INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES & SEGURIDAD

21

SERVIDORES ADICIONALES

En esta clase conoceremos diversos servidores adicionales que nos permitirán implementar funciones específicas en nuestra red. Revisaremos su configuración y los primeros pasos en su uso.

- SERVIDOR DE BACKUP
- BACKUP CORPORATIVO
- SERVIDOR DE ACTUALIZACIÓN
- PROTOCOLO KERBEROS
- SERVIDOR PROXY
- TÉCNICA EVILGRADE

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Santiago Crocioni
Alejandro Gómez
Gilberto González
Javier Medina
Gustavo Martín Moglie
Juan Ortiz
Pablo Pagani
Gerardo Pedraza
Marcelo Soria

Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Características y funciones de servidores adicionales, entre ellos, servidores de backup, servidores de actualización, de antivirus y también servidores proxy.

En la clase anterior, conocimos las funciones que desempeña un File Server, y aprendimos a administrarlo en un sistema Windows y también en un sistema GNU/Linux. Vimos las opciones de seguridad y, además, alternativas de auditoría que es necesario tener en cuenta. Luego, analizamos el funcionamiento de un servidor de impresión, la forma correcta de administrarlo, aumentar su nivel de seguridad y realizar tareas de auditoría.

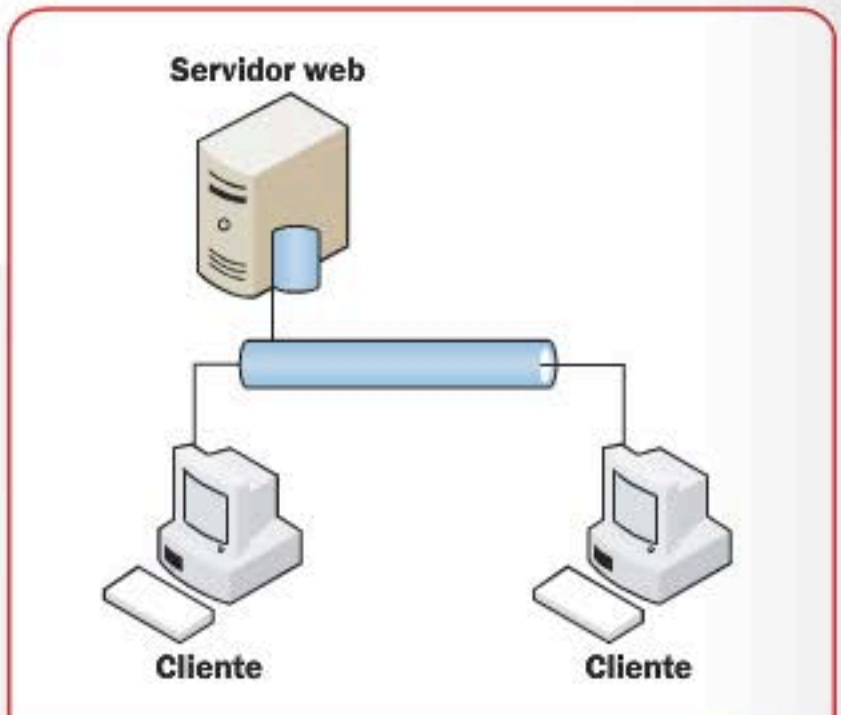
En el presente fascículo, revisaremos diversas alternativas de servidores, conoceremos el funcionamiento de los servidores de backup, y entregaremos algunas recomendaciones de aplicaciones y consejos para administrarlos.
Veremos el funcionamiento de los servidores de actualización y de los servidores de antivirus. Aprenderemos a instalar y a configurar un servidor proxy y los clientes correspondientes; por último, conoceremos algunos protocolos de autenticación y analizaremos la técnica Evilgrade.

21

Servidores de backup

A medida que aumentan los servicios que ofrecemos en nuestra red, necesitamos contar con servidores destinados a realizar las tareas de respaldo; aquí conoceremos sus características y ventajas.

En cuanto nuestra plataforma tecnológica crece, debemos contar con una estrategia de copia de seguridad que acompañe el crecimiento.
Existe una gran cantidad de eventos que pueden afectar la continuidad de los sistemas de nuestra red y requieren que recuperemos información desde una copia de seguridad: desde errores humanos, problemas de integridad de sistemas operativos y bases de datos hasta fallas físicas en nuestros servidores y desastres naturales, como inundaciones o incendios.
Cuando los sistemas implementados en nuestra red se vuelven críticos, la estrategia de copia de seguridad juega un papel fundamental para poder recuperarnos en el menor tiempo posible ante algún evento que afecte la continuidad de nuestros servicios.
Los servidores de backup son los equipos a los que asignamos el rol de implementar nuestra estrategia de copias de seguridad.
La evolución de la estrategia de copias de seguridad a medida que nuestra infraestructura tecnológica crece se puede resumir en tres etapas, las cuales describiremos a continuación.



Una red con un solo servidor, en la que se realiza el backup en forma manual, almacenado de manera local.

Primera etapa: copias manuales y locales

Si el número de servidores con los que contamos lo permite y cuando los servicios que ofrecemos no tienen una criticidad relevante para nuestra red, es suficiente con realizar una copia de nuestros sistemas cuando lo consideremos necesario; por ejemplo, cada vez que se realiza una modificación importante en nuestro sitio web o sobre nuestra base de datos, llevamos a cabo una copia de respaldo en forma manual, la cual almacenamos en el mismo servidor.

LOS SERVIDORES DE BACKUP SON LOS EQUIPOS A LOS QUE ASIGNAMOS EL ROL DE IMPLEMENTAR LA ESTRATEGIA DE COPIAS DE SEGURIDAD.

Segunda etapa: copias locales y automáticas

Cuando la cantidad de servicios y servidores en nuestra red aumenta, la estrategia de copias de seguridad realizadas en forma manual deja de ser la óptima, ya que debemos ingresar a cada servidor en el momento en que necesitamos realizar una copia de respaldo. Para sobrellevar los inconvenientes de la administración del backup en forma manual, ejecutamos las tareas de copia de seguridad mediante el administrador de tareas del sistema operativo; un ejemplo sería realizar el backup mediante archivos de proceso por lotes (.BAT) desde el administrador de tareas de Microsoft Windows en todos los servidores en los que necesitemos realizar copias de respaldo.

Tercera etapa: copias centralizadas y automáticas

A medida que aumenta la cantidad de servidores en nuestra red y los servicios que brindamos incrementan su criticidad, es necesario contar con una estrategia de backup automática y centralizada; en los casos en los que tengamos que prever recuperaciones ante desastres naturales, necesitamos incluso que las copias de respaldo se almacenen en medios extraíbles, como cintas de backup, las que debemos resguardar en un sitio distinto del que aloja a nuestros servidores.
Al llegar a esta etapa, necesitamos contar en nuestra red con equipos dedicados a implementar nuestra estrategia de backup;

a estos equipos los denominamos **servidores de backup**.
Para que nuestro servidor de backup lleve a cabo de forma óptima la estrategia de copias de seguridad, debe implementar al menos las cuatro funciones básicas que ahora mencionamos.

Concentrar las copias de seguridad

Nuestro servidor de backup debe ser el centro especializado en recibir las copias de seguridad de los distintos servidores de la red, los cuales pueden estar ubicados en diferentes puntos geográficos. Para implementar esta funcionalidad, debemos instalar, en cada servidor de nuestra red, el software necesario para integrarlo a nuestra estrategia de backup y, de ese modo, poder extraer la información que necesitamos copiar.

Almacenar

A medida que nuestro servidor de backup recibe las copias de seguridad desde los distintos orígenes, debe almacenarla en los medios que correspondan; para esto, tiene que agrupar los medios según la estrategia definida. Por ejemplo, podemos definir un grupo de cintas de backup para cada día de la semana; según esta configuración, nuestro servidor de backup debe solicitarnos la cinta de acuerdo al día en el que se ejecutan las copias de respaldo.

Catalogar las copias de seguridad

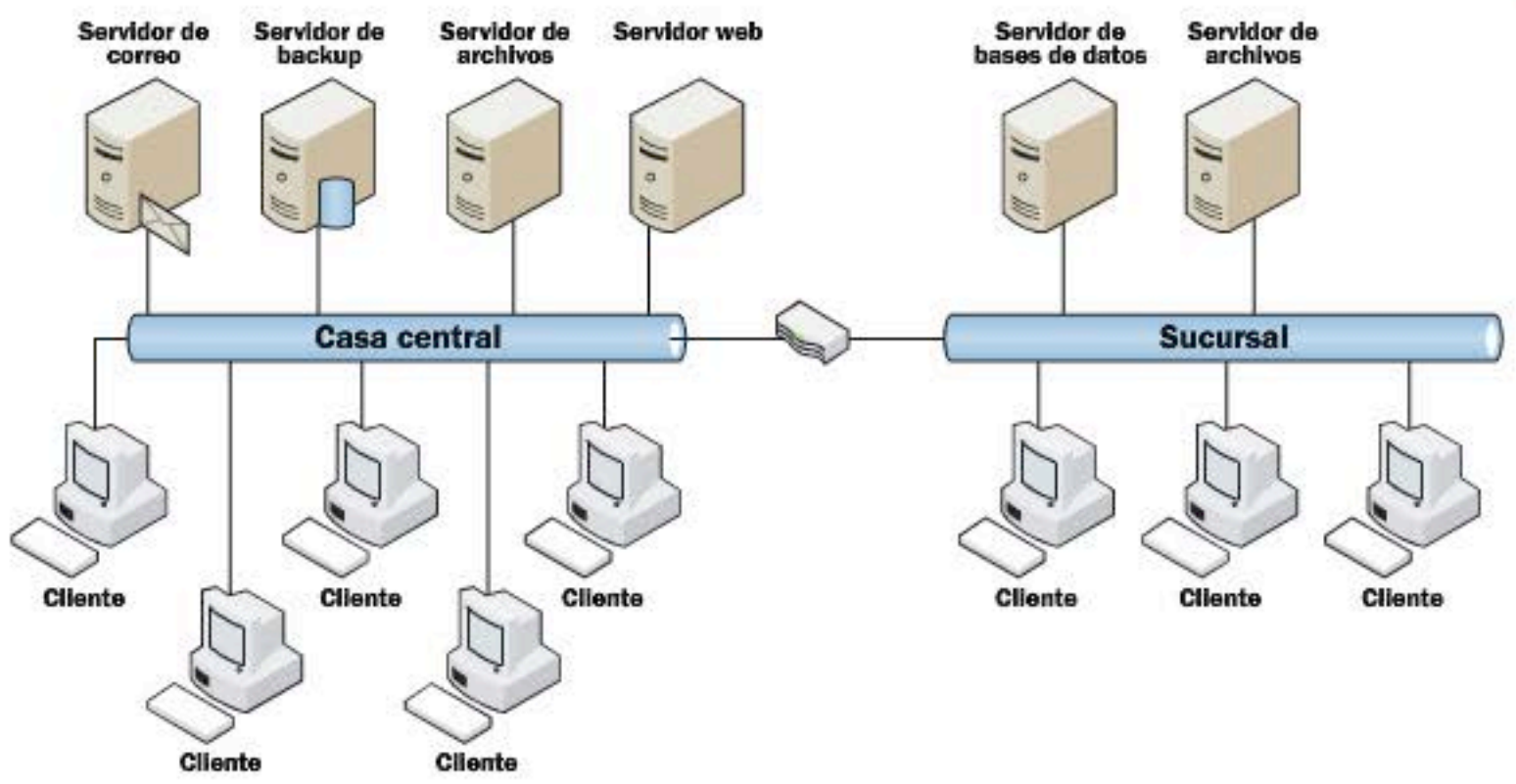
En el momento menos pensado, tendremos que recurrir a nuestras copias de seguridad. En ese instante, lo que no deseamos es tener incertidumbre acerca del medio en el que se encuentra la información que necesitamos recuperar.
El servidor de backup debe llevar un catálogo detallado en el que se registre qué información se halla en cada medio de almacenamiento y a qué fecha corresponde; de ese modo, nos permite localizar la información que necesitamos restaurar en el menor tiempo posible, optimizando los tiempos de ejecución y ofreciendo un entorno más eficiente para encontrar las copias.

Dirigir la ejecución del proceso

Como sabemos, nuestra red puede contar con múltiples sitios y una gran cantidad de servidores con sistemas operativos distintos. Es necesario que nuestro servidor de backup coordine las tareas de copias de respaldo entre los distintos orígenes de datos y los dispositivos que tienen la finalidad de transferir las copias a los medios de almacenamiento finales.
Para definir los parámetros que necesita nuestro servidor de backup para coordinar las tareas de copia de seguridad en nuestra red, es necesario que configuremos la programación de las tareas, indicando al menos la periodicidad en las que se realizan las copias, el tipo de backup y el listado de la información que se deberá transferir desde cada servidor a los medios de almacenamiento.

Conclusión

Cuando nuestra infraestructura pasa a tener una cantidad importante de servicios, servidores y computadoras conectadas, aumentarán las exigencias relacionadas con la disponibilidad de los servicios que brindamos. En estos casos, es imprescindible que contemos con equipos especializados para implementar nuestra estrategia de copias de seguridad, esto nos permitirá recuperar los servicios en el caso de que ocurra algún evento no deseado o un problema que afecte a un grupo de servicios o a un servidor completo. ■



En este diagrama vemos una red con dos sitios, en la cual se implementó la estrategia de copia de seguridad centralizada en un servidor, que se encarga de las copias de seguridad de ambas redes.

Tipos de backup

Una correcta definición de los tipos de copias de respaldo es fundamental para aprovechar al máximo los recursos de nuestro esquema de backup.

Una vez que tenemos instalado el software de backup, definidos los equipos que contienen la información que necesitamos respaldar y establecidos los grupos de archivos por copiar, es necesario que definamos los parámetros que implementarán nuestra estrategia de copia de seguridad.
Una de las opciones más importantes que deberemos definir es qué tipo de backup realizamos; a continuación, se describen las diferentes opciones.

Backup completo

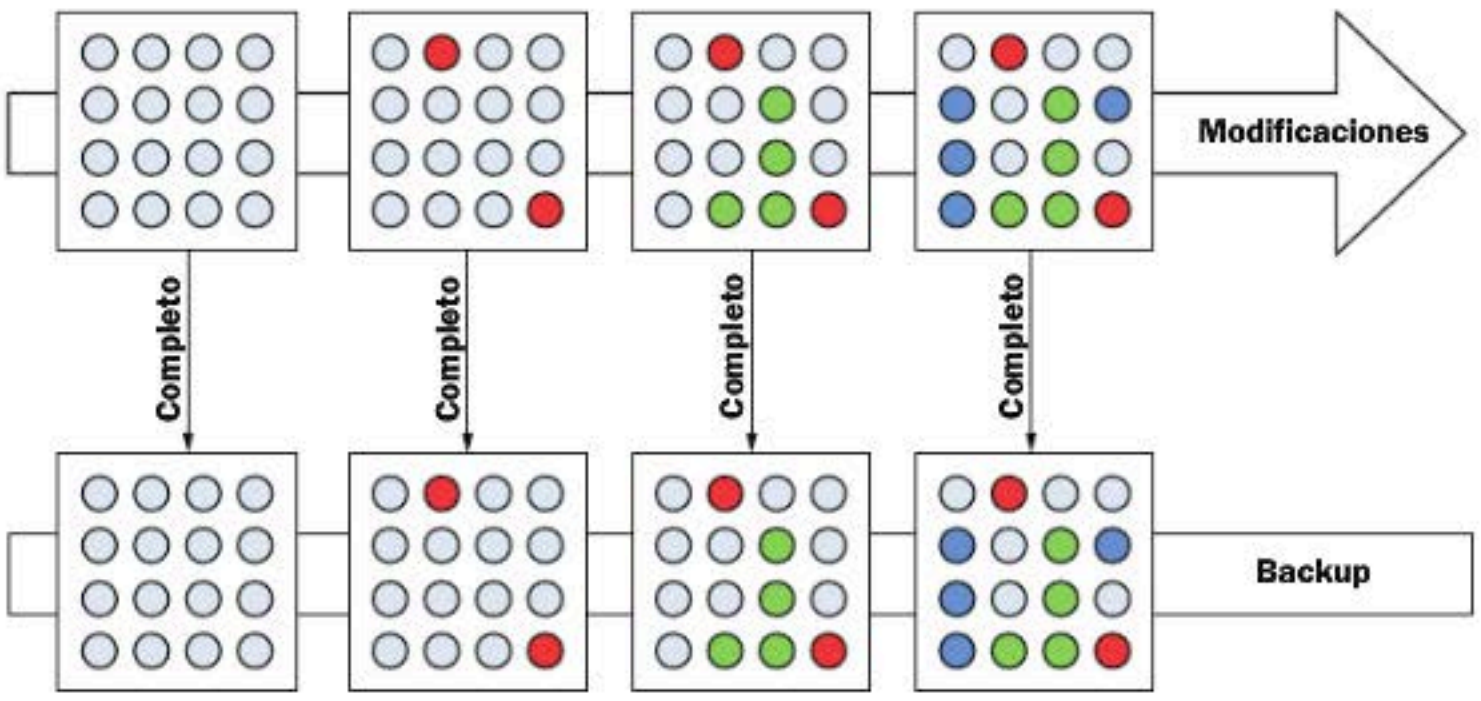
Se trata del método más simple para realizar nuestras copias de seguridad. Consiste en efectuar la copia completa de un grupo de objetos especificado. Por ejemplo, si tenemos que copiar una carpeta que contiene un conjunto de archivos, mediante el backup completo realizamos la copia de todos los archivos, independientemente de si han sido modificados o no. Este tipo de backup es el que, por lo general, implementamos cuando realizamos las copias de respaldo de forma manual, ya que solo es necesario utilizar las funcionalidades básicas que nos brinda el sistema operativo.

LOS DISTINTOS TIPOS DE BACKUP PERMITEN APROVECHAR LOS RECURSOS AL MÁXIMO.

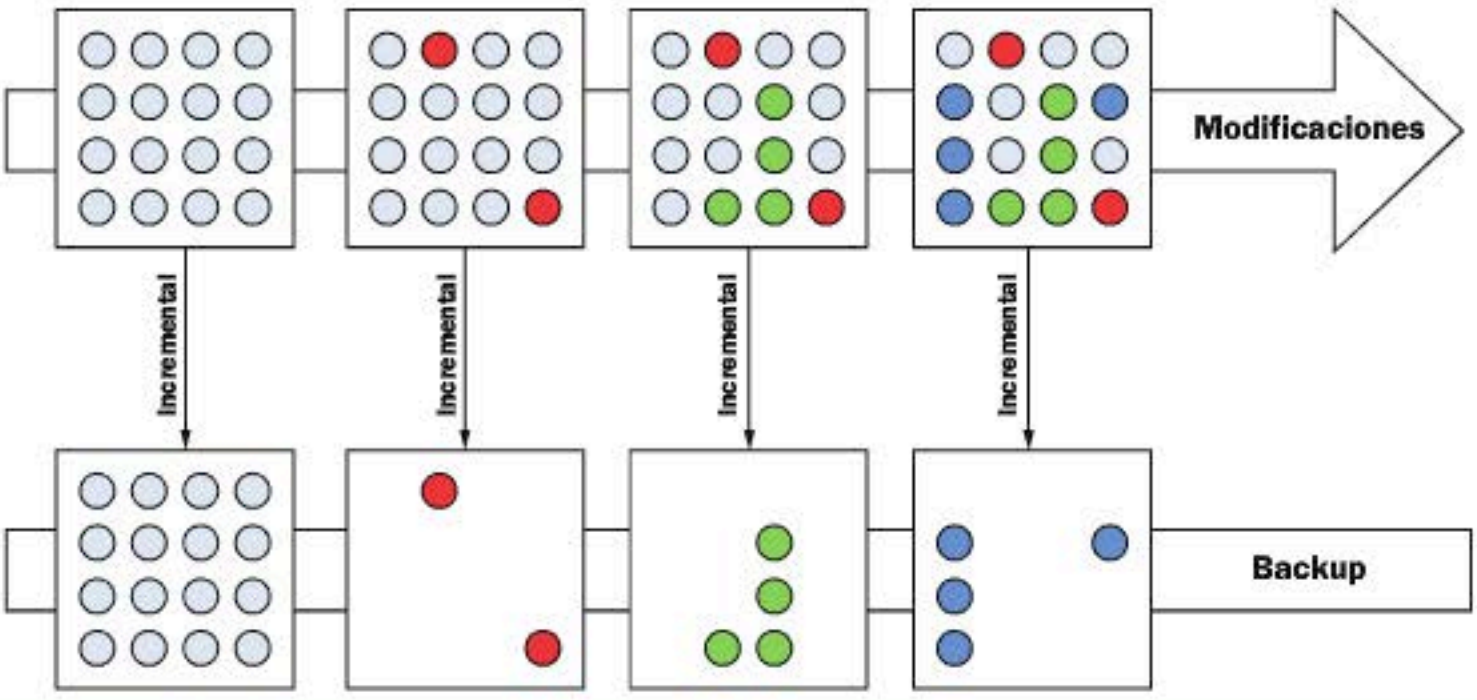
Las principales ventajas de este tipo de backup son la facilidad con la que se implementa, así como también la simpleza con la que se recuperan los datos, dado que siempre tenemos la copia completa en un solo medio. Como desventaja podemos mencionar que, para volúmenes de datos importantes, el tiempo que se tarda en realizar la copia y el tamaño del backup que resulta hacen que esta no sea la opción más adecuada.

Backup diferencial

Cuando el volumen de información que tenemos que resguardar aumenta, el modelo de backup completo puede no ser el más adecuado, sobre todo si en el grupo de objetos a los que les realizamos la copia de seguridad existe una gran proporción que no sufre modificaciones con frecuencia.
El backup diferencial realiza la copia de los objetos que sufrieron modificaciones desde el último backup completo. Debido a que es necesario registrar los datos de los objetos que copiamos para



Aquí vemos un esquema del backup completo, en el que se puede apreciar la forma en que se realiza una copia de la totalidad de los objetos que fueron seleccionados para la creación de la copia de seguridad.



En este diagrama vemos una demostración del backup de tipo incremental, en el que se copian solamente los objetos que sufrieron cambios desde la realización de la última copia de seguridad.

realizar luego el cálculo de cuáles son los que sufrieron modificaciones, necesitamos software específico de backup para realizar este tipo de copias de respaldo.
Esta clase de backup, al transferir solo los objetos modificados, produce copias de seguridad que ocupan menos tamaño que las de tipo completa y, por consiguiente, se copian en menos tiempo.
La principal desventaja es la complejidad en la recuperación ya que, para realizar una recuperación del grupo completo de objetos a la versión más reciente, necesitaremos el medio que contiene el backup completo y el medio que almacena el último backup diferencial del grupo de objetos por restaurar.

Backup incremental

El tipo de backup incremental es similar al de tipo diferencial; lo único que cambia es que, en este caso, se copian los objetos que fueron modificados teniendo en cuenta el último backup, sin importar si la última copia de respaldo fue del tipo completa, diferencial o incremental.
Al igual que en el caso del backup diferencial, el tipo de backup incremental se lleva a cabo mediante software específico de backup. Su ventaja es que genera las copias de seguridad más rápido y tiene como resultado backups de menor tamaño que las otras dos alternativas.
La desventaja de este tipo de backup reside en que es el que tiene la recuperación más compleja ya que, en el caso de que debamos restaurar un grupo completo de objetos, necesitaremos, en el peor de los casos, el medio que contiene el último backup completo y todos los medios que contienen las copias de seguridad del tipo incremental, para poder realizar la recuperación.

Aspectos para tener en cuenta

En el momento de definir el tipo de backup que realizaremos para cada grupo de objetos por copiar, debemos tener en cuenta algunos aspectos básicos; a continuación, se detallan los más importantes. Quizás el aspecto más relevante que es necesario tener en cuenta a la hora de decidir el tipo de backup para un grupo de objetos sea el espacio que ocupa. Si el tamaño del grupo de objetos no es significativo, la opción más recomendada es siempre realizar backups completos; a medida que el tamaño del grupo de objetos aumenta, comenzaremos a considerar el uso de un esquema mixto, entre copias de respaldo del tipo completas y también copias del tipo diferenciales o incrementales.
Otro factor que condiciona la elección del tipo de copia de seguridad por realizar es la capacidad de los medios a los que vamos a transferir el backup. Si la capacidad del disco duro, cinta de backup, DVD o CD al que vamos a transferir nos resulta suficiente, podemos optar por realizar todas las copias en el modo completo, de lo contrario debemos plantear un esquema mixto.
La frecuencia en la que se modifican los datos nos define si es conveniente o no optar por copias del tipo diferencial o incremental si el volumen de la información y la capacidad de los medios lo justifican. En el caso de que, en un grupo de archivos, la mayor parte de ellos sufra modificaciones en forma continua, las copias del tipo diferencial o incremental tendrán un tamaño similar a las del tipo completo, por lo que en algunos casos nos conviene realizar solo copias del tipo completo, ya que las ventajas relacionadas con el espacio ocupado por el backup son mínimas.

Conclusión

Debemos ser cuidadosos al definir los diferentes tipos de backup que utilizaremos para implementar nuestra estrategia de copia de seguridad. Teniendo en cuenta cada uno de los aspectos que conocimos y analizamos hasta aquí, lograremos crear una configuración óptima de copias de seguridad, que se encargue de aprovechar al máximo los recursos disponibles y que, además, nos permita recuperar la información que necesitamos en el menor tiempo posible. ■

Soporte de los backups

Tener una copia de la información de una empresa es clave para recuperar datos en situaciones imprevistas o frente a errores humanos; aquí conoceremos los diversos soportes disponibles.

Si bien sobre este tema hay mucha información y programas, nos vamos a enfocar en el ámbito empresarial. Antes de realizar una copia de seguridad de información, hay que ver realmente qué es lo importante para realizar la copia de respaldo ya que, el espacio que necesitamos podría ser considerable. En una empresa que cuenta con tres PCs, pero no tiene servidor, quizás, el backup se realice de forma manual en un disco externo; sin embargo, cuando hablamos de un gran número de PCs, con información confidencial, esto se vuelve engorroso, no productivo y consume horas laborales del departamento de sistemas.
Al hablar de servidores basados en plataformas Windows (2003, 2008, 2012) y también Linux, si bien hay herramientas que realizan este trabajo, es recomendable usar un script que controle tanto la copia de archivos como su compresión (para ahorrar espacio), el envío de e-mails y su borrado cada cierto período. Para ello, vamos a necesitar dos programas: uno llamado **Robocopy**, que permite solo la copia de los archivos modificados, con log incluido; y también **Postie**, un pequeño cliente SMTP para el envío de correo.

Las cintas pueden guardar más información y en menos tiempo.

Implementación

En primer lugar, creamos un archivo de extensión .BAT, en el cual escribiremos las líneas de código que nos permitirán controlar las tareas de respaldo.
A continuación, vemos un ejemplo de este archivo; sus líneas se pueden modificar dependiendo del tipo de backup y de las necesidades específicas:

```
@echo off
setlogbakdiarios="E:\gyb\Tareas
Programadas\Logs\%1_LogBackup_
po12.txt"
setlogerror="E:\gyb\Tareas
Programadas\Logs\ERROR.txt"
set origen="E:\backup\temp\
documentos"
set destino="E:\backup\%1\
documentos"
set origen2="E:\backup\gb_admin"
set destino2="E:\backup\%1\gb_admin"
```

▶ Para establecer la fecha como nombre de archivo:

```
for /f "tokens=1-2 " %%A in ('DATE
/T') do set datedia=%%A
for /f "tokens=1-3 delims=/" %%A in
('echo %DATEDIA%')
do set datedia=%%A-%%B-%%C
```

Respaldo completo

Si bien el respaldo de la información es crucial, muchas veces el backup del entorno también lo es, ya que trae problemas a la hora de restaurarlo. Un ejemplo de esto son las máquinas virtuales o servidores de base de datos. Esto quiere decir que, en máquinas virtuales, está bien hacer un backup del disco, pero a la hora de restaurarlo también hay que crear la máquina virtual con las mismas especificaciones que tenía, si no, cuando se restaura el disco, es probable que tenga problemas de incompatibilidad o paquetes sin instalar.

▶ Comienzo de backup:

```
%logbakdiarios%
echo. >> %logbakdiarios%
```

▶ Mostrar la fecha y la hora:

```
echo. >> %logbakdiarios%
echo ************************** >> %logbakdiarios%
echo * %DATE% %TIME% * >> %logbakdiarios%
echo ************************** >> %logbakdiarios%
echo. >> %logbakdiarios%
```

▶ Backup de sistema:

```
robocopy E:\gyb\ E:\backup\temp\gyb /MIR /e /copy:D
/R:1 /W:1 /NP >> %logbakdiarios%
```

▶ Creación de los archivos comprimidos:

```
7za.exe -ssw -tzip -r a %destino2%\gb_admin.zip
%origen2%\ >> %logbakdiarios%
del /q origen2%\*.* >> %logbakdiarios%
```

▶ Backup de documentos:

```
robocopy E:\documentos\ E:\backup\temp\documentos /
MIR /e /copy:D /R:1 /W:1 /NP >> %logbakdiarios%
```

▶ Compresión de los logs:

```
7za.exe a ..\Logs\%datedia%.zip %logbakdiarios%
::Busqueda de errores
::FIND /N "ERROR " %logbakdiarios% > %logerror%
```

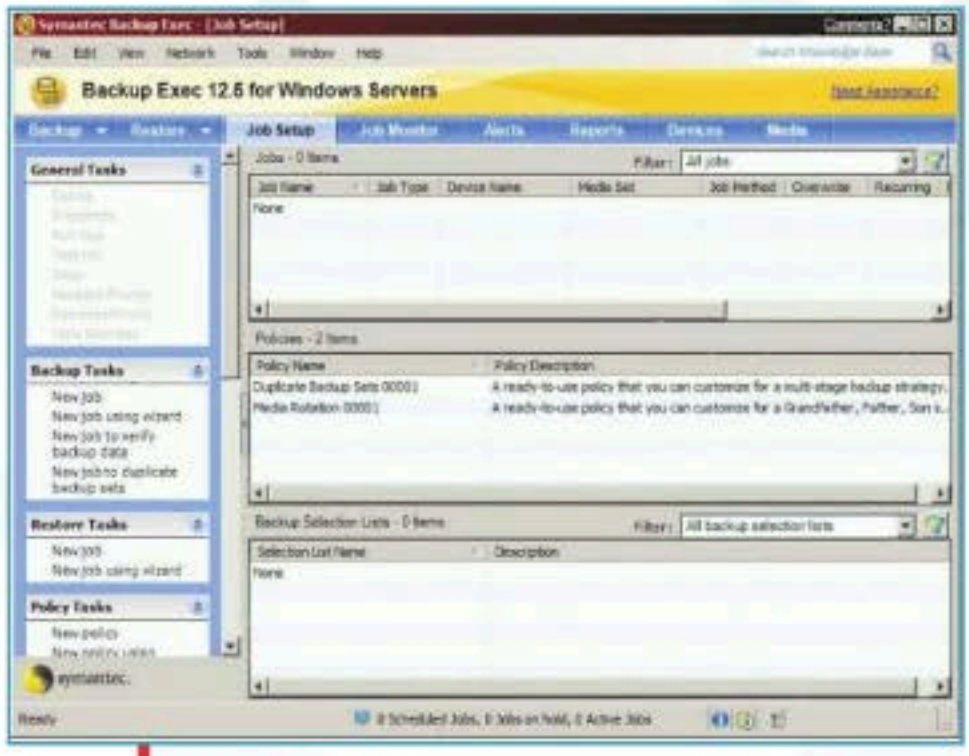
▶ Envío de e-mail:

```
postie.exe -esmtp -host:mail.gbconsulting.com.
ar -user:backups@consultora.com.ar -pass:xxxxxxx
-to:soporteit@consultora.com.ar -from:backups@consultora.
com.ar -s:"Empresa- Backup del %date%" -msg:"Reporte de
backup del servidor Empresa" -a:"E:\ \Tareas Programadas\
Logs\%datedia%.zip"
del /q %logbakdiarios%
```

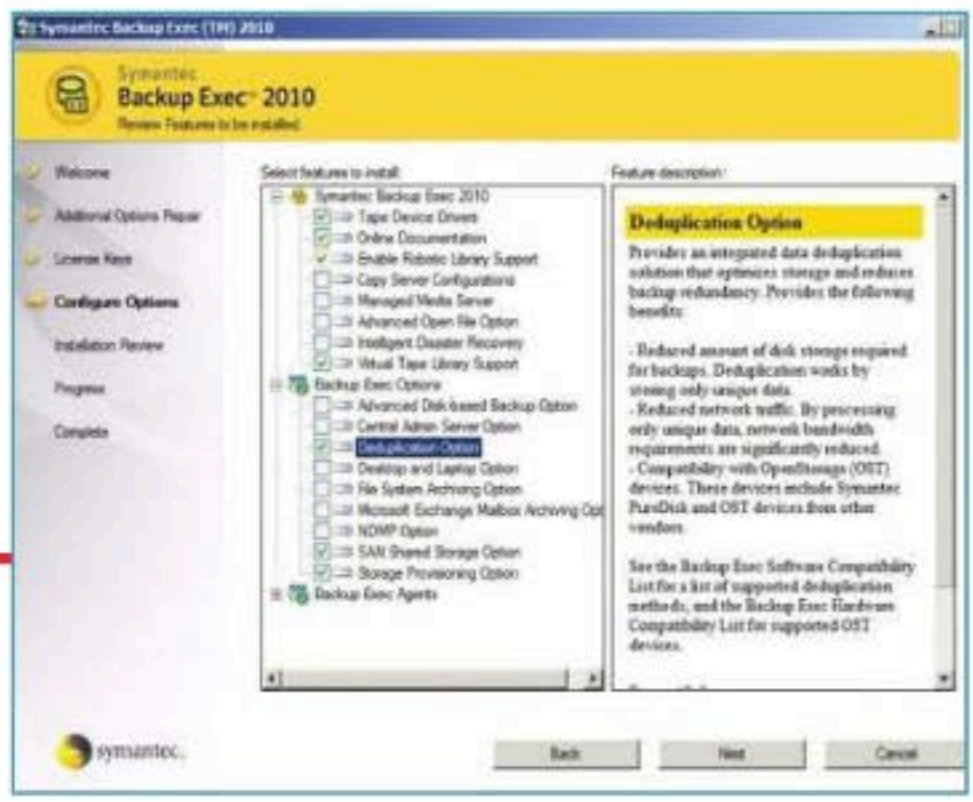
Como se puede ver, en primer lugar se copian los archivos a una carpeta temporal y, luego, sobre esa carpeta, se realiza la compresión. Al finalizar esto, el script nos envía un e-mail con el reporte del backup comprimido.

Otras soluciones

Existe una gama de herramientas muy importantes, pero la más recomendable es **Symantec Backup Exec**, que cuenta además con la integración a diferentes aplicaciones propias de entornos corporativos o **Pymes**. Es muy configurable en cuanto a los períodos de backups y la forma en que estos se hacen. Actualmente, los medios en los cuales se realizan copias de seguridad son bastantes. Los más difundidos por su redundancia en seguridad en cuanto a información son los discos duros internos, con métodos de redundancia RAID. Luego, tenemos medios externos que nos facilitan esta tarea y su transporte: discos duros portátiles y cintas, los cuales pueden tener una capacidad de almacenamiento igual o superior a un disco duro interno, pero que poseen un grado mayor de durabilidad. Si bien son más recomendables las cintas por su duración, tenemos que disponer de una unidad de cinta a la hora de restaurar, por lo que debemos invertir en este dispositivo. ■



Con el uso de Symantec Backup Exec, las opciones de administración resultan sencillas y amigables para el usuario.



Symantec Backup Exec se adapta fácilmente a una gran cantidad de plataformas y sistemas físicos.

Software para backup corporativo

El software de backup es una de las partes fundamentales de un correcto planeamiento tecnológico que se adapte al corazón de nuestra empresa; aquí conoceremos algunas opciones.

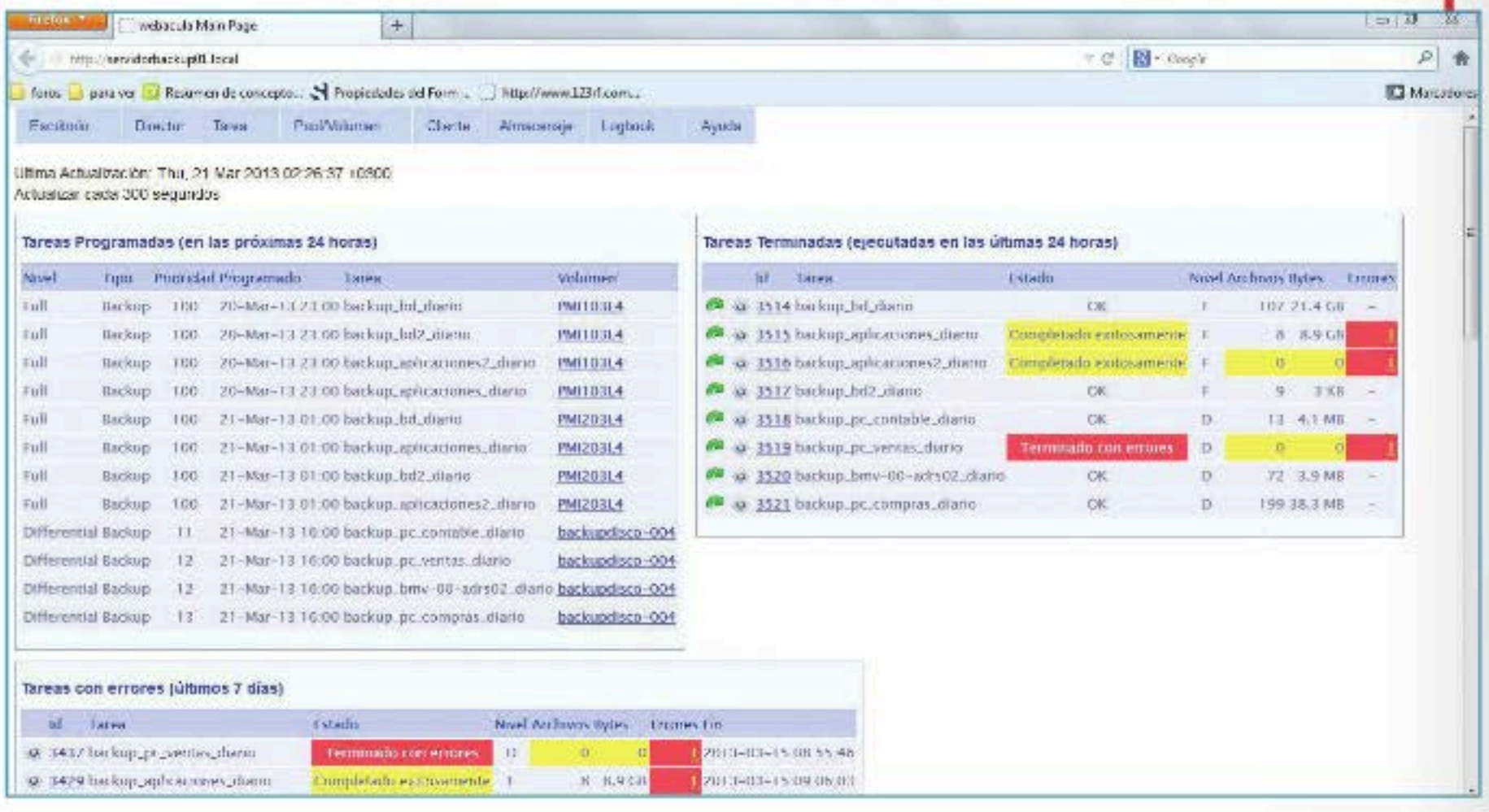
Una vez que tenemos el servidor y el hardware de backup destinado a implementar nuestra estrategia de copias de respaldo, necesitamos el software que se encargue de hacerla funcionar. Existe una gran cantidad de alternativas posibles; aquí analizaremos la herramienta **Symantec Backup Exec**, como representante de las aplicaciones comerciales, y el paquete **Bacula**, del mundo del software libre.

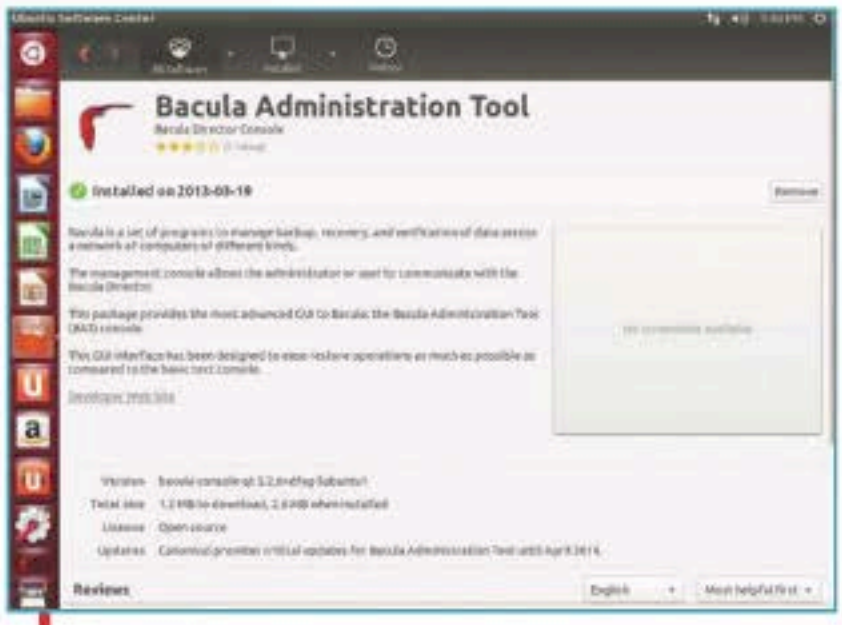
Symantec Backup Exec

La empresa **Symantec**, reconocida en todo el mundo, desarrolla la herramienta **Backup Exec**, la cual implementa una solución de backup que apunta a integrar las copias de respaldo de los servidores de archivos, los equipos con bases de datos, y los servidores dedicados a las tareas de virtualización.

En Backup Exec, básicamente existen los roles de servidor de multimedia (**Media Server**) y servidor de backup (**Backup Server**). Durante los trabajos de copias de respaldo, la información es transferida desde los servidores de multimedia hacia los servidores de backup, desde donde es enviada hacia los medios correspondientes. En la solución Symantec Backup Exec, los servidores de backup almacenan la información relacionada con el catálogo de backup en bases de datos que utilizan tecnología Microsoft SQL Server en cualquiera de sus versiones (podemos utilizar la versión Express, que es gratuita, o las versiones pagas,

La aplicación Webacula permite administrar el paquete Bacula mediante una interfaz web.





Bacula se encuentra disponible en los repositorios de las principales distribuciones GNU/Linux.

como por ejemplo la denominada Standard o Enterprise). Las ventajas de esta aplicación son las siguientes:

▶ **Integración:** debido a la interacción con los fabricantes de tecnología y las más importantes empresas de desarrollo de software, Backup Exec posee una mejor integración con el hardware de servidores y de dispositivos de backup, con los sistemas operativos, las bases de datos y los sistemas de virtualización; por ejemplo, nos permite realizar copias y restauración de sistemas operativos Windows Server completos y copia de respaldo a nivel de objetos de una base de datos SQL Server o de una máquina virtual VMWare.

▶ **Programación de tareas avanzada:** desde la versión 2012 de Backup Exec, es posible implementar las copias de seguridad mediante flujos de trabajo, los cuales permiten combinar distintos tipos de tareas en la definición de un trabajo de backup; por ejemplo, se puede configurar un flujo de trabajo, para que se realice la copia de seguridad primero a un disco duro y, luego, se la convierta a una máquina virtual alojada en un servidor de virtualización de respaldo.

La desventaja se relaciona con su costo. En el caso de que decidamos implementar nuestra estrategia de backup mediante Symantec Backup Exec, debemos tener en cuenta los costos de las licencias correspondientes para nuestro proyecto. En esencia, el esquema de licenciamiento es por cada servidor y por cada equipo desde el que tengamos que transferir información.

Bacula

Desarrollado por una gran comunidad de programadores, el software de backup **Bacula** ofrece una solución de nivel empresarial con el objetivo de implementar un esquema robusto de copias de respaldo. Dentro de su esquema, existen tres tipos de roles para los equipos que participan: **director**, **servidor de almacenamiento** y **servidor de archivos**.

▶ **Director:** los equipos con el rol de directores son los encargados de coordinar las copias de seguridad desde los servidores de archivos hacia los servidores de almacenamiento siguiendo un cronograma establecido e indicando los parámetros según los cuales se realizará cada copia de respaldo, por ejemplo, el nivel de backup.

▶ **Servidor de almacenamiento (Storage Daemon):** aquellos equipos a los que asignamos el rol de servidores de almacenamiento son los que tienen la capacidad de recibir la información desde los servidores de archivos, y almacenarlos en los medios que correspondan.

▶ **Servidor de archivos (File Daemon):** a los equipos en los que se ubican los objetos (por ejemplo archivos o bases de datos) que necesitamos respaldar, se les asigna el rol de servidor de archivos. Durante los trabajos de backup, se transferirá información desde los servidores a los equipos.

Las ventajas de esta aplicación son las siguientes:

▶ **Licencia libre:** Bacula es libre de costos de licenciamiento, y permite modificar el código en caso de ser necesario.

▶ **Flexibilidad:** si bien la administración de la herramienta se realiza nativamente mediante una consola en modo texto, existen múltiples herramientas web y de escritorio que nos permiten administrar el paquete Bacula mediante una interfaz gráfica; un ejemplo es la herramienta PHP, Webacula.

Conclusión

Si bien la decisión sobre la mejor alternativa para realizar las tareas de backup estará fuertemente influenciada por el presupuesto asignado a nuestro proyecto de copias de seguridad, debemos también tener en cuenta si las ventajas de las alternativas pagas son productivas para nuestro escenario, y si la alternativa seleccionada es compatible con nuestro hardware de servidor y dispositivos de backup. Otra sugerencia, en caso de optar por una alternativa libre, es asegurarnos de contar con los recursos humanos que hagan posible el despliegue de la solución. ■

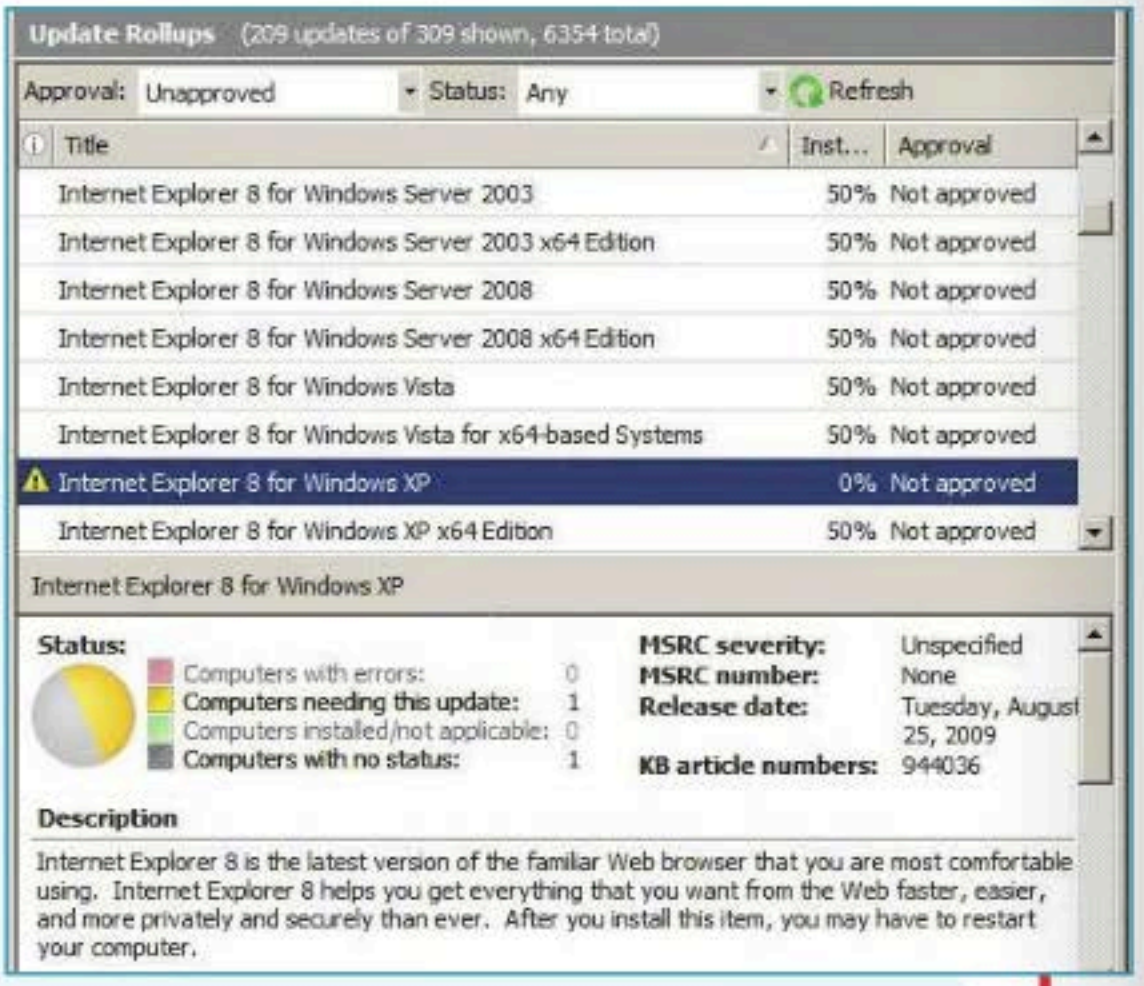
Sitios de interés

Dos sitios que no podemos dejar de visitar son las páginas web oficiales del paquete Bacula (www.bacula.org) y del sistema de backup Symantec Backup Exec (www.symantec.com), en las cuales encontraremos cientos de ejemplos de configuraciones y las respuestas a las preguntas más frecuentes, así como también los manuales en línea y el listado de dispositivos de backup que son compatibles con ambas herramientas.

Servidores de actualización

Mantenernos actualizados, hoy en día, es clave para estar a la vanguardia de las nuevas implementaciones, evitando bugs y vulnerabilidades.

Estamos ante un mundo muy cambiante en el cual, día a día, aparecen nuevas implementaciones, hardware y descubrimientos de vulnerabilidades que ponen en situación riesgosa nuestro sistema e infraestructura informática.
En este caso, vamos a revisar el concepto de servidor de actualización tanto de Windows como en sistemas GNU/Linux. De esta forma, conoceremos sus principales características y, también, las opciones que tenemos a nuestra disposición para implementar un servidor de este tipo.



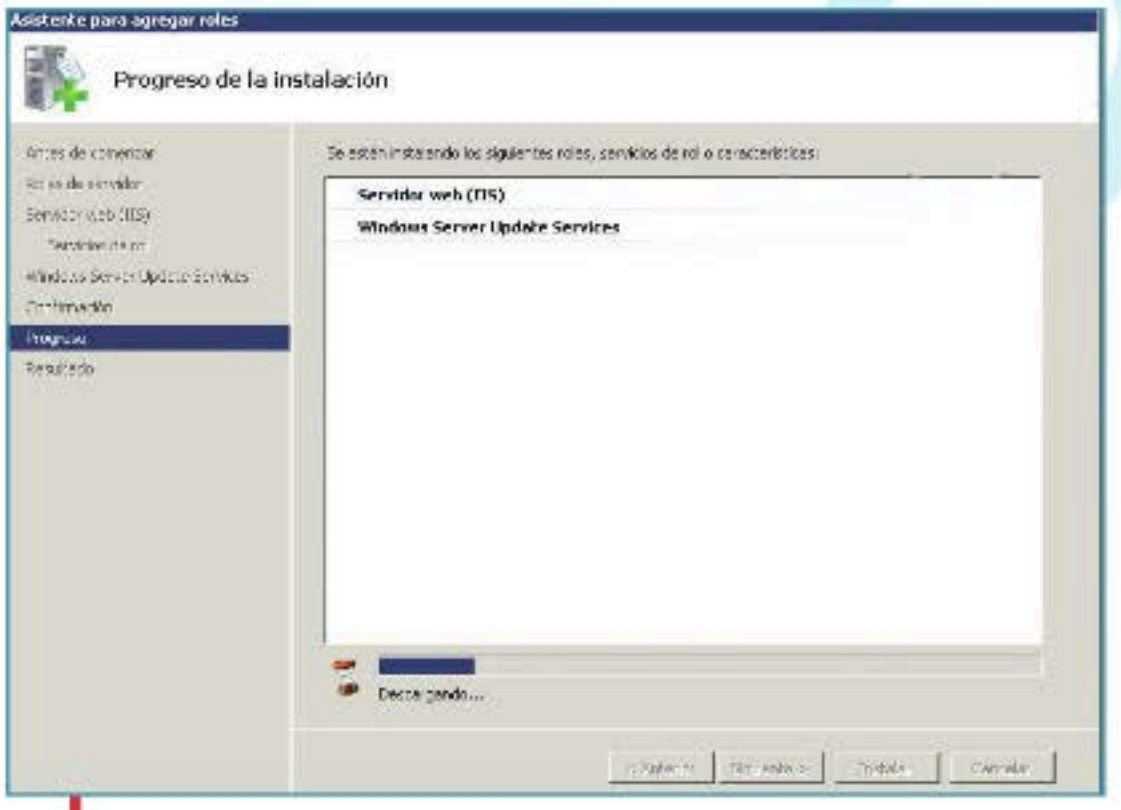
Sistemas Windows

Para el caso de **Windows Server** (2003 R2, 2008 R2 y 2012), uno de los roles que se instalan para implementar un servidor de actualizaciones es **Windows Server Update Services**, el cual permite a los administradores de red especificar las actualizaciones de Microsoft que se deben instalar, crear grupos separados de equipos para los diferentes conjuntos de actualizaciones y obtener informes sobre los niveles de compatibilidad de los equipos y actualizaciones que se deben instalar. Esto permite optimizar el funcionamiento de la red y obtener un entorno controlado. Una vez instalado

> Es fácil la distribución de actualizaciones en equipos del dominio.

Actualizaciones

Si bien la actualización del sistema operativo con los últimos paquetes es una práctica que se recomienda para favorecer el rendimiento y preservar la seguridad, no siempre ocurre esto. Muchas veces, los paquetes se instalan mal o tienen problemas de versionado y ocasionan problemas, como lentitud del sistema o la no carga de la plataforma, por lo que nunca hay que borrarlos manualmente, sino desinstalándolos del asistente de Microsoft o usando alguna herramienta. Siempre hay que elegir con cuidado qué se va a instalar, y en qué sectores o áreas va a repercutir cada cambio.



La instalación de Windows Server Updates Services es sencilla; requiere IIS incluido en Windows Server en todas sus versiones.

el rol desde Windows Server, debemos acceder a las opciones de administración de nuestro servidor; allí especificamos qué tipos de actualizaciones se destinarán para determinados equipos. No se trata de una tarea compleja, ya que Windows Server nos entrega un completo asistente que nos orientará durante su configuración.

EN EL APARTADO DIST DEBEMOS ESPECIFICAR QUE DISTRIBUCIONES SE REPLICARÁN.

Sistemas GNU/Linux

En entornos GNU/Linux, la actualización es más compleja, ya que requiere que realicemos algunos pasos previos para que las computadoras hagan uso del servidor de actualizaciones ubicado en la red LAN. El objetivo es lograr que todos estos paquetes puedan ser leídos por las otras máquinas. Para ello, utilizaremos el comando **apt-move**. Básicamente, esta herramienta toma una serie de paquetes **.DEB** de cualquier sitio y los inserta en una estructura con la misma jerarquía que un espejo de Debian. Lo primero que debemos hacer es instalar el paquete **apt-move**, para esto utilizamos el comando **apt-getinstallapt-move**.

El siguiente paso consiste en configurar el archivo **/etc/apt-move.conf**, aquí debemos cambiar una serie de valores para que funcione en forma correcta.

En la variable **APTSITES**, especificamos los sitios de **sources.list** que estarán disponibles. Un ejemplo del archivo **sources.list** es el siguiente:

ftp://ftp.us.debian.org/debian/ unstablemain non-free contribdeb http://non-us.debian.org/debian-non-US unstable/non-US maincontrib non-free

La variable **APTSITES** podría definirse como **ftp.us.debian.org non-us.debian.org**; recordemos que los sitios especificados deben estar separados por espacios.

En la variable **ARCHS**, especificamos las arquitecturas que queremos replicar; para una arquitectura Intel escribimos lo siguiente: **ARCHS="i386"**. En **LOCALDIR**, ingresamos el directorio que va a contener el espejo que crearemos. Por ejemplo **/mnt/disk2**. Este directorio debe ser accesible por HTTP, FTP, NFS o SMB, por cada uno de los clientes de la red. Para ello, podemos utilizar un servidor Apache en **/var/www**; en ese directorio, creamos un enlace (**ln -s /var/www/apt /mnt/disk2**) al directorio **LOCALDIR**, de forma que una petición **http://192.168.0.1/apt** devolvería el contenido de **LOCALDIR**.

En el apartado **DIST** especificamos las distribuciones que deseamos replicar; aquí tenemos a nuestra disposición las opciones **stable**, **unstable**, **potato**, **woody** y también **sid**.

Un ejemplo de configuración para este parámetro es el siguiente: **DIST="unstable"**.

En **PKGTYPE** especificamos qué tipo de paquetes queremos replicar: binarios, fuentes o ambos, las opciones son **binary**, **source** y **both**; solo se puede elegir una de ellas.

En **FILECACHE** y **LISTSTATE**, especificamos dónde están los archivos locales de los paquetes. Salvo que hubiésemos cambiado la configuración de **apt-get**, los valores predeterminados funcionarán de modo correcto:

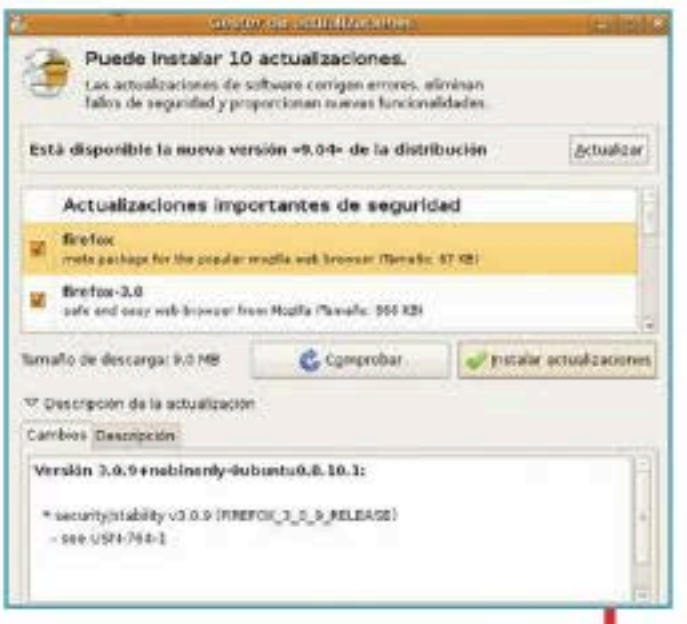
FILECACHE=/var/cache/apt/archives y LISTSTATE=/var/lib/apt/lists

Existe la opción **DELETE** que nos permite eliminar la versión más antigua de cada programa. Las opciones son **yes** o **no**.

Una vez guardados los cambios en el archivo **/etc/apt-move.conf**, podemos utilizarlo.

El procedimiento es el siguiente: en el servidor actualizamos con el comando **apt-getupdate** y **apt-getdist-upgrade**; al finalizar, tecleamos **apt-moveupdate**. En los clientes, debemos editar el archivo **/etc/apt/sources.list** de forma que en la primera línea añadiremos la ruta que hemos creado en el servidor.

Un ejemplo para esta configuración sería la siguiente línea: **deb http://192.168.27.1/apt/ distribución main non-free.** ■



Los gestores GNU/Linux como Synaptic comprueban la compatibilidad de las actualizaciones.

Servidor de antivirus

Hacer más segura la red de computadoras en una empresa es primordial para resguardar los datos. Para eso, se necesita una herramienta centralizada, capaz de prevenir y detectar diversas amenazas.

En la actualidad, sabemos que existen una infinidad de amenazas que hacen que no solo nuestros sistemas sean vulnerables, sino que nuestra información personal esté expuesta al quehacer de desconocidos. Si bien podemos tener en nuestras PCs hogareñas antivirus gratuitos, antimalware, antispyware o antiphishing, que por cierto son medidas altamente efectivas a la hora de combatir los ataques, estos recursos, aun juntos, no son capaces de brindarnos una seguridad total a nivel empresarial, y que estén centralizados para actuar en conjunto. A la hora de hablar del ámbito empresarial, estamos de acuerdo en que, en materia de seguridad, hace falta invertir en capital humano o en software. En este punto, los servidores de antivirus se hacen presentes, ya que la mayoría son comerciales. Nos permiten manipular la detección y el tratamiento de virus y malware, así como monitorear los archivos del sistema para asegurar que no sean modificados. Existen varias opciones de servidores de antivirus, aunque bajo la plataforma Windows (2003 y 2008 R2; con Active Directory), los que entregan mejores resultados son **Microsoft Forefront EndPoint Protection** y **Bitdefender Security**.

En la consola de administrador del servidor, hay una solapa de Microsoft Forefront donde vemos el estado de cada PC.

UN SERVIDOR DE ANTIVIRUS NOS PERMITE AISLAR AMENAZAS EN FORMA MÁS EFICIENTE.

Microsoft Forefront EndPoint Protection

Si bien contamos con **Microsoft Security Essential**, que es gratuito, este sirve solo para 10 PCs, y su administración no es centralizada. Al encontrarnos en una infraestructura más grande, la solución es **Microsoft Forefront EndPoint Protection**. Este producto no tiene más complejidad que su implementación, ya que la administración es muy sencilla. Simplemente tenemos que contar con una versión de **SQL Server Express** y tener en cuenta que se va a instalar solo en nuestro servidor. Una vez concluida la instalación, tenemos dos formas de acceder: vía HTTP o por la consola de administración del servidor. El servidor va a ser el único que recibirá las actualizaciones correspondientes, que luego va a distribuir en las demás PCs, mostrándonos en cuáles se pudo instalar el agente Forefront para la detección de virus o malware.

Desde la administración, podemos configurar intervalos de escaneo, actualizaciones y qué se va a hacer en cada caso al detectarse una amenaza. Es transparente para los usuarios, y ninguno de ellos puede administrarlo. En caso de detectarse una amenaza, se pueden especificar los pasos por seguir para ver de qué manera se trata sin interferir con los demás usuarios de la empresa y que tampoco noten esto, para no parar la productividad; todo se realiza de forma automatizada. Si bien, en forma predeterminada, Windows 7 y 8 en todas sus versiones posee instalado Microsoft Security Essentials, este se debe desinstalar ya que no es compatible.

Bitdefender Security

Bitdefender, por otro lado, nos muestra una solución más personalizable pero administrable, con algo de complejidad, ya que este producto también sirve tanto para plataformas Windows como Linux/Unix; en este último caso, la instalación y la configuración son un poco más complejas. Si bien la instalación en el servidor es similar a Microsoft Forefront

Endpoint, presenta una serie de complejidades en cuanto a la instalación en servidores Linux. El **Management Server** de Bitdefender proporciona una potente consola de administración centralizada para todas las soluciones de protección de puesto final, servidores críticos y puertas de enlace. Combina tanto la visibilidad a la hora de implementar políticas de seguridad en la empresa mediante la configuración remota de puntos finales, como la política de refuerzo a través de una interfaz centralizada. La instalación del agente en plataformas Linux requiere que se descargue el paquete desde el CD de instalación, luego debe ubicarse en la carpeta `/opt`, y la instalación se realiza desde una consola:

```
# sh BitDefender-Security-Mail-3. 1. 2-linuxgcc3x-i586. rpm. run.
```

En algún momento, se nos preguntará si queremos activar la integración con **Bitdefender Management Server**. Entonces, escribimos S y pulsamos ENTER. Luego hay que especificar el host de Bitdefender Management Server:

```
# cd /opt/BitDefender/bin
# . /bdsafebdem host <host[:port]>
```

A continuación, reiniciamos el producto:

```
# cd /opt/BitDefender/bin
# . /bdrestart
```

Desde este momento, vemos las soluciones instaladas para servidores Unix en la consola de administración de Bitdefender en Windows. Esta integración se puede desactivar en cualquier momento usando los comandos siguientes:

```
# cd /opt/BitDefender/bin
# . /bdsafebdem enable N
# . /bdrestart
```

Bitdefender es mucho más configurable; permite incorporarse a Active Directory y distribuir políticas con facilidad.

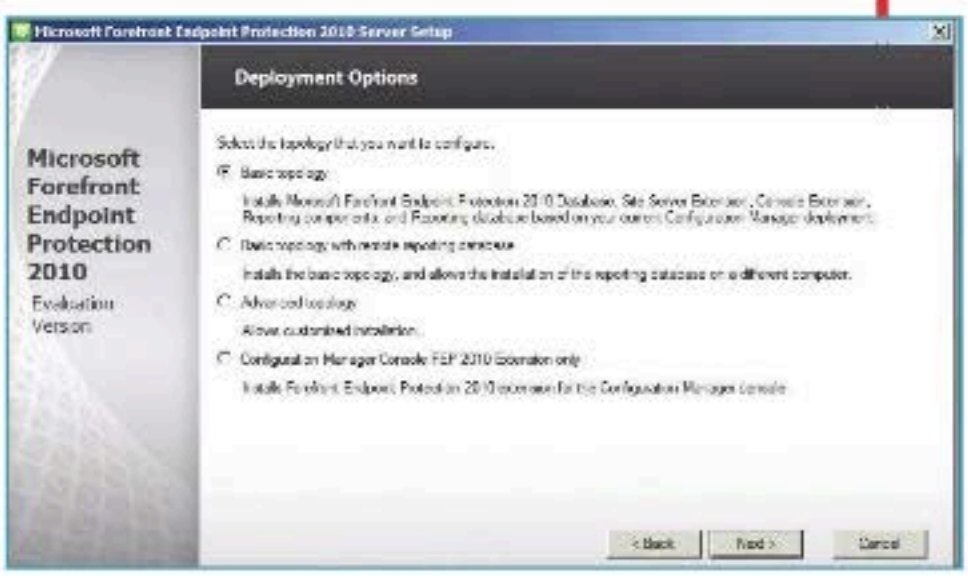
Para tener en cuenta

Siempre es necesario tener una herramienta que centralice el uso y la detección de virus o malware, pero lo más importante es no perder esa información ni que sea robada más allá del servidor antivirus que se utilice. Usando los reportes, se pueden prevenir muchas amenazas al detectar qué usuarios entran a ciertas páginas o descargan software infectado, para advertirles sobre esto o bien bloquear sus accesos. Siempre hay que tener una copia de respaldo de todos los datos, ya sea local o externa, por la posibilidad de que exista cualquier incidente.

Ventajas

Sin duda, una de las ventajas más importantes de centralizar el servidor de antivirus, malware, etc., es no solo la posibilidad de realizar su administración en forma más sencilla y eficiente, sino el rápido aislamiento de una amenaza, ya que se encargará de separarla del resto de la red, tanto LAN como WAN, sin que sea necesaria la intervención de ningún técnico o administrador de redes. Esto hace que, siempre previniendo el problema, no se pierda información alguna o que esta sea robada, ya que es lo más valioso para una empresa. Este trabajo tiene que estar acompañado por una buena planificación y un diagrama de infraestructura de la red, para que esté completamente segura y no haya ningún agujero. Así, vemos que la implementación de un servidor de antivirus ofrece un nivel mayor de seguridad y eficacia en la respuesta a posibles amenazas, ya que será capaz de actuar en forma centralizada y programada. ■

Al instalar **Microsoft Forefront Endpoint Protection**, seleccionamos la topología básica; la segunda opción sirve para un servidor de bases de datos dedicado.



Servidores proxy

En estas páginas, conoceremos en profundidad qué son y para qué sirven los servidores proxy; además, veremos sus opciones y ventajas.

Cuando Internet comenzaba a ampliar sus horizontes, nuestras máquinas se conectaban a la Web con direcciones IP públicas y, más allá de eso, nadie se preocupaba por la seguridad. En la década de los 80, con la adopción por parte de ARPANET del protocolo TCP/IP, dividimos las redes en distintas clases; de cada una se separaron redes especiales de carácter privado. Estas redes privadas se crearon para evitar la exposición de los equipos de las organizaciones. Las redes creadas, y que actualmente utilizamos, se clasifican en tres tipos: A, B y C. Cada una tiene lo que se denomina una **máscara de subred**, lo cual permite subdividirla en varias redes más pequeñas (para que podamos manejar mejor la administración de las máquinas y las direcciones).

Conexión a Internet

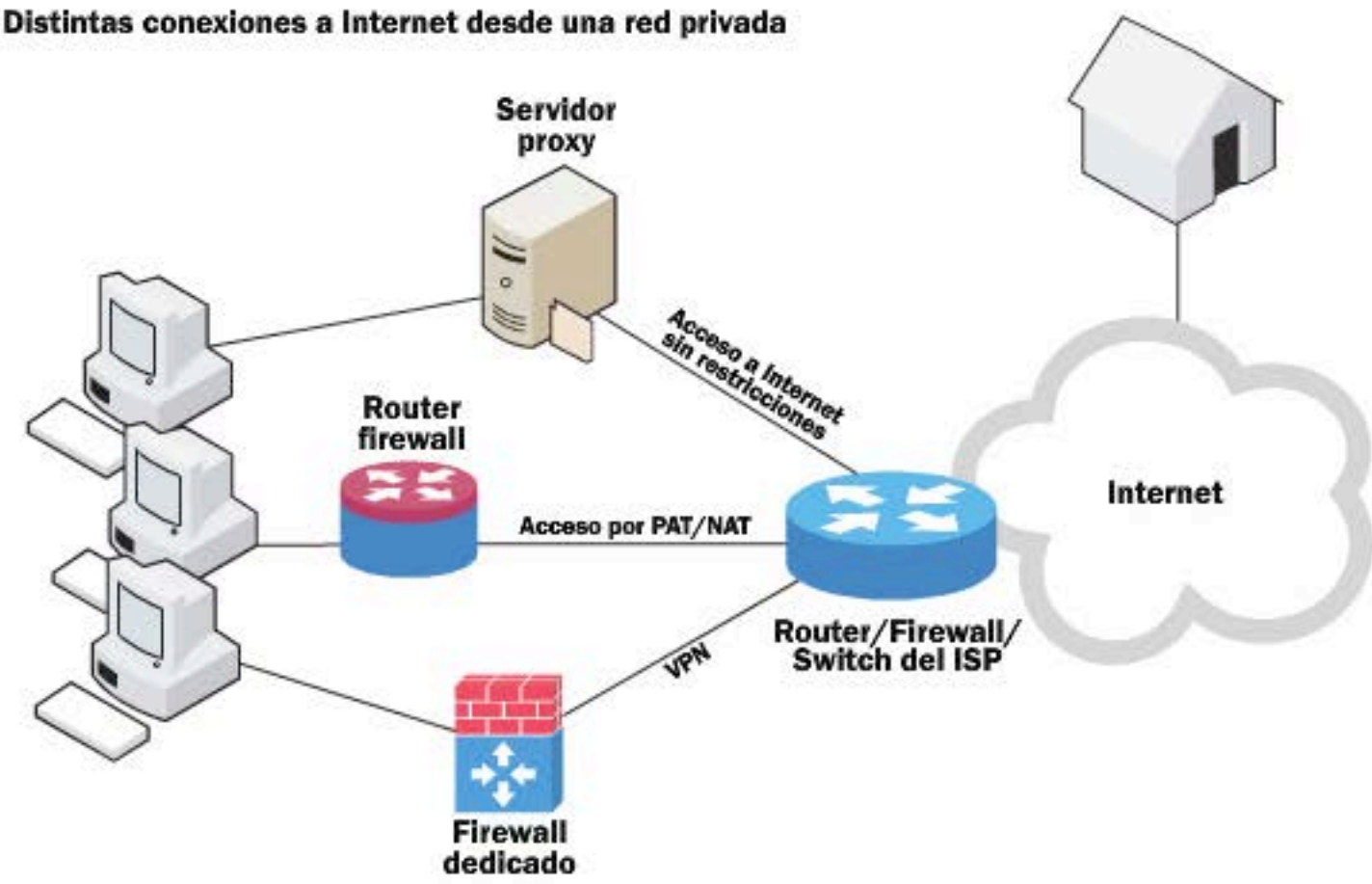
Para conectarnos a Internet, utilizamos varias técnicas de networking entre las que se encuentran **NAT/PAT** (*Network/Port Address Translation*) en firewalls, **VPN** (*Virtual Private Network*) y **proxies**. Estos últimos tuvieron auge en la década de 1990 con el protocolo HTTP y su consecuente expansión debido al éxito comercial que tuvo la WWW (*World Wide Web*).

LAS REDES PRIVADAS FUERON CREADAS PARA EVITAR LA EXPOSICIÓN EN INTERNET, DE LOS EQUIPOS QUE PERTENECEN A ORGANIZACIONES.

Proxy

Proxy significa **intermediario**, y su acepción la utilizamos en distintos ámbitos como sinónimo de *representante*; y es que la

Distintas conexiones a Internet desde una red privada



Esquema donde se pueden ver los tres tipos de conexión a Internet: por NAT-PAT a través de un firewall, por proxy caché y por VPN.

función principal de este software o hardware es justamente intermediar o ser representante de un ente, ante otras entidades. Hablamos de *entes* ya que los representados por el proxy pueden ser desde máquinas a partes de software. Encontramos distintos tipos de proxy; su implementación puede ser por software o hardware. Entre los implementados mediante software, se hallan los denominados **proxy caché**, **proxy database**, **proxy pattern**, **proxy socks**, **proxy local**, **proxy público** y **proxy Ajax**. De los que lo son por hardware, tenemos los **proxy ARP** y **proxy firewall**. Podemos acercarnos a la definición declarando que proxy es un software utilizado por una máquina para representar una red de computadoras ante otras máquinas; en nuestro caso particular, para representar una red ante Internet. Nuestro enfoque aquí es sobre el proxy caché, que nos permite, entre otras cosas, navegar con seguridad por páginas.

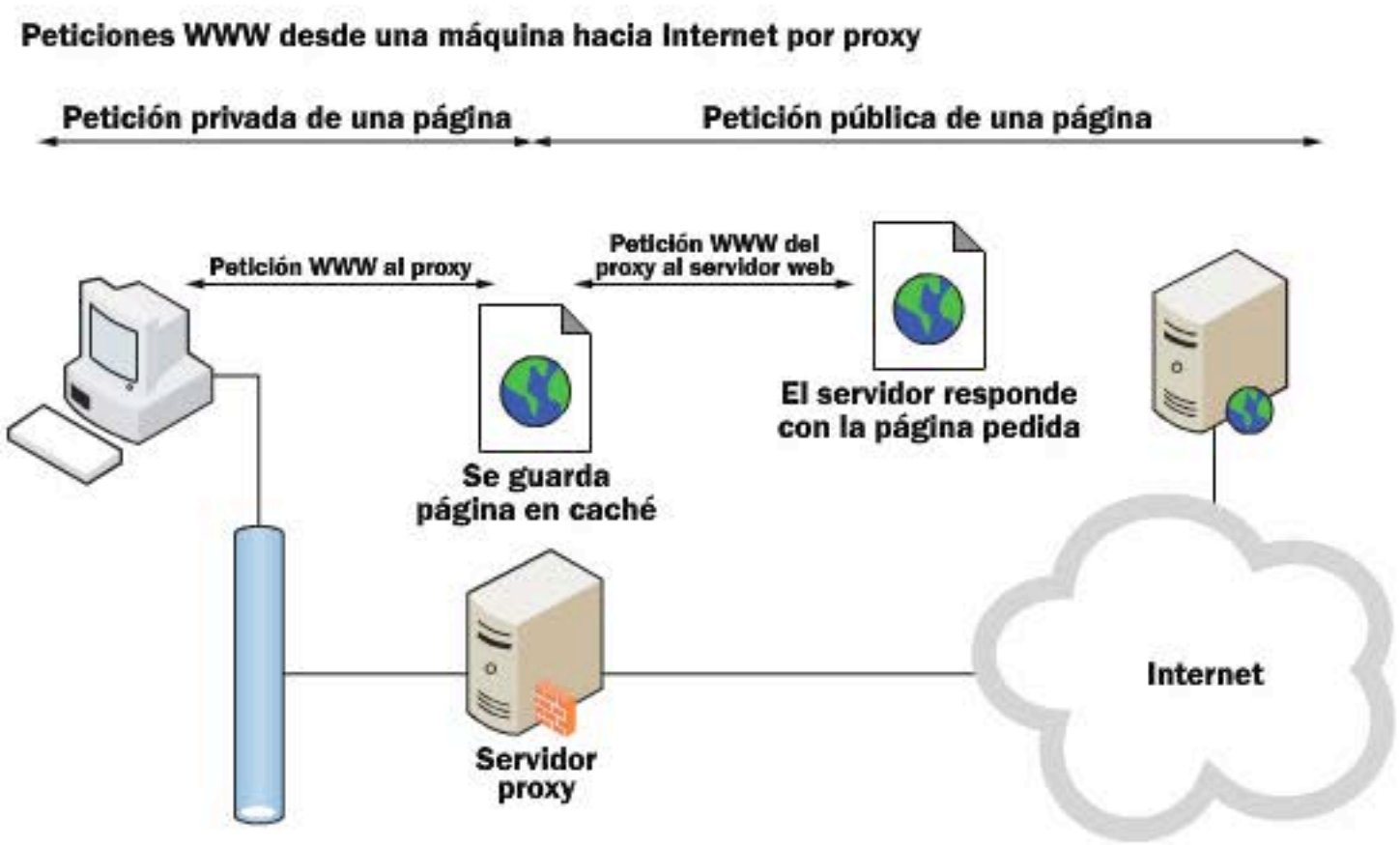
Proxy caché

El nombre de caché, se adicionó ya que, para acelerar la navegación en la era en que las computadoras se conectaban a un ISP por módem, el proxy utilizaba un banco de memoria o disco para almacenar temporalmente las páginas más visitadas (la caché), lo cual era un alivio para aquellas conexiones que utilizaban 56.000 bps. El funcionamiento del proxy es muy simple y se basa en la topología cliente-servidor. Esta topología otorga el título de servidor a quien ofrece un servicio, en este caso el proxy, y el cliente es quien consume este servicio, en este caso las PCs que están en una red.

Propiedades del proxy caché

Las propiedades de un **servidor de proxy caché** son las siguientes: permite navegar por Internet sin necesidad de consumir direcciones públicas IPv4; permite aumentar el nivel de seguridad, pero solo en un servicio en particular; es vulnerable a ataques informáticos DOS/DDOS; aumenta las necesidades de control para evitar fraudes desde la red interna; disminuye las capacidades de los atacantes informáticos para conocer la topología que corresponde a la red privada; permite manejar el ancho de banda consumido en la navegación por Internet; se mantiene el control de usuarios habilitados para la navegación y, en algunos casos, las aplicaciones clasificadas como públicas podrian dejar de funcionar.

Sin embargo, para el caso particular del proxy caché, el servicio se da a nivel de aplicación, por lo tanto la PC (el cliente) debe tener una aplicación que consuma este servicio; esta aplicación es, por lo general, un navegador web. En la actualidad, existen muy pocos navegadores que no



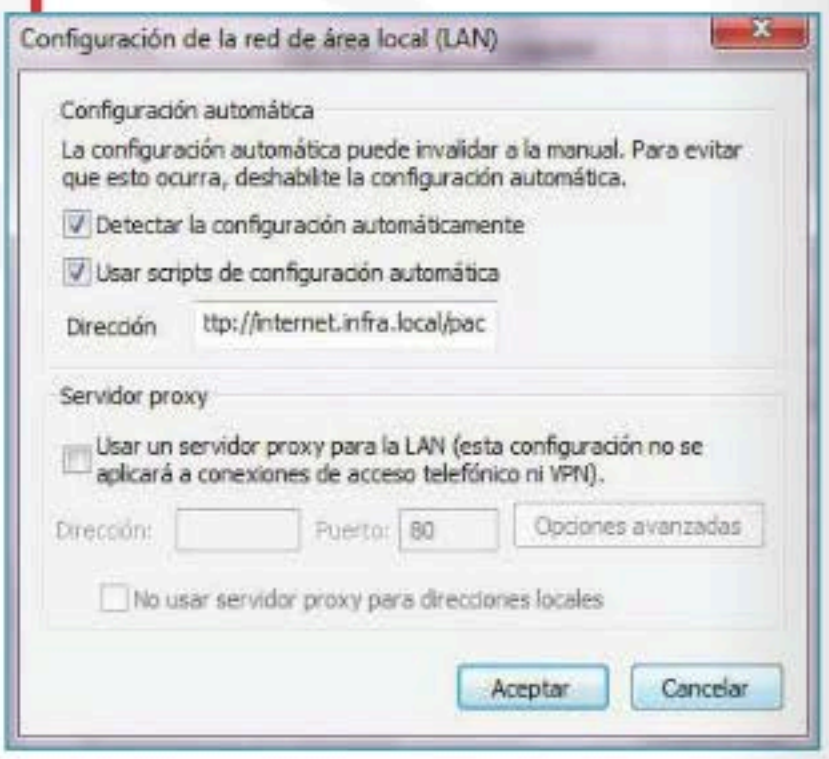
Esquema donde se puede visualizar cómo las peticiones de páginas son administradas por el servidor proxy.

permiten la configuración de proxy entre sus funciones; casi siempre, son versiones muy viejas o muy específicas. Entre estos, se encuentran el navegador **Lynx** de Linux y **Mosaic** o **Erwise** para Windows. En las versiones modernas de los navegadores más populares, estas opciones están disponibles en todos los casos. Para que el circuito funcione, el navegador web deberá tener configurado los datos necesarios para realizar las peticiones al servidor proxy; entre estos datos, deberemos brindar una URL, una dirección IP, o un archivo con las políticas propias de conexión. Una vez configurado, el navegador realiza una petición HTTP al servidor proxy, este toma la consulta y primero verifica si la URL solicitada está guardada en la caché propia, si es así, le da al cliente la copia que tiene localmente; en el caso contrario, realiza la consulta HTTP al server destino, toma la respuesta y, además de dársela al cliente, se guarda la copia en la caché. De esta forma, el servidor presenta a Internet su IP pública, mientras el rango de direccionamiento de toda la organización queda oculta para el resto del mundo.

UN PROXY SE ENCARGA DE REENVIAR LAS PETICIONES DE OTRAS MÁQUINAS, DIRIGIÉNDOLAS A LA RED EXTERNA.

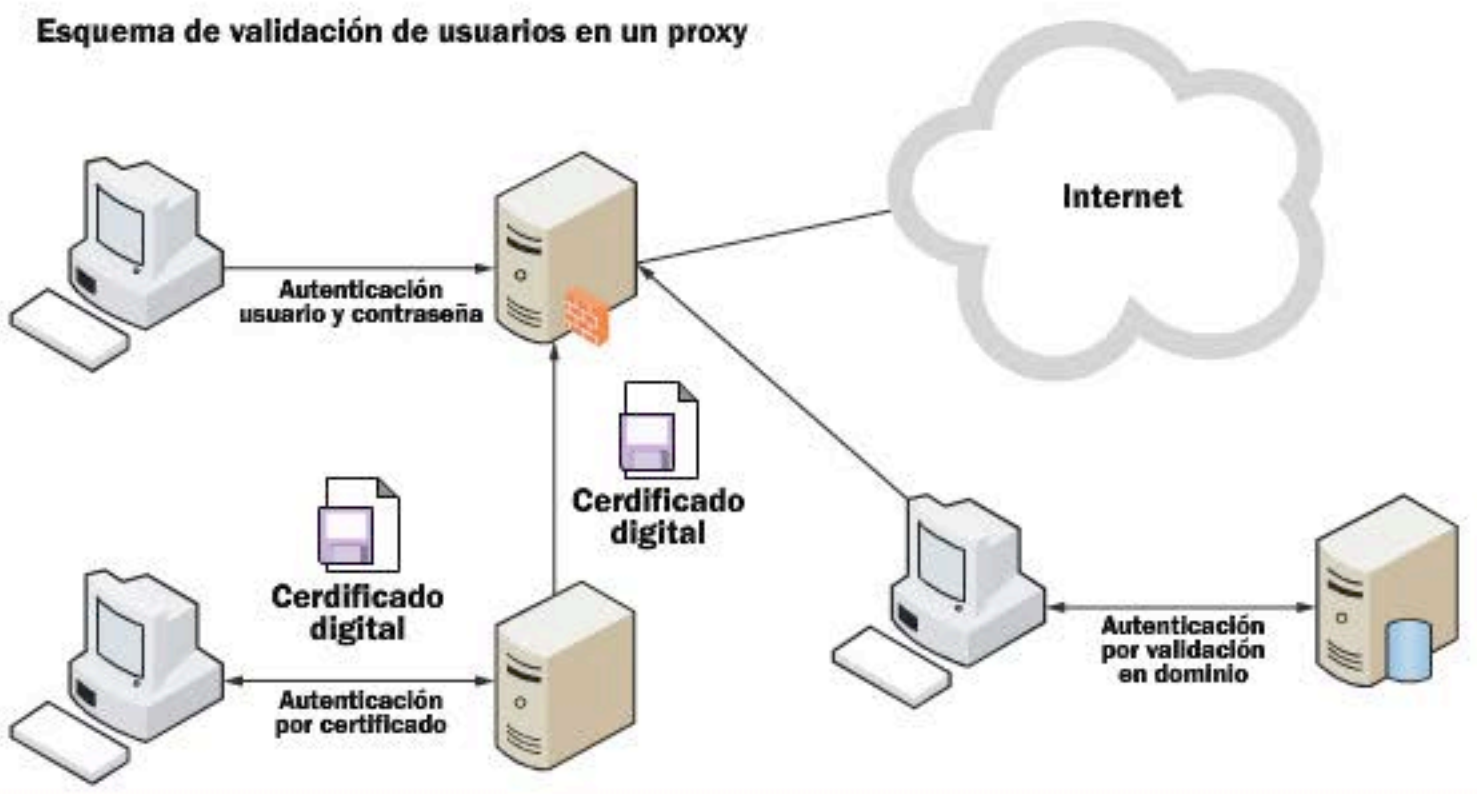
En algunos casos, se pedirá un usuario y contraseña para acceder a las páginas externas al servidor; en otros casos que cuentan con medios de autenticación más sofisticados, esta tarea es realizada mediante el uso de certificados digitales, los cuales pueden ser emitidos por una entidad pública o privada; incluso la conexión al servidor proxy puede llegar a encriptarse para lograr un mayor nivel de seguridad.

Configuración de un proxy mediante un archivo de comandos propio de la organización en IE 9.



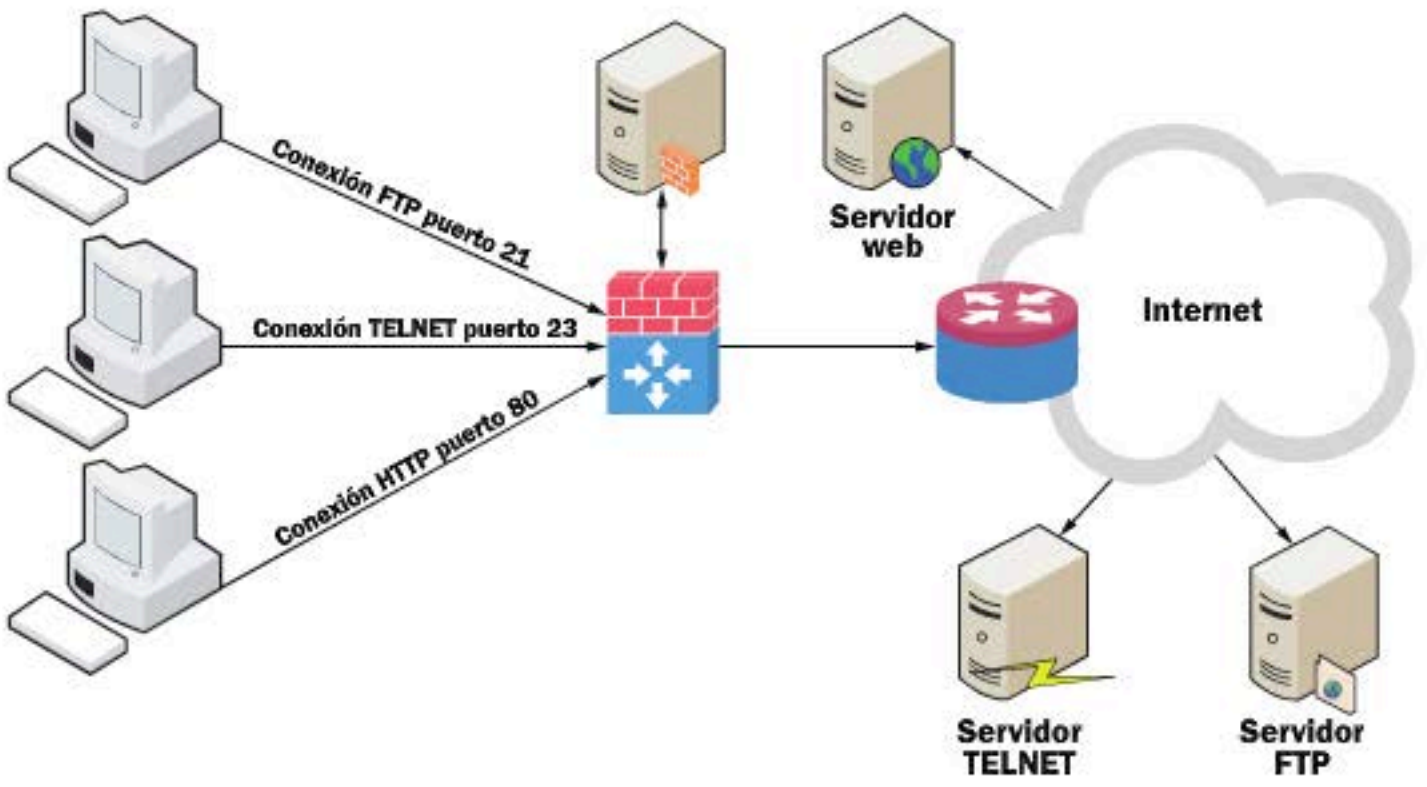
Conexiones

Algunas organizaciones pueden requerir que el proxy realice conexiones internas y externas, por lo cual se creará un archivo en el servidor con una extensión particular, para que la configuración sea automática. La instalación de un servidor proxy puede establecerse mediante un asistente, como en el caso de los servidores proxy bajo plataformas Windows; o mediante instalaciones muy complicadas y con administración de archivos de texto, como los que están bajo plataformas Linux.



Distintas formas de validación de un servidor proxy, por usuario y contraseña, por certificado digital y por autenticación remota.

Servidor SOCKS y sus conexiones a distintos servicios



En este diagrama, vemos la representación de un esquema del proxy socks para conexiones a través de otros servicios IP.

Ambos tienen sus pros y sus contras. En el caso de Windows, si bien la instalación es muy fácil, la adaptación del software a esquemas donde las tareas son muy complicadas resulta muy difícil y, muchas veces, imposible. Todo lo contrario sucede en las plataformas GNU/Linux donde el servidor es muy flexible ante las necesidades de las redes modernas, pero su implementación nos llevará mucho tiempo y esfuerzo.
En ambos casos, la tarea del administrador del proxy es balancear entre el espacio asignado para la caché en disco del servidor, qué sitios web o URL son permitidos o negados a los clientes, qué cantidad de conexiones concurrentes puede haber desde un mismo cliente y hasta qué cantidad de ancho de banda o tráfico está permitido para cada uno.

Ventajas y desventajas

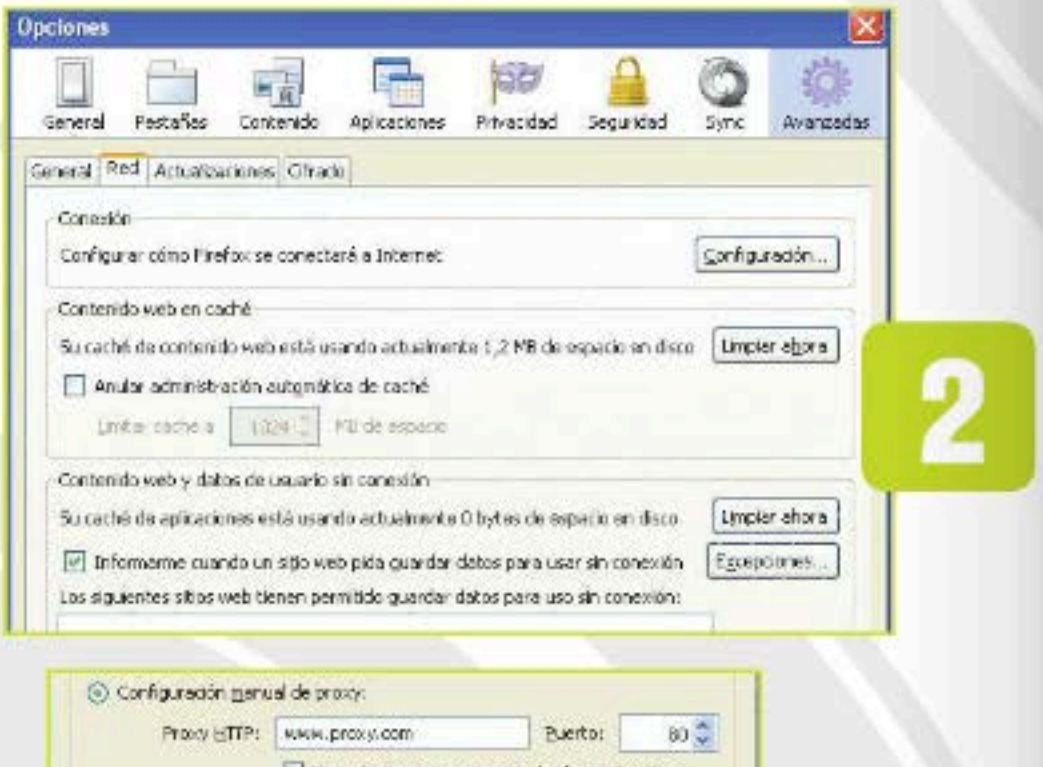
Las ventajas no solo se encuentran del lado de quien quiere acceder a Internet al acelerar la navegación, sino también del lado administrador, ya que nos permite disminuir el ancho de banda que se consume en la conexión a Internet, bajamos las colisiones de paquetes y podemos administrar el acceso a los sitios.
Una de las desventajas de utilizar un proxy caché para navegar por Internet consiste en que no sabemos si las páginas a las que accedemos están correctamente actualizadas, como sucede en el caso de los sitios de Internet que poseen un tiempo de refresco muy bajo; otra de las desventajas es que el poseer un solo punto de falla o proxy deja a la organización muy vulnerable a un ataque DoS; también en el caso de ciertas aplicaciones con tecnologías nuevas, como las que utilizan JavaScript y contenido dinámico, es muy posible que estas no funcionen bajo este tipo de navegación, por esta razón debemos ser cuidadosos con la elección de esta aplicación. Además, podemos tener inconvenientes en la administración de los usuarios ya que, cuando nos encontramos en grandes organizaciones, estos pueden necesitar la implementación de una gran cantidad de servidores de bases de datos para administrarlos, lo cual se encargará de complejizar aún más el sistema que implementemos, en vez de simplificarlo.

Ubicación

Por lo general, ubicaremos un servidor proxy caché en un área de seguridad informática denominada **DMZ** (*Demilitarized Zone*), que se encuentra aislada por medio de un firewall (que puede ser un software o hardware) corporativo tanto de Internet como de la red privada de la organización. Esta estructura de seguridad se diseña para brindar una mayor restricción a la organización, ya que impide que se pueda acceder libremente al servidor desde el interior de la red corporativa, así como también protege al servidor de las intrusiones externas (desde Internet).
Existen versiones de proxy caché, que también brindan servicios a otras aplicaciones que no son necesariamente web; en ese caso, se llaman proxy socks, ya que realizan el redireccionamiento de protocolos y puertos hacia los servidores destino. El funcionamiento es similar, solo que en este caso, debido a la naturaleza del servicio, no pueden cachearse los datos para volver a brindarlos.
La evolución del servicio proxy continúa en la actualidad, permitiendo no solo una navegación segura, sino también una administración de recursos para optimizar su utilización. ■

Configurar un servidor proxy y cliente proxy

En estas páginas, revisaremos los procedimientos que necesitamos completar para configurar un servidor y un cliente proxy.

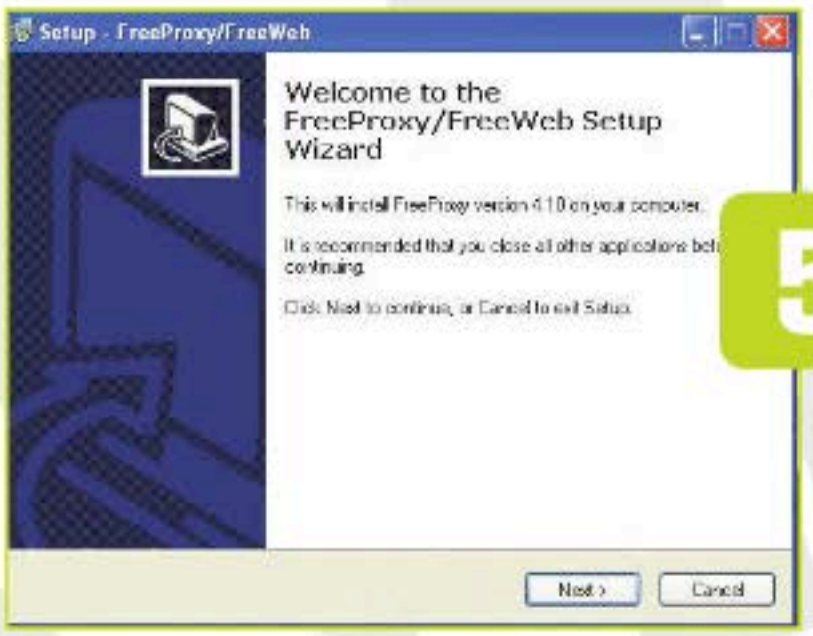


1 Para comenzar la configuración de proxy para el cliente Firefox para Windows versión 19.0.2, ingresamos al menú **Herramientas**. A veces, esta opción puede estar oculta; para hacer que se vea, hay que presionar **F10**. En ese caso, vamos a **Herramientas/Opciones**.

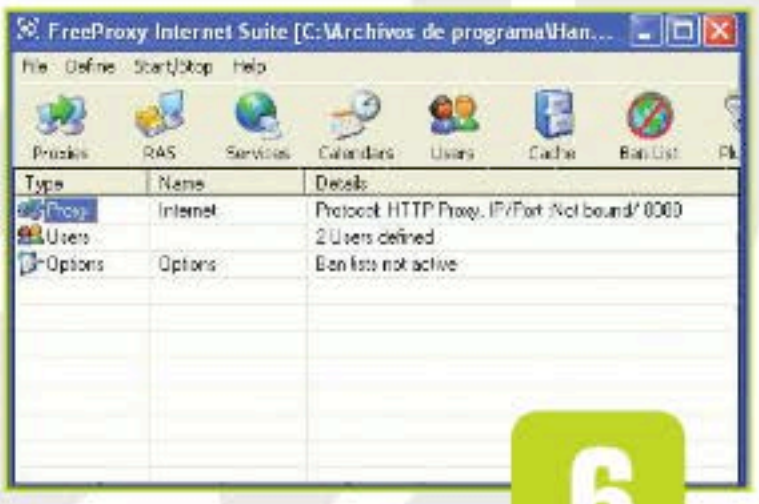
2 En cuanto hacemos clic, se abrirá la pantalla que se muestra en la imagen; hacemos clic en **Configuración**. Como se podrá observar, también están aquí las opciones de caché; en esta ocasión, debemos dejar las opciones predeterminadas.

3 Ingresaremos en la pantalla que aparece en la imagen. En este caso, tenemos varias opciones de configuración; utilizaremos la configuración manual, por lo cual haremos clic para comenzar a configurar nuestro proxy ingresando sus datos (**FQDN/IP** y **Puerto de conexión**).

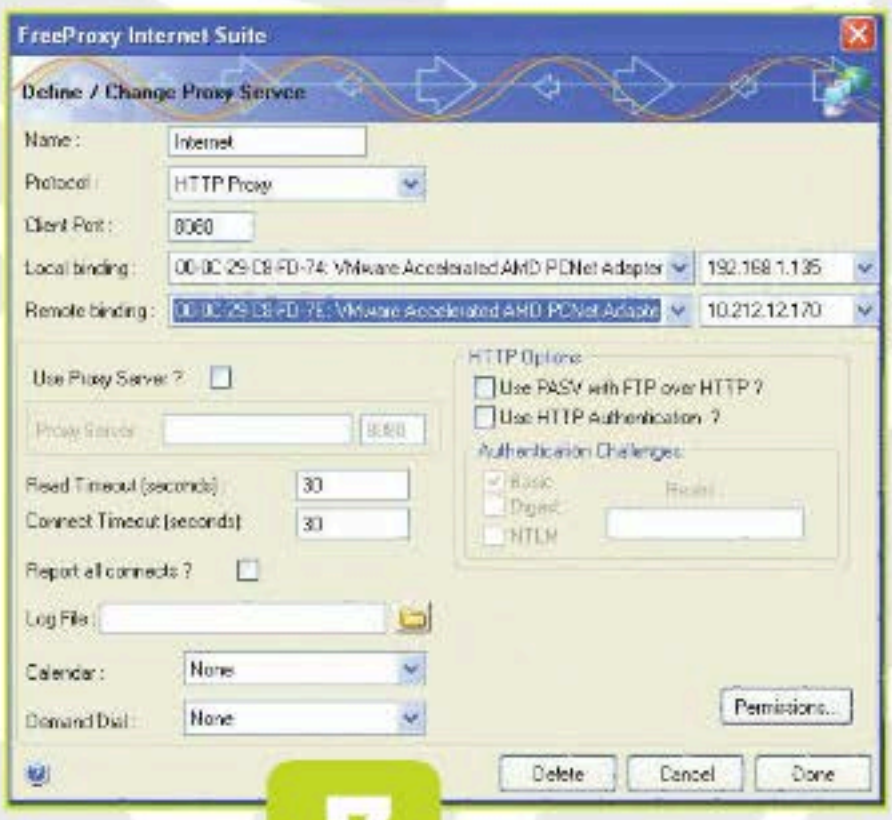
4 Después, ingresaremos los datos del proxy en cuestión. El **FQDN** (*Fully Qualified Domain Name*) o el nombre de host, y el **Puerto de conexión** (generalmente el **8080**). Nuestro proxy está configurado en nuestro navegador.



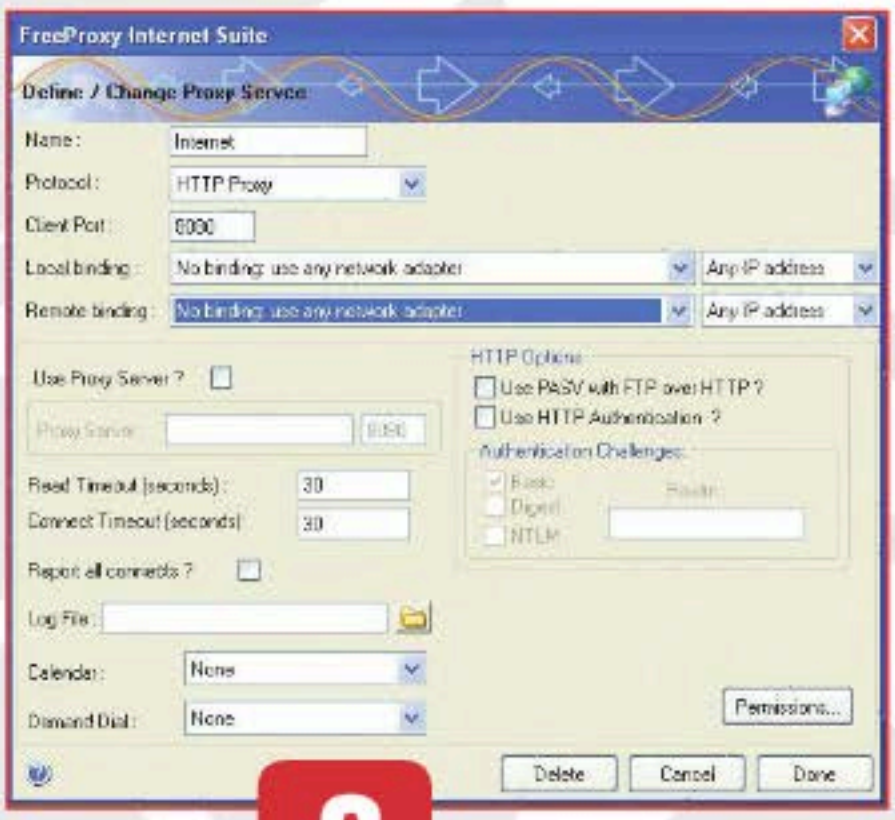
5



6



7



8

5 Ahora configuraremos el servidor; para ello, obtenemos el software **FreeProxy** de **Hancred Software**. Y procedemos a hacer doble clic en el ejecutable. Aparecerá un asistente muy sencillo. Ingresamos los datos de configuración inicial y hacemos clic en finalizar.

6 Procederemos a configurar el proxy server caché de acuerdo a nuestras necesidades; vamos a **Inicio/Todos los programas/Freeproxy/ Free Proxy Control Centre**. Veremos el puerto de conexión, los usuarios autorizados, y la lista de IP no autorizadas.

7 Hacemos doble clic en el icono de las **PCs (Proxy)**. Veremos dos opciones, **Local Binding** (o conexiones locales) y **Remote Binding** (o adonde nos queremos conectar, Internet u otra red distinta a la nuestra). En este caso, hay dos adaptadores, y cambiamos las IP para que uno sea **Local**, y el otro, **Remote**.

8 En la imagen, mostramos lo que nunca debe dejarse configurado por defecto, en este caso la opción de **No Binding**, ya que cualquier interfaz actúa como receptora y emisora de conexiones. Tampoco hay que cambiar el puerto por uno ya conocido, como por ejemplo el **80**.

Servidores y protocolos de autenticación

Conocer los servidores y protocolos de autenticación que utilizaremos nos permitirá dotar de un nivel de seguridad mayor a nuestra instalación de red; aquí revisaremos los conceptos asociados.

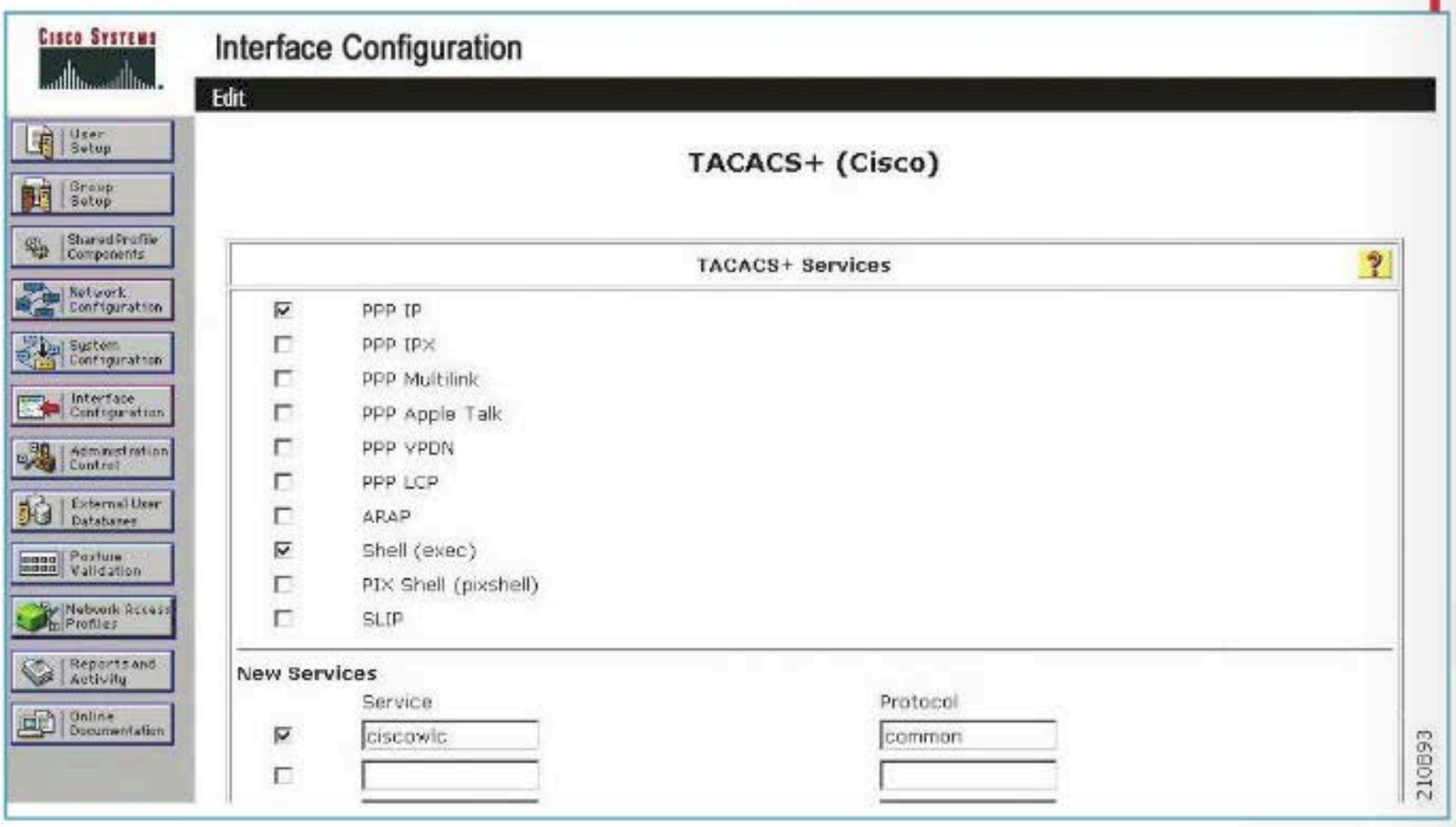
Un protocolo de autenticación es un tipo de protocolo encriptado, que tiene el propósito de **autentificar** entidades, usuarios, computadoras o servidores, que desean comunicarse de forma segura y de acuerdo con una serie de pasos establecidos. Los protocolos de autenticación se negocian inmediatamente después de determinar la calidad del vínculo y antes de negociar el nivel de red. El proceso de autenticación es un componente crítico en la actividad de la computadora. Los usuarios no pueden realizar muchas funciones en una red de computadoras o en Internet sin autenticarse antes en el servidor. Acceder a una computadora individual o a un sitio web requiere un protocolo de autenticación confiable para ejecutar un proceso de fondo y establecer la verificación del usuario.

Es necesario tener en cuenta que una variedad de protocolos están en uso activo por parte de muchos servidores por el mundo, en diferentes situaciones cotidianas.

Protocolos

Vamos a separar protocolos de autenticación, ya que no son los mismos protocolos los que se usan para autenticarse en Windows, para la conexión remota, o para establecer un VPN o, incluso, medios físicos (métricos, eléctricos, biométricos).

TACACS es un protocolo de Cisco muy utilizado en redes Unix; aquí vemos su interfaz de configuración.



Un típico caso es el nombre de usuario y contraseña en Windows, mediante una autenticación RADIUS.

Elegir el protocolo

La elección del protocolo depende de lo que busquemos a la hora de hacer más segura la conexión y la forma en que se conectan los usuarios, además de estar acorde con la infraestructura y tener compatibilidad con programas y dispositivos. El más usado es RADIUS, pero no se trata del más seguro, por eso, si bien se puede usar RADIUS para autenticación de usuarios y envío de información, en los enlaces externos o en situaciones críticas que contengan información confidencial o su manipulación es preferible usar TACACS y, en su versión mejorada, presentada como TACACS+.

Algunos protocolos son los siguientes:

- **PAP**: protocolo de autentificación de contraseña.
- **CHAP**: protocolo de autentificación por desafío mutuo.
- **SPAP**: protocolo de autentificación de contraseña de Shiva.
- **MS-CHAP y MS-CHAP v2**: protocolo de autentificación por desafío mutuo de Microsoft (variantes de CHAP).
- **EAP**: protocolo de autentificación extensible.
- **Diameter**: protocolo para conexión por línea conmutada o RTC.
- **Kerberos**: protocolo de autenticación de usuario/contraseña.
- **NTLM**: protocolo de autenticación utilizado en redes Microsoft.
- **PEAP**: protocolo de autenticación extensible protegido.
- **RADIUS**: se trata de un protocolo relacionado con la autenticación, administración y autorización.
- **TACACS**: protocolo de autenticación remota.
- **TACACS+**: protocolo de autenticación remota (no compatible con TACACS).

Protocolos más difundidos

A continuación, vamos a referirnos a los tres protocolos más difundidos: RADIUS, Diameter y TACACS.

Empezaremos por **RADIUS** (*Remote Authentication Dial In User Service*). Es un protocolo **AAA** (Autenticación, Autorización y Administración); este protocolo es usado por los ISP. Es requerido para que ingresen y se conecten los usuarios usando un nombre y contraseña. Una vez que los datos han sido escritos, la información pasa por un dispositivo **NAS** (*Network Access Server*) sobre un protocolo de capa de enlace y, luego, hacia un servidor RADIUS sobre un protocolo RADIUS.

El servidor RADIUS chequea que esa información sea correcta usando esquemas de autentificación como **PAP**, **CHAP** o **EAP**. Si es aceptada, el servidor autorizará el acceso al sistema del ISP y seleccionará una dirección IP y parámetros L2TP. Además de esto, RADIUS nos provee de diferente información, como el inicio de sesión del usuario, la finalización de sesión del usuario, el total de paquetes transferidos durante la sesión, el volumen de datos transferidos durante la sesión y la razón para la terminación de la sesión. Por otro lado, **Diameter** es un protocolo que se usa para las personas y los servicios que se conectan de manera remota a Internet a través de una línea conmutada o RTC. También, según el caso, provee de servicios de autorización y auditoría para aplicaciones, como por ejemplo, acceso de red o movilidad IP. El concepto básico del protocolo Diameter, cuyo desarrollo se ha basado en el protocolo RADIUS, es proporcionar un protocolo que esté diseñado tanto para trabajar de una manera local como en un estado de alerta, sondeo y captura, que le permite ofrecer servicios sumamente móviles, dinámicos, flexibles y versátiles.

DIAMETER SE USA EN CONEXIONES REMOTAS A INTERNET A TRAVÉS DE UNA LÍNEA CONMUTADA.

Un servidor TACACS provee una ubicación centralizada AAA para dispositivos **Cisco**. La autenticación se realiza con la base de datos local del dispositivo o con el servidor TACACS. El modelo TACACS provee funcionalidades como la autorización de comandos según el usuario y un registro histórico detallado de los accesos a los dispositivos y los comandos ejecutados.

Diferencias

A simple vista, no parece haber mucha diferencia entre TACACS y RADIUS, pero las diferencias son las siguientes: TACACS utiliza TCP mientras RADIUS utiliza UDP, RADIUS encripta las contraseñas en el paquete de respuesta al acceso mientras que TACACS+ encripta el cuerpo completo del paquete, y RADIUS no permite al usuario el control de los comandos que pueden ser ejecutados. ■

Protocolo Kerberos

Un uso correcto de Kerberos erradica la amenaza de analizadores de paquetes que intercepten contraseñas en su red.

Kerberos es un protocolo de validación e identificación usado en muchos sistemas para comprobar la identidad del usuario o de la máquina.

Un servidor **Kerberos** se denomina **KDC** (*Kerberos Distribution Center*); provee de dos servicios fundamentales: el de autenticación (AS, *Authentication Service*) y el de tickets (TGS, *Ticket Granting Service*). El primero tiene como función autenticar inicialmente a los clientes y proporcionarles un ticket para comunicarse con el segundo, el servidor de tickets, que proporcionará a los clientes las credenciales necesarias para comunicarse con un servidor final, que es quien realmente ofrece un servicio. Además, el servidor posee una base de datos de sus clientes (usuarios o programas) con sus respectivas claves privadas, conocidas únicamente por dicho servidor y por el cliente al que pertenece.

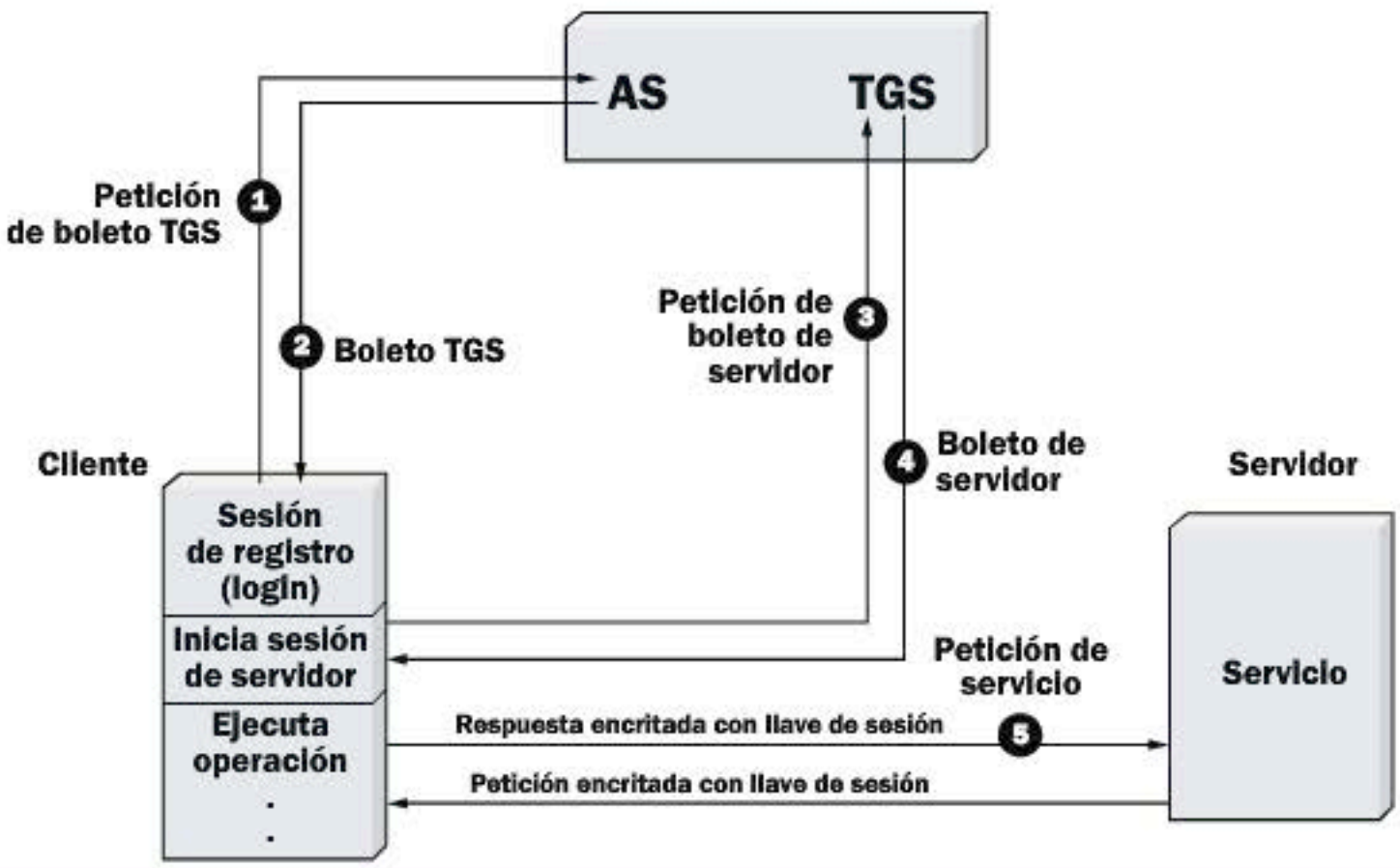
Arquitectura

La arquitectura de Kerberos está basada en tres objetos de seguridad: **Clave de Sesión**, **Ticket** y **Autenticador**. La clave de sesión es una clave secreta generada por Kerberos y entregada a un cliente para su uso con un servidor durante una sesión; no es obligatorio utilizarla en toda la comunicación con el servidor, solo si el servidor lo requiere (porque los datos son confidenciales) o si el servidor es un servidor de autenticación. Se suele denominar a esta clave **KCS**.

Las claves de sesión se utilizan para minimizar el uso de las claves secretas de los diferentes agentes: estas últimas son válidas durante mucho tiempo, por lo que es conveniente, para minimizar ataques, utilizarlas lo menos posible.

El Ticket es un testigo entregado al cliente para solicitar los servicios de un servidor; garantiza que el cliente ha sido autenticado en forma reciente.

Kerberos siempre proporciona el ticket ya cifrado con la clave secreta del servidor al que se le entrega. Por otra parte, el Autenticador es un testigo construido por el cliente y enviado a un servidor para probar su identidad y la actualidad de la comunicación; consideremos que solo puede ser utilizado una vez.



Este diagrama nos muestra la forma en que funciona Kerberos y, también, cómo se comunica en sus distintos procesos.

Instalación

En este apartado, vamos a ver la instalación en GNU/Linux. Para configurar un servidor Kerberos básico, seguimos las indicaciones proporcionadas a continuación. En primer lugar, nos aseguramos de que tanto el reloj como el DNS funcionen correctamente en todas las máquinas servidor y cliente antes de configurar **Kerberos 5**. Debemos poner atención a la sincronización de la hora entre el servidor Kerberos y sus clientes; si la sincronización de los relojes del servidor y de los clientes se diferencia en más de cinco minutos (la cantidad predeterminada es configurable en Kerberos 5), los clientes de Kerberos no podrán autentificarse al servidor.

KERBEROS ELIMINA LA TRANSMISIÓN A TRAVÉS DE LA RED DE INFORMACIÓN DE AUTENTICACIÓN.

La sincronización de los relojes es necesaria para evitar que un intruso use un ticket viejo de Kerberos para hacerse pasar como un usuario autorizado.
Se recomienda configurar una red cliente/servidor compatible con **Network Time Protocol** (NTP) aun si no está usando Kerberos. **Red Hat Enterprise Linux** incluye el paquete `ntp` para este propósito.
Instalamos los paquetes `krb5-libs`, `krb5-server`, y `krb5-workstation` en una máquina dedicada que ejecutará el KDC. Esta máquina tiene que ser muy segura; si es posible, no debería ejecutar ningún otro servicio excepto KDC. Si deseamos usar una utilidad de interfaz gráfica para administrar Kerberos, instalaremos el paquete `gnome-kerberos`. Este contiene **krb5**, que es una herramienta tipo GUI para manejar tickets. Los archivos de configuración se encuentran en `/etc/krb5.conf` y `/var/kerberos/krb5kdc/kdc.conf`; en ellos, debemos reflejar las opciones que corresponden a nuestra implementación de seguridad.
Creamos la base de datos usando: `shell:/usr/kerberos/sbin/kdb5_util create–s`.
Luego, modificamos el archivo `/var/kerberos/krb5kdc/kadm5.acl`.
Este archivo es usado para determinar los accesos administrativos a la base de datos Kerberos. La mayoría de las organizaciones pueden resolverse con una sola línea: `*/admin@EXAMPLE.COM*`.
De igual forma, la mayoría de los usuarios serán presentados en la base de datos por un principal simple. Con esta configuración, los usuarios con un segundo principal que tengan una instancia de `admin` podrán tener todo el acceso sobre la base de datos.
Escribimos el comando `kadmin.local` en una terminal KDC para crear la primera entrada como usuario principal: `/usr/kerberos/sbin/kadmin.local -q "addprincusername/admin"`

▶ Iniciamos Kerberos usando los comandos: `/sbin/service krb5kdc start ;/sbin/servicekadminstart;/sbin/service krb524 start`

En Windows 7 y 2008 está la directiva local de asignación.

▶ Agregamos principales para sus usuarios: `addprinc kadmin`

Verificamos que el servidor KDC esté creando tickets. En primer lugar, ejecutamos `kinit` para obtener un ticket y guardarlo en un archivo caché. Usamos `klist` para ver la lista de credenciales en su caché y `kdestroy` para eliminar la caché y las credenciales.
Para que exista compatibilidad entre Windows y Linux, activamos roles de Windows; en Windows 2008, activamos **Active Directory Rights Management Services** con autenticación Kerberos. ■

Técnica Evilgrade

Evilgrade ha sido reconocida como una de las mayores vulnerabilidades para Internet; aquí conoceremos sus detalles.

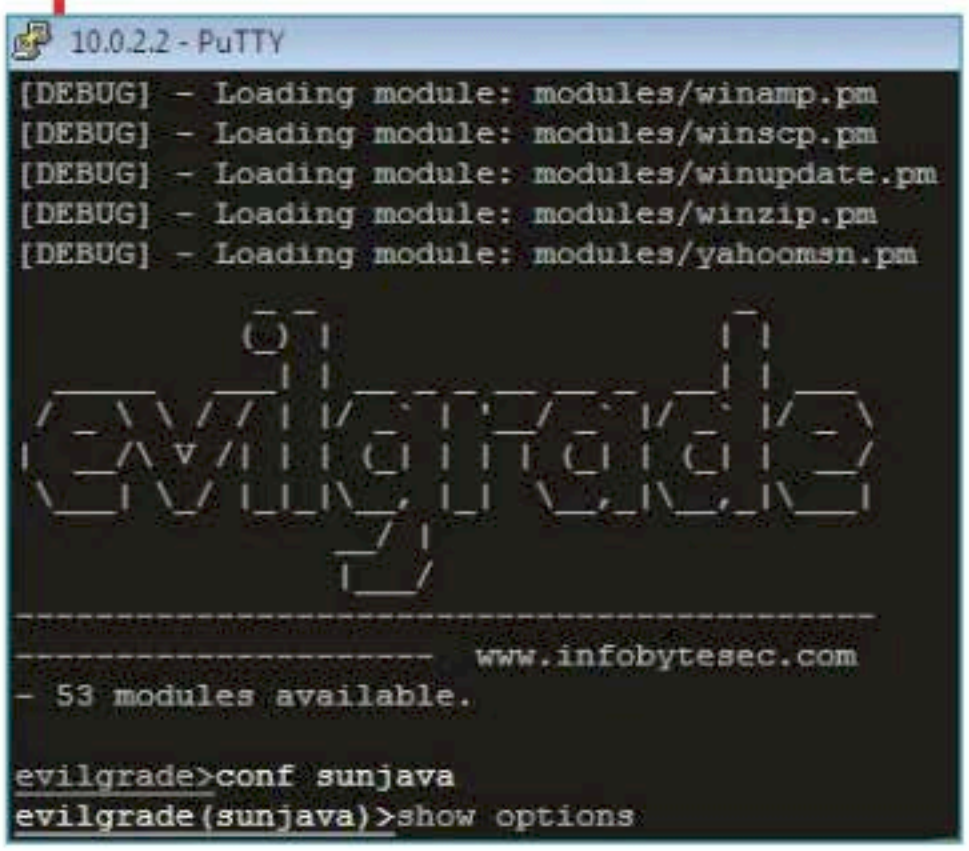
La vulnerabilidad de **Evilgrade** es un framework modular que permite realizar la intrusión en sistemas cuyas implementaciones son débiles en cuanto a la autenticación de fuentes. Fue creado alrededor del año 2007 por el especialista en seguridad informática Francisco Amato. Está basado en programación PERL, pero podemos portarlo a cualquier lenguaje.

Se trata de una técnica utilizada para ataques informáticos con el que podemos realizar otro tipo de irrupciones de penetración profunda, tales como acceso interno a DNS, arrebatamiento de ARP, envenenamiento de DNS, sustitución TCP, entre otros.

Funcionamiento

Este framework permite trabajar en forma modular y cada módulo del sistema actúa de manera independiente. La vulnerabilidad la encontramos en el fabricante del producto de software y, para comprobarlo, solo hay que obtener la distribución para Linux de Evilgrade, disponible actualmente en una gran cantidad de sitios en Internet, y comenzar a realizar las pruebas de penetración desde nuestra consola; hasta es posible modificar su código fuente para realizar tareas más puntuales. Entre el software vulnerable más conocido están **Adobe**, **Microsoft**, **VMWare**, **VirtualBox**, entre otros. El framework es de sistema operativo cruzado, razón por la cual puede ejecutarse bajo muchos SO, ya que depende más del software cliente y de la autenticación del servidor.

Podemos encontrar **Evilgrade** en la distribución Bug Track Linux; se trata de una herramienta muy popular entre hackers y crackers.



EVILGRADE FUE PRESENTADO EN LA EKOPARTY EN LA ARGENTINA EN EL AÑO 2007.

Problemas y soluciones

Entre las posibles soluciones, está implementar un certificador de servidores por IP-MAC address. En este caso, un servidor de actualizaciones intermedio entre el servidor público y la red privada realiza una autenticación del origen de la conexión de aviso para el upgrade. Esta técnica de firewall es muy complicada de llevar a cabo, ya que depende mucho de la información que brinde el proveedor, y requiere de muchos recursos humanos para poder administrarla.

Del lado de los proveedores de software, se está llevando a cabo una incesante búsqueda de métodos de autenticación robustos tales como la aplicación de autenticación hash; pero no se han tenido resultados esperanzadores (el hash también puede ser simulado por Evilgrade). Desde su aparición en 2007 (en forma oficial), Evilgrade fue y sigue siendo un problema para los analistas de seguridad informática debido a la compleja tarea que se necesita para tratar de detener esta vulnerabilidad desde afuera de las organizaciones que son propietarias.

Sin embargo, esta vulnerabilidad se vio potenciada por otra de Dan Kaminsky a nivel de los servidores DNS, y es que, antes de esta novedad, el ataque por Evilgrade a lo sumo podía darse en forma local; con la vulnerabilidad de Kaminsky, el proceso se extendió a Internet en 2008. Desde ese entonces, han aparecido multitud de parches de seguridad para los servidores vulnerables al bug Kaminsky, lo cual disminuye en gran parte la técnica de EG (Evilgrade). Desde la otra vereda, tenemos un set de herramientas de intrusión que utiliza Evilgrade como plataforma de lanzamiento, así como también varias *Intruders Tools* (ITS) que automatizan el proceso; incluso, se habla de virus que utilizarían un set de herramientas entre las cuales se encuentra EG, para poder infectar otras máquinas. ■

PRÓXIMA ENTREGA

22

VLAN, VPN Y TRABAJO REMOTO

En el próximo número conoceremos los diferentes tipos de redes virtuales existentes y entregaremos recomendaciones sobre seguridad. Además, veremos herramientas para trabajar sobre VPN.

Técnico en REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00021
9 789871 857784

CONTENIDO DE LA OBRA