistemas distribuidos a partir de una única consola de gestión. Esta herramienta nos asegura que las implementaciones de seguridad están siempre al día proporcionándonos un mayor control y eficiencia mientras se disminuye radicalmente los costes de mantenimiento de la gestión de instalaciones de seguridad global.

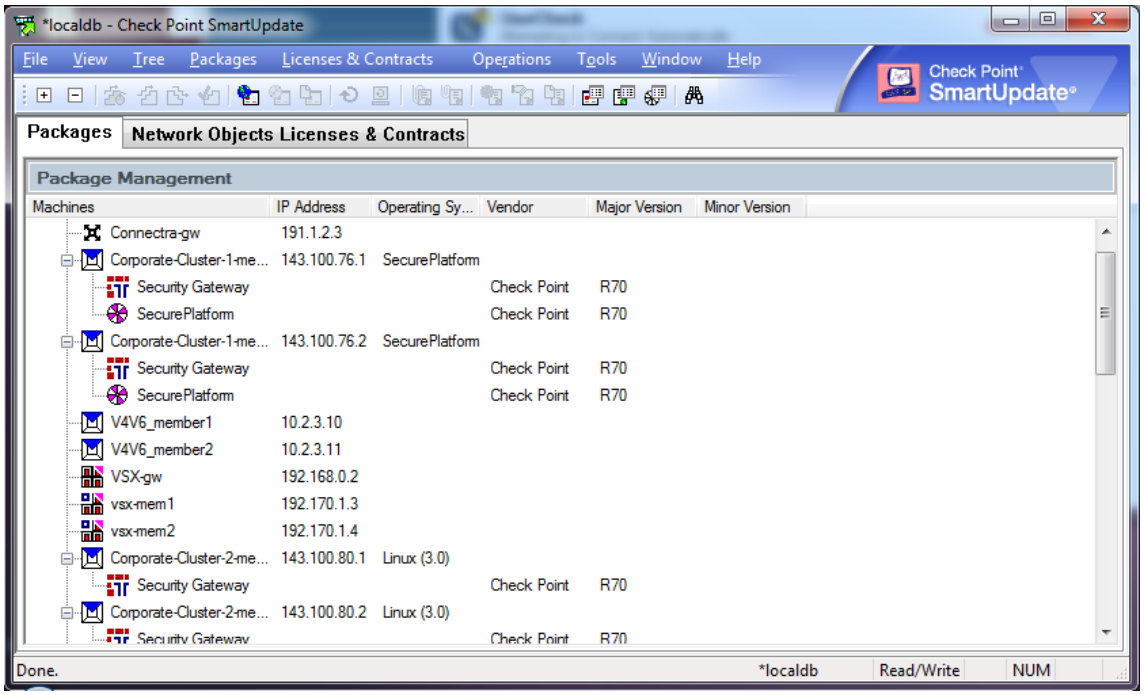

Ilustración 39: Pantalla principal de SmartUpdate

1.5.4. Data Types

Los Data Types en DLP son la parte más importante de la política de seguridad, ya que nos permiten definir las restricciones que queremos realizar en las comunicaciones que ocurrirán en nuestra red. Algunas de estas palabras restringidas pueden ser números de teléfono, cuentas bancarias, DNI, etc.

El SmartConsole de Check Point divide los tipos de datos en 8 categorías distintas:

- **Keywords:** Define varias palabras prohibidas e indicar el número mínimo de repeticiones que se permiten para que se infrinja la política.

- **Documents based on a corporate template:** Compara un archivo enviado con la plantilla definida. Si supera un porcentaje de similitud, se detectara. (Ej.: modelo de facturas, currículum vitae… etc.).

- **File attributes:** Define un tipo de archivo a rastrear.

- **Regular Expressions:** Generador de expresiones que detecta patrones de palabras o números como el DNI, número de teléfono, etc.

- **Compound data types:** Une dos o más tipos de datos en uno.

- **Weighted Keywords:** Asigna diferentes pesos de importancia a las palabras prohibidas. De esta forma, en cuanto llegamos a un límite numérico detectado en un mensaje, se registrará.

- **Words from a dictionary:** Importa un archivo con palabras prohibidas.

- **CPcode:** Lenguaje de programación de Check Point que nos permite programar nuestras propias reglas.

De los tipos de datos citados anteriormente, los más innovadores que proporciona DLP son Regular Expressions y CPcode ya que nos permite definir tipos de datos adaptados a nuestras necesidades. Por ejemplo para crear una expresión regular que captase el DNI, elegiríamos Pattern (regular expresión) en la ventana de nuevo tipo de dato y añadiríamos la expresión regular.

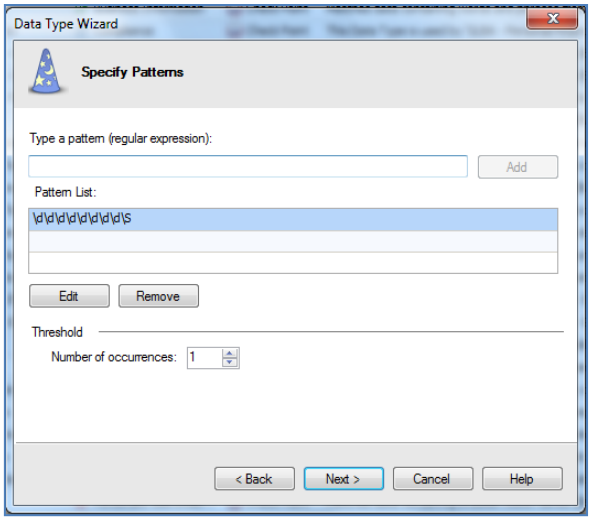

Ilustración 40: Expresión regular

1.5.4.1. CPcode

CPcode es un lenguaje de programación capaz de crear multitud de funciones personalizables. La principal ventaja del lenguaje de programación CPcode es muy similar a otros lenguajes de programación que existe y por lo tanto facilita el aprendizaje. Una vez que codificado se guarda con extensión ".cpc".

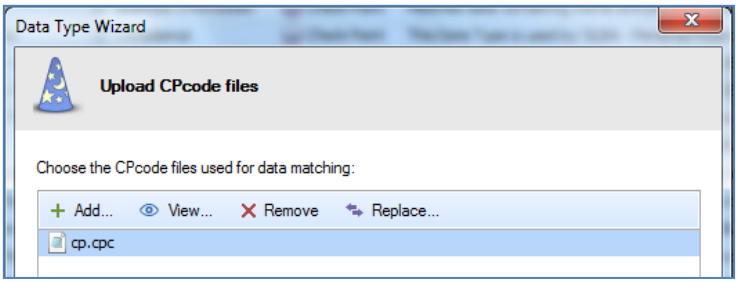

Ilustración 41: CPcode

Para probar el funcionamiento de CPCode, hemos desarrollado un pequeño Script que detecta si existe en el texto un número de empresa australiano (ABN). Este código sirve para identificar a cada trabajador en Australia y se compone de 11 dígitos numéricos.

La forma de saber si el código analizado es un ABN o no, es realizar el sumatorio de los 11 dígitos y dividir el resultado entre 89, si el resto es igual a 0 el código analizado será un ABN.

A continuación definimos los principales parámetros para la creación de una función en CPcode.

Tabla 3: Sintaxis CPcode

Función	**Detalles**
Sintaxis	func name {[statement]}

Parámetros	**Parámetros**	**Descripción**
	Name	nombre
	Statetement	Declaración
Valor de retorno	Se utiliza la sentencia return para devolver valores de una función. Los Valores de retorno puede ser cualquier tipo, excepto los punteros de función.	

Ejemplo	`func counter`
	`{`
	`if ($count)`
	`$count = $count +1;`
	`else`
	`$count = 1;`
	`}`	

En la siguiente figura se muestran una serie de Data Types definidos para algunas de las pruebas realizadas.

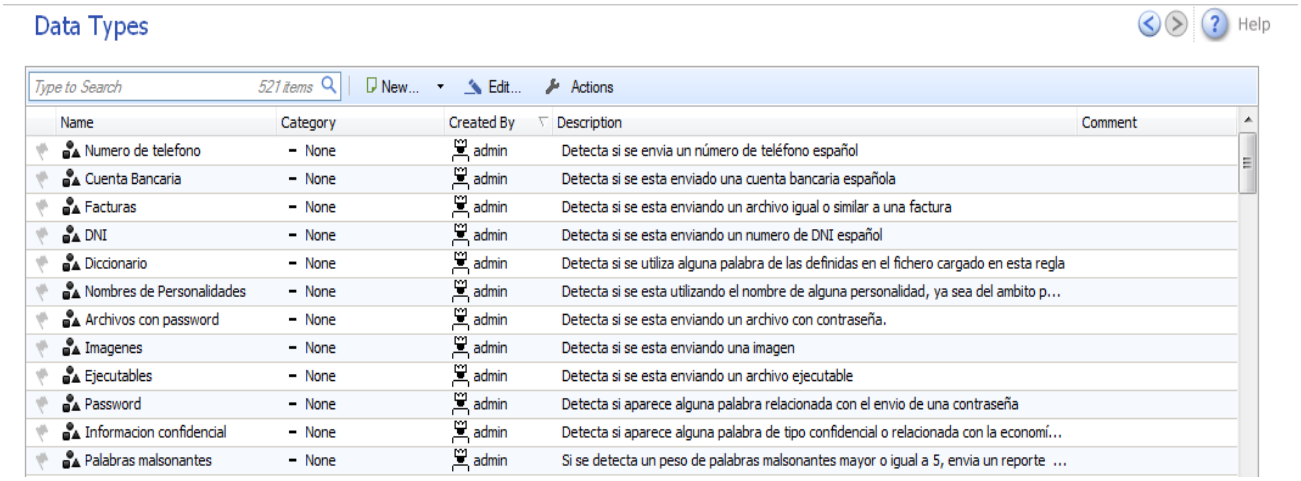

Ilustración 42: Data Types

BLOQUE 2:
Elección de escenario y montaje de un laboratorio de pruebas

En este bloque se hará una elección de un escenario apropiado para el montaje de un laboratorio de pruebas. Este escenario será escogido de una lista de propuestas posibles descritas a fondo en el *TFG de Sara Carral Ramos 'Análisis, funcionalidades y propuestas de implantación de la herramienta CheckPoint DLP-1 2571'* [2]. Se describirán los motivos por los cuales hemos escogido uno de ellos en concreto para llevar a cabo las pruebas.

Por último, en este bloque se especificará también el procedimiento paso a paso llevado a cabo para la creación de un laboratorio de pruebas que utilizaremos en el siguiente bloque, así como el material necesario para llevar a cabo las mismas.

2.1. Elección de escenario

Para poder realizar las distintas pruebas que se plantearán en el siguiente bloque es necesario configurar un entorno adecuado.

Para las pruebas que queremos realizar se necesitará configurar un servidor de correo, un servidor FTP y un servidor web. Para una mayor simplificación de instalación se utilizará una misma máquina para alojar los tres servidores.

Se necesitará también una máquina que tenga instalado el sistema operativo propietario de Check Point Gaia versión R75.40 y un PC que haga la función de

Management, desde el cual se configurarán las políticas y desde el cual se hará el seguimiento a través de las herramientas de SmartConsole. En éste caso, tal y como se hace en un gran número de empresas, estas dos máquinas estarán en el mismo PC. Por supuesto el SO Gaia se alojará en una máquina virtual.

Por último, se necesitará al menos una máquina cliente mediante la cual acceder a los servicios prestados por el servidor. En ella se prepararán los correos electrónicos, archivos para subir al FTP y desde ella se accederá a la web alojada en el servidor.

Todos estos elementos se ven representados en la siguiente ilustración en la cual se detallan también las conexiones entre ellos.

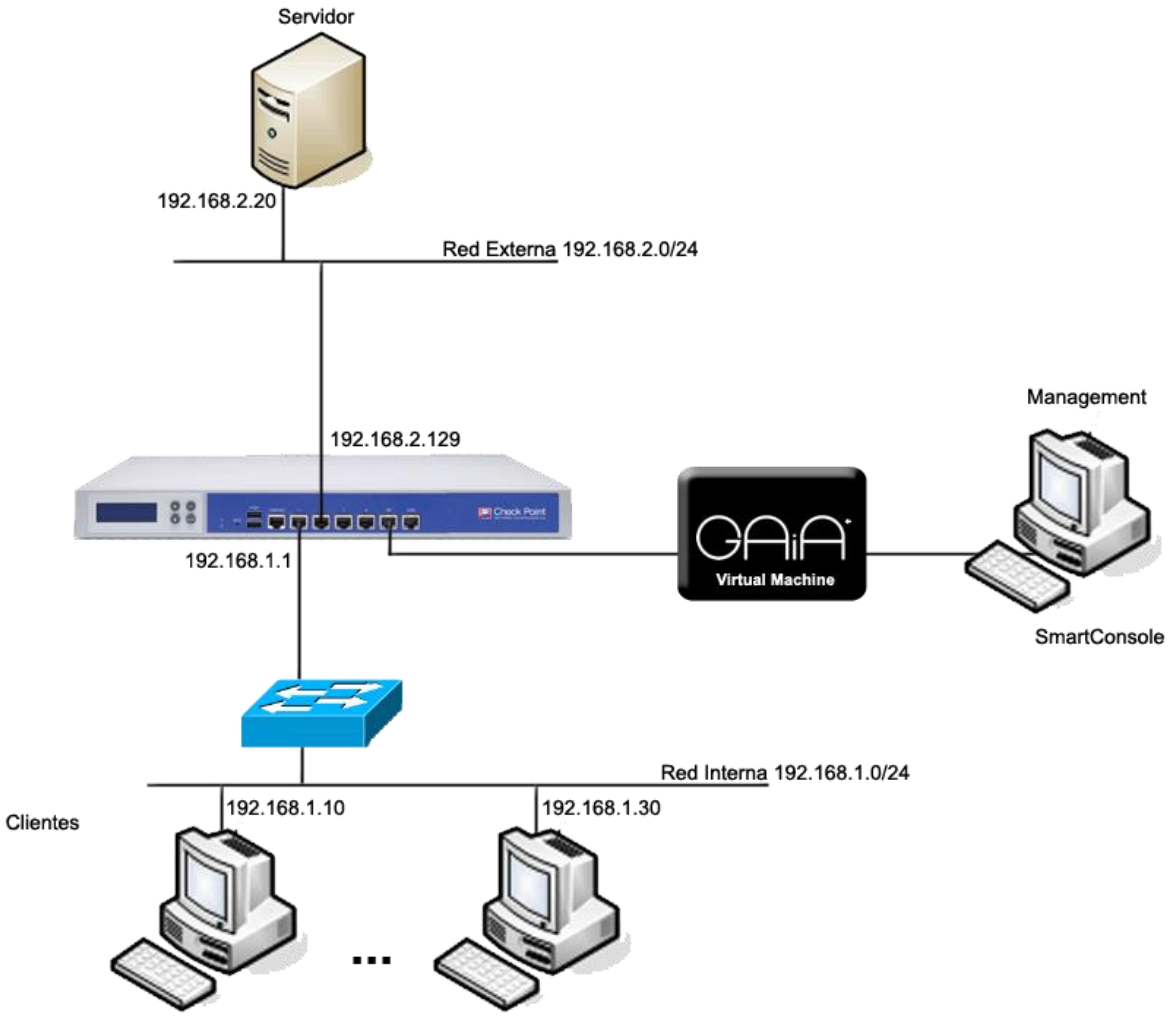

Ilustración 43: Escenario del laboratorio de pruebas

A continuación se va a detallar el sistema operativo y el software utilizado para cada una de las máquinas que componen el escenario.

Tabla 4: Software utilizado

Máquina	Sistema operativo	Software utilizado	
		Tipo	**Programas**
Cliente	Windows XP	Navegador	Firefox
		Cliente FTP	Filezilla y cmd
		Cliente de correo	Foxmail
Servidor	Windows XP SP3	Servidor web	XAMPP
		Servidor FTP	Filezilla Server
		Servidor correo	ArGoSoft Mail Server
Management	Windows 7	Máquinas virtuales	VMware Workstation 8.0
		Navegador	Google Chrome
		Gestión	SmartConsole
Consola de gestión	Check Point Gaia R75.40	Consola	Propietaria

2.2. Creación del laboratorio de pruebas

Para una mejor visión del funcionamiento de la herramienta sin la necesidad de montar una infraestructura demasiado compleja implementaremos el escenario presentado en el apartado anterior en una misma máquina haciendo uso de máquinas virtuales, utilizaremos la máquina de gestión para alojar las máquinas virtuales.

A continuación se va a detallar el proceso necesario a llevar a cabo para la configuración de las redes y la creación de las máquinas virtuales.

2.2.1. Configuración de las redes

Vamos a mostrar una tabla de direccionamiento donde se indica la IP de cada uno de los interfaces así como su máscara de subred y puerta de enlace por defecto.

Tabla 5: Direccionamiento de los nodos

PC o VM	Interfaz	Dirección IP	Puerta enlace
Management	Conexión de área local	Asignada por DHCP	-
	VMnet1	192.168.1.3 / 24	192.168.1.1
	VMnet2	192.168.2.3 / 24	192.168.2.1
Servidor	Conexión de área local	192.168.2.20 / 24	192.168.2.129
Cliente	Conexión de área local	192.168.1.10 / 24	192.168.1.1
Check Point Gaia R75.40	eth0	192.168.1.1 / 24	-
	eth1	192.168.2.129 / 24	-
	lo	127.0.0.1 / 24	-

2.2.1.1. Ajustes de interfaces en Gaia R75.40

Una vez que hayamos instalado el sistema operativo Gaia 75.40 (ver apartado 2.2.3.) accedemos al Gaia Portal (interfaz web de gestión) y configuramos las IPs de los interfaces para que queden de la siguiente manera.

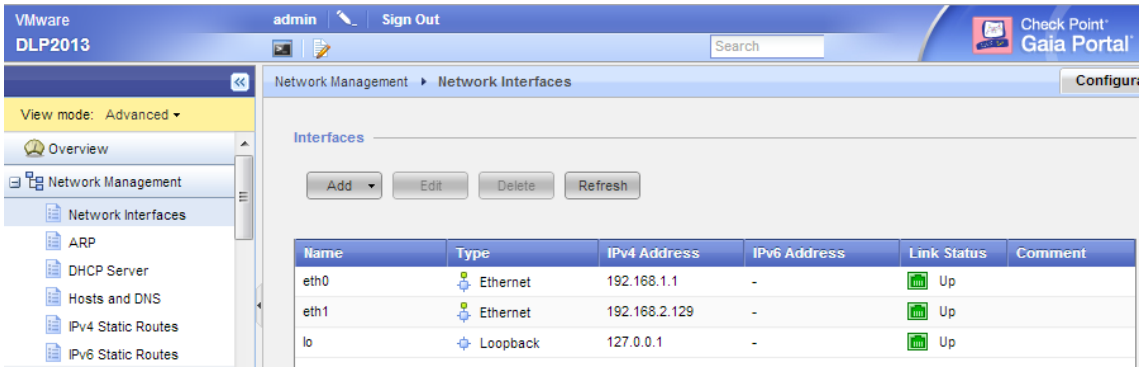

Ilustración 44: Interfaces en Gaia Portal

Tal y como vemos en la imagen debemos entrar en el apartado *Network Interfaces* en el menú de la izquierda. Seleccionamos el interfaz al que deseemos cambiar la IP, hacemos clic en *Edit* y establecemos la dirección que deseemos.

Los interfaces que definimos aquí son los que servirán de puerta de enlace predeterminada a los direccionamientos IP de las máquinas virtuales con Windows XP. La máquina servidor establecerá la puerta de enlace la dirección 192.168.2.129 mientras que la máquina cliente establecerá como puerta de enlace la dirección 192.168.2.129, tal y como veremos en los siguientes apartados.

2.2.1.2. Ajustes de Virtual Network Editor

Para la creación de dos subredes a utilizar por dos máquinas virtuales distintas hemos de hacer ciertos ajustes en los direccionamientos de la herramienta Virtual Network Editor.

Virtual Network Editor tiene como finalidad la creación de tantos interfaces como necesitemos para utilizar posteriormente en máquinas virtuales creadas con

VMware Workstation. Este programa se encuentra generalmente en el menú *Inicio* → *Todos los programas* → *VMware* → *Virtual Network Editor*.

Ya que lo que queremos es crear dos subredes distintas hemos de establecer los siguientes ajustes para el interfaz *VMnet1* del PC Management.

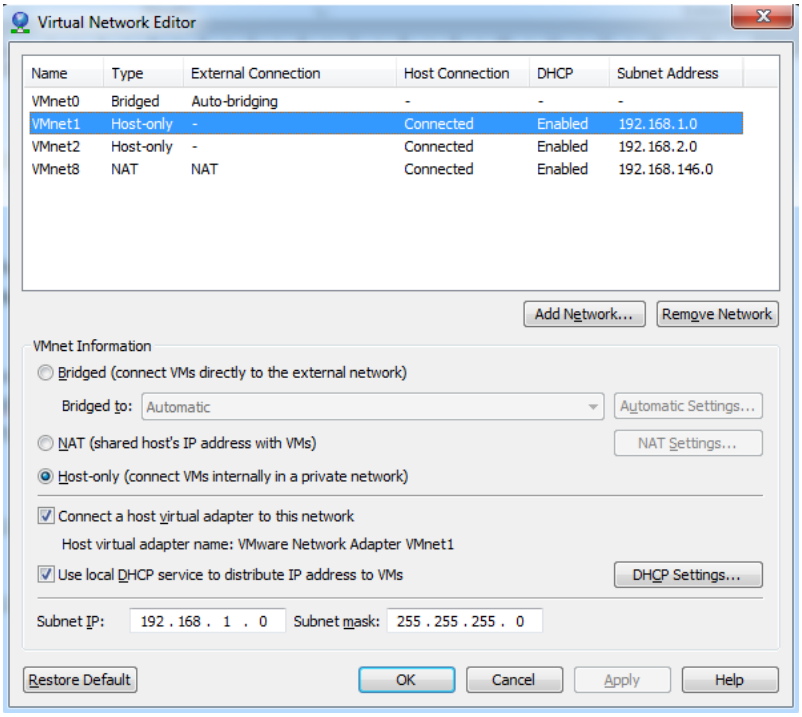

Ilustración 45: Direccionamiento VMware1 en VNE

Y de manera análoga hemos de establecer los siguientes ajustes para el interfaz VMware2.

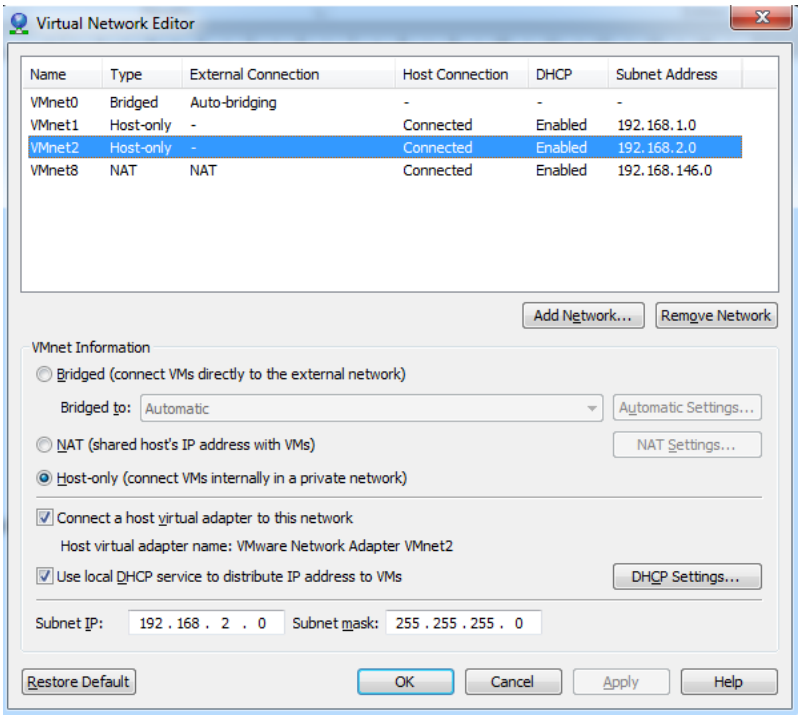

Ilustración 46: Direccionamiento VMware2 en VNE

2.2.1.3. Interfaz VMnet1 de Management

Para dotar de una IP acorde a la subred definida en los interfaces de VMware hemos de establecer una IP de esa misma subred al adaptador de red *VMnet1*. Para ello, hemos de situarnos en *Panel de control→Redes e Internet→Conexiones de red*, hacemos doble clic en el adaptador *VMnet1* y hacemos clic en *Propiedades*. A continuación hacemos doble clic en *Protocolo de Internet versión 4 (TCP/IPv4)* y establecemos la IP que deseemos, en nuestro caso tiene que quedar de la siguiente manera.

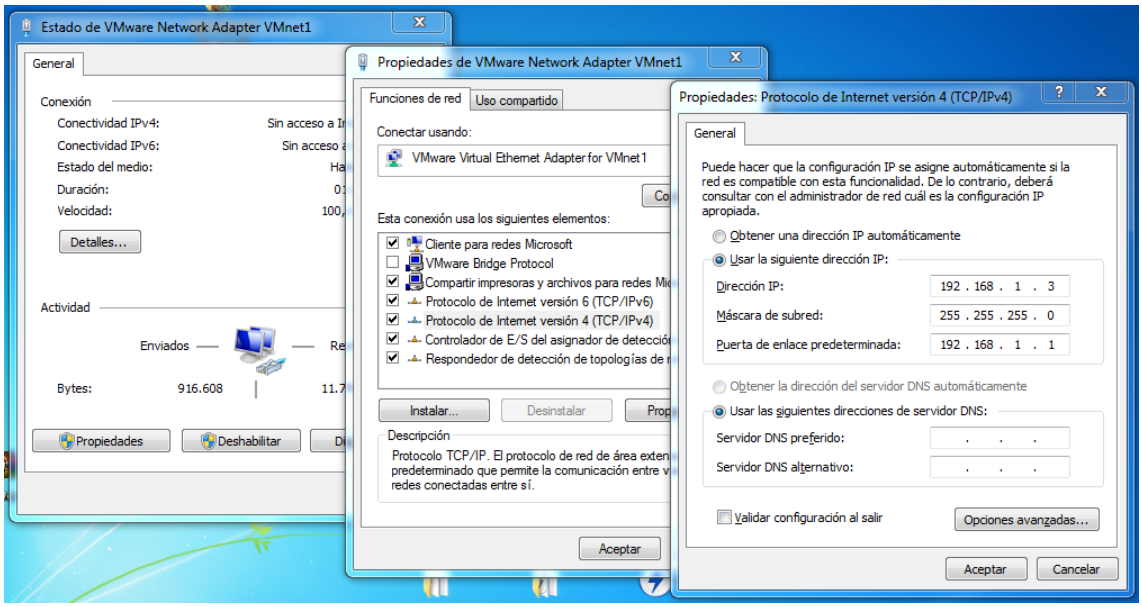

Ilustración 47: Direccionamiento VMnet1 en W7

2.2.1.4. Interfaz VMnet2 de Management

De forma análoga al apartado anterior hemos de establecer una IP dentro de la subred definida en el adaptador *VMnet2*. Para ello actuamos de la misma manera que en el apartado anterior pero definiendo una IP válida para la segunda subred.

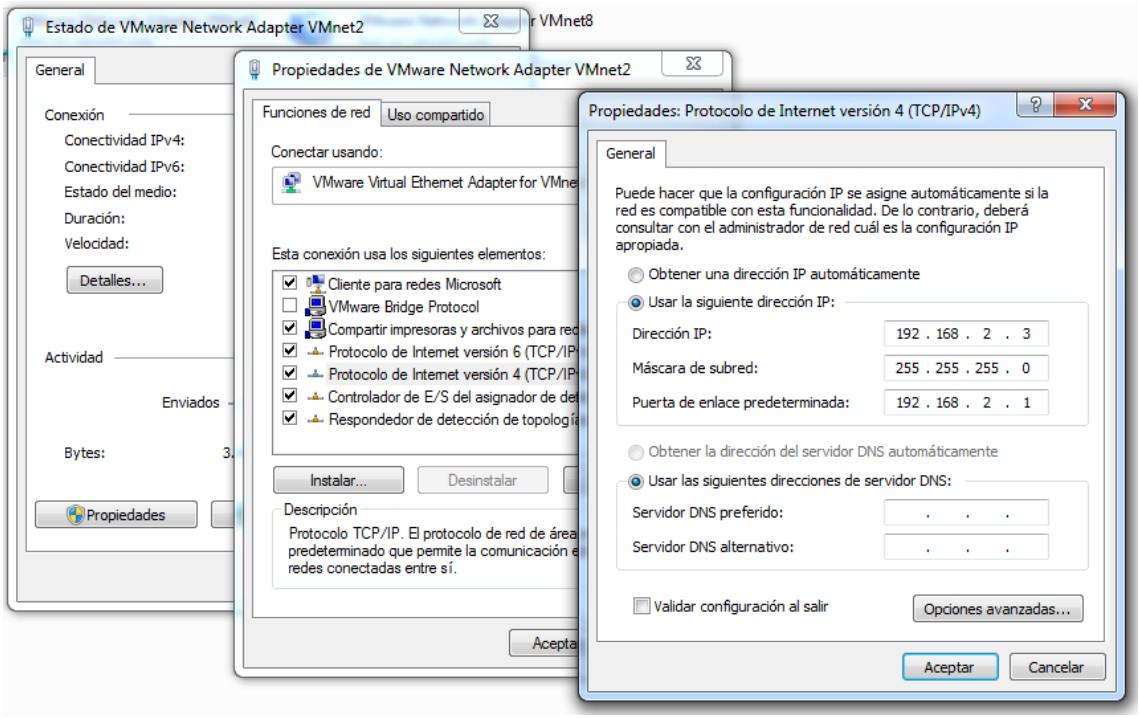

Ilustración 48: Direccionamiento Vnet2 en W7

2.2.1.5. Conexión de área local de Cliente

Para dar una IP válida para la subred en la que se encuentra el cliente hemos de definirla manualmente acorde con la tabla de direccionamiento vista en el punto 2.2.3. Para ello tenemos que situarnos en *Panel de control→Conexiones de red*, hacemos doble clic en el adaptador *Conexión de área local* y hacemos clic en *Propiedades*. A continuación hacemos doble clic en *Protocolo de Internet (TCP/IP)* y establecemos la IP que deseemos, en nuestro caso tiene que quedar de la siguiente manera.

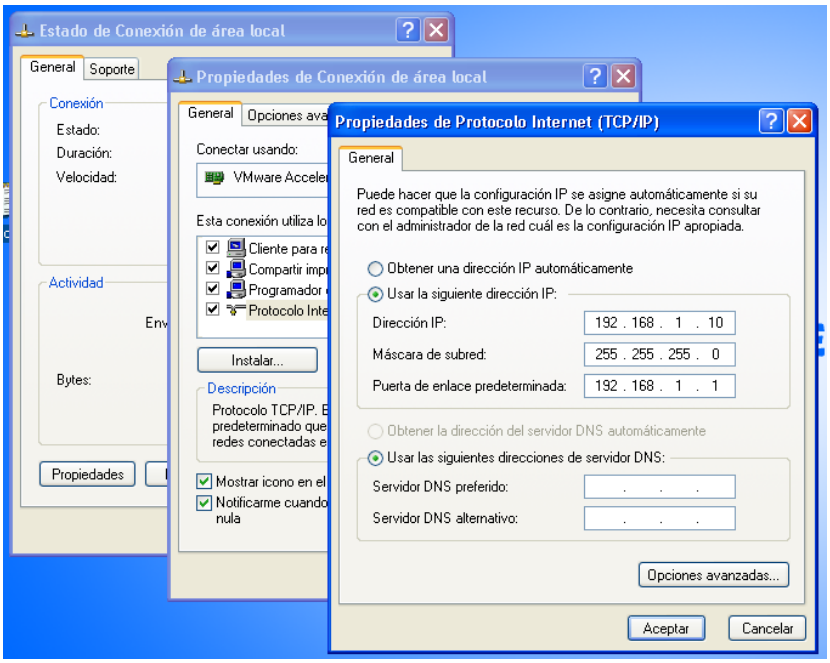

Ilustración 49: Direccionamiento cliente WinXP

2.2.1.6. Conexión de área local de Servidor

Por ultimo tenemos que dar una IP válida en su subred para el servidor. Establecemos la indicada en la tabla de direccionamiento del apartado 2.2.3. Para ello tenemos que situarnos en *Panel de control→Conexiones de red*, hacemos doble clic en el adaptador *Conexión de área local* y hacemos clic en *Propiedades*. A continuación hacemos doble clic en *Protocolo de Internet (TCP/IP)* y establecemos la IP que deseemos, en nuestro caso tiene que quedar de la siguiente manera.

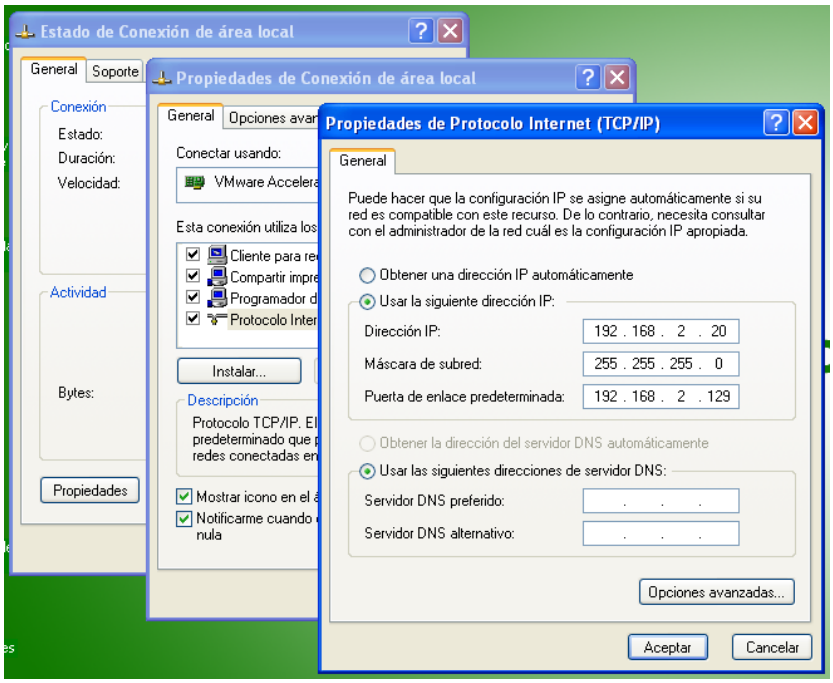

Ilustración 50: Direccionamiento servidor WinXP

2.2.2. Creación de máquinas virtuales

Necesitaremos una serie de pasos para la creación de las máquinas virtuales necesarias para el alojamiento de cada uno de los nodos necesarios para la implementación del laboratorio de pruebas. A continuación se hace una descripción detallada del proceso para cada una de ellas.

2.2.2.1. Máquina virtual GAiA R75.40

- Abrimos VMware Workstation 8.0 y pinchamos en Create a New Virtual Machine.

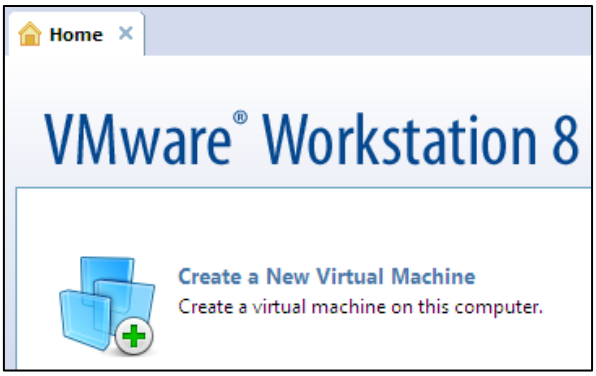

Ilustración 51: Creación Gaia VM paso 1

- Seleccionamos el tipo de configuración, en nuestro caso seleccionaremos Custom.

Ilustración 52: Creación Gaia VM paso 2

- Seleccionamos la imagen del CD que contiene la instalación del sistema operativo y hacemos clic en *Next*.

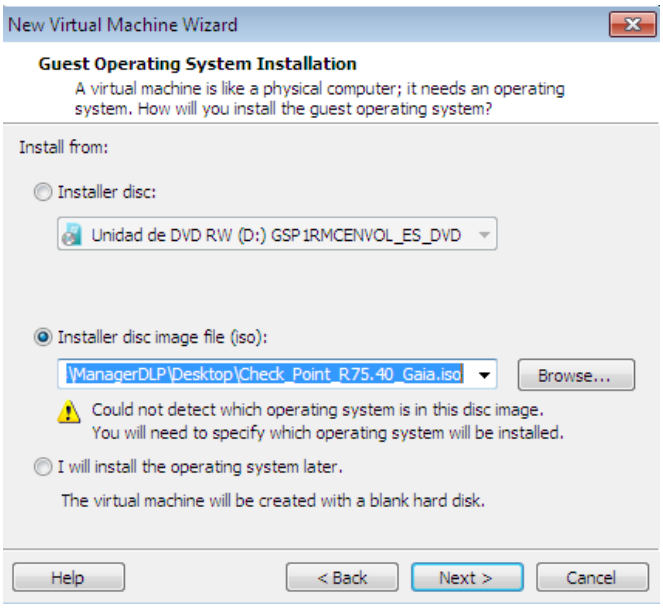

Ilustración 53: Creación Gaia VM paso 3

- Seleccionamos la cantidad de memoria RAM con la que dotaremos a la máquina virtual. En este caso bastará con seleccionar 512 MB. Hacemos clic en *Next*.

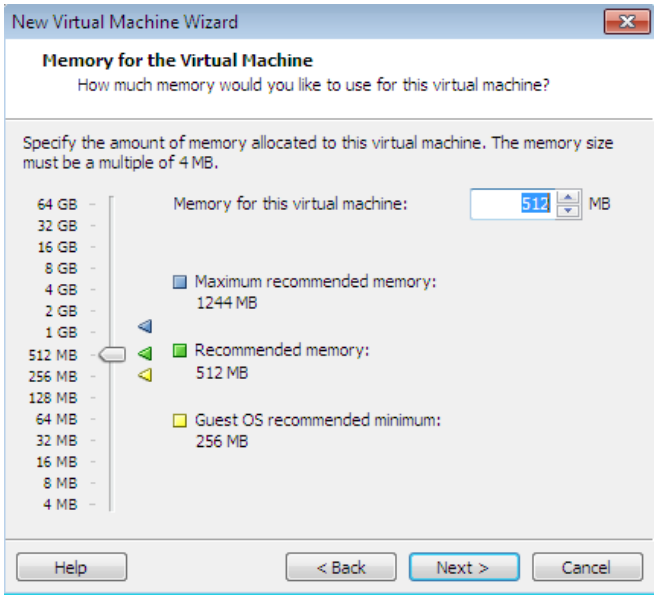

Ilustración 54: Creación Gaia VM paso 4

- Seleccionamos el tipo Use host-only networking. Hacemos clic en *Next*.

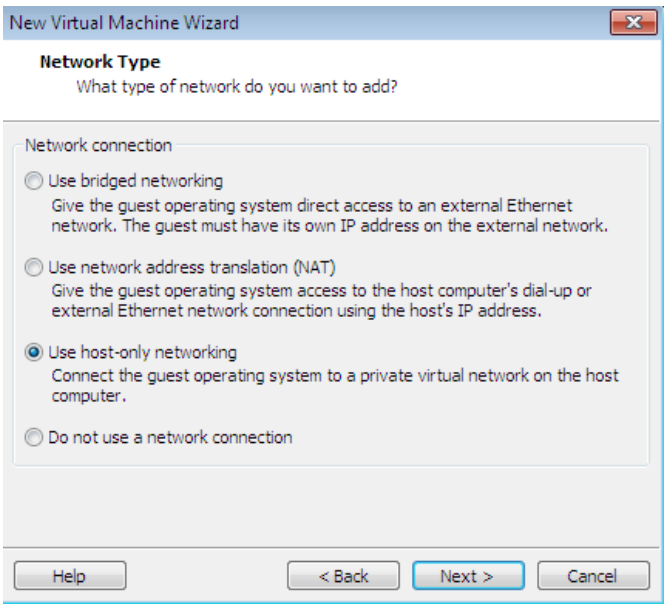

Ilustración 55: Creación Gaia VM paso 5

- Seleccionamos la capacidad del disco duro virtual. En este caso necesitaremos como mínimo 60 GB. Hacemos clic en *Next*.

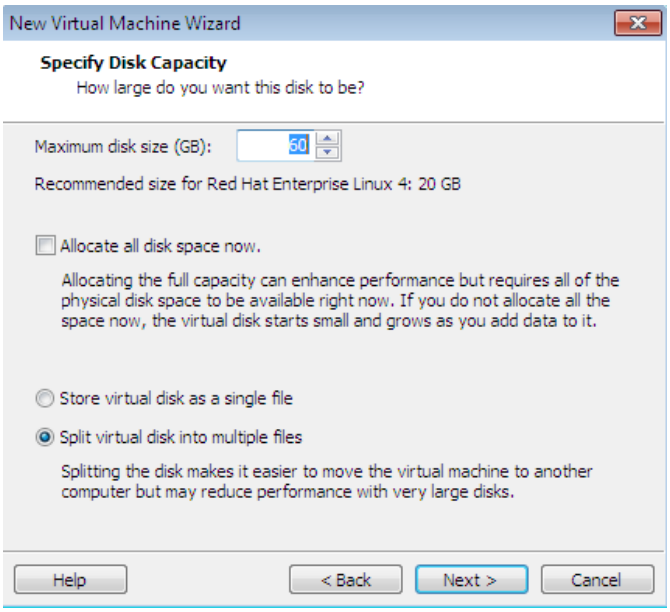

Ilustración 56: Creación Gaia VM paso 6

- Revisamos los ajustes finales y hacemos clic en *Finish*. Nuestra máquina virtual estará preparada para instalar Gaia en el primer arranque.

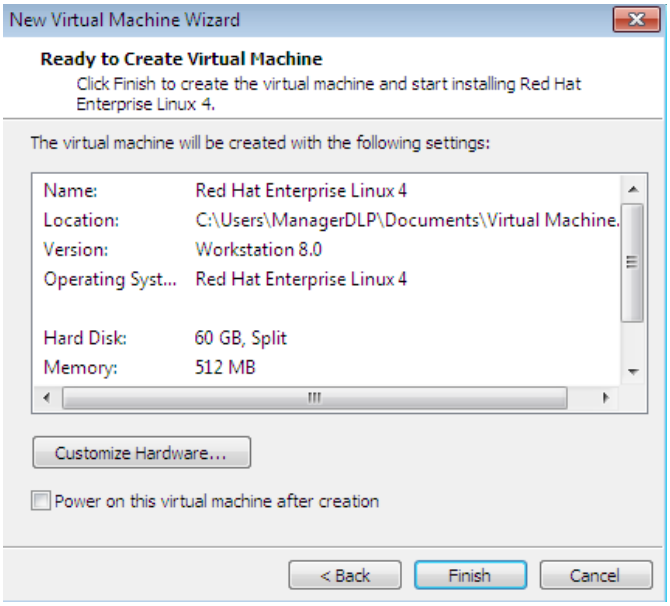

Ilustración 57: Creación Gaia VM paso 7

2.2.2.2. Máquina virtual Cliente y Servidor

La creación de ambas máquinas (cliente y servidor) requiere una serie de pasos similares. Son los que se detallan a continuación.

- Abrimos VMware Workstation 8.0 y pinchamos en Create a New Virtual Machine.

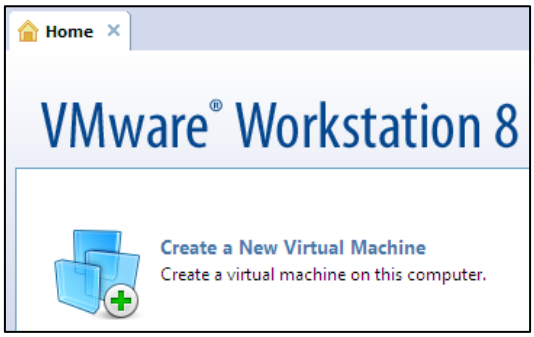

Ilustración 58: Creación VM Cliente/Servidor paso 1

- Seleccionamos el tipo de configuración, en nuestro caso seleccionaremos Custom.

Ilustración 59: Creación VM Cliente/Servidor paso 2

- Seleccionamos la imagen del CD que contiene la instalación del sistema operativo y hacemos clic en *Next*.

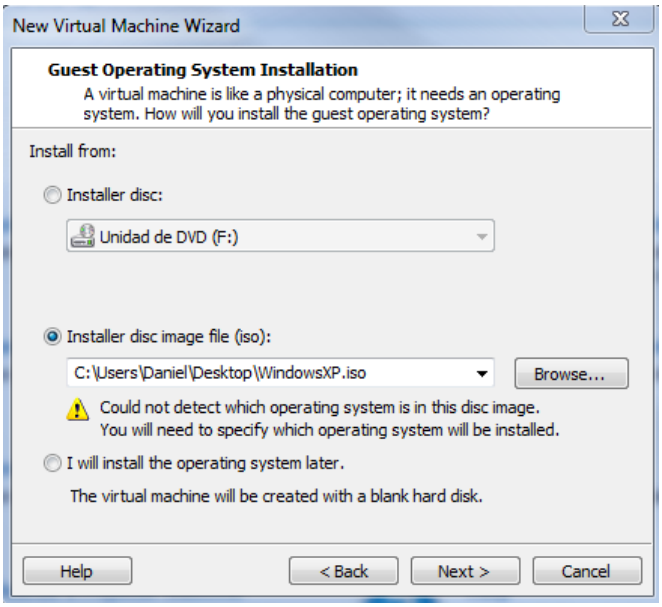

Ilustración 60: Creación VM Cliente/Servidor paso 3

- Seleccionamos la cantidad de memoria RAM con la que dotaremos a la máquina virtual. En este caso bastará con seleccionar 512 MB. Hacemos clic en *Next*.

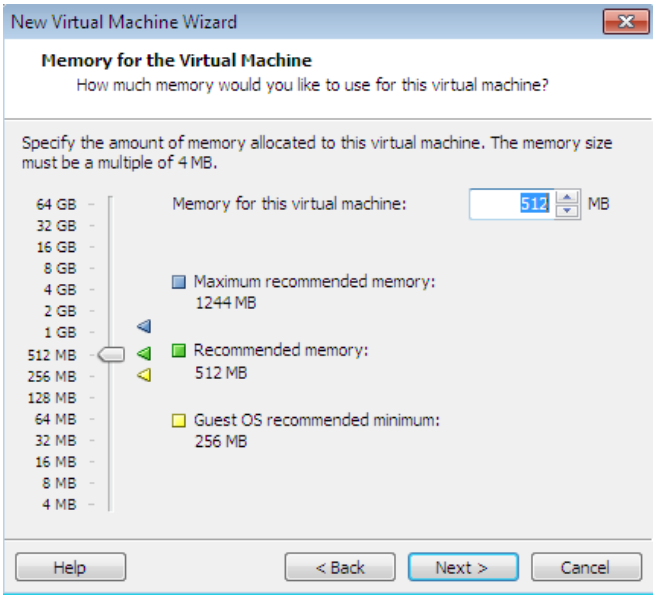

Ilustración 61: Creación VM Cliente/Servidor paso 4

- Seleccionamos el tipo Use host-only networking. Más tarde tendremos que editarlo para seleccionar el adaptador que está en la subred interna (en caso del cliente) o el que está en la red externa (para el servidor). Hacemos clic en *Next*.

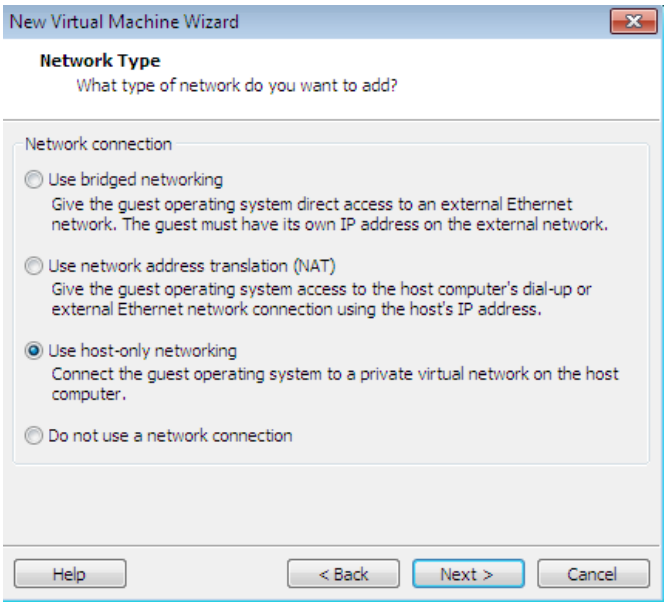

Ilustración 62: Creación VM Cliente/Servidor paso 5

- Seleccionamos la capacidad del disco duro virtual. En este caso necesitaremos como mínimo 15 GB. Hacemos clic en *Next*.

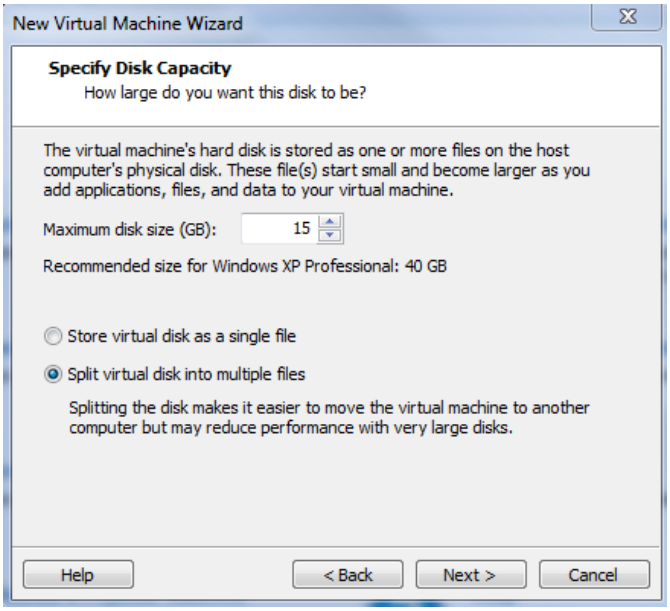

Ilustración 63: Creación VM Cliente/Servidor paso 6

- Revisamos los ajustes finales y hacemos clic en *Customize Hardware* para editar los ajustes del servidor.

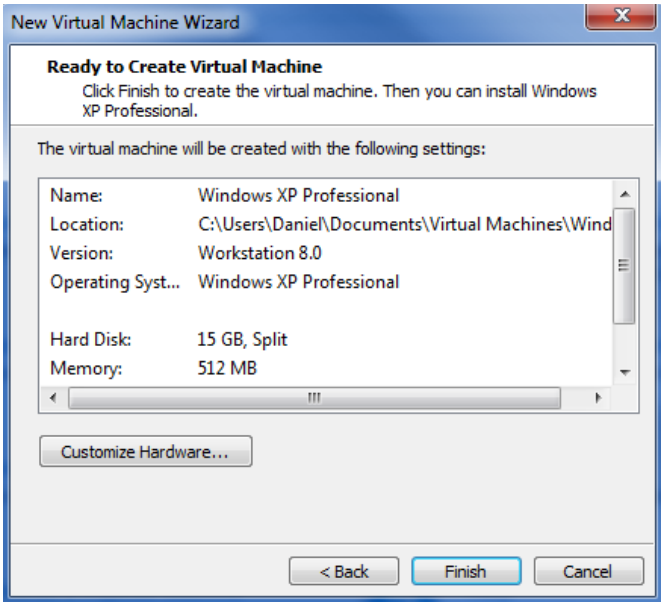

Ilustración 64: Creación VM Cliente/Servidor paso 7

- Por último, debemos elegir el adaptador *VMnet1* para la máquina cliente y el *VMnet2* para la máquina servidor.

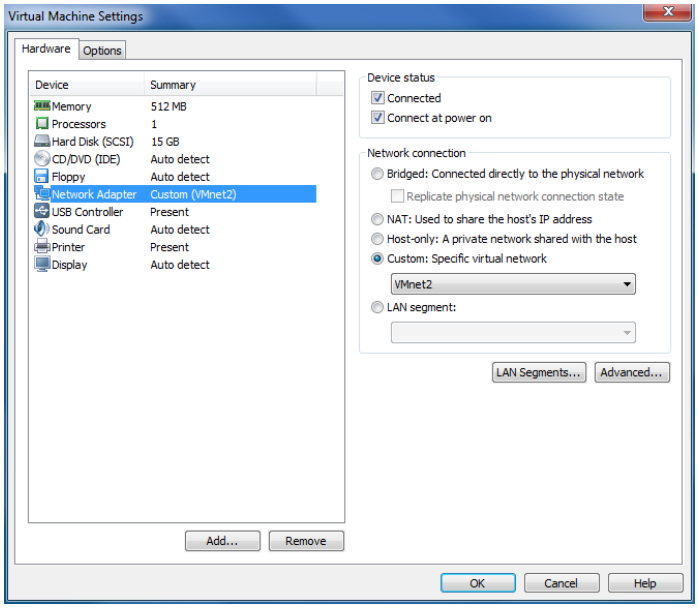

Ilustración 65: Creación VM Cliente/Servidor paso 8

2.2.3. Instalación del SO Gaia R75.40

Al arrancar por primera vez la máquina virtual en la que instalaremos Gaia R75.40 se iniciará automáticamente el proceso de instalación del mismo.

- Seleccionamos la opción *Install Gaia on this system*

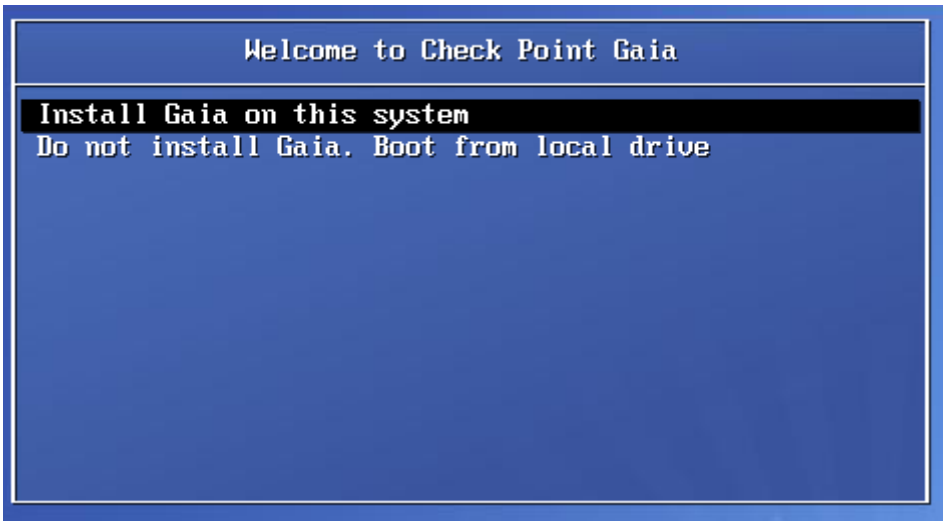

Ilustración 66: Instalación Gaia paso 1

- La primera pantalla nos advierte de que estamos a punto de iniciar el proceso de instalación del sistema operativo Gaia R75.40. Seleccionamos OK para continuar.

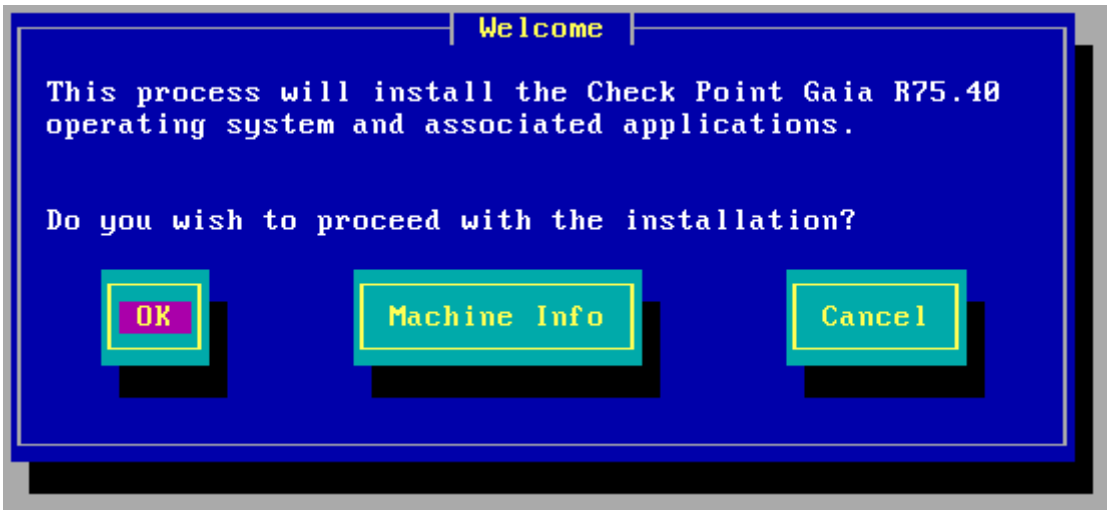

Ilustración 67: Instalación Gaia paso 2

- Seleccionamos la configuración de teclado que queremos utilizar, en nuestro caso Spanish.

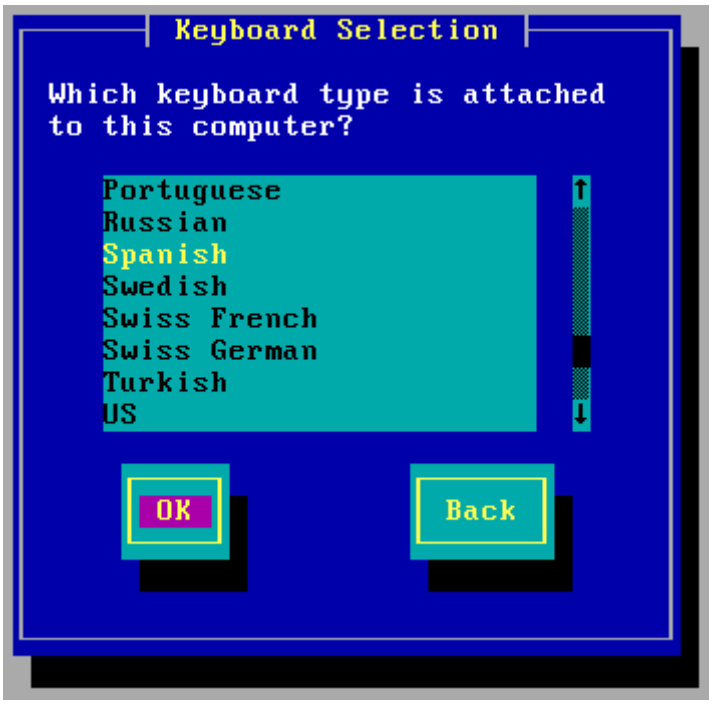

Ilustración 68: Instalación Gaia paso 3

- Elegimos la distribución de las particiones. Aquí basta con dejarlo todo por defecto y seleccionamos OK.

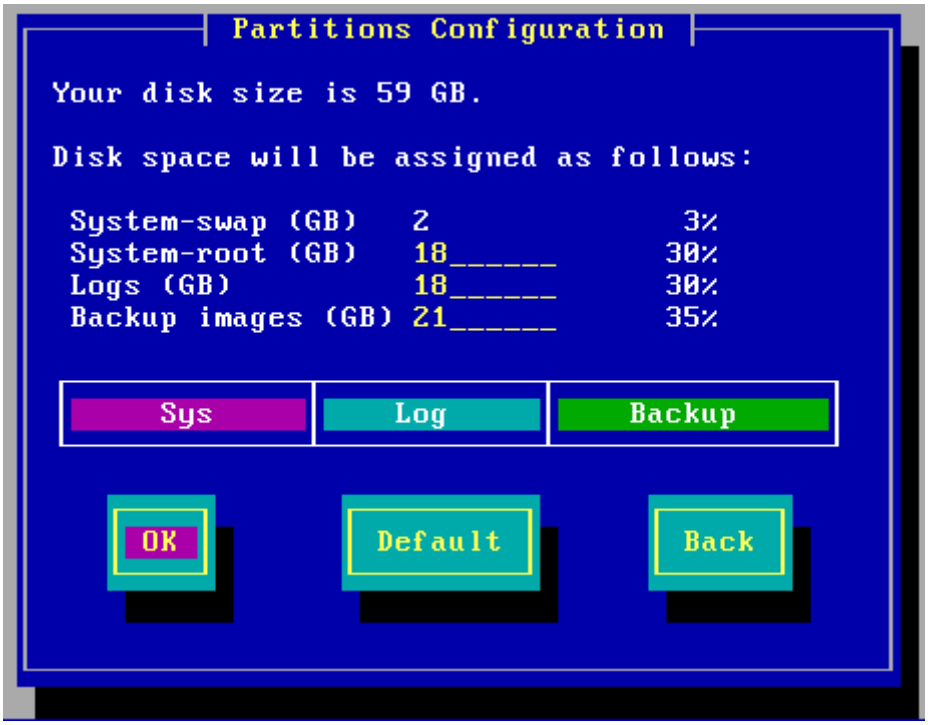

Ilustración 69: Instalación Gaia paso 4

- Debemos fijar una contraseña para el acceso a la cuenta de administrador. En nuestro caso la contraseña elegida es TGF2013.

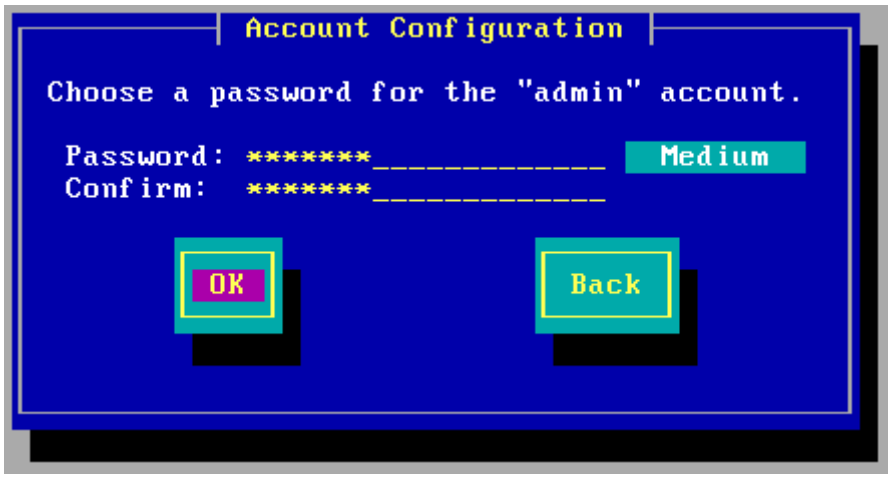

Ilustración 70: Instalación Gaia paso 5

- A continuación indicamos la IP mediante la que entraremos a la configuración a través de la interfaz GUI.

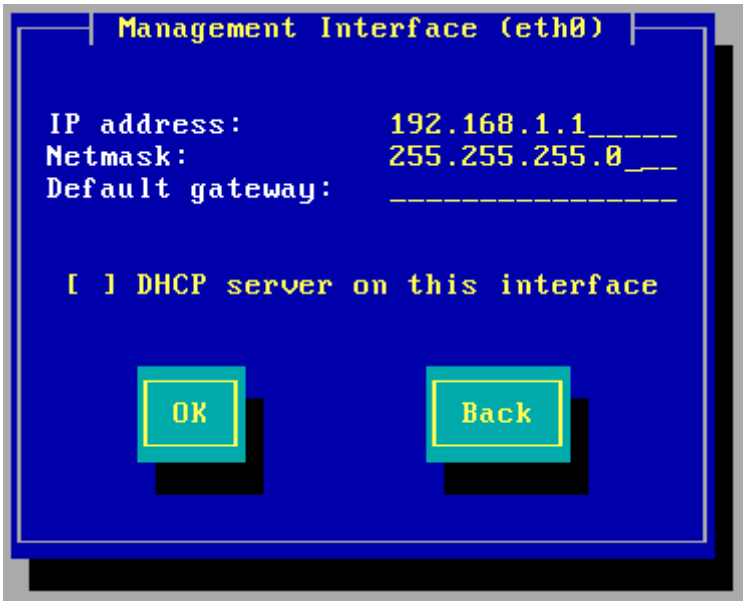

Ilustración 71: Instalación Gaia paso 6

- El proceso de instalación nos advierte de que el disco duro será formateado. Seleccionamos OK para continuar.

Ilustración 72: Instalación Gaia paso 7

- Esperamos unos minutos para que se complete la instalación del sistema operativo.

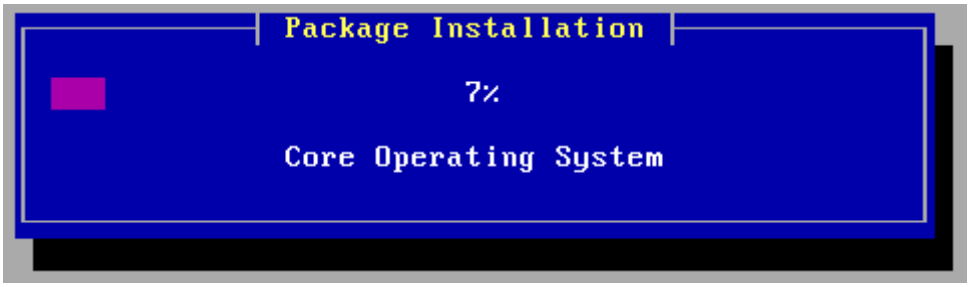

Ilustración 73: Instalación Gaia paso 8

- Al finalizar el proceso de instalación se nos indica la URL a la que debemos acceder para iniciar la configuración mediante la interfaz GUI.

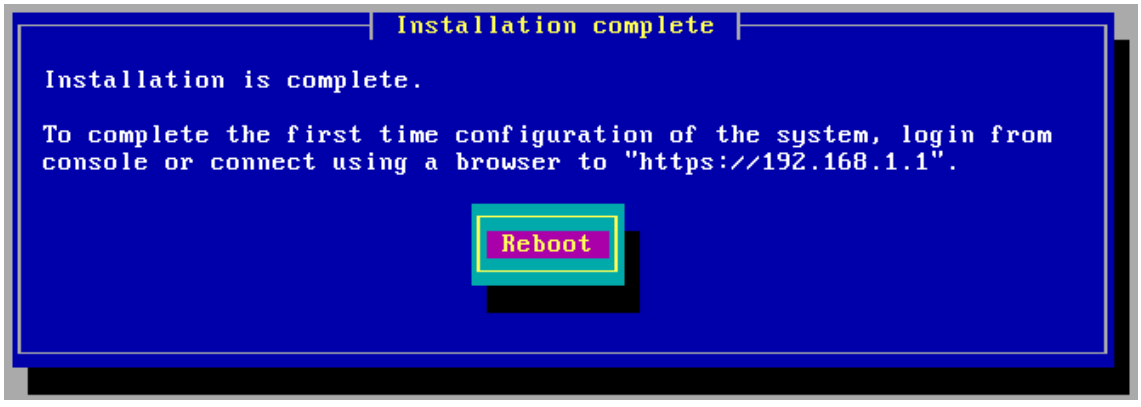

Ilustración 74: Instalación Gaia paso 9

- Una vez finalizado el proceso de reinicio el sistema operativo nos pedirá el nombre de usuario y password para acceder al sistema operativo en modo consola. Este modo apenas lo utilizaremos, no obstante, a través de la consola

se puede llevar a cabo todos los comandos de configuración para la herramienta.

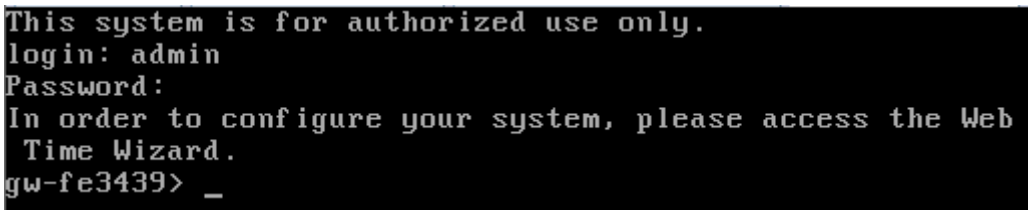

Ilustración 75: Instalación Gaia paso 10

2.2.4. Instalación de software en la máquina Servidor

Una vez creada la máquina virtual e instalado el Sistema Operativo Windows XP en la misma, tenemos que instalar el software necesario para proveer servicios como correo electrónico, servicio FTP y servicio web.

2.2.4.1. FileZilla Server

Lo utilizaremos para alojar el servidor FTP. La instalación es prácticamente automática. No obstante, la configuración merece la pena ser vista por pasos.

Primeramente debemos especificar la dirección de correo donde está el servidor (en caso de que queramos crearlo en nuestra propia máquina, como es en nuestro caso, debemos especificar la dirección de localhost 127.0.0.1).

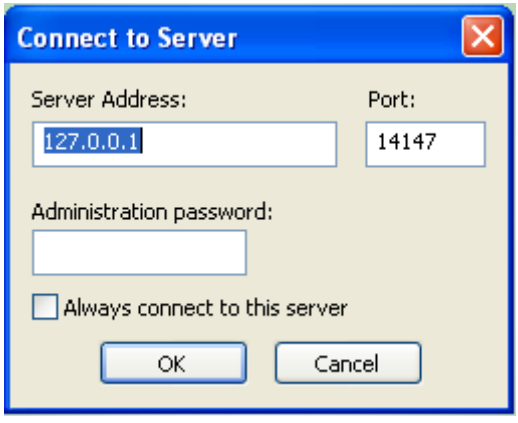

Ilustración 76: Configuración FileZilla Server

En ese momento ya tenemos nuestro servidor corriendo. Para dotarle de más realismo al caso, vamos a definir un usuario mediante el que se va a conectar el usuario cliente. La cuenta será "cliente". Se puede crear haciendo clic en *Edit* → *Users* → *Add*.

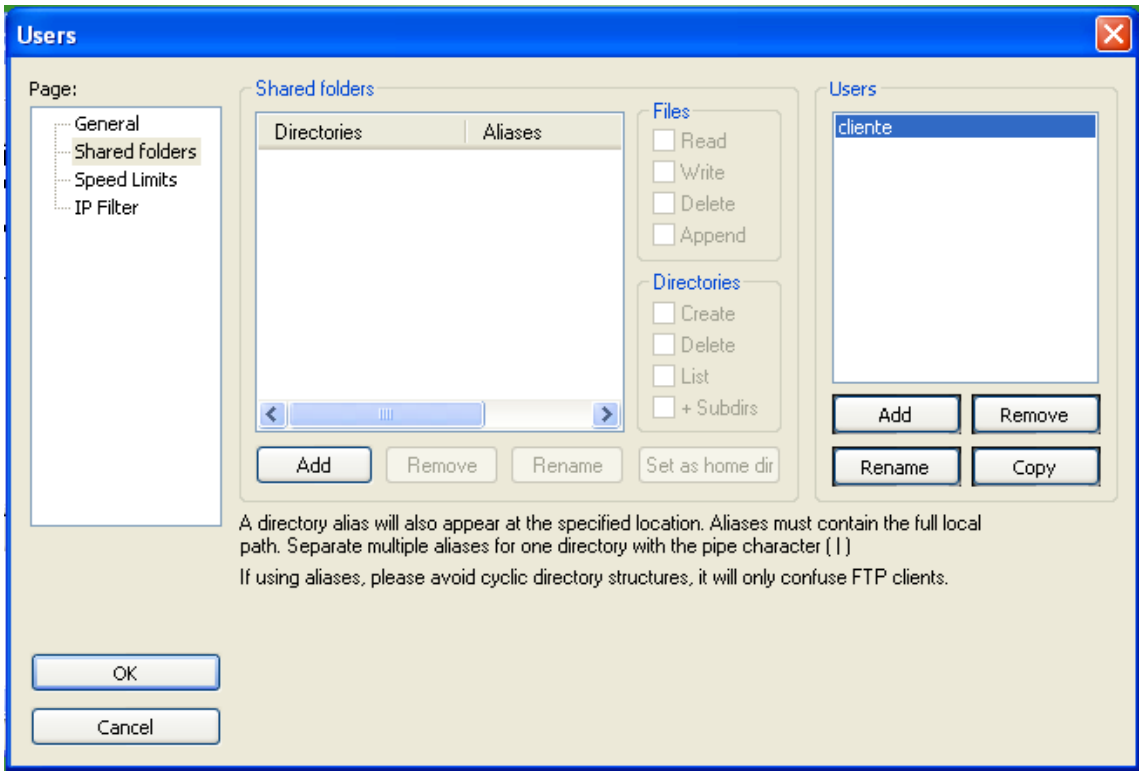

Ilustración 77: Crear usuario FileZilla Server

A continuación debemos seleccionar el directorio donde se almacenarán los archivos haciendo clic en *Shared folders* → *Add*, seleccionamos el directorio y hacemos clic en *OK*.

Esta configuración es suficiente para que el servidor FTP funcione correctamente accediendo desde otras máquinas con el usuario cliente. Esta aplicación debe estar abierta en la máquina servidor continuamente para proporcionar acceso en cualquier momento.

2.2.4.2. ArGoSoft Mail Server Pro 1.8.6.1

Éste es la aplicación que utilizaremos como servidor de correo electrónico para el intercambio de correos en un dominio personal. Antes de la instalación del mismo es

necesaria la instalación de .NET Framework 2.0 (adjuntado también en el material electrónico del proyecto).

Tras llevar a cabo la sencilla instalación de ArGoSoft Mail Server Pro ya podemos ejecutarlo por primera vez. Antes de iniciar el servidor tenemos que configurarlo, para ello seguiremos unos sencillos pasos.

Primeramente debemos agregar el dominio y los usuarios que tendrán acceso al mismo para el intercambio de mensajes. Para ello hacemos clic en el botón *Local Comains*, *Users and Distribution Lists* tal y como se muestra en la imagen.

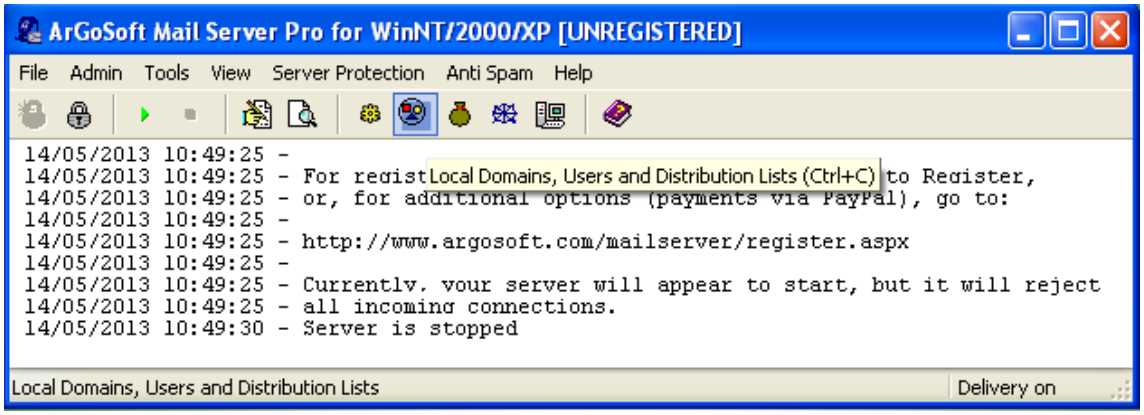

Ilustración 78: Configuración ArGoSoft Mail Server Pro

A continuación hacemos clic en *Add* → *New Domain* como se muestra en la siguiente imagen.

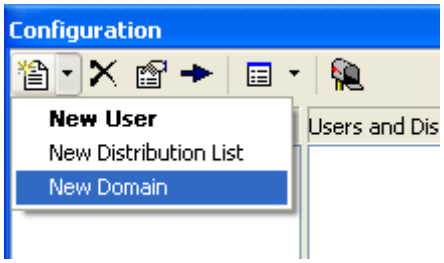

Ilustración 79: Crear dominio

Escribimos el nombre del dominio de correo electrónico (en nuestro caso miempresa.com) y hacemos clic en *OK*.

Para que el dominio pueda ser utilizado por usuarios debemos agregar una cuenta por cada uno de ellos. Para ello acemos clic en *Add* → *New User*. Rellenamos los datos que se nos piden (la contraseña será TFG2013 para todos los que he creado). Y hacemos clic en *OK* para finalizar su creación.

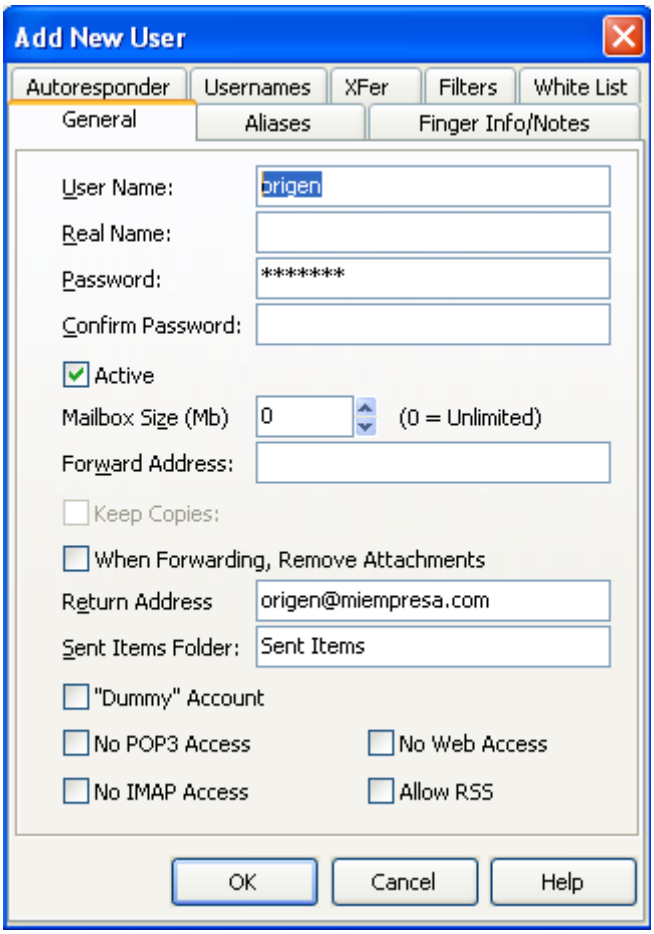

Ilustración 80: Crear usuario

Se han creado tres usuarios necesarios para las pruebas que se verán en el siguiente bloque.

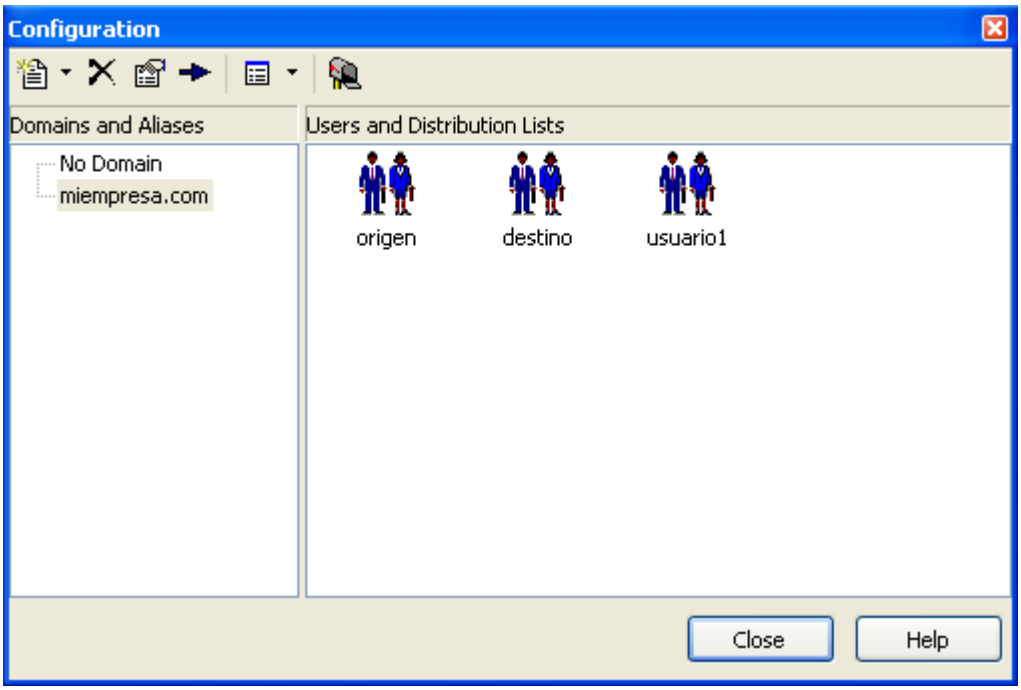

Ilustración 81: Usuarios de correo

Una vez llevada a cabo la satisfactoria configuración del servidor de correo ya podemos arrancar el servidor haciendo clic en *Start Server*. Esta aplicación debe estar arrancada permanentemente para proporcionar un correcto funcionamiento del servidor.

2.2.4.3. XAMPP 1.7.3

Hemos elegido la aplicación XAMPP 1.7.3 como servidor web ya que se utiliza generalmente como base a las páginas web creadas con Joomla! 3.0, que será nuestro sistema de gestión de contenidos para una web de prueba.

XAMPP es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl.

La instalación del software es prácticamente automática. Una vez instalado debemos ejecutar el XAMPP Control Panel Application e iniciar los procesos Apache MySQL y FileZilla.

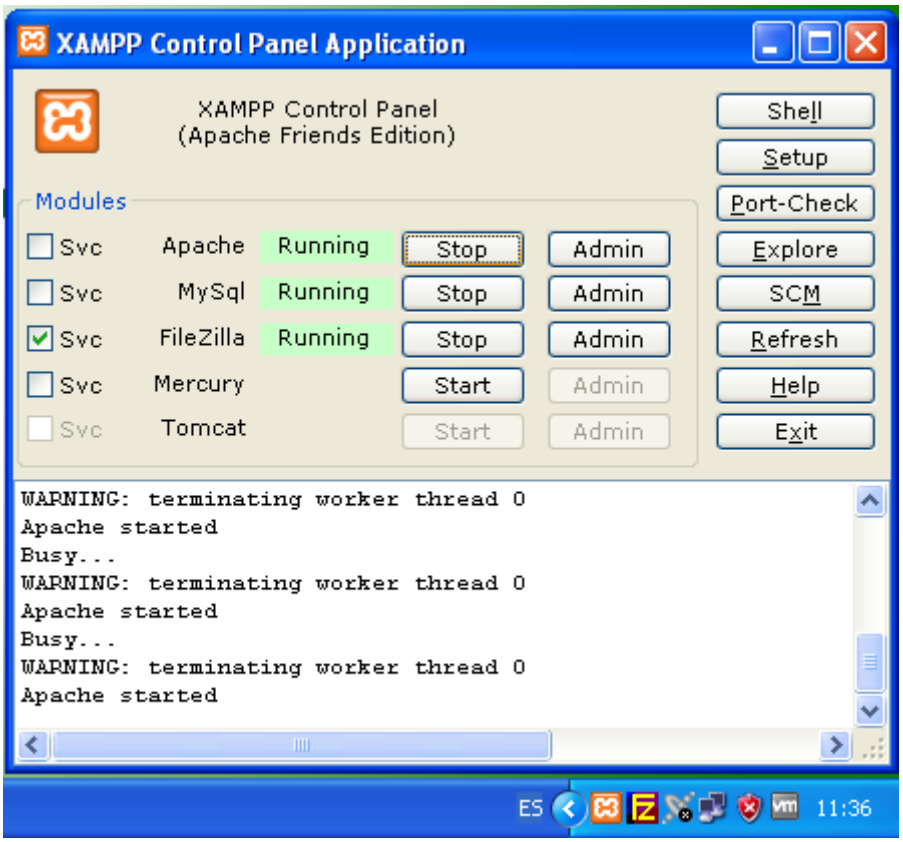

Ilustración 82: XAMPP Control Panel Application

A continuación debemos pegar el contenido de la página web en la carpeta C:\xampp\htdocs para poder acceder a ella desde otras máquinas con la URL http://192.168.2.20/web/.

Si copiamos la web, debemos importar la base de datos de la misma para un correcto funcionamiento. Para ello, accedemos a la URL http://localhost/phpmyadmin/, hacemos clic en la pestaña *Importar* y seleccionamos el archivo adjunto en el material del proyecto "script_bd_web.sql" y hacemos clic en *Continuar*.

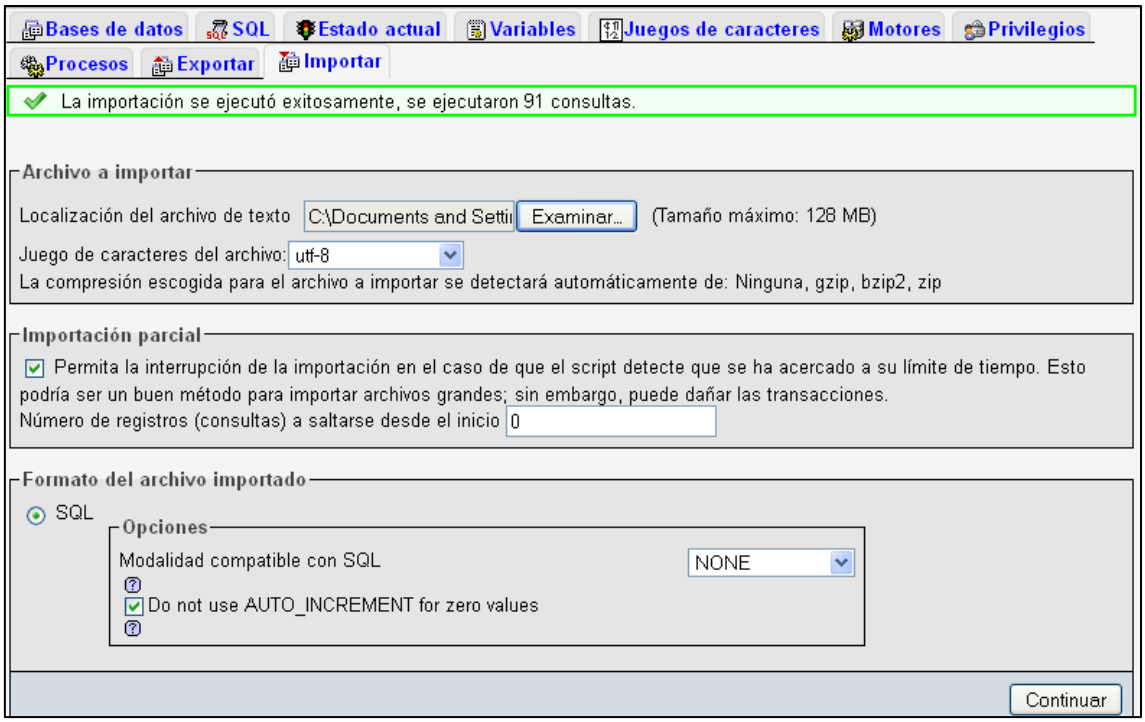

Ilustración 83: Importar base de datos phpMyAdmin

Ya tenemos la web lista para acceder desde cualquier máquina a través de la URL: http://192.168.2.20/web/.

2.2.5. Instalación de software en la máquina Cliente

Una vez creada la máquina virtual e instalado el Sistema Operativo Windows XP en la misma, tenemos que instalar el software necesario para acceder a los recursos que el servidor pondrá a nuestra disposición como correo electrónico, servicio FTP y servicio web.

2.2.5.1. Check Point UserCheck

Lo utilizaremos para recibir las alertas de las políticas incumplidas a través de pop-ups. La instalación es totalmente automática, basta con arrancar el instalador y en pocos segundos estará haciendo intentos de conexión.

Será necesario que nos autentiquemos para poder recibir las alertas. Para ello hay que acceder a *Settings* haciendo clic en el botón derecho del icono de la barra de tareas.

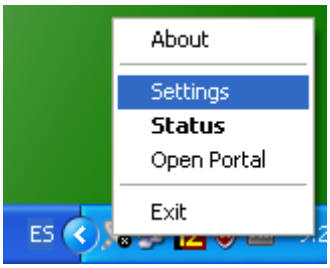

Ilustración 84: Opciones de UserCheck

Ahora debemos marcar la opción *Authentication with Check Point user accounts defined internally in SmartDashboard* para que nos pida nuestro nombre de usuario y contraseña definido en la aplicación Smart Dashboard.

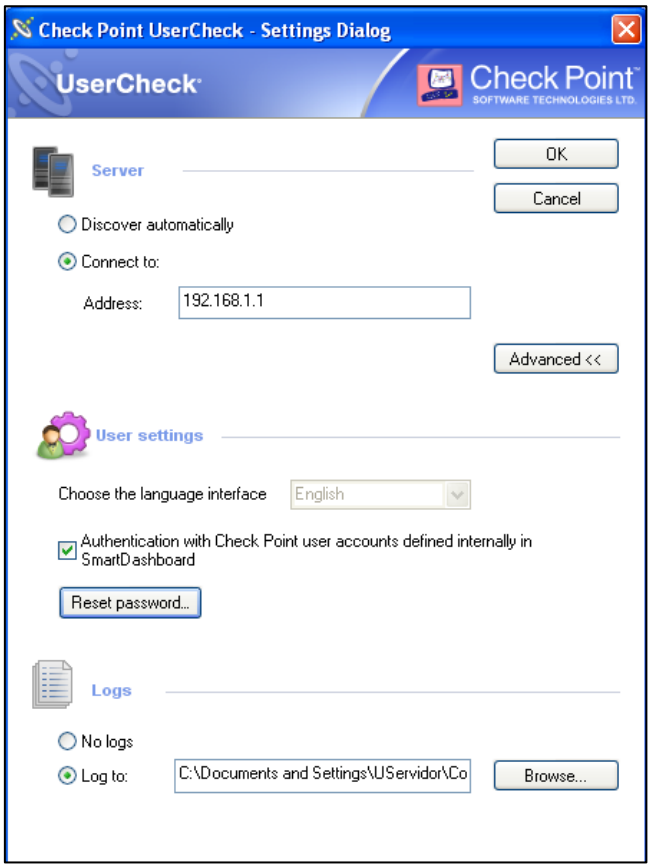

Ilustración 85: Ventana de opciones de UserCheck

2.2.5.2. FileZilla FTP client

Para acceder de una manera más rápida que el propio cmd al servidor FTP vamos a utilizar el cliente FileZilla.

Tras su instalación (prácticamente automática) se tiene que configurar los parámetros para realizar las conexiones al servidor especificadas en el apartado anterior.

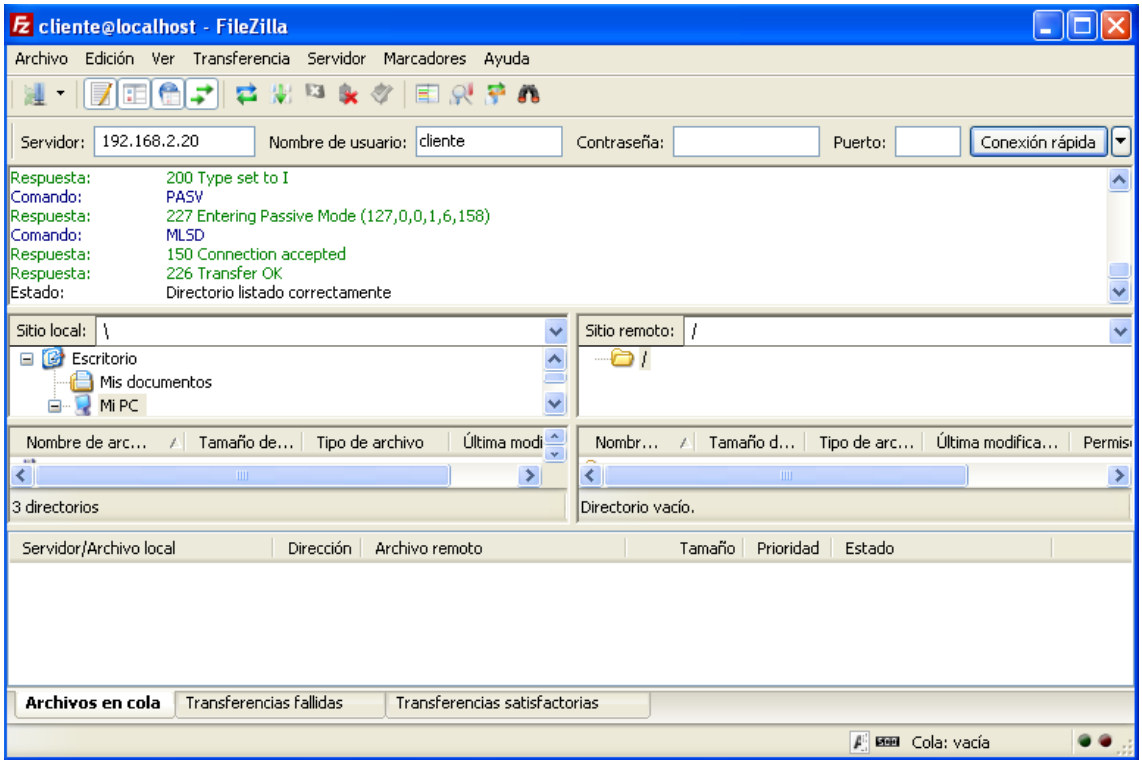

Ilustración 86: FileZilla Cliente FTP

2.2.5.3. Foxmail 6.5

Como cliente de correo electrónico utilizaremos Foxmail 6.5. Su instalación es sencilla y automática, no obstante la configuración requiere una serie de instrucciones que detallamos a continuación.

Nada más abrir por primera vez se ejecutará un asistente que nos ayudará con la configuración de nuestro cliente. Debemos establecer el correo electrónico y contraseña que hemos configurado en el servidor.

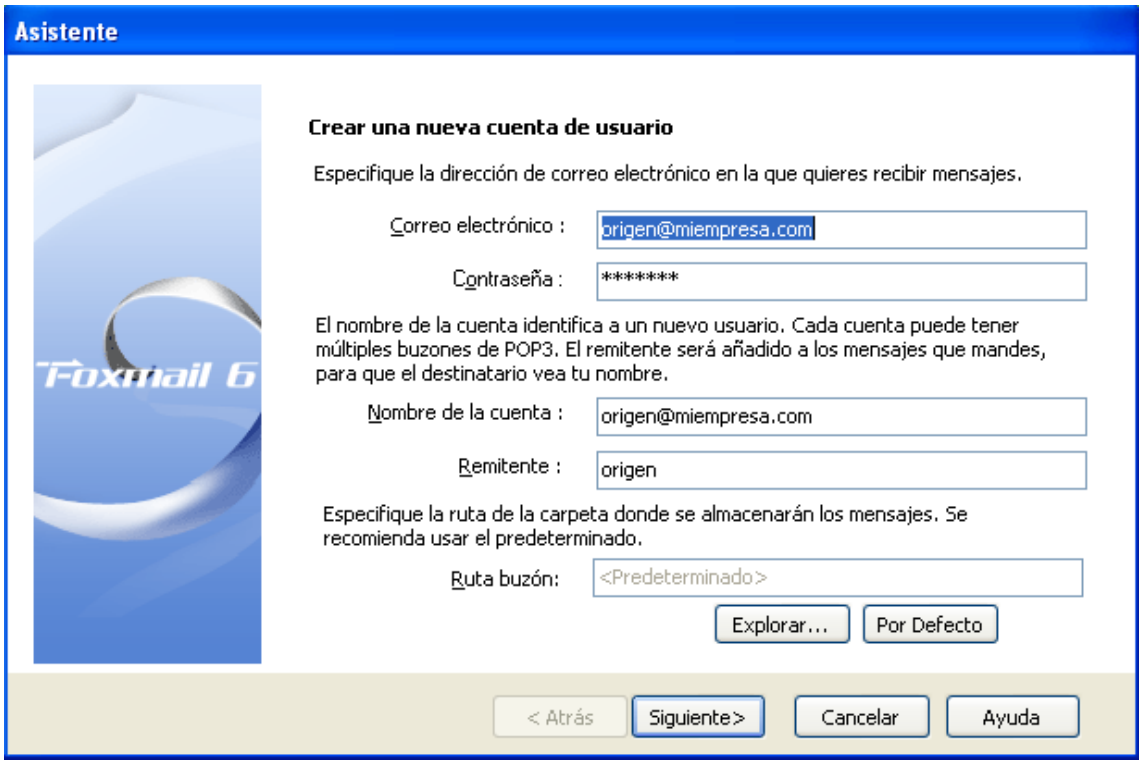

Ilustración 87: Asistente Foxmail paso 1

A continuación se tiene que configurar la dirección IP del servidor POP3 y la del servidor SMTP. En nuestro caso en ambos es la misma.

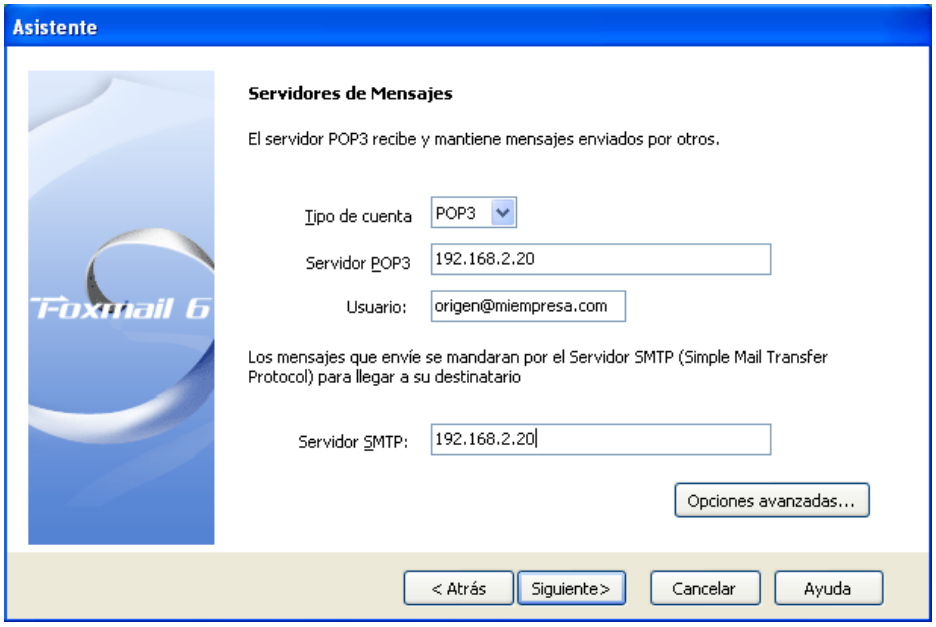

Ilustración 88: Asistente Foxmail paso 2

Hacemos clic en *siguiente* y probamos la configuración para comprobar que las conexiones están debidamente conectadas.

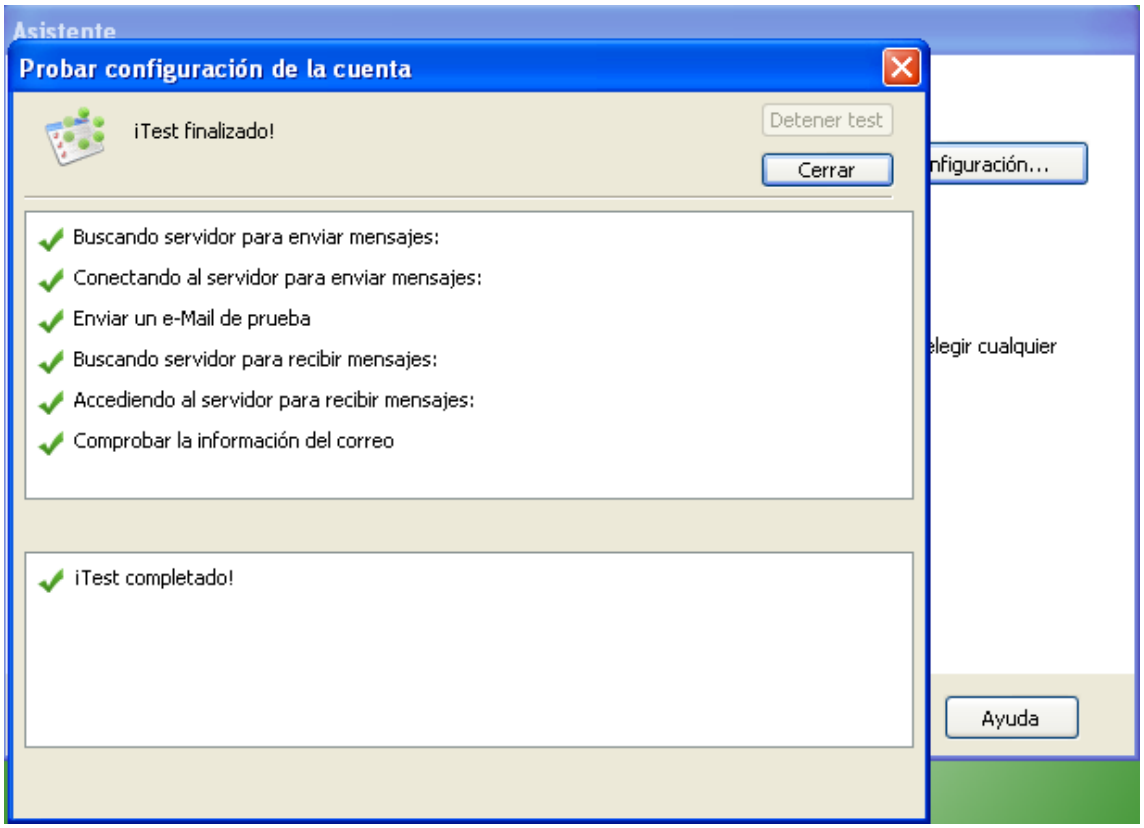

Ilustración 89: Asistente Foxmail paso 3

Por último, hacemos clic en *Finalizar* para terminar la configuración de nuestro cliente de correo electrónico.

2.2.6. Configuración inicial mediante GUI

Una vez puesta en marcha la máquina virtual con el sistema operativo Gaia R75.40, podemos acceder a través del PC de gestión al portal de configuración (a partir de ahora Gaia Portal) de la herramienta mediante la URL definida en la instalación del SO. En nuestro caso la URL para acceder será la 192.168.1.1.

Ilustración 90: Acceso a Gaia Portal

La primera vez que accedemos al Gaia Portal un asistente nos guía en los primeros pasos para establecer una configuración inicial.

Ilustración 91: Asistente de configuración inicial de Gaia

Establecemos la fecha y hora del sistema.

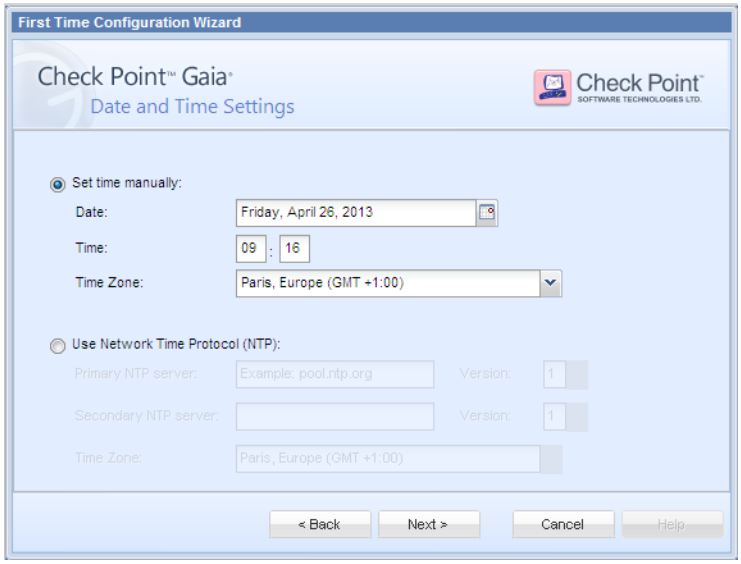

Ilustración 92: Fecha y hora del sistema

Podemos cambiar el nombre con el que será conocido el dispositivo DLP-1 2571 en las herramientas de SmartConsole.

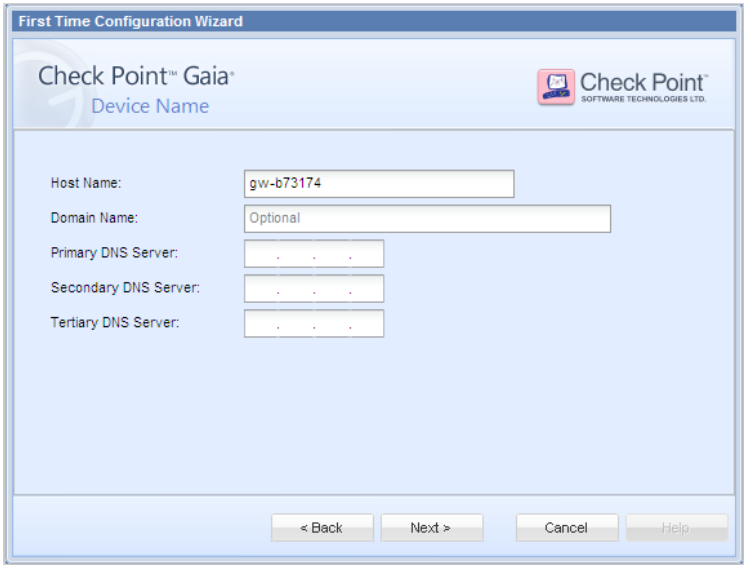

Ilustración 93: Nombre del dispositivo

Establecemos la IP de acceso al Gaia Portal que será la misma que la del interfaz MGNT del DLP-1 2571, la máscara de subred y la IP por defecto de la puerta de enlace (estos ajustes pueden cambiarse en un futuro a través del Gaia Portal).

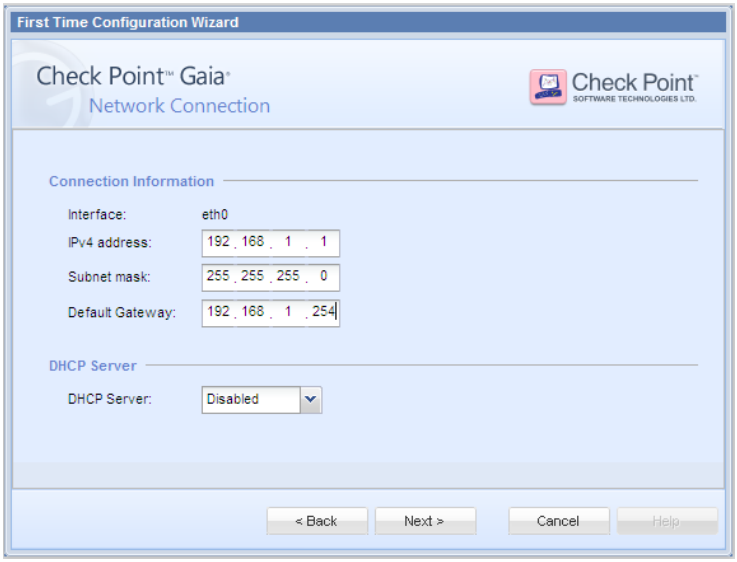

Ilustración 94: Configuración de IPs

En la pantalla final del asistente hacemos clic en *Finish* para que comience el establecimiento de los ajustes.

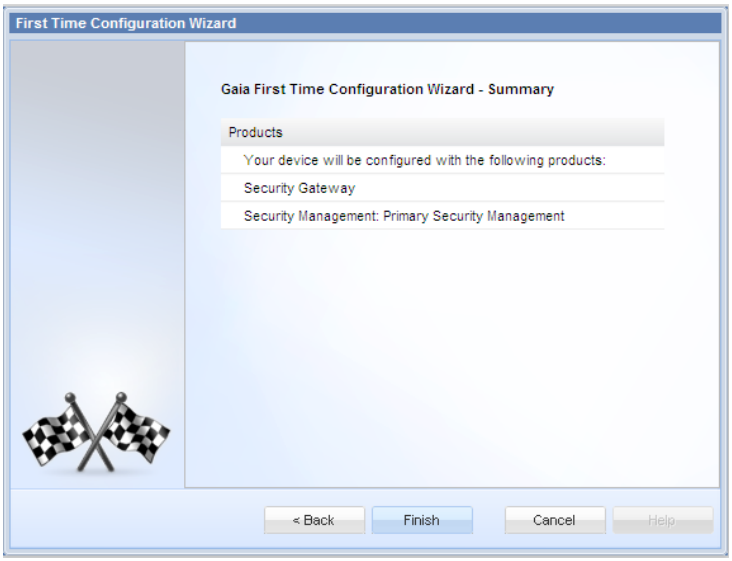

Ilustración 95: Pantalla final del asistente

Una vez finalizado, será necesario reiniciar el sistema, durante este proceso la máquina virtual con el sistema operativo Gaia se reiniciará automáticamente.

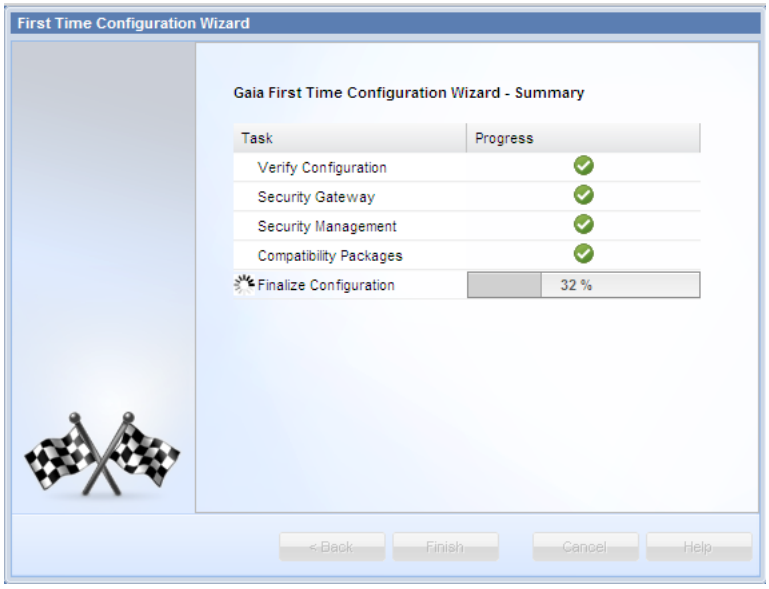

Ilustración 96: Finalizando la configuración

Ya podremos acceder al Gaia Portal, desde esta interfaz web podremos modificar y establecer todos los ajustes posibles en cuanto a conexiones, IPs, establecimiento de DNS, tablas de enrutamiento, etc.

En la parte superior de la página principal del Gaia Portal se encuentra un enlace mediante el cual podremos descargar el instalador de la herramienta de gestión del Software Blade, el conjunto de aplicaciones llamado SmartConsole. Para descargarlo hacemos clic en *Download Now!*.

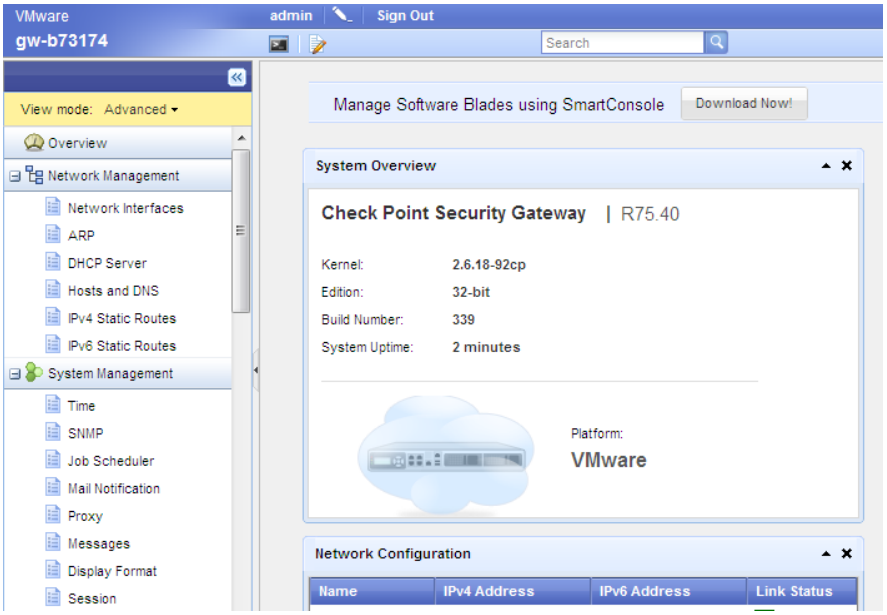

Ilustración 97: Visión general de Gaia Portal

2.2.7. Instalación SmartConsole

Una vez descargado el instalador de SmartConsole lo ejecutamos y seguimos los siguientes pasos.

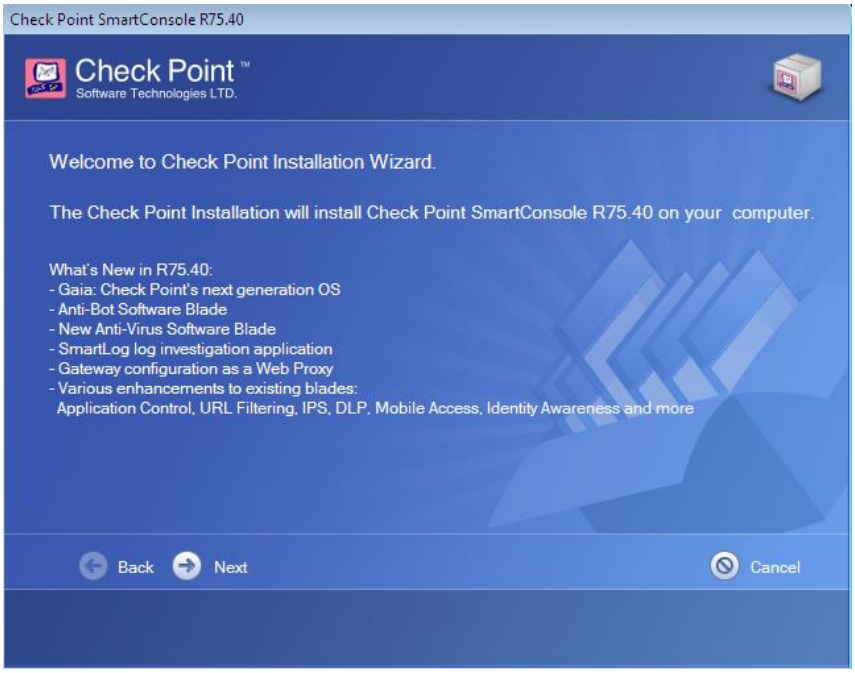

Ilustración 98: Instalación SmartConsole

Vamos avanzando en la instalación y seleccionamos las herramientas que queramos instalar de las que componen el conjunto SmartConsole, en la mayoría de los casos se seleccionará todo.

Ilustración 99: Aplicaciones SmartConsole

Una vez finalizada la instalación ya podemos iniciar las aplicaciones de SmartConsole.

2.2.8. Configuración inicial SmartDashboard

Es necesario realizar una pequeña configuración básica de la red en SmartDashboard en la primera ejecución de la herramienta.

Ilustración 100: Pantalla principal SmartDashboard

Primeramente, tenemos que agregar el host que contiene los servidores. Para ello tenemos que pinchar en la pestaña *Firewall*, hacemos clic derecho en *Nodes* y seleccionamos *Node→Host*, como se muestra a continuación.

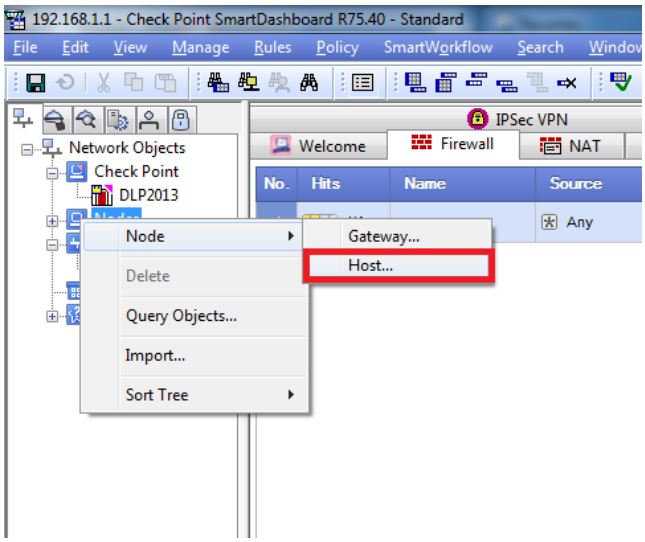

Ilustración 101: Agregar nodo

Establecemos el nombre de la máquina, el color y su dirección IP. Pinchamos en Configure Servers y marcamos Mail Server y Web Server para poder ver las opciones de ambos servidores. Por último, pulsamos OK.

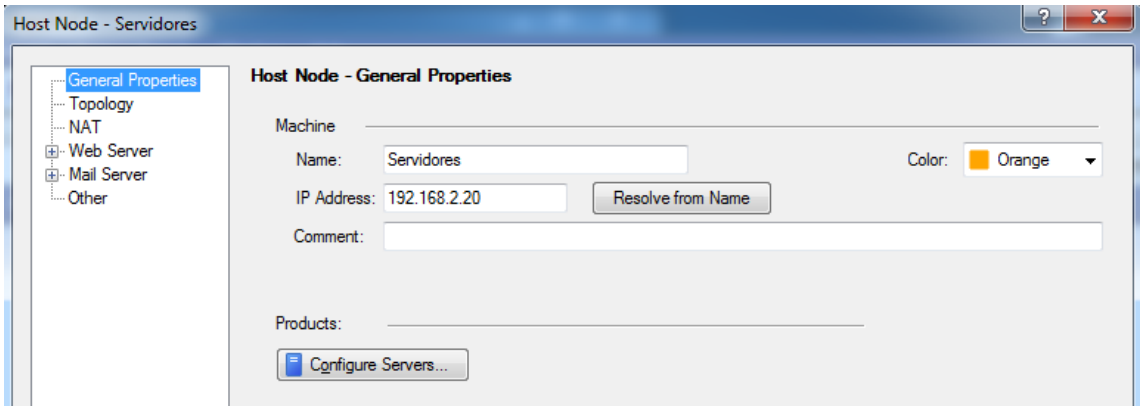

Ilustración 102: Propiedades de nodo Host

Ahora tenemos que ir al panel de navegación, apartado Check Point, ahí aparecerá nuestro dispositivo UTM. Hacemos clic con el botón derecho y seleccionamos *Security Gateway / Management*.

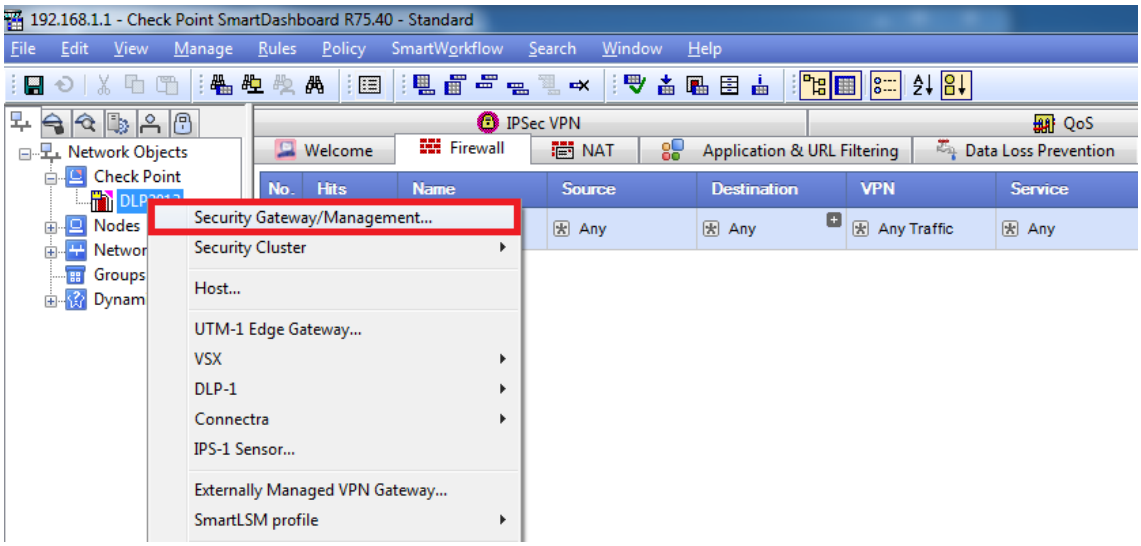

Ilustración 103: Abrir propiedades UTM

Se abrirá la ventana de propiedades generales. En ella seleccionamos las herramientas de Software Blade que desee habilitar. De momento seleccionaremos únicamente los que vemos en la imagen.

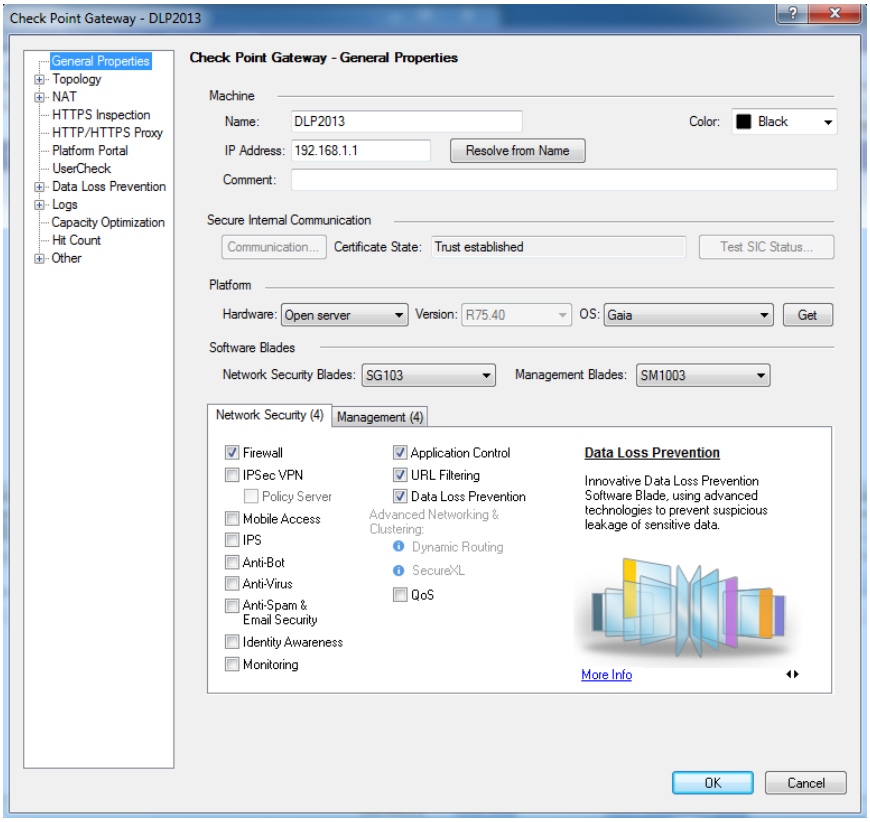

Ilustración 104: Propiedades generales del Gateway

Ahora debemos agregar la topología correspondiente que tenemos implementada. Para ello en el panel de navegación de la izquierda hacemos clic en *Topology*. Hacemos clic en el botón *Get→Interfaces with Topology*. De esta forma se detectan las redes que hay conectadas a nuestro UTM y las identifica para un buen funcionamiento.

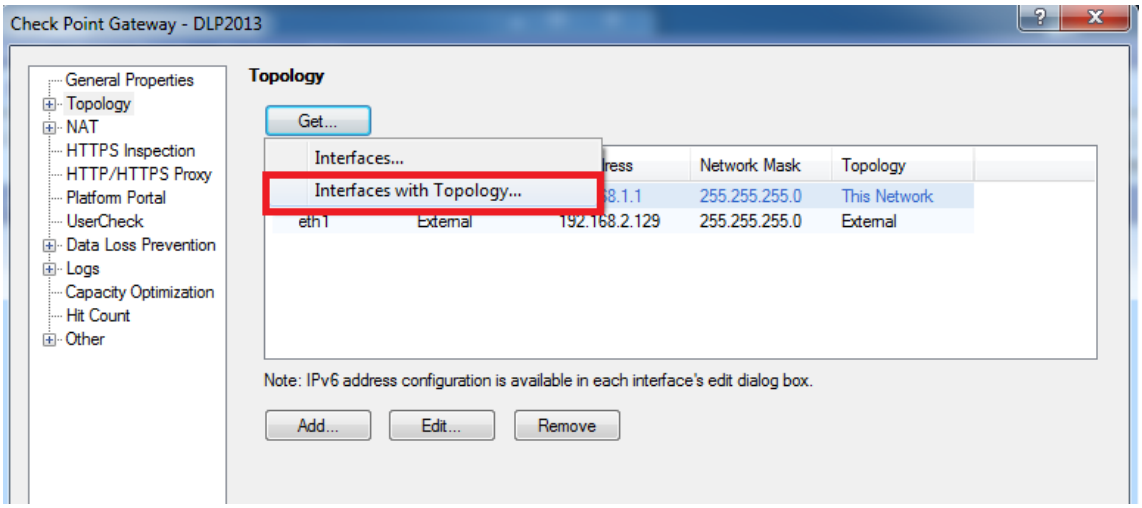

Ilustración 105: Topología de la red

Para que el software UserCheck funcione y muestre los avisos en forma de pop-up en el cliente tenemos que habilitar la opción *Enable UserCheck for Application control and URL Filtering*, en el apartado *UserCheck* del panel de navegación de la izquierda.

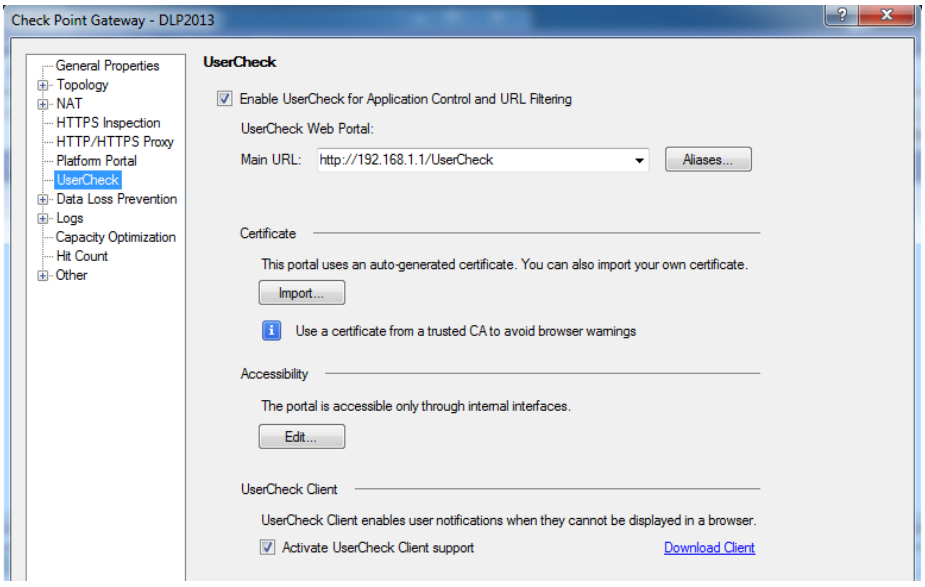

Ilustración 106: Habilitar UserCheck

En el apartado Data Loss Prevention tenemos que configurar una URL para manejar nuestras propias incidencias y habilitar los pop-up de UserCheck ante la violación de alguna de las reglas DLP de la política definida.

Dentro del apartado Data Loss Prevention debemos configurar el servidor de correo para el envío y la recepción de mensajes relacionados con las incidencias ocurridas.

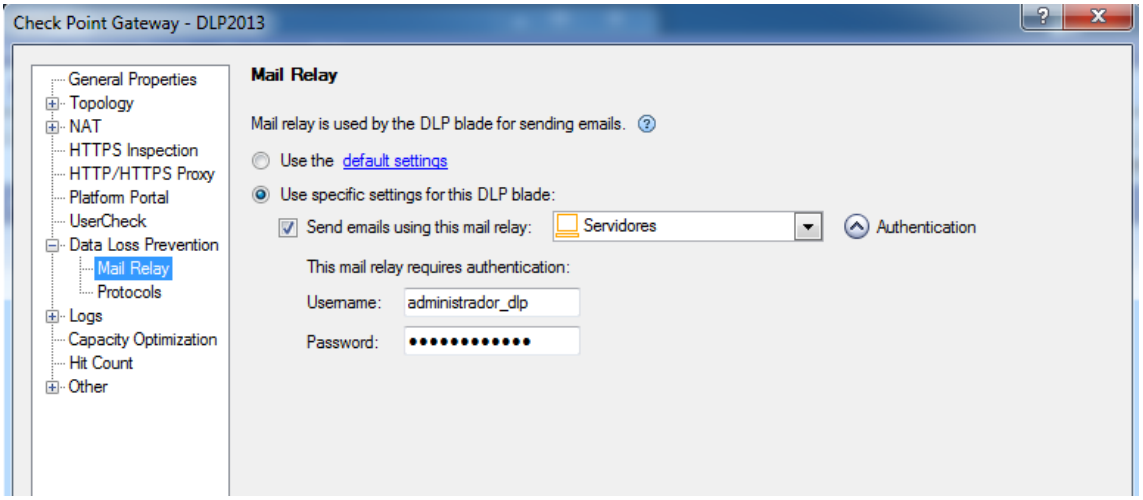

Ilustración 107: Configuración DLP

Primeramente añadiremos una regla firewall que sea permisiva con todo el tráfico que entre y salga a nuestra organización.

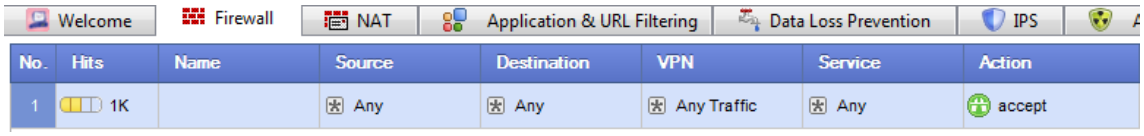

Ilustración 108: Regla firewall

Una vez establecida toda esta configuración es recomendable guardar los ajustes. Ya sólo falta aplicar la política. Para ello hacemos clic en el menú *Policy* → *Install*, se nos muestra una ventana dándonos a elegir en qué Gateway lo queremos instalar, seleccionamos el nuestro y hacemos clic en *OK*.

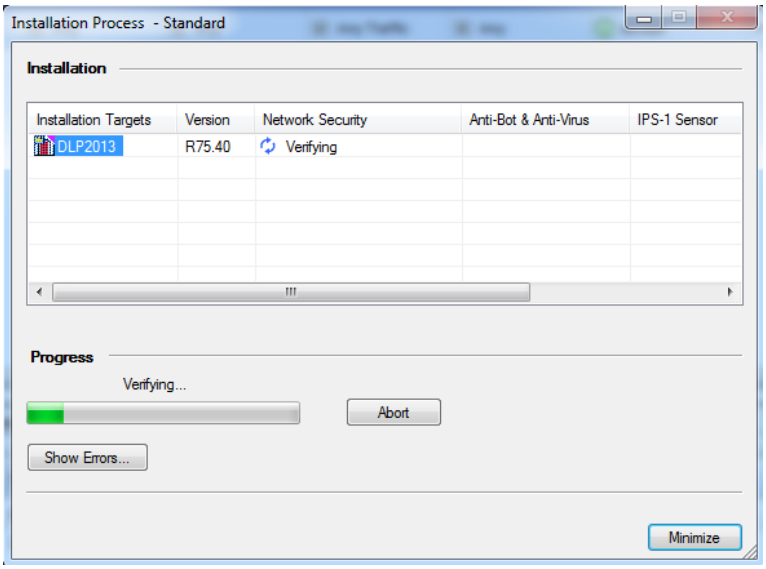

Ilustración 109: Instalación de políticas

Este proceso puede tardar varios minutos ya que primero verifica los ajustes y luego los instala a través del sistema operativo Gaia.

BLOQUE 3:
Casos prácticos

En este último gran apartado vamos a describir cada una de las pruebas llevadas a cabo. Documentaremos cada una de ellas con amplias descripciones y pantallazos. Se contrastará su utilidad con una serie de hipotéticos casos reales con el fin de demostrar en qué situaciones es útil implementar algo parecido en las empresas de hoy en día.

Describiremos el proceso de creación de la política de la empresa. Para definirla son necesarios dos pasos, creación de Data Types y creación de reglas. Además definiremos también los tipos de acciones (User Actions) de las reglas.

Las pruebas que se llevarán a cabo estarán basadas en la creación de una serie de reglas de Data Loss Prevention simulando una política de empresa. Para cada una de ellas realizaremos una demostración de lo que vería un usuario de la red de una empresa.

Las pruebas estarán divididas en cuatro grandes apartados, cada uno haciendo referencia al protocolo que trasladará los datos de un lado cliente a un lado servidor: FTP, HTTP, HTTPS y SMTP.

3.1. Creación de Data Types

Para empezar con la realización de las pruebas hemos creado una serie de Data Types definiendo en cada uno de ellos las palabras o ficheros que van a ser rastreados dentro de la organización (palabras o ficheros conflictivos).

Los Data Types se definen en DLP como tipos de datos que son utilizados en las políticas de seguridad, definiendo que tipos de datos no queremos que circulen por nuestra red, como por ejemplo DNI, cuentas bancarias, tipos de archivos, etc. En SmartDashboard existen predefinidos más de 600 tipos de datos. No obstante, también existe la posibilidad de crear nuestros propios tipos de datos.

Podemos definir los Data Types en la pestaña *Data Loss Prevention→Data Types* en la herramienta SmartDashboard.

Se pueden definir Data Types de 8 tipos distintos:

- **Keywords:** Nos permite definir varias palabras prohibidas e indicar el número máximo que se permite sin que se infrinja la política.

- **Documents based on a corporate template:** Nos permite comparar un archivo enviado con un Template definido. Si supera un porcentaje de similitud, se detectará (por ejemplo similitud del 80%).

- **File attributes:** Nos permite definir un tipo de archivo a rastrear.

- **Regular Expressions:** Nos permite definir una expresión que detecte si hay una palabra prohibida oculta de alguna forma o pensada para saltarse las restricciones (por ejemplo Bomba1, bombaa, etc.).

- **Compound data types:** Nos permite unir dos o más Data Types en uno.

- **Weighted Keywords:** Nos permite asignar diferentes pesos de importancia a las palabras prohibidas. De esta forma, en cuanto llegamos a un límite numérico detectado en un mensaje, se bloqueará.

- **Words from a dictionary:** Nos permite importar un archivo con palabras prohibidas.

- **CPcode:** Es un lenguaje de programación de Check Point que nos permite programar nuestras propias reglas.

Hemos creado una lista de Data Types y la hemos implementado en la política de la empresa para posteriormente crear las reglas que hagan saltar notificaciones a los usuarios.

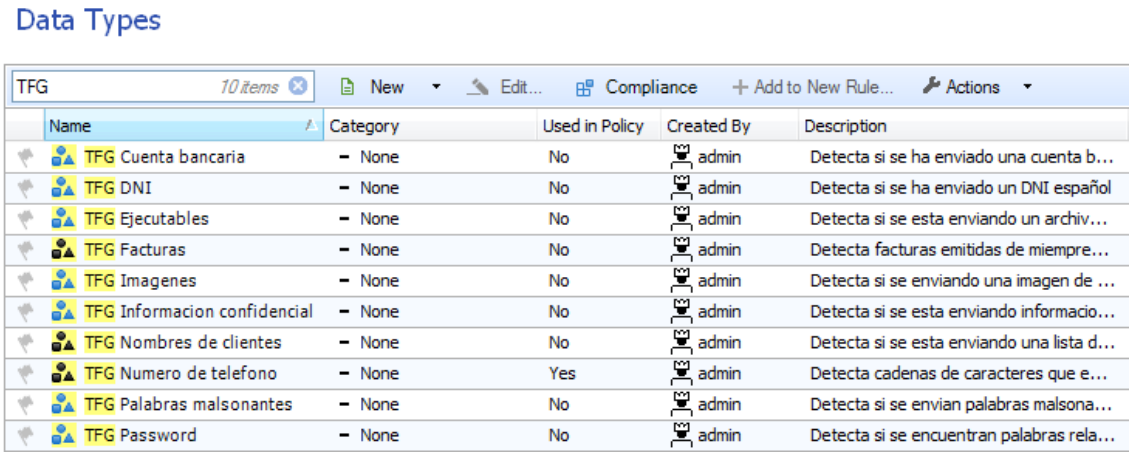

Ilustración 110: Lista de Data Types creados para las pruebas

A continuación vamos a ver unos ejemplos de creación de Data Types que utilizaremos en las pruebas con características propias que queremos detectar.

Para ello, definimos un nuevo Data Type, abrimos la aplicación SmartDashboard y hacemos clic en la pestaña *Data Loss Prevention* → *Data Types* → *New* → *Data Type*, y completamos el siguiente asistente.

3.1.1. Ejemplo Data Type 1

Primeramente vamos a crear un Data Type que detecte los números de teléfono españoles, es decir, números de nueve cifras que empiecen por 9 o 6, y números que empiecen por +34 o 0034 (prefijo de España).

Primero nos pide que introduzcamos el nombre y el tipo de Data Type, nos encontramos con los tipos definidos en este mismo apartado.

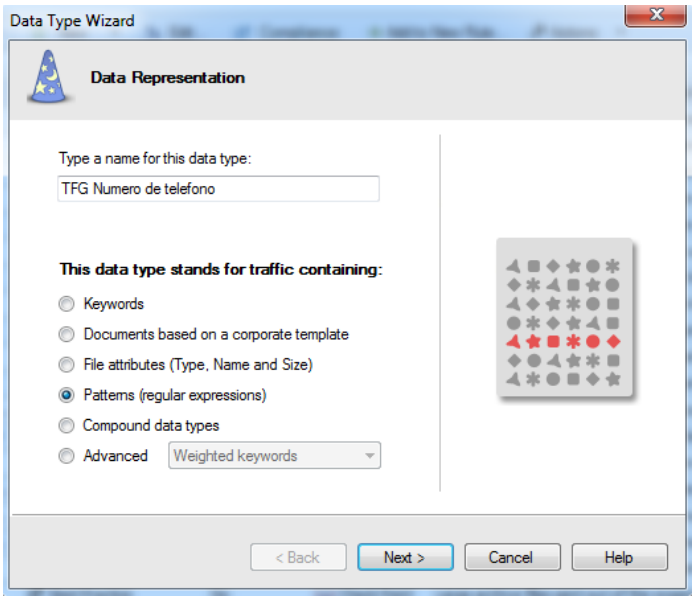

Ilustración 111: Crear Data Type Número de teléfono paso 1

A continuación nos pide especificar los patrones, o expresiones regulares, que van a detectar los números de teléfono. Para entender el significado de los caracteres que se pueden utilizar es muy recomendable pulsar el botón *Help*. En esta ayuda viene definida la utilidad de cada carácter.

Para la definición de este Data Type hemos utilizado el \d, que representa a cualquier dígito decimal.

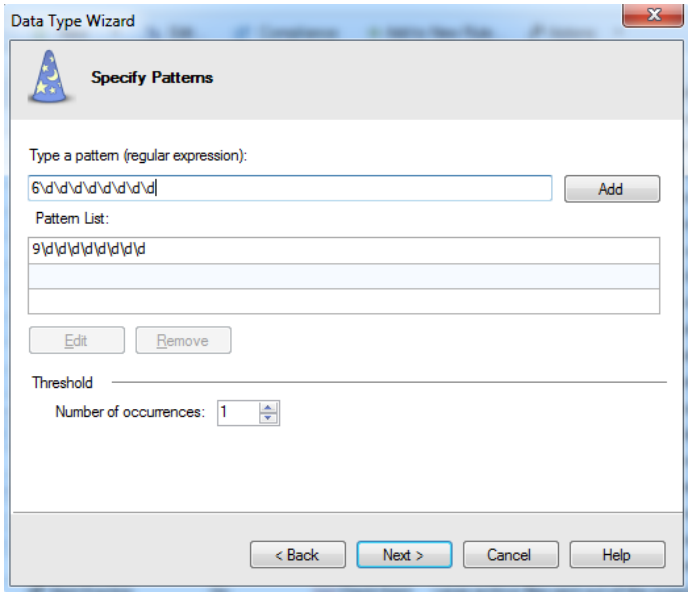

Ilustración 112: Crear Data Type Número de teléfono paso 2

Por último hacemos clic en *Finish* para terminar la creación del Data Type. Podemos definir más opciones del Data Type como comentarios, descripción, categoría, etc. haciendo doble clic en el Data Type creado.

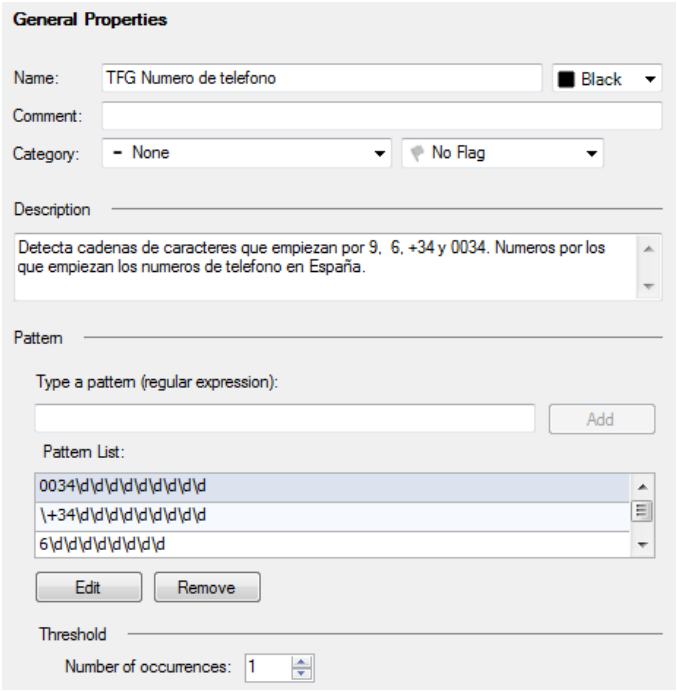

Ilustración 113: Propiedades generales de un Data Type

3.1.2. Ejemplo Data Type 2

Para este segundo ejemplo hemos creado una plantilla de facturas de una empresa. Utilizaremos el tipo Documents base don a corporate template para detectar el envío de archivos similares a las facturas de la empresa.

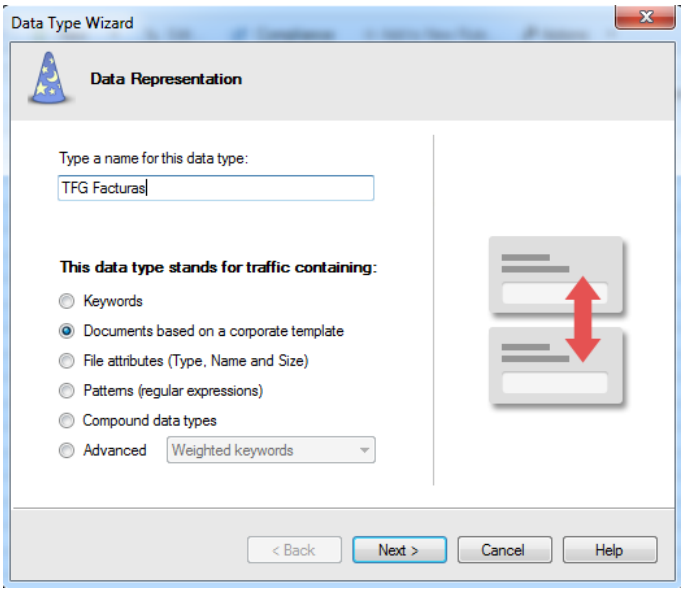

Ilustración 114: Creación del Data Type Facturas paso 1

A continuación tenemos que subir la plantilla de la factura que hemos creado (plantilla_factura.xlsx) y seleccionar el porcentaje de similitud para que salte la notificación, en nuestro caso el 50%.

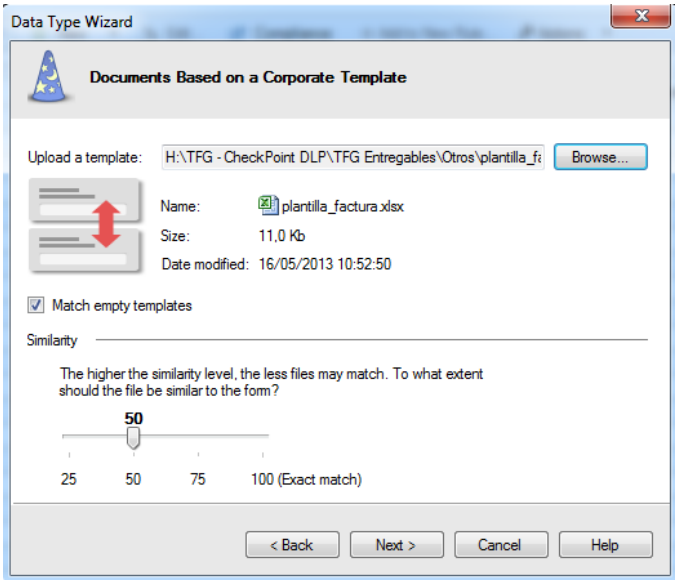

Ilustración 115: Creación del Data Type Facturas paso 2

Por último, al igual que en el anterior ejemplo, escribimos una pequeña descripción del Data Type abriendo las propiedades generales del mismo.

3.1.3. Ejemplo Data Type 3

En este tercer ejemplo vamos a crear un Data Type que detecte si se está enviando una lista de nombres de clientes de la empresa. Para ello seleccionamos el tipo avanzado Words from a dictionary.

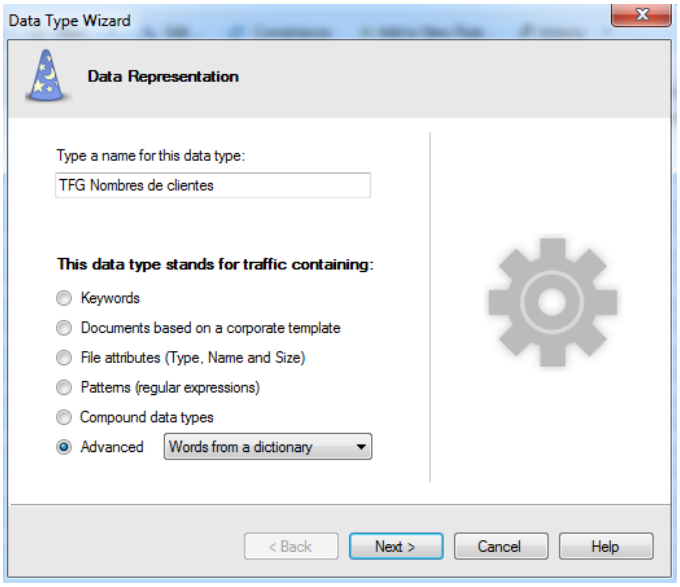

Ilustración 116: Creación del Data Type Nombres de clientes paso 1

A continuación tenemos que seleccionar la lista de clientes (lista_clientes.txt) y seleccionar la cantidad de nombres que se tienen que detectar para que sea considerado el Data Type.

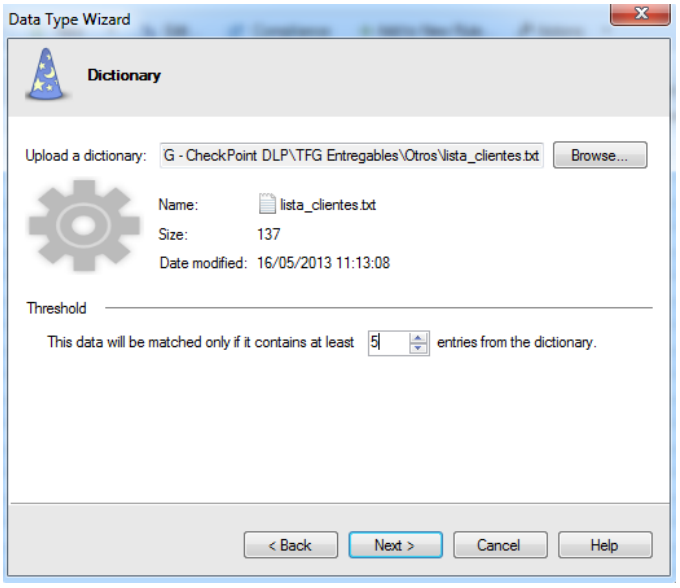

Ilustración 117: Creación del Data Type Nombres de clientes paso 2

Por último, podemos escribir una pequeña descripción del Data Type en las propiedades generales del mismo.

3.2. Tipos de acciones (User Actions)

Antes de definir las reglas que van a componer la política de DLP es necesario que conozcamos los cuatro tipos de acciones que se pueden asociar a cada una de ellas. Según el tipo de acción que se establezca le aparecerá al usuario un tipo de pop-up u otro, y podrá interactuar y tomar decisiones a través del mismo.

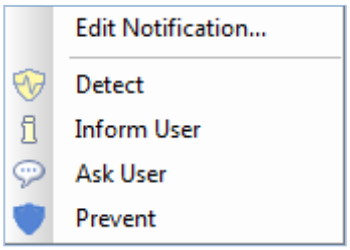

Ilustración 118: User Actions

3.2.1. Prevent

Como su propio nombre indica, con ella se previene la fuga de datos. Es la acción más restrictiva, con ella la comunicación es interceptada, el emisor recibe una notificación alertándole de que acaba de infringir una regla y el receptor no recibe el mensaje o archivo. Toda la información acerca de la incidencia queda registrada en el sistema.

3.2.2. Ask User

En esta acción la comunicación es interceptada, el emisor recibe una notificación alertándoles de que acaba de infringir una regla. En este caso el emisor puede decidir si enviarlo o descartarlo. En caso de descartarlo el mensaje no llegará a su destinatario. Toda la información acerca de la incidencia queda registrada en el sistema.

3.2.3. Inform User

Esta acción la comunicación es interceptada pero, al contrario que en los dos tipos anteriores, el mensaje o archivo sí llega al receptor. No obstante, una notificación es enviada al emisor alertándole de que acaba de infringir una regla. Toda la información acerca de la incidencia queda registrada en el sistema.

3.2.4. Detect

En éste caso, al igual que en todos los anteriores, la comunicación es interceptada y la información de la incidencia queda registrada en el sistema. Pero, al contrario que en todos los anteriores, el receptor no recibe ninguna notificación alertándole del incumplimiento de la regla.

3.3. Creación de la política de empresa

Una vez definidos los Data Types, podemos crear reglas de la política DLP utilizando los Data Types creados o los que vienen por defecto. A continuación describiremos los pasos principales con tres ejemplos de creación de reglas.

Para agregar una nueva regla debemos hacer clic en el botón resaltado de la siguiente imagen correspondiente con la sección *Policy* de la pestaña *Data Loss Prevention*.

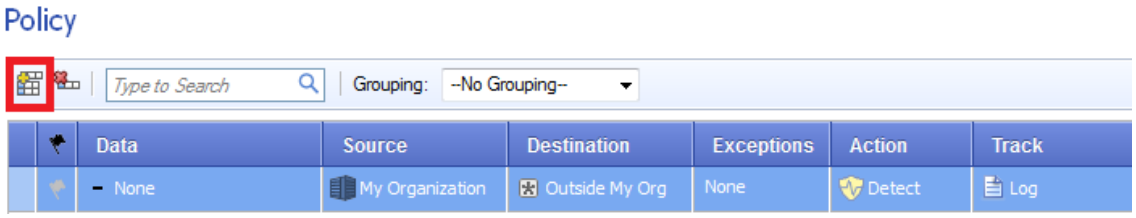

Ilustración 119: Crear regla en la política

A continuación hacemos clic en el campo *Data* de nuestra nueva regla para seleccionar el Data Type que será la base de nuestra regla. Hay que destacar que se pueden elegir más de un Data Type en la misma regla, no obstante, nosotros utilizaremos sólo uno por cada regla.

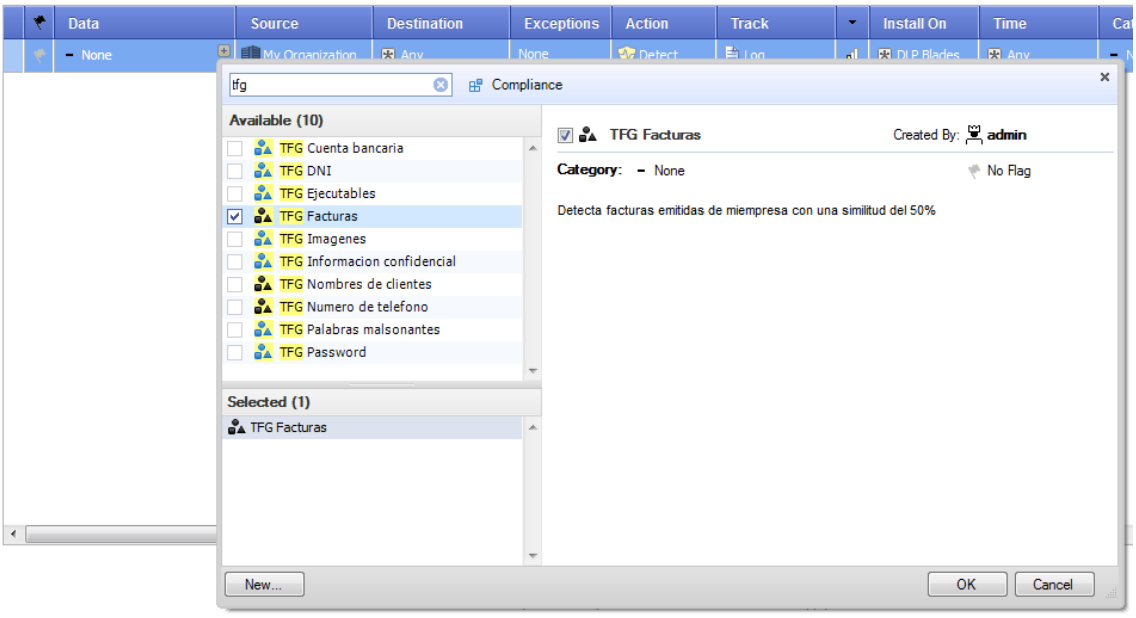

Ilustración 120: Selección Data Type Facturas

Una vez agregado el Data Type, tenemos que elegir un tipo de acción para la regla en caso de que algún usuario la incumpla. Para ello hacemos clic derecho en el campo *Action* de nuestra regla y seleccionamos uno de los siguientes tipos.

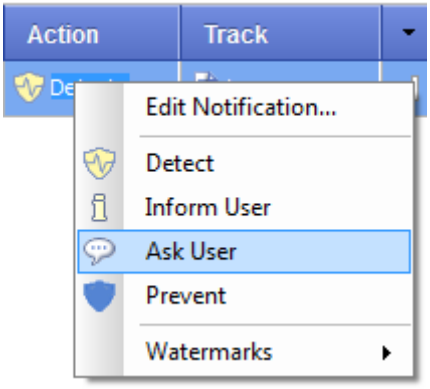

Ilustración 121: Selección de User Action

La aplicación nos permite editar la información acerca de la regla que se mostrará al usuario que la incumpla, un mensaje que se mostrará al usuario en el pop-up que se ejecute en su máquina. Para editarlo hacemos clic derecho en el campo *Action* y seleccionamos *Edit Notification*. Se abrirá una ventana como la siguiente en la cual podremos escribir nuestro mensaje personalizado.

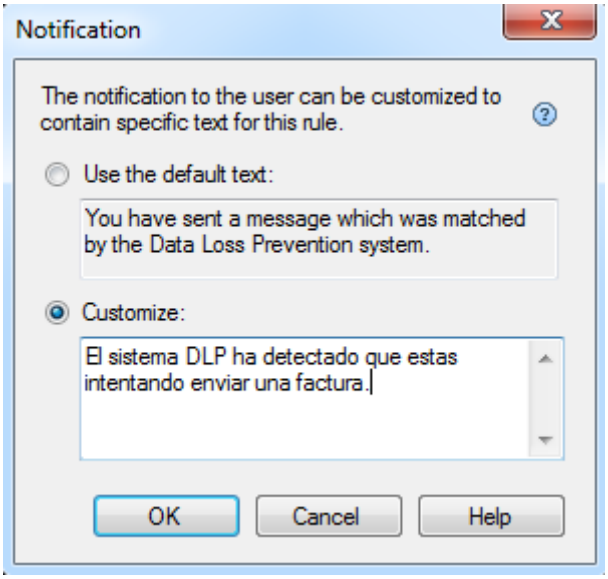

Ilustración 122: Mensaje personalizado de notificación

Para completar la definición de la regla tenemos que seleccionar un nivel de importancia de incumplimiento de la misma. Para ello hacemos clic derecho encima del símbolo de importancia y seleccionamos entre los cuatro niveles disponibles.

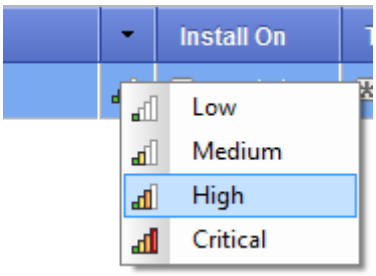

Ilustración 123: Niveles de importancia

Ahora vamos a crear una nueva regla que utilice dos de los Data Types que vienen predefinidos en SmartDashboard, como por ejemplo *Encrypted Archive* y *Password Protected File*.

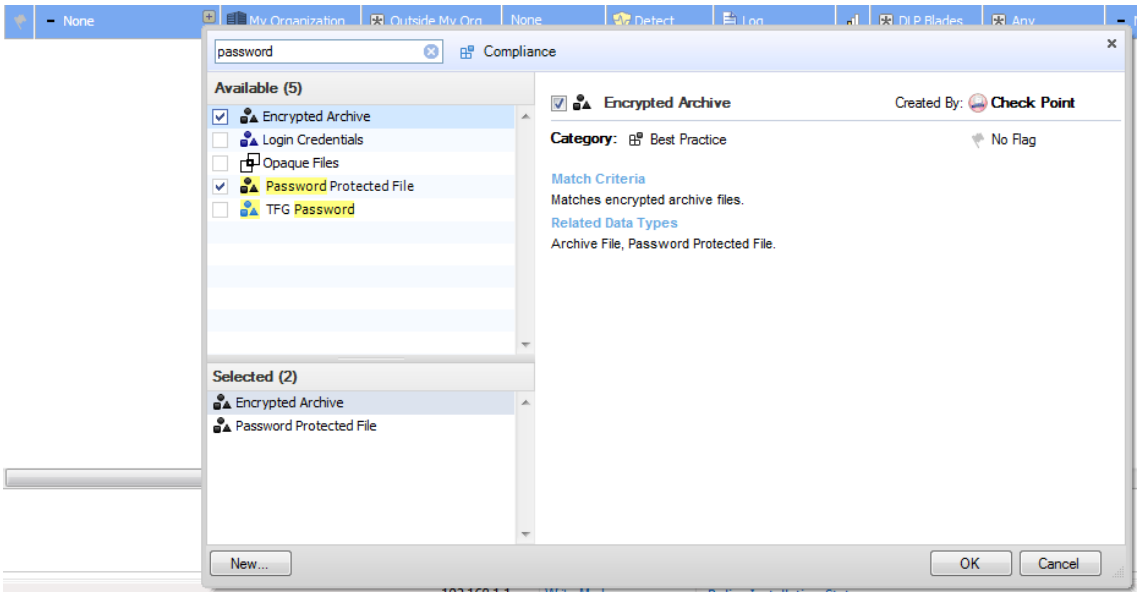

Ilustración 124: Elección de Data Types predefinidos

Establecemos la acción *Prevent* para bloquear todos los archivos que vaya encriptados o protegidos con contraseña y establecemos un mensaje personalizado para el incumplimiento de esta regla.

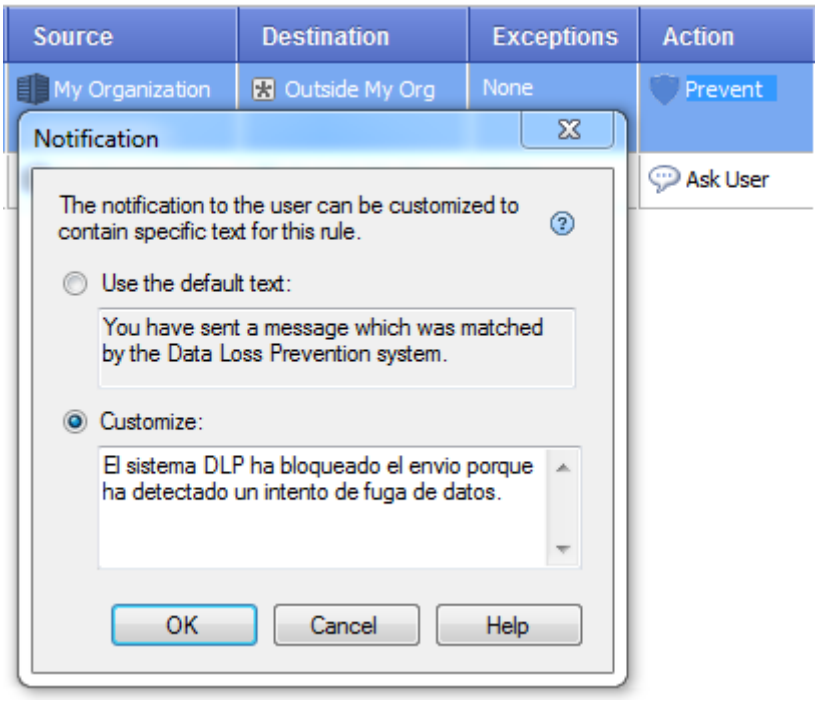

Ilustración 125: Mensaje personalizado para otra regla

De manera análoga vamos definiendo el resto de reglas para cada uno de los Data Types que hemos definido.

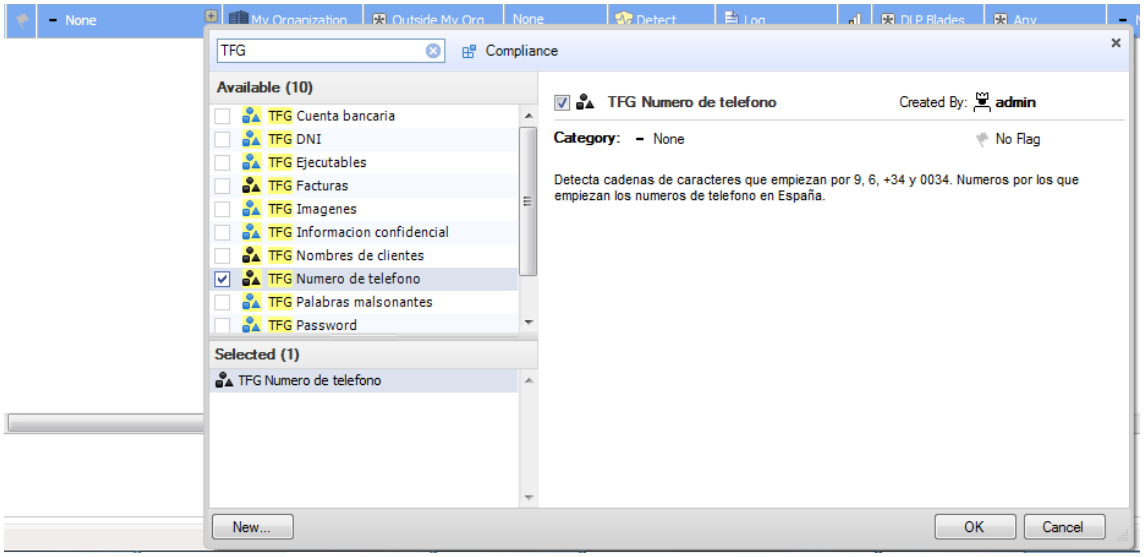

Ilustración 126: Creación de regla Número de teléfono

Una vez completada todas las reglas tendremos una política de Data Loss Prevention lista para verificarla e instalarla. La lista de reglas creadas para las pruebas de los siguientes apartados es la siguiente.

Policy

Type to Search | Grouping: --No Grouping--

	Data	Source	Destination	Exceptions	Action	Track		Install On
	Password Protected File Encrypted Archive	My Organization	Outside My Org	None	Prevent	Log		DLP Blades
	TFG Imagenes	My Organization	Outside My Org	None	Prevent	Log		DLP Blades
	TFG Cuenta bancaria	My Organization	Any	None	Prevent	Log		DLP Blades
	TFG Facturas	My Organization	Outside My Org	None	Ask User	Log		DLP Blades
	TFG Palabras malsonan...	My Organization	Any	None	Ask User	Log		DLP Blades
	TFG Informacion confid...	My Organization	Outside My Org	None	Detect	Log		DLP Blades
	TFG DNI	My Organization	Any	None	Prevent	Log		DLP Blades
	TFG Nombres de clientes	My Organization	Outside My Org	None	Inform User	Log		DLP Blades
	TFG Ejecutables	My Organization	Outside My Org	None	Ask User	Log		DLP Blades
	TFG Numero de telefono	My Organization	Outside My Org	None	Detect	Log		DLP Blades

Ilustración 127: Política DLP de nuestra empresa

Por último, para que todo esté listo para las pruebas tenemos que verificar e instalar la política. Para ello hacemos clic en el menú *Policy* → *Install*.

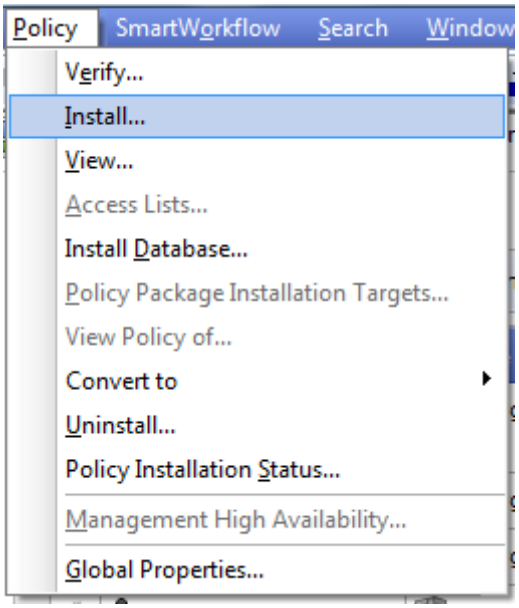

Ilustración 128: Menú instalar política

Esperamos unos minutos a que se instale la política y ya tendremos listo nuestro laboratorio de pruebas.

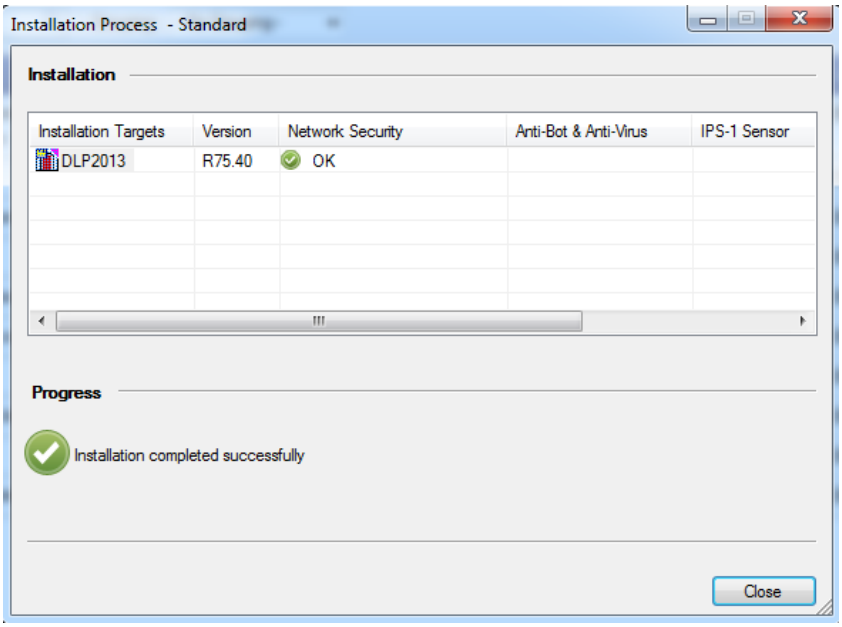

Ilustración 129: Ventana indicativa del éxito de la instalación

3.4. Pruebas FTP

Para investigar cómo actúa el sistema DLP con el protocolo FTP, realizamos conexiones entre un cliente y un servidor FTP. El servidor FTP está equipado con el software FileZilla Server y los clientes se conectan al servidor mediante el cliente FTP que provee Windows, escribiendo en el CMD 'ftp ip_servidor_ftp', el nombre de usuario y la contraseña.

Los clientes suben archivos al servidor FTP mediante el comando 'put 'ruta del archivo'', los cuales serán analizados para comprobar si contienen palabras o tipos restringidos por las reglas definidas.

También podemos utilizar un cliente FTP como FileZilla Client, en el cual introducimos los parámetros necesarios para la conexión y podemos subir archivos a través de una interfaz de usuario.

3.4.1. Archivos protegidos o encriptados

Para esta prueba hemos creado un archivo ZIP protegido con contraseña y vamos a tratar de subirlo a través del cliente FTP de Windows al servidor FTP. Como hemos visto en la política, hemos definido una regla para que detecte este tipo de comportamiento.

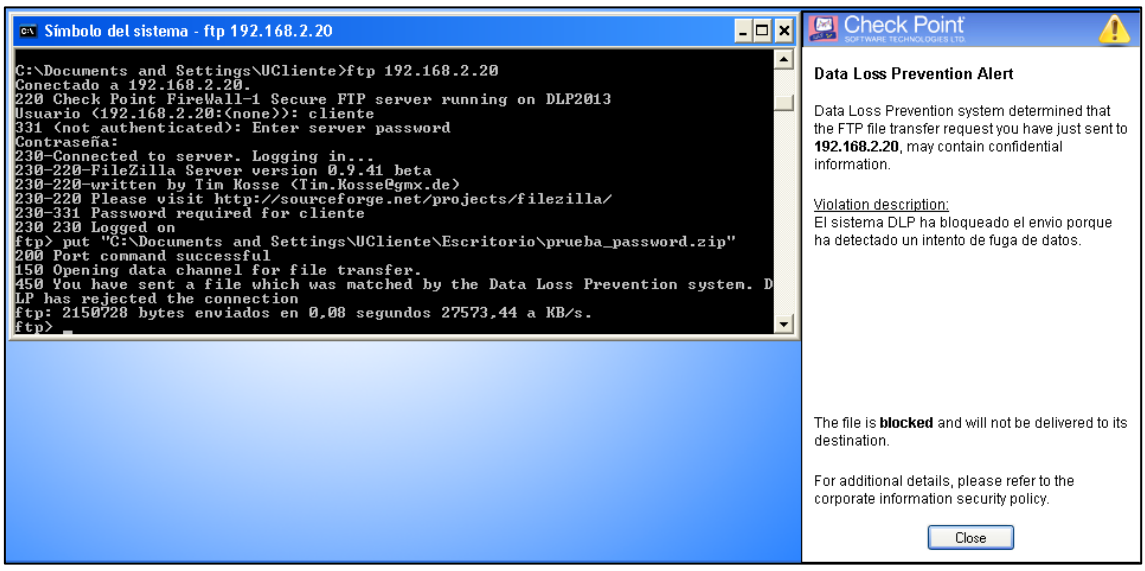

Ilustración 130: Subida de archivo con contraseña al FTP

La regla tiene asociada una acción *Prevent*, por tanto una notificación nos alerta de que hemos infringido una de las reglas de la política y la subida ha sido bloqueada.

La incidencia queda registrada y puede ser visualizada en SmartView Tracker, programa a disposición del administrador para revisar las incidencias ocurridas. En él se observa toda la información relacionada con la misma.

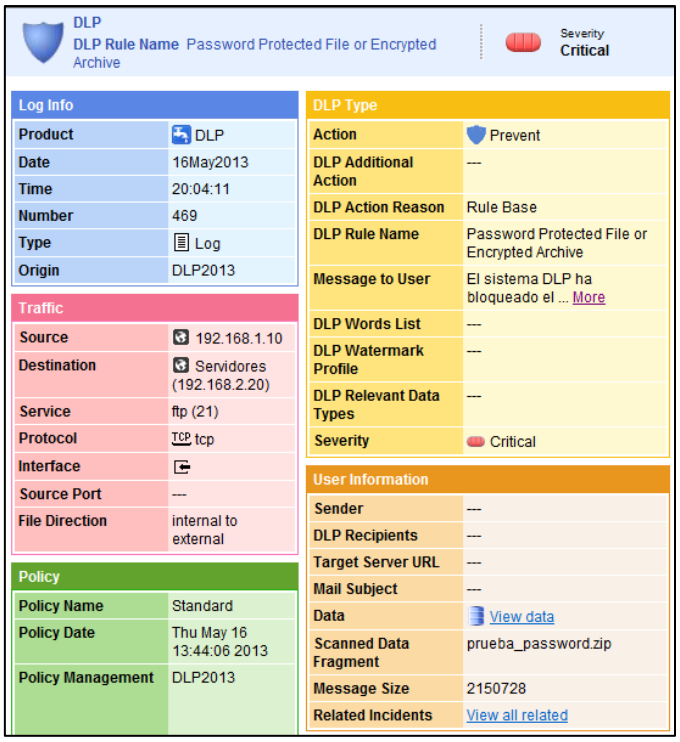

Ilustración 131: Visualización de incidencia de subida de archivo con contraseña

Si cliqueamos en la infracción que acabamos de cometer podemos ver información acerca de quién ha cometido la infracción, la hora y la IP de la máquina desde la que se produce la infracción, la IP del servidor al que se iba a subir, el protocolo de transporte utilizado, la regla infringida, la importancia de la incidencia, la acción de la regla, el fichero que ha infringido la regla y demás información acerca del mensaje y la conexión.

3.4.2. Imágenes

En esta prueba subimos al servidor FTP una imagen de formato PNG desde un cliente. Para este tipo de información existe una regla llamada Imágenes, la cual comprueba si el fichero enviado tiene un formato de imagen (jpg, png, gif, bmp, etc.).

Al intentar subir el fichero desde el cliente nos aparece un mensaje de aviso alertándonos de que estamos infringiendo una regla y nos bloquea la subida del archivo al FTP.

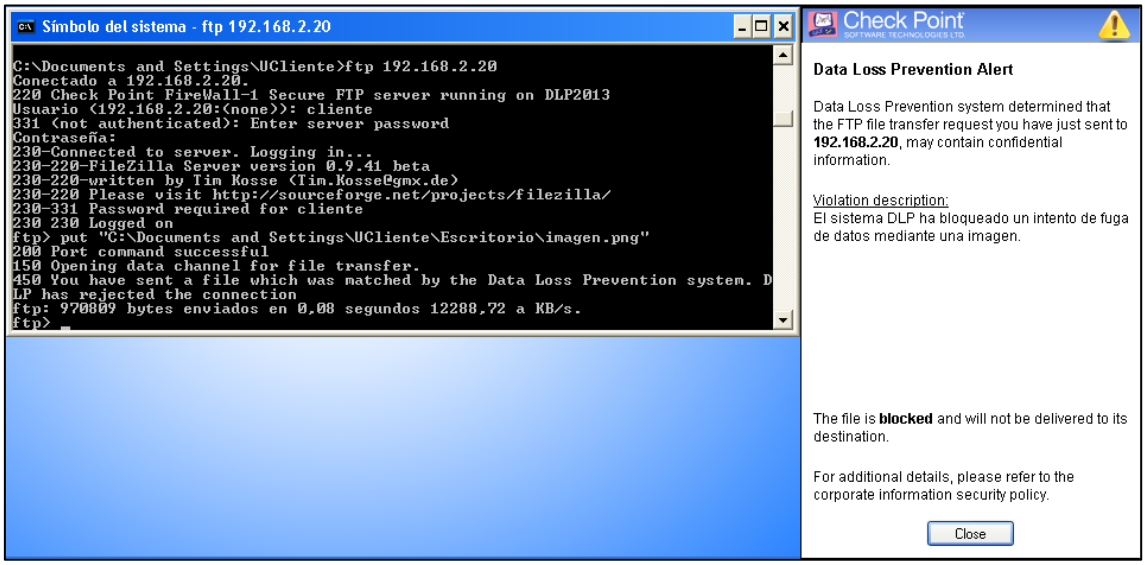

Ilustración 132: Subida de imagen al FTP

La regla tiene asociada una acción *Prevent*, por tanto el fichero no llegará a ser subido al servidor. La incidencia queda registrada y puede ser visualizada en SmartView Tracker, programa a disposición del administrador para revisar las incidencias ocurridas. En él se observa toda la información relacionada con la misma.

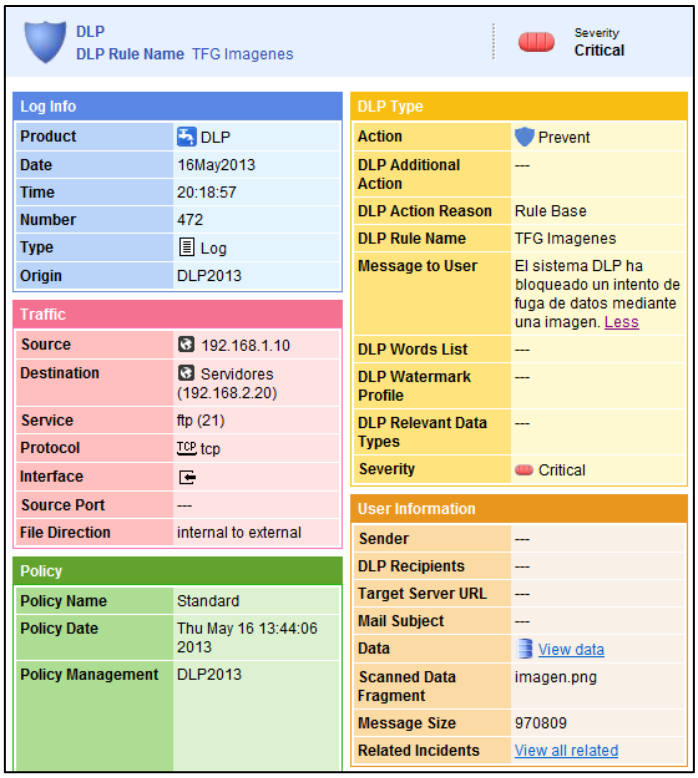

Ilustración 133: Visualización incidencia subida de imagen al FTP

3.4.3. Facturas

Hemos creado una factura en formato Excel xlsx con una estructura similar al subido en la regla Facturas definida en el apartado anterior.

Hemos tratado de subirla desde un cliente FTP como FileZilla a un servidor FTP. La regla Facturas inspecciona un documento y lo compara con la plantilla subida. Al definir un porcentaje de coincidencia en el Data Type al 50% el sistema detectará una fuga de datos si supera ese porcentaje.

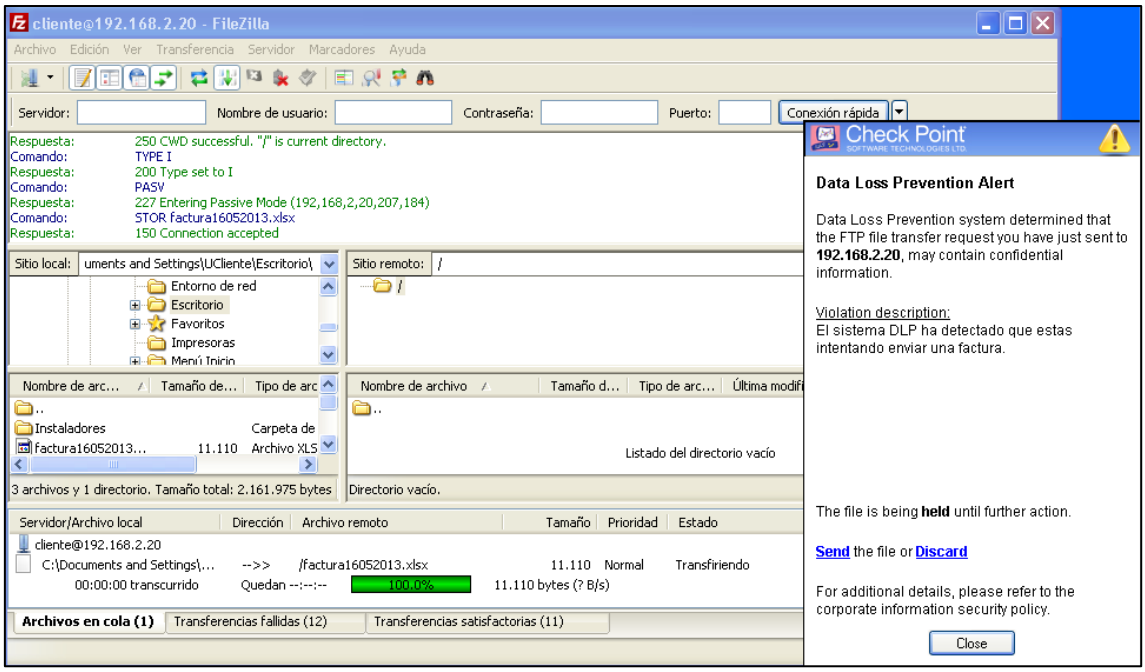

Ilustración 134: Subida de factura al FTP

La regla definida tiene asociada la acción *Ask User*, por lo que nos mostrará una notificación preguntándonos si estamos seguros de querer continuar con la subida del fichero o si queremos descartarlo.

Si decidimos enviarlo el archivo se subirá al servidor, por el contrario, si decidimos descartarlo el archivo no se subirá al servidor. No obstante, en ambos casos la incidencia quedará registrada en el log de SmartView Tracker.

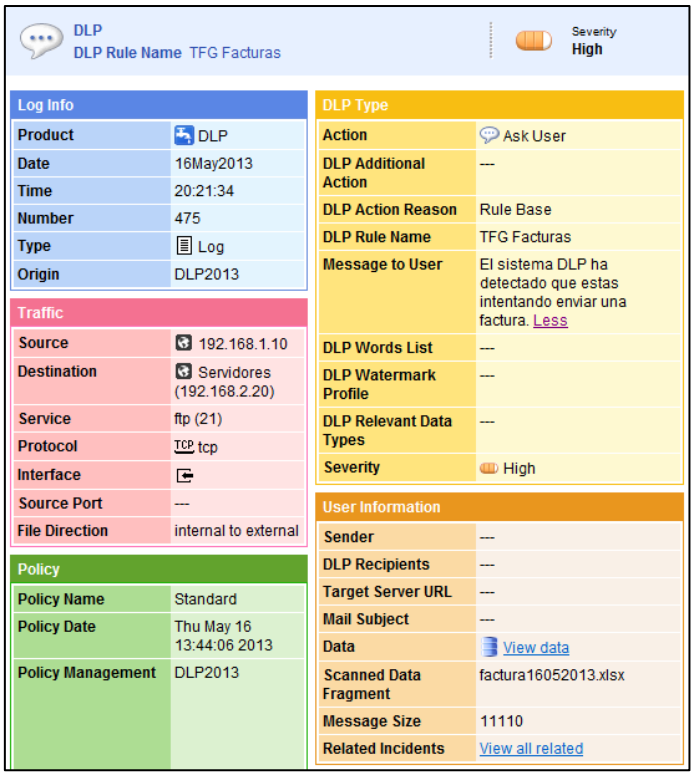

Ilustración 135: Visualización incidencia subida de factura al FTP

3.5. Pruebas HTTP

Para comprobar el comportamiento del sistema DLP creado sobre el protocolo HTTP ha sido necesaria la creación de una página web de pruebas. La página web está alojada en la máquina virtual de servidores y es posible acceder a ella desde la URL http://192.168.2.20/web. Para la creación de la web se ha utilizado el gestor de contenidos Joomla! 3.0 y como soporte al mismo el conjunto de servicios XAMPP, el cual incluye servidor Apache, MySQL y soporte para lenguajes PHP y Perl.

El único requisito software que necesitan los clientes para visualizarla es un navegador como Internet Explorer, Mozilla Firefox o Google Chrome. En nuestro caso tenemos instalado en la máquina cliente el navegador Mozilla Firefox.

Esta página web está dotada de un apartado llamado *Contact Us*, el cual nos proporciona un formulario de entrada de datos como Nombre, e-Mail, Asunto y Descripción. Este formulario lo utilizaremos para llevar a cabo las pruebas de algunas reglas definidas en la política.

3.5.1. Palabras malsonantes

En la primera prueba para el protocolo HTTP trataremos de infringir la regla de Palabras malsonantes. Para ello utilizaremos el formulario de contacto para escribir un mensaje con palabras inapropiadas para la política de la empresa.

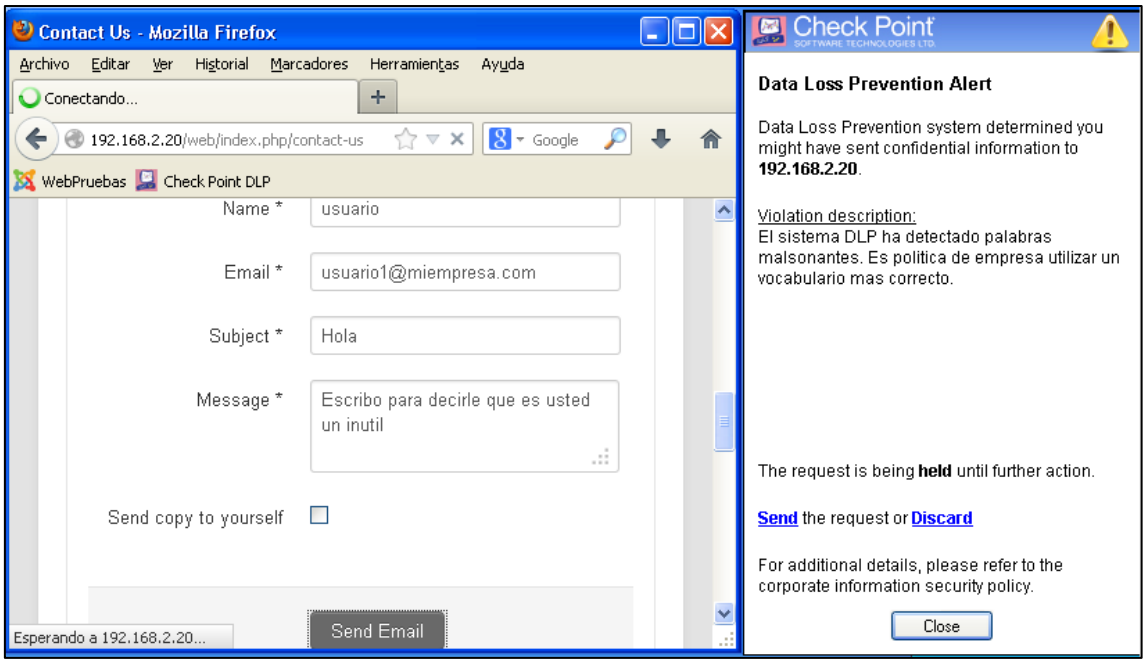

Ilustración 136: Incumplimiento de la regla Palabras malsonantes

Como podemos observar en la captura, nuestro cliente UserCheck nos advierte del incumplimiento de esta regla dotada con la acción *Ask User*. Por tanto la notificación que aparece nos permite decidir si queremos continuar y enviar el mensaje o, por el contrario, descartarlo.

La incidencia quedará registrada y visible para el administrador del sistema DLP. Gracias a la herramienta SmartView Tracker podremos ver el log de incidencias y haciendo doble clic sobre ella veremos una serie de detalles acerca de la misma, tal y como se muestra a continuación.

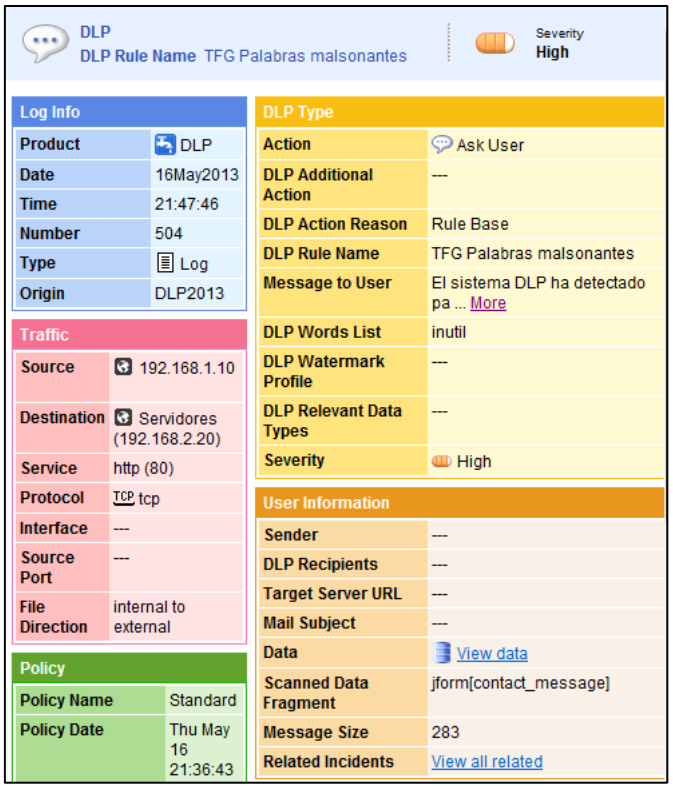

Ilustración 137: Incidencia en regla Palabras malsonantes

En nuestro caso, la decisión acerca de si continuar con el envío del formulario o no, fue que no se enviase, por lo que la elección quedó registrada en el log de la siguiente manera.

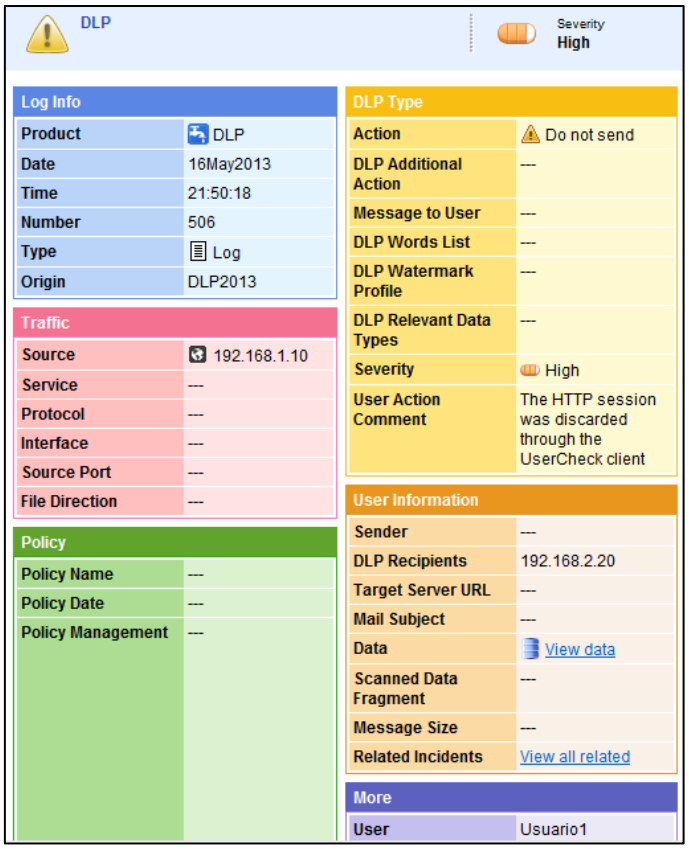

Ilustración 138: Decisión de descarte del envío

3.5.2. Números de teléfono

En la siguiente prueba utilizaremos el mismo formulario de la web de pruebas para tratar de infringir la regla Números de teléfono. Para ello rellenaremos el formulario con el envío de un par de teléfonos.

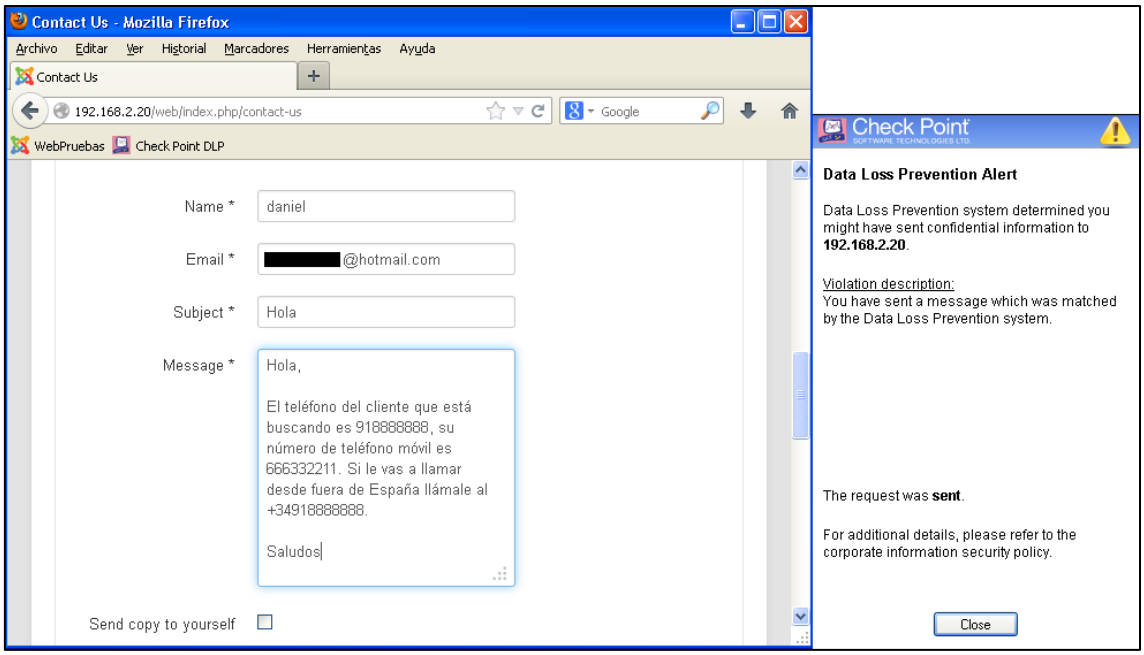

Ilustración 139: Incumplimiento de la regla Números de teléfono

Como se muestra en la captura anterior, una notificación aparece en nuestra máquina advirtiendo el incumplimiento de la regla. Esta regla, al tener asociada la acción *Inform User*, simplemente nos avisa de que la incidencia ha quedado registrada pero que la información ha sido enviada.

La incidencia quedará registrada y visible para el administrador del sistema DLP. Gracias a la herramienta SmartView Tracker podremos ver el log de incidencias y haciendo doble clic sobre ella veremos una serie de detalles acerca de la misma, tal y como se muestra a continuación.

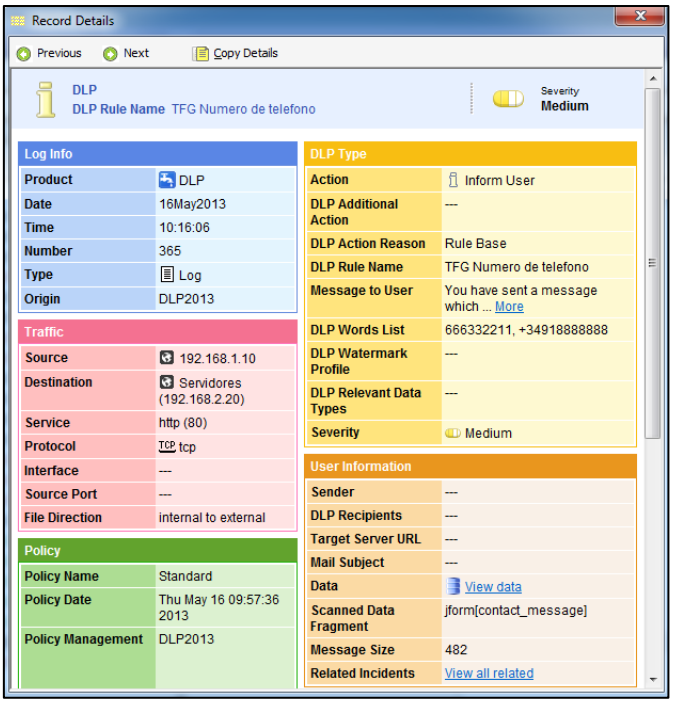

Ilustración 140: Incidencia en regla Números de teléfono

3.6. Pruebas HTTPS

Para observar el comportamiento del sistema DLP sobre el protocolo HTTPS se van a realizar las pruebas de un modo similar al utilizado sobre el protocolo HTTP. La diferencia entre ambos protocolos es que el protocolo HTTPS cifra el contenido de las tramas, lo que podría permitir camuflar datos fugados en sistemas DLP que no tengan soporte para este protocolo.

El modo de actuar que tiene este sistema DLP con este protocolo es actuar como Man in the Middle, es decir, el sistema DLP se encuentra entre el cliente y el servidor web, actuando como un cliente para el servidor web y como un proveedor para el cliente, tal y como muestra el siguiente esquema.

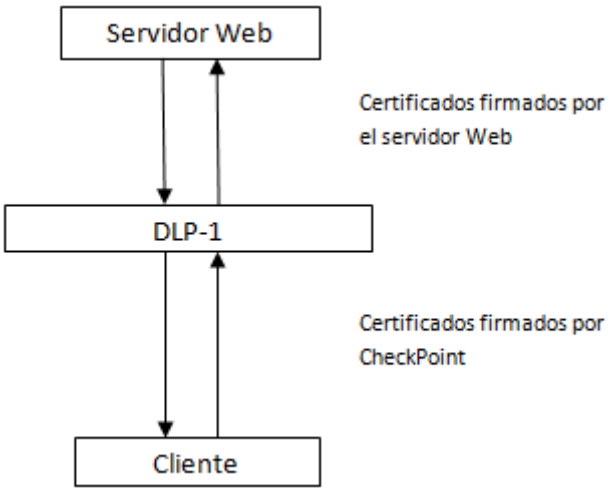

Ilustración 141: Comportamiento ante HTTPS

Para habilitar esta funcionalidad, debemos abrir desde la máquina Management la herramienta SmartDashboard. En la pestaña *Firewall* seleccionamos el icono que representa a nuestro sistema DLP y hacemos doble clic para acceder a sus propiedades generales. En el panel de navegación de la izquierda seleccionamos *HTTPS Inspection.* Una vez en este apartado, debemos seguir los tres pasos que se indican:

- **Paso 1:** Crear o importar un certificado firmado por Check Point, es el certificado que se utilizará para firmar las webs a las que accedan los clientes una vez hayan sido examinadas por el sistema DLP.

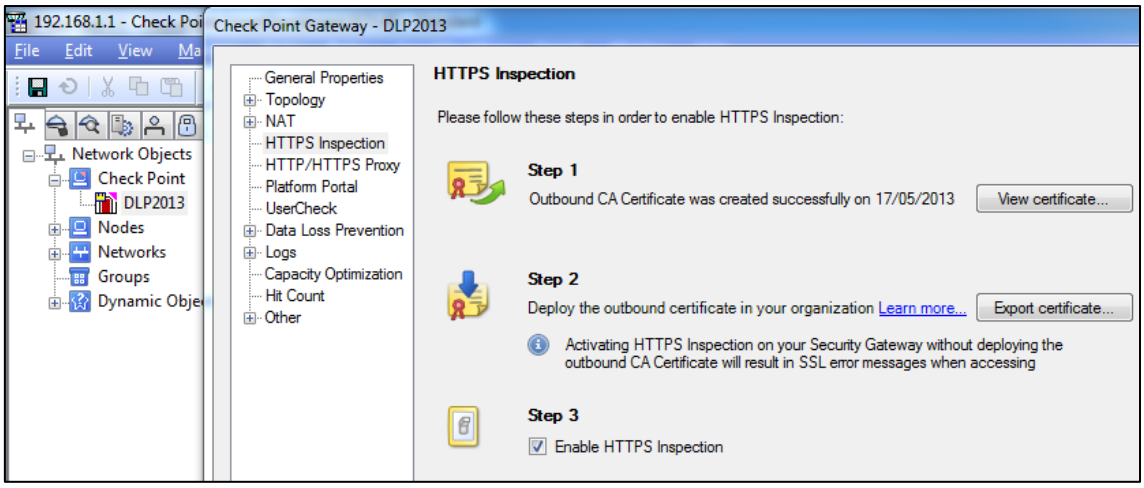

Ilustración 142: Habilitando la inspección del protocolo HTTPS

- **Paso 2:** Exportar el certificado e instalarlo en todas las máquinas de la organización agregándolo a la lista de certificados de confianza del navegador. En nuestro caso, lo agregamos en el navegador de la máquina virtual que ejerce de cliente.

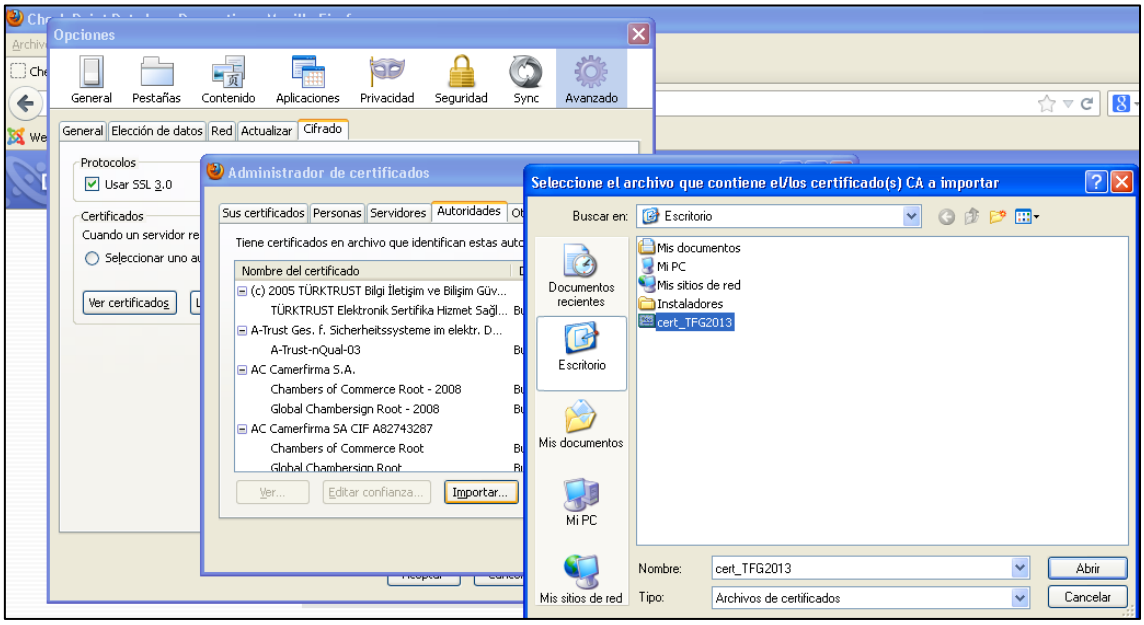

Ilustración 143: Importando el certificado a Mozilla Firefox

- **Paso 3:** Habilitar la inspección del protocolo HTTPS.

Una vez llevados a cabo estos pasos debemos volver a instalar las políticas en nuestro sistema DLP haciendo clic en *Policy* → *Install*.

A partir de ahora, para las pruebas de HTTPS debemos acceder a la web de pruebas utilizando el protocolo HTTPS por lo que debemos indicarlo en la URL de la misma: https://192.168.2.20/web/.

3.6.1. Cuenta bancaria

En la primera prueba de éste protocolo observaremos el comportamiento del sistema DLP ante la regla Cuenta bancaria. Para ello utilizaremos el mismo formulario web que hemos utilizado en pruebas anteriores, en la pestaña *Contact Us* de la web de pruebas.

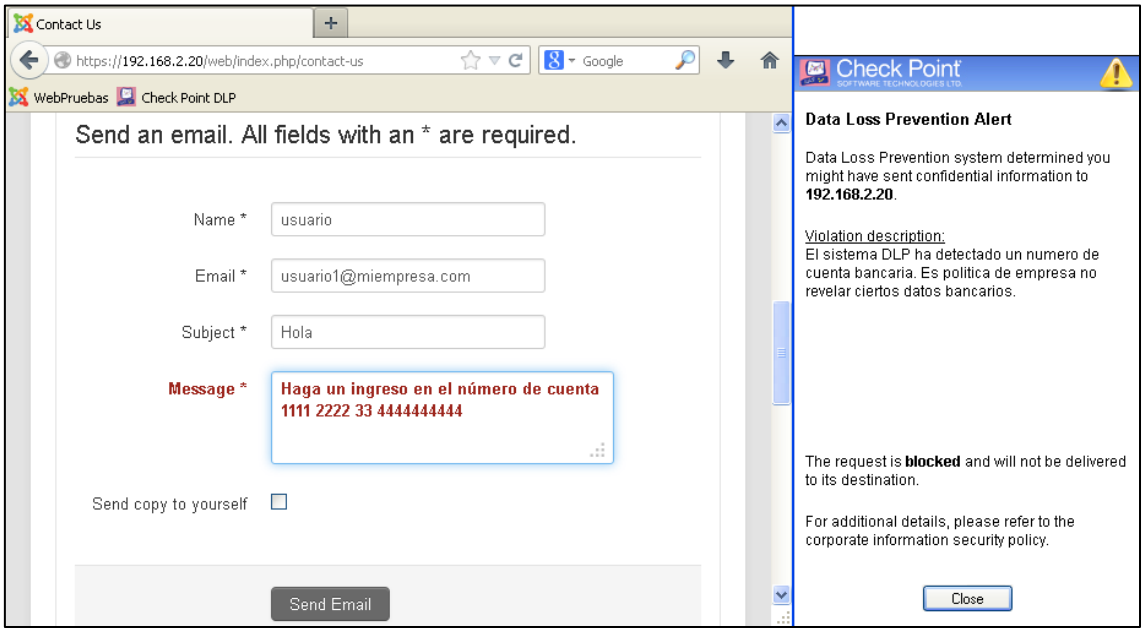

Ilustración 144: Infringiendo regla Cuenta bancaria

Como muestra la captura, la regla Cuenta bancaria está definida con una acción *Prevent*, la cual nos genera una notificación indicándonos que la petición HTTPS ha sido bloqueada.

La incidencia quedará registrada y visible para el administrador del sistema DLP. Gracias a la herramienta SmartView Tracker podremos ver el log de incidencias y haciendo doble clic sobre ella veremos una serie de detalles acerca de la misma, tal y como se muestra a continuación.

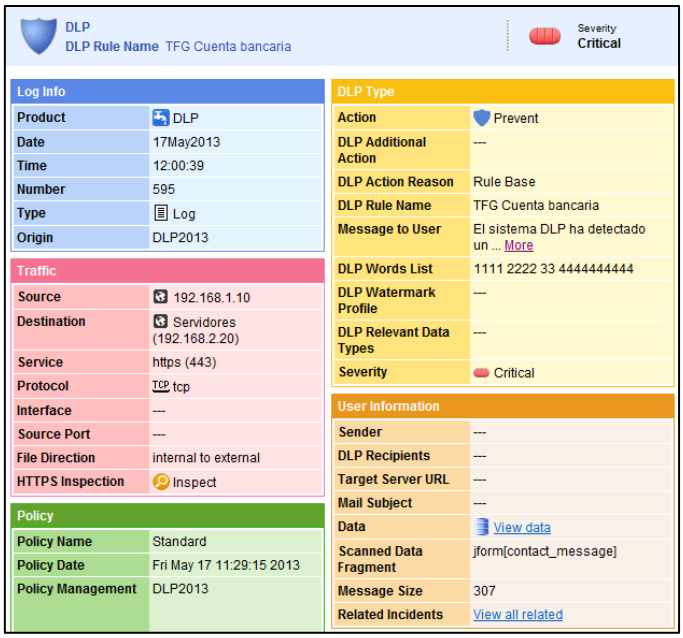

Ilustración 145: Incidencia en regla Cuenta bancaria

3.6.2. DNI

En la primera prueba de éste protocolo observaremos el comportamiento del sistema DLP ante la regla DNI. Para ello utilizaremos el mismo formulario web que hemos utilizado en pruebas anteriores.

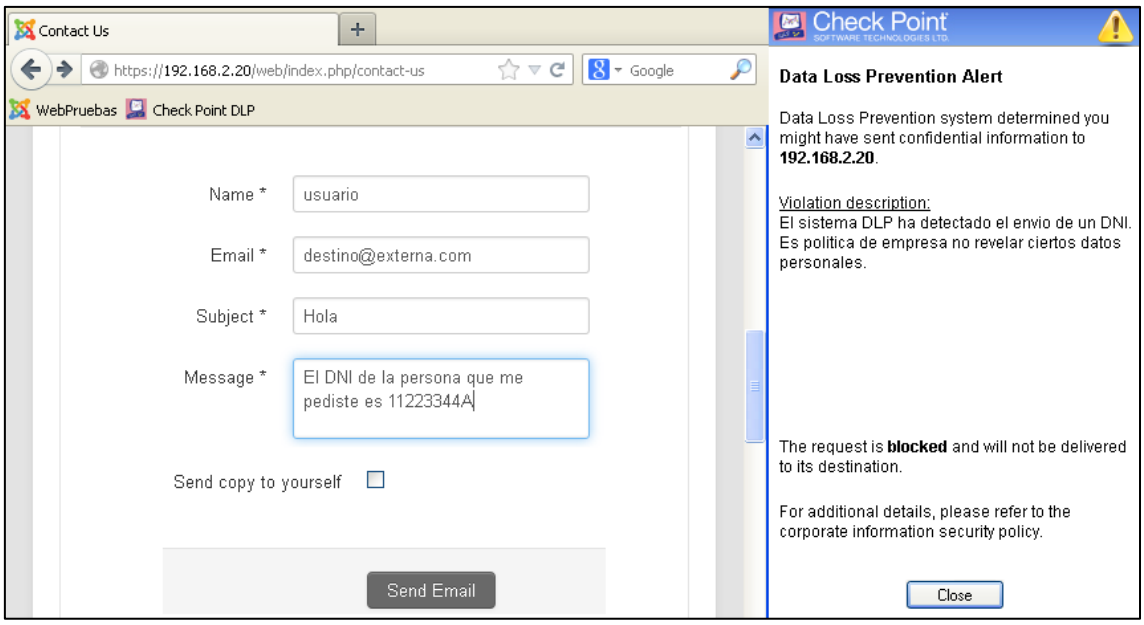

Ilustración 146: Infringiendo la regla DNI

Como muestra la captura, la regla DNI está definida con una acción *Prevent*, la cual nos genera una notificación indicándonos que la petición HTTPS ha sido bloqueada.

La incidencia quedará registrada y visible para el administrador del sistema DLP. Gracias a la herramienta SmartView Tracker podremos ver el log de incidencias y una serie de detalles acerca de la misma, tal y como se muestra a continuación.

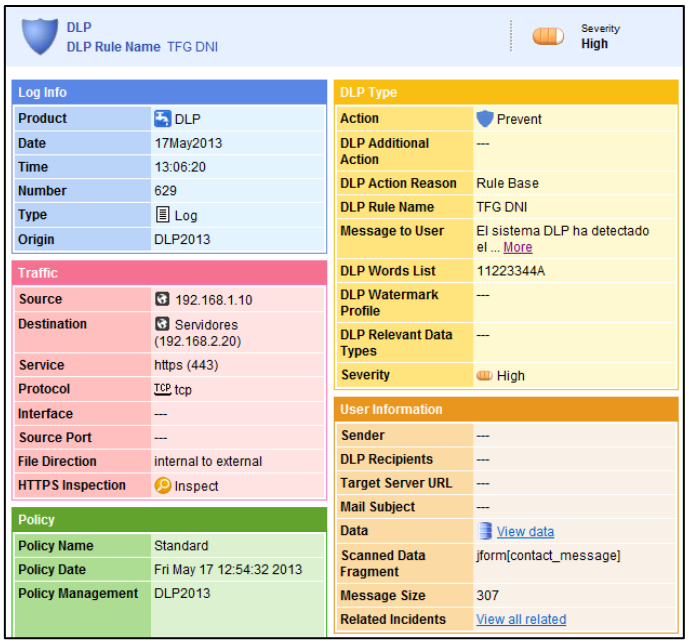

Ilustración 147: Incidencia en regla DNI

3.7. Pruebas SMTP

Para comprobar el funcionamiento del sistema DLP implementado sobre el protocolo SMTP, vamos a intercambiar mensajes de correo electrónico entre dos cuentas de correo electrónico. Estos mensajes llevarán la información de manera escrita en el cuerpo del correo o, como suele ser más común en la vida real, en archivos adjuntos.

Tal y como hemos visto en el apartado de la creación del laboratorio, utilizaremos como servidor de correo electrónico el software ArGoSoft Mail Server Pro 1861 y como cliente de correo electrónico el software Foxmail 6.5.

3.7.1. Información confidencial

En esta prueba vamos a tratar de infringir la regla Información confidencial, para ello escribiremos un correo con información sospechosa de fuga de datos.

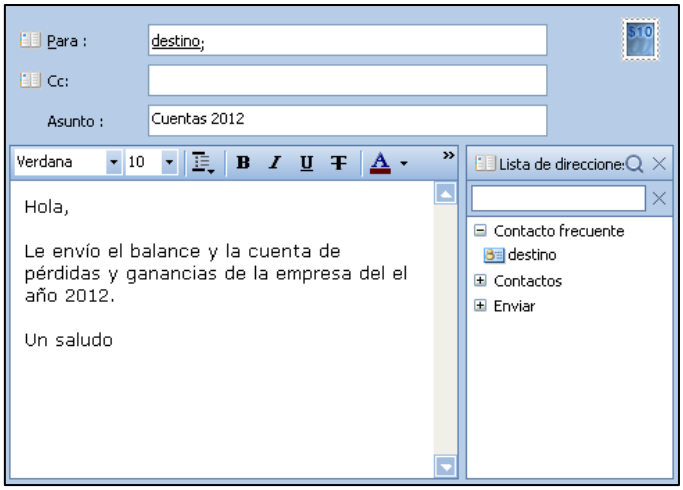

Ilustración 148: Infringiendo la regla Información confidencial

La regla Información confidencial tiene asociada una acción *Detect*. Esta acción no muestra ninguna notificación al usuario que ha infringido la regla pero, no obstante, la incidencia queda registrada en el log de incidencias que tenemos visible a través de la herramienta SmartView Tracker.

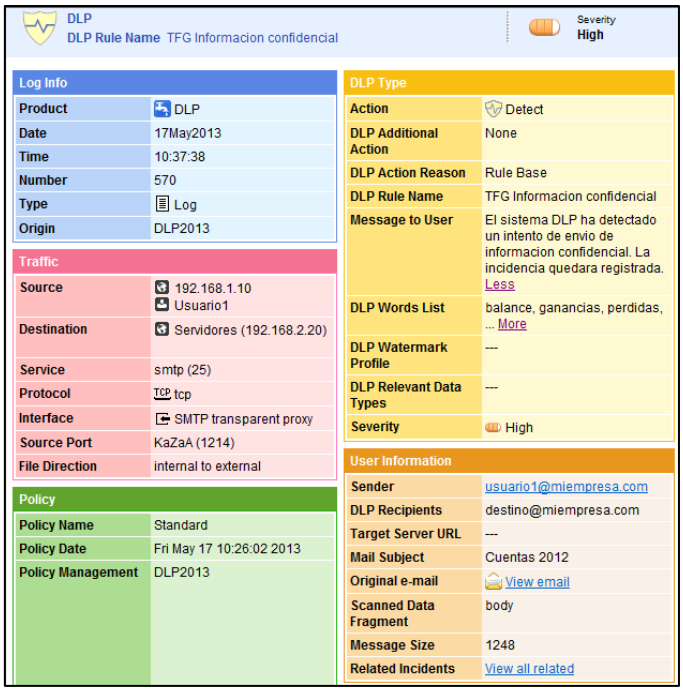

Ilustración 149: Incidencia en regla Información confidencial

3.7.2. Nombres de clientes

En esta prueba vamos a tratar de infringir la regla Nombres de clientes, para ello escribiremos un correo con un fichero adjunto que contenga una lista de clientes de la empresa.

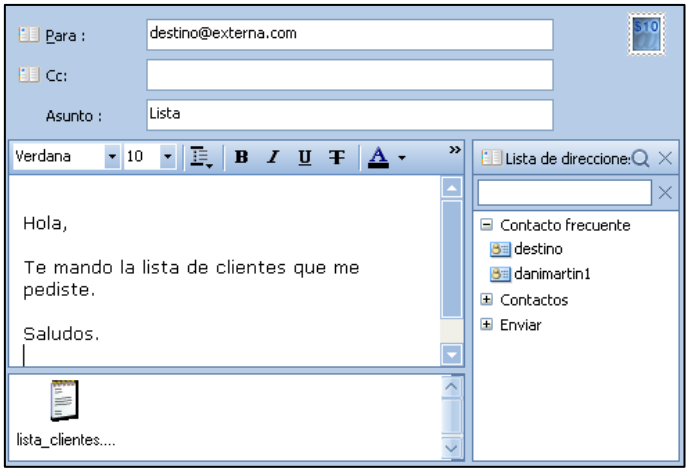

Ilustración 150: Infringiendo la regla Nombres de clientes

Esta regla fue creada con una acción *Inform User*, por lo que se mostrará al usuario una notificación advirtiéndole de que ha infringido una regla de la política DLP y de que la incidencia quedará registrada en el log de incidencias.

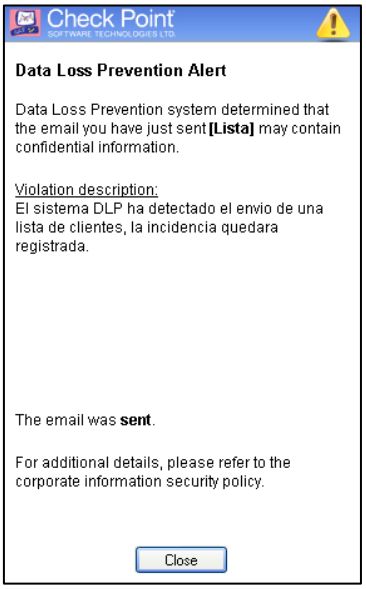

Ilustración 151: Notificación regla Nombres de clientes

Como podemos comprobar, la incidencia ha quedado registrada en el log visible a través de la herramienta SmartView Tracker.

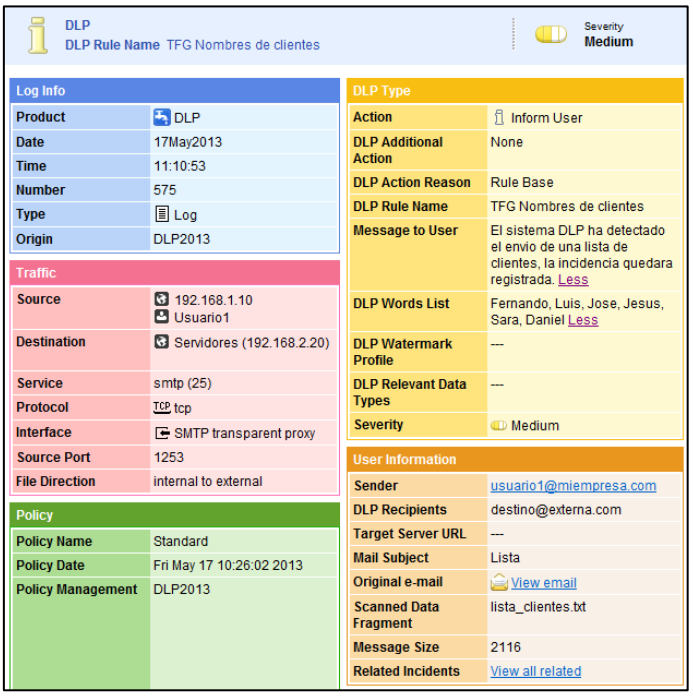

Ilustración 152: Incidencia en regla Nombres de clientes

3.7.3. Ejecutables

Por último, vamos analizar el comportamiento del sistema DLP al infringir la regla Ejecutables definida en la política DLP de nuestra empresa. Para ello escribiremos un correo electrónico que contenga un archivo adjunto que sea un archivo con extensión EXE.

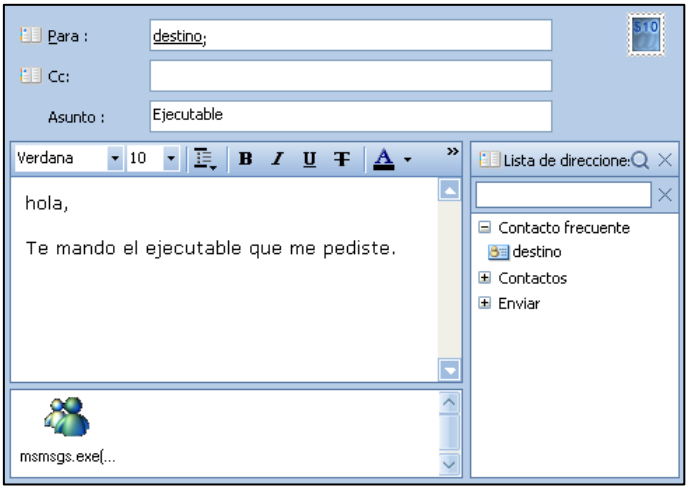

Ilustración 153: Infringiendo la regla Ejecutables

La regla Ejecutables tiene asociada una acción de *Ask User*, por lo que se mostrará al usuario una notificación como la siguiente.

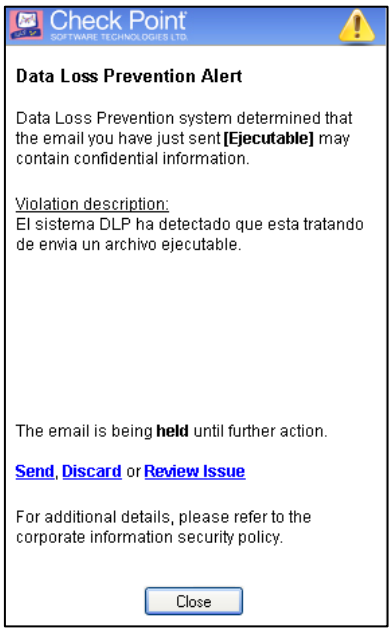

Ilustración 154: Notificación regla Ejecutables

El usuario puede interactuar con esta notificación de tres maneras, enviar, descartar y revisar. Pinchando en la opción revisar se nos abrirá una ventana del navegador con el siguiente aspecto.

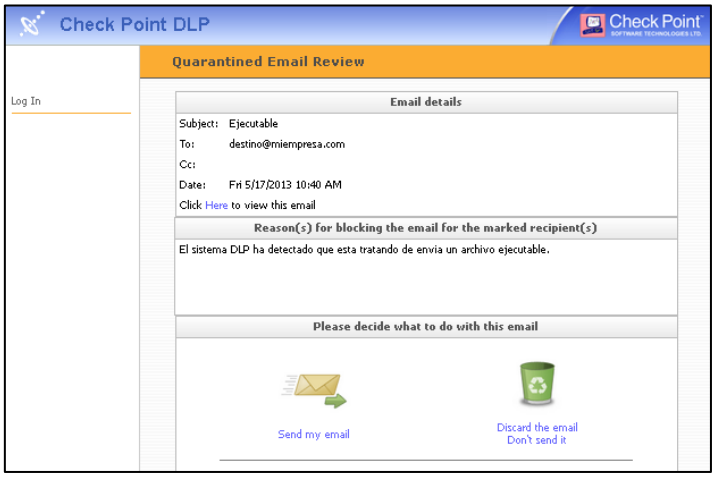

Ilustración 155: Ventana revisión e-Mails en cuarentena

En ella se muestra información acerca del correo electrónico que ha sido interceptado. Si no recordamos a qué correo electrónico se está haciendo referencia podemos verlo haciendo clic en el enlace correspondiente para verlo.

Ilustración 156: Vista de correo interceptado

Si decidimos enviarlo, se nos pedirá un motivo de la decisión tomada, se nos abrirá una ventana solicitando esa información, la cual podrá ser vista en el registro de la incidencia.

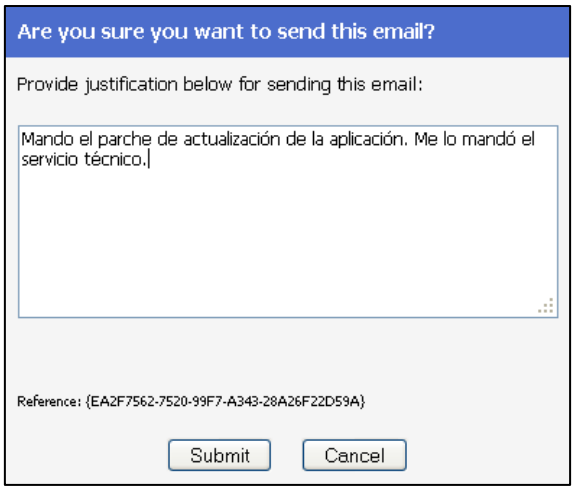

Ilustración 157: Justificación del envío del e-Mail

La incidencia queda registrada en dos partes, la primera muestra el momento del envío del correo electrónico y los motivos de su alerta.

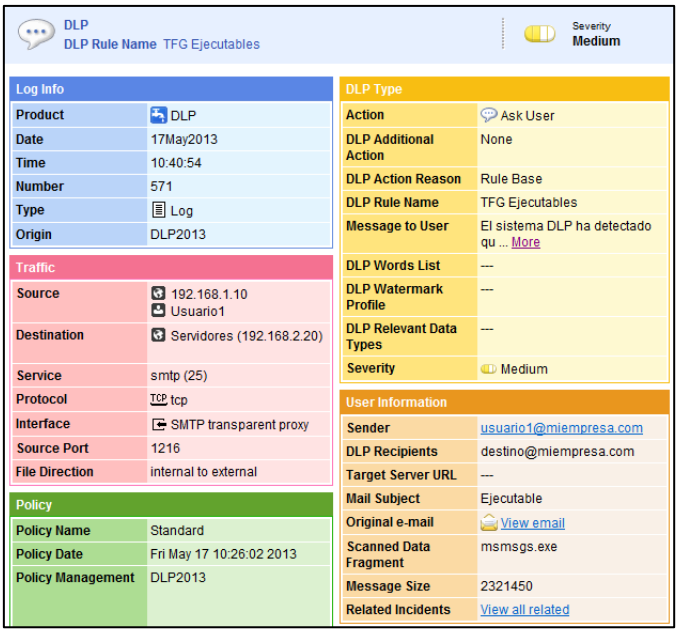

Ilustración 158: Incidencia en regla Ejecutables

La segunda, queda registrada con la decisión tomada por el usuario y la justificación del envío del correo electrónico.

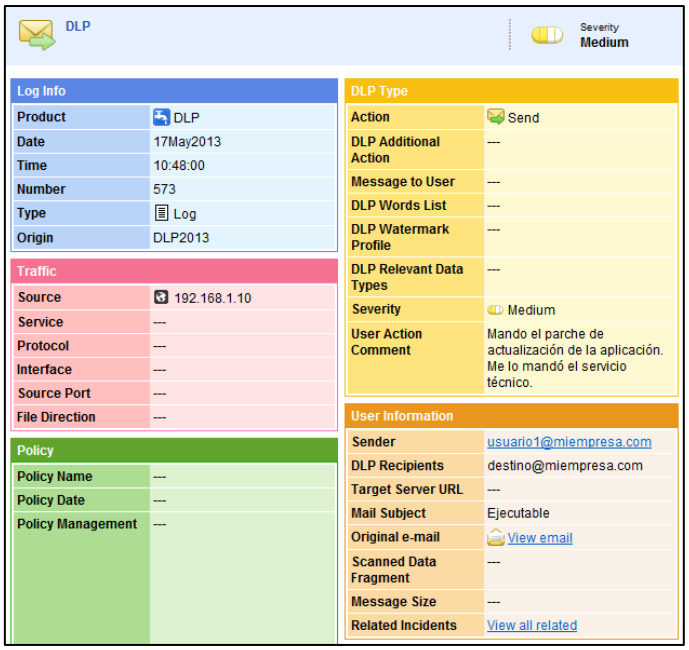

Ilustración 159: Log de justificación de envío de e-Mail

Conclusiones

Debido a su demostrada efectividad, la demanda de sistemas de control de pérdida de datos, o sistemas de Data Loss Prevention, ha crecido de manera considerable. Esto ha provocado un rápido y gran desarrollo en herramientas de éste tipo que, poco a poco, se van integrando de una manera muy eficaz junto con los sistemas de Firewall y proxies en las redes locales corporativas.

La herramienta DLP-1 2571, de la empresa Check Point Software Technologies LTD, es un buen ejemplo de éste tipo de tecnología que cada vez se va implantando en más empresas y que empieza a tomar fuerza de cara al futuro en una industria en la que la fuga de ciertos datos corporativos puede tirar por la borda meses de esfuerzo y trabajo.

Lo visto en este proyecto no es más que una guía de primeros pasos para la instalación del software y el hardware necesario a pequeña escala, en un laboratorio en el que sólo se conectará un cliente para realizar las pruebas. No obstante, lo visto aquí es totalmente adaptable a una empresa, ya que la magnitud de la red no afecta a la configuración y creación de la política DLP.

Esta herramienta cumple totalmente con lo esperado de una herramienta de este estilo, ya que permite una configuración amigable, gestión de incidencias rápida y eficaz y un sinfín de posibilidades más aparte de la funcionalidad DLP como, entre otros, definición de tablas de enrutamiento, reglas de Firewall, configuración de DNS, restricciones de aplicaciones y portales web, funciones anti-bot, anti-virus, anti-spam, securización IP a través de VPNs, etc.

Trabajo futuro

En este trabajo se ha centrado principalmente en la investigación de la base del Data Loss Prevention, el montaje de un laboratorio de pruebas y dar los primeros pasos con la herramienta viendo la configuración inicial y ciertos pasos para la creación de casos prácticos.

Como se puede comprobar, la herramienta utilizada para este trabajo ofrece una gran cantidad más de posibilidades, además del Data Loss Prevention, gracias a las llamadas Software Blades de Check Point. De esta manera, quedan abiertos varios frentes de investigación para continuar probando el funcionamiento de la herramienta, por ejemplo, con funcionalidades Firewall, filtros URL, funcionalidades anti-virus, anti-spam, anti-bots, etc. con el fin de poner a funcionar la herramienta a pleno rendimiento.

Un frente más abierto sería llevar a cabo una implantación de la herramienta en una red real con varios PCs en un mismo laboratorio, con el fin de documentar los pasos recomendados para cualquier empresa que decida implantar un sistema de este estilo en su empresa.

Presupuesto

El desglose del presupuesto de este trabajo de fin de grado se hará teniendo en cuenta varios factores: Mano de obra del trabajador, valor de equipos informáticos, coste de conexiones a Internet y licencias de software.

Hay que destacar que el coste de la herramienta ha sido nulo ya que ha sido proporcionada por la Universidad de Alcalá. Por otro lado, el coste de la licencia de la aplicación ha sido cero también ya que hemos aprovechado las licencias gratuitas de 15 días (activándolas varias veces). No obstante el cálculo del presupuesto se hará teniendo en cuenta estos costes.

Mano de obra

Puesto del trabajador	Salario (euros/día)
Ingeniero	80

Tabla 6: Salario base de un ingeniero

La realización del trabajo fin de grado ha sido de 2 meses y medio, de los cuales he utilizado unos 40 días laborables.

La media de horas utilizadas para la realización del trabajo fin de grado ha sido de unas 4 horas al día. Lo que hace un total de unas 160 horas aproximadas.

Por tanto la mano de obra de un ingeniero para la realización de este trabajo fin de grado es de:

Puesto del trabajador	Días	Salario (euros/día)	Coste total (euros)
Ingeniero	40	80	3.200

Tabla 7: Coste de mano de obra

Coste de equipos informáticos

Equipo	Descripción	Valor (euros)
Portátil Samsung NP300E5A [27]	Equipo utilizado para el alojamiento de las máquinas virtuales, gestión de la herramienta y documentación	599
DLP-1 2571 [26]	UTM utilizado para la arquitectura de la red	9.119,29 *

Tabla 8: Coste equipos informáticos

(*) Coste estimado ya que la Universidad de Alcalá disponía de esta herramienta.

Coste de conexión a Internet

Concepto	Tarifa (euros/mes)	Meses	Coste (euros)
ADSL 10MB	24,90	2	49,80

Tabla 9: Coste de conexión a Internet

Licencia de aplicaciones

Aplicación	Tipo de licencia	Descripción	Coste (euros)
GAiA R75.40 /	15 días	Prueba	0

SmartConsole			
GAiA R75.40 / SmartConsole [26]	1 año	Data Loss Prevention Blade	2.333,82 *

Tabla 10: Coste licencia de aplicaciones

(*) Coste estimado ya que he activado varias veces la licencia de prueba.

Presupuesto total

Concepto	Coste estimado (euros)	Coste real (euros)
Mano de obra	3.200,00	3.200
Equipos informáticos	9.718,29	599
Conexión a Internet	49,80	49,80
Licencia de aplicaciones	2.333,82	0
Coste total	15.301,91	3.848,80
IVA (21 %)	3.213,41	808,25
Coste total (con IVA)	**18.515,31**	**4.657,05**

Tabla 11: Presupuesto total

Bibliografía

Documentación en papel

[1] JAMES F. KUROSE Y KEITH W. ROSS (2010). Redes de computadoras: Un enfoque descendente (5ª Edición) Ed. Pearson.

[2] SARA CARRAL RAMOS (2013). Trabajo fin de grado de la Universidad de Alcalá: Análisis, funcionalidades y propuestas de implantación de la herramienta CheckPoint DLP-1 2571.

[3] CHECK POINT SOFTWARE TECHNOLOGIES (2012). R75.40 DLP Administration Guide, R75.40 Gaia Administration Guide, R75.40 Installation and Upgrade Guide, R75.40 SmartView Tracker Administration Guide.

Documentación digital

[4] SYSADMIN TUTORIALS (2011). Check Point R75 SecurePlatform Installation Part 1: http://www.sysadmintutorials.com/tutorials/check-point/check-point-r75-installation/check-point-r75-secureplatform-installation-part-1/

[5] SYSADMIN TUTORIALS (2011). Check Point R75 SecurePlatform Installation Part 2: http://www.sysadmintutorials.com/tutorials/check-point/check-point-r75-installation/check-point-r75-secureplatform-installation-part-2/

[6] DIGITAL CRUNCH (2012). Check Point VMWare Tutorials: http://digitalcrunch.com/lab/

[7] CHECK POINT SOFTWARE (2012). Unified Threat Management (UTM): http://www.checkpoint.com/products/utm/index.html

[8] WIKIPEDIA (2013). Unified Threat Management: http://es.wikipedia.org/wiki/Unified_Threat_Management

[9] CHECK POINT SOFTWARE TECHNOLOGIES (2012). Check Point presenta el sistema operativo de seguridad unificada GAiA con su nuevo software Blade R75.40: http://cxo-community.com/articulos/blogs/blogs-seguridad-informatica/4842-presenta-check-point-el-sistema-operativo-se-seguridad-unificada-gaia-con-su-nuevo-software-blade-r7540.html

[10] ERMEST HARD AND SOFT (2010). Configuración CheckPoint NG: http://www.ermez.com/soporte/documentacion/Todos/AQCT_NET/Web/Recepcion_Envio/Configuracion_CheckPoint_NG.htm

[11] WIKIPEDIA (2013). Cortafuegos: http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

[12] WIKIPEDIA (2013). Proxy: https://es.wikipedia.org/wiki/Proxy

[13] WIKIPEDIA (2013). Redes de computadores: https://es.wikipedia.org/wiki/Red_de_computadoras

[14] CHECK POINT SOFTWARE TECHNOLOGIES(2012). Check Point GAIA: http://www.checkpoint.com/gaia/

[15] DEVILBSD(2012). Check Point Security Gateway R75.40 Curso Práctico: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDgQFjAA&url=http%3A%2F%2Fmictlan.webfactional.com%2Fdownload%3Ffile%3Dcptrainning%2FR75.40_Curso_Practico.pdf&ei=EnqDUfnZLamg7Abd1oDYBw&usg=AFQjCNF7UdncCQVS8uJQ1rUM-9ThBegz5g&sig2=jnt9IQbGWsnTtk_Yf82IcQ&bvm=bv.45960087,d.ZGU

[16] UNIVERSIDAD DE SAN CARLOS DE GUATEMALA (2012). Instalación Firewall Checkpoint R70: http://www.slideshare.net/symple9/instalacin-firewall-checkpoint-r70

[17] NDM TECHNOLOGIES (2012). Checkpoint DLP-1 2571: http://www.ndm.net/ips/checkpoint/checkpoint-dlp-1-2571#twoj_fragment1-3

[18] NDM TECHNOLOGIES (2012). Datasheet DLP-1 2571: http://www.ndm.net/ips/pdf/checkpoint/DS_DLP-1_2571.pdf

[19] HANS STEFFENS (2010). Prevención de fuga de datos (DLP) en 5 sencillos pasos: http://liacolombia.com/2010/09/prevencion-de-fuga-de-datos-dlp-en-5-sencillos-pasos/

[20] FLORENCIO CANO (2012). ¿Qué es el "Data Loss Prevention"?: http://www.seinhe.com/blog/42-que-es-el-data-loss-prevention

[21] KARL-HEINZ HOLTSCHMIT (2010). Data Loss Prevention: http://www.isacamty.org.mx/archivo/Evento%20Anual%202010.pdf

[22] CHECK POINT SOFTWARE TECHNOLOGIES (2012). Gaia Portal Administrator Guide: http://dl3.checkpoint.com/paid/e5/CP_R75.40VS_Gaia_AdminGuide.pdf?HashKey=1368003448_959ebd42ebe9cd2137afe57c1e0f7c7d&xtn=.pdf

[23] PEARSON EDUCATION (2011). SmartDashboard: http://www.pearsonhighered.com/samplechapter/0789731096.pdf

[24] ERIE COMPUTER COMPANY AND COSTCENTRAL (2010). Precio DLP-1 2571: http://www.costcentral.com/searchresults.php?keywords=dlp-1+2571&x=-742&y=-46

[25] CHECK POINT SOFTWARE TECHNOLOGIES (2013). UserCheck Client: https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/84372.htm

[26] CHECKFIREWALLS (2013). Checkpoint DLP-1 2571: http://www.checkfirewalls.com/DLP-1-2571.asp

[27] SAMSUNG (2013). Samsung NP300E5A: http://www.samsung.com/us/computer/laptops/NP300E5A-A01UB

Universidad de Alcalá
Escuela Politécnica Superior

ESCUELA POLITECNICA
SUPERIOR

Universidad
de Alcalá