laSalle
UNIVERSITAT RAMON LLULL

Escola Tècnica Superior d'Enginyeria
Electrònica i Informàtica La Salle

Treball Final de Màster

Màster Universitari en Enginyeria de Telecomunicació

PROYECTO DE IMPLEMENTACIÓN DE MCAFEE EPOLICY ORCHESTRATOR 5.9.1 Y PRUEBA DE CONCEPTO DE CIFRADO DE UNIDADES EXTRAÍBLES

Alumne
Ferran Angulo Montserrat

Professor Ponent
Christian Adell Querol

ACTA DE L'EXAMEN DEL TREBALL FI DE CARRERA

Reunit el Tribunal qualificador en el dia de la data, l'alumne

D. Ferran Angulo Montserrat

va exposar el seu Treball de Fi de Carrera, el qual va tractar sobre el tema següent:

PROYECTO DE IMPLEMENTACIÓN DE MCAFEE EPOLICY ORCHESTRATOR 5.9.1 Y PRUEBA DE CONCEPTO DE CIFRADO DE UNIDADES EXTRAÍBLES

Acabada l'exposició i contestades per part de l'alumne les objeccions formulades pels Srs. membres del tribunal, aquest valorà l'esmentat Treball amb la qualificació de

Barcelona,

VOCAL DEL TRIBUNAL VOCAL DEL TRIBUNAL

PRESIDENT DEL TRIBUNAL

AGRADECIMINETOS

Para la realización del proyecto de actualización y mejora del antivirus y prueba de concepto de cifrado de unidades extraíbles en la empresa dónde EY está proveyendo el servicio, se ha necesitado la intervención de distintas personas de diversos departamentos que han sido clave para alcanzar el éxito de este. Por este motivo, me gustaría hacer énfasis sobre todas estas personas que, de forma directa o indirecta, se han visto involucrados.

En primer lugar, mis agradecimientos a mis padres, Esther Montserrat y Javier Angulo, por el gran esfuerzo que han realizado siempre para que pudiera tener una buena educación y valores que me han permitido cursar ingeniería telemática y, posteriormente, el Máster Universitario de Ingeniería de Telecomunicaciones. También, agradecer tanto a ellos como a mi entorno personal, especialmente a Clara Pedrerol, Sergi Bosch y Jaume Baltasar, por el apoyo recibido a lo largo de estos últimos años que me han llevado a poder realizar este trabajo final de máster en las mejores condiciones posibles.

Por otro lado, mis agradecimientos al profesor Christian Adell Querol, quién ha sido mi tutor del trabajo final de máster y quién me ha proporcionado apoyo a lo largo del mismo. Además, quiero agradecerle todo el tiempo invertido en las reuniones realizadas que han sido de gran valor e importancia para poder enfocar debidamente el proyecto.

Finalmente, quiero dar mis agradecimientos a la empresa en la que estoy trabajando actualmente, Ernst & Young S.L, por ofrecerme la oportunidad de realizar un proyecto tecnológico de estas características donde he podido desarrollar nuevas habilidades y capacidades dentro de un entorno real, profesional y diverso. Quiero hacer mención especial a mi compañero Sergio Tomás Fernández, quien también ha dado soporte en el proyecto, y a mi mánager Oscar López por la confianza depositada en mí.

RESUMEN

El proyecto tecnológico que se presenta a continuación se enmarca en el ámbito profesional, más concretamente, se trata de un proyecto realizado en uno de los clientes de la empresa Ernst & Young S.L.

Este, pretende realizar una actualización y mejora del antivirus McAfee de la empresa a la versión más reciente, con todos los requerimientos y limitaciones que puedan surgir e identificarse a lo largo del proyecto (en el diseño actual del antivirus, a nivel de Comunicaciones, Infraestructura, gestión de equipos y servidores, etc.) Adicionalmente, se realizará una prueba de concepto (PoC) para implementar el cifrado de unidades extraíbles en la compañía mediante un producto del antivirus McAfee llamado FRP (File and Removable Media Protection).

El principal objetivo del proyecto consiste en identificar el estado actual del antivirus en la compañía, detectar deficiencias, y proceder con un plan de acción para actualizar y mejorar la situación actual del antivirus entorno a la compañía. De este modo, se pretende que todos los equipos puedan disponer del antivirus McAfee ya que actualmente, por deficiencias en el diseño del antivirus, no era así.

Para la realización y elaboración del proyecto, se han definido las distintas fases teniendo en cuenta la situación del antivirus previa al proyecto, y las deficiencias que éste tenía.

Finalmente, el proyecto ha permitido identificar las deficiencias del antivirus, previo al proyecto, y en base a ello, diseñar y desplegar la nueva versión antivirus McAfee para que fuera accesible a todos los equipos de la red de la compañía.

Palabras clave: McAfee ePolicy Orchestrator 5.9.1; Consola Central ePo McAfee; *File and Removable Media Protection;* Prueba de concepto

PRÓLOGO

Para poder entender la necesidad por la cual nace el proyecto, es de vital importancia conocer el contexto y las circunstancias actuales de la empresa cliente.

La empresa cliente, en la que se realiza el proyecto, es una empresa importante del sector de la automoción a nivel internacional. Además, la empresa cuenta con un histórico suficientemente amplio como para tenerlo en cuenta y analizarlo para poder trazar la planificación, diseño y ejecución del proyecto. De este modo, será muy importante conocer la infraestructura y arquitectura de la empresa para poder desplegar el producto de antivirus de McAfee *on-premise* (Infraestructura del cliente), así como identificar cómo se comunican los componentes de la red, equipos y servidores dentro de la misma compañía para poder habilitar las funcionalidades del propio producto de McAfee.

Paralelamente, es importante tener en cuenta que actualmente el cliente tiene desplegado el antivirus de McAfee en su compañía con la peculiaridad que existen limitaciones técnicas derivadas del diseño y despliegue del mismo producto que se realizó en su día. De este modo, estas limitaciones permiten que sólo algunas zonas o “capas” de la red de la compañía se encuentren securizados mediante el antivirus de McAfee, y en cambio otras zonas de la red no dispongan de este servicio. Por este motivo, el principal objetivo del proyecto se basará en poder abastecer de antivirus a todos los equipos y servidores pertenecientes a la red de la compañía.

Adicionalmente, se aprovechará este proyecto para realizar una prueba de concepto para cifrar las unidades extraíbles (por ejemplo los dispositivos de almacenamiento llamados *pen*) en los equipos de la compañía.

De forma resumida, vemos que las fases iniciales del proyecto serán de gran importancia para poder trazar un diseño y despliegue del producto eficaz, completo y escalable hacia todos los equipos y servidores de la red interna, garantizando así el éxito del proyecto.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

1. INTRODUCCIÓN

El proyecto que se presenta a continuación se enmarca en el ámbito profesional, en concreto, se muestra la planificación, diseño y ejecución del producto antivirus de McAfee para su despliegue a todos los equipos y servidores de una compañía líder en el sector de automoción y cliente de EY, empresa en la que actualmente se encuentra trabajando Ferran Angulo, realizador del proyecto.

Actualmente, y previo a este proyecto, la compañía dispone de antivirus McAfee sólo en algunos servidores y equipos ubicados en una determinada zona de la red de la compañía. Esta limitación, que puede suponer un gran riesgo a nivel de seguridad, ha llevado a la empresa a tener que contratar la empresa EY para realizar un proyecto que permita tener toda la red en un entorno seguro y monitorizado mediante el producto antivirus de McAfee.

Por lo tanto, el principal propósito de este proyecto es entender la arquitectura, infraestructura y comunicaciones entre las distintas capas de la red del cliente, para así, diseñar la arquitectura que permita abastecer a todas las capas de la red de la compañía con el antivirus de McAfee.

Adicionalmente, y una vez realizado el despliegue del antivirus exitosamente, se procederá a realizar una prueba de concepto de un nuevo módulo de McAfee llamado FRP (*File and Removable Media Protection*) para configurar el cifrado de las unidades extraíbles como, por ejemplo, los dispositivos de almacenamiento llamados *pen.*

1.1. Conceptos previos

Antes de profundizar en materia e ir más en detalle, se mencionan y desarrollan, aquellos conceptos básicos y claves para una mejor comprensión:

- **McAfee ePolicy Orchestrator 5.3.1:** versión de la plataforma que se ha utilizado en la compañía hasta la llegada del actual proyecto. Esta plataforma permite centralizar la administración de los equipos finales, asegurando así una correcta implementación de las políticas de seguridad.
- **McAfee ePolicy Orchestrator 5.9.1**: versión de la plataforma utilizada en el proyecto que permite la administración e implementación centralizada de las directivas de seguridad. Además, lleva a cabo la administración completa de la red, protegiendo los equipos finales o *endpoints* frente a posibles amenazas. Previo al proyecto, la versión que se utilizaba para la plataforma era la versión McAfee ePolicy Orchestrator 5.3.1.
- ***Agent Handler*** o **controlador de agentes:** servidor que permite distribuir el tráfico de red generado por la comunicación agente-servidor mediante la dirección de los sistemas gestionados o los grupos de sistemas a un controlador de agentes concreto. Una vez dirigido, un sistema gestionado se comunica con el controlador de agentes asignado en el lugar del servidor de McAfee ePo principal permitiendo así una mayor escalabilidad. Asimismo, el controlador de agentes permitirá proporcionar a todos los sistemas gestionados asignados *Sitelist*, directivas creadas en McAfee ePo principal,

caché del contenido del Repositorio principal para que los agentes puedan extraer paquetes de actualización de productos, archivos DAT y cualquier otra información necesaria.

- **Repositorio distribuido *o Distributed Repository:*** los agentes instalados en los sistemas o equipos gestionados obtienen su contenido de seguridad desde repositorios ubicados en el servidor de McAfee ePo. Este contenido mantiene el entorno actualizado. Los *Distributed Repository* no administran directivas, recopilan eventos ni tienen código insertado en ellos. Un repositorio no es más que un archivo compartido ubicado en un entorno al que pueden acceder los clientes. Los repositorios permiten:
    - Software gestionado para su despliegue en los clientes finales o equipos.
    - Contenido de seguridad, como archivos DAT y firmas.
    - Parches y demás software necesario para las tareas cliente que se crean con McAfee ePo.
- **McAfee VirusScan Enterprise** o **McAfee Endpoint Security:** *software* antivirus que se instala en los *endpoints* y que permite gestionar y bloquear las amenazas detectadas en cada uno de los equipos. De esta forma, mediante McAfee VirusScan Enterprise se centraliza la gestión de:
    - **Archivos DAT:** archivos que se actualizan de forma diaria que contienen firmas de virus para proteger los equipos contra amenazas existentes y potenciales.
    - **Archivos extraDAT**: archivos de detección temporal creados por McAfee Labs para detectar y eliminar amenazas que no se han agregado a los archivos DAT diarios.
    - **Versión del motor de análisis**: parte fundamental para el software antivirus de McAfee, McAfee VirusScan Enterprise. Este, se va actualizando de forma automática y actualmente está implementada la versión 6000.8403. El motor de análisis consta de un único archivo llamado “mcscan32.dll” que contiene la lógica del programa para llevar a cabo las siguientes acciones:
        - Analizar archivos en puntos concretos.
        - Procesar y ejecutar coincidencias de patrones de definiciones de virus con datos encontrados en los archivos analizados.
        - Descifrar y ejecutar códigos de virus en un entorno emulado.
        - Aplicar técnicas heurísticas, es decir, técnicas que se basan en estimaciones y aproximaciones para reconocer virus nuevos.
        - Eliminar códigos infecciosos procedentes de archivos legítimos.

- **McAfee Agent:** componente de *software* distribuido de McAfee ePolicy Orchestrator. Permite la descarga y aplicación de políticas, y ejecuta tareas de cliente lanzadas desde el servidor McAfee ePo. Asimismo, permite cargar los eventos del equipo y proporcionar datos adicionales sobre el estado de cada sistema. Se deberá instalar dicho software en todos los equipos que se quieran gestionar (sistemas gestionados).
- **Sistema gestionado:** equipo de la compañía que tiene instalado el *software* McAfee Agent y que por lo tanto, puede ser gestionado desde la consola central McAfee ePolicy Orchestrator. De esta forma, se podrá realizar la instalación de cualquier otro producto de McAfee como McAfee VirusScan Enterprise, lanzar tareas cliente como la actualización del archivo DAT, etc.

Por otra parte, y para tener una visión global de cómo se encuentra estructurada la red del cliente, se explica y se muestran las distintas capas de red dónde se encuentran equipos y servidores, así como los componentes de red más relevantes a tener en cuenta:

- **Capa de publicación (zona desmilitarizada)**: se ubican los servidores web desde dónde se publicarán los servicios a Internet. Adicionalmente, es uno de los dos únicos puntos de conexión a Internet de la compañía.
- **Capa de aplicaciones o *middle***: se ubican los servidores que contienen la parte lógica de las aplicaciones de la compañía, es decir, la aplicación en sí.
- **Capa de *Content Check:*** se ubican los servidores que contienen las bases de datos de las aplicaciones, es decir, vendría a ser el *core* de datos de la compañía.
- **Capa de CBB o interna:** se ubican todos los equipos de los empleados. Adicionalmente, se pueden montar servidores en casos excepcionales y debidamente justificados. Como se puede ver en la siguiente imagen, existe una capa CBB segmentada en dos y donde entre las dos capas se encuentra un IPS para tener una mayor securización del entorno (se explica a continuación).
- **Alteons:** dispositivo de red que permite balancear la carga que se recibe tanto desde dentro de la compañía como desde Internet hacia los servidores de la compañía. Adicionalmente, este dispositivo de red, ubicado en capa de publicación, es utilizado para publicar servicios web o aplicaciones dentro de la compañía para que sea accesibles a los empleados (capa interna o CBB).
- **IPS (*Intrusion Prevention System*):** *software* que controla el acceso a una red para proteger a los sistemas de ciberataques. Permite identificar el tráfico de los paquetes y bloquearlo o permitirlo en función de una serie de reglas o bloquearlo en caso de detección de patrones maliciosos o en caso de que se detecte la explotación de vulnerabilidades de seguridad a través de la red.
- **Proxy:** servidor autorizado para actuar como intermediario entre dispositivos finales y un servidor donde se quieren realizar peticiones, o desde dónde las peticiones del servidor serán recibidas para redirigirlas a los dispositivos finales.
- ***Firewall*:** dispositivo de seguridad de red que monitoriza tráfico de red entrante y saliente y decide si bloquear o permitir dicho tráfico en base a las reglas de seguridad definidas.

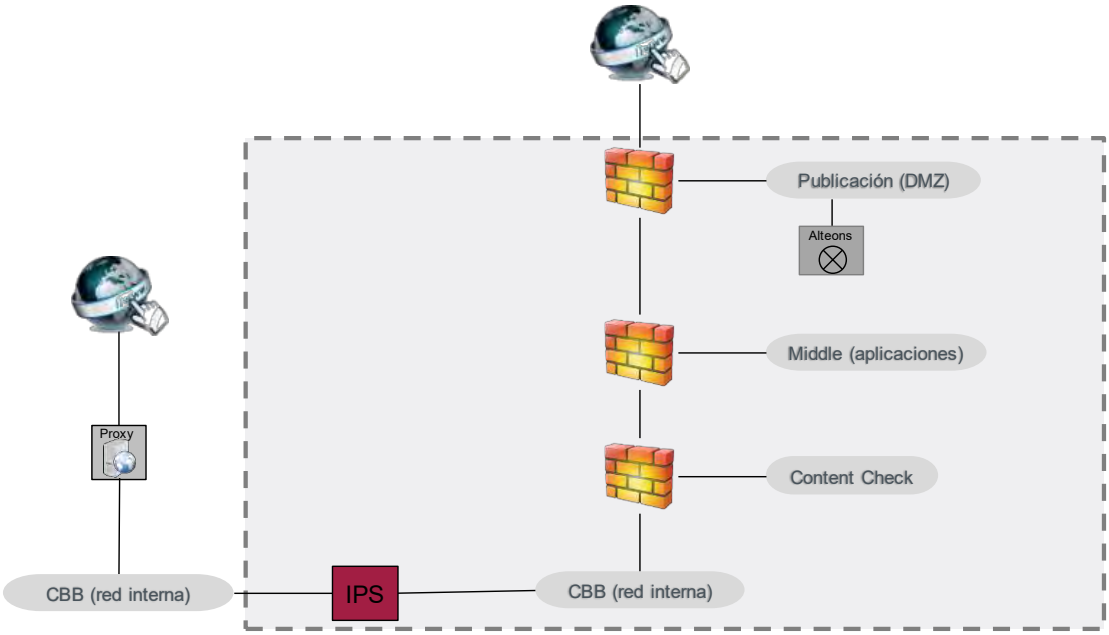


Figura 1: Diseño en capas de la red del cliente

1.2. Diseño actual del antivirus McAfee en la compañía

Tal y como se ha explicado en la introducción, la compañía dispone de antivirus McAfee en equipos y servidores ubicados en zonas determinadas de la red, básicamente los equipos y servidores ubicados en capa interna o CBB. Para poder realizar el nuevo diseño y abastecer a toda la red, es necesario entender el actual. Así se podrá aplicar la mejor solución a nivel de arquitectura, infraestructura y de comunicaciones.

En este sentido, se procede a mostrar el diseño montado actualmente para así explicar las limitaciones derivadas del diseño y entender los puntos de mejora que se implementan en la nueva solución:

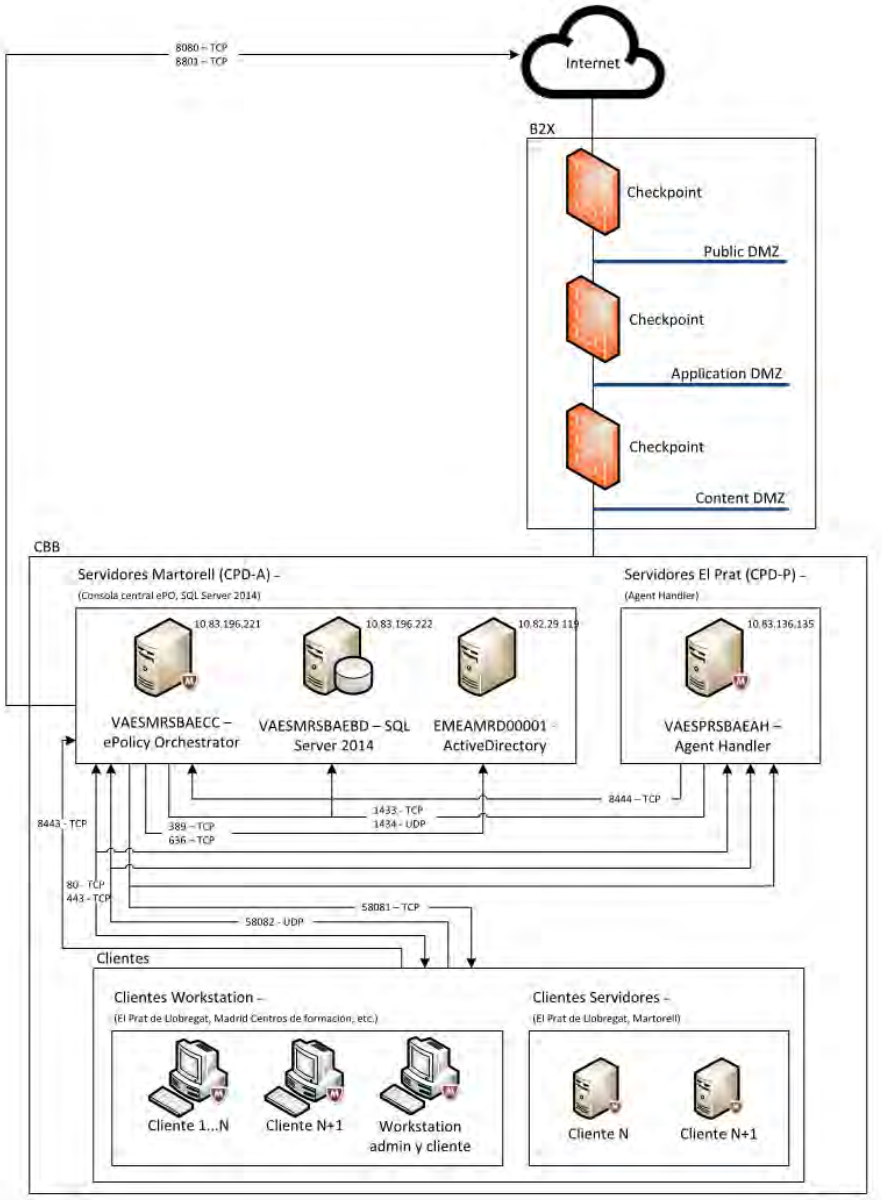


Figura 2: Diseño McAfee ePolicy Orchestrator (versión 5.3.1) actual en la compañía

Gracias al entendimiento del diseño actual, se pueden extraer una serie de conclusiones que permitirán mejorar el diseño y subsanar las limitaciones actuales:

- Tanto la instalación del servidor McAfee ePolicy Orchestrator como la BBDD se encuentran en la capa CBB o red interna, más concretamente en el CPD (Centro de Procesamiento de Datos) ubicado en Martorell.
- En la capa CBB o red interna existen dos zonas delimitadas por un dispositivo de red ya explicado, IPS (que actúa como si fuera un firewall, pero a nivel de paquetes, es decir, su función es ir filtrando los paquetes en busca de tráfico de red sospechoso o malicioso). Este hecho, provoca que a la hora de diseñar la arquitectura se deba contemplar la instalación de un *agent handler* en el CPD del Prat, al otro lado del IPS para agilizar la comunicación entre los equipos/servidores y puedan ser monitorizados de forma escalable y eficiente.
- Como se observa en el diseño, existe una comunicación constante entre los distintos componentes que ofrecen el servicio. Cada flujo de comunicación requiere la apertura de puertos correspondiente en cada servidor. Este hecho será de vital importancia, ya que cuando haya un *firewall* (salto entre capas) de por medio, se deberá solicitar la apertura de dicho tráfico (IP origen, IP destino, puertos) por el *firewall* para que sea permitido y exista la comunicación necesaria. Asimismo, al tratarse del servicio antivirus que va dirigido a todos los equipos de la compañía (y por lo tanto se debería realizar una apertura de puertos para una subred entera) la apertura de puertos sería rechazada por las políticas de seguridad del cliente, ya que se abriría la comunicación para una subred entera. En el actual diseño, esta acción no era necesaria ya que sólo se abastecía la capa CBB o red interna, y por lo tanto no se daba servicio a los servidores de las demás capas, por lo que no había ningún *firewall* de por medio.
- Otro punto relevante a tener en cuenta es que el servidor central, donde se encuentra instalado el McAfee ePolicy Orchestrator, deberá conectarse con el servidor del directorio activo para poder integrar el servicio con las cuentas de la compañía, y por lo tanto, haya una sincronización en todo momento.

1.3. Necesidad del proyecto

Teniendo en cuenta el contexto donde se desarrollará el proyecto, así como el diseño limitado que existe actualmente para ofrecer el servicio de McAfee, surgieron en la compañía una serie de necesidades, objetivo con el cual nace este proyecto:

1. Debido al *end of support* en 2018 de McAfee ePolicy Orchestrator 5.3 es necesario hacer un *upgrade* a la versión 5.9.1.
2. Adicionalmente, se quiere generar una nueva arquitectura de la solución actual para poder acceder a todos los segmentos/capas de la red de la compañía y así abastecer del servicio antivirus a todas las estaciones de trabajo y servidores.

3. Cambiar y actualizar el producto de protección de las estaciones de trabajo a la última versión McAfee Endpoint Security 10.5, producto con más opciones de protección que la actual consola de VirusScan Enterprise 8.8.
4. Realizar una prueba de concepto (PoC) de McAfee *File and removable media protection* o FRP con el objetivo de comprobar la viabilidad de la ejecución del producto, a *posteriori,* en la compañía.
5. Garantizar la securización de todas las estaciones de trabajo y servidores ante cualquier posible ciberataque, *phishing* o *malware*.

2. OBJETIVOS Y ALCANCE

A continuación, se detallan los principales objetivos que tiene por objeto el presente proyecto:

1. Actualizar la consola centralizada de antivirus a la última versión disponible (McAfee ePolicy Orchestrator 5.9.1) en el mercado y abastecer a todos los elementos de la red de la compañía.
2. Dotar a la compañía de un producto de protección (McAfee Endpoint Security) en las estaciones de trabajo y servidores que nos permita aplicar políticas de seguridad más avanzadas y así proteger los activos ante cualquier ciberataque, *phishing* o *malware*.
3. Asegurar el correcto funcionamiento del producto McAfee ePolicy Orchestrator 5.9.1 en todas las estaciones de trabajo y servidores.
4. Realizar una prueba de concepto de la posible implementación de la solución *File and Removable Media Protection* o FRP de McAfee para el cifrado de dispositivos extraíbles para dar cumplimiento a las exigencias de la compañía.

Por otro lado, y para focalizar correctamente los esfuerzos del proyecto, se procede a detallar los componentes que quedan dentro y fuera del alcance del proyecto:

Dentro del alcance	Fuera del alcance
Servidores administrados por la compañía.	Servidores con sistemas operativos UNIX (RedHat, Linux, NetApp OnTap, etc.)
Estaciones de trabajo o *workstations* propiedad de la compañía.	
Workstations de colaboradores externos con maqueta de la compañía.	
Generación de políticas para los servidores corporativos.	

Tabla 1: Alcance del proyecto

3. PLANIFICACIÓN

Tal y como se puede deducir, por la magnitud del proyecto, éste es de vital relevancia para el correcto funcionamiento de la empresa ya que permitirá estar totalmente protegido ante ciberataques o cualquier intento malicioso hacia la compañía. Por este motivo, es muy importante segmentar correctamente las distintas fases e identificar los pasos a seguir para ejecutar correctamente el proyecto con la mínima afectación posible a los empleados, y consecuentemente, a la compañía.
Concretamente, el proyecto se ha dividido en 8 fases que se explican a continuación:

1. **Estudio de la infraestructura y preparación:** como indica la fase, inicialmente será vital entender e identificar el contexto en el que se desarrollará el proyecto. Asimismo, se adquirirá todo el conocimiento previo a la ejecución. Además, se leerá toda la documentación referente al producto McAfee para identificar y solicitar correctamente los requisitos técnicos al departamento de Infraestructura, Comunicaciones o cualquier otro departamento que pueda visto involucrado por el proyecto.
2. **Instalación y configuración de McAfee ePolicy Orchestrator 5.9.1:** una vez entendido el contexto, y con la aprobación de todos los departamentos implicados, se procederá a realizar la instalación y configuración de la última versión del producto de McAfee ePolicy Orchestrator 5.9.1.
3. **Instalación y configuración de McAfee Agent Handler:** siguiendo con el proceso de instalación, se procederá a instalar el *software* de McAfee Agent Handler a los servidores necesarios para poder desplegar correctamente el producto a todos los equipos de la compañía.
4. **Instalación y configuración de *Distributed Repository*:** los servidores que se utilicen como Agent Handler deberán también tener instalado el *software* Distributed Repository. Más adelante, se detallará el motivo de dicho requerimiento.
5. **Análisis del despliegue de los productos a los equipos:** antes de realizar el despliegue del producto en toda la compañía, se realizará una fase piloto para identificar el mejor método de despliegue (se realizarán reuniones con los departamentos involucrados para identificar todas las opciones).
6. **Definición equipos piloto y despliegue de McAfee VirusScan Enterprise:** se seleccionarán una serie de equipos que formaran parte de la fase piloto y se mostrará el detalle de cómo se ha realizado el despliegue del antivirus o McAfee VirusScan Enterprise.
7. **Valoración de los resultados:** llegados a este punto, se realizará un análisis de los resultados obtenidos en la fase piloto que serán presentados a la compañía. Una vez validado por la compañía, se realizará el despliegue a toda la compañía.
8. **Prueba de concepto *File and Removable Media Protection***: por último, se realizará una prueba de concepto para comprobar la viabilidad de la implementación del cifrado de medios extraíbles a toda la empresa.

Para un mayor entendimiento, se muestra la planificación del proyecto en una tabla:

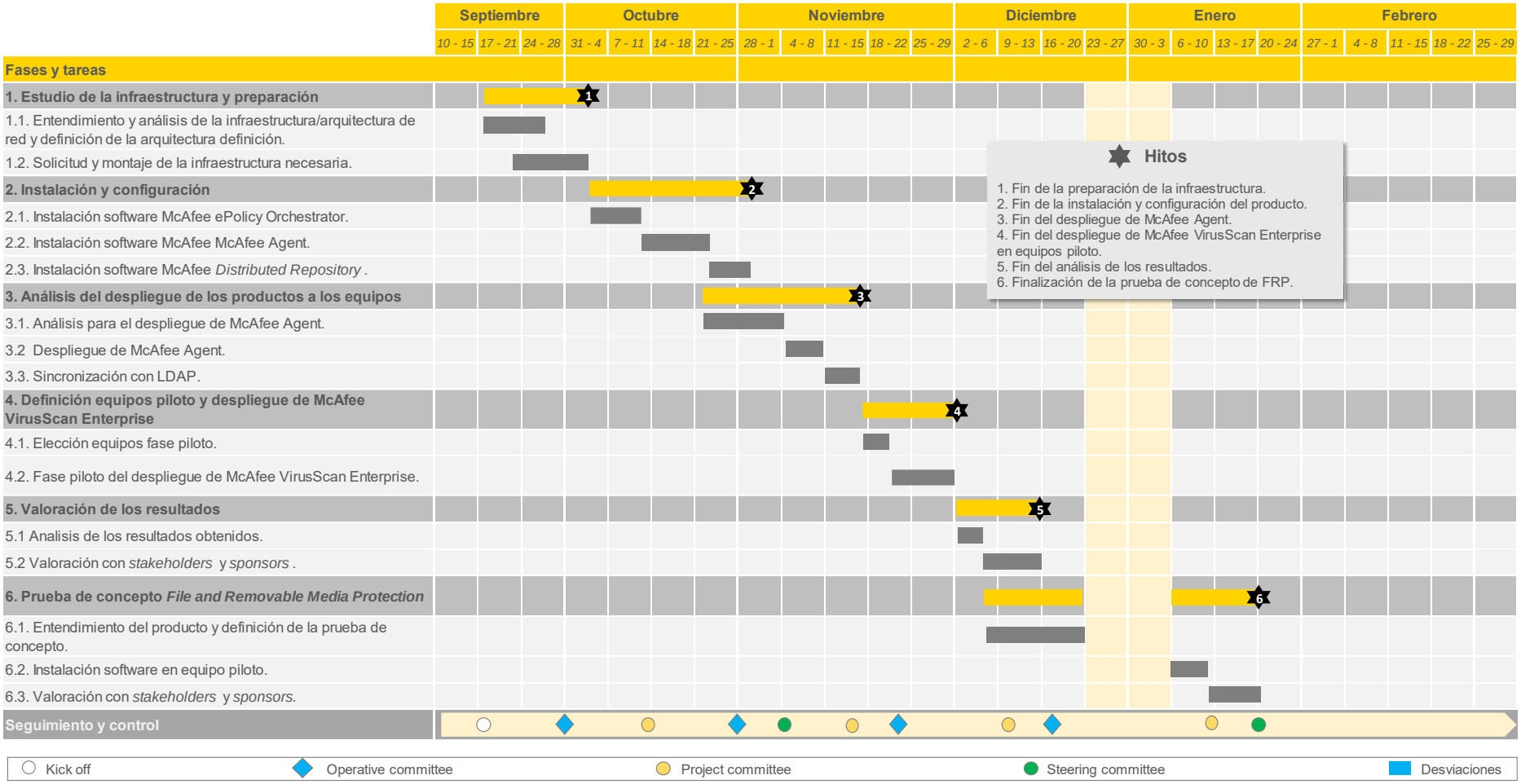


Figura 3: Planificación del proyecto

4. RIESGOS IDENTIFICADOS

En este apartado, se detallan los principales riesgos identificados para que, en todo momento, el cliente sea consciente de los posibles riesgos que puede suponer la ejecución del proyecto en la compañía. Este ejercicio, será de total relevancia para poder realizar el proyecto ya que nos permitirá realizarlo teniendo en cuenta los posibles riesgos que pueden derivarse del mismo, y lo más importante, tenerlo documentado para saber cuál puede ser el impacto, la probabilidad de que ocurra y el riesgo final que supondría para la compañía.

En este sentido, se exponen los conceptos utilizados para dicha valoración:

- **Impacto**: efecto sobre los objetivos del proyecto y/o compañía.
- **Probabilidad**: posibilidad de que, una vez presentada la situación de riesgo, se origine el evento o amenaza.
- **Riesgo**: es el impacto y la probabilidad de que una amenaza o evento puedan afectar de manera adversa la consecución de los objetivos de la compañía.

Una vez identificados los conceptos necesarios para representar los riesgos, será importante poder diferenciar entre los distintos grados de impacto o probabilidad por el que se puede regir un riesgo. Por este motivo, definimos 5 grados:

Impacto	Descripción por grado
Muy Alto	El daño derivado de la materialización de la amenaza tiene consecuencias muy graves para la organización a nivel económico y de pérdida de imagen.
Alto	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización a nivel económico y de pérdida de imagen.
Medio	El daño derivado de la materialización de la amenaza tiene consecuencias moderadas para la organización a nivel económico y de pérdida de imagen.
Bajo	El daño derivado de la materialización de la amenaza tiene consecuencias mínimas para la organización a nivel económico y de pérdida de imagen.
Muy Bajo	El daño derivado de la materialización de la amenaza no tiene consecuencias para la organización a nivel económico y de pérdida de imagen.

Tabla 2:Definición de los 5 posibles grados de Impacto del riesgo

Probabilidad	Descripción por grado
Muy Alta	La amenaza se materializa a lo sumo una vez cada semana.
Alta	La amenaza se materializa a lo sumo una vez cada mes.
Media	La amenaza se materializa a lo sumo una vez al año.
Baja	La amenaza se materializa a lo sumo una vez en un periodo entre 1-3 años.
Muy Baja	La amenaza se materializa a lo sumo una vez cada 5 años.

Tabla 3: Definición de los 5 posibles grados de Probabilidad de materializar el riesgo

Finalmente, después de haber definido los conceptos utilizados para representar el riesgo del proyecto y haber diferenciado los distintos grados de afectación, se detallan los principales riesgos derivados del proyecto:

Descripción riesgo	Impacto	Probabilidad	Riesgo
Bajo grado de satisfacción de los empleados (FRP)	Medio	Medio	Medio
Indisponibilidad del servicio Antivirus	Alto	Bajo	Medio
Retraso en el desarrollo de la solución de infraestructura	Medio	Bajo	Bajo
Pérdida de imagen	Medio	Bajo	Bajo

Tabla 4: Principales riesgos identificados en el proyecto

Para una mejor visualización, mediante los riesgos del proyecto mencionados anteriormente se puede realizar el mapa de riesgos derivado del proyecto:

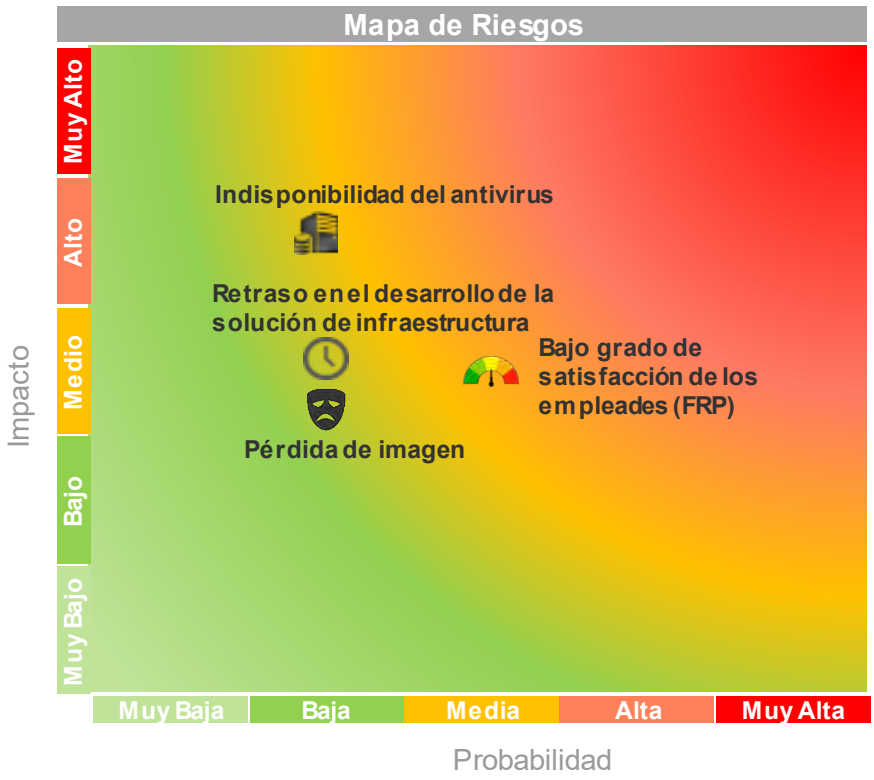


Figura 4: Mapa de riesgos del proyecto

4.1. Gestión de los riesgos identificados

Teniendo en cuenta los riesgos identificados anteriormente, se ha procedido a definir una serie de controles que nos permitirán, como mínimo, estar preparados ante la materialización de cualquiera de los riesgos y proceder a su mitigación al máximo grado posible:

- **Bajo grados de satisfacción de los empleados (FRP):** principalmente, se plantea realizar desde un inicio (fase piloto con usuarios) encuestas a los usuarios para cuantificar el agrado con la herramienta. De esta forma, se podrá predecir la satisfacción de los empleados con la nueva herramienta y tomar las medidas oportunas en función del resultado.
- **Indisponibilidad del antivirus:** en este caso hay dos aspectos importantes a destacar:
  - Actualmente, la compañía sólo ofrece el servicio antivirus a una zona de red de la compañía. Por lo tanto, cualquier indisponibilidad en una de las áreas donde previamente no tenían antivirus no supondrá ningún impacto para la compañía.
  - La zona de red que actualmente dispone de antivirus será más sensible, ya que habrá usuarios conectados con sus equipos a Internet. En este caso, se propone realizar una segmentación del alcance total de los equipos en esta zona de la red para reducir al máximo la posibilidad de que existen usuarios sin servicio antivirus. Con este control no eliminaríamos el riesgo, pero lo reduciríamos lo suficiente como para tener controlada la situación (p. ej. si se realiza la actualización de 3 equipos conocidos, en caso de fallo se podrá contactar con el usuario para que no utilice Internet de forma temporal, etc).
- **Retraso en el desarrollo de la solución de Infraestructura:** el proveedor de infraestructuras utiliza tiempos acordados a nivel de servicio o SLAs. En este sentido, la demora en el desarrollo de la infraestructura es muy poco probable. Asimismo, en el caso de que el riesgo se materializara, se podrían dar dos casuísticas:
  - **Se retrasan en la entrega de todos los servidores:** en este caso es aun menos probable, ya que estaríamos en la situación de que el proveedor no cumpliría los SLAs para ningún servidor solicitado. Consecuentemente, se escalaría la situación a los *sponsors* y *stakeholders* para que a nivel interno de la compañía pudieran tomar las medidas oportunas con la finalidad de que el proyecto pudiera salir adelante.
  - **Se retrasan en la entrega de algunos servidores:** si ya han entregado algunos servidores y se retrasan en otros, se podrá empezar y priorizar la instalación y configuración del servidor que se disponga. De esta forma, mientras existiera una demora en la entrega de algunos servidores, se podría avanzar igualmente en el proyecto sin afectar la planificación de este.

- **Pérdida de imagen:** el proyecto de McAfee ePolicy Orchestrator 5.9.1 se ha lanzado dentro del departamento IT. Concretamente, se trata un proyecto incentivado por el CISO (*Chief Information Security Officer*) del área de seguridad de la información. De este modo, el fracaso del proyecto supondría una pérdida de imagen en la reputación de dicha área. En este caso, la forma de minimizar el riesgo será realizando puntos de control con todas las partes involucradas (*stakeholders* y *sponsors*). En el transcurso del proyecto, cuando se realice el despliegue del producto a los usuarios, se realizarán pruebas piloto con equipos de usuarios conocidos para controlar incidencias previamente no contempladas y, evitar así, ruido innecesario entre los empleados. De este modo, sólo cuando estemos seguros del correcto funcionamiento de la nueva versión del antivirus, se procederá a su despliegue.
  Finalmente, en caso necesario y dado el conocimiento de los profesionales de la empresa EY, se podrá contactar con profesionales experimentados en el ámbito para hacerles consultas sobre posibles incidencias detectadas asegurando así, el éxito del proyecto.

5. IMPLEMENTACIÓN DE MCAFEE EPOLICY ORCHESTRATOR 5.9.1

En este apartado se definen las fases del proyecto, así como todas las tareas técnicas y organizativas realizadas para llevar a cabo de forma exitosa la ejecución e implementación del proyecto:

- **Tareas técnicas**: todas aquellas tareas que han sido realizadas por los ejecutores del proyecto, entre ellos Ferran Angulo.
- **Tareas organizativas**: aquellas tareas técnicas que, por las dimensiones y funcionamiento de la compañía, han sido solicitadas a los departamentos encargados de realizarlas. Ejemplo: solicitar el montaje de servidores para el proyecto al departamento de infraestructuras.

Como se ha ido comentando a lo largo del trabajo, para la realización del proyecto ha sido de vital importancia la participación de distintos departamentos que han permitido dar la visión actual de la compañía a nivel de redes y de infraestructura. Adicionalmente, la experiencia de EY en proyectos similares ha permitido disponer de un conocimiento previo que ha permitido agilizar y optimizar los recursos y tiempos dedicados al proyecto.

De este modo, y tal y como se ha avanzado en el apartado de planificación, el proyecto se ha dividido en distintas fases que permitirán ir ejecutando el proyecto de forma gradual.

5.1. Estudio de la Infraestructura y preparación

Como cualquier otro proyecto de este tipo, la principal tarea que se debe realizar es entender la arquitectura de red, el diseño de la infraestructura y el funcionamiento de la compañía para asegurarse de conocer bien todos los flujos de trabajo necesarios para llevar a cabo todas las tareas del proyecto sin causar retrasos en la ejecución de este. Otro de los puntos relevantes a tener en cuenta, es identificar los requerimientos a nivel de infraestructura y comunicaciones que requiere el proyecto, así como identificar todas las tareas que van a requerirse para llevarse cabo el proyecto.

5.1.1. Requerimientos del proyecto

A continuación, se detallan los distintos requerimientos técnicos necesarios para la correcta ejecución del proyecto:

5.1.1.1. Infraestructura del entorno

Para poder montar la infraestructura necesaria del proyecto, se han tenido que solicitar 7 servidores correspondientes a 5 controladores de agente o *Agent handler*, la consola central de McAfee ePolicy Orchestrator y la base de datos SQL del aplicativo. Con la finalidad de no dilatar el apartado más de lo necesario, se adjuntan en el apartado Anexos los requerimientos técnicos solicitados al departamento de Infraestructura por cada tipo de servidor, es decir, 3 (Consola central McAfee ePolicy Orchestrator, controlador de agentes, BBDD SQL). Es importante tener en cuenta, que tanto el montaje del servidor, como la instalación del sistema operativo y de la base de datos se realizarán desde el departamento de infraestructuras. Por otro lado, la instalación de todo el *software* relacionado con McAfee se realizará mediante el presente proyecto.

Tal y como se ha comentado, se añade en el apartado “Anexos”, los requerimientos técnicos solicitados al departamento de Infraestructuras para cada tipo de servidor. Adicionalmente, se debe tener en cuenta que en dichos requerimientos no se podía la información de las IPs ya que las IPs las asignan al momento de montar los servidores y añadirlos en el dominio de la compañía.

Una vez ejecutadas las peticiones anteriores, se ha recopilado la información relevante relacionada con cada uno de los 7 servidores: ubicación física dónde se encuentra, ubicación lógica dónde se encuentra el servidor en la red, las direcciones IP asignadas (distintas tarjetas de red por servidor ya que hay distintas subredes, como la red de administración, necesaria para comunicar los distintos elementos).

Nombre del Servidor	Descripción	Ubicación física	Ubicación de red	Dirección IP	SO
VGP0EPOC01	Consola central de ePolicy Orchestrator	Martorell	CBB Martorell Administración	10.83.196.221 10.240.8.148 10.240.8.20	Windows Server 2016
VGP0EPOB01	Servidor de base de datos de ePolicy Orchestrator	Martorell	CBB Martorell Administración	10.83.196.222 10.240.8.21 10.240.8.149	Windows Server 2016
VGP0EPOS01	*Agent handler* de ePolicy Orchetrator capa CBB Martorell	Martorell	CBB Martorell Administración	10.83.196.148 10.240.20.50	Windows Server 2016
VGP0EPOS02	*Agent handler* de ePolicy Orchetrator capa CBB Prat	Prat	CBB Prat Administración	10.83.196.5	Windows Server 2016
VGP1EPOS01	*Agent handler* de ePolicy Orchetrator capa Content Check	Martorell	B2X – Content Check / Administración	10.82.4.30 10.240.44.36	Windows Server 2016
VGP2EPOS01	Agent handler de ePolicy Orchetrator capa Aplicaciones	Martorell	B2X – Aplicaciones / Administración	10.82.12.12 10.240.12.241	Windows Server 2016
VGP3EPOS01	*Agent handler* de ePolicy Orchetrator capa Publicación	Martorell	B2X - Publication / Administración	217.10.82.133 10.240.36.15	Windows Server 2016

Tabla 5: Descripción de cada uno de los servidores involucrados en el proyecto

5.1.1.2. Software del entorno

En la siguiente tabla se detalla el software instalado en la infraestructura para el correcto funcionamiento de la aplicación:

Nombre del Servidor	Software	Versión
VGP0EPOC01	McAfee ePolicy Orchestrator	5.9.1
VGP0EPOB01	Microsoft SQL Server 2016	2016
VGP0EPOS01	McAfee Agent Handler Distributed Repository	5.9.1 N/A
VGP0EPOS02	McAfee Agent Handler Distributed Repository	5.9.1 N/A
VGP1EPOS01	McAfee Agent Handler Distributed Repository	5.9.1 N/A
VGP2EPOS01	McAfee Agent Handler Distributed Repository	5.9.1 N/A
VGP3EPOS01	McAfee Agent Handler Distributed Repository	5.9.1 N/A

Tabla 6: Software y versión instalada en los servidores

En este trabajo se detallará la instalación del *software* correspondiente a McAfee ePolicy Orchestrator 5.9.1 y el *software* correspondiente a los *Agent Handler* (*McAfee Agent Handler* y *Distributed Repository*).

5.1.1.3. Usuarios de sistema

En la siguiente tabla, se detallan los usuarios utilizados en la infraestructura ePolicy Orchestrator. Además, cada uno de ellos serán totalmente imprescindibles ya que permitirán habilitar funcionalidades necesarias para el correcto funcionamiento del aplicativo, tal y como se indica en la columna “descripción”:

Servidor	Usuario	Descripción
VGP0EPOC01	.\SYSVAEPOAM	Usuario de acceso al servidor. Permisos de administración de máquina
	EMEA\SYSVAEPOLA	Usuario de lectura de ActiveDirectory de la compañía.
	EMEA\SYSVAEPONA	Usuario de navegación proxy para el sistema ePolicy Orchestrator. Configurado dentro de la aplicación.
	EMEA\SYSVAEPOAM	Usuario utilizado en despliegue de agentes. También utilizado para la conexión con los repositorios distribuidos.
	EMEA\RESVAEPOEM	Usuario buzón genérico para el recibo y envío de correos relacionados con el antivirus.
VGP0EPOB01	.\SYSVAEPOAM	Usuario de acceso al servidor. Permisos de administración de máquina.
	SYSVAEPOBD	Usuario local de la base de datos SQL Server.
VGP0EPOS01	.\SYSVAEPOAM	Usuario de acceso al servidor. Permisos de administración de máquina.
	EMEA\SYSVAEPOAM	Usuario utilizado en despliegue de agentes. También utilizado para la conexión con los repositorios distribuidos.
VGP0EPOS02	.\SYSVAEPOAM	Usuario de acceso al servidor. Permisos de administración de máquina.
	EMEA\SYSVAEPOAM	Usuario utilizado en despliegue de agentes. También utilizado para la conexión con los repositorios distribuidos.
VGP1EPOS01	.\SYSVAEPOAM	Usuario de acceso al servidor. Permisos de administración de máquina.
	EMEA\SYSVAEPOAM	Usuario utilizado en despliegue de agentes. También utilizado para la conexión con los repositorios distribuidos.
VGP2EPOS01	.\SYSVAEPOAM	Usuario de acceso al servidor. Permisos de administración de máquina.
	EMEA\SYSVAEPOAM	Usuario utilizado en despliegue de agentes. También utilizado para la conexión con los repositorios distribuidos.
VGP3EPOS01	.\SYSVAEPOAM	Usuario de acceso al servidor. Permisos de administración de máquina.
	EMEA\SYSVAEPOAM	Usuario utilizado en despliegue de agentes. También utilizado para la conexión con los repositorios distribuidos.

Tabla 7: Usuarios de sistema utilizados en la infraestructura de ePolicy Orchestrator

5.1.1.4. Puertos de comunicación

Otro de los puntos que se han tenido en cuenta para el despliegue de la infraestructura han sido los puertos requeridos para la comunicación entre los distintos servidores (ePolicy Orchestrator consola central, base de datos y controladores de agentes).

Pero ¿por qué es tan importante identificar los puertos de comunicación previo a la implementación de la aplicación? Para responder esta pregunta, primero de todo debemos contextualizar el hecho de que estamos realizado un proyecto temporal para una compañía, y esto hace más estricto el hecho de tener que controlar, desde un inicio, las restricciones que pueda haber en los procedimientos internos, a nivel de infraestructura, comunicaciones, etc. De este modo, mediante el análisis previo, y el contacto con dichos departamentos, se asegura la viabilidad del proyecto a nivel técnico previo al arranque de este. Este análisis, se ha resumido en el primer punto, “Introducción”, donde se define el entorno y se muestran las limitaciones del diseño y/o dificultades que pueda haber en el desarrollo del proyecto.

Por lo tanto, y después de las validaciones iniciales, se llega la conclusión de que los puertos necesarios son viables y seguros para que sean habilitados en los servidores pertinentes.

A continuación, se procede a mostrar los puertos utilizados para la comunicación entre los elementos de la infraestructura de ePolicy Orchestrator, así como la dirección de la comunicación:

Servidor	Dirección	Conexión	Protocolo y Puerto
McAfee ePo	Hasta	Navegador Web	HTTPS 443
McAfee ePo	Hasta	Base de datos SQL	JDBC/SSL 1433
Controlador de agentes	Desde	McAfee ePo	HTTPS 8443 (instalación) y HTTPS 8444
Controlador de agentes	Ambos	McAfee ePo	HTTP 80 y HTTPS 443
Controlador de agentes	Hasta	Base de datos SQL	ADO/SSL 1433
Controlador de agentes	Hasta	Clientes	HTTP 8081 y 8082
Controlador de agentes	Desde	Clientes	HTTP 80 y HTTPS 443

Tabla 8: Puertos necesarios para la comunicación entre los elementos de McAfee

5.1.1.5. Sincronización con servicios corporativos

A continuación, se detallan los accesos de los sistemas de ePolicy Orchestrator con otros elementos de la infraestructura del cliente para el correcto funcionamiento del sistema:

Servidor Origen	Servidor Destino	Puertos	Usuario	Permisos
VGP0EPOC01 (McAfee ePo)	Controlador de dominio (AD)	389 - TCP 636 - TCP	EMEA\SYSVAEPOLA	Lecutra del *Active Directory*
VGP0EPOC01 (McAfee ePo)	Proxy	8080 - TCP	EMEA\SYSVAEPONA	Permisos básicos del Proxy
VGP0EPOC01 (McAfee ePo)	Outlook	25 -TCP	EMEA\RESVAEPOEM	Envío de correos

Tabla 9: Servicios corporativos necesarios

De la tabla anterior, se reconocen tres servidores nuevos que se deberán contemplar en el diseño para que pueda existir la comunicación detallada:

- **Servidor controlador de dominio** (AD): utilizado para la sincronización de los equipos de la compañía con el servidor de antivirus.
- **Servidor Proxy**: utilizado para la comunicación entre el servidor antivirus y los servicios de McAfee para la actualización de archivos DAT, productos, software, etc.
- **Servidor Outlook**: utilizado para el recibo y envío de correos relacionados con el antivirus (por ejemplo, para alertar de *malware* detectado en algún equipo).

Finalmente, se resume la información de dichos:

Servidor	Ubicación física	Ubicación de red	Dirección IP
Controlador de dominio (AD)	Martorell	CBB Martorell	10.82.29.119
Proxy	Prat	CBB Prat	10.83.214.70
Outlook	Martorell	CBB Martorell	10.83.196.209

Tabla 10: Servidores necesarios para los servicios corporativos

5.1.2. Diagrama de red del entorno

Seguidamente, una vez obtenida la visión de la compañía en los aspectos comentados y analizados los requerimientos técnicos del proyecto, se ha realizado la solución de la arquitectura de red del proyecto. Este diseño define cada uno de los elementos necesarios para implementar el antivirus McAfee, así como, en qué zonas de la red de la compañía se deberán instalar.
Adicionalmente, se realizarán reuniones con el cliente para asegurarse que se aprueba la solución del diseño, ya que cada compañía dispone de casuísticas distintas (se han detallado las principales casuísticas en el primer apartado de Introducción) y el hecho de que las partes implicadas aprueben la solución, permite garantizar, en mayor probabilidad, el éxito en la implementación, sin contratiempos inesperados que como proveedor no puedes prever (funcionamiento interno entre departamentos, viabilidad de lo demandado a nivel de infraestructuras, etc).

Previo a mostrar la solución de arquitectura de red final aprobada por los *stakeholders* y *sponsors*, se procede a la justificación de las decisiones tomadas para alcanzar dicha solución:

- Tal y como se ha comentado en el apartado “Diseño actual del antivirus McAfee en la compañía”, la comunicación entre equipos ubicados en zonas de red separadas por un *firewall* está limitada. Concretamente, y por políticas del grupo, en nuestro proyecto no podremos hacer uso de las aperturas de puerto para habilitar comunicaciones cuando haya un *firewall* de por medio. El principal motivo viene dado por el hecho de que se requeriría realizar una apertura para una subred entera (p. ej. IP servidor antivirus hacia todos los equipos/servidores de capa de publicación, aplicaciones, content check, CBB). Además, el salto de 2 *firewall* para una comunicación está estrictamente prohibida. Por lo tanto, la mejor solución en una primera instancia es pensar en implementar un servidor (*Agent Handler*) por cada capa, de tal forma que podamos evitar cualquier restricción a nivel de comunicación entre los distintos componentes de McAfee ePolicy Orchestrator 5.9.1 y los equipos.
- Como se ha comentado en el punto anterior, los *Agent Handler* se colocarán estratégicamente en cada capa. Pero hay que tener en cuenta que entre los servidores *Agent Handler* y los servidores consola central de McAfee ePo y BBDD deberá existir comunicación. Entonces, ¿cómo se comunicarán los *Agent Handler* con la consola central de McAfee ePo y la BBDD? Para poder llegar a la respuesta de dicha pregunta, se tuvieron que realizar reuniones con los departamentos involucrados para llegar a la conclusión de que sólo había una posible solución: hacer uso de la red de administración. Mediante la red de administración, puedes llegar a cualquiera de las capas sin tener que pasar por ningún *firewall*. De este modo, se procedió a realizar el diseño teniendo en cuenta que el servidor de la consola de McAfee ePo y el servidor de BBDD se ubicarían en la red de administración para que fueran accesibles desde cualquier capa. Por lo tanto, entre los *Agent Handler* y dichos servidores podrá haber una comunicación constante y sin restricciones (ya que sólo de esta forma se puede garantizar el correcto funcionamiento del producto).

- Como conclusión de los dos puntos anteriores, los servidores deberán tener distintas interfaces de red para poder comunicarse entre ellos y poder ofrecer el servicio. De esta forma, los servidores se podrán comunicar:
    - **Consola McAfee ePolicy Orchestrator y BBDD:** una interfaz conectada a la red de administración de las capas content check, aplicaciones y publicación, otra interfaz conectada a la subred de administración de la CBB de Martorell, y la otra interfaz a la subred de CBB del Prat (no es una subred de administración).
    - ***Agent Handlers*:** cada uno de los *Agent Handler* tendrá dos IPs (a excepción del de la CBB del Prat), una para conectarse a la red de administración y así comunicarse con la consola McAfee ePolicy Orchestrator y la BBDD; y la otra para comunicarse con los equipos desde su misma capa. Finalmente, el *Agent Handler* de la capa CBB del Prat no necesitará tener una interfaz a la red de administración ya que tanto la consola McAfee como la BBDD tendrán una interfaz apuntando directamente a la misma subred de CBB del Prat.

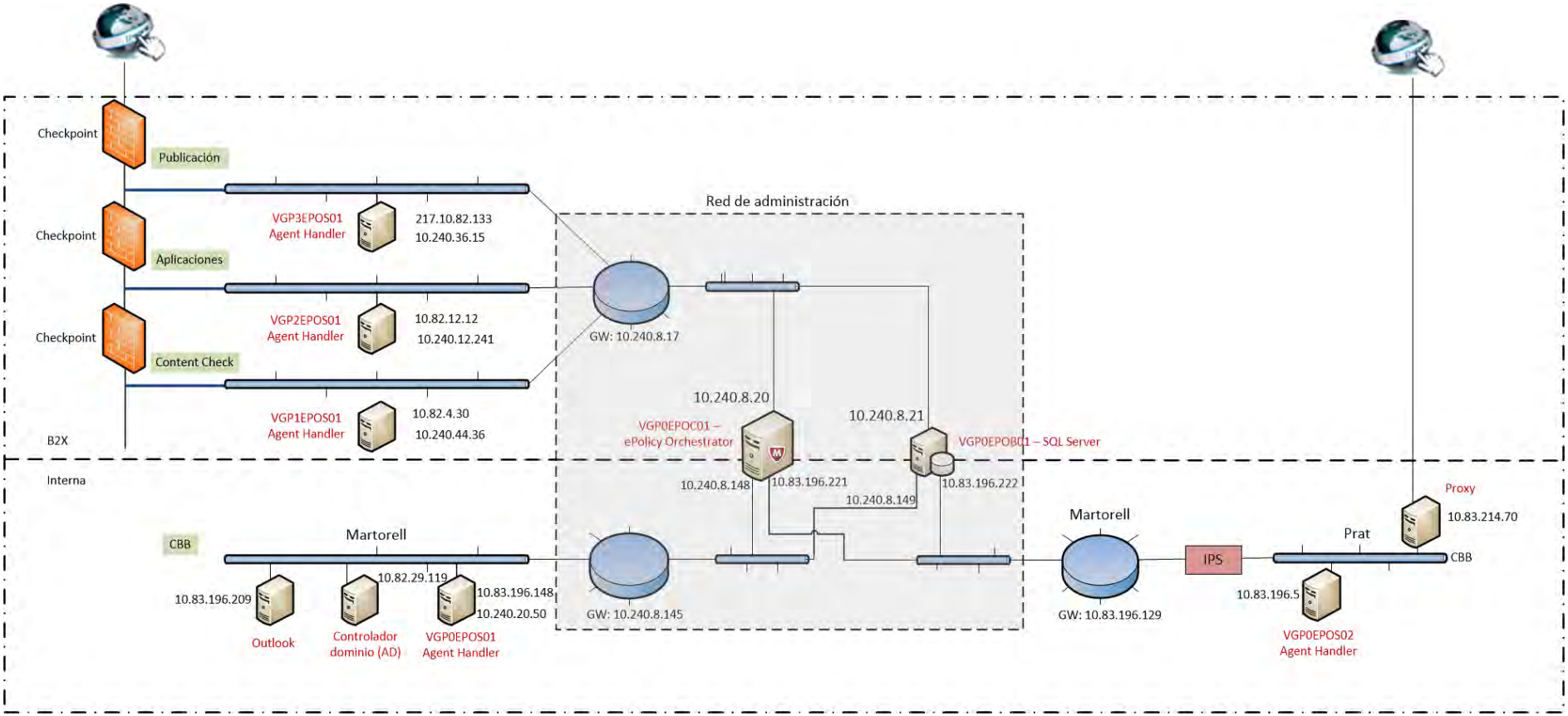
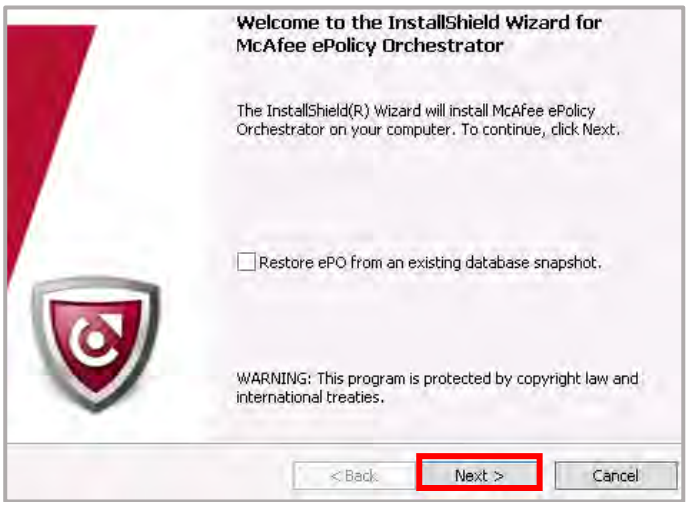
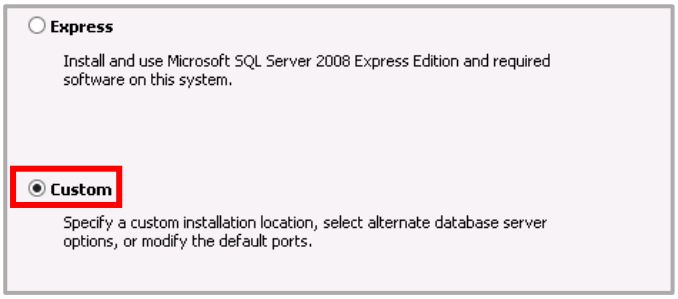
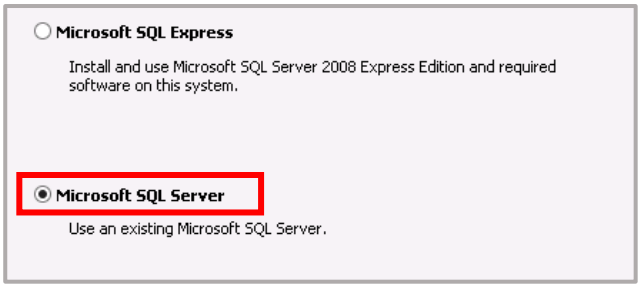


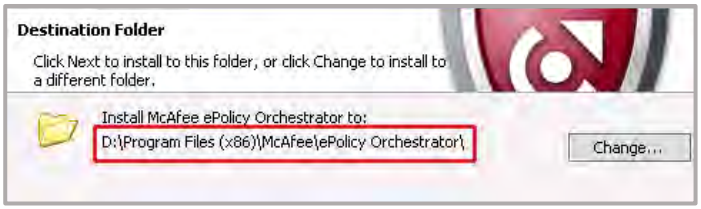
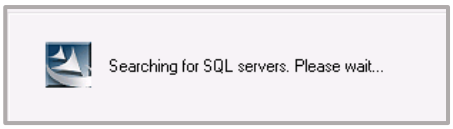
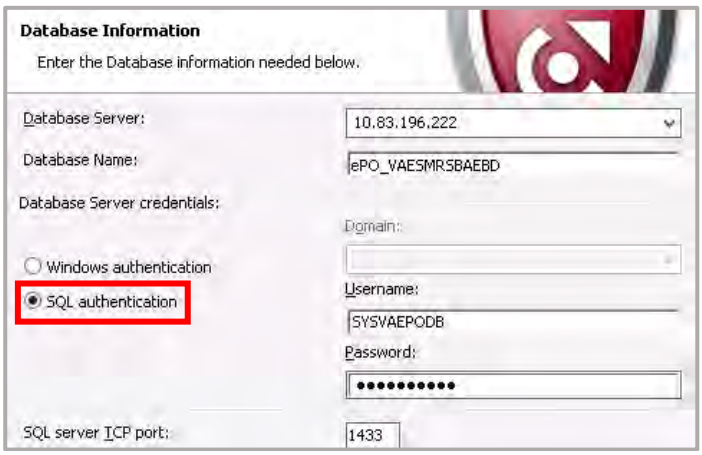
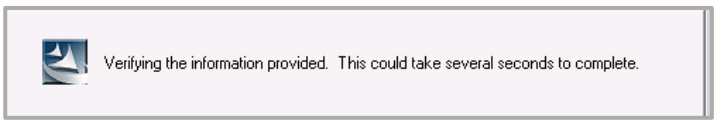
Figura 5: Diagrama de red del entorno del proyecto

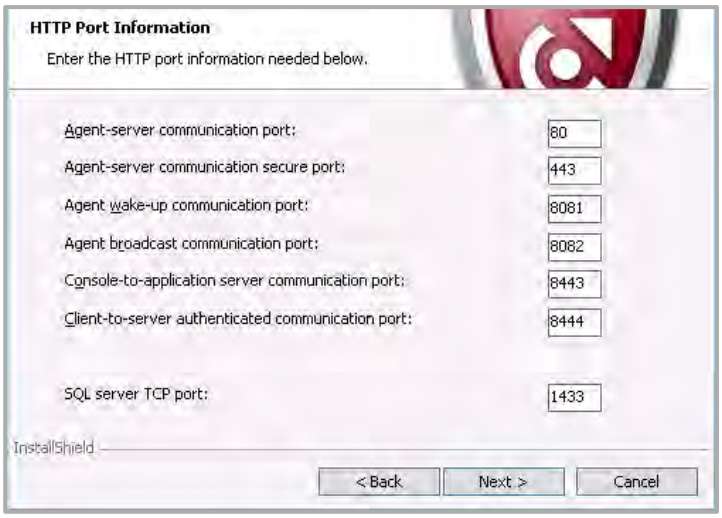
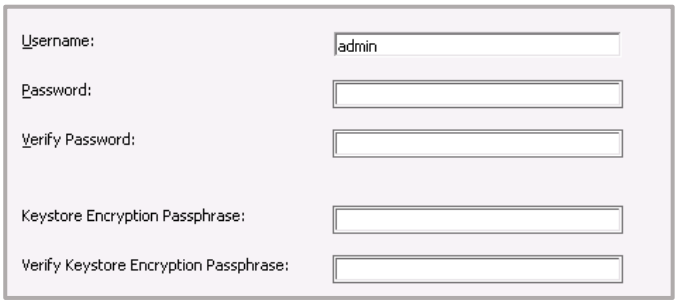
5.2. Instalación y configuración de McAfee ePolicy Orchestrator

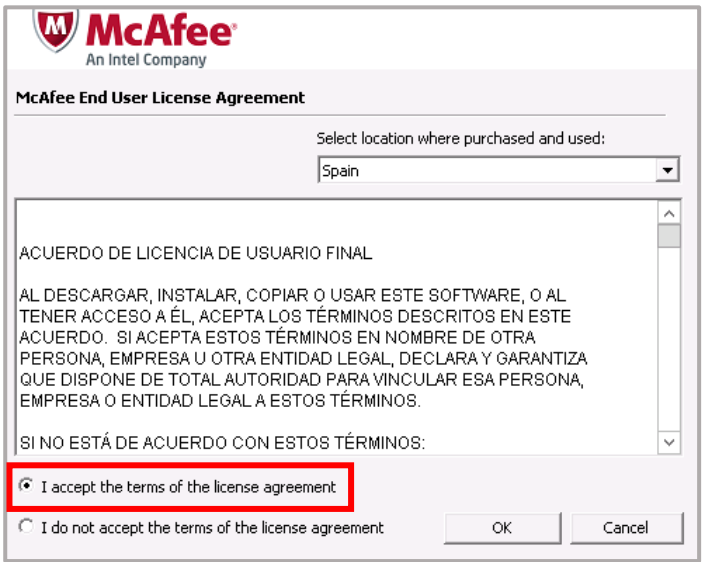
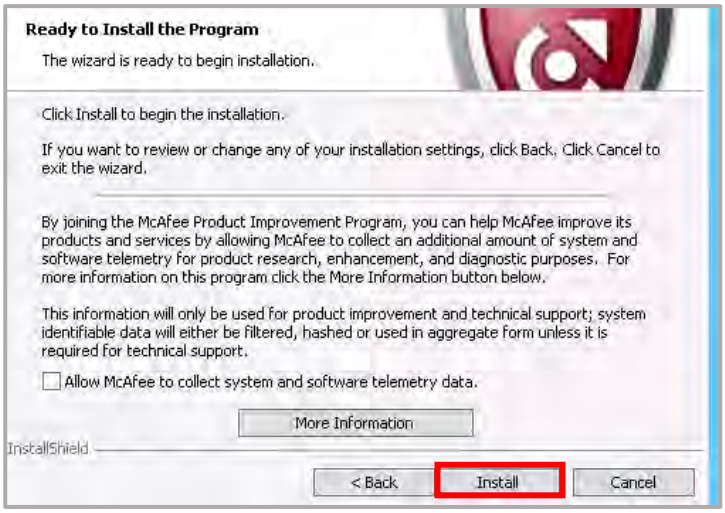
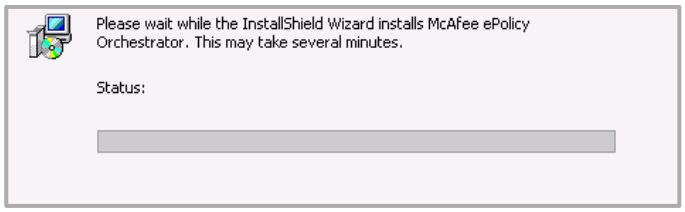
Previo a realizar la instalación del software McAfee ePolicy Orchestrator 5.9.1, y tal y como se ha detallado en el punto “Infraestructura del entorno”, se deberán solicitar los servidores con una serie de requisitos (descritos en los Anexos).

Una vez obtenido el servidor de la base de datos (con el software SQL Server 2016. El nombre de la base de datos se llamará ePo_VAESMRSBAEBD), se procede con la instalación de McAfee ePolicy Orchestrator 5.9.1:

1. Se abrirá la ventana de instalación y se debe hacer *click* sobre “Next>”.	
2. Seleccionamos el tipo de instalación “Custom” y hacemos *click* en “Next>”.	
3. Seleccionamos la opción “Microsoft SQL Server” y hacemos *click* en “Next>”.	

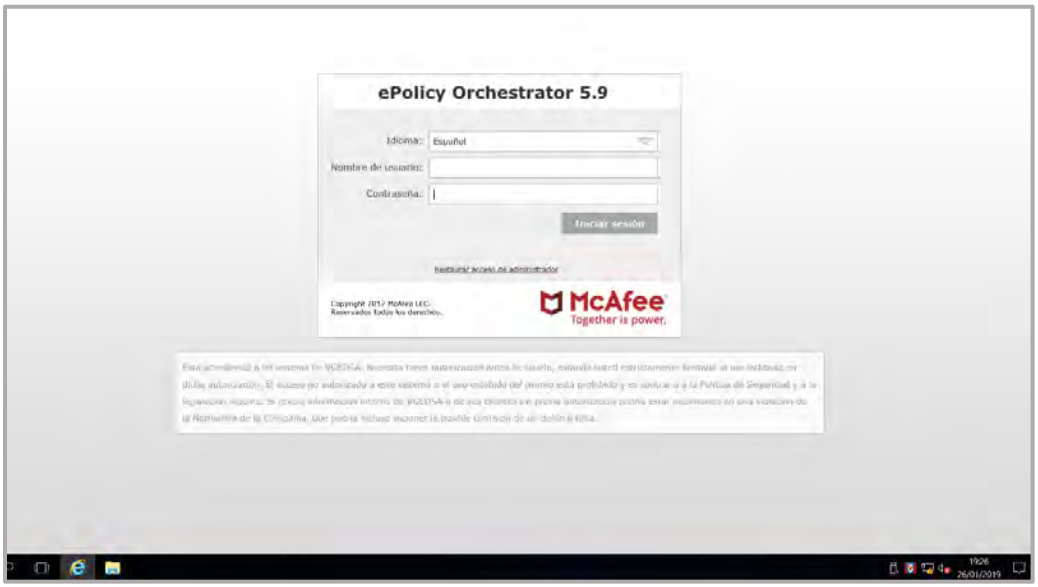
4. Seleccionar como “Destination Folder” la unidad D:\ de disco y utilizando la ruta habitual de instalación: D:\Program Files (x86)\McAfee\ePolicy Orchestrator\ Una vez seleccionada la ruta hacemos *click* en “Next>”.	
5. El instalador comenzará a hacer varias búsquedas. Una de ellas los Domain Controllers. Se debe dejar que cargue.	
6. Otra de las cosas que busca son instalaciones de SQL servers. Dejamos que cargue hasta que finalice.	
7. En la ventana de configuración de la BBDD se deberán insertar los datos de conexión. **Database Server:** 10.83.196.222 **Database Name:** ePO_VAESMRSBAEBD **SQL Authentication:** SYSVAEPODB **SQL server TCP port:** 1443 Una vez introducidos los datos hacemos *click* en “Next>”.	
8. El instalador realizará la verificación de la conexión. Si todo es correcto pasará a la siguiente ventana.	

9. En esta ventana se deben introducir los puertos de comunicación del servidor con los diferentes componentes. Los únicos puertos que se podrán modificar tras la instalación son: Agent wake-up communication port Agent broadcast communication port Una vez introducidos los puertos, hacer click en "Next>".	
10. En esta ventana se deberán introducir los datos de administrador local de la ePolicy Orchestrator. El usuario se llamará ePoLocalAdmin para una mayor seguridad. También se introducirá la "Keystore Encryption Passphrase". Hacemos *click* en "Next>".	
11. En esta ventana se deberá introducir el número de licencia de ePolicy Orchestrator para la instalación. Hacemos *click* en "Next>".	

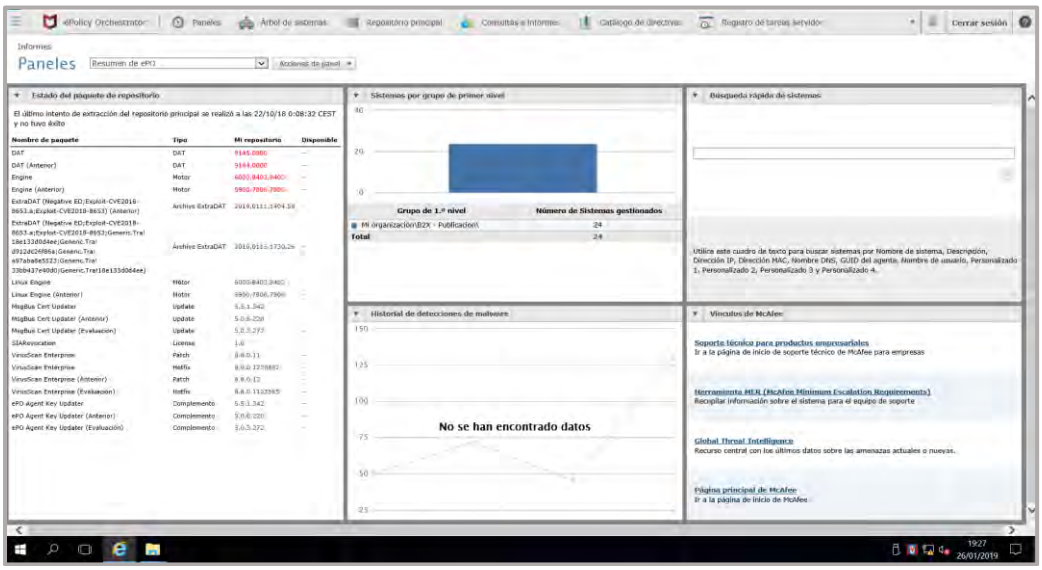
12. Deberemos seleccionar la ubicación desde donde ha sido comprado el producto y aceptar los términos de licencia. Hacemos *click* en "OK".	
13. Finalmente hacemos click en "Install" para iniciar la instalación.	
14. La barra de progreso comenzará a crecer hasta llegar al final indicando que la instalación ha finalizado.	
15. Una vez cargada la barra de "Status" aparecerá la pantalla de finalización de la instalación.	

16. Una vez instalado, se puede proceder a abrir la aplicación desde el ejecutable que aparece en el escritorio.

17. Accedemos a McAfee ePolicy Orchestrator 5.9.1 mediante las credenciales administradores introducidas durante el proceso de instalación:



18. Accedemos a la aplicación:



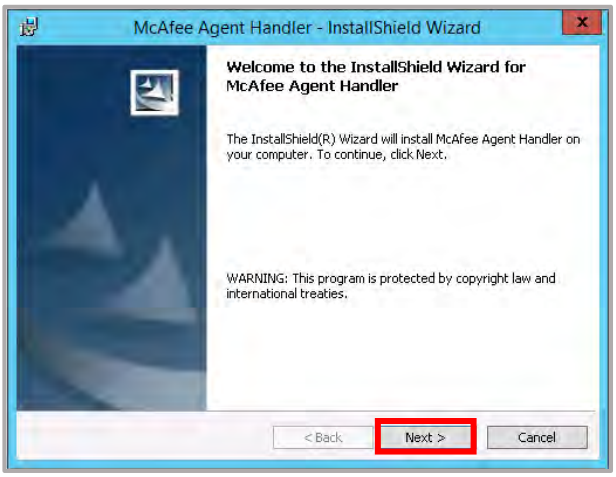
5.3. Instalación y configuración de McAfee Agent Handler

En este apartado, se procede a explicar el proceso de instalación y configuración del administrador de agentes, o más comúnmente llamado *Agent Handler*. Por el tipo de infraestructura de la compañía, en el proyecto llegaremos a contar con 5 *Agent Handler*. Estos servidores permitirán acceder de forma más ágil a los distintos equipos y servidores de la compañía permitiendo la inclusión de muchos más sistemas gestionados que se encuentran segmentados en distintas subredes además de permitir una mayor escalabilidad del producto:

1. Para proceder a la instalación del Agent Handler, deberemos coger la carpeta "AgentHandler", incluida en el paquete de instalación de ePolicy Orchestrator 5.9.1, e instalarlo en el servidor deseado.

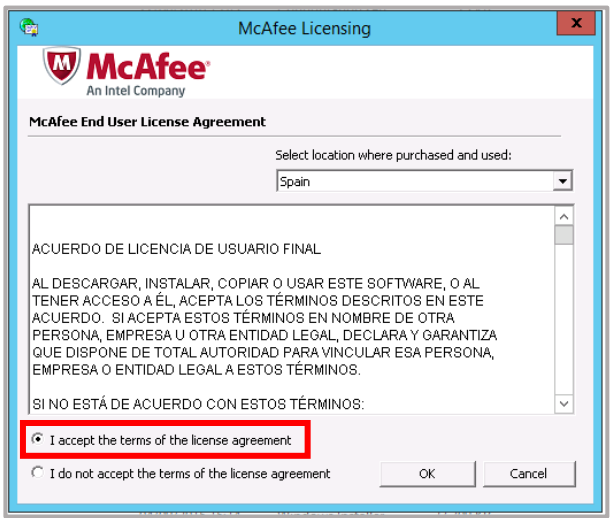
Para iniciar la instalación hacemos *click* en Setup.exe con permisos de administración sobre la máquina.

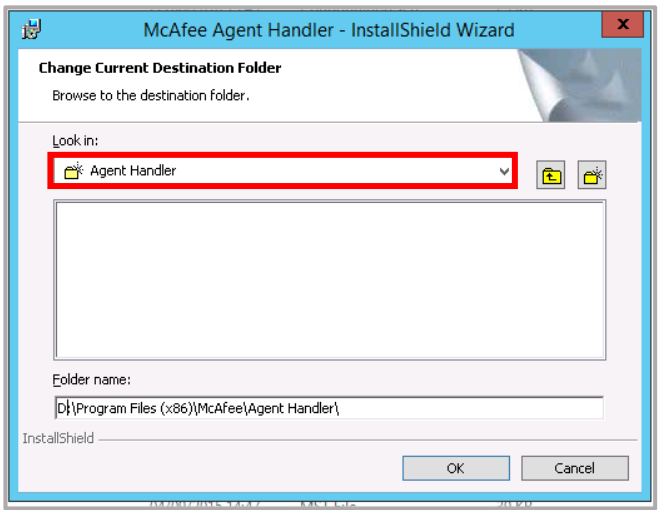
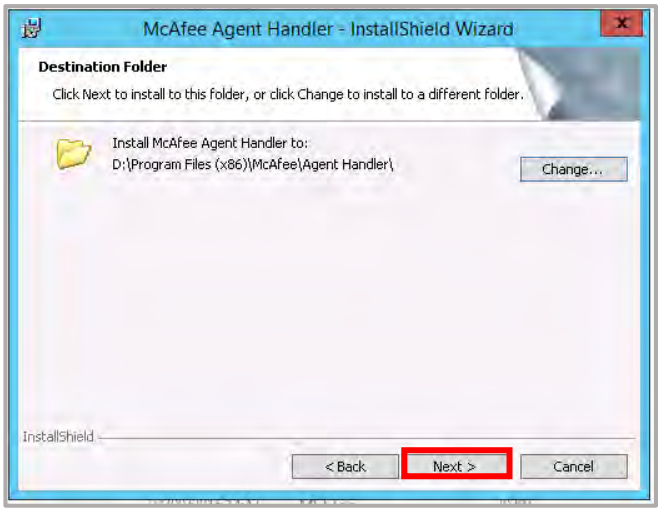
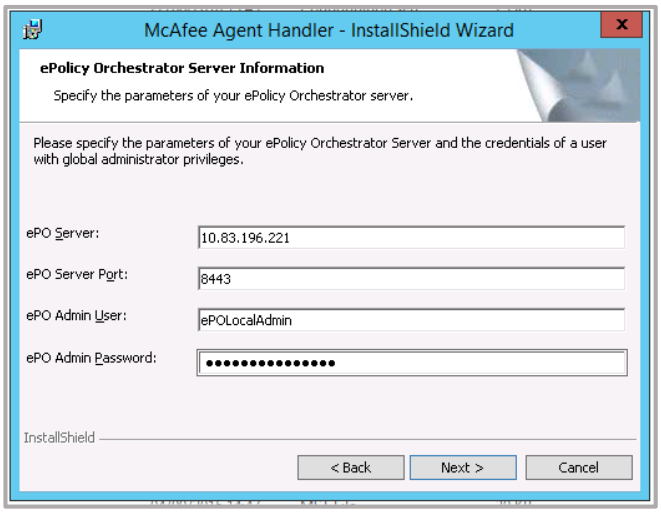
2. Se iniciará la ventana de instalación y hacemos *click* sobre "Next>".

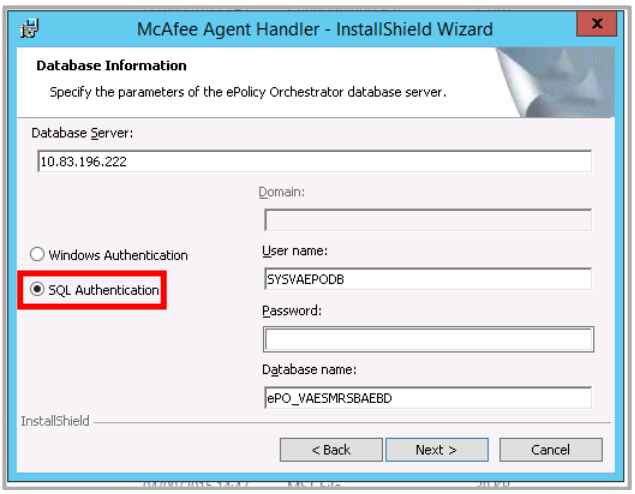
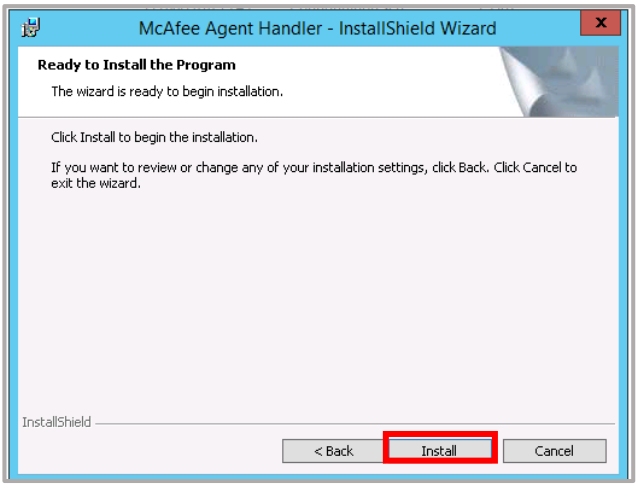
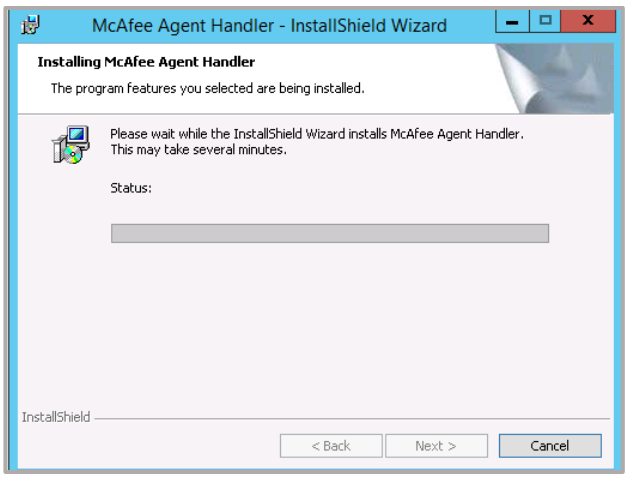


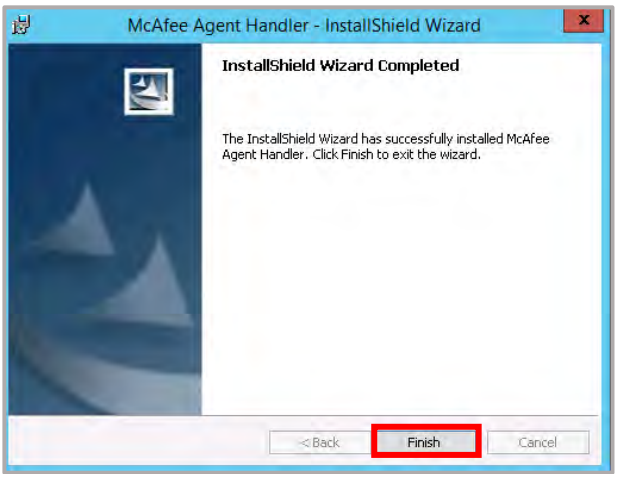
3. Deberemos seleccionar la ubicación desde ha sido comprado el producto y aceptar los términos de licencia.

Hacemos *click* en "OK"



4. Seleccionar como “Destination Folder” la unidad D:\ de disco y utilizando la ruta habitual de instalación: D:\Program Files (x86)\McAfee\Agent Handler\ Una vez seleccionada la ruta hacemos click en “Next>”.	
5. Aparecerá la ventana de confirmación de la carpeta de instalación. Hacemos *click* en “Next>”.	
6. En esta ventana deberemos introducir los datos de conexión con la ePolicy Orchestrator. Hacemos *click* en “Next>”.	

7. En esta ventana deberemos introducir los datos de conexión con BBDD. Hacemos *click* en “Next>”.	
8. Aparecerá la ventana de inicio de instalación. Hacemos *click* en “Install”.	
9. Aparecerá la ventana con la barra de progreso. Esperamos hasta que se complete la instalación.	

10. Una vez completada la barra de instalación aparecerá la ventana de finalización de instalación. Hacemos *click* en "Finish" para finalizar la instalación.	

Es muy importante destacar los pasos 6 y 7, ya que, dado el diseño de red de la compañía, los servidores McAfee ePolicy Orchestrator y el servidor de la base de datos se encontrarán en la red de administración y esto hará que deban tener 3 interfaces de red necesarias para comunicarse con todas las subredes y capas de la compañía. En la instalación, se ha mostrado el procedimiento para el *Agent Handler* ubicado en la capa CBB del Prat, correspondiente al servidor VGP0EPOS02.

Para un mayor entendimiento, se indican los valores que deberían introducirse en la instalación de cada *Agent Handler* para habilitar la comunicación con los servidores McAfee ePolicy Orchestrator y la base de datos (ver apartado "Diagrama de red del entorno" para entender las IPs utilizadas):

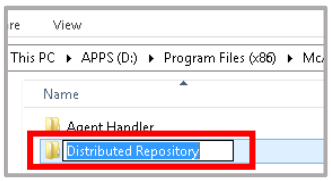
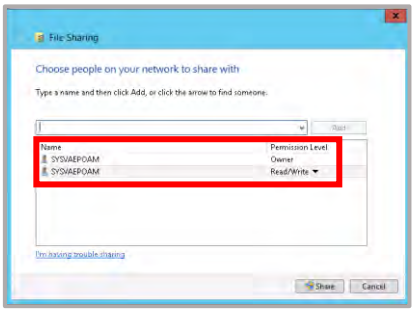
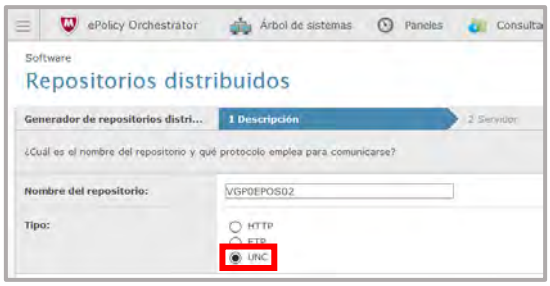
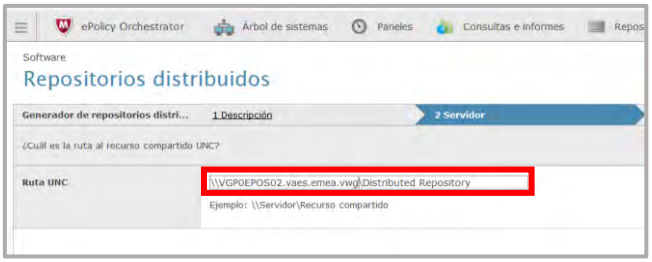
Nombre *Agent Handler*	Ubicación *Agent Handler*	IP Agent Handler	IP servidor BBDD	IP McAfee ePo
VGP0EPOS01	CBB Martorell	10.240.20.50	10.240.8.149	10.240.8.148
VGP0EPOS02	CBB Prat	10.83.196.5	10.83.196.222	10.83.196.221
VGP1EPOS01	Content Check	10.240.44.36	10.240.8.21	10.240.8.20
VGP2EPOS01	Aplicaciones	10.240.12.241	10.240.8.21	10.240.8.20
VGP3EPOS01	Publicación	10.240.36.15	10.240.8.21	10.240.8.20

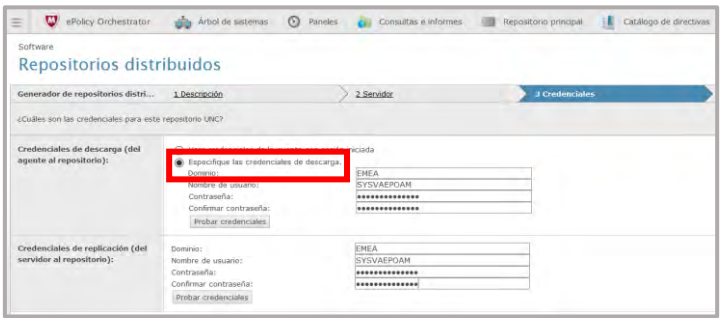
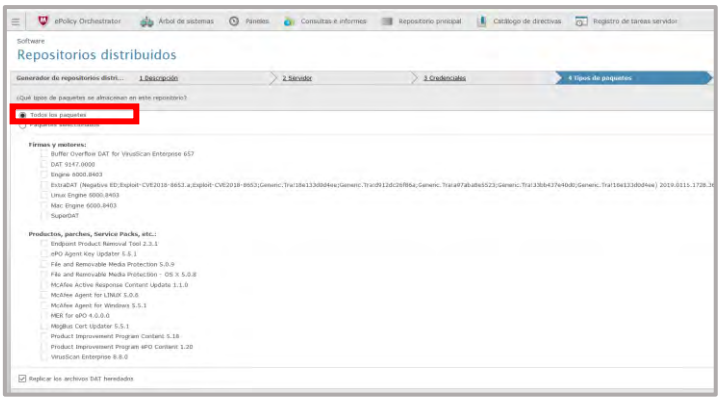
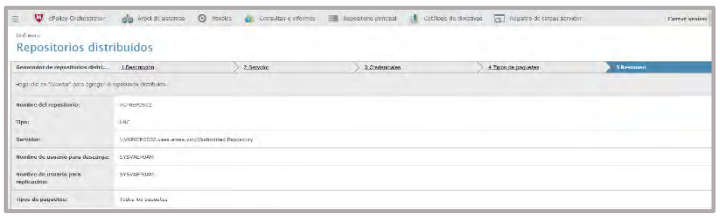
Tabla 11: Configuración en la instalación de los Agent Handlers con servidores McAfee ePo y BBDD

5.4. Instalación y configuración de Distributed Repository

Para poder tener servidores que hagan de réplica del servidor central de McAfee ePo, será necesario que todos los servidores *Agent Handler* (por definición, balancea el tráfico de red para no cargar el servidor McAfee ePo para generar una mayor escabilidad además de permitir proporcionar a los sistemas gestionados asignarles *Sitelist*, directivas creadas en McAfee ePo, archivos DAT,etc) contengan un complemento adicional instalado: el *distributed repository*. Concretamente, se instalarán del tipo Repositorios de recursos compartidos UNC (*Universal Naming Convention*), ya que podrán alojar el repositorio del servidor McAfee ePo.

La instalación que se muestra a continuación será necesaria para cada uno de los 5 *Agent Handler*. En este caso, siguiendo el ejemplo de la instalación anterior, se muestra la instalación del *Distributed Repository* en el *Agent Handler* ubicado en CBB del Prat:

1. Crear en el *Agent Handler* una carpeta para dicho propósito en la ruta: D:\Program Files (x86)\McAfee\	
2. Seleccionar que usuarios tienen permisos para escribir/leer en el directorio utilizado como repositorio distribuido.	
3. Dentro de ePolicy Orchestrator, acceder a: Menú > Software > Repositorios Distribuidos > Nuevo Repositorio Se deberá escoger el nombre y el tipo de repositorio.	
4. Se deberá escribir la ruta donde se encuentra la carpeta compartida que albergará el repositorio de la ePO.	

5. Se deberán escoger las credenciales de acceso a dicha carpeta compartida. Deberán coincidir con las definidas en el punto 2.	
6. Seleccionar que paquetes se replicarán en el repositorio distribuido.	
7. Finalizar y guardar la creación del nuevo repositorio.	

5.5. Análisis del despliegue de los productos a los equipos

Una vez montada la infraestructura de la aplicación y realizada la instalación del *software*, es necesario que se defina el método de despliegue del producto en los equipos de la compañía. Para seleccionar el mejor método de despliegue, se realizan diversas reuniones con los departamentos involucrados (Infraestructura, Comunicaciones y Workplace). Las reuniones permiten identificar la vía perfecta del despliegue del producto, mediante el *System Center Configuration Manager* o SCCM. Este, permitirá distribuir el *software* necesario a través de un gestor de *software* desarrollado por Microsoft.

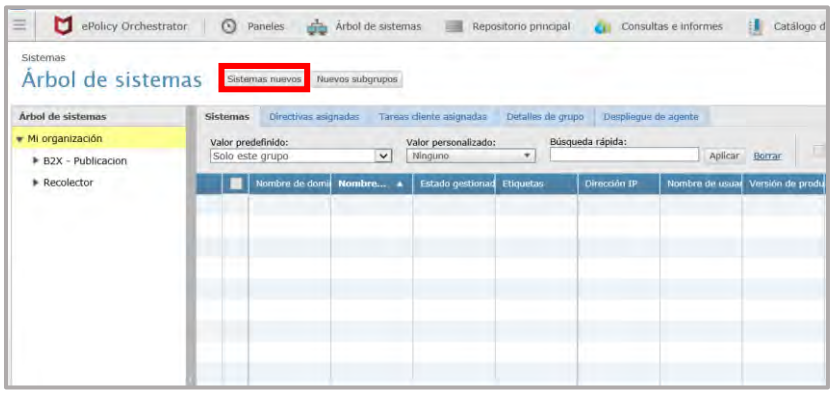
Previo a realizar el despliegue a una serie de equipos identificados como piloto, se requiere identificar qué *software* será necesario distribuir a los equipos:

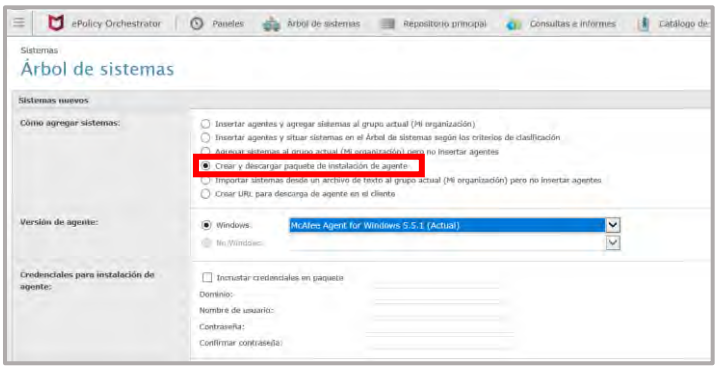
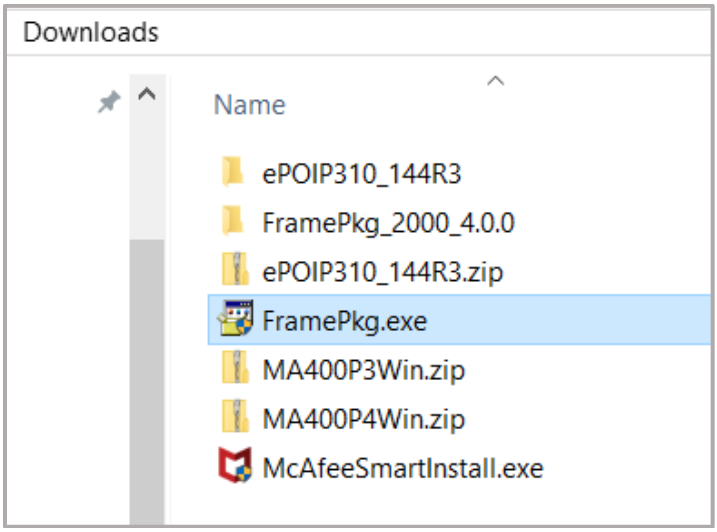
- **McAfee Agent:** *software* necesario para poder gestionar el equipo destino. Si el equipo contiene dicho producto, se podrá lanzar la instalación de VirusScan Enterprise de forma ágil y eficaz.
- **McAfee VirusScan Enterprise o McAfee Endpoint Security:** *software* antivirus que se instala en los *endpoints* y que permite gestionar y bloquear las amenazas detectadas en cada uno de los equipos. Se puede instalar, *a posteriori* del McAfee Agent, a través de la gestión desde la consola central de McAfee ePolicy Orchestrator.

Tal y como se ha comentado anteriormente, si se instala el McAfee Agent en el equipo, se podrá instalar *a posteriori* el McAfee VirusScan Enterprise. De esta forma, se llega a la conclusión que se desplegará el software McAfee Agent a través del sistema SCCM de la empresa para poder gestionar todos los equipos de la compañía, y así, instalarle el *software* antivirus de protección McAfee VirusScan Enterprise.

5.5.1. Despliegue McAfee Agent

Para realizar con éxito el despliegue del producto McAfee Agent, se debe generar un paquete que pueda ser enviado a través de SCCM. Para generarlo, se realizan los siguientes pasos:

1. En el apartado “Árbol de Sistemas”, seleccionar “Sistemas nuevos”.	

2. Seleccionar “Crear y descargar paquete de instalación de agente”. En el apartado versión de agente, seleccionar la versión que ponga actual.	
3. Seleccionar Paquete de agente para empezar la descarga del producto McAfee Agent.	
4. Buscar y guardar el paquete “.exe” descargado.	
5. El paquete descargado contendrá el producto para gestionar los equipos de la compañía, es decir, el McAfee Agent. De esta forma, ahora se podrá enviar al departamento Workplace para que puedan proceder a enviarlo a través de SCCM a los equipos definidos como piloto.	

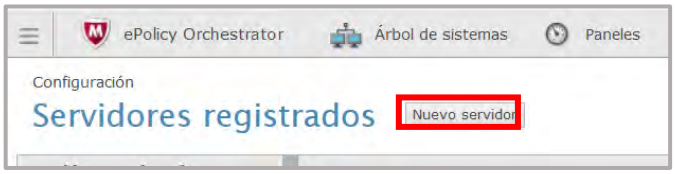
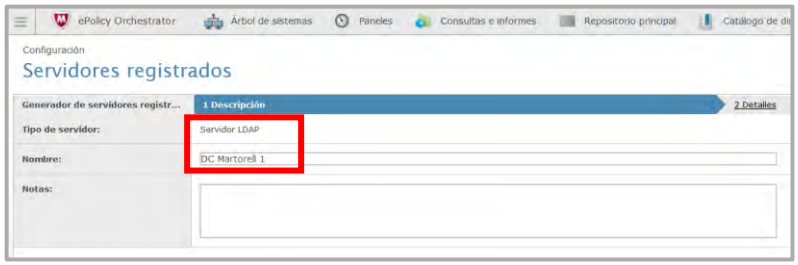
5.5.2. Sincronización con LDAP

Aunque para el despliegue y el correcto funcionamiento del producto McAfee ePolicy Orchestrator 5.9.1 no sea necesario sincronizarlo con ningún servidor LDAP, sí que será interesante sincronizar el producto con dicho servidor ya que nos permitirá tener una trazabilidad que generará valor añadido para la compañía.

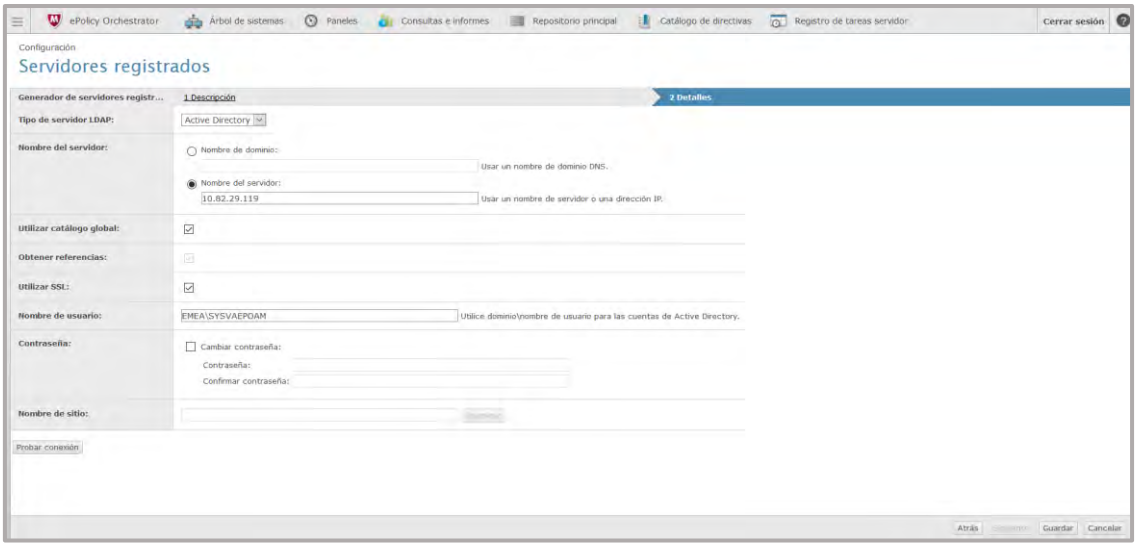
Antes de empezar a detallar como se procede a realizar la sincronización con el LDAP, es primordial entender qué nos aportará el servidor LDAP:

- **Servidor LDAP:** permite procesar consultas y actualizaciones a un directorio activo de forma ágil. En nuestro caso, nos permitirá por un lado que los usuarios que administren la herramienta (McAfee ePo) se puedan validar mediante su cuenta del directorio activo sin la necesidad de crear usuarios locales, y por otro lado, utilizar reglas de asignación de directiva (esto nos servirá por ejemplo a la hora de realizar la prueba de concepto del módulo *File and Removable Protection* ya que podremos elegir qué usuarios del AD se les aplicará el cifrado de medios extraíbles) y activar los conjuntos de permisos asignados de forma dinámica.

De esta forma, procedemos a mostrar el procedimiento seguido para sincronizar el producto McAfee ePo con el servidor LDAP:

1. En el apartado "Configuración", seleccionamos "Servidores registrados", "Nuevo servidor".	
2. Se añade el tipo de servidor y nombre que tendrá el servidor nuevo añadido. En nuestro caso, será un un servidor LDAP (*Domain Controller*) y se encontrará ubicado en Martorell.	

3. En la pestaña “Detalles”, seleccionamos el tipo de servidor LDAP que en nuestro caso será *Active Directory*. Seguidamente, se añade la IP del servidor (10.82.29.119). Por último, se especifica el nombre de usuario de sistema encargado de recopilar la información del servidor LDAP “SYSVAEPOAM”:



5.6. Definición equipos piloto y despliegue de McAfee VirusScan Enterprise

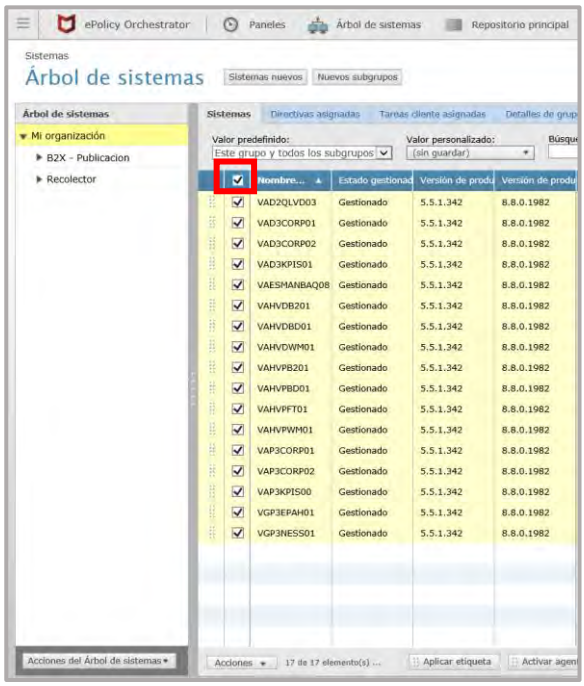
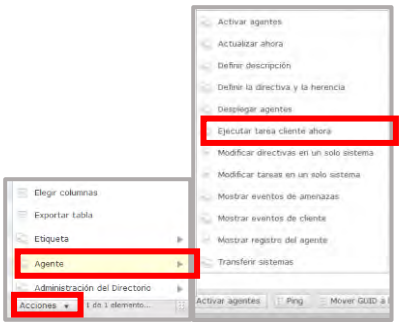
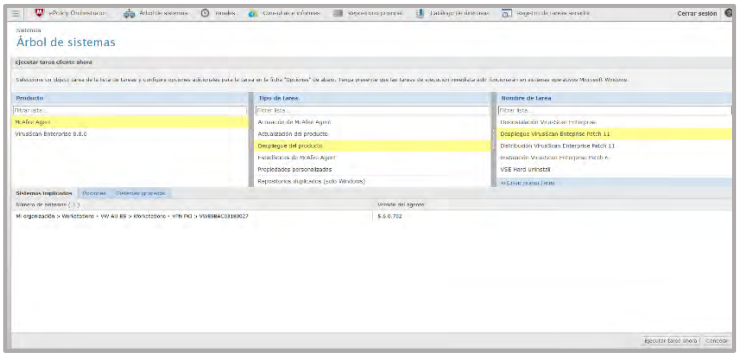
A continuación, se definen los equipos que han sido seleccionados para realizar el despliegue en la fase piloto para verificar su correcto funcionamiento. Concretamente, se trata de 17 equipos:

Nombre del sistema
VAD2QLVD03
VAD3CORP01
VAD3CORP02
VAD3KPIS01
VAESMANBAQ08
VAHVDB201
VAHVDBD01
VAHVDWM01
VAHVPB201
VAHVPBD01
VAHVPFT01
VAHVPWM01
VAP3CORP01
VAP3CORP02
VAP3KPIS00
VGP3EPAH01
VGP3NESS01

Tabla 12: Equipos seleccionados para la fase piloto

Mediante el soporte del departamento de Workplace, estos equipos recibirán el paquete de McAfee Agent (previamente se ha explicado como extraer dicho paquete para ser desplegado). Una vez desplegado el agente, la consola central McAfee ePolicy Orchestrator nos permitirá ejecutar tareas cliente. Estas, permiten desplegar cualquier producto, actualización, directivas o políticas desde la consola central hacia los equipos destinos. De esta forma, se procederá a instalar el *software* antivirus de protección ante amenazas de seguridad, McAfee VirusScan Enterprise:

A continuación, se muestra la ejecución de la tarea cliente responsable de instalar el McAfee VirusScan Enterprise en los equipos:

1. En el apartado “Árbol de Sistemas”, seleccionamos todos los equipos piloto.	
2. Seleccionar “Acciones”, “Agente” y “Ejecutar tarea cliente ahora”.	
3. Seleccionar: ▪ “McAfee Agent” en la pestaña producto. ▪ “Despliegue del producto” en la pestaña Tipo de tarea. ▪ “Despliegue VirusScan Enterprise Patch 11” (última versión disponible) en la pestaña nombre de tarea.	
4. Ejecutando esta tarea en todos los equipo pilotos, se forzará de forma centralizada y automática la instalación del *software* McAfee VirusScan Enterprise en los equipos seleccionados.	

5.7. Valoración de los resultados

Llegados a este punto, con la infraestructura montada, los servidores configurados, el producto McAfee ePolicy Orchestrator 5.9.1 correctamente instalado y testeado a través del piloto de equipos seleccionados previamente, se decide realizar una valoración del avance del proyecto con los *stakeholders* y *sponsors* del proyecto implicados.

El resultado ha sido exitoso, todos los equipos del piloto han recibido correctamente el *software* McAfee Agent para ser gestionado desde la consola central, y, además, posteriormente, han recibido el despliegue del producto antivirus McAfee VirusScan Enterprise a través de dicha consola.
Otro punto que destacar es la importancia de la cooperación entre los distintos departamentos de la compañía, ya que nos han permitido contemplar una solución muy ágil y eficaz para el despliegue.

De forma resumida, se explica la información principal que podemos obtener de los equipos que se encuentran correctamente gestionados por la consola McAfee y tienen instalado el producto McAfee VirusScan Enterprise:

- **Nombre de sistema:** nombre que la empresa le asigna al equipo para tener su registro y para poder tener trazabilidad (usuario que lo adquiere, fecha de entrega, etc).
- **Estado del sistema:** esta columna tiene dos valores: Gestionado y No gestionado. Si el equipo se encuentra Gestionado quiere decir que se ha desplegado correctamente el McAfee Agent, quién se comunica con la consola central o McAfee ePo. Si se encuentra No gestionado, quiere decir que McAfee ePo ha identificado el equipo al mapear la información de los equipos activos en el AD y que éste, no contiene el producto McAfee Agent. En nuestro caso, al haber realizado una fase piloto con una serie de equipos seleccionados, se ha lanzado directamente el software a dichos equipos mediante SCCM, y estos, han comunicado con la consola McAfee ePo.
- **Versión del producto (Agent):** tal y como se ha ido comentando, esta columna indica la versión del producto McAfee Agent que se encuentra instalado en los equipos. Este valor de la versión corresponde con la versión que nos hemos descargado en McAfee ePo para que SCCM pudiera desplegar el producto a los equipos. Actualmente, la última versión disponible es 5.5.1.342.
- **Versión de producto (VirusScan Enterprise):** esta columna muestra la información de la versión que tienen instalado los equipos en referencia al *software* de protección antivirus. Al igual que con la versión de McAfee Agent, todos los equipos tienen la última versión disponible instalada gracias al despliegue del producto a través de la consola McAfee ePo: 8.8.0.1982.

- **Versión de DAT (VirusScan Enterprise):** el archivo DAT se instala y se actualiza de forma automática mediante el *software* McAfee VirusScan Enterprise. Es decir, si tenemos instalado dicho producto, tendremos una gestión del archivo DAT que nos permitirá proteger a los equipos contra amenazas existentes y potenciales. Cada día se actualiza el archivo DAT, y por este motivo el número irá variando (número de ayer + 1).
- **Versión del motor (VirusScan Enterprise):** este componente aporta la lógica básica para que el producto VirusScan Enterprise funcione correctamente. Por lo tanto, este también se integra con el software mencionado. Además, cada cierto tiempo la compañía McAfee realiza actualizaciones y lanzan nuevas versiones que son actualizadas de forma automática (primero McAfee ePo recibe la actualización, la despliegue a los *Agent Handler*, y estos a los equipos clientes finales). De forma resumida, permite:
    - Analizar archivos en puntos concretos.
    - Procesar y ejecutar coincidencias de patrones de definiciones de virus con datos encontrados en los archivos analizados.
    - Descifrar y ejecutar códigos de virus en un entorno emulado.
    - Aplicar técnicas heurísticas, es decir, técnicas que se basan en estimaciones y aproximaciones para reconocer virus nuevos.
    - Eliminar códigos infecciosos procedentes de archivos legítimos.

Por último, se adjuntan los resultados obtenidos con los equipos de la fase piloto:

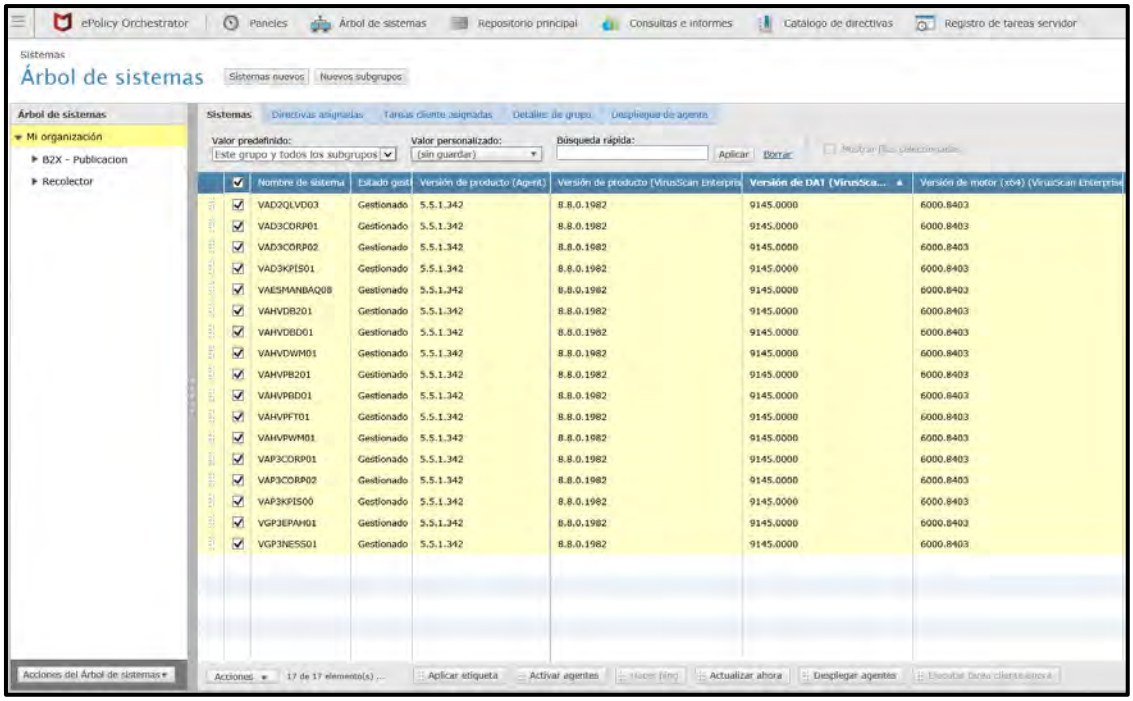


Ilustración 1: Resultados obtenidos sobre los equipos de la fase piloto

Finalmente, aunque se ha comprobado con éxito el resultado de la implementación del producto McAfee ePolicy Orchestrator 5.9.1, el cliente ha decidido paralizar el proyecto y el despliegue final del producto a todos los equipos de la compañía debido a un contratiempo:

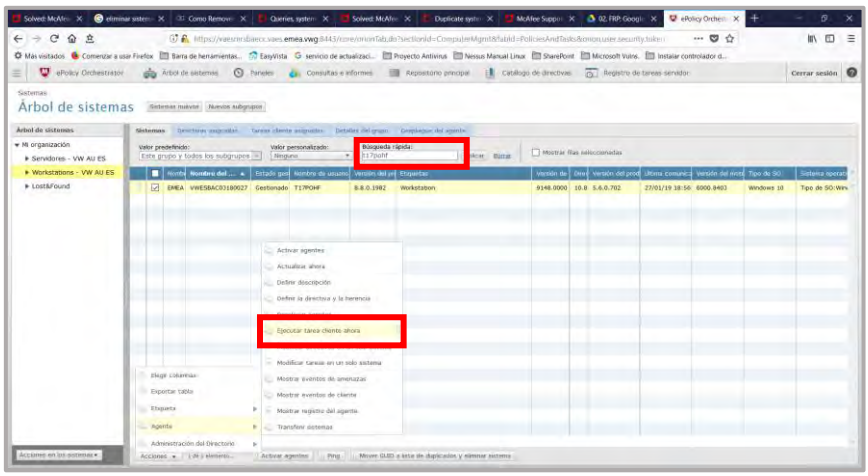
Se realizará un cambio de equipos a toda la compañía y no tiene sentido desplegar el McAfee Agent dos veces en un periodo de tiempo tan corto por el esfuerzo que supondría a los departamentos involucrados. En este sentido, se ha dejado lista la infraestructura y el procedimiento del despliegue para que, una vez se haya realizado el cambio de equipos, se pueda desplegar de forma ágil el producto a todos los equipos y servidores habiendo realizado las pruebas necesarias para garantizar el éxito del proyecto (fase piloto).

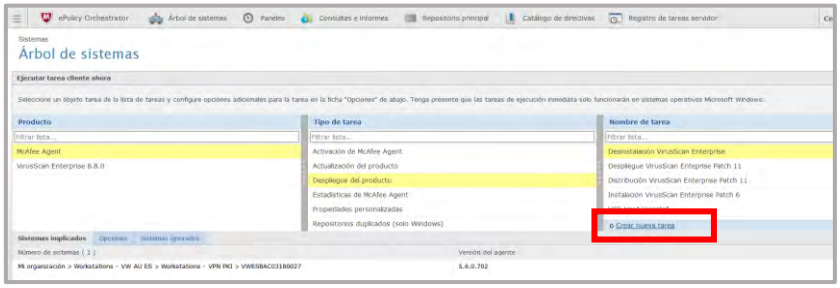
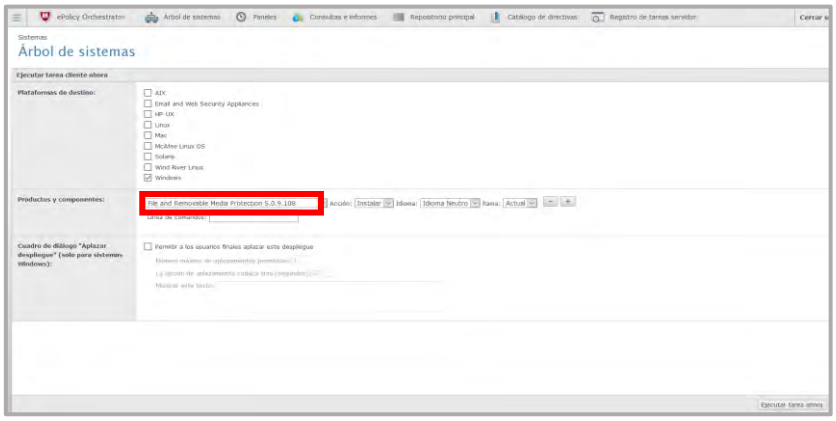
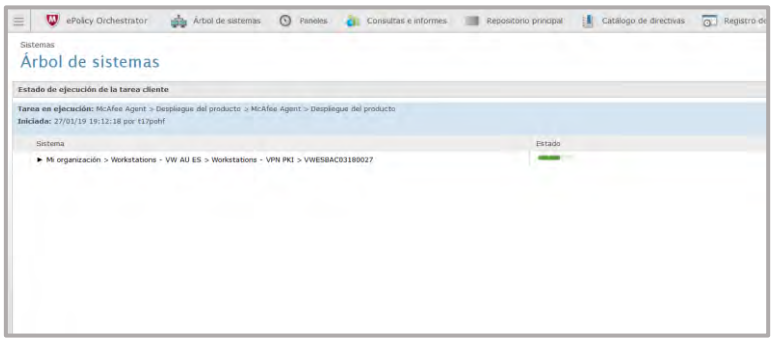
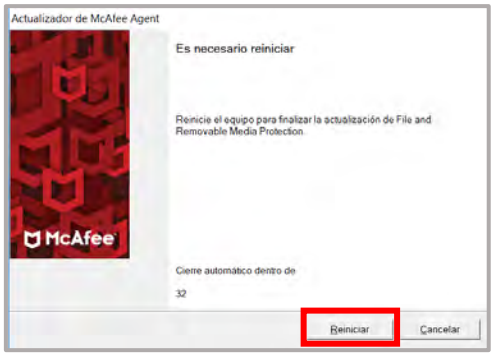
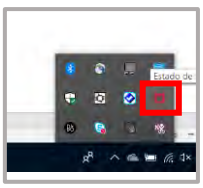
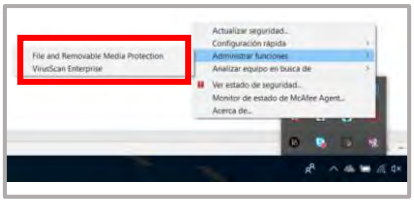
6. PRUEBA DE CONCEPTO FILE AND REMOVABLE MEDIA PROTECTION

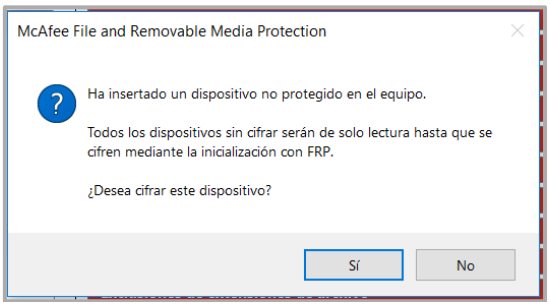
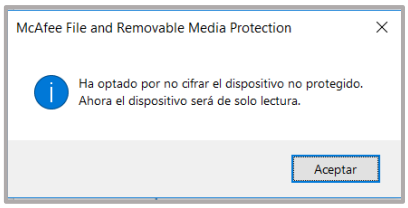
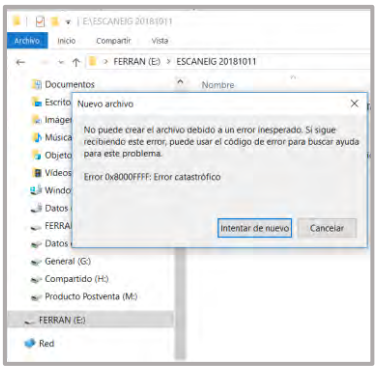
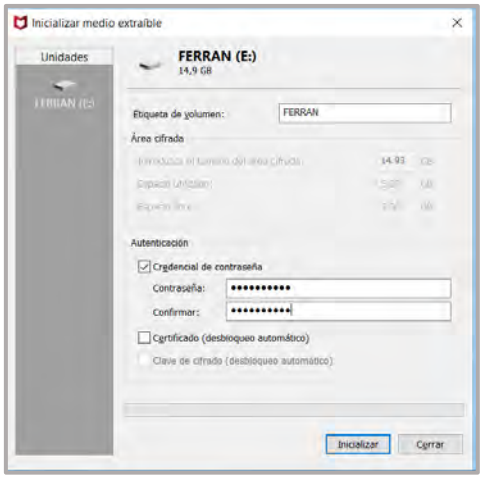
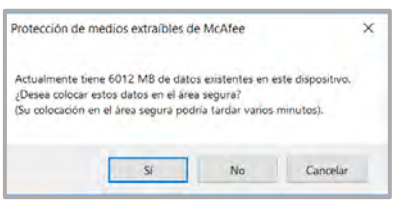
En este apartado se presenta el módulo FRP o *File and Removable Protection*. Este, nos ofrece muchas funcionalidades de seguridad adicionales al propio antivirus de McAfee (VirusScan Enterprise). Concretamente, FRP proporciona la aplicación de políticas automática y un cifrado transparente de ficheros y carpetas almacenadas o compartidas en equipos, *file servers* (servidores que sirven para compartir ficheros dentro de una compañía), servicios de almacenamiento en cloud, emails, y medios extraíbles como dispositivos USB, CD/DVDs, ficheros ISO. En nuestro caso, nos centraremos en el cifrado de medios extraíbles.

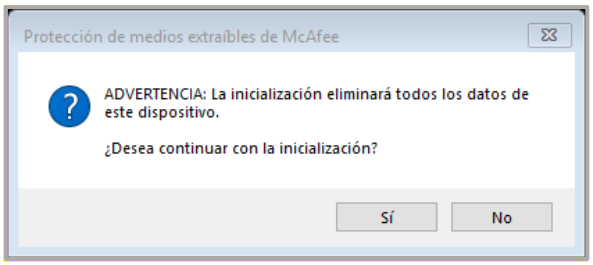
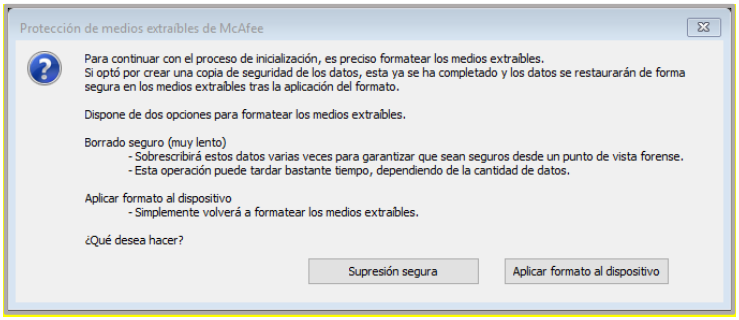
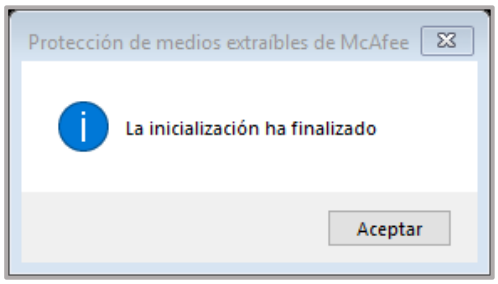
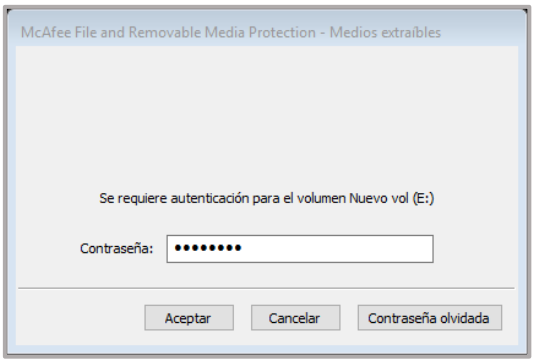
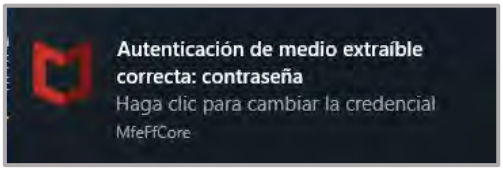
Concretamente, en el proyecto se pedía una prueba de concepto del módulo FRP en referencia al cifrado de medios extraíbles; es decir, por definición, una implementación resumida o incompleta con el propósito de verificar que dicha funcionalidad sea susceptible de ser explotada de manera útil por la compañía. Por lo tanto, la intención será recrear la funcionalidad de cifrado de medios extraíbles, como por ejemplo de USB, y que el equipo responda según lo esperado.
Una vez realizada la prueba de concepto, los *sponsors* serán los encargados de decidir si se explotará la idea y por lo tanto se implementará, o de otro modo, se renunciará a su implementación. Dado que el despliegue ha sido paralizado debido al contratiempo de cambio de equipos, la decisión de implementar o no el *FRP* no será tomada hasta que se remprenda de nuevo el proyecto.

A continuación, se muestra el proceso seguido para la implementación del módulo FRP, concretamente, el cifrado de medios extraíbles (por ejemplo, USB) en el equipo del cliente prestado a Ferran Angulo (usuario en el AD t17pohf):

1. En el apartado "Árbol de Sistemas", buscamos el equipo asignado a Ferran Angulo, con usuario "t17pohf". Seleccionamos ejecutar tarea cliente ahora:	

2. Seleccionar “Crear nueva tarea”.	
3. Seleccionar el producto “File and Removable Media Protection” del desplegable:	
4. Ejecutando esta tarea el equipo asignado a Ferran Angulo se forzará de forma centralizada y automática la instalación del *software* FRP.	
5. Una vez finalizada la ejecución de la tarea en el equipo final, solicitará al usuario de dicho equipo, reiniciarlo:	
6. Una vez reiniciado, comprobamos que se ha instalado correctamente:	 

7. El producto se encuentra instalado en el equipo. Comprobamos que al insertar USB funcione debidamente:	
8. Si optamos por no cifrar el dispositivo USB, el equipo no nos dejará escribir en él ya que será solo de lectura:	 
9. Si optamos por cifrar el dispositivo USB, deberemos introducir un nombre para el dispositivo y asignarle una contraseña que nos permitirá descifrar la información y escribir en el mismo. Seguidamente, si tubieramos datos en el USB, nos preguntará si queremos colocar los datos en área segura y indicamos la respuesta en	 

función de si tenemos datos sensibles y/o importantes. Por último, para aplicar los cambios se deberá eliminar los datos del dispositivo USB (indicar sí). Se podrá elegir entre "Supresión segura" o "Aplicar formato al dispositivo":	  
10. La próxima vez que insertemos el dispositivo USB en el portátil nos aparecerá la siguiente ventana solicitando la contraseña que introducimos.	 

7. CONCLUSIONES

El hecho de que el proyecto se haya realizado dentro del ámbito profesional en una empresa de grandes dimensiones ha permitido garantizar un profundo aprendizaje técnico, ya que previamente no había realizado ningún proyecto del estilo. Por otro lado, el proyecto en si me ha obligado a desarrollar nuevas habilidades, complementarias a las trabajadas habitualmente en el mundo académico. Quizás se trate de un conocimiento más social, o de saber dónde encontrar las respuestas a mis dudas iniciales del proyecto. En cualquier caso, este proyecto me ha dado un punto de vista distinto al que tenía hasta ahora, y es que la parte técnica del proyecto es muy importante, aunque también lo es la forma como gestionan todos los recursos necesarios, a nivel organizativo, para que este se ejecute.

Resumidamente, se detallan las principales conclusiones del proyecto:

- Previo a la ejecución de cualquier proyecto, es muy importante contextualizar y analizar el entorno de trabajo donde se desarrollará, para así garantizar el éxito de este.
- El producto McAfee ePolicy Orchestrator 5.9.1 es una solución flexible, robusta y que permite centralizar la gestión de todos los equipos de la compañía de forma ágil y eficiente. Adicionalmente, el producto puede ser implementado de tal forma que se adapte a la perfección al diagrama de red de cualquier empresa para poder ofrecer el servicio sin restricciones ni limitaciones por la zona de la red en la que se encuentren los usuarios o servidores.
- Actualmente, se está ofreciendo la posibilidad de dar servicio antivirus a todos los equipos de la compañía sin importar la zona de red en la que se encuentre. De esta forma, este hecho permite garantizar en mayor grado la seguridad alrededor de la compañía.
- La cooperación con otros departamentos ha sido vital para garantizar el éxito del proyecto, así como todas las relaciones que se han llevado a cabo para entender el funcionamiento y estado actual de la compañía.
- Realizar una fase piloto es totalmente necesario para garantizar el buen funcionamiento de la solución y para verificar la correcta instalación y implementación de cualquier herramienta.
- La integración de servicios corporativos con la solución McAfee ePolicy Orhcestrator 5.9.1 me ha permitido tener una visión más clara de cómo se interconectan las aplicaciones dentro de una compañía y como se relacionan entre ellas a nivel más técnico (p. ej. cómo delegar la autenticación de una aplicación a un servidor LDAP para sincronizarlo con el directorio activo).

- El cifrado de medios extraíbles en los equipos es una medida de seguridad ingeniosa y que permite proteger los datos del dispositivo incluso en caso de robo o pérdida del equipo. De esta forma, mediante el antivirus y el cifrado de medios extraíbles se asegura, en todo momento, la monitorización a nivel de seguridad del equipo. Esto permite reducirel riesgo de tener una incidencia de seguridad en cualquier equipo (infección por *malware*, fuga de datos, etc).

8. BIBLIOGRAFIA

A continuación, se citan los manuales públicos de McAfee utilizados para el desarrollo del proyecto:

- epo_590_Introduccion.pdf
- epo_590_pg_0b02_es-es.pdf
- epo_590_GuiaDelProducto
- epo_590_GuiaDeInstalacion.pdf

Adicionalmente, también hay que destacar toda la información proporcionada por el cliente en relación con el aprendizaje del entorno, así como todas las reuniones realizadas con el fin de conocer profundamente el entorno.

Por último, se adjuntan todas las referencias de información extraídas de Internet:

1. (10 de 11 de 2009). Obtenido de Tux para todos: https://comunicacionestux.wordpress.com/2009/11/10/servidor-ldap/

2. (9 de 5 de 2012). Obtenido de Wiki EOi: https://www.eoi.es/wiki/index.php/GESTI%C3%93N_DE_RIESGOS_en_Gesti%C3%B3n_de_proyectos

3. (10 de 12 de 2013). Obtenido de McAfee: https://kc.mcafee.com/corporate/index?page=content&id=KB52425&locale=es_ES&viewlocale=es_ES

4. (Enero de 2015). Obtenido de WhatIs: https://whatis.techtarget.com/definition/proxy-server

5. (11 de 2015). Obtenido de Deloitte: https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Evaluacion-Riesgos-COSO.pdf

6. (13 de 04 de 2017). Obtenido de McAfee: https://kc.mcafee.com/corporate/index?page=content&id=KB66741&locale=es_ES&viewlocale=es_ES

7. (2017). Obtenido de McAfee: https://www.mcafee.com/enterprise/en-gb/downloads/trials/epo-mcafee-agent-deployment.html

8. (2018). Obtenido de CISCO: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

9. *WIKIPEDIA*. (10 de Noviembre de 2018). Obtenido de https://es.wikipedia.org/wiki/System_Center_Configuration_Manager

9. ANEXOS

9.1. Requerimientos solicitados a infraestructura

A continuación, se muestran los requerimientos solicitados al departamento de infraestructura por cada uno de los 3 tipos de servidores necesarios para el montaje del proyecto:

- Servidor ePolicy Orchestrator Central: 1 servidor.
- Servidor Base de Datos de McAfee: 1 servidor.
- Servidor Controlador de Agentes o *Agent handler*: 5 servidores.

9.1.1. Servidor ePolicy Orchestrator Central

Requerimientos de hardware	
Dominio	VWGROUP
Ubicación:	Martorell
Servidor dedicado:	Sí
Tipo de servidor:	Virtual
Sistema de archivos:	NTFS
Software infraestructura virtual admitido:	VMware ESXi 5.5 **VMware ESXi 6**
Espacio de disco:	50GB
Memoria:	8GB de RAM mínimo
Tarjeta de red:	100MB mínimo recomendado
Procesador:	Intel Pentium D de 64 bits o superior @2,66 GHz o superior
Direccionamiento IP:	IP estática IP: TBD (to be defined) Mascara: TBD (to be defined) Gateway: TBD (to be defined)
Sistema Operativo:	Windows Server 2016 – 64 bits

Requerimientos de software	
Software preinstalado requerido:	Microsoft .NET Framework 3.5 o Posterior. Microsoft Visual C++ 2005 SP1 Redistributable. Microsoft Visual C++ 2008 Redistributable Package (x86). MSXML 6.0. Internet explorer 10 o superior.
Requisitos de preinstalación:	Actualizaciones de Microsoft en el momento de la instalación.

Tabla 13: Requerimientos técnicos servidor ePolicy Orchestrator Central

9.1.2. Servidor Base de Datos de McAfee

Requerimientos de hardware	
Dominio / Standalone	VWGROUP
Ubicación:	Martorell
Servidor dedicado:	Sí
Tipo de servidor:	Virtual
Sistema de archivos:	NTFS
Software infraestructura virtual admitido:	VMware ESXi 5.5 **VMware ESXi 6**
Espacio de disco:	60GB
Direccionamiento IP:	IP estática IP: TBD (to be defined) Mascara: TBD (to be defined) Gateway: TBD (to be defined)
Memoria:	8 GB
Tarjeta de red:	100 Mbps
Procesador:	Procesador x64: Intel Xeon compatible con Intel EM64T @2 GHz o superior
Sistema Operativo:	Windows Server 2016 – 64 bits

Requerimientos de software	
Software preinstalado requerido:	.NET 3.5 SP1 .NET 4.0 Windows PowerShell 2.0 SQL Server 2016
Requisitos de preinstalación:	Actualizaciones de Microsoft en el momento de la instalación.
Otros:	Las credenciales de la cuenta de usuario, tanto para la autenticación de Windows como de SQL, deben tener concedidas estas funciones de servidor en el servidor SQL Server de destino: • public • dbcreator • db_owner

Tabla 14: Requerimientos técnicos servidor base de datos de McAfee

9.1.3. Servidor controlador de agentes

Requerimientos de hardware	
Dominio	VWGROUP
Ubicación:	Martorell
Servidor dedicado:	Sí
Tipo de servidor:	Virtual
Sistema de archivos:	NTFS
Software infraestructura virtual admitido:	VMware ESXi 5.5 **VMware ESXi 6**
Espacio de disco:	50GB
Memoria:	8GB de RAM mínimo
Tarjeta de red:	100MB mínimo recomendado
Procesador:	Intel Pentium D de 64 bits o superior @2,66 GHz o superior
Direccionamiento IP:	IP estática IP: TBD (to be defined) Mascara: TBD (to be defined) Gateway: TBD (to be defined)
Sistema Operativo:	Windows Server 2016 – 64 bits

Requerimientos de software	
Software preinstalado requerido:	Microsoft .NET Framework 3.5 o Posterior. Microsoft Visual C++ 2005 SP1 Redistributable. Microsoft Visual C++ 2008 Redistributable Package (x86). MSXML 6.0. Internet explorer 10 o superior.
Requisitos de preinstalación:	Actualizaciones de Microsoft en el momento de la instalación.

Tabla 15: Requerimientos técnicos servidor Controlador de agentes (Agent handler)