UNIVERSIDAD GABRIELA MISTRAL
FACULTAD DE INGENIERIA

EndPoint un agente para la seguridad de la Información, Conexiones Remotas y Antivirus.

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : María Silvana Zapata Emblico
Profesor Guía : Roberto Carú Cisternas
Profesor Integrante : Jorge Tapia Castillo

Santiago – Chile
Octubre, 2017

INDICE

AGRADECIMIENTOS

Quiero Agradecer de manera especial a mis Hijos, Fernanda y Esteban, que con su cariño, comprensión y apoyo permitieron pudiera avanzar en mi desarrollo profesional, fueron ellos los que asumieron mi ausencia y estuvieron ahí dándome las fuerzas necesarias para lograr esta importante meta.
Agradezco a la Tía Isabel por haber cuidado a mis hijos en mis horas de ausencia, también agradecer a Xstrata que fue el gran impulsor y su apoyo fue primordial.

A mis Padres y Hermanos por guiar mi vida, por su gran ejemplo y valioso apoyo.

Doy las gracias a todos los profesores que aportaron de una u otra manera a mi crecimiento personal e intelectual.

A mi amigo José Acevedo por ese optimismo que siempre me impulso a seguir adelante para lograr terminar esta tesis.

Gracias a Dios por bendecirme, darme fuerza y Fe, para hacer realidad este anhelado sueño.

.¡¡Muchas Gracias a Todos!!

1 *INTRODUCCION*

Para todos la Integridad y seguridad de la información es un punto de gran importancia en la vida de hoy cada vez más móvil, nunca antes los datos corporativos han resultado ser más accesibles y transferibles que en la actualidad, y la inmensa mayoría de los datos son sensibles en diferentes niveles, es por esto que en Xstrata Copper necesitamos herramientas flexibles, seguras y rápidas para enfrentar las necesidades de manera eficiente, por lo que una de nuestras grandes preocupaciones ha sido la seguridad e integridad de la información, hoy en día es una obligación garantizar el acceso a los recursos y proteger los escritorios remotos.

Xstrata Copper

Es una de las unidades de negocio de commodities que conforman el importante grupo minero internacional diversificado Xstrata plc. Su sede central se encuentra en Brisbane, Australia y opera en ocho países: Argentina, Australia, Canadá, Chile, Estados Unidos, Filipinas, Papúa Nueva Guinea y Perú. Emplea a más de 20.000 personas y desempeña un papel esencial en las comunidades en las que habita y trabaja, al proporcionar empleo, capacitación, infraestructura, una fuente de ingresos para los proveedores y desarrollo social.

Paso a ser el cuarto mayor productor mundial de cobre y uno de los principales productores del mundo de cobre fundido, refinado y reciclado, incluidos los materiales de terceros.

El Cobre que producimos es vital para nuestra sociedad moderna y se utiliza ampliamente en la generación y distribución de la energía, en materiales de construcción y en equipos electrónicos. Gracias a su creciente aplicación en tecnologías ecológicas y como agente antimicrobiano, además de su capacidad para

ser reciclado, el cobre desempeña un papel relevante en la creación de un futuro sostenible.

El gran problema que necesitamos solucionar es la conexión a todos nuestros servicios para los usuarios viajeros, además resguardar la información que llevan en sus notebook, esto debido a que cuando están de viaje deben llevar la información en sus equipos o discos externos y con el problema latente de perdida de información ya sea por daños en los equipos o perdidas de estos en la mayoría de los casos por robo, como solución necesitamos una única aplicación que cumpla las expectativas, para esto se optó por Endpoint Security.

Dado lo anterior es que el trabajo estará enfocado en la aplicación mencionada como la solución viable para resguardar la información de la empresa ante las amenazas, por tal motivo la presente Tesis está orientada en el proceso de habilitación y puesta en marcha de la aplicación Sharepoint Endpoint.

Esta aplicación nos proporciona:

- Antivirus: Para identificar y bloquear el malware
- Antibot: Para detectar y prevenir el daño por robots
- IPS: Para evitar intrusiones de forma proactiva
- Control Web - Filtrado URL y Control
- Acceso Remoto: conexiones a través de VPN
- Protección del dato a través de la encriptación.

1.1 Motivación

Las operaciones y proyectos de cobre de Xstrata se encuentran distribuidos en al menos diez países, por ser una empresa perteneciente al sector minero tiene

departamentos de un nivel de exigencia de viajes y trabajos en terreno muy alto, lo que implica tener que moverse mucho con sus notebook poniendo en riesgo la información, datos valiosos que de perderlos significan mucho en valor tanto monetario como en lo confidencial, por lo que pasa a ser uno de los problemas graves en lo que la empresa necesita tener un resguardo.

Al menos un 10% de los equipos eran perdidos en los viajes, (generalmente por robos de equipos), un 30% por daño en los discos duros de los equipos de terreno debido a las exposiciones de estos al medio ambiente donde se encontraban trabajando. (Polvo, calor, altura) donde el área de exploraciones es el departamento más afectado dentro de la empresa, un 5% perdida de data por borrado accidental de esto y un 10% por virus.

Con el objetivo de brindar la tranquilidad de que los datos robados o perdidos ya no será una preocupación porque ya estaremos prevenidos al momento de tener habilitada e instalada la aplicación, qué será sin duda una mejora para la eficiencia y operatividad de Xstrata. Además debemos diseñar la mejor forma que esta implementación cause el menor impacto en nuestros usuarios.

1.2 Hipótesis

La Hipótesis de esta tesis está basada en la búsqueda de una metodología que nos permita resguardar la información de los equipos móviles ante un evento de pérdida o robo de datos relevantes para nuestra empresa donde la perdida de estos podría provocar graves problemas, el que la empresa tenga un nivel de exigencia de viajes y trabajos en terreno muy alto, nuestros usuarios constantemente están poniendo en riesgo la información es por esto que el resguardo ante una pérdida de equipo o robo de este, debe existir la tranquilidad que no podrán tener acceso de forma alguna a estos.

Para todo lo anteriormente mencionado nos lleva utilizar Check Point Endpoint Security agente que combina todos los componentes críticos para la seguridad total y ofrece mayores niveles de seguridad mientras que proporciona un manejo transparente al usuario final.

“Los datos perdidos o robados es una preocupación que puede prevenirse.”

1.3 Objetivo General

La encriptación previene el robo y manipulación de información confidencial almacenada en notebooks, discos duros y otros dispositivos. Aun cuando estos equipos se encuentren fuera de la organización por haber sido robado o extraviados, el estar encriptados se preserva la privacidad de la información.

Para esto se decidió implementar la aplicación EndPoint, esta nos permite resguardar la información por medio de la encriptación de los disco, también utilizarla para conexión remota solucionando otro punto importante como es poder conectarse desde cualquier punto donde se encuentren a nuestra red y como antivirus tema no menor importante que los mencionados antes.

Nuestra propuesta es “beneficios de tener una única solución de seguridad”, para lo cual se optó por esta aplicación, el proyecto implica instalar en todos los equipos móviles de la empresa, permitiendo cumplir con esto la solución a nuestro problema, esto significa además tener que capacitar a los usuarios.

Objetivos Principales:

- Delegar e instruir al personal de Field Support en los pasos requeridos para llevar a cabo la administración del cliente Checkpoint Endpoint Security.
- Administración de políticas de Media Encryption
- Habilitación de encriptación de medios.

1.4 Alcances

Para el proceso de este trabajo de titulación se desarrollarán las actividades que permitían implementar e instalar en los diferentes sitios asignados la única solución de seguridad que se optó a nivel global para Xstrata, el software Endpoint Security de Checkpoint.

2 MARCO TEORICO.

2.1 Virus Informáticos.

Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador.

Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este, aunque también existen otros más inofensivos, que solo producen molestias.

Tienen básicamente, la función de propagarse a través de un software, son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Los virus informáticos son, desde hace varios años, la mayor amenaza para los sistemas informáticos y es una de las principales causas de pérdidas económicas en las empresas y usuarios.

2.1.1 Historia

Desde la aparición de los virus informáticos en 1984 y tal como se les concibe hoy en día, han surgido muchos mitos y leyendas acerca de ellos. Esta situación se agravó con el advenimiento y auge de Internet.
Existen multitud de fechas equivocadas y diferentes para los mismos acontecimientos de la historia de los virus, por ello es bastante complicado establecer fechas exactas.

Tras contrastar diferentes fuentes de información esta sería una breve cronología de la historia de los virus:

- **En 1939**, el famoso científico matemático John Louis Von Neumann, de origen húngaro, escribió exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

- **1949 – 1950** en los laboratorios de la Bell Computer, subsidiaria de la AT&T, tres jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, desarrollaron inspirados en la teoría de John Louis Von Neumann un “juego” llamado CoreWar. Los contenedores del CoreWar ejecutaban programas que iban poco a poco disminuyendo la memoria del computador. Ganaría este “juego” el que consiguiera eliminarlos totalmente. El conocimiento de la existencia de CoreWar era muy restringido.

- **1972, aparece Creeper** desarrollado por Robert Thomas Morris que atacaba a las conocidas IBM 360. Simplemente mostraba de forma periódica el siguiente mensaje: "I'm a creeper... catch me if you can!" (Soy una enredadera, cójanme si pueden). Fue aquí donde podríamos decir que apareció el primer antivirus conocido como Reaper (segadora) el cual eliminaba a Creeper.

- **1975, John Brunner** concibe la idea de un “gusano” informático que crece por las redes.

-**En 1980 la red ArpaNet** del ministerio de Defensa de los Estados Unidos de América, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa antivirus correspondiente.

-**1983 Keneth Thompson,** este joven ingeniero, quien en 1969 creó el sistema operativo UNIX, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública en la que presentó y demostró la forma de desarrollar un virus informático.

- **1984, Fred Cohen** en su tesis acuña el término “virus informático”. Fue en este año donde se empezó a conocer el verdadero peligro de los virus, ya que los usuarios del BIX BBS, un foro de debates de la ahora revista BYTE, avisaron de la presencia y propagación de una serie de programas que habían infectado sus computadoras.

- 1986, aparece lo que se conoce como el primer virus informático, Brain, atribuido a los hermanos pakistaníes. Además este año se difundieron los virus , Bouncing Ball y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión EXE y COM.

- 1987, el gusano Christmas tree satura la red de IBM a nivel mundial.

- 1988, Robert Tappan Morris, hijo de uno de los precursores de los virus, difunde un virus a través de ArpaNet, (precursora de Internet) infectando a unos 6,000 servidores.

- 1989, el virus Dark Avenger también conocido como "vengador de la oscuridad", se propaga por Europa y Estados Unidos. Sobre dicho virus se han escrito multitud de artículos e incluso un libro ya que se diferenciaba de los demás en su ingeniosa programación y su rápida infección.

- 1990, Mark Washburn crea “1260”, el primer virus polimórfico, que muta en cada infección.

- **1992, aparece el conocido virus Michelangelo** sobre el cual se crea una gran alarma sobre sus daños y amplia propagación, aunque finalmente fueron pocos los ordenadores infectados.

- 1994, Good Times, el primer virus broma.

- 1995, aparece Concept con el cual comienzan los virus de macro. Y es en este mismo año cuando aparece el primer virus escrito específicamente para Windows 95.

- 1997, comienza la difusión a través de internet del virus macro que infecta hojas de cálculo, denominado Laroux.

- 1998, aparecen un nuevo tipo de virus macro que ataca a las bases de datos en MS-Access. Llega CIH o Chernobyl que será el primer virus que realmente afecta al hardware del ordenador.

- 1999, A principios de este año se empezaron a propagar masivamente por Internet los virus anexados a mensajes de correo como puede ser Melissa, BubbleBoy, etc. Este último (BubbleBoy) infectaba el ordenador con simplemente mostrar el mensaje (en HTML).
- 2000, se conoce la existencia de VBS/Stages.SHS, primer virus oculto dentro del Shell de la extensión .SHS. Aparece el primer virus para Palm.
- 2001, el virus Nimda atacó a millones de computadoras, a pocos días del ataque a las Torres Gemelas de la isla de Manhattan.
Actualmente, existen multitud de técnicas mucho más sofisticadas y conocidas, lo que permite que se hagan mayor cantidad de virus (13 diarios según Panda Software) y sean más complejos. De esta forma aparecen virus como MyDoom o Netsky. A pesar de esto no solo la sofisticación de los virus ha aumentado la infección de equipos sino también la “Ingeniería Social” y la, a veces increíble, ingenuidad de usuarios y administradores que facilitan bastante la labor de los virus. Aun con todos los avances que se están haciendo en la actualidad para mejorar la seguridad de los sistemas, no podemos decir que éstos nos reporten la seguridad necesaria.

Hoy día los desarrolladores de antivirus resuelven un problema de virus en contados minutos.

Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de "graffiti cibernético", así como los crackers jamás se detendrán en su intento de "romper" los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades. Podemos afirmar que la eterna lucha entre el bien y el mal ahora se ha extendido al ciber espacio.

2.1.2 Métodos de infección

Hay muchas formas con las que un computador puede exponerse o infectarse con virus. Veamos algunas de ellas:

- Mensajes dejados en redes sociales como Twitter o Facebook.
- Archivos adjuntos en los mensajes de correo electrónico.
- Sitios web sospechosos.
- Insertar USBs, DVDs o CDs con virus.
- Descarga de aplicaciones o programas de internet.
- Anuncios publicitarios falsos.

2.2 Antivirus

Los antivirus nacieron como una herramienta simple cuyo objetivo fuera detectar y eliminar virus informáticos, durante la década de 1980. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar un Virus informáticos, sino bloquearlo para prevenir una infección por los mismos, así como actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, entre otros.

2.2.1 Funcionamiento de los Antivirus

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador. Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuales son potencialmente dañinas para el ordenador, con técnicas como Heurística, HIPS, entre otros.

Usualmente, un antivirus tiene un (o varios) componente residente en memoria que se encarga de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso. Asimismo, cuentan con un componente de análisis bajo demando (los conocidos scanners, exploradores), y módulos de protección de correo electrónico, Internet. El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección

Un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

Los virus, gusanos, troyanos, spyware son tipos de programas informáticos que suelen ejecutarse sin el consentimiento (e incluso, conocimiento) del usuario o propietario de un ordenador y que cumplen diversas funciones dañinas para el sistema. Entre ellas, robo y pérdida de información, alteración del funcionamiento, disrupción del sistema y propagación hacia otras computadoras.

Los antivirus son aplicaciones de software que han sido diseñados como medida de protección y seguridad para resguardar los datos y el funcionamiento de sistemas informáticos caseros y empresariales de aquellas otras aplicaciones conocidas comúnmente como virus o malware que tienen el fin de alterar, perturbar o destruir el correcto desempeño de las computadoras.

Un programa de protección de virus tiene un funcionamiento común que a menudo compara el código de cada archivo que revisa con una base de datos de códigos de virus ya conocidos y, de esta manera, puede determinar si se trata de un elemento perjudicial para el sistema. También puede reconocer un comportamiento o patrón de conducta típico de un virus. Los antivirus pueden registrar tanto los archivos

que se encuentran adentro del sistema como aquellos que procuran ingresar o interactuar con el mismo.

Como nuevos virus se crean en forma casi constante, siempre es preciso mantener actualizado el programa antivirus, de forma de que pueda reconocer a las nuevas versiones maliciosas. Así, el antivirus puede permanecer en ejecución durante todo el tiempo que el sistema informático permanezca encendido, o bien, registrar un archivo o serie de archivos cada vez que el usuario lo requiera. Normalmente, los antivirus también pueden revisar correos electrónicos entrantes y salientes y sitios web visitados.

Un antivirus puede complementarse con otras aplicaciones de seguridad como firewalls o anti-spyware que cumplen funciones accesorias para evitar el ingreso de virus.

2.3 Red Privada Virtual

Una red privada virtual (RPV), (Virtual Private Network (VPN) Figura 1), es la tecnología de red de computadoras que nos permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde cualquier sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

La conexión VPN a través de Internet es técnicamente una unión WAN (wide area network figura 2) entre los sitios pero para el usuario le parece como si fuera un enlace privado de allí la designación "virtual private network".

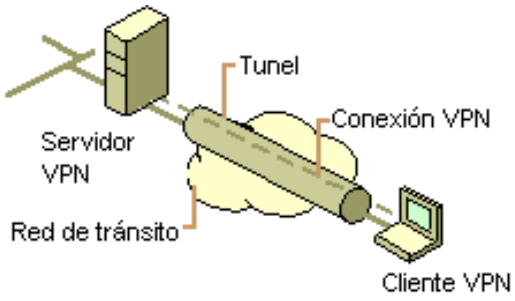


Figura 1: Conexión de red privada virtual

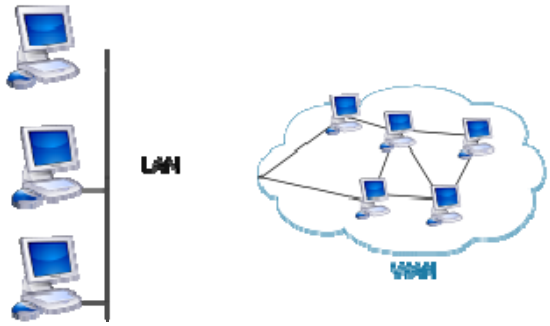


Figura 2: Interconexión entre la red de área local (LAN) y la red de área amplia (WAN).

2.3.1 Requisitos básicos

- Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

- Cifrado de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que únicamente pueden ser leídos por el emisor y receptor.
- Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.
- Nuevo algoritmo de seguridad SEAL.

2.3.2 Tipos de VPN

Básicamente existen cuatro arquitecturas de conexión VPN:

1. **VPN de acceso remoto:** Considerado como el más común en este momento es la conexión remota de un usuario o grupo de usuarios desde sitios externos de la empresa utilizando el internet como modo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

2. **VPN punto a punto:** Está basado en las conexiones desde un eje central (Sede principal de la empresa) o componente central VPN y los servidores de otras oficinas que estén remotas. Se conectan a internet solo utilizando internet de los proveedores de servicios, en definitiva es medida de ahorro en cables y conexiones físicas o denominados conexiones punto a puntos tradicionales, sobre todo si se encuentran ubicadas en diversos estados del país o incluso fuera de él.

3. **Tunneling:** Consiste en la apertura de conexiones dentro de dos dispositivos mediante un protocolo. Un ejemplo de un protocolo seguro puede ser el SSH (Secure Shell) la cual funciona encapsulando un protocolo de red sobre otro

protocolo de red para poder acceder a dispositivos, de esta forma pasando toda comunicación IP de modo inseguro a seguro a través de un túnel.

4. **VPN Interna (over LAN):** Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Una VPN puede aportar grandes beneficios si está bien diseñada. Por ejemplo, puede:

- Ampliar la conectividad geográfica
- Reducir los costos de funcionamiento en comparación con las WAN tradicionales
- Reducir el tiempo de tránsito y los gastos de viaje de los usuarios remotos
- Mejorar la productividad
- Simplificar la topología de red
- Proporcionar oportunidades de trabajo en red global
- Servir de apoyo al trabajador que está desplazándose
- Proporcionar un retorno de inversión (ROI) más rápido que el de una WAN tradicional.

Una VPN bien diseñada debe incluir lo siguiente:

- Seguridad
- Fiabilidad
- Escalabilidad
- Administración de la red
- Administración de política

2.4 Encriptación

La Criptografía (criptos), oculto, y (grafé), grafo ó escritura, literalmente escritura oculta). Tradicionalmente se ha definido como el ámbito de la criptología el que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

La Criptología es la ciencia que estudia la transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original.

La mayoría de los algoritmos modernos del cifrado se basan en una de las siguientes dos categorías de procesos:

- Problemas matemáticos que son simples pero que tienen una inversa que se cree (pero no se prueba) que es complicada
- Secuencias o permutaciones que son en parte definidos por los datos de entradas.

La Encriptación es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros. Opcionalmente puede existir además un proceso de desencriptación a través del cual la información puede ser interpretada de nuevo a su estado original, aunque existen métodos de encriptación que no pueden ser revertidos. El término encriptación es traducción literal del inglés y no existe en el idioma español. La forma más correcta de utilizar este término sería cifrado.

2.4.1 *Usos de la Encriptación*

Algunos de los usos más comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas de crédito, reportes administrativo-contables y conversaciones privadas, entre otros.

Como sabemos, en un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, y confidencialidad.
Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encriptación de Datos.

2.4.2 *Métodos de Encriptación*

Para poder Encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes:

Los algoritmos HASH, los simétricos y los asimétricos.

1. Algoritmo HASH:

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

2. Criptografía de Clave Secreta o Simétrica

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

Los criptosistemas de clave secreta se caracterizan porque la clave de cifrado y la de descifrado es la misma, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

Sus principales características son:

- Rápidos y fáciles de implementar
- Clave de cifrado y descifrado son la misma
- Cada par de usuarios tiene que tener una clave secreta compartida
- Una comunicación en la que intervengan múltiples usuarios requiere muchas claves secretas distintas

Actualmente existen dos métodos de cifrado para criptografía de clave secreta:

- Cifrado de flujo
- Cifrado en bloque

3. Algoritmos Asimétricos (RSA):

Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir. El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. El usuario, ingresando su PIN genera la clave Pública y Privada necesarias. La clave Pública podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada. Cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la Clave Publica porque el utilizó su Clave Privada.

2.4.3 Firma Digital

La firma digital permite garantizar algunos conceptos de seguridad que son importantes al utilizar documentos en formato digital, tales como Identidad o autenticidad, integridad y no repudio. El modo de funcionamiento es similar a lo explicado para los algoritmos de encriptación, se utilizan también algoritmos de clave pública, aplicados en dos etapas.

Ventajas Ofrecidas por la Firma Digital

- Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, el receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor

• Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.

• No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

2.5 Firewall

El término firewall es de origen inglés y en los últimos años ha adquirido un uso especialísimo en el ámbito de la informática y aún a pesar de pertenecer a otro idioma la palabra firewall se ha incorporado al idioma español y es usada como propia, en la jerga de los usuarios y técnicos del área informática. Su traducción literal a la lengua castellana sería cortafuegos.

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a iinformación confidencial. Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Es un mecanismo para restringir acceso entre Internet y la red corporativa interna. Típicamente se instala un firewall en un punto estratégico donde una red (o redes) se conectan a Internet.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para

permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser la web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

Un buen Firewall para Internet puede ayudarle a impedir que extraños accedan a su PC desde Internet. Los Firewalls pueden ser de dos tipos, de software o de hardware, y proporcionan una frontera de protección que ayuda a mantener fuera a los invasores no deseados de Internet, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con softwares específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

La existencia de un firewall en un sitio Internet reduce considerablemente las probabilidades de ataques externos a los sistemas corporativos y redes internas, además puede servir para evitar que los propios usuarios internos comprometan la seguridad de la red al enviar información peligrosa (como password no encriptados o datos sensitivos para la organización) hacia el mundo externo.

Si el Firewall observa alguna actividad sospechosa como que alguien de fuera esté intentando acceder a nuestro Pc o que algún programa espía trate de enviar información sin consentimiento, el Firewall nos advertirá con una alarma en el sistema.

Para entender el funcionamiento de este sistema, debes saber que el ordenador dispone de varias puertas de salida y entrada cuando se conecta a Internet. Éstas se llaman puertos y cada servicio que utilizas se sirve de un puerto diferente: Los navegadores de internet necesitan el puerto 80, los programas FTP el 21, en general tenemos todos los puertos abiertos.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web.

Entonces, mayormente, el firewall se destina para que usuarios de internet que no estén autorizados ingresen a algunas redes privadas, en especial a las intranets.

Ahora bien, cabe destacarse que el firewall provee de una protección correcta a cualquier red, aunque, no debe considerarse como infalible y a veces es necesario incorporar más condiciones y elementos a la seguridad para hacerla más fuerte.

Por caso es que el firewall no podrá contrarrestar: aquellos ataques que no transiten por él, la acción negligente de usuarios propios, los virus que ingresan por software o archivos.

2.5.1 Objetivo de un Firewalls

Un firewall sirve para múltiples propósitos, entre otros podemos anotar los siguientes:

- Restricción de entrada de usuarios a puntos cuidadosamente controlados de la red interna.

- Prevención ante los intrusos que tratan de ganar espacio hacia el interior de la red y los otros esquemas de defensas establecidos.

- Restricción de uso de servicios tanto a usuarios internos como externos.

- Determinar a qué servicios de red tendrán accesos los que están fuera, es decir, quién puede entrar a utilizar los recursos de red pertenecientes a la organización.

Todo el tráfico que viene de la Internet o sale de la red corporativa interna pasa por el firewall de tal forma que él decide si es aceptable o no.

2.5.2 Beneficios de un firewall

- Administra los accesos posibles del Internet a la red privada.

- Protege a los servidores propios del sistema de ataques de otros servidores en Internet.

- Permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no-autorizados, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red.

- Ofrece un punto donde la seguridad puede ser monitoreada.

- Ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall es ideal para desplegar servidores WWW y FTP.

2.5.3 Limitación de un Firewalls

- Puede únicamente autorizar el paso del tráfico, y él mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno a éste.

- No puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación.

- No puede proteger de las amenazas a que está sometido por traidores o usuarios inconscientes.

- No puede prohibir que los traidores o espías corporativos copien datos sensitivos y los substraigan de la empresa.

- No puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado.

- No puede proteger contra los ataques posibles a la red interna por virus informativos a través de archivos y software.

***Política interna de seguridad*.**

Un firewall de Internet no está solo, es parte de la política de seguridad total en una organización. Para que ésta sea exitosa, la organización debe conocer qué es lo que se está protegiendo.

3 *DESARROLLO DEL TRABAJO*

3.1 Endpoint Security de Check Point

Check Point Software Technologies Ltd. Es proveedor global de soluciones de seguridad de IT. Es Conocido por sus productos Firewall y VPN, Check Point y fue el pionero en la industria con el FireWall-1 y su tecnología patentada de inspección de estado. Check Point ha lanzado el primer agente de seguridad del endpoint que incluye todas las características y funciones necesarias para una real e eficiente seguridad. No es necesario gastar tanto tiempo y recursos para testear, configurar e implementar su solución de seguridad. Este agente combina el mejor firewall, control de acceso a la red (NAC), control de programas, anti-virus, anti-spyware, encripción total del disco duro, encripción de medios, con protección de los puertos y acceso remoto, todo en un único agente.

Check Point Software Technologies Ltd. (www.checkpoint.com), el líder mundial en seguridad en Internet, proporciona a los clientes protección sin compromiso frente a todo tipo de amenazas, reduce la complejidad de la seguridad y reduce el coste total de la propiedad. Hoy Check Point continua desarrollando nuevas soluciones basadas en la arquitectura Software Blade, que ofrece a los clientes las soluciones flexibles y sencillas que pueden personalizarse completamente para ajustarse a las necesidades de seguridad específicas de cualquier organización.

Check Point es el único proveedor que va más más allá de la tecnología y define la seguridad como un proceso más del negocio. Check Point 3D Security combina de forma única políticas, personas y la aplicación de un mayor nivel de protección de los activos de información y ayuda a las organizaciones a implementar un plan de seguridad que se alinee con las necesidades del negocio. Entre sus clientes se incluyen decenas de miles de organizaciones de todos los tamaños, incluyendo todas las empresas Fortune y Global 100. Las galardonadas soluciones ZoneAlarm de

CheckPoint protegen millones de consumidores de hackers, spyware y robos de identidad.

Las amenazas y los peligros de una fuerza móvil.

Al proporcionar a los empleados, contratistas y socios de negocios un acceso instantáneo remoto y seguro a la red corporativa, se proporciona una enorme ventaja en términos de productividad y eficiencia, pero también se presentan importantes riesgos para la seguridad de la empresa. Computadoras portátiles que contiene datos confidenciales de la empresa o de clientes pueden ser perdidos o robados; archivos confidenciales, las credenciales de inicio de sesión y contraseñas pueden quedar en dispositivos no confiables al final de una sesión, haciéndolos fácilmente disponible a los usuarios posteriores. Además, los empleados que se autentican en forma remota, podría estar usando una máquina poco confiable o una máquina con software malintencionado y abrir un puerto directo a la red de la empresa, haciéndola vulnerable a una matriz de amenazas de seguridad.

3.1.1 Su Historia

Fundada en 1993, en Ramat-Gan, Israel por el Presidente actual de la compañía y CEO Gil Shwed, a la edad de 25 años, y junto a , Marius Nacht (actualmente Vice-Presidente) y Shlomo Kramer (en el 2003 dejó Check Point para crear una nueva empresa).Gil tuvo la idea inicial de la tecnología base de la empresa que se conoce como inspección de estado, siendo esta la raíz para el primer producto de la compañía (llamado simplemente FireWall-1), poco después desarrollaron uno de los primeros productos VPN del mundo (VPN-1).

La empresa tuvo su primer éxito comercial en 1994, cuando Check Point firma un acuerdo OEM con Sun Microsystems, seguido por un acuerdo de distribución con HP en 1995. El mismo año, se abre la oficina central de EE.UU. establecida en l ciudad de Redwood, California.

Para febrero de 1996, la compañía es nombrada líder del mercado mundial en Firewall por IDC, con un 40% del Mercado. En junio de 1996 Check Point recauda $ 67 millones de su oferta pública inicial de acciones en el NASDAQ.

En 1998, Check Point establece una exitosa alianza con Nokia, que combina el software de Check Point con los accesorios de seguridad de red para ordenadores de Nokia, para el 2000 la empresa se convirtió en el principal proveedor mundial de soluciones de VPN (en términos de cuota de mercado). Durante la década del 2000, Check Point adquiere otras empresas de seguridad IT, culminando con la adquisición de la unidad de negocio de Nokia en seguridad de red en el año 2009, poco más de 10 años después de la primera asociación con Nokia.

Check Point cuenta con una larga historia, formación y certificaciones en sus productos, incluyendo las siguientes:

- CPCS - Check Point Certified Specialist
- CCSA - Check Point Certified Security Administrator
- CCSE - Check Point Certified Security Expert
- CCSE+ - Check Point Certified Security Expert Plus
- CCMSE - Check Point Certified Managed Security Expert
- CCMA - Check Point Certified Master Architect

3.1.2 *Comparación con otros Productos*

En el cuadro siguiente (Figura 3) un resumen del estudio realizado, aquí se tomaron dos de las opciones propuestas más el antivirus usado en ese momento con el fin de poder identificar cual es el que cumplía con las necesidades requeridas por Xtrata.

En la actualidad existe una alta gama de productos compatibles para la solución al problema, luego de revisar las características de los productos estudiados se determina que el que cumple con todo es Endpoint Checkpoint de software Technologies Ltda.

	Kaspersky Antivirus	Microsoft Forefront	Check Point Endpoint
Antivirus			
Protección			
Detección de virus	100,00%	98,30%	99,50%
Detección de nuevas amenazas	99,90%	99,00%	99,00%
Desinfección	93,00%	85,00%	89,00%
Fallos en detección	2	5	2
FUNCIONES			
Protección contra virus	✓	✓	✓
Protección del bloqueo de archivos	✓	✓	✓
Protección de identidad	✓	✓	✓
Escaneo de email	✓	✓	✓
Escaneo de arch. comprimidos	✓	✓	✓
Autolimpieza de amenazas	✓	✓	✓
Protección de redes sociales	✓	✓	✓
Navegador seguro	✓	✗	✓
Auto-escaneo de URL	✓	✓	✓
Auto-escaneo de USB	✓	✓	✓
Administrador de contraseñas	✓	✓	✓
Disco de rescate	✓	✓	✓
VPN			
FUNCIONES			
Seguridad	✓	✗	✓
Fiabilidad	✓	✗	✓
Escabilidad	✓	✗	✓
Adminnistracion de red	✓	✗	✓
Administracion de Politicas	✓	✗	✓
Control de Programas	✓	✗	✓
Acceso remoto seguro a correo electronico.	✓	✗	✓
Firewall			
FUNCIONES			
Firewall/NAC/Programa de Control	✓	✓	✓
Encriptación de discos			
FUNCIONES			
Cifrado de datos disco local	✗	✗	✓
Cifrado datos perifericos	✗	✗	✓
SOPORTE			
Teléfono	✓	✓	✓
Email / Ticket/ Foros	✓	✓	✓
Chat en directo	✓	✓	✓
Soporte remoto	✓	✗	✓
COMPATIBILIDAD			
Windows 10	✓	✓	✓
Windows 8 / 8.1	✓	✓	✓
Windows 7 / Vista	✓	✓	✓

Figura 3: Cuadro del estudio comparativo.

En el cuadro se puede apreciar el motivo por el cual se eligió Endpoint, una de las principales necesidades era la seguridad de la data en los equipos móviles y esto sin duda se da con la encriptación y Kasperky no lo proveía, es por esta principal razón que no se seleccionó.

3.1.3 Porque Checkpoint?

Gracias a la tecnología de Check Point se ha podido lograr una solución que responde a todos los requerimientos y ofrece además una seguridad inmejorable y constante en toda la red frente a cualquier tipo de ataque o amenaza.
Dentro de las características del producto, Check Point Web Check asegura el Endpoint contra el creciente número de amenazas basadas en Web, Check libera los sistemas de seguridad en los PCs con un solo login.
Media Encryption, con su cifrado completo proporciona una sólida protección de datos para los ordenadores portátiles.
Checkpoint permite robustecer y simplificar las comunicaciones, así como incorporar nuevas funcionalidades para optimizar la infraestructura tecnológica.
Check Point Endpoint Security combina todas las funciones de seguridad para el Endpoint en un único agente administrado en forma centralizada que suministra completa seguridad, administración de seguridad vía una única y unificada consola.

3.1.4 *Productos que ofrece Checkpoint*.

Checkpoint WebCheck: navegación segura, a la empresa de las amenazas basadas en la Web con un manejo transparente a los usuarios

Checkpoint OneCheck: proporciona una información de acceso fácil de Windows y todas las funciones de punto final de seguridad (cifrado de disco completo, VPN de acceso remoto y Media Encryption).

VPN de acceso remoto: permite el acceso remoto seguro a los recursos de la empresa mediante la encriptación y la autenticación de los datos transmitidos durante las sesiones de acceso remoto. Otorga nuevas capacidades de conexión, mientras que mantiene la conectividad roaming entre LAN, WiFi y redes GPRS y configura automáticamente la sesión de VPN en el acceso de redes remotas.

Checkpoint Firewall: líder de la industria de la seguridad, bloquea el tráfico no deseado, previene que el malware infecte los sistemas de punto final y los hace invisibles para los piratas informáticos.

Programa de Control: asegura la legitimidad de los programas autorizados a circular por el endpoint. Programa Advisor de Check Point: utiliza una base de conocimientos de más de un millón de solicitudes de confianza y sospecha de malware para establecer automáticamente la configuración del programa de control.

Anti-virus/Anti-spyware: detecta y elimina virus, programas espía, capturadores de teclado, troyanos, rootkits y otro malware basado en una combinación de firmas, bloqueadores de comportamiento y análisis heurístico, con las mayores tasas de detección y las actualizaciones de firmas por hora.

Cifrado de disco completo: proporciona el mayor nivel de seguridad de los datos, para los datos almacenados en equipos portátiles y de escritorio a través de una combinación de autenticación previa al arranque y los algoritmos de cifrado fuerte.

Media Encryption: Protege los datos sensibles de las empresas y contra el malware entrante mediante la encriptación de medios removibles como dispositivos de almacenamiento USB, CDs y DVDs y la actividad de control (lectura, escritura y ejecución) en los puertos y dispositivos.

Network Access Control (NAC): Aplica una política integral de control de acceso a la red y garantiza que cada extremo está al día con los últimos antivirus, parches críticos, service packs y aplicaciones como navegadores y agentes de VPN.

Administración Centralizada: La gestión de Check Point Endpoint Security ofrece la configuración de la consola central, la administración de políticas, informes y análisis de seguridad de punto final.

Checkpoint Endpoint.

Endpoint Security, es un agente para la seguridad del puesto de trabajo que fusiona firewall, control de acceso de red (NAC), control de programa, antivirus, anti-spyware, protección del dato y acceso remoto a la red corporativa. La nueva solución protege los PCs, sin necesidad de implantar y gestionar múltiples agentes.

Checkpoint Endpoint Security es el primer y único agente que combina todos los componentes críticos para la seguridad total, ofrece mayores niveles de seguridad mientras que proporciona un manejo transparente al usuario final, asegura el punto final contra el creciente número de amenazas basadas en web, abre todos los sistemas de seguridad en el PC con un inicio de sesión único y simple, es además agente para incluir los datos de seguridad y VPN de acceso remoto y antivirus.

Provee de seguridad al punto final con más de 10 funciones de seguridad integradas, incluyendo la seguridad del navegador único, acceso remoto VPN y cifrado de disco completo y con una sola instalación, inicio de sesión único, gestión simplificada y operación con un solo agente, centralizada con criterios de valoración integrada y capacidades de seguridad de red, incluidos los integrados en VPN de acceso remoto, Network Access Control (NAC), correlación de eventos opcionales y presentación de informes.

La arquitectura dinámica del Software Blade ofrece soluciones seguras, flexibles y sencillas que pueden ser completamente adaptables para cumplir con las necesidades de seguridad específicas de cualquier organización o ámbito. Las soluciones premiadas de ZoneAlarm de Check Point protegen a millones de consumidores de hackers, spyware y robo de identidad.

3.1.5 Beneficios

- Exhaustiva seguridad de Endpoint con más de 10 funciones de seguridad integradas, incluyendo seguridad de navegador única, acceso remoto VPN, encriptación completa de discos y más.
- Mejor desempeño con escaneo anti-malware más veloz.
- Es transparente al usuario final, con instalación, inicio de sesión y actualización sencilla.
- Administración y operación simplificada con manejo centralizado.
- Funciones integradas de endpoint y seguridad de redes incluyendo acceso remoto VPN, Control de acceso a redes y correlación de eventos y reportes opcionales.

Endpoint nos Proporciona:

- Un único agente de software.
- Una única consola de gestión.
- Una única instalación, controlada por un único administrador.

3.1.6 Principales características de Endpoint Security de CheckPoint:

- Firewall/NAC/Programa de Control – Protege los sistemas endpoint al restringir tanto el tráfico que entra como el que sale, asegurándose de que este tráfico se encuentra en un estado seguro antes de permitir el acceso a la red.

Automáticamente aplica las políticas de seguridad sobre qué programas se permite que corran en los PCs.

- Antivirus/Anti-spyware – Detecta y elimina virus, spyware y otro tipo de malware mediante una combinación de firmas, bloqueadores de comportamiento, y análisis heurístico.
- Acceso Remoto - Da a los usuarios finales un acceso remoto, encriptando y autenticando los datos transmitidos.
- Protección del Dato – Proporciona protección del dato en portátiles, PCs y medios removibles con una fusión de encriptación total del disco, control de acceso, gestión de puertos y encriptación durante las sesiones de acceso remoto entre el puesto de trabajo y la red corporativa.

Características y opciones de seguridad del programa.

- Para usuarios en red, puede cifrar los archivos y subdirectorios del servidor utilizando SafeLan para poder almacenar y compartir archivos cifrados y en forma segura. Soporta NTFS, Novell y otros sistemas de redes. El cifrado se realiza usando un algoritmo AES en modo CBC con claves de 256 bits.
- Encriptar unidades removibles, por ejemplo pendrives, memorias USB, discos extraíbles. El usuario puede elegir si va a utilizar los medios extraíbles en formato encriptado.
- Administración de autenticación: El ID de usuario y la contraseña deben ser introducidos antes de que el sistema operativo se inicie. Si el disco duro está cifrado, la clave de cifrado sólo estará disponible cuando el usuario se ha autenticado correctamente en Windows. El sistema operativo de ID de usuario, contraseña y dominio son encriptados y almacenados, para que los usuarios puedan ser automáticamente registrados y puedan acceder correctamente.
- Cifrado del disco duro completo incluyendo todos los sectores del disco.

3.1.7 Seguridad de accesos

Endpoint Security

Como los empleados cada vez más móviles, sofisticadas soluciones VPN tienen las políticas de seguridad adicional. Obligación de garantizar el acceso a los recursos y proteger los escritorios remotos. Endpoint Security se extiende a la VPN segura para los usuarios remotos, el acceso a la red y la comunicación. Se encripta y autentifica datos para realizar conexiones completamente seguras.

Endpoint Security Secure Access

Protección completa de acceso remoto. CheckPoint Endpoint Security Secure Access combina las capacidades de líder en el mercado de Endpoint Security y entregar lo más avanzados de acceso remoto, protección de punto final, y la aplicación de políticas de acceso a la red en una solución. Múltiples garantías en un solo paquete que sea más fácil de implementar y gestionar, a partir de la misma plataforma unificada de gestión de la seguridad como de otros productos de CheckPoint.

Endpoint Security Secure Access está respaldada por Servicios SmartDefense, que protejan contra las nuevas amenazas, proporcionando en tiempo real defensa de los avisos de cambios y configuración.

3.1.8 Seguridad en Desktop

Endpoint Security Full Disk Encryption

Es una herramienta de encripción de datos tanto para desktop como para portátiles. Endpoint Security Full Disk Encrytion brinda soluciones de seguridad que mediante Check Point han demostrado en las empresas y agencias gubernamentales de todo el mundo, la entrega de los más altos niveles de seguridad de datos mediante el suministro de una fuerte herramienta para el cifrado completo del disco, esta solución

diseñada para portátiles, permite efectuar un control de acceso a los datos. Este software funciona con Linux o Windows, y ofrece la gestión centralizada de la seguridad de los datos.

Las funciones como tener acceso a correo electrónico sólo hacen más difícil hacer un seguimiento de la información. Pointsec móvil da la seguridad de los productos CheckPoint, y brindan una poderosa herramienta de encriptación de los datos para estos equipos, con los cuales la conexión se hace de forma segura a la empresa. Pointsec Mobile asegura completamente los datos en los dispositivos que ejecutan Symbian, Pocket PC, Windows Mobile Smartphone y Palm, así como de sus correspondientes tarjetas de memoria. Este proceso sencillo para proteger los datos empresariales en los dispositivos móviles, da seguridad sin reducir la velocidad. El cifrado se realiza automáticamente sin intervención del usuario, lo que proporciona amplio grado de seguridad.

PointSec Protector

La presencia de puertos USB en las computadoras portátiles y las computadoras personales ha impulsado la posibilidad de que se produzcan fugas de datos graves en su empresa. Estos puertos permiten a los usuarios extraer cualquier tipo de dato en cualquier instante haciendo a los ordenadores vulnerables. La capacidad para copiar los datos de la empresa provoca una brecha de seguridad, que probablemente no se tiene manera de hacer un seguimiento e incluso si se lo hace no se podrá detectar de donde fueron extraídos los datos. Pointsec Protector es una herramienta de cifrado de Check Point que evita la copia no autorizada de datos a través de dispositivos USB o de dispositivos móviles permitiendo así una seguridad en los datos, también proporciona una auditoria completa que mediante informes muestra el movimiento de los datos hacia cualquier dispositivo móvil o fuente de almacenamiento.

*3.1.9 **Checkpoint propone Software Blade como arquitectura de seguridad**.*

En la nueva arquitectura de seguridad de CheckPoint, Software Blade, cada función de seguridad, cortafuegos, VPN, detección de intrusos, corre como una pieza separada dentro del mismo entorno de software, y sobre una diversidad de sistemas operativos, incluido el de VMware.

Los gestores de seguridad podrán correr tantas funcionalidades como requieran en distintos “contenedores”, pero el sistema en su conjunto será gestionable de forma integrada y consistente utilizando un mismo conjunto de políticas. Para conseguir algo parecido, hoy la única alternativa es correr cada función como una gateway de seguridad separada físicamente, o, en despliegues de menor gama, utilizar las soluciones “todo en uno”, caracterizadas por correr múltiples capacidades de seguridad en un único producto, pero que plantean problemas de escalabilidad.

Los responsables de CheckPoint, que explican la nueva arquitectura como una propuesta basada en el concepto de “blade”, ya popular en el mundo de los servidores, aseguran que Software Blade pretende controlar la creciente complejidad asociada a tener que correr cada vez más funciones de seguridad como elementos separados. Esta situación obliga, según CheckPoint, a duplicar políticas de protección y hace la gestión del conjunto tan difícil que a menudo crea por sí misma riesgos para la seguridad.

Un único entorno lógico

Por el contrario, la arquitectura de CheckPoint, que concentra el entorno en uno o más blades de seguridad, genera un único entorno lógico de seguridad que sustituye la noción de gateways físicos independientes.

Software Blade soporta configuraciones de hasta 20 blades, que permitirán ampliar las comunes capacidades de seguridad basada en firewall con módulos como seguridad web, filtrado URL, antivirus, antispam, aceleración de red, clustering y VoIP. Además, la arquitectura podrá escalarse mediante la adición de nuevos “núcleos” para satisfacer las demandas de rendimiento

La nueva solución de la compañía permite identificar, aceptar, bloquear o limitar el uso de miles de aplicaciones Web en la empresa. Con esta nueva solución, el mercado encontrará la combinación de tres factores claves en un único producto: tecnología exclusiva, participación del usuario y amplio control de las aplicaciones.

El nuevo Blade integra la tecnología CheckPoint UserCheck que involucra a los empleados en la toma de decisiones y permite a los administradores de TI adaptar las políticas de uso de la aplicación a sus necesidades empresariales específicas.

Según el reciente estudio llevado a cabo por CheckPoint y Ponemom, la mayoría de los encuestados consideran que los trabajadores son esenciales a la hora de mitigar los riesgos de seguridad procedentes de las aplicaciones de internet. Integrado en el software Application Identity de CheckPoint, la tecnología UserCheck alerta a los usuarios de los posibles riesgos que se pueden originar en las aplicaciones, y pregunta a los trabajadores si el motivo de acceso es para uso comercial o personal. Finalmente, la solución educa a los usuarios sobre los riesgos de aplicación y las políticas corporativas, al tiempo que provee a los administradores TI de las principales tendencias.

Basado en la arquitectura CheckPoint Software Blade, Application Identity puede activarse con un solo clic en cualquier gateway de seguridad de CheckPoint, incluyendo UTM-1, Power-1, IP Appliances, IAS Appliances y servidores abiertos. El nuevo blade también se administra desde una única consola de gestión de la seguridad, y los administradores de TI pueden monitorear y controlar el uso de aplicaciones basadas en la identidad, el usuario o grupo, la frecuencia y nivel de riesgo con un análisis unificado.

Como herramienta clave para crear una seguridad 3D verdadera, la arquitectura Software Blade de CheckPoint permite a las empresas hacer cumplir las políticas de Seguridad mientras ayuda a formar a los usuarios en esas políticas. La arquitectura Software Blade es la primera y única arquitectura de seguridad que suministra seguridad integral, flexible, y administrable a empresas de cualquier tamaño. Es más, a medida que aparecen nuevas amenazas la arquitectura Software Blade de CheckPoint amplía rápidamente y de forma flexible sus servicios de seguridad bajo demanda sin la adición de nuevo hardware o complejidad de administración. Las soluciones se gestionan centralmente a través de una única consola que reduce la complejidad y la sobrecarga operativa. La protección multicapa es fundamental hoy en día para combatir las amenazas dinámicas como bots, troyanos, y amenazas persistentes avanzadas.

3.2 Endpoint Security Client y Vision General de Acceso Remoto

3.2.1 Endpoint Security Client y Acceso Remoto

Las computadoras portátiles que viajan fuera de la red de Xstrata están asegurados adicionalmente usando Checkpoint Endpoint Security. Se permite entonces el acceso remoto a la red mediante el uso de un cliente VPN que está autenticado en el servidor de seguridad utilizando RSA SecurID.

3.2.2 *Acceso Remoto*

El acceso remoto proporcionará a los usuarios de Xstrata con acceso a correo electrónico y otros sistemas basados en LAN. Este servicio se basa en una conexión a Internet a través de la cual se crea una red privada virtual (VPN). Este VPN proporciona

un vínculo seguro en la red y garantiza que todos los datos que viajan a través de la VPN se cifran utilizando el estándar de la industria AES 256.

El cliente de Checkpoint tiene una funcionalidad adicional, ya que proporciona el ordenador con un servidor de seguridad local. Esto limita servidor de seguridad local conexiones con el ordenador a través de Internet y, como tal protege tanto al equipo local y la red corporativa Xstrata.

Los usuarios deberán utilizar 2 autenticaciones de dos factores con el fin de conectarse a la VPN. (Ver diagrama en figura4) La VPN permitirá al usuario acceder a sus mensajes de correo electrónico y otros servicios como si estuvieran en la oficina.

El siguiente diagrama muestra la Solución VPN y conexión VPN.

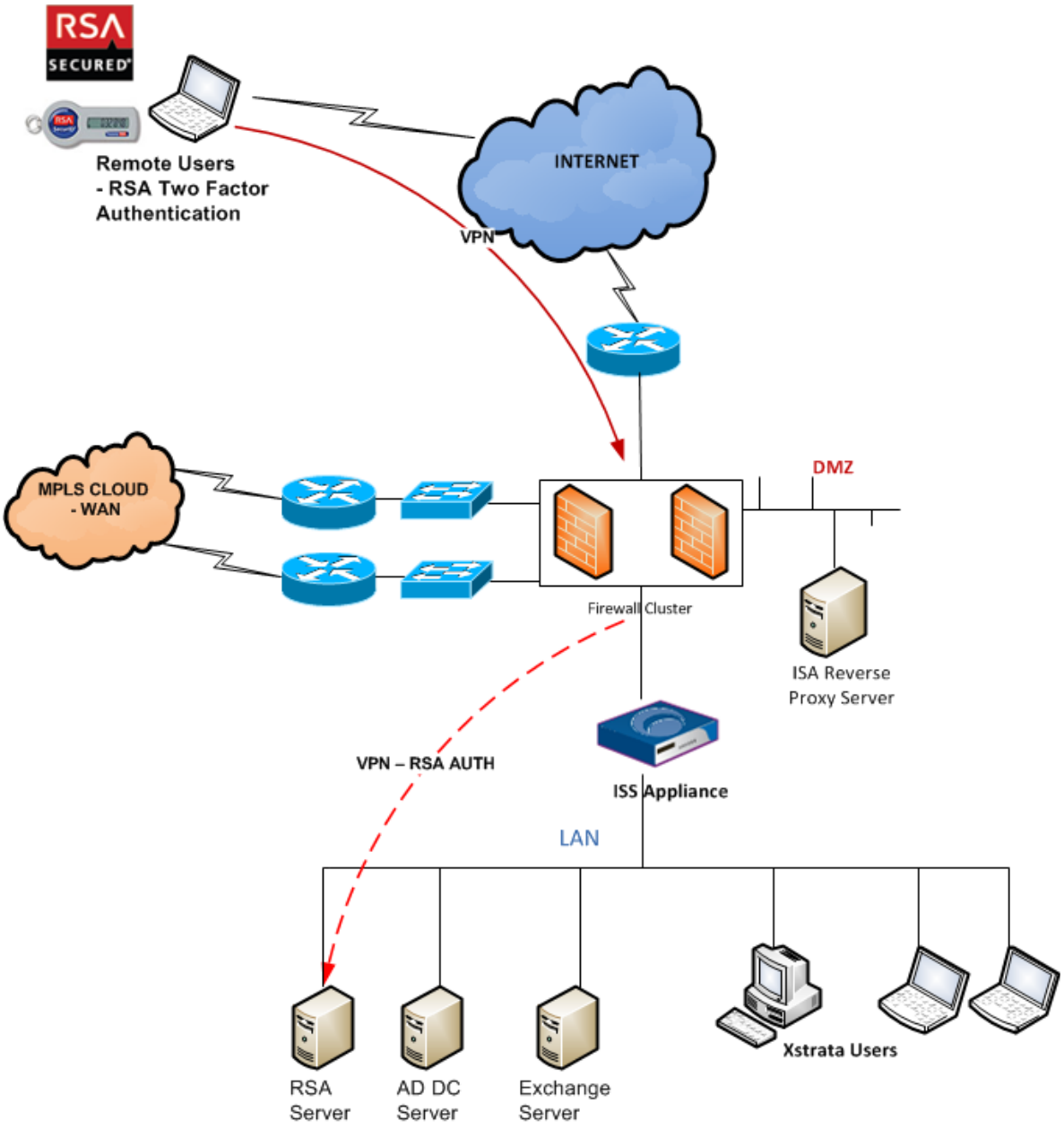


Figura 4: Diagrama de una conexión VPN

3.3 Topología de Acceso Remoto

3.3.1 RSA SecurID

RSA otorga a los usuarios acceso a un servicio después de que se hayan introducido correctamente sus dos factores de identificación, esto forma parte de su número de identificación personal (PIN) y el código único generado aleatoriamente, el acceso desde un token SecurID asignado.

El número PIN de usuario es constante, mientras que el código de acceso cambia cada 60 segundos. Después de que el usuario ha sido autenticado, se permite el acceso a los servicios requeridos, ya sea una conexión VPN o una sesión de Outlook Web Access. Si el usuario no puede introducir su número de PIN con éxito después de tres intentos consecutivos, el token se desactiva automáticamente. El usuario debe ponerse en contacto con su equipo local de TI que son responsables de gestionar el servidor RSA.

3.3.2 CheckPoint Endpoint Protection

CheckPoint Endpoint Protection ofrece múltiples capas de seguridad para máquinas cliente Xstrata y ha recibido el mandato para la instalación en todos los portátiles propiedad de está. El cliente Endpoint proporciona las siguientes mejoras más allá de las opciones estándar del sistema operativo de Microsoft:

• Cifrado de unidad de disco duro - Encriptación total de la unidad de disco duro local
• Protección USB - Monitoreo basado en la política y el bloqueo activo de dispositivos USB configurados en los notebook de Xstrata estando conectados a la red.
• Cifrado USB - Capacidad para cifrar automáticamente los dispositivos USB externos
• Firewall Client - Máquinas detectará cuando están fuera de la red de Xstrata y pondrá

en funcionamiento automáticamente las políticas de seguridad del cortafuegos más estrictas.

• Aplicación de sensibilización - Las aplicaciones pueden ser autorizados / bloqueados depende de la ubicación actual.

• Mejora de cliente VPN - EndPoint se volverá a conectar automáticamente y volverá autenticarse de haber una interrupción temporal de la conexión a Internet

Para el despliegue dentro de Xstrata una política por defecto ha sido creado como un requisito obligatorio. Las mejoras en esta política pueden adaptarse a requerimientos específicos de cada unidad de negocio, sin embargo las opciones de seguridad de nivel de base se han configurado para incluir como mínimo:

• Cifrado de disco duro local completa con una contraseña local antes de la inicialización

• La política de cortafuegos para proteger el cliente local cuando este fuera de la WAN Xstrata

• Cliente VPN para cifrar todas las comunicaciones remotas entre el cliente y operaciones de Xstrata WAN

• Auditoría de todo el hardware externo que se utiliza y se accede desde el cliente.

3.3.3 *Acceso remoto seguro al Correo electrónico.*

Un requisito clave para la mayoría de los usuarios que viajan es darles la posibilidad de tener acceso a su correo electrónico "en movimiento". (Ver diagrama en figura 5)

Hay una serie de tecnologías aprobadas por el Grupo de IT para este propósito:

• Los teléfonos Blackberry en conjunto con un servidor BES.

• Outlook Web Access para acceso desde cualquier navegador de Internet (RSA "de dos factores" Autenticación)

• Acceso a Outlook en cualquier lugar del cliente de Outlook - RPC sobre HTTPS

Todos los servicios utilizan las comunicaciones cifradas para garantizar la

privacidad y apoyar a estos en una serie de políticas clave. Los detalles de estas políticas puede ser comparada con el llamado Sistema de Gestión de Seguridad de la Información Xstrata que contiene información detallada sobre las políticas necesarias. El acceso a OWA está disponible desde cualquier conexión a Internet, un token de RSA es obligatorio para la autenticación de Outlook Web Access con sus credenciales de usuario de dominio.

El siguiente diagrama muestra una implementación típica BES

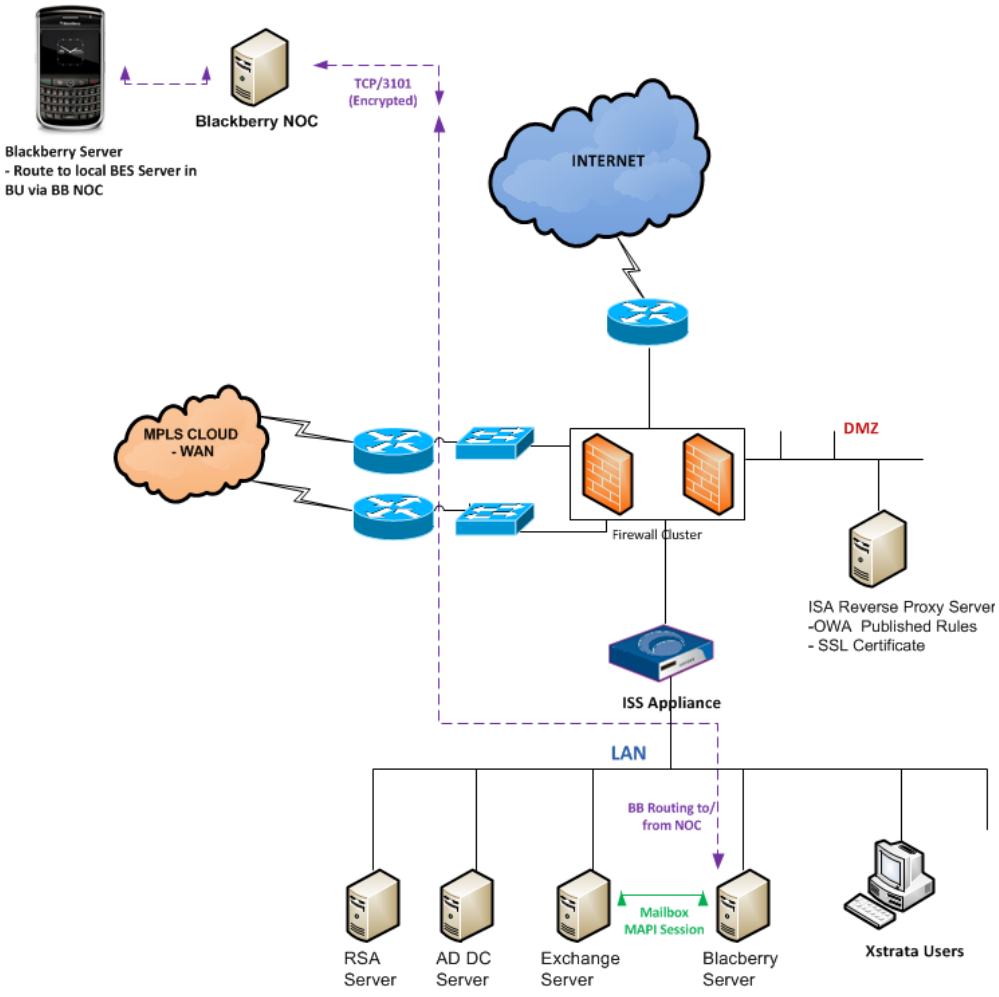


Figura 5: Implementación en el BES

3.4 Outlook Web Access y Outlook Anywhere

Además de usar un cliente de correo electrónico remoto Checkpoint VPN puede facilitarse utilizando Outlook Web Access o Microsoft Outlook en cualquier lugar. (Ver diagrama en figura 6)

Outlook Web Access utiliza un servidor Microsoft ISA para publicar el acceso a los buzones de los usuarios a través de una página web estándar.

Con el fin de acceder a su correo electrónico es necesario introducir un nombre de usuario y una contraseña válidos y su actual nombre de usuario y clave de RSA.

Cada cliente tiene que haberse configurado para el acceso durante la conexión a la red WAN Xstrata y tener copias de los certificados PKI emitidos internamente requeridos.

Con el fin de conectar a los usuarios estos necesitan una conexión abierta a Internet con acceso HTTPS. Todos los datos se cifran mediante SSL a través de Internet hacia el servidor proxy inverso ISA mediante RPC de Microsoft a través de HTTPS.

Descripción de la arquitectura OWA y Outlook en cualquier lugar.

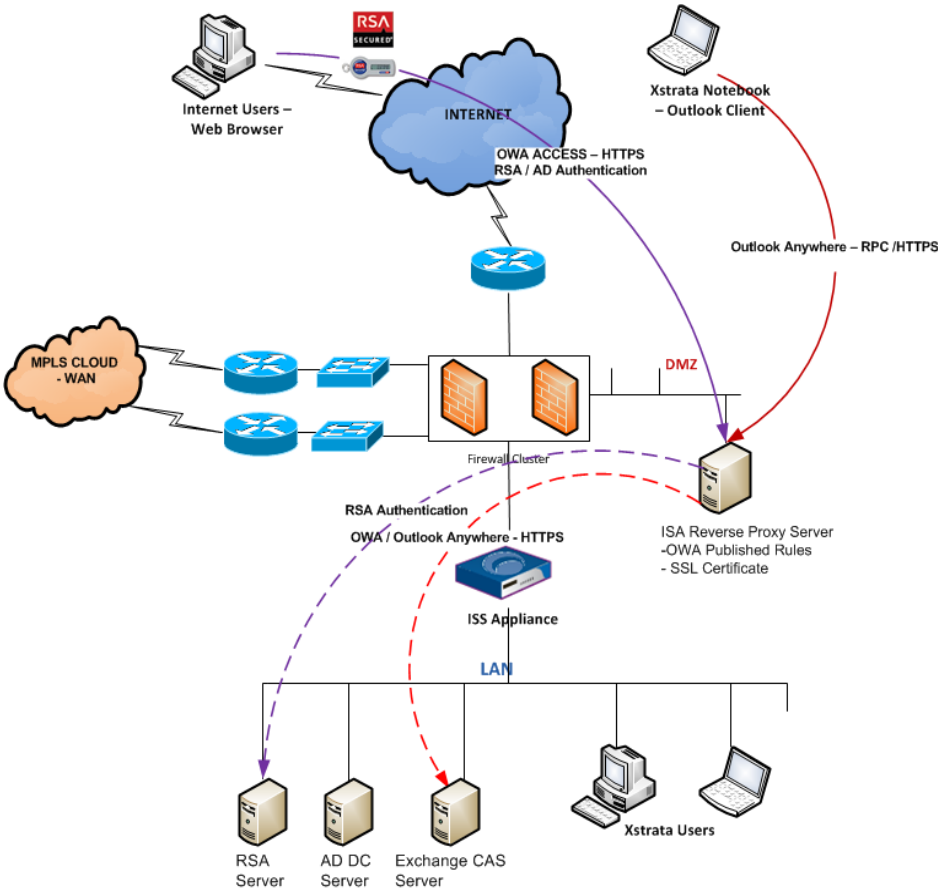


Figura 6: Esquema descriptivo de Outlook Anyware

3.5 Administración Cliente Checkpoint Endpoint Security.

3.5.1 Objetivo

Delegar e instruir al personal de Field Support en los pasos requeridos para llevar a cabo la administración del cliente Checkpoint Endpoint Security.

3.5.2 Alcance

El alcance de la administración del cliente Checkpoint Endpoint Security se basa en:

- Instalación de cliente
- Uso de cliente
- Desinstalación de cliente
- Cambio de contraseña en forma local
- Cambio de contraseña en forma remota usando WebRH
- Recuperación de información con BartPE-DMU

El cliente Checkpoint Endpoint Security cuenta con cinco funcionalidades incorporadas en una sola aplicación:

- VPN

  Acceso de forma remota a la red de Xstrata
- Firewall

  A nivel de equipo, aplicando reglas para redes externas e internas.
- Program Control - Control de programas

  Reporta todos los programas no permitidos a niveles corporativos e instalados en equipo del usuario.

- Full Disk Encryption (FDE) - Encriptación de disco duro

  Encripta todas las particiones activas del disco duro del usuario con la finalidad de que en caso de pérdida o robo de equipo, la información no pueda ser obtenida.

- Media Encryption - Encriptación de dispositivos de almacenamiento masivo

Permite encriptar los dispositivos de almacenamiento masivo que el usuario conecte al equipo.

Otras funcionalidades que entrega el nuevo cliente son:

- Monitoreo y bloqueos de dispositivos 3G – Permite bloquear MODEMS 3G en caso de estar conectado a la red corporativa de Xstrata.

- Restricciones Inalámbricas – Permite restringir completamente el acceso a una red inalámbrica en caso de estar conectado a la red corporativa de Xstrata por un medio cableado.

3.5.3 Consideraciones previas a la instalación

Instalar cliente solo en máquinas portátiles con Windows 7 Enterprise. Usuarios con Windows XP, Windws 7 Pro, entre otros deben ser migrados a W7 Enterprise.

Equipos Desktop, solo cuentan con la funcionalidad de Media Encryption, la cual es instalada a través de Altiris Deployment.

El cliente Endpoint se debe instalar con privilegios de administrador.

El perfil del usuario (C:\Usuarios) debe estar en su ubicación que viene por defecto (C:\Usuarios\nombre_logon_usuario) y no en otra unidad y/o ruta.

3.5.4 Riesgos asociados a la instalación de cliente Endpoint

A continuación se enumeran los riesgos asociados a la instalación del cliente Endpoint y como mitigarlos.

Riesgo	Probabilidad	Impacto	Efecto	Mitigación	Acciones adicionales
Falla en proceso de encriptación	Muy baja	Muy alto	Perdida de información	Recuperar información crítica desde disco duro de respaldo	Reportar suceso a soporte corporativo, indicando usuario, nombre de equipo, características del equipo
Falla en proceso de encriptación	Muy baja	Muy alto	Sistema operativo corrupto	Reinstalar SO y recuperar información critica desde disco duro de respaldo	Reportar suceso a soporte corporativo, indicando usuario, nombre de equipo, características del equipo
Problema para conectar a la red corporativa	Muy Baja	Muy Alto	Sin conectividad cableado o inalámbrica	Revisar si la opción "Network Protección" se ha iniciado correctamente. En caso de que no logre iniciar, reinstalar cliente Endpoint. Revisar que política On-Net se encuentra activada	
Mensaje que indica dispositivos 3G y Bluetooth bloqueados	Baja	Bajo	No se puede hacer uso de MODEM 3G y dispositivos Bluetooth	Reiniciar equipo para que actualice las políticas. Una vez actualizada la política no debe aparecer mensaje y dispositivo se puede usar.	En caso de que dispositivos sigan bloqueados, reportar a soporte corporativo.

3.5.5 Instalación y uso de cliente Checkpoint Endpoint Security

Para acceder al instalador del cliente, se debe ingresar a la siguiente carpeta compartida:

\\glkxxsrv700\Agent

Se debe copiar el cliente XTA-GLKXXX-EPS-0007-HFA3.sfx.exe y el archivo cliente XTA-GLKXXX-EPS-0007-HFA3.ini al equipo local donde se instalará el cliente (BNE: para usuarios de Brisbane, DBX: para usuario de Dubái y STG: para usuario de Santiago)

El proceso de instalación, se encuentra automatizado y no requiere mayor internación con el usuario, aparece mensaje que se está instalando como se muestra en figura 7.

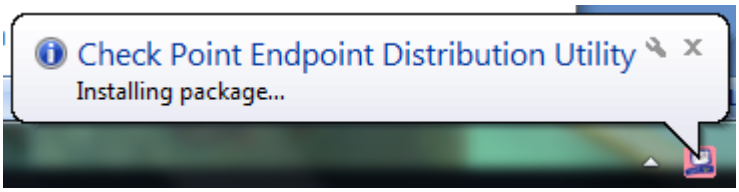


Figura: 7

Durante el proceso de instalación, etapa donde se instala el firewall, se perderá conectividad a la red por un par de segundos debido a que la aplicación activa y desactiva todas las conexiones de red del equipo. Una vez finalizada la instalación, se debe reiniciar el equipo. (Ver mensaje en Figura 8)

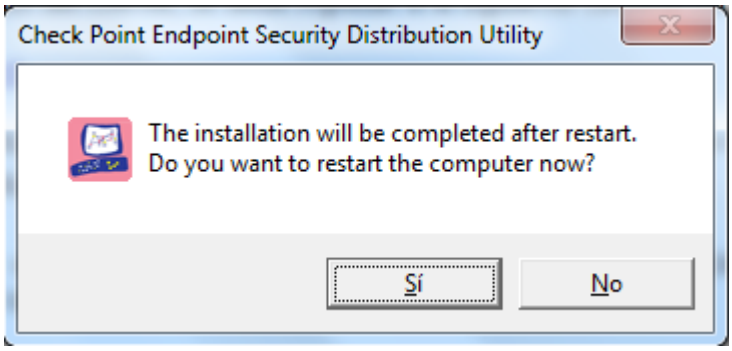


Figura: 8

Una vez reiniciado el equipo, se procederá con el proceso de pre encriptación, donde se detectaran las particiones del equipo; luego el equipo se volverá a reiniciar y

solicitará las credenciales temporales para configurar la cuenta de usuario. (Figura 9 indica campos a completar.)

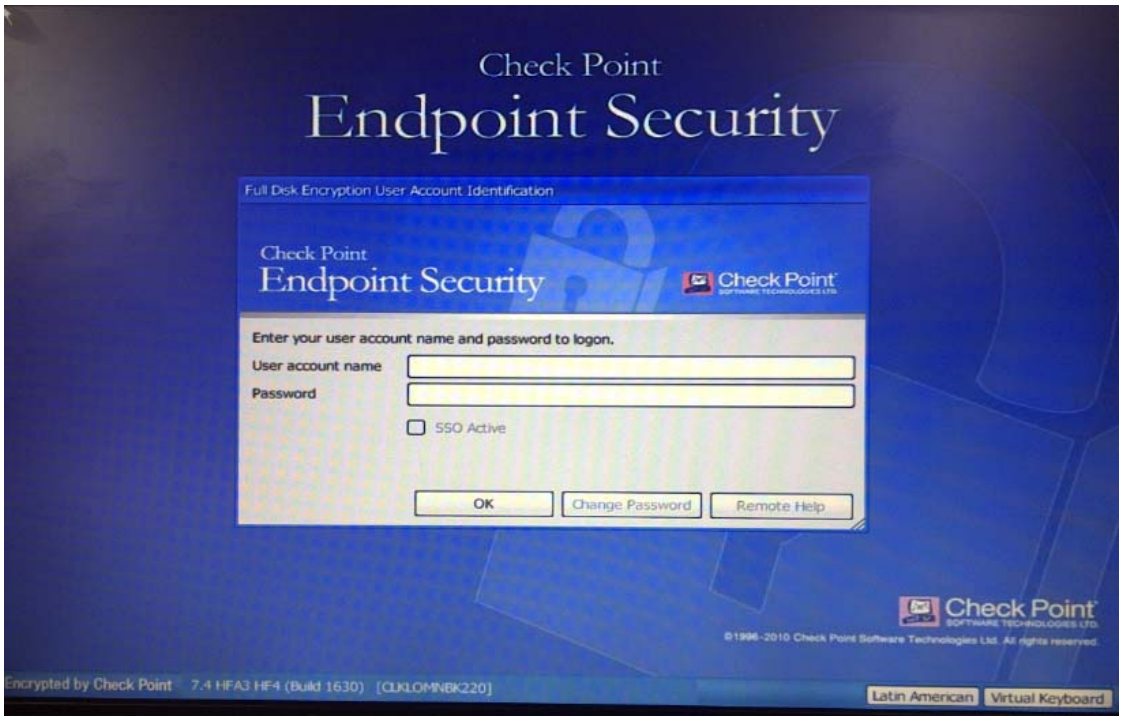


Figura 9

Llenar los campos con los siguientes datos:

User account name: XXXXXX
Password: comeonletmxxx

Una vez ingresadas las credenciales anteriores, se desplegará el siguiente mensaje (Figura 10) que hace referencia al ingreso de la cuenta del usuario.

Figura 10.

Ingresar el nombre de la cuenta de red del usuario. (Figura 11)

Figura 11.

Una vez ingresado el usuario, se debe ingresar la nueva contraseña del usuario. Aunque se puede ingresar una nueva contraseña, se recomienda ingresar la misma que el usuario tiene asignada en Active Directory. (Ver figura 12)

Figura 12.

Luego de haber ingresado las credenciales, el equipo iniciará de forma normal, donde no solicitará las credenciales de Windows para ingresar. Se desplegará el siguiente mensaje (Figura 13) que hace referencia a la habilitación de “single sing-on”. Las credenciales se almacenan encriptadas de forma local en el equipo.

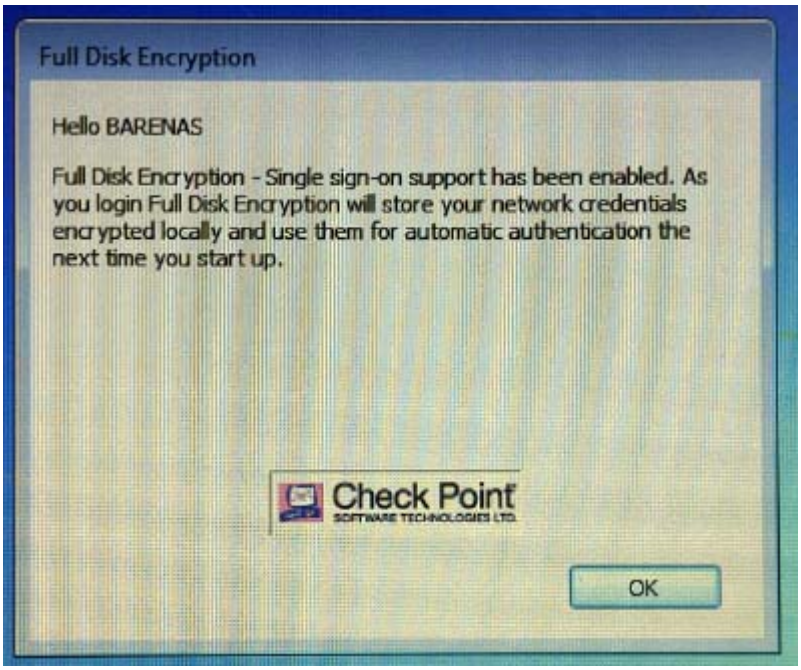


Figura 13.

Una vez terminada la instalación, se iniciaran las aplicaciones del cliente en conjunto con el proceso de encriptación de discos duros.

Para acceder a la vista general del cliente Checkpoint Endpoint Security, hacer clic con el botón secundario sobre el icono del cliente en la bandeja de sistema; (ver figura 14) luego hacer click en Settings.

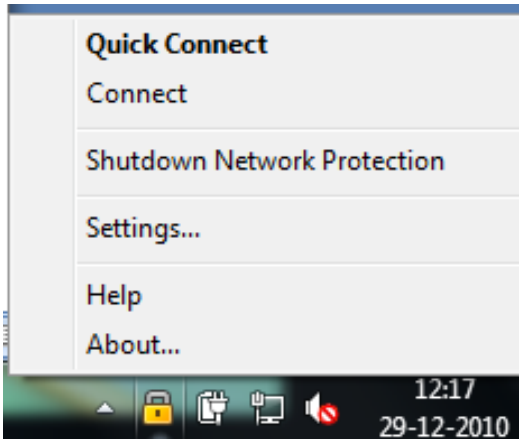


Figura 14.

En Figura 15 una vista general cliente Checkpoint Endpoint Security

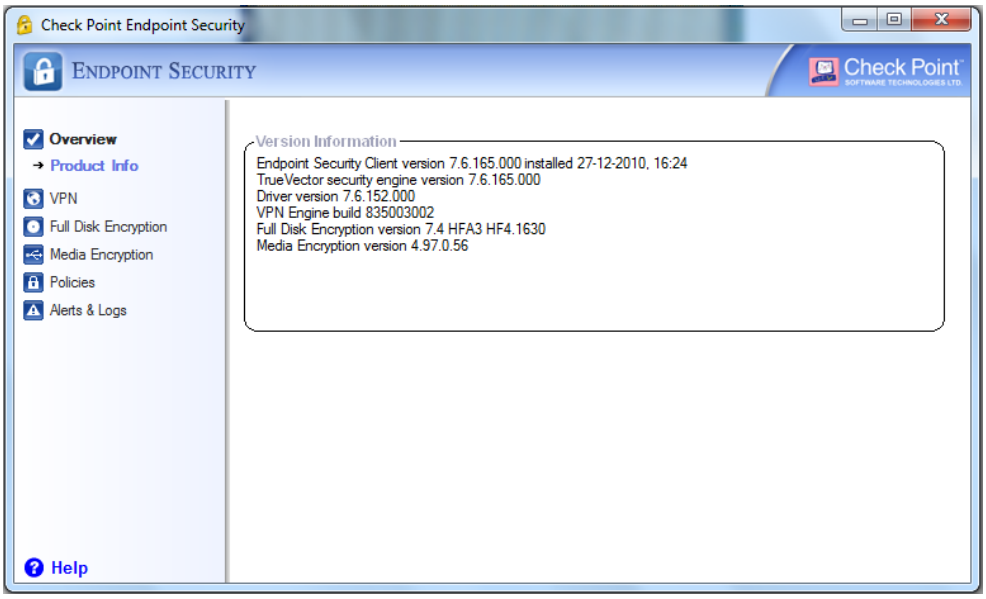


Figura 15.

Vista aplicación VPN. En “VPN Settings” se pueden revisar las configuraciones de los sitios agregados al cliente.

Para conectarse a la red de Xstrata vía VPN, seleccionar el site (GLK), ingresar “Username”, “PIN” y “Tokencode” (ver Figura 16)

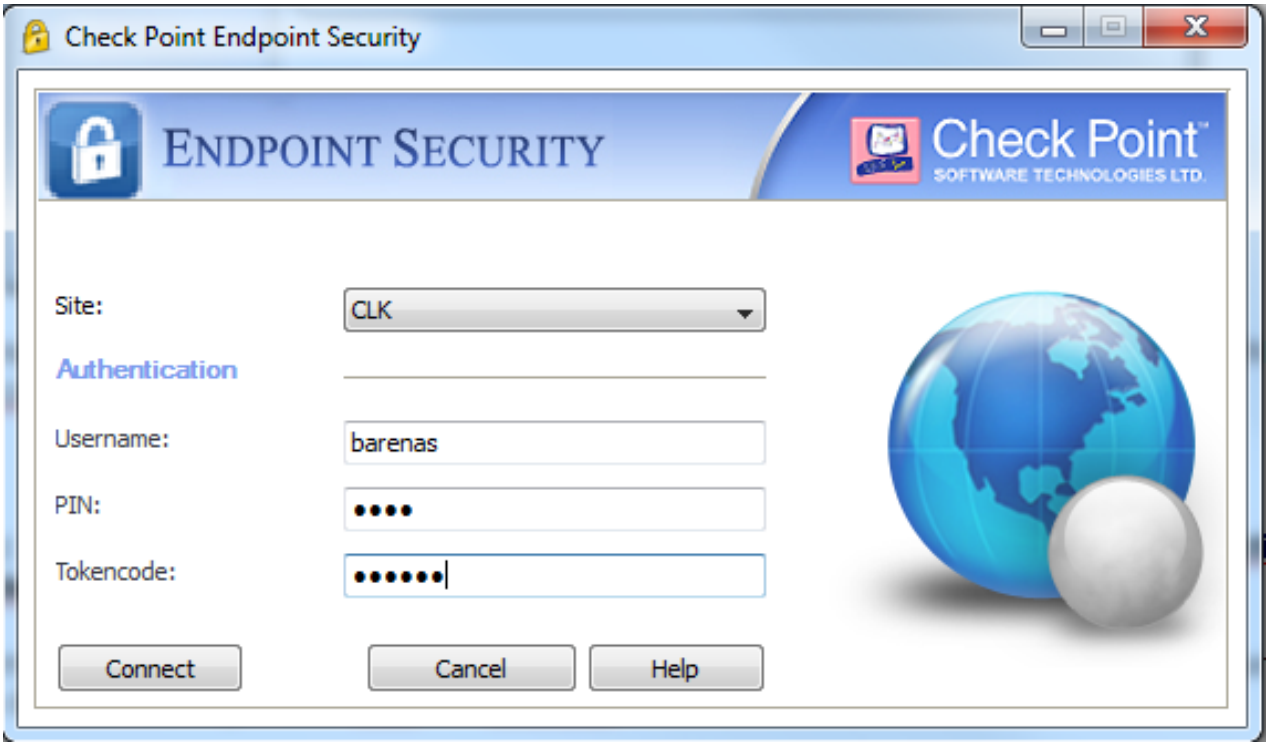


Figura 16.

Una vez realizada la conexión, se despliega la siguiente pantalla con el mensaje “Connection succeeded”. (Ver figura 17)

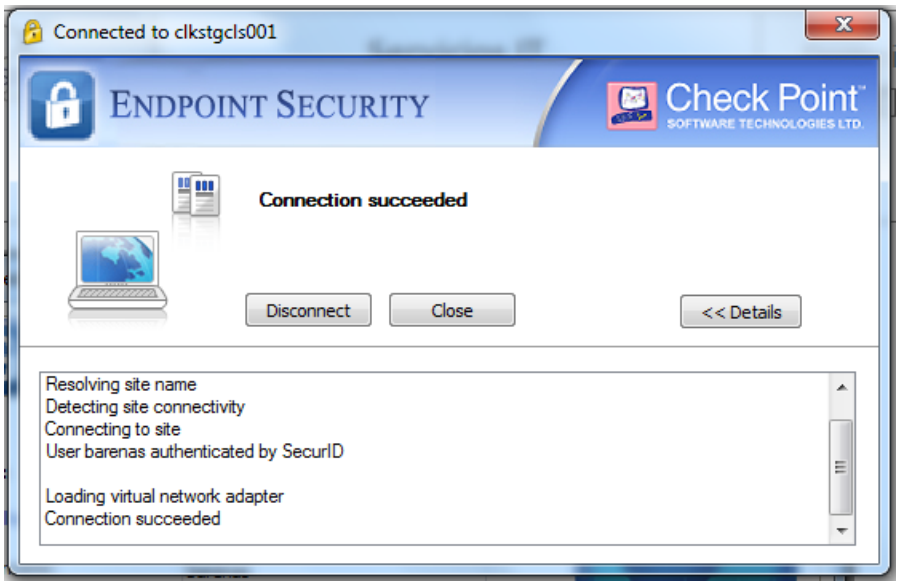


Figura 17.

Vista Full Disk Encryption (FDE – Encriptación de Disco Duro). Permite revisar si las particiones activas del disco duro se encuentran completamente encriptadas (Figura 18).Las particiones no activas, ejemplo: partición de booteo de Windows, no se encriptan.

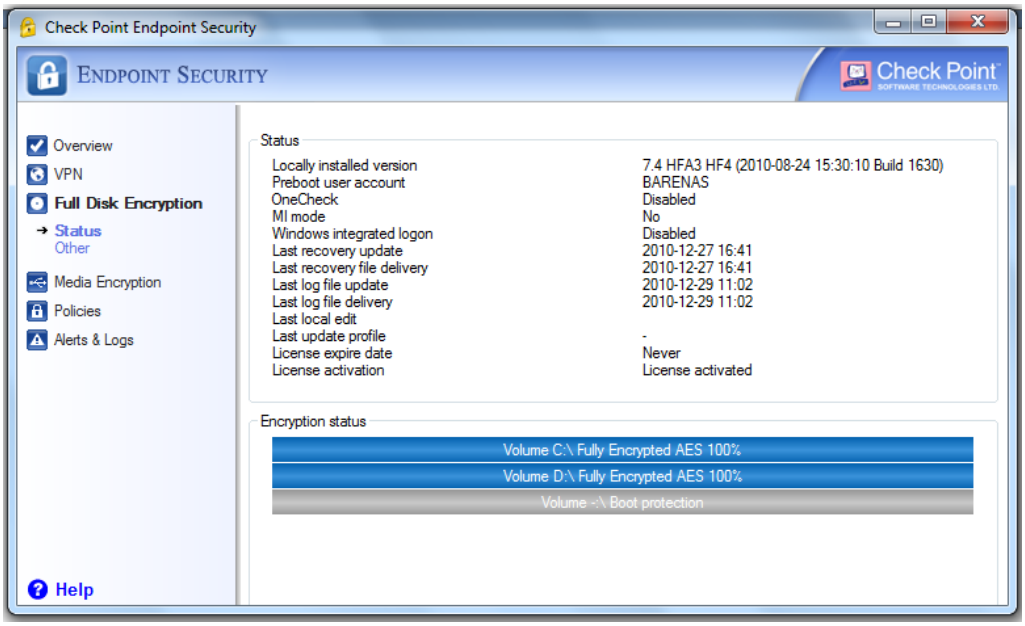


Figura 18.

Vista Media Encryption (Figura 19). Permite encriptar las unidades de almacenamiento masivo.

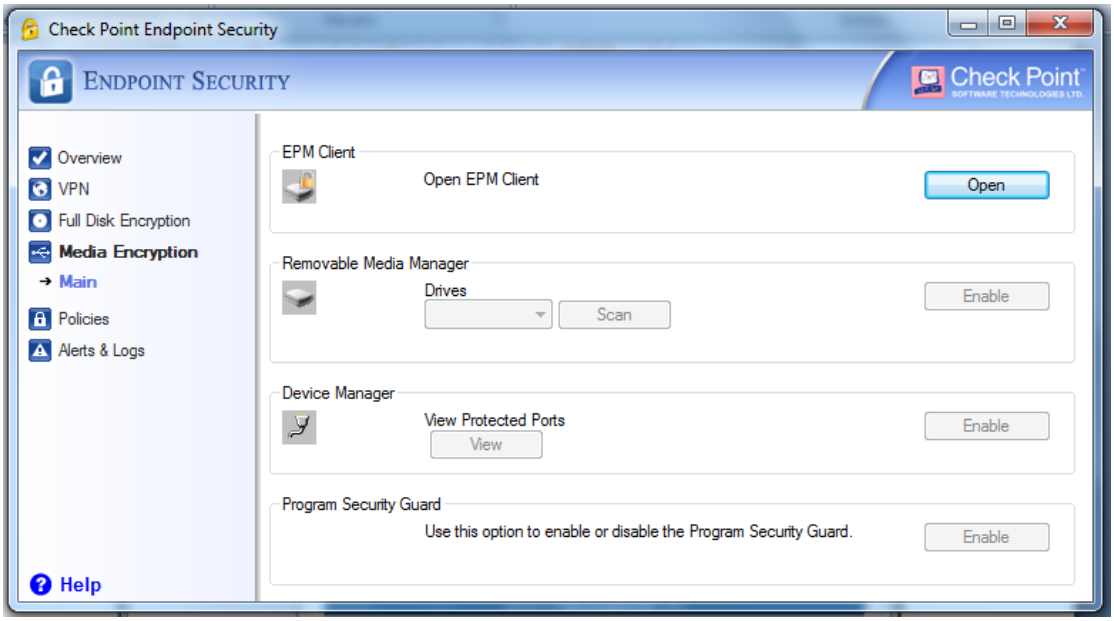


Figura 19.

Vista Policies. Permite revisar que las políticas de seguridad estén aplicadas correctamente.

- **Personal Policy**: Política por defecto que se aplica la primera vez que se ejecuta el cliente.

- **VPN_Connected_Policy:** Política que se aplica cuando usuario se conecta a red de Xstrata vía VPN.

- **Off-Net_Policy:** Política que se aplica cuando usuario está conectado fuera de la red de Xstrata.

- **On-Net_Policy:** Política que se aplica cuando usuario está conectado dentro de la red de Xstrata.

El número que se encuentra entre paréntesis al final del nombre de la política, se aprecia en figura 20, corresponde a la versión de la política. Si se generan cambios de políticas en el servidor, estos se pueden actualizar de forma manual haciendo clic en el botón "***Update Policy***". Las políticas se actualizan de forma automática cuando el usuario se conecta a la red de Xstrata.

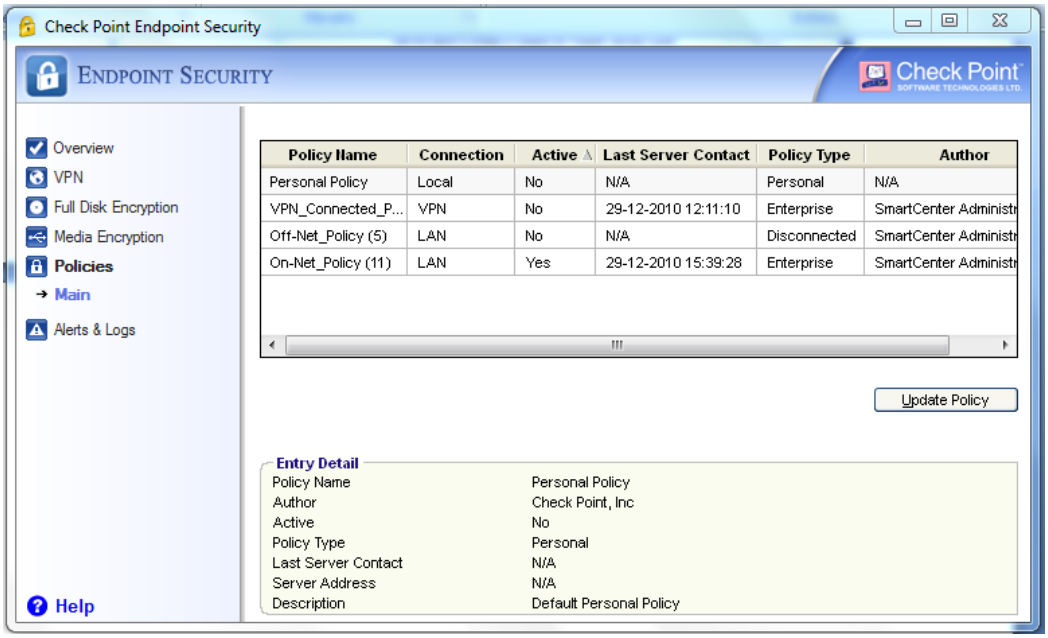


Figura 20.

Vista Alerts & Logs como se aprecia en la figura 21, Permite revisar las alertas y los logs que genera el Firewall, Program Control y Smart Defense. En caso de tener algún problema de comunicación con alguna aplicación, es recomendable revisar estos logs y en especial la columna "Action Taken", donde se indica si se permite ("Allowed") o se bloquea el trafico ("Deny").

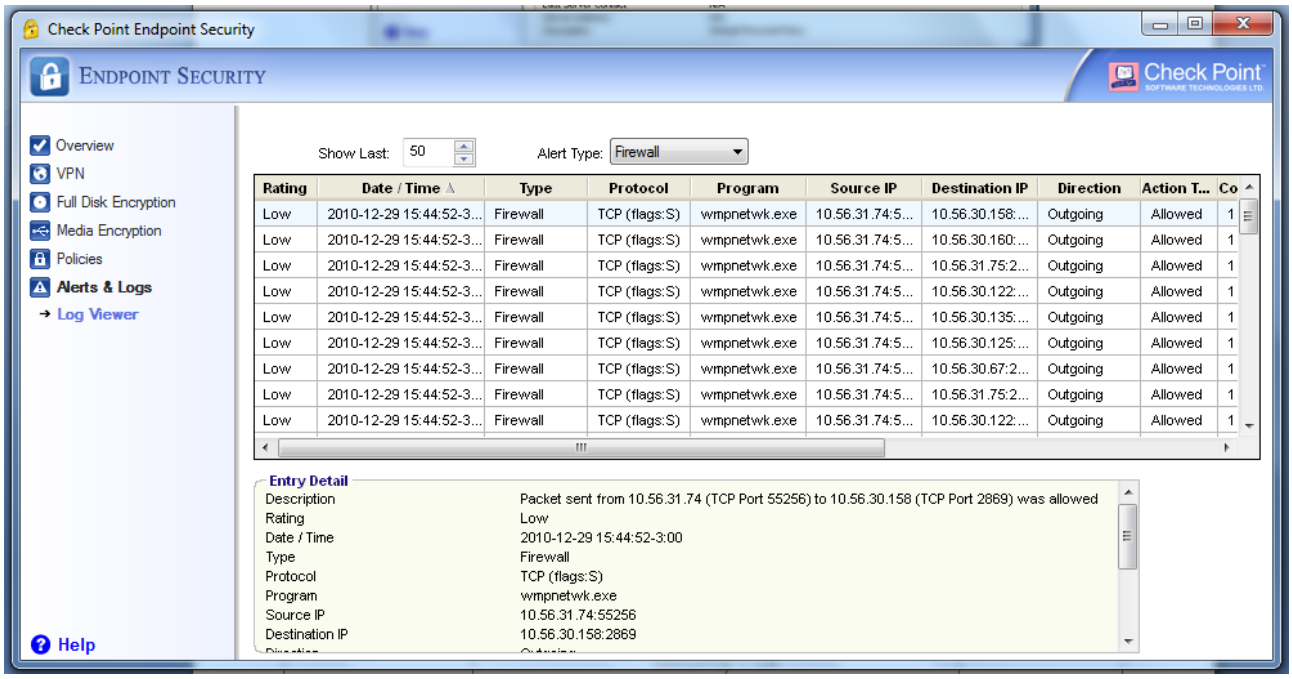


Figura 21.

IMPORTANTE: En caso de que el usuario cambie la contraseña, éste recibirá un mensaje indicando de que la contraseña ha sido encriptada y almacenada en forma local. Figura 22)

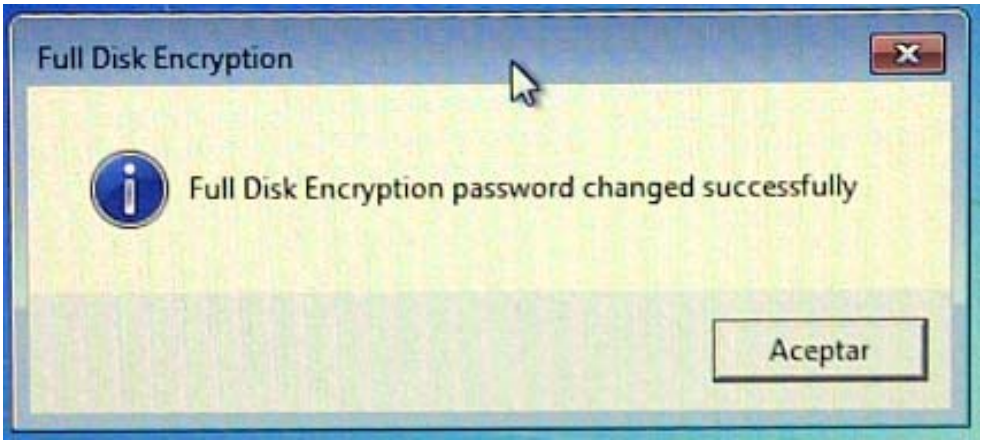


Figura 22.

Desinstalación de cliente Checkpoint Endpoint Security

Los programas a desinstalar son:

- Checkpoint Endpoint Connect se desinstala de forma normal hacienda uso de la siguiente contraseña:
  G1K#ndP0***

- Checkpoint Endpoint Security – Full Disk Encryption, solicitará dos usuarios para desinstalar. IMPORTANTE: Al desinstalar Full Disk Encryption, se desencriptarán todas las particiones del disco duro que fueron encriptadas; esto permite obtener la información sacando el disco duro y conectarlo a otro computador en caso de que se requiera.

User account name: RALPH
Password: Ch1efWxxxxxxxx!

User account name: MOE
Password: M0eTheB*****!**

Se seleccionan todas las particiones. (Ver figura 23)

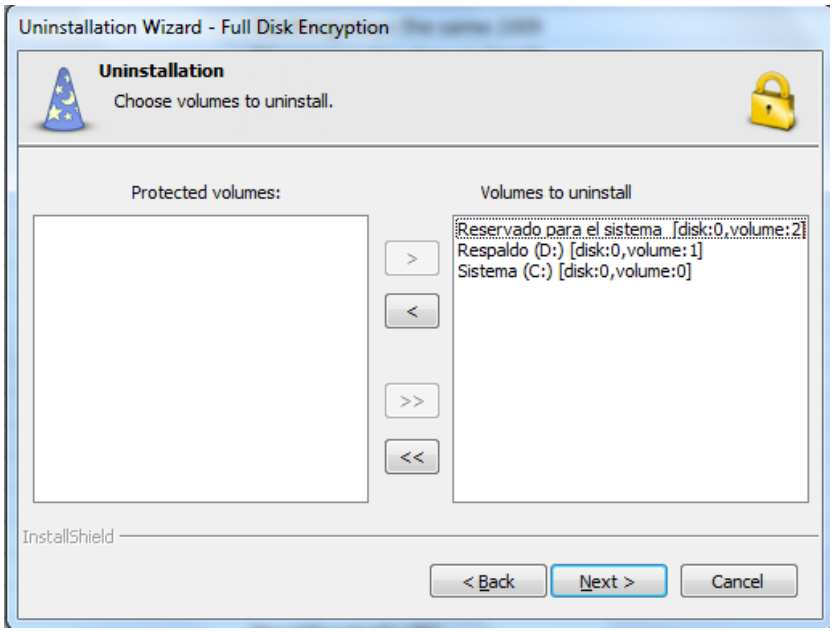


Figura 23.

Luego se muestra un resumen de la desinstalación de Full Disk Encription, como se muestra en la figura 24.

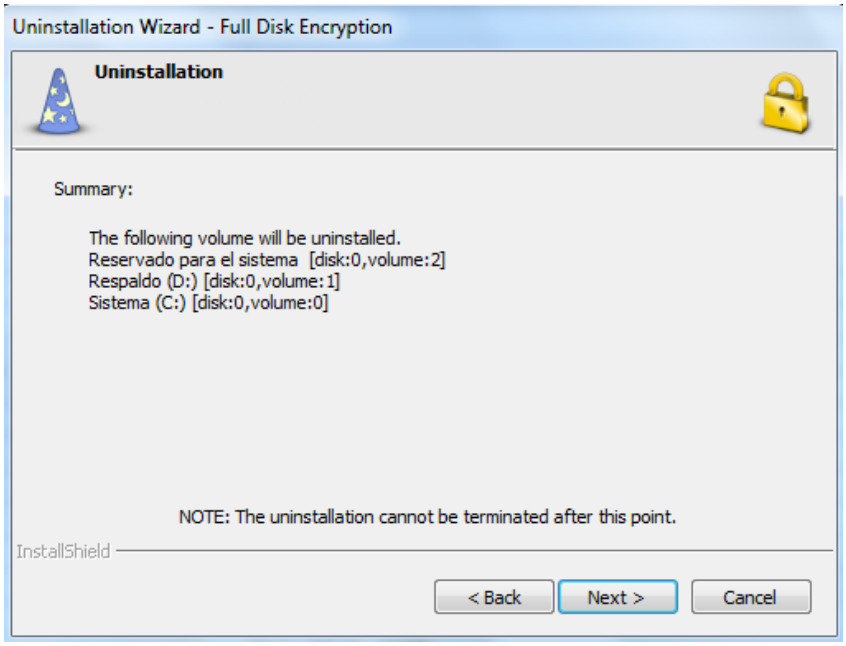


Figura 24.

Se debe reiniciar el equipo para completar la desinstalación. (Figura 25)

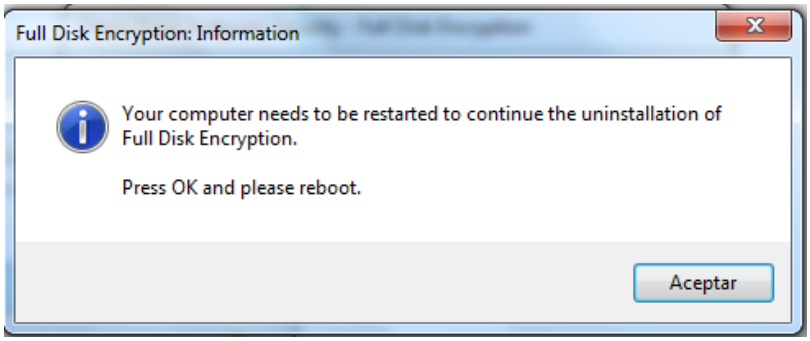


Figura 25.

Una vez que el equipo reinicie, el proceso tomará varias horas en desencriptar, el avance lo va indicando como se muestra en la figura 26.El equipo se puede apagar, suspender pero no hibernar en esta etapa.

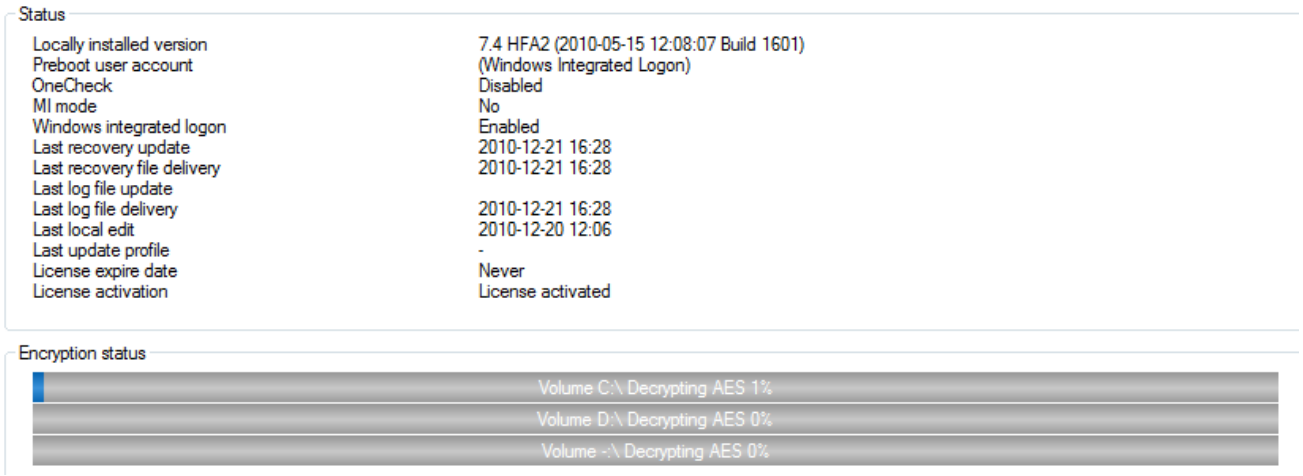


Figura 26.

3.5.6 Reseteo de password en forma local

En caso de que un usuario bloquee su cuenta de Endpoint, esta se puede desbloquear en forma remota. En caso de que no sea posible el desbloqueo en esta forma, se puede realizar un reseteo de password en forma local.

En caso de que el usuario se encuentre fuera de la oficina, se puede asistir entregando la cuenta y contraseñas de Helpdesk. Dicha cuenta y contraseña no permite modificar opciones, pero si iniciar el equipo:

User account name:	KERMIT
Password:	Mupp3tSh0wTo*****
User account name:	GONZO
Password:	M1ssPiggy19****

Para resetear una cuenta y password en forma local, primero se debe ingresar desde el botón de Inicio de Windows – Todos Los Programas – Checkpoint – Endpoint Security – Management Console. (Ver figura 27).

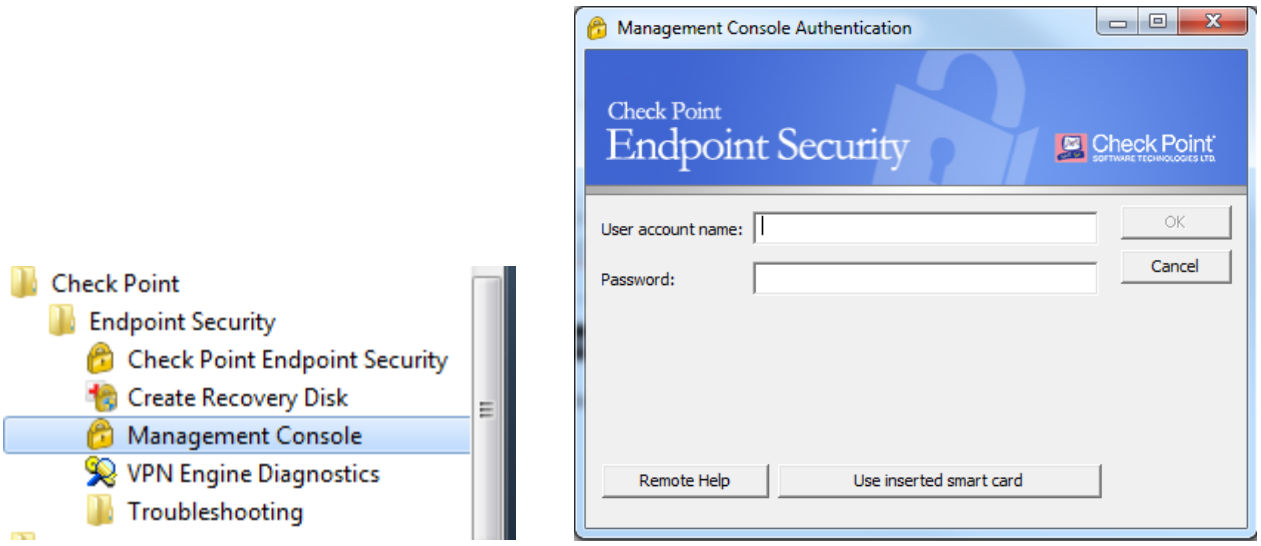


Figura 27.

Luego ingresamos con alguna de las siguientes contraseñas (estas contraseñas no pueden ser entregadas a los usuarios):

User account name:	RALPH
Password:	Ch1efW1ggamsS***
User account name:	MOE
Password:	M0eTheBart3nd***

Ingresadas las credenciales se mostrara la pantalla indicada en la figura 28.

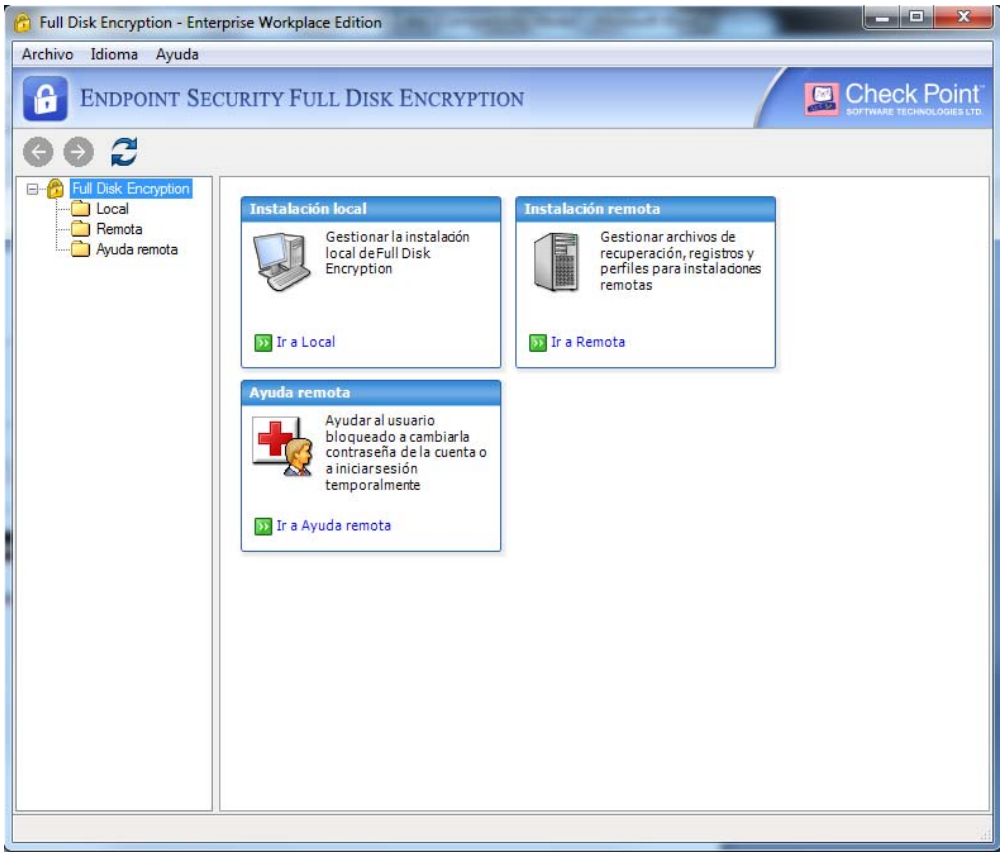


Figura 28.

Luego se debe ingresar a la carpeta “Local” (panel izquierdo) y luego a “Editar Configuración” (panel derecho). (Ver figura 29)

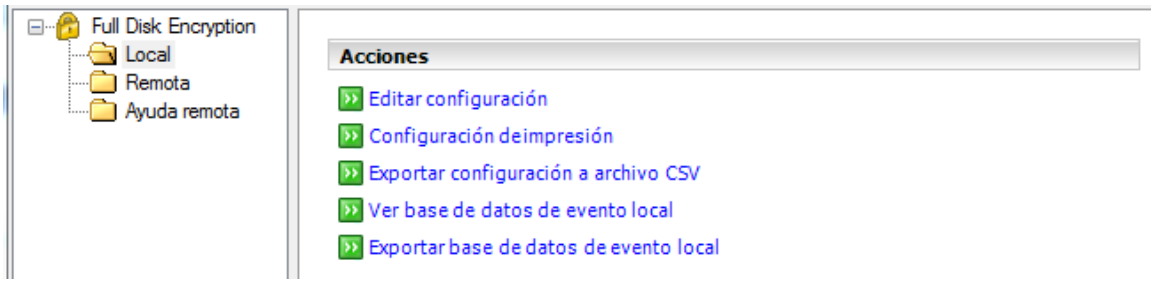


Figura 29.

Luego de haber ingresado a la opción “Editar configuración”, no dirigimos a Grupos (panel izquierdo) - “PBA-Group-User” – “Cuentas de usuario” como muestra la figura 30.

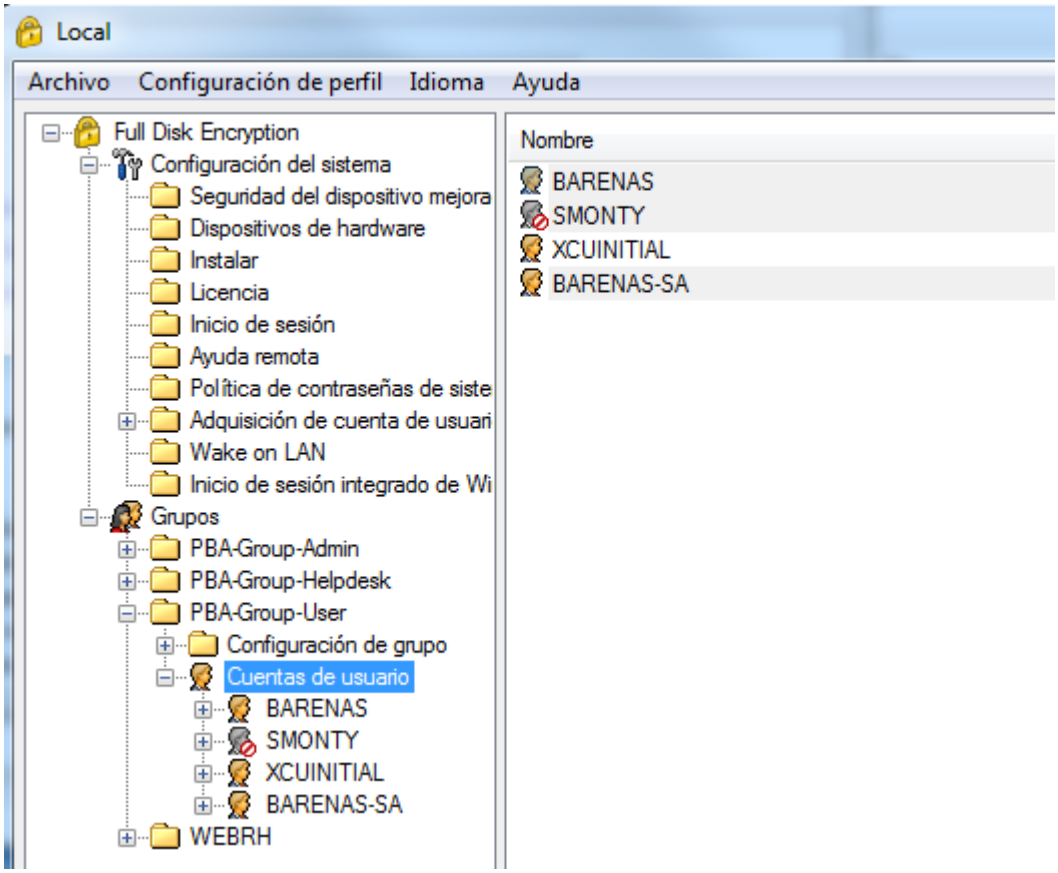


Figura 30.

En el panel derecho, podemos observar si la cuenta se encuentra bloqueada. En caso de que la cuenta se encuentre bloqueada, lo recomendable es eliminar la cuenta (Marcar para eliminar) y luego “Guardar” la configuración.

Después de guardar, se debe volver a ingresar a “Editar configuración” y crear la cuenta con el mismo nombre (AD), a través de la opción “Agregar cuenta de usuario” desde el menú de cuenta de usuario, como se puede ver en la figura 31.

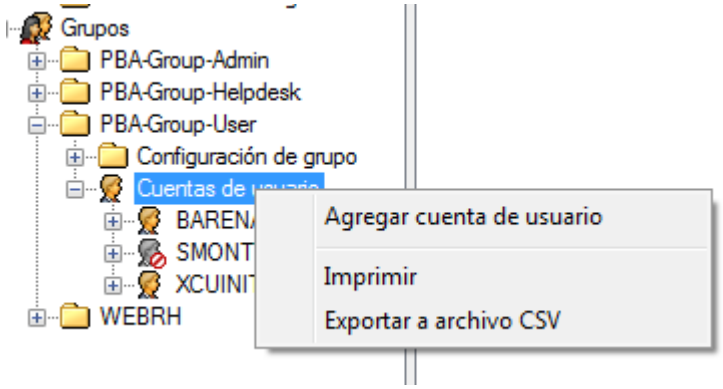


Figura 31.

Se debe ingresar el nombre de la cuenta del usuario y seleccionar “Contraseña” como método de autenticación. (Ver figura 32)

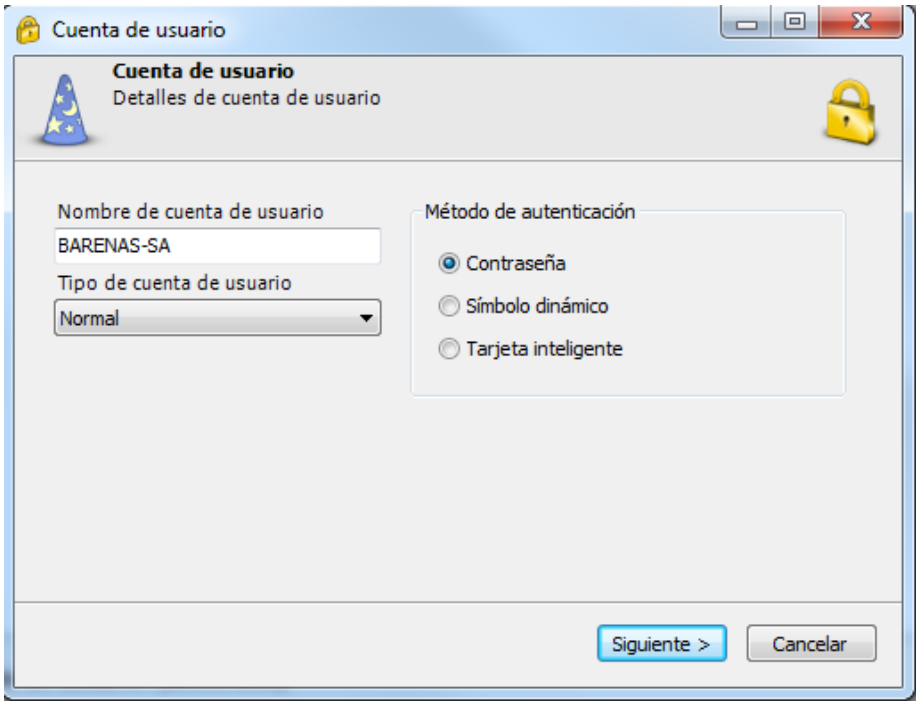


Figura 32.

Luego, se debe ingresar la misma contraseña que posee la cuenta en Active Directory de la forma indicada en la figura 33.

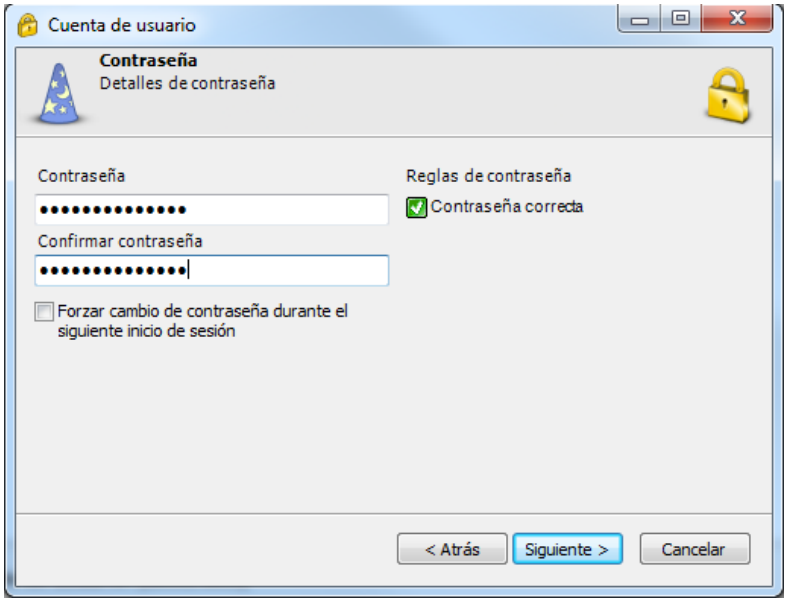


Figura 33.

Una vez finalizada la operación, se mostrará la pantalla indicada en la figura 34. Dar clic en Finalizar y Guardar.

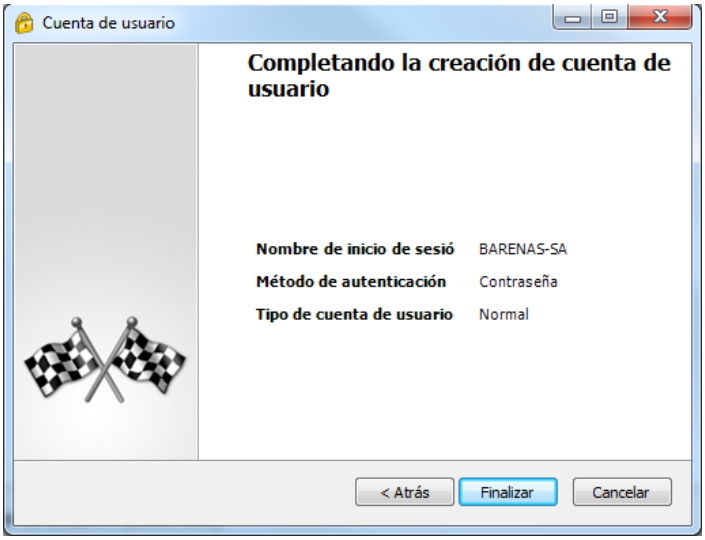


Figura 34.

3.5.7 Reseteo de password en forma remota usando WebRH

Se puede hacer desbloqueo de cuentas en forma remota para esto debemos ingresar al sitio Checkpoint Endpoint Security WebRH (Remote Help) a través de la siguiente URL:

http://10.10.10.1/webRH/

Usar las siguientes credenciales:

User name	glk\svc-glk-endpoint
Password	Xstratacusa20**

Una vez ingresado al sistema, se desplegará una interface como se muestra en la siguiente figura número 35, donde se debe seleccionar la opción “Remote Help” (lado izquierdo):

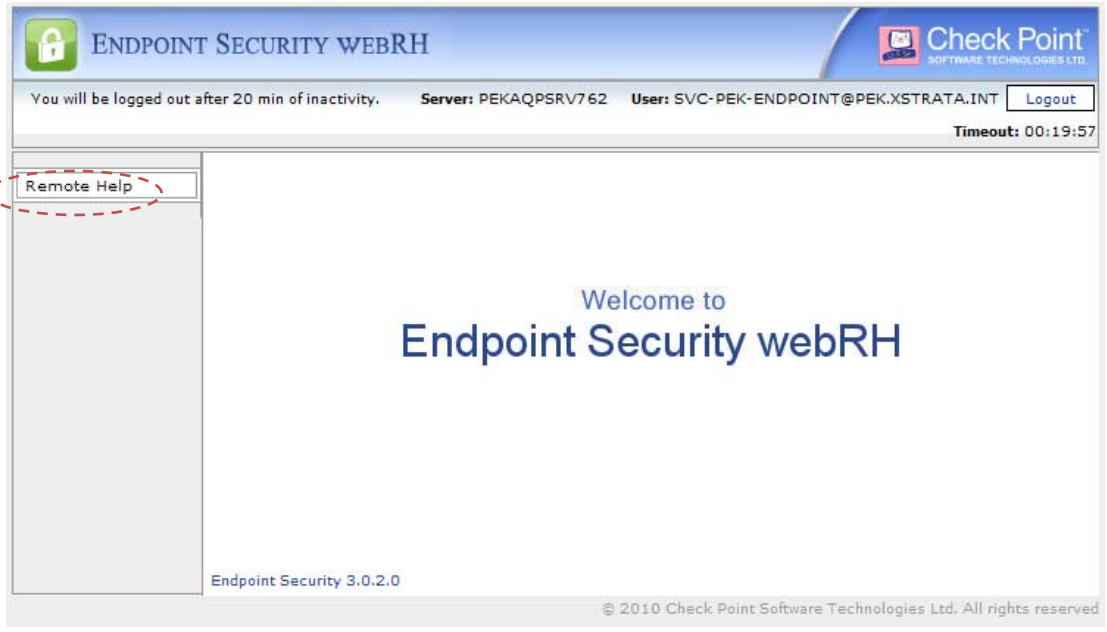


Figura 35.

Seleccionar “WebRH Full Disk Encryption Module” indicado en la figura 36, para poder iniciar el cambio de contraseña en forma remota.

Figura 36.

Para este caso, usaremos como ejemplo la cuenta “ECORNEJO”, seleccionando “Remote password change” (ver figura 37).

Figura 37.

El sistema entregará la primera respuesta del usuario “Response One to end user”, la cual debe ser entregada al usuario.

El usuario, desde la pantalla de inicio de Endpoint (boot), debe hacer clic en el botón “Remote Help”, e ingresar el valor entregado por “Response One to end user”.

En este punto, el usuario generará un respuesta “Challenge”, la cual debe ser entregada e ingresada en el campo “Challenge from end user”. Luego de ingresar la información hacer clic en el botón “Get Response”. (Ver figura 38)

Figura 38.

Finalmente la segunda respuesta es generada por el sistema como se aprecia en la figura 39 y debe ser entregada al usuario.

Figura 39.

El usuario deberá ingresar el número entregado por el sistema y dar clic en OK. (Ver figura 40).

Figura 40.

Una vez que este proceso haya sido completado, el cliente podrá cambiar la contraseña, donde se desplegara la siguiente pantalla de la figura 41:

Figura 41.

Al ingresar a Windows, el sistema le solicitará la contraseña de red de Windows (antigua) y luego la nueva contraseña de Full Disk Enryption de Endpoint.

El sistema actualizara la contraseña de Endpoint con la contraseña de red (prevaleciendo la contraseña de Windows sobre la de Endpoint) lo que implica que el usuario la próxima vez que ingresa, en la pantalla de inicio de Windows debe ingresar con la antigua contraseña solo la primera vez.

3.5.8 Recuperación de información con BartPE DMU

En caso de que un computador no pueda iniciar sistema operativo Windows de forma correcta, y se desee recuperar la información de las particiones de ese disco, se

debe hacer uso de la utilidad BartPE DMU (Disk Mount Utility), la cual permite desbloquear y desproteger de forma temporal el acceso al disco.

La utilidad BartPE DMU (bartpe-cp-dmu.iso) debe ser descargada de la siguiente ruta y quemarse en un CD virgen:

\\clkstgsrv111\Agent

Se debe iniciar el computador desde la unidad de CD/DVD-ROM. BartPE es un sistema operativo Live basado en Windows XP.

Una vez iniciado el sistema, cargar la aplicación “Dynamic Mount Utility” desde el menú de programas (ver figura 42). Seleccionar las particiones que se desean desproteger que se verán como indica la figura 43.

Figura 42

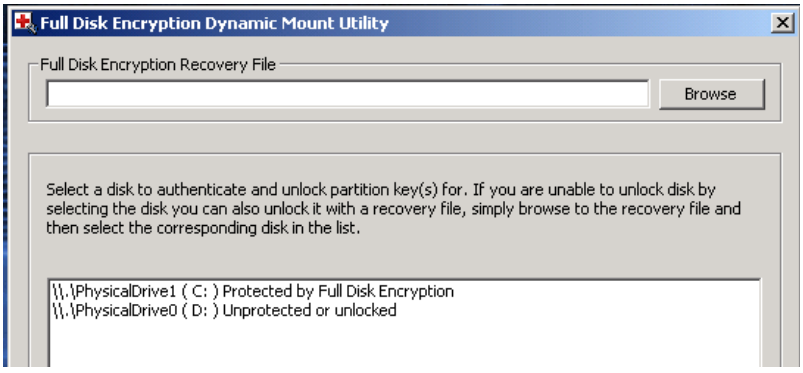


Figura 43.

Después de seleccionar las unidades se solicitarán las credenciales de administrador Full Disk Encryption, como se puede apreciar en la figura 44.

Figura 44.

User account name : RALPH
Password : Ch1efW1ggamsS**!

User account name : MOE
Password : M0eTheBart3nd**!

Una vez ingresadas las credenciales, se puede recuperar la información haciendo uso del explorador de archivos de BartPE.

3.6 Administración de Políticas Media Encription

3.6.1 Introducción

Los siguientes pasos explican el proceso de administración de políticas, y la habilitación de la encriptación de medios para dispositivos de almacenamiento masivo vía Checkpoint Endpoint Media Encryption (discos duros externos, memorias, pendrives, etc.)

3.6.2 Administración de Políticas de Media Encription

Para realizar la administración de políticas de Media Encryption, estas se llevan a cabo a través del servidor de Endpoint. Los servidores de Endpoint para cada uno de los dominios del ámbito de administración de BUIT SA son:

- ARK: arkcrnsrv710.ark.xstrata.int
- CLK: clkstgsrv713.clk.xstrata.int
- GLK: glkbnesrv706.glk.xstrata.int
- PEK: pekaqpsrv761.pek.xstrata.int

Una vez ingresado al servidor, se debe ejecutar al aplicación Administration Console, ubicada en “Start – Check Point - Check Point ESME Server”. (Ver figura 45)

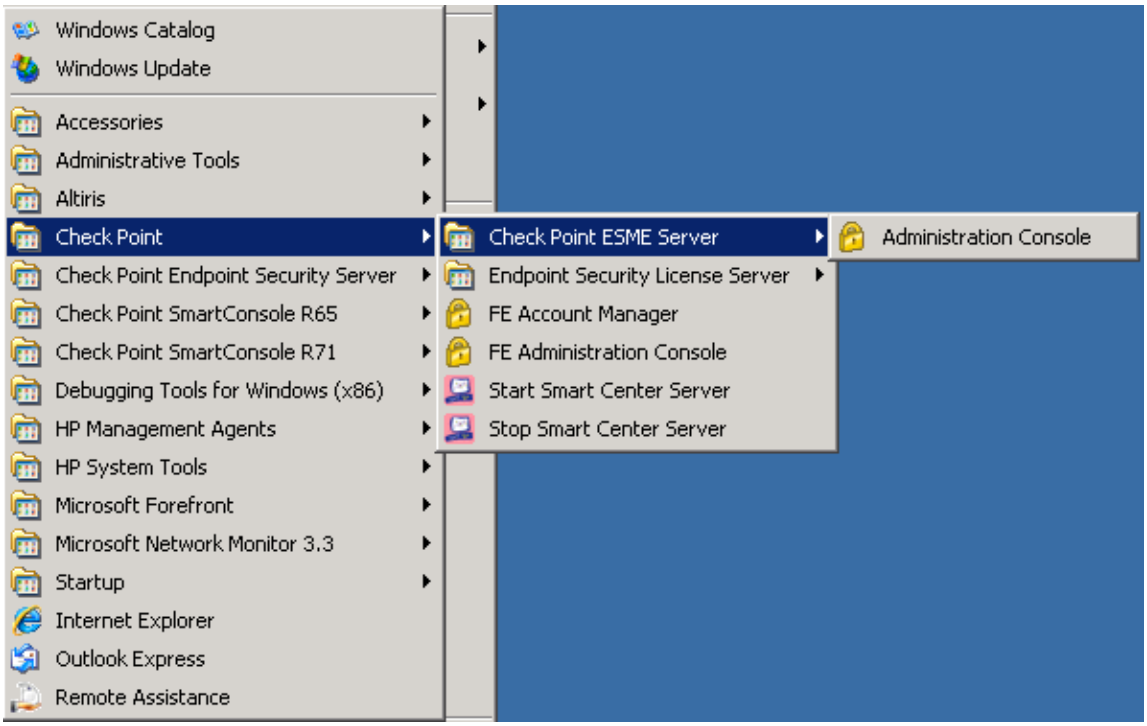


Figura 45.

Una vez que ingresemos a la aplicación, tendremos acceso a la consola de administración de Media Encryption como se muestra en la figura 46:

Figura 46.

Las secciones en el panel izquierdo entregan la siguiente información:

- Users:

  Listado de todos los usuarios del Dominio (Active Directory).

- Computers:

  Listado de todos los equipos (Notebooks / Workstations) que tienen Media Encryption instalado.

- Groups:

  Usuarios y Equipos que adquieren las políticas de Media Encryption.

- Profile Template:

  Planillas donde se administran cada una de las políticas de Media Encryption.

- Alerts:

  Listado de posibles alertas relacionadas con Media Encryption.

- Log:

  Registros de actividad de dispositivos que han sido autorizados o bloqueados por Media Encryption.

- Removable Media Log:

  Permite visualizar las actividades de Log asociadas a Media Encryption por equipo y por usuarios.

- Reports:

  Permite la generación de reportes en base a parámetros preestablecidos, como por ejemplo usuarios que no se han conectado durante los últimos “x” días (útil para la eliminación de equipos y mantención de licencias). Todos los reportes se visualizan vía Web.

Para realizar administración de las políticas, debemos ingresar a “Profile Templates”, (figura 47) donde encontraremos las planillas que se aplican a todos los usuarios que tengan el cliente Endpoint instalado o aquellas estaciones de trabajo que cuentan solamente con Media Encryption.

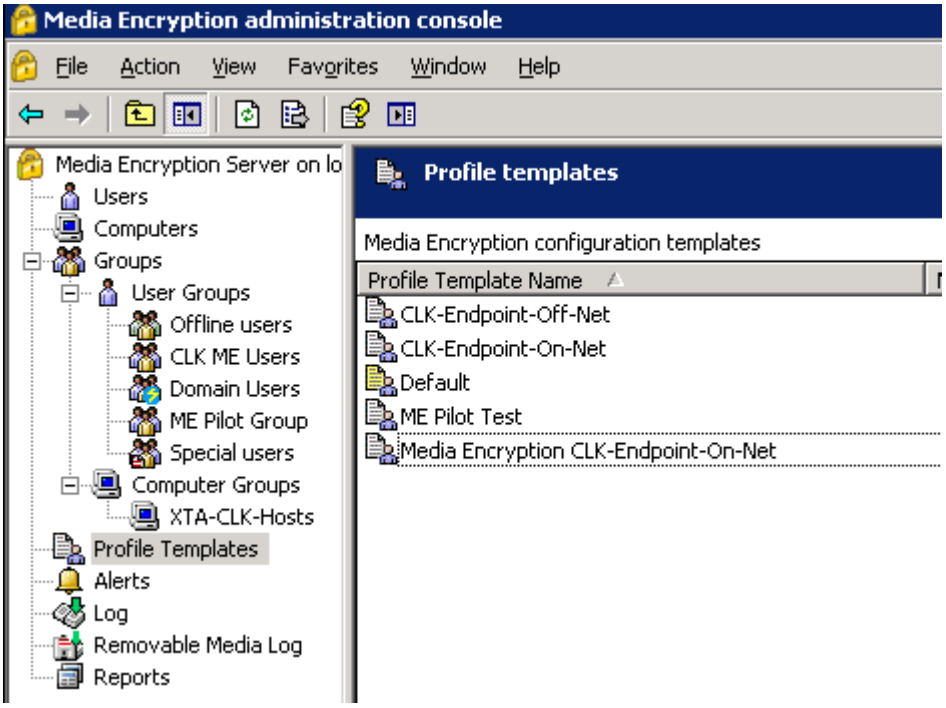


Figura 47.

Las políticas CLK-Endpoint-Off-Net y CLK-Endpoint-On-Net, se aplican a los clients Endpoint y Media Encryption que se encuentran desconectados o conectados a la red de Xstrata respectivamente, mientras que la política Media Encryption CLK-Endpoint-On-Net se aplica en forma transversal a usuarios de Notebooks y Workstations.

En caso de que se requiera modificar la política Media Encryption CLK-Endpoint-On-Net, se deben ingresar a las propiedades de dicha política, luego ingresar a la pestaña

"Device Manager", donde podemos seleccionar los tipos de dispositivos que queremos que se encripten.

En la imagen a continuación, (figura 48) se puede observar que los dispositivos considerados como almacenamiento externo removible (Removable Media Devices) y discos duros externos (External Hard Drives) tienen forzada la encriptación (Access, Create). El dispositivo Modems, tiene bloqueado el funcionamiento, pero en algunos casos se ha tenido que habilitar, ya que dispositivos de comunicación son considerados Modems.

El resto de las pestañas no requiere de otras configuraciones, ya que heredan las configuraciones de las políticas CLK-Endpoint-Off-Net y CLK-Endpoint-On-Net.

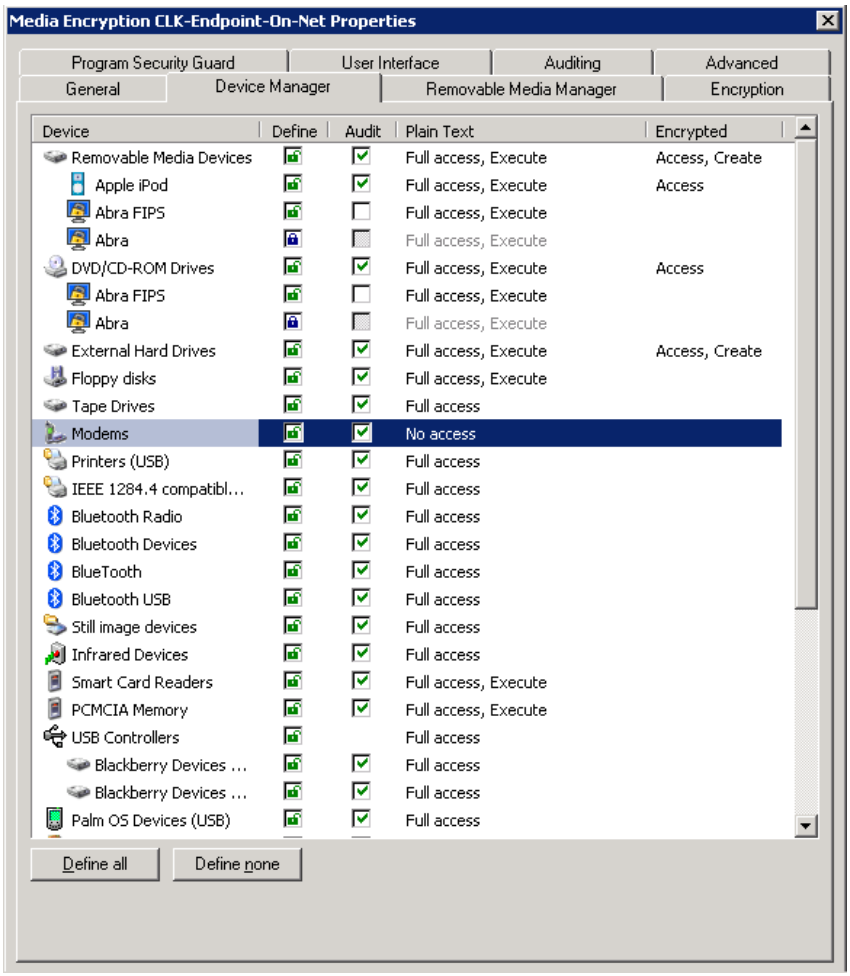


Figura 48.

Para que un equipo, adquiera las políticas, este debe tener el cliente Endpoint o el modulo Media Encryption instalado y reportarse al servidor Endpoint del dominio local.

Una vez que el equipo se reporta en el servidor de Media Encryption, se debe asociar al usuario al grupo donde se aplica el perfil o política, en este caso es el perfil Media Encryption CLK-Endpoint-On-Net.(Figura 49).

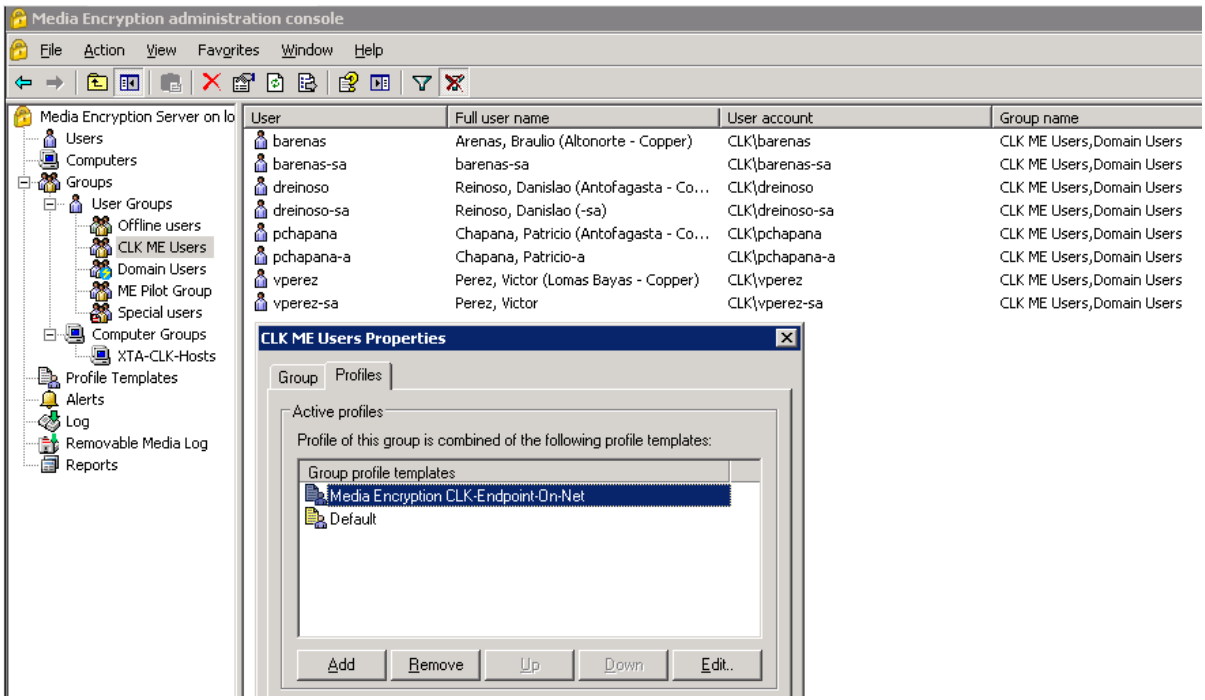


Figura 49.

Para validar que las políticas se estén aplicando correctamente sobre el equipo, ir a Settings en el cliente Endpoint, ingresar a la opción Media Encryption y presionar Shift-Control-F6. Esto desplegará una pantalla en código XML, (Figura 50) donde al final de dicha pantalla, se observan que las políticas se aplican correctamente.

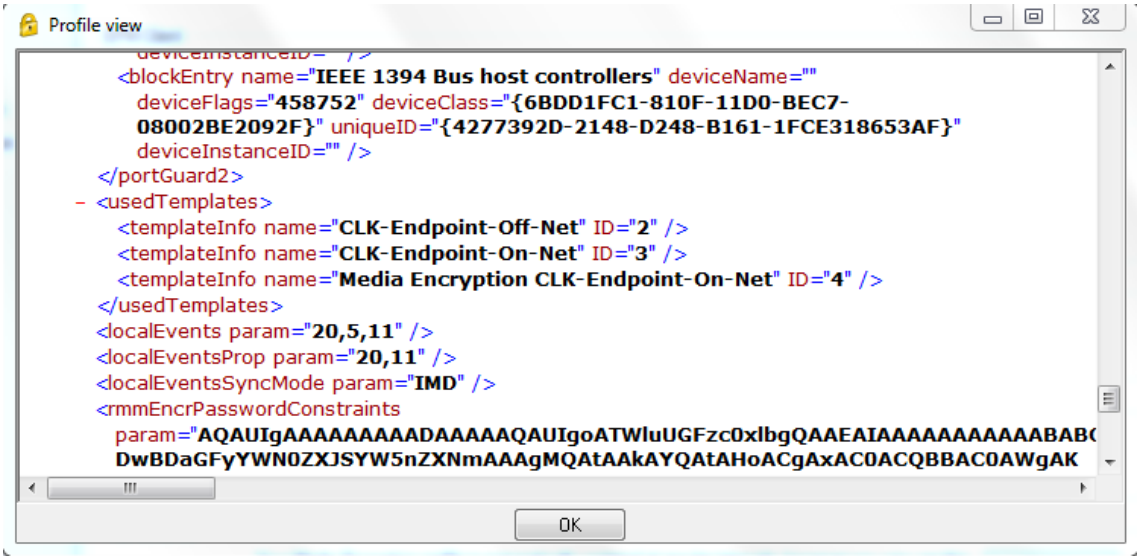


Figura 50.

3.6.3 Generación de Reportes

Una opción bastante útil en la administración de Media Encryption, es la generación de reportes, para obtener datos estadísticos y/o realizar administración de licencias.

Desde la opción Reports (panel izquierdo, botón derecho), se puede generar un nuevo reporte, donde se desplegara un asistente (Figura 51).

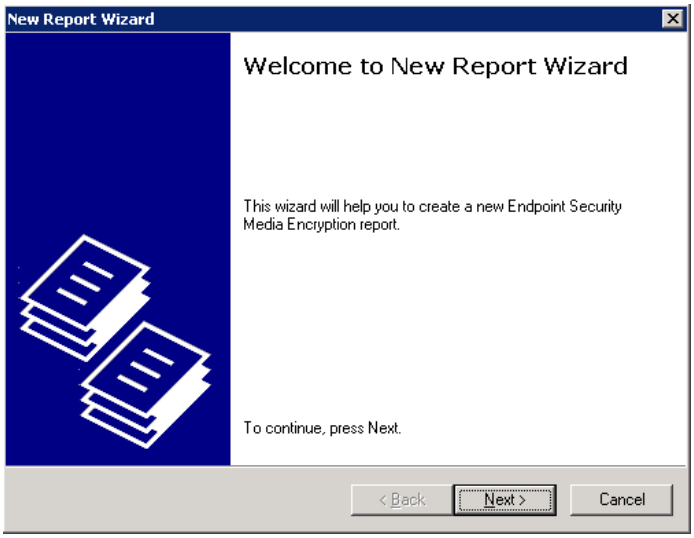


Figura 51

En este caso y como ejemplo, se generará un reporte indicando los equipos que no se han conectado durante los últimos 90 días. (Ver figura 52)

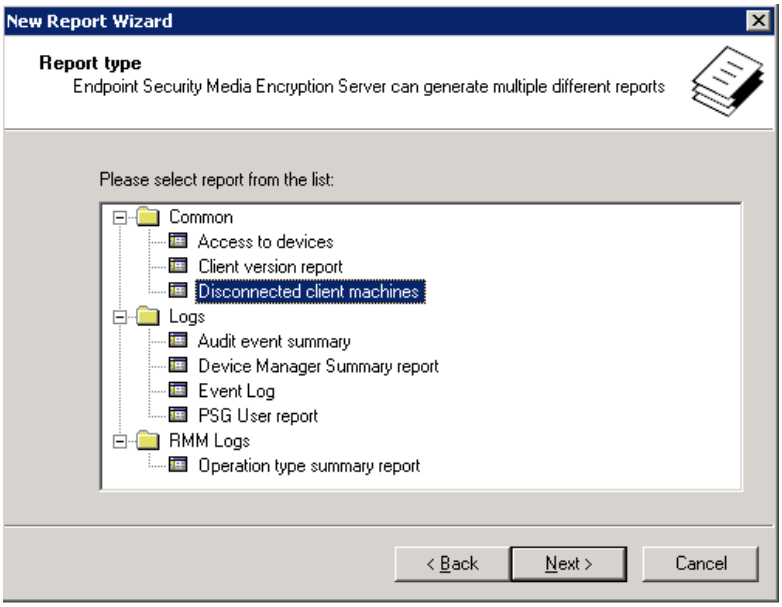


Figura 52.

A través del botón Edit, se pueden editar la cantidad del días de no conexión (figura 53).

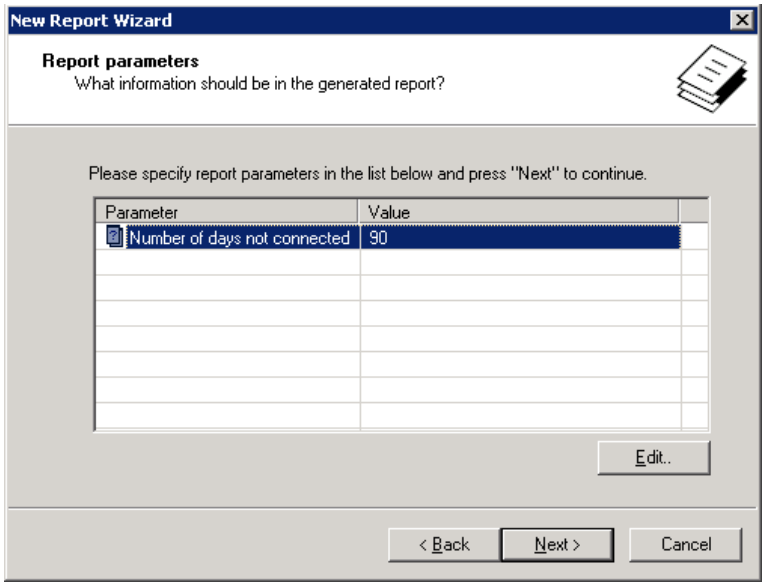


Figura 53.

El Informe se puede generar inmediatamente o en un tiempo especificado como se puede ver en la figura 54.

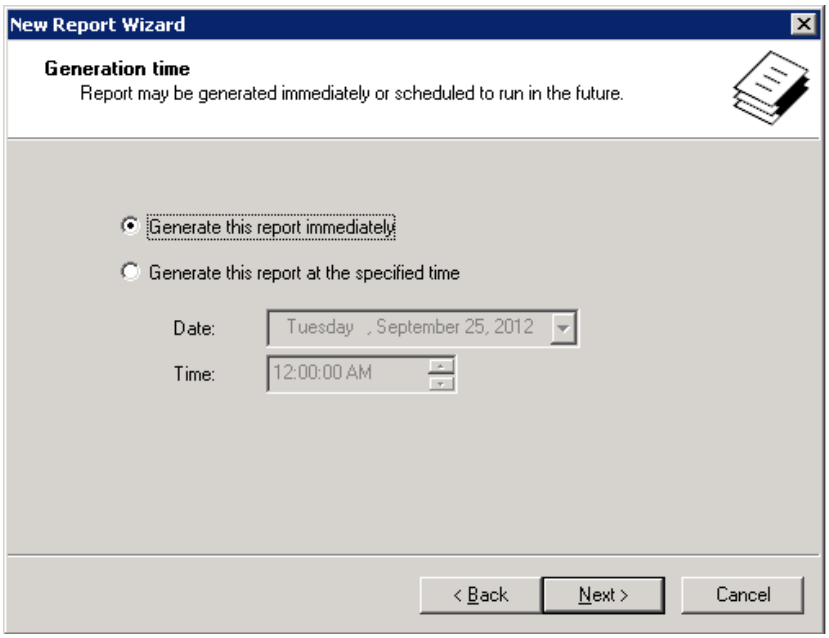


Figura 54.

Como ves en la figura 55, se debe agregar una descripción.

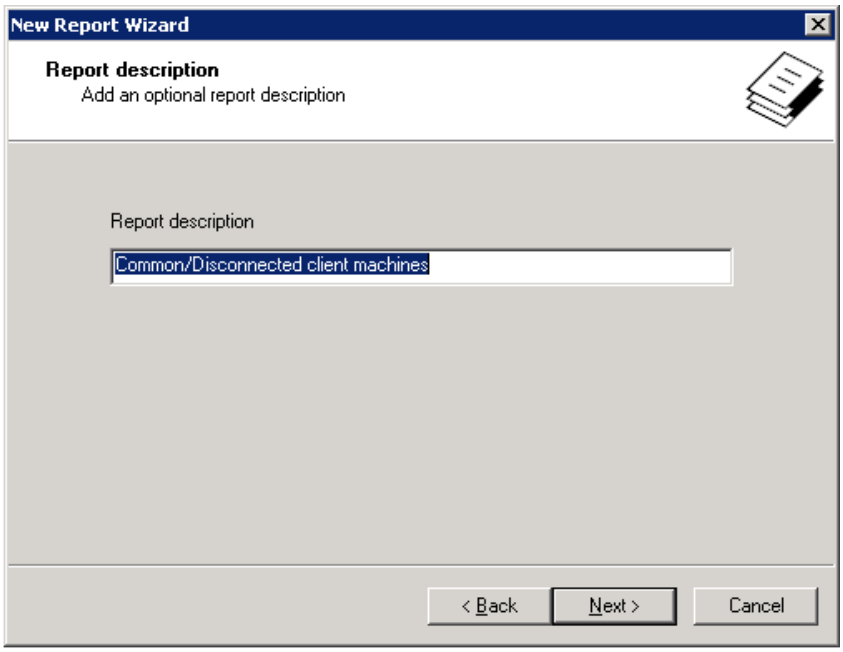


Figura 55.

La pantalla siguiente muestra el resumen, se puede apreciar en la figura 56.

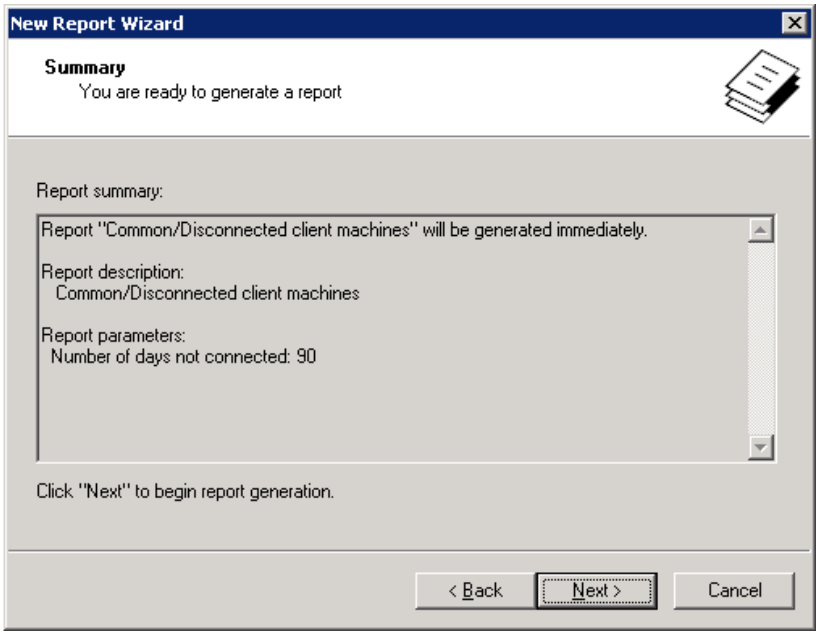


Figura 56.

Luego se muestra en la figura 57 la pantalla donde debes indicar finalizar para que quede generado el reporte.

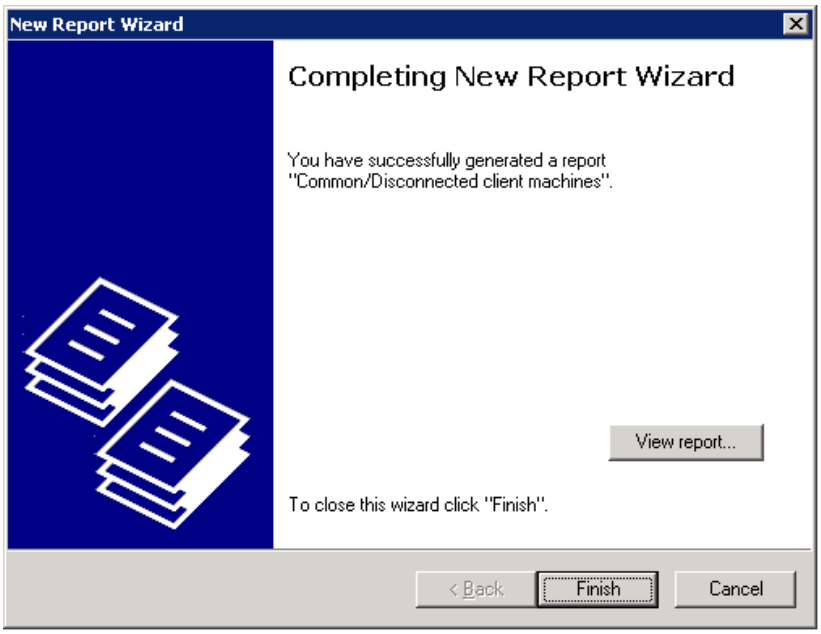


Figura 57.

Una vez que el reporte se ha generado, se puede visualizar vía Web. (Ver figura 58)

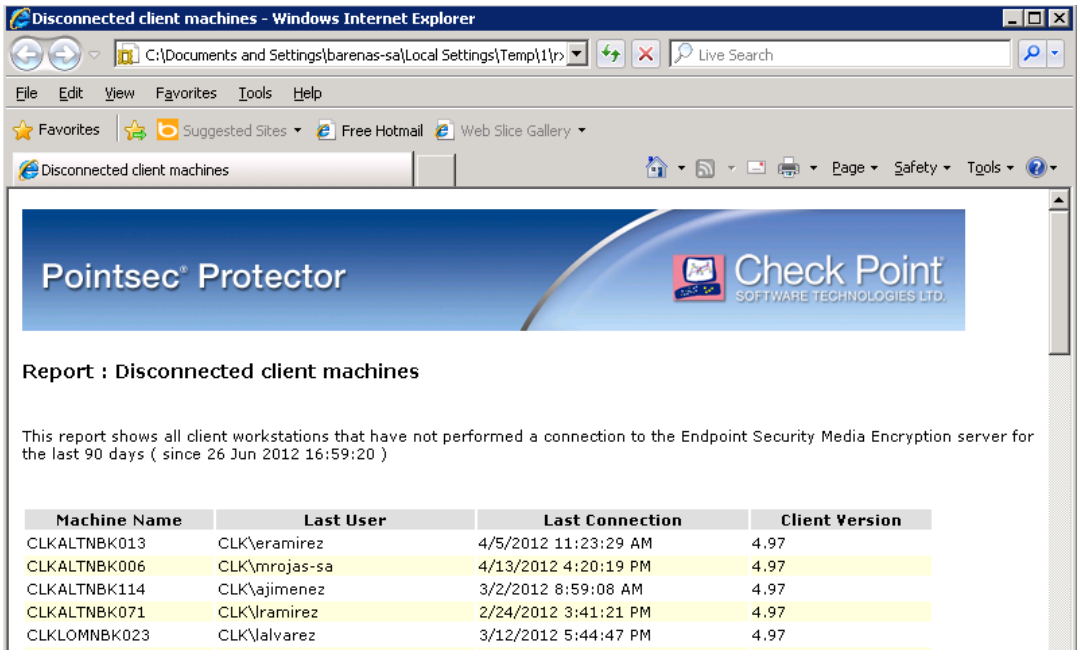


Figura 58.

3.7 Habilitación De Encriptación De Medios

3.7.1 Introducción

A continuación se explica el proceso de habilitación de la encriptación de medios para dispositivos de almacenamiento masivo (discos duros externos, memorias, pendrives, etc.). Cada vez que se inserta un dispositivo de almacenamiento externo, se preguntará al usuario si desea encriptar el contenido del dispositivo para asegurar la información de éste.

3.7.2 *Proceso de habilitación de encriptación de los medios*

En el momento de insertar un dispositivo de almacenamiento masivo, se desplegará la siguiente pantalla como se indica en la figura 59:

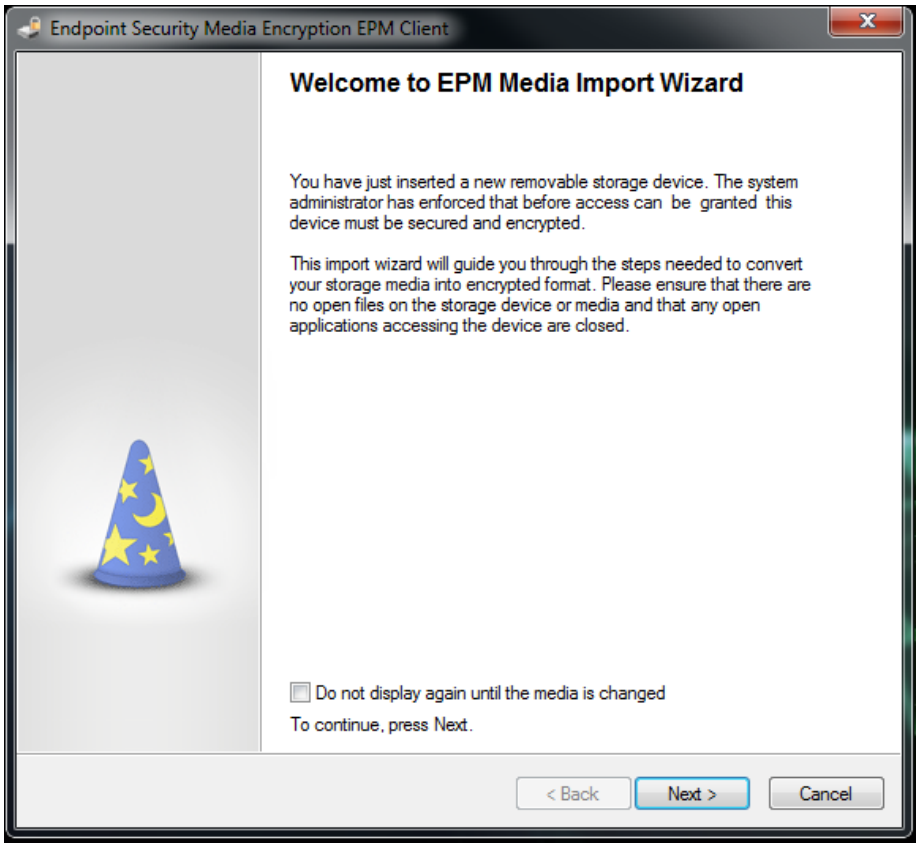


Figura 59.

El proceso de encriptación, no es obligatorio y se puede cancelar. En caso de que el usuario requiera encriptar el medio de almacenamiento, dar clic en Next (Siguiente) y se mostrará la siguiente pantalla (Figura 60), donde se muestra la letra de unidad y capacidad del dispositivo. Dar clic en Next (Siguiente).

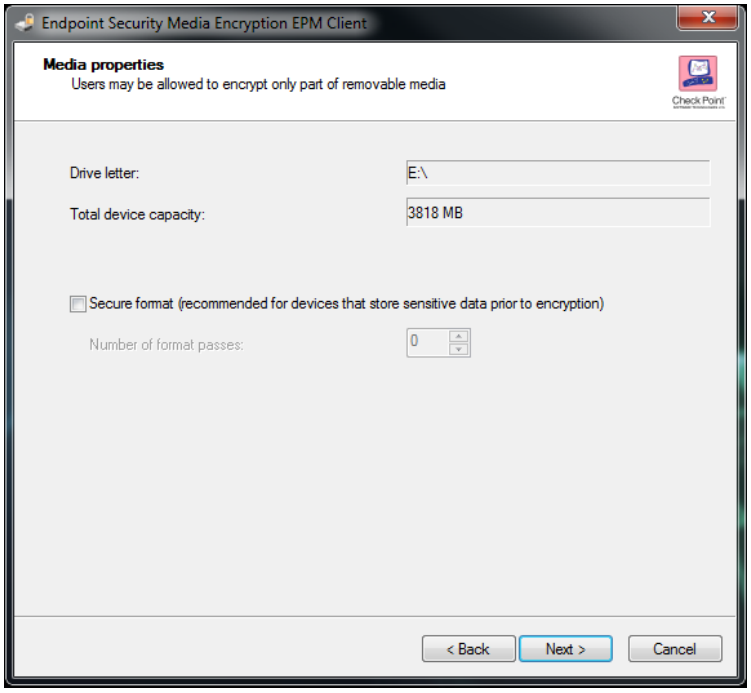


Figura 60.

Ingresar las contraseñas deseadas para encriptar el dispositivo (ver figura 61). Esta contraseña se solicitara cuando se conecte el dispositivo en otro computador distinto a donde se encriptó el dispositivo.

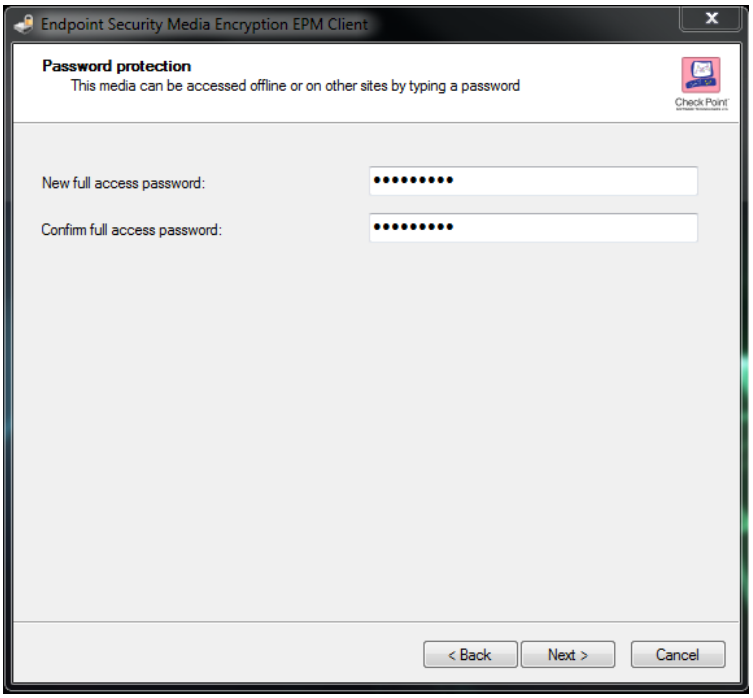
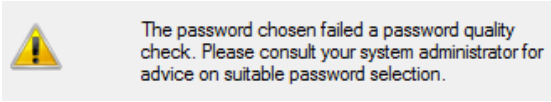


Figura 61.

Si la contraseña no es suficientemente compleja, el proceso nos avisará. Se recomienda usar una contraseña que contenga mayúsculas, minúsculas, números y algún carácter especial ($#%.&=).



El proceso durará según el tamaño del dispositivo y a la cantidad de información que este contenga. A mayor cantidad de información, más tiempo tomará el proceso de encriptación. (Figura 62)

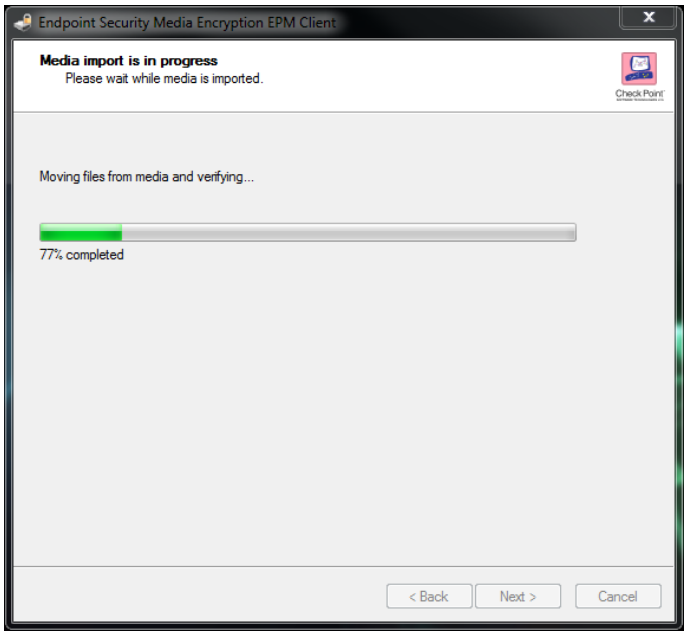


Figura 62.

Una vez completado el proceso de encriptación, se desplegara la siguiente pantalla indicada en la figura 63.

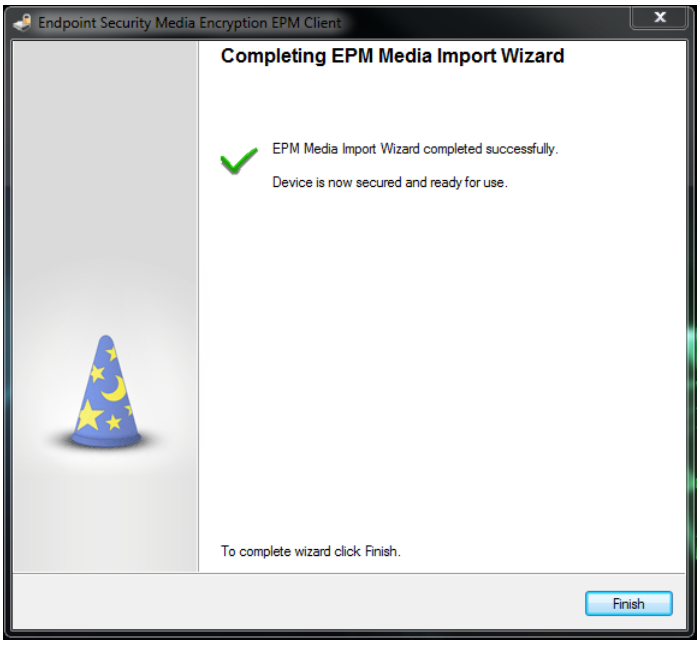


Figura 63.

3.7.3 *Ingreso de claves al insertar medio encriptado en otro PC*

En caso de insertar el medio encriptado en otro PC, con Media Encryption instalado, se solicitará la contraseña para leer la información del dispositivo, ver figura 64.

Figura 64.

En caso de cancelar o ingresar de forma incorrecta la contraseña se despliega el siguiente aviso como se aprecia en la figura 65:

Figura 65.

En caso de ingresar correctamente la contraseña, se abrirá de manera normal el Explorador de Windows.

3.7.4 *Ingreso de claves al insertar medio encriptado en otro PC*

En caso de insertar el medio encriptado en otro PC, sin Media Encryption instalado, se solicitará la contraseña para leer la información del dispositivo. (Ver figura 66.)

Figura 66.

En caso de ingresar correctamente la contraseña, se abrirá el Explorador de Media Encryption. (Figura 67)

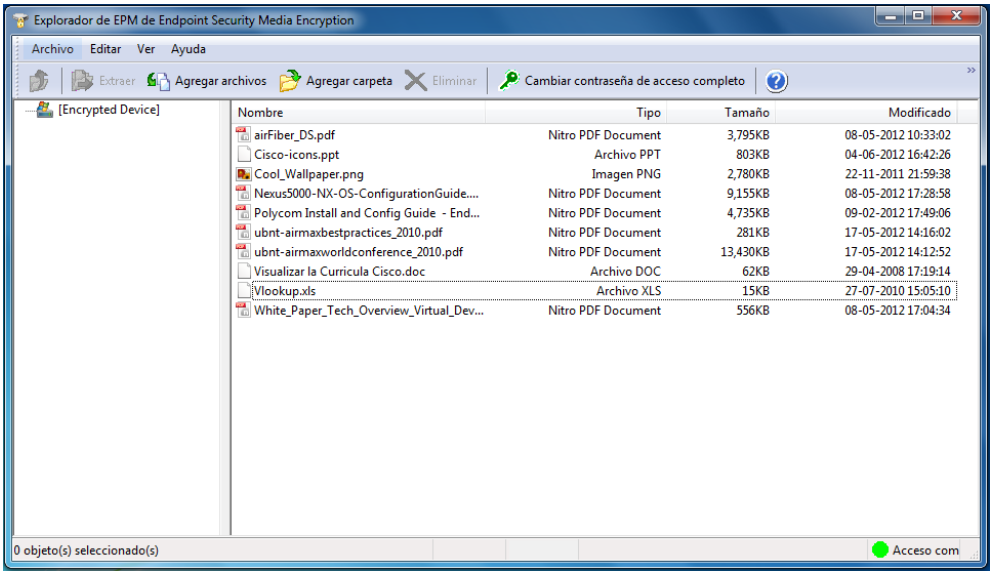
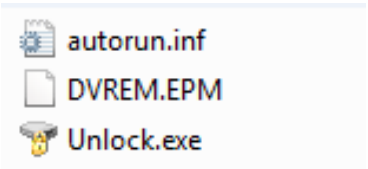


Figura 67.

En caso de que no se soliciten las contraseñas en el momento de insertar el media encriptado, ir a la unidad del dispositivo a través del Explorador de Windows y ejecutar el archivo “Unlock.exe”, el cual a su vez ejecutará la aplicación donde se solicitaran las credenciales.



Deshabilitando la encriptación de medios en el dispositivo de almacenamiento.

En caso que se requiera deshabilitar la encriptación de un dispositivo, se puede realizar en opción Settings donde se encuentra el candado de la aplicación Endpoint Security.

Opción Settings para Workstations indicado en la figura 68:

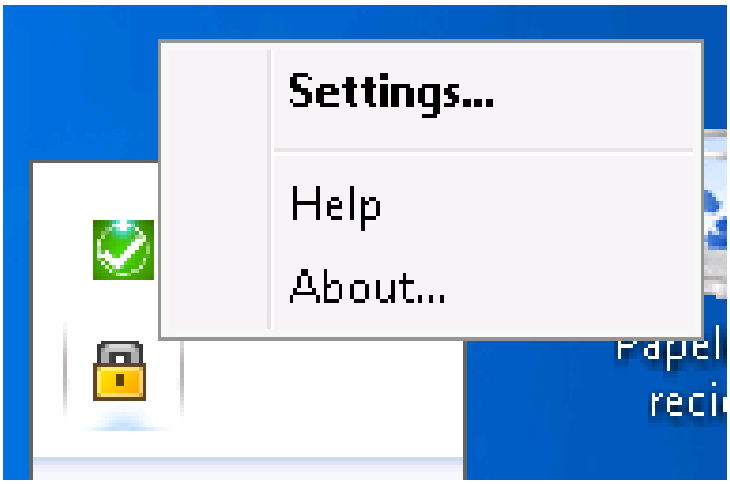


Figura 68.

Opción Settings para Laptops indicado en la figura 69:

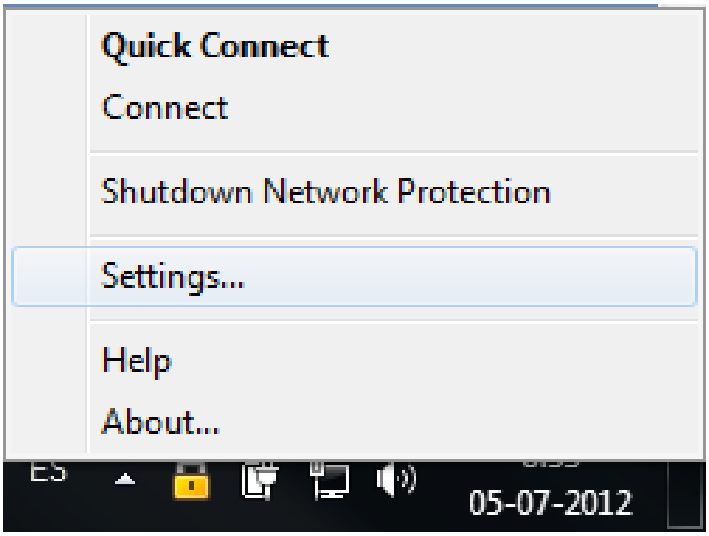


Figura 69.

Luego ir al módulo Media Encryption (panel izquierdo) y presionar el botón Open en la opción Endpoint Policy Management Client.

Opción Endpoint Policy Management Client para Workstations indicado en la figura 70.

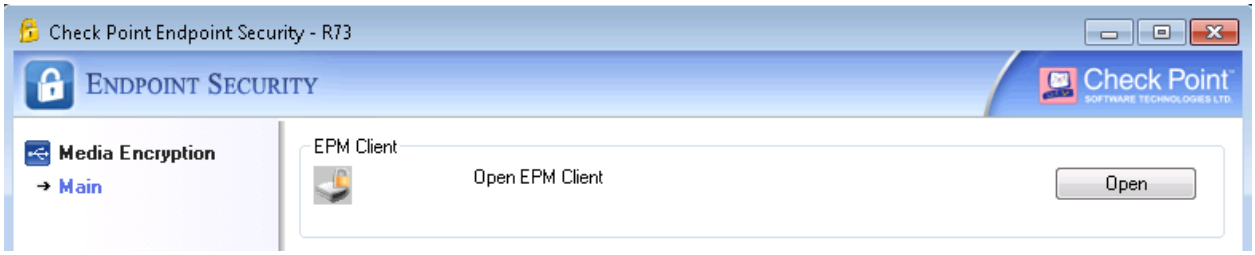


Figura 70.

Opción Endpoint Policy Management Client para Workstations indicado en la figura 71.

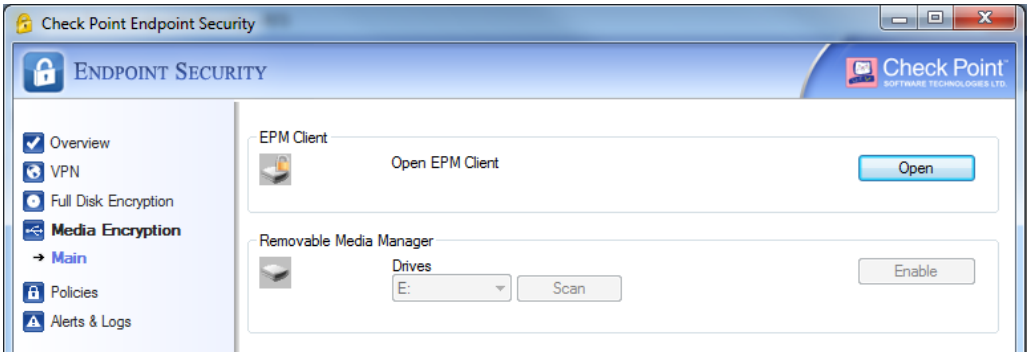


Figura 71.

A continuación se desplegará el siguiente cuadro, (Figura 72) donde a través de la opción “Export”, podremos deshabilitar la encriptación del dispositivo. A través de la opción Set (Set EPM media full access password) podremos cambiar la contraseña de encriptación del medio.

Figura 72.

Una vez presionado el boton “Export”, se desplegara la siguiente pantalla (Figura 73). Dar clic en siguiente para iniciar el proceso de desencriptación.

Figura 73.

Una vez finalizado el proceso, se desplegará la siguiente pantalla (Figura 74).

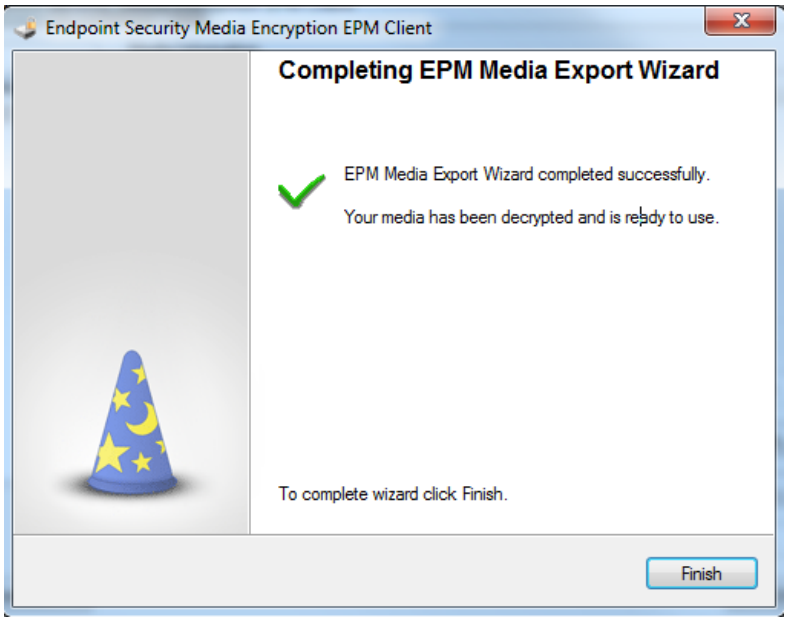


Figura 74.

El medio insertado ahora se encuentra desencriptado (Figura 75) y se puede volver a encriptar a través de la opción “Import”.

Figura 75.

4 *CONCLUSIONES*

El desarrollo del trabajo presentado tiene como objetivo central poder asegurar los datos, contar con una conexión segura a través de internet permitiendo accesos a todos nuestros sistemas, contar con un antivirus y firewall que sean confiable, para ello se determinó implementar la aplicación Checkpoint Endpoint elegida por Xstrata.

Para la conexión remota se habilita una conexión VPN que permite a los usuarios conectarse a través de una conexión de internet segura a todos los servicios de Xstrata como si estuvieran en su escritorio, con esta conexión además nos aseguramos que al conectar inmediatamente se actualiza el antivirus y se aplican las actualizaciones de Windows con lo que el equipo estará con estas al día aunque este fuera de nuestra red por largo tiempo.

Se logró a través de la encriptación de discos asegurar la data, la información está segura y no podrá ser accesada por ningún ente externo, con esto los usuarios viajeros hoy en día tienen la tranquilidad de viajar con sus equipos personales sin riesgo alguno.

Al valorar la seguridad de la información en una empresa se debe plantear un sistema que nos permita preservar la confidencialidad, la integridad y la disponibilidad de dicha información con lo cual todo sistema de seguridad debe cumplir con cinco objetivos principales:

- Integridad: garantizar que los datos sean los que se supone que son.
- Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información.
- Evitar el rechazo: garantizar de que no pueda negar una operación realizada.

- Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos.

Al tratarse de una tendencia que está en constante crecimiento se debe poner en consideración que los sistemas de seguridad se encuentran desarrollados para mitigar las amenazas y salvaguardar la información importante y se debe complementar con una cultura de seguridad y mejores prácticas a los empleados para atenuar las brechas de seguridad.

En conclusión, se logró cumplir a cabalidad con los objetivos planteados al comenzar el presente trabajo, la herramienta seleccionada permite el control granular y la integración con más módulos y soluciones del mismo fabricante; permitiendo cubrir gran parte del espectro de la empresa.

Todo lo mencionado lo encontramos en esta aplicación, Checkpoint de Endpoint es VPN segura para los usuarios remotos el acceso a la red y la comunicación, este agente combina el mejor firewall, control de acceso a la red (NAC), control de programas, anti-virus, anti-spyware, Antibot , IPS, encriptación total del disco duro, encriptación de medios, con protección de los puertos y acceso remoto, y lo más importante todo en un único agente.

5 *GLOSARIO*

AES

Es uno de los algoritmos de criptografía más usados en la actualidad, es un algoritmo simple, rápido y de cifrado por bloques, inicialmente fue diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits, por lo tanto los datos a ser encriptados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se lo puede ver como un bloque o matriz de 4x4 bytes al que se lo llama estado.

Algoritmos

Se denomina algoritmo a un grupo finito de operaciones organizadas de manera lógica y ordenada que permite solucionar un determinado problema. Se trata de una serie de instrucciones o reglas establecidas que, por medio de una sucesión de pasos, permiten arribar a un resultado o solución.

Cabe mencionar por último que los algoritmos son muy importantes en la informática ya que permiten representar datos como secuencias de bits. Un programa es un algoritmo que indica a la computadora qué pasos específicos debe seguir para desarrollar una tarea.

Bots

La palabra bot es parte de la jerga informática y no es seguro si será sustituida por una equivalente en español, o se usará la palabra original de la cual procede, robot. Es importante distinguir que bot es una definición funcional, y no hace diferencias en cuanto a su implementación. Un bot puede estar diseñado en cualquier lenguaje de programación, funcionar en un servidor o en un cliente, o ser un agente móvil, la programación de un bot puede estar diseñada para cumplir tareas muy básicas como lo son el recordar alguna tarea o bien automatizar algún proceso, también existen bots

con programación más compleja que buscan realizar actividades que conllevan toma de decisiones.

Choke point

Definido como Embudo o cuello de botella, Un punto en el que el tráfico u otros movimientos pueden bloquearse fácilmente.

Clustering

El término clúster (del inglés cluster, "grupo" o "racimo") se aplica a los conjuntos o conglomerados de ordenadores unidos entre sí normalmente por una red de alta velocidad y que se comportan como si fuesen una única computadora.

Simplemente, un clúster es un grupo de múltiples ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador, más potente que los comunes de escritorio.

Core War

Es un juego de programación en donde combaten entre sí programas escritos en un lenguaje similar al ensamblador con el objetivo de ocupar toda la memoria de la máquina eliminando así a los oponentes.

Criptografía

Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Criptología

La Criptología es, tradicionalmente, la disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas.

Criptosistemas

Un criptosistema es el conjunto de procedimientos que garantizan la seguridad de la información y utilizan técnicas criptográficas.

DES – 3DES

(Data Encryption Standard), (Triple Data Encryption Standard)

Es un algoritmo de cifrado, es decir, un método para cifrar información, DES es el algoritmo prototipo del cifrado por bloques, un algoritmo que toma un texto en claro de una longitud fija de bits y lo transforma mediante una serie de operaciones básicas en otro texto cifrado de la misma longitud.3Des, se basa en aplicar el algoritmo DES tres veces.

FDE

Encriptación de disco completo (FDE) es el cifrado en el nivel de hardware. FDE funciona mediante la conversión automática de datos en un disco duro en un formulario que no puede ser entendido por cualquier persona que no tiene la clave para "deshacer" la conversión. Sin la clave de autenticación adecuada, incluso si el disco duro se extrae y se coloca en otra máquina, los datos permanecen inaccesibles.

FTP

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

Firewall

Muro de fuego, dispositivo de seguridad, un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Un firewal es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso.

Heuristica

En los productos antivirus se conoce como heurística a las técnicas que emplean para reconocer códigos maliciosos (virus, gusanos, troyanos, etc.) que no se encuentren en su base de datos (ya sea porque son nuevos, o por no ser muy divulgados).

IPS

Por sus siglas en Ingles significa sistema de prevención de intrusos, es un software que controla el acceso a las redes de informática para asi proteger de ataques y abusos s los sistemas computacionales**.**

IRC

Internet Relay Chat, más conocido como IRC o simplemente Chat, es un servicio de Internet que permite la comunicación inmediata a través de Internet entre dos o más personas en formato textual en tiempo real. Se dice que es el medio de comunicación en tiempo real más rápido y eficaz que existe en la Red.

MAC

Control de acceso al medio, se conoce también como dirección física, y es única para un dispositivo en particular.

Una dirección MAC es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet).

Malware

El malware (del inglés “malicious software”), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario

NAC

El Control de Acceso a la Red, también conocido por las siglas NAC (Network Access Control), tiene como objetivo asegurar que todos los dispositivos que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información entre otros.

El objetivo es realizar exactamente lo que su nombre implica: control de acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios y dispositivos, y que pueden hacer en ella.

NTFS

El sistema de archivos NTFS (siglas en inglés New Technology File System (Sistema de archivos de nueva tecnología)) se basa en una estructura llamada tabla maestra de archivos, la cual puede contener información detallada en los archivos. Este sistema permite el uso de nombres extensos, aunque, a diferencia del sistema FAT32, distingue entre mayúsculas y minúsculas.

Pin

El PIN (de las siglas en inglés, Personal Identification Number) es un número de identificación personal utilizado en ciertos sistemas, para identificarse y obtener acceso al sistema. El PIN es un tipo de contraseña y sólo la persona beneficiaria del servicio conoce el PIN que le da acceso al mismo; esa es su finalidad. El PIN tiene que ser suficientemente seguro para evitar la intrusión no autorizada al servicio que protege.

Rootkits

Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas

herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

SEAL

Es un generador de secuencia cuya estructura está especialmente pensada para funcionar de manera eficiente en computadores con una longitud de palabra de 32 bits. Cifrado de seguridad necesario para la vida informática.

Spyware

El spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador por lo que puede traer graves problemas a nuestras computadoras, que entra de forma disfrazada a través de Internet.

SSH (Secure Shell)

Secure Shell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X (Sistema de Ventanas X) para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (en sistemas Unix y Windows).

VPN

Alude a la expresión del idioma inglés Virtual Private Network, que puede traducirse como Red Virtual Privada, permite la extensión de una red pública como Internet a un espacio de red local.

Si bien se utiliza una red pública como es la de conexión a Internet, los datos son transmitidos por un canal privado, de forma que no peligra la seguridad ni la integridad de la información interna. Los datos son cifrados y descifrados alternativamente, ahorrando dinero y problemas a empresas de distinta escala.

WAN

Es la sigla de Wide Área Network (Red de Área Amplia). El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso a nivel mundial. Un ejemplo es la propia Internet.

6 *BIBLIOGRAFIA*

1994-2017 Check Point Software Technologies Ltd.
https://www.checkpoint.com/products/endpoint-policy-management/

UMEX.
http://seguridadinformatica-umex.blogspot.cl/p/encriptacion.html

Wikipedia®
https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

André Goujon
http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-nformacion

Proweb Chile
http://www.proweblatam.com/producto_checkpoint.html

1994-2017 Check Point Software Technologies Ltd.
http://www.etek-reycom.com.ar/tecno/proveedor/check_point.htm

https://www.checkpoint.com/products/media-encryption/

Intranet
http://copper.xstratanet/ES/BUIT/default.aspx

http://copper.xstratanet/ES/BUIT/DOCUMENTACION%20BUIT/Forms/AllItems.aspx

http://brisbane.copper.xstratanet/Pages/Default.aspx

http://brisbane.corporate.xstratanet/Document%20Centre/Forms/AllItems.aspx