Seguridad activa

Jordi Serra Ruiz

PID_00200515

Universitat Oberta de Catalunya

Los textos e imágenes publicados en esta obra están sujetos –excepto que se indique lo contrario– a una licencia de Reconocimiento-NoComercial-SinObraDerivada (BY-NC-ND) v.3.0 España de Creative Commons. Podéis copiarlos, distribuirlos y transmitirlos públicamente siempre que citéis el autor y la fuente (FUOC. Fundación para la Universitat Oberta de Catalunya), no hagáis de ellos un uso comercial y ni obra derivada. La licencia completa se puede consultar en http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es

Índice

Introducción..... 5

Objetivos..... 6

1. Certificados y sistemas de clave pública y privada..... 7
1.1. Clave simétrica 8
1.2. Clave asimétrica 8
1.3. Clave de sesión 9
1.4. Firma digital 10
1.5. Certificado digital 11
1.6. Petición de un certificado 12

2. Certificados en GNU/Linux..... 14
2.1. Creación de una CA 16
2.2. Revocación de un certificado 18

3. Certificados en Windows Server 2012..... 20
3.1. Gestión de certificados 21
3.1.1. Importar y exportar certificados 22
3.1.2. Complemento de certificados 23
3.2. Utilización de certificados 24
3.2.1. Firma electrónica 24
3.2.2. Cifrado de archivos 24
3.2.3. Aceptación de certificados 25
3.3. Emisión de certificados 25
3.3.1. Entidad certificadora de confianza 25
3.3.2. Servidor de certificación 26

4. IPsec..... 30
4.1. Instalación de IPsec en GNU/Linux 31
4.1.1. Modo túnel 32
4.1.2. Modo transporte 33
4.2. Herramientas de control de IPsec en Windows Server 2012 34
4.3. Utilización de directivas IPsec predefinidas 36
4.4. Utilización de directivas IPsec personalizadas 36

5. Redes privadas virtuales..... 39
5.1. GNU/Linux 39
5.1.1. Secure Shell 39
5.1.2. *Secure socket layer*..... 41
5.1.3. IPsec 42

5.1.4. Otros sistemas 43
5.2. Windows Server 2012 43
5.2.1. Configuración del servidor 43
5.2.2. Configuración del cliente 49

6. Monitorización de la Red..... 51
6.1. Monitorización en GNU/Linux 51
6.2. Monitorización en Windows Server 2012 56

7. Herramientas de comprobación..... 59
7.1. Herramientas de GNU/Linux 60
7.1.1. NMAP 60
7.1.2. Snort 61
7.2. Herramientas de Windows Server 2012 63
7.2.1. Listas de comprobación de seguridad 63
7.2.2. Microsoft Baseline Security Analyzer 64
7.2.3. Configuración de seguridad local 65
7.2.4. Configuración y análisis de seguridad 66

Introducción

La seguridad activa de las organizaciones y empresas es de las más importantes que hay que tener en cuenta, puesto que nos protegemos de todos los posibles ataques maliciosos que nos puedan venir básicamente por la Red (teniendo conciencia de que se toman medidas adicionales para que los intrusos no tengan acceso a la información de la empresa).

Para protegerse de lecturas no deseadas de la información guardada en un fichero o de los datos que circulan por Internet, basta con cifrar los mensajes o archivos con un par de claves públicas y privadas para que nadie a quien antes no se haya dado permiso expreso pueda acceder a la información.

En este módulo, mostraremos los conceptos de certificados en la información y claves públicas y privadas.

Por otro lado, todas las aplicaciones que se tienen que ejecutar para tener el acceso mediante la Red las podemos autenticar. Es decir, podemos pedir que el usuario se autentique para utilizar estas aplicaciones.

Por ejemplo, en lugar de utilizar el protocolo HTTP de intercambio de ficheros por Internet se puede usar el protocolo HTTPS, que tiene que autenticar al usuario que intenta acceder al servidor web para bajarse la información.

Otra manera de asegurarnos de que no se accede a la información privada son las extensiones IPsec (seguridad del control de Internet), canales seguros de información que viaja por Internet.

Una de las tareas de un administrador, aparte de estas que hemos indicado y de las que hemos descrito en el módulo de seguridad pasiva, es la monitorización de la Red. El tráfico de información de la Red da mucha información de la manera en que se puede acceder a los datos y de quién ha accedido a cada uno de los recursos compartidos. Veremos cómo se puede obtener esta información.

Objetivos

En este módulo, pretendemos que conozcáis los diferentes métodos de seguridad activa que se pueden implantar en una máquina. Para algunos de estos métodos, como por ejemplo las herramientas de comprobación, sería necesario un módulo entero para llegar a ver todas las posibilidades que pueden llegar a proporcionar estas herramientas; además, se requieren conocimientos de redes bastante avanzados, lo que excede el temario de la asignatura. Por lo tanto, simplemente pretendemos explicar qué son estas herramientas, cómo se instalan y cuáles son los propósitos que tienen. Después, cada administrador puede estudiar estas herramientas con más detenimiento y de manera más avanzada.

Los objetivos de este módulo son los siguientes.

1. Conocer el uso de certificados y saber cómo los tenemos que instalar en las máquinas.

2. Conocer el funcionamiento y la instalación de IPsec.

3. Saber instalar y configurar VPN.

4. Conocer las herramientas de monitorización de la Red.

5. Saber qué herramientas de comprobación hay.

1. Certificados y sistemas de clave pública y privada

A lo largo de la historia, el ser humano ha desarrollado sistemas de seguridad para determinar varios factores que intervienen en una comunicación o un contrato. En la lista siguiente, enumeramos algunos de estos sistemas.

1) Identificar las identidades de los interlocutores, es decir, comprobar que las personas que intervienen en la comunicación son las que dicen que son (documentos de identificación, firma).

2) Ninguna de las dos partes puede modificar la información de manera arbitraria. Es decir, una vez firmado un contrato, no se pueden cambiar los acuerdos que se han descrito en el mismo. Para verificar estos acuerdos, están los notarios.

3) Ninguna de las dos partes puede negar el hecho de que se comprometió con esta información. Una vez firmado el contrato, no lo podemos incumplir.

4) En el caso concreto de las comunicaciones encontramos el correo certificado, que sirve para asegurarnos de que el destinatario ha recibido la información.

En la mayoría de estos casos, el sistema de seguridad se basa en la identificación física de la persona. Actualmente hay que trasladar estos sistemas de seguridad al entorno de las comunicaciones digitales, debido a un aumento de las actividades comerciales por Internet.

El principal problema de este tipo de comunicaciones es que no tenemos ninguna seguridad de la identidad de la persona o entidad que hay en el otro extremo de la comunicación. La causa principal de este problema es que no hay contacto directo entre las personas que están implicadas en la transferencia de esta información. Necesitamos, por lo tanto, un documento digital que ofrezca las mismas funcionalidades que los documentos que están implicados en las transacciones presenciales (identificación, integridad, no repudio y confidencialidad).

Las soluciones a estos problemas son la firma electrónica y el certificado digital. Antes de entrar a explicar estos puntos, sin embargo, es preciso que comentemos conceptos más básicos sobre criptografía.

Curiosidad criptográfica

Por ejemplo, si desplazamos todas las letras doce posiciones en el abecedario normal, la *a* pasa a ser la *m*, la *b* la *n*, etc., y un mensaje como *atacar hoy* pasa a ser *mfmomd rak*.

La criptografía tiene su origen en el Imperio Romano, en la época del emperador Julio César, que utilizaba un esquema criptográfico simple –pero efectivo– para comunicarse con sus generales. El método consistía en desplazar cada letra del alfabeto un número determinado de posiciones.

Este método de cifrado tan simple nos introduce en el concepto de clave criptográfica: el algoritmo necesario para codificar el mensaje. En este caso, el algoritmo es desplazar doce posiciones cada letra en el abecedario. Para resumir, el concepto de cifrado es muy simple: a un texto sin cifrar le aplicamos un algoritmo de transformación del mensaje (cifrado) y obtenemos un mensaje cifrado que solo pueden saber las personas que conocen la clave criptográfica.

1.1. Clave simétrica

Decimos que una clave es simétrica cuando se utiliza la misma clave criptográfica para cifrar y para descifrar, es decir, cuando el receptor necesita tener la clave para descubrir el mensaje codificado. El proceso de cifrar un mensaje con la clave simétrica es muy sencillo y lo veremos con un ejemplo de comunicación entre dos usuarios, como por ejemplo Alicia y Roberto.

1) Alicia escribe un mensaje en texto plano.
2) Alicia aplica un algoritmo de cifrado con clave simétrica conocida.
3) Alicia envía el mensaje a Roberto.
4) Roberto, utilizando la misma clave, descifra el mensaje.

La gran ventaja del cifrado con clave simétrica es la velocidad, y esto hace que este tipo de cifrado sea muy apropiado para cifrar grandes volúmenes de información. El problema del cifrado con clave simétrica es que el receptor ha de tener la clave criptográfica; por lo tanto, es preciso distribuir la clave entre todas las personas o entidades entre las que nos queremos comunicar de manera cifrada. Si alguien es capaz de interceptar el mensaje y la distribución de la clave, también será capaz de descifrar el mensaje.

1.2. Clave asimétrica

Decimos que una clave es asimétrica cuando se utilizan claves diferentes para cifrar y para descifrar un mensaje. Este método usa dos claves que están relacionadas entre sí: la clave privada y la clave pública. La clave privada solo la tiene que saber el propietario de la clave, y la pública se debe distribuir de manera arbitraria por la red (más adelante veremos que el sistema de distribución de claves no es tan arbitrario, sino que sigue unos pasos muy concretos).

Esta pareja de claves es complementaria, es decir, el mensaje que cifra una clave solo lo puede descifrar la otra. Puesto que la obtención de las dos claves se consigue con métodos matemáticos muy complejos, es imposible (por razones

de coste temporal) deducir la clave privada a partir de la clave pública. Costaría tantos años hacer esto que no merece la pena y, por lo tanto, el método se considera seguro.

Veremos el funcionamiento de las comunicaciones mediante este método con un ejemplo. Imaginemos que Alicia se quiere comunicar con Roberto. Los dos tienen una clave pública y una privada. La clave privada solo la sabe el propietario, cada cual la suya, pero las públicas las saben los dos, puesto que han accedido mediante la red a la clave pública de la otra persona.

Si Alicia quiere mandar un mensaje a Roberto que solo pueda leer él, debe seguir los pasos siguientes:

1) Alicia escribe un mensaje en texto plano.

2) Alicia cifra el mensaje usando como clave criptográfica la clave pública de Roberto.

3) El destinatario (Roberto) recibe el mensaje cifrado y lo descifra con su clave privada (que solo conoce él y que es la única que puede descifrar el mensaje).

Si Roberto quiere responder a Alicia, tiene que usar como clave criptográfica la clave pública de Alicia. De este modo, se asegura de que la respuesta solo la podrá abrir ella. Mediante el uso de las claves asimétricas obtenemos mucha más seguridad, puesto que para descifrar una comunicación hay que utilizar la clave privada y esta clave no se distribuye. Para generar un mensaje, es necesario especificar a quién se quiere enviar y utilizar la clave pública del destinatario, que solo él puede abrir con su clave privada.

La desventaja de este método es que las claves asimétricas, por su complejidad, son muy lentas a la hora de cifrar y descifrar. En el caso de que una clave privada fuera distribuida, sería preciso invalidarla y crear una nueva pareja de claves asimétricas para volver a tener seguridad en las comunicaciones.

1.3. Clave de sesión

La clave de sesión es un uso combinado de las dos claves anteriores para aprovechar la velocidad de la clave pública con la seguridad de la clave privada. Ahora, mediante un ejemplo de comunicación entre Alicia y Roberto, veremos el proceso de cifrado de este método.

1) Alicia escribe un texto plano.

2) Alicia lo cifra con una clave simétrica generada de manera aleatoria, denominada clave de sesión.

3) Alicia ya puede enviar el mensaje a Roberto.

4) Para hacer llegar la clave a Roberto, cifra la clave de sesión con la que ha cifrado el mensaje con la clave pública de Roberto y se la envía.

5) Roberto, con su clave privada, descifra el segundo mensaje con la clave y, una vez tiene la clave de sesión, puede descifrar y cifrar los mensajes y, por lo tanto, se puede comunicar con Alicia de manera rápida usando la clave simétrica que se ha distribuido entre ellos mediante una sola comunicación con clave asimétrica, mucho más lenta.

De este modo, hasta que no cierren la comunicación o quieran cambiar la clave simétrica, el sistema usará la clave simétrica, que hace que la comunicación sea mucho más rápida. Los portales web que utilizan protocolos seguros usan técnicas parecidas a esta.

Mediante este método, conseguimos identificación y confidencialidad de la comunicación y una velocidad de comunicación más rápida que utilizando solo las claves asimétricas. Si la comunicación se establece entre un cliente y un servidor, la negociación de las claves que se lleva a cabo entre uno y otro se hace de manera transparente para el usuario (situado en el cliente). En estos casos, las claves de sesión pueden tardar hasta un día en caducar. Es decir, si durante este día hacemos varias conexiones con el servidor, utilizaremos en todas las conexiones la misma clave de sesión, sin tener que volver a negociar el intercambio de claves.

1.4. Firma digital

La firma digital se usa con el mismo fin que una firma manuscrita. Por lo tanto, el objetivo es que el receptor sepa que el emisor es quien dice que es, que el receptor y el emisor sepan que no se ha modificado el contenido del mensaje y que el emisor no pueda repudiar un mensaje enviado. La firma digital funciona del mismo modo que las claves asimétricas, pero en lugar de utilizar la clave pública del receptor usa la clave privada del emisor. Puesto que se trata de claves complementarias, todo lo que se cifra con la clave privada se descifra con la pública, y viceversa.

Sin embargo, ya hemos visto que el principal inconveniente de las claves asimétricas es su lentitud, que aumenta según la longitud del mensaje que hay que cifrar. Para solucionar este problema, la firma digital utiliza unas funciones *hash*.

Una función *hash* es una operación que se hace sobre un conjunto de datos de cualquier tamaño y que da como resultado un subconjunto de estos datos de tamaño fijo (denominado resumen), que tiene la propiedad de estar unido de

manera unívoca al texto original. Como hemos hecho hasta ahora, veremos el proceso de una firma digital con el ejemplo de comunicación entre Alicia y Roberto.

1) Alicia escribe un mensaje original.

2) Alicia ejecuta un *hash* sobre el mensaje original y obtiene un resumen.

3) Alicia cifra el resumen con su clave privada (este proceso se denomina firma digital).

4) Alicia envía el mensaje junto con la firma a Roberto (notad que no se tiene que enviar la clave privada, sino solo la firma digital).

5) Roberto, para asegurarse de que el mensaje es de Alicia, debe comprobar su firma; para hacerlo, tiene que descifrar la firma con la clave pública de Alicia, y así obtiene el resumen.

6) Roberto aplica un *hash* sobre el mensaje original, y de este modo obtiene otro resumen.

7) Finalmente, compara los dos resúmenes: si son iguales, puede estar seguro de que el mensaje lo ha enviado Alicia y de que no se ha modificado desde que se ha generado.

1.5. Certificado digital

Los métodos comentados hasta ahora, que se basan en las claves asimétricas, tienen algo en común: su éxito depende del hecho de que la clave privada de los usuarios solo la sepan estos usuarios y de que la clave pública sea distribuida por la red sin dar pie a confusiones entre las claves públicas de los diferentes usuarios. Las claves privadas suelen estar integradas en tarjetas inteligentes (son las tarjetas que llevan un chip) o en otro tipo de soporte que impida duplicarlas. Para que haya más seguridad, estas tarjetas también están protegidas con contraseñas numéricas que garantizan que en caso de pérdida no se puedan utilizar las claves.

Si la clave privada es para una máquina (para hacer comunicaciones seguras por la Red), tiene que estar en un directorio solo accesible para el usuario administrador y solo con permiso de lectura para este usuario. Las claves públicas están asociadas a los usuarios, pero para asegurar que una clave pública concreta pertenece a un determinado usuario se utilizan los certificados digitales.

Los certificados digitales son documentos electrónicos que asocian una clave pública con la identidad de un usuario. Además de estos datos, un certificado digital puede contener otros atributos, como por ejemplo la fecha de principio y fin de validez o el ámbito en el que se puede utilizar esta clave pública.

¿Cómo sabemos que es válido un certificado digital? Puede suceder que alguien falsifique el certificado digital de Roberto; de este modo, cuando Alicia consulte el certificado digital de Roberto y obtenga su clave pública para mandarle un mensaje, en realidad habrá obtenido la clave pública de una tercera persona que quiera conocer la comunicación que mantienen los dos. De este modo, cuando Alicia mande un mensaje a Roberto este no lo podrá descifrar, pero sí lo podrá hacer la tercera persona que está a la escucha.

La validez de un certificado es muy importante para la comunicación, puesto que mediante el certificado nosotros confiamos en que la persona a quien identifica este certificado es la que esperamos que sea. La manera de confiar en un certificado digital de una persona con la que hasta ahora no hemos tenido ninguna relación consiste en el uso de lo que se denominan terceras personas de confianza. La idea es que dos usuarios puedan confiar entre sí si los dos tienen en común a una tercera persona que dé fe del proceso. Esta idea no es nueva: en el ámbito comercial tradicional, esta figura es el notario. En el caso concreto del mundo electrónico, esta tercera persona es la entidad certificadora o autoridad de certificación (CA).

Un certificado es de mayor confianza si lo avala una entidad certificadora que si no lo avala nadie. ¿Cómo sabemos, sin embargo, que esta entidad certificadora es reconocida? La respuesta la encontramos en la estructura de las entidades certificadoras. Esta estructura es jerárquica (parecida a la estructura del servidor de nombres de dominio o DNS): hay una entidad certificadora a escala mundial que certifica a las entidades certificadoras principales de cada país, las cuales, a su vez, certifican a las entidades certificadoras de cada comunidad, y así de manera sucesiva hasta llegar a las entidades que, como usuarios, nos pueden emitir un certificado digital. El modelo de confianza basado en terceros de confianza (TTP) es la base de la definición de la infraestructura de clave pública o *public-key infrastructure* (*PKI*). Una PKI es un conjunto de protocolos, servicios y estándares que son compatibles con aplicaciones basadas en criptografía de clave pública. Este sistema se considera seguro, pese a que en algunos casos se han vulnerado sistemas, y terceras personas han obtenido certificados válidos que han utilizado para certificar programas que eran maliciosos. La solución viene dada por la revocación de estos certificados generales y, por lo tanto, de todos los que puedan colgar de estos.

1.6. Petición de un certificado

Un servidor también puede tener un certificado. Estos certificados se utilizan en la familia de protocolos denominados seguros. Los pasos que se tienen que seguir son, en primer lugar, pedir un certificado para un servidor y, después,

instalar este certificado. La instalación del certificado en la máquina es tan fácil como ponerlo en un directorio. Para usar un certificado, sin embargo, no basta con tenerlo en la máquina, sino que debemos configurar los servicios que lo quieren utilizar para que puedan trabajar con certificados. En el módulo siguiente, explicaremos cómo se instalan y se configuran la mayoría de los servicios; por lo tanto, es en aquel módulo donde comentaremos los pasos que se tienen que seguir para configurar los certificados en los diferentes servicios.

2. Certificados en GNU/Linux

El primer paso es asegurarnos de que tenemos instalado el paquete `openssl`. Para saber si tenemos instalado un paquete en nuestro servidor, debemos utilizar la aplicación de gestión de paquetes de Debian. De este modo, ejecutamos la orden siguiente.

```
root# dpkg -l openssl
```

Un resultado parecido a este:

```
root@debian:~# dpkg -l openssl
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-instr/trig-aWait/Trig-pend
|/Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name Version Description
+++-==============-==============-====================================
ii  openssl  0.9.8o-4squeez Secure Socket Layer (SSL) binary and related
root@debian:~#
```

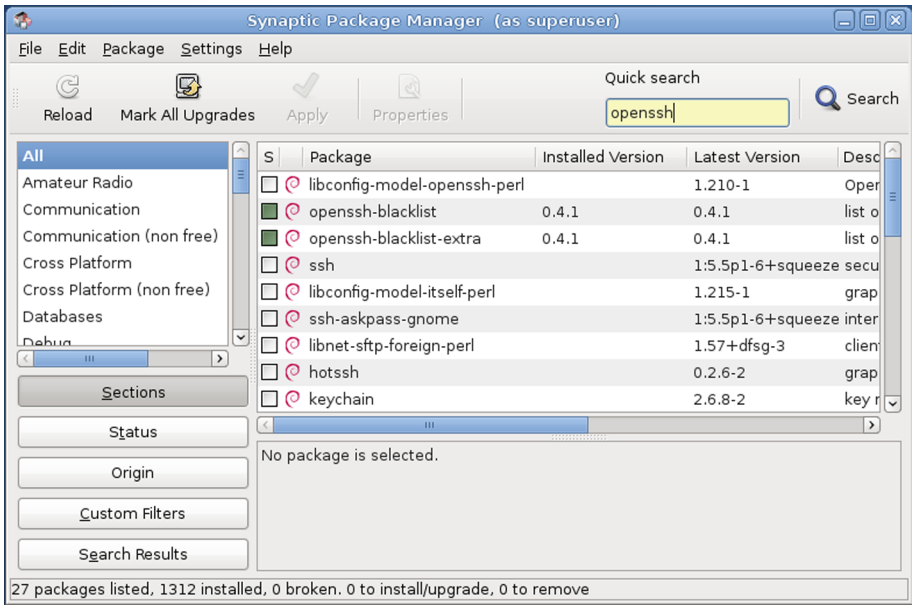
nos indica que tenemos este paquete instalado y, además, qué versión usamos. Si en el campo `version` sale `<none>` y la descripción del paquete no está disponible, entonces no tenemos el paquete instalado.

Para solucionarlo, solo hay que instalar el paquete usando la orden apt-get:

```
root# apt-get install openssl
```

o directamente desde el gestor de paquetes Synaptic:

Gestor de paquetes Synaptic



El siguiente paso es crear una clave privada para nuestra máquina. Para hacerlo, solo tenemos que ejecutar la orden siguiente:

```
root# openssl genrsa -aes256 -out Server.key 1024
```

Esto genera una clave privada de 1.024 bits, con el formato de encriptación AES. La clave se crea en el directorio en el que estamos, con el nombre `Server.key`.

También podemos proteger la clave privada generada con una contraseña. Si no queremos poner ninguna contraseña, cuando nos lo pida tenemos que pulsar la tecla "Enter". No pasa nada si después cambiamos de opinión, puesto que hay órdenes para cambiar las contraseñas de las claves privadas.

Para cambiar la contraseña de una clave privada, debemos ejecutar las órdenes siguientes.

```
root# openssl rsa -aes256 -in Server.key -out Server.key.new
root# mv Server.key.new Server.key
```

La primera orden nos pide la contraseña vieja de la clave privada y después nos pide la nueva, y escribe el resultado en un fichero nuevo (`server.key.new`). El último paso sobrescribe el fichero con la clave vieja. De este modo, no hace falta cambiar la configuración de ninguna aplicación que utilice este nombre de fichero como clave privada del servidor.

Una vez disponemos de la clave privada, podemos generar la clave pública a partir de esta. Para hacerlo, podemos certificar nosotros mismos esta clave pública, algo no muy recomendable, puesto que entonces nadie confiará en

nosotros porque no nos avalará ninguna entidad certificadora; o podemos hacer una solicitud de certificado de firma o *certificate signing request* (*CSR*) a una entidad certificadora avalada.

Evidentemente recomendamos el uso de esta opción, puesto que así las comunicaciones con terceras personas estarán más seguras y se dará más confianza a las mismas.

Para hacerlo, tenemos que ejecutar la orden:

```
root# openssl req -new -key server.key -out server.csr
```

Cuando se ejecuta esta orden, lo primero que pide es la contraseña de la clave privada con la que se quiere crear la clave pública; después el país, el estado o la región, la ciudad, la organización o empresa, la sección de la empresa, el nombre del administrador de la máquina y una dirección de correo electrónico. Finalmente, nos pide unos atributos adicionales; si no se los queremos poner, pulsamos la tecla "Enter".

Una vez tenemos la petición de un certificado, debemos enviar esta petición (`server.csr`) a una entidad certificadora. Cuando nos retornen la petición (`server.pem`), ya tenemos un certificado real que podemos utilizar para configurar los servicios seguros que queremos que tenga el servidor.

Este último paso, el de enviar el certificado a una entidad, varía un poco según la entidad que elijamos para que nos certifique. En Internet hay algunas entidades que lo hacen (Verisign, Thawte Consulting, BelSign, etc.), en las que es posible contratar la validación de los certificados anualmente y que también ofrecen otros servicios para hacer más segura la comunicación por la Red.

2.1. Creación de una CA

La creación de nuestra propia CA es a veces un proceso innecesario, puesto que nuestros certificados autenticados por nosotros mismos no tienen mucha credibilidad. Hay casos, sin embargo, en los que este proceso resulta muy útil; por ejemplo, casos en los que solo puedan acceder a nuestra intranet los usuarios que tienen un certificado avalado por nosotros. Clientes que tienen que conectarse tanto a la red Wi-Fi, como a la parte segura de la intranet.

En primer lugar, tenemos que crear una clave privada para la CA. Para hacerlo, ejecutamos la orden siguiente:

```
root# openssl genrsa -des3 -out ca.key 1024
```

Al igual que en los casos anteriores, tenemos que guardar muy bien este fichero puesto que es nuestra clave privada de la autoridad certificadora local que se está creando.

En segundo lugar, una vez tenemos la clave privada, debemos certificarla con nuestro propio certificado. Para hacerlo, ejecutamos la orden siguiente:

```
root# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

Que creará un certificado (`can.crt`) de un año de validez con formato x509.

Ahora, en principio, ya estamos en disposición de certificar nuestros propios certificados, pero para hacerlo primero debemos tener un *script* de certificación. Podemos hacer nuestro propio *script* o, si hemos instalado el `mod_ssl` mediante la complicación del código fuente, podemos encontrar un *script* de certificación en el directorio `pkg.contri/sign.sh` de las fuentes. En cualquier caso, el *script* ha de ser parecido a este:

```
#!/bin/sh
#  argument line handling
CSR=$1
if [ $# -ne 1 ]; then
echo "Usage: sign.sign <whatever>.csr"; exit 1
fi
if [ ! -f $CSR ]; then
echo "CSR not found: $CSR"; exit 1
fi
case $CSR in
*.csr ) CERT="`echo $CSR | sed -e 's/\.csr/.crt/'`" ;;
* ) CERT="$CSR.crt" ;;
esac
#  make sure environment exists
if [ ! -d ca.db.certs ]; then
mkdir ca.db.certs
fi
if [ ! -f ca.db.serial ]; then
echo '01' >ca.db.serial
fi
if [ ! -f ca.db.index ]; then
cp /dev/null ca.db.index
fi
#  create an own SSLeay config
cat >ca.config <<EOT
[ ca ]
default_ca = CA_own
[ CA_own ]
dir = .
```

```
certs = \$dir
new_certs_dir = \$dir/ca.db.certs
database = \$dir/ca.db.index
serial = \$dir/ca.db.serial
RANDFILE = \$dir/ca.db.rand
certificate = \$dir/ca.crt
private_key = \$dir/ca.key
default_days = 365
default_crl_days = 30
default_md = md5
preserve = no
policy = policy_anything
[ policy_anything ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
EOT
# sign the certificate
echo "CA signing: $CSR -> $CERT:"
openssl ca -config ca.config -out $CERT -infiles $CSR
echo "CA verifying: $CERT <-> CA cert"
openssl verify -CAfile ca.crt $CERT
# cleanup after SSLeay
rm -f ca.config
rm -f ca.db.serial.old
rm -f ca.db.index.old
# die gracefully
exit 0
```

Una vez tenemos este *script*, ya podemos certificar. Imaginemos que tenemos una petición de una máquina que se denomina `server.crt`. Para hacer este certificado, tenemos que ejecutar la orden siguiente:

```
root# ./sign.sh server.crt
```

2.2. Revocación de un certificado

Las autoridades certificadoras (CA) no solo avalan los certificados, sino que también los administran. Administrar un certificado implica determinar su periodo de validez, renovarlo o revocarlo. La revocación de un certificado consiste en dejar de avalar uno que hasta ahora era válido.

Ejemplos de revocación de certificado

1) Imaginemos que Alicia empieza a trabajar en una nueva empresa, que le tramita un certificado personal en el momento de entrar. El periodo de validez de este certificado es de dos años, pero al cabo de seis meses Alicia deja la empresa. El certificado de Alicia se tiene que revocar cuando deja la empresa, puesto que a partir de entonces no tiene ninguna vinculación con la misma.

2) Otro ejemplo de revocación de un certificado: detectamos que nuestra máquina ha sido vulnerada, es decir, que se han introducido intrusos en la misma y que, además, lo han hecho con privilegios de administrador. En este caso, el certificado se tiene que revocar porque tenemos dudas sobre la duplicación de nuestra clave privada. No basta con cambiar la contraseña de la clave privada, se tiene que revocar para estar completamente seguros de que no se usará en otro lugar.

Los certificados que se han revocado los publican las autoridades certificadoras en unas listas, que se denominan listas de revocación de certificados o *certificate revocation lists* (*CRL*). Puesto que los certificados se distribuyen muy rápidamente, es imposible saber si lo han revocado mirando solo el certificado.

Cuando nos fijamos en la validez de los certificados, debemos contactar con una autoridad certificadora y comprobar en su lista de revocación si se ha revocado el certificado. La mayoría de las autoridades certificadoras tienen una página web en la que publican los certificados que se han revocado.

Si nosotros tenemos nuestra propia autoridad certificadora y queremos revocar un certificado porque consideramos que ha sido comprometido, debemos ejecutar la orden siguiente:

```
root# openssl -revoke Server.pem
```

Después, tenemos que regenerar la lista de los certificados revocados mediante la orden siguiente:

```
root# openssl ca -gencrl - config /etc/openssl.cnf -out
crl/sopac-ca.crl
```

3. Certificados en Windows Server 2012

Como se ha explicado, una infraestructura de clave pública (PKI) consiste en un conjunto de servicios, tecnologías, protocolos y estándares que permiten llevar a cabo acciones de manera segura en entornos distribuidos. La infraestructura de clave pública de una red, que necesitaremos para los servidores Windows, consta de los elementos siguientes:

1) Certificados digitales. Un certificado digital es una credencial electrónica que se compone de una clave pública y una clave privada, y se utiliza para autenticar a los usuarios.

2) Entidad emisora de certificados. Son entidades de confianza que crean certificados de autenticación. Hay autoridades de certificación reconocidas mundialmente, aunque se puede configurar un emisor de certificados propio para propósitos específicos.

3) Herramientas de administración de claves y certificados. Son herramientas de gestión para administrar certificados digitales en un servidor de emisión de certificados.

4) Punto de publicación de certificados. Lugar donde se almacenan y se publican los certificados. En el caso de entidades emisoras de certificados basadas en Windows, los certificados se almacenan mediante *active directory*, en el módulo adicional que ya se ha instalado y que hace de gestor de certificados. El *AD-CS* (*active directory certificate services*) se encarga de la gestión de los certificados dentro del directorio activo.

5) Aplicaciones y servicios preparados para el uso de claves públicas. Para que los certificados sean útiles, las aplicaciones y los servicios de transferencia de información tienen que estar preparados para usarlos. Ejemplos de aplicaciones preparadas para el uso de certificados son Microsoft Outlook y Microsoft Internet Explorer. También son compatibles con el uso de certificados los servicios de archivos cifrados o *encrypting file system* (*EFS*) y de seguridad del protocolo de Internet.

6) Lista de revocaciones de certificado. Consiste en una lista de certificados que se han revocado (anulado) antes de que caducaran.

3.1. Gestión de certificados

Para gestionar los certificados locales disponibles en el propio sistema Windows, utilizamos la opción "Certificados" de la ventana "Propiedades de Internet", que se abre al seleccionar el elemento "Opciones de Internet" del panel de control del sistema. En esta pantalla (figura siguiente) salen los certificados instalados en la cuenta local del equipo, separados en diferentes categorías.

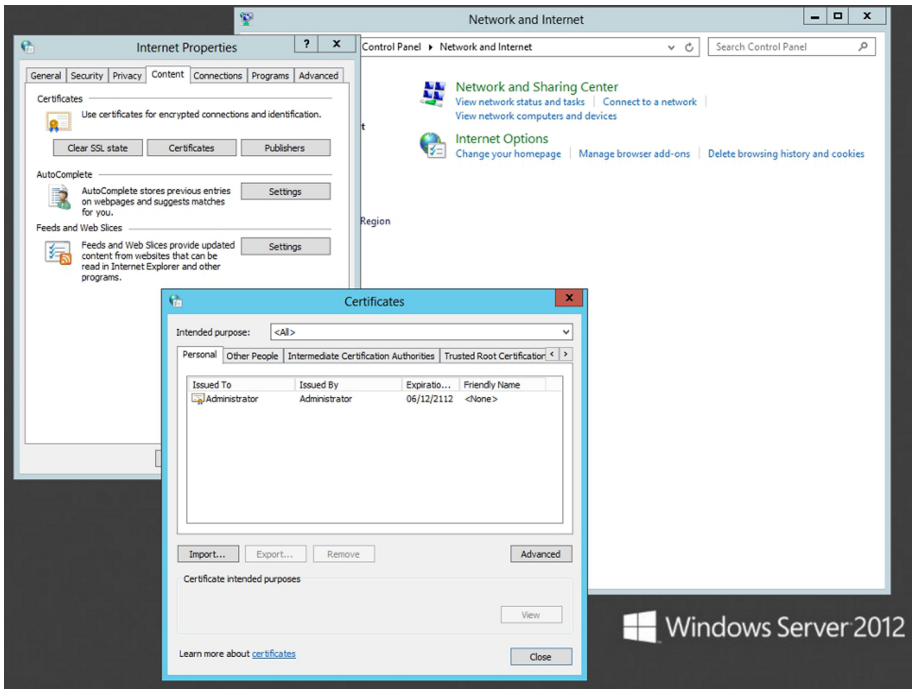
1) Personal: certificados personales con una clave privada que les está asociada.

2) Otras personas: certificados de otras personas con las que se comparte el acceso a ficheros cifrados.

3) Entidades emisoras de certificados intermedias: certificados de entidades de certificación que dependen de otras entidades de certificación.

4) Entidades emisoras de certificados raíz de confianza: certificados de entidades de certificación que emiten certificados raíz de confianza (se confía en los mismos de manera implícita).

Certificados propios del sistema



En la lista de selección "Propósito planteado", podemos filtrar los certificados por el propósito que tienen. Para tener más información sobre un certificado en concreto, hacemos doble clic sobre el elemento correspondiente en la lista de certificados o sobre el botón "Ver". Mediante el botón "Modificar propiedades" podemos modificar los propósitos por los que se utiliza este certificado

digital. También podemos modificar los propósitos del certificado seleccionado en la lista de certificados de la ventana "Certificados", mediante el botón "Avanzadas...".

Hay distintos propósitos para un certificado; entre estos, la autenticación de usuarios que acceden al servidor, la firma de código (para permitir la ejecución en otros equipos), la utilización del certificado en mensajes de correo electrónico, la seguridad IP, el cifrado de archivos y la firma de documentos. También es posible definir nuevos propósitos para usos personalizados de los certificados.

3.1.1. Importar y exportar certificados

Podemos importar y exportar certificados con los botones "Importar" y "Exportar" de la ventana "Certificados". También se puede eliminar un certificado mediante el botón "Quitar". Importar un certificado añade un certificado a la lista de certificados que ya hay, ya se trate de un certificado personal, un certificado de otra persona o un certificado de una entidad emisora de certificados. Cuando pulsamos el botón "Importar", empieza el asistente de importación de certificados. Después de seleccionar el archivo que queremos importar, tenemos que seleccionar también el almacén de certificados en el que lo queremos guardar. Podemos dejar que el almacén se seleccione de manera automática o seleccionar un almacén concreto. Un almacén de certificados no es más que una pequeña base de datos en la que se almacena un conjunto de certificados.

Finalmente, el asistente muestra un resumen de la importación del certificado. Una vez aceptamos el resumen, nos pide confirmación para hacer la operación de importación del certificado en el almacén especificado. La exportación de certificados es útil para transmitir una clave pública o como medida de seguridad. Cuando pulsamos el botón "Exportar", empieza el asistente de exportación del certificado seleccionado en la lista.

El asistente nos pide si queremos exportar también la clave privada (en caso de certificados personales que incluyan clave pública y privada) y el formato del archivo de exportación. Finalmente, tenemos que seleccionar la localización y el nombre del fichero donde queremos exportar el certificado. Se tiene que estar seguro de que se quiere exportar también la clave privada, puesto que si se pierde y cae en manos de otra persona, esta podrá hacer absolutamente todo lo que quiera con el certificado. Por lo tanto, si es necesario exportar la clave privada (por ejemplo, para tener una copia de seguridad del certificado y así instalarlo en otro ordenador), se tendrá que proteger con una contraseña lo bastante segura.

3.1.2. Complemento de certificados

Aparte de la ventana de certificados, dentro de la ventana de propiedades de Internet encontramos un complemento del gestor de consola, Microsoft Management Console (MMC), para gestionar certificados. Para instalar el complemento en la consola, la abriremos escribiendo la orden `mmc.exe` en una ventana de PowerShell.

En la ventana de la consola que aparece, se tiene que seleccionar la opción Agregar o quitar complementos del menú Consola. En la ventana de agregar componentes, pulsamos el botón Agregar para agregar el complemento Certificados que hay en la lista de complementos disponibles.

Si se ha iniciado sesión con una cuenta de administrador, aparecen tres opciones sobre los certificados que se gestionarán.

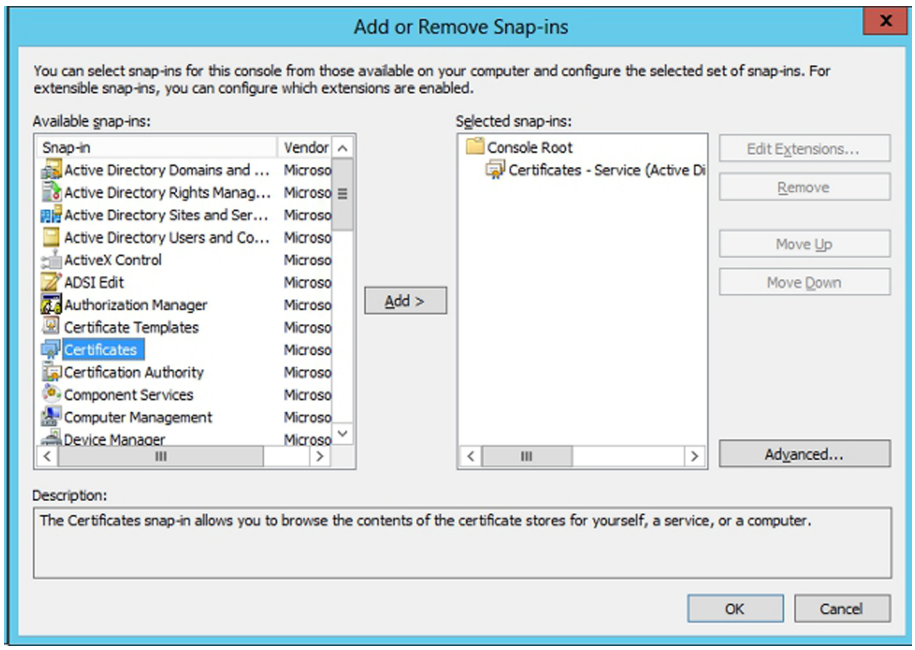
1) Mi cuenta de usuario: permite gestionar los certificados de la cuenta actual.

2) Cuenta de servicio: permite gestionar los certificados de una cuenta de servicio del sistema.

3) Cuenta de equipo: permite gestionar los certificados de una cuenta de otro equipo. Podemos instalar los certificados en otros equipos.

Finalmente sale el nuevo complemento en la consola, donde vemos los certificados organizados por tipos y donde podemos hacer las acciones que ya hemos visto antes sobre certificados.

Complementos para la consola. Instalación de certificados



3.2. Utilización de certificados

Los certificados digitales se pueden usar para distintas utilidades, con el objetivo de garantizar la autenticidad de documentos o autenticar usuarios. Entre estas utilidades, las más comunes son la de firma electrónica, el cifrado de archivos y la autenticación de software por Internet.

3.2.1. Firma electrónica

Los programas de correo como MS Outlook permiten firmar un mensaje de correo electrónico para que el destinatario pueda comprobar que nosotros hemos enviado el mensaje, y no un tercero en nuestro nombre.

Firma en Outlook Express

Para firmar un mensaje en Outlook Express, utilizamos la opción Firmar digitalmente del menú Herramientas de la ventana de creación del mensaje. Esto hace que se firme el mensaje con el certificado digital asociado a la cuenta con la que hemos iniciado sesión.

3.2.2. Cifrado de archivos

El cifrado de archivos sirve para proteger documentos, de tal modo que solo los puedan leer o modificar las personas autorizadas. Para cifrar un archivo, abrimos la ventana de propiedades (opción Propiedades del menú contextual que sale al hacer clic con el botón secundario del ratón sobre el icono del fichero) y pulsamos el botón Avanzadas.... En la ventana que sale seleccionamos la opción "Cifrar contenidos para proteger datos", con lo que se cifra el archivo con el certificado asociado a la cuenta con la que hemos iniciado sesión. Cuando aceptamos, nos pide si queremos cifrar solo el archivo seleccionado o también la carpeta que lo contiene.

Otra opción mucho más nueva y completa es la herramienta BitLocker, que se puede instalar como una característica más del servidor y, por lo tanto, hay que ir al administrador del servidor y hacerlo desde este. Esta herramienta está pensada para entornos más empresariales y permite cifrar únicamente ficheros separados o una unidad entera. Asimismo, permite gestionar todos los discos cifrados de los ordenadores de la red y descifrarlos automáticamente de manera remota, en caso necesario (esto es útil para instalar algún software de manera remota en el caso de que el ordenador cliente tenga el disco completamente cifrado). Esta característica se tiene que instalar aparte, es decir, no forma parte de las características de BitLocker puesto que facilita el acceso a estos discos remotamente.

Además, permite cifrar todo un volumen (un disco entero) o solo el contenido, lo que hará que sea mucho más rápido y, además, que la parte que no está cifrada puedan utilizarla otras personas. Por lo tanto, se puede pensar en que cada usuario tenga una parte del disco duro del ordenador –sobre todo los portátiles– cifrada y el resto no, de modo que este recurso sea compartido sin que la información de un usuario pueda ser accedida por otro usuario sin

permiso. Esto se configura directamente desde las políticas de grupo del directorio activo, por lo que se tiene mucho más control sobre los ordenadores, si es preciso. Se puede dejar que el usuario decida qué quiere cifrar de su disco duro, o decidir que se tiene que cifrar todo el volumen o solo la parte con datos y liberar el resto del disco. Se puede encontrar en la política de grupo:

```
\Configuración del equipo\Directivas\Plantillas administrativas\Componentes de Windows\
Cifrado de unidad BitLocker
```

Que aparecerá en el momento de instalar la característica de cifrado con BitLocker.

3.2.3. Aceptación de certificados

Las aplicaciones web tienen una serie de acciones restringidas para evitar que aplicaciones malintencionadas puedan dañar el sistema del usuario. A veces, encontramos páginas web que requieren algunos privilegios –en principio vetados– para llevar a cabo la actividad que tienen que hacer, como por ejemplo acceder al disco duro. Para esto, se firma digitalmente la aplicación de modo que cada usuario puede decidir si confía o no en la entidad que ha desarrollado la aplicación.

Certificado de Microsoft

La primera vez que visitamos el centro de actualizaciones de Microsoft (Windows Update), se nos pide la confirmación para ejecutar el componente necesario para hacer las actualizaciones. Si aceptamos, se instala el certificado de Microsoft, al que se dan los privilegios necesarios para hacer las actualizaciones. También podemos confiar siempre en el certificado de Microsoft (mediante la casilla de selección o *checkbox*), de modo que no nos vuelva a pedir confirmación para instalar ningún componente web desarrollado y firmado por Microsoft (se instala directamente).

3.3. Emisión de certificados

Tenemos básicamente dos maneras de obtener un certificado digital. Si necesitamos el certificado para hacer operaciones de autenticación con otras personas ajenas a nuestra empresa, para solicitar permisos en una página web con el fin de ejecutar código no seguro, etc. tenemos que solicitar el certificado a una entidad certificadora de confianza. En cambio, si el certificado es para hacer gestiones dentro de la empresa misma, lo más seguro es que haya un servidor de certificación que gestione y emita los certificados a los trabajadores.

3.3.1. Entidad certificadora de confianza

Hay entidades de certificación conocidas como Securenet (www.securenet.net), Verisign (www.verisign.com) o Thawte (www.thawte.com) que emiten certificados de autenticación que son acepta-

dos en la mayoría de las aplicaciones, puesto que los certificados de estas compañías están incluidos en el almacén de certificados predeterminado del sistema operativo Windows.

Encontramos otras entidades de certificación con propósitos más específicos, como por ejemplo la Fábrica Nacional de Moneda y Timbre en el Estado español, que expiden los certificados digitales que identifican a los usuarios a la hora de hacer gestiones con la Administración pública y Hacienda por Internet (www.cert.fnmt.es).

3.3.2. Servidor de certificación

El trabajo de un servidor de certificación lo tienen que llevar a cabo un servidor o más de un servidor de la empresa. Su cometido es recibir solicitudes de emisión o renovación de certificados por parte de los usuarios (trabajadores o quizá clientes de la empresa) que necesiten este certificado para hacer alguna gestión.

Como se ha indicado anteriormente, Windows Server 2012 incorpora ADCS (*active directory certificate server*), que proporciona esta funcionalidad. Para instalar este rol, basta con seleccionarlo en el administrador del servidor, como se ha indicado en el apartado de la instalación. A continuación, nos avisan de que si instalamos estos servicios no podremos cambiar el nombre del servidor más adelante, ni añadirlo ni quitarlo de un dominio, puesto que los certificados pertenecen al servidor con aquellas características. Antes de instalar el rol, también tenemos que especificar el tipo de servidor de certificados que queremos instalar, que dependerá de lo que se quiera hacer en cada caso.

Los tipos de entidad emisora de certificados que se pueden configurar son los siguientes:

1) Entidad emisora raíz de la empresa: entidad principal, de máxima confianza en la empresa.

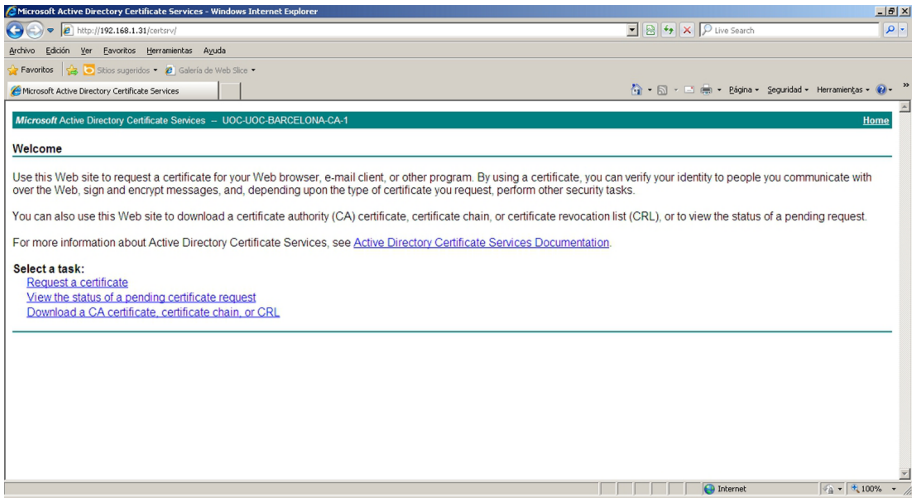
2) Entidad emisora subordinada de la empresa: entidad secundaria de certificación en la empresa. Tiene que obtener un certificado de entidad emisora de certificados de otra entidad emisora de certificados de la empresa.

3) Entidad emisora raíz independiente: entidad principal, de máxima confianza en una jerarquía.

4) Entidad emisora subordinada independiente: entidad secundaria de certificación en una jerarquía. Tiene que obtener un certificado de entidad emisora de certificados de otra entidad emisora de certificados.

Una vez introducidos todos los datos, empieza el proceso de instalación. En el caso de tener también instalado el rol de inscripción web (*web enrollment*), el proceso de instalación crea una serie de páginas web que permiten a los usuarios de los equipos clientes –o desde otros servidores– acceder al servidor emisor de certificados para solicitar un certificado digital. La dirección de la página inicial de solicitud de certificados es `http://nombreservidor/certsrv`, en la que `nombreservidor` es el nombre del servidor de emisión de certificados. Dependiendo de la configuración del servidor de información de Internet (IIS), es posible que nos tengamos que autenticar antes de acceder al sitio web, aunque una vez validados podemos acceder directamente al mismo utilizando las credenciales del usuario con el que estamos autenticados en nuestra estación de trabajo.

Página web de obtención y renovación de los certificados



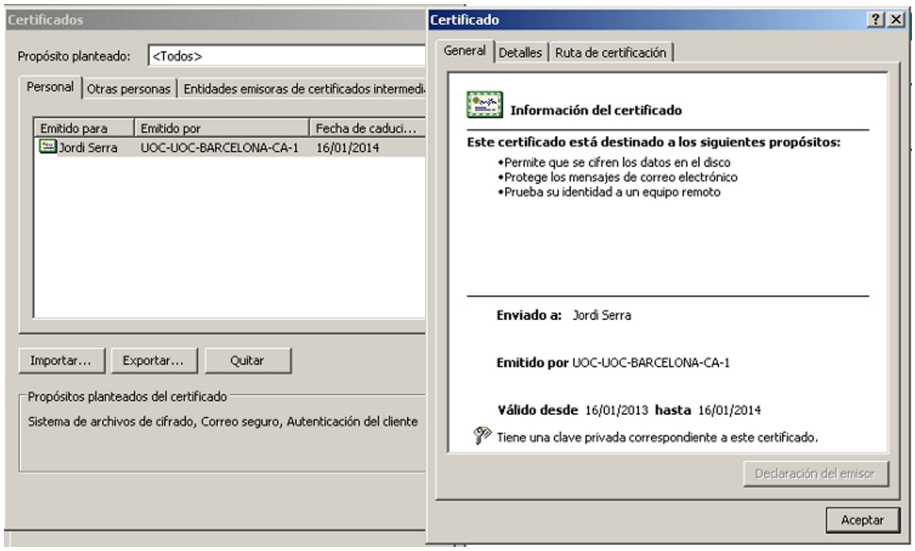
En la pantalla inicial de esta página web (figura anterior) encontramos tres opciones.

1) Solicitar un certificado: permite solicitar un certificado a la entidad de certificación.

2) Ver el estado de una solicitud de certificado: permite comprobar el estado de un certificado solicitado con anterioridad.

3) Bajar un certificado de entidad emisora, cadena de certificados o lista de revocación: permite recuperar el certificado de la entidad emisora de certificados o la lista de certificados que ha revocado esta entidad.

Certificado instalado



Para solicitar un certificado, seleccionamos la primera opción. En la página siguiente, seleccionamos el tipo de certificado. En el caso de una entidad emisora de empresa, el único tipo de certificado disponible es el certificado de usuario. En cambio, en una entidad emisora independiente podemos solicitar certificados para exploración web o de protección de correo electrónico.

Si la entidad de certificación es de empresa, la información del usuario se recupera de manera automática y el certificado se emite directamente. En la página siguiente, se puede instalar el certificado.

Si vamos a la herramienta "Entidad de certificación" de "Herramientas administrativas" o a las propiedades de Internet, vemos el nuevo certificado emitido (figura anterior). Desde esta herramienta, también podemos revocar certificados emitidos anteriormente, revisar peticiones pendientes de certificados, etc.

En cambio, si la entidad de certificación es independiente, hay que introducir los datos del usuario o del equipo para el que pedimos el certificado. La petición de la solicitud queda pendiente en el servidor hasta que un administrador confirme la emisión del certificado.

Si vamos a la herramienta "Entidad de certificación", vemos que hay un certificado pendiente. Mediante las opciones del menú "Acción" podemos emitir el certificado solicitado o denegarlo.

Para comprobar el estado de tramitación de un certificado, podemos utilizar la segunda opción de la página web del servidor de certificación. Seleccionamos el certificado solicitado y en la página siguiente se nos muestra el estado del certificado, tanto si está denegado como pendiente de tramitación o concedido. En este último caso, se nos permite bajarlo e instalarlo.

La última de las opciones de la página web del servidor de emisión de certificados es recuperar el certificado de la entidad de certificación, o la lista de certificados revocados, para no confiar en estos certificados de ahora en adelante. Bajar el certificado de la entidad emisora permite confiar en los certificados que ha emitido la entidad. En lo que respecta a la ruta de certificación de la entidad, no hay que instalarla si se ha solicitado e instalado un certificado que ha emitido esta entidad, puesto que se instala de manera automática.

Si elegimos bajar la lista de revocación de certificados, obtenemos un archivo con extensión .clr. Para instalar la lista, seleccionamos la opción "Instalar CRL" del menú contextual que sale al hacer clic en el botón secundario del ratón sobre el archivo que hemos bajado. A continuación, empieza el asistente de importación de certificados que ya hemos visto antes para importar la lista de certificados revocados al almacén de certificados que seleccionemos.

4. IPsec

IPsec es una extensión del protocolo IP que proporciona seguridad al protocolo IP y a los protocolos de capas superiores. La arquitectura de IPsec está descrita en la RFC2401. En los párrafos siguientes, veremos una pequeña introducción a este protocolo y después veremos cómo se configura de manera básica en entornos GNU/Linux y en entornos Windows. Para dar seguridad al protocolo IP, IPsec utiliza dos protocolos: la autenticación de cabecera o *authentication header* (*AH*) y la carga de seguridad encapsuladora o *encapsulating security payload* (*ESP*). La función de estos dos protocolos es asegurar la autenticación, la integridad y la confidencialidad de la comunicación. Puede proteger el datagrama IP completo (modo túnel) o solo los protocolos de capas superiores (modo transporte). En el modo túnel, el datagrama IP es "encapsulado" dentro de otro datagrama IP, con una cabecera IPsec segura, mientras que en el modo transporte solo añade la cabecera IPsec al datagrama original. Como se muestra en la tabla siguiente:

Estructura de los paquetes TCP/IP

Paquete original	IP	TCP	Datos			
Paquete en modo transporte	IP	AH	TCP	Datos		
Paquete en modo túnel	IP	AH	IP	TCP	Datos	

Con el objetivo de asegurar la confidencialidad, IPsec utiliza claves simétricas pero, como hemos visto antes, estas claves tienen un problema: ¿cómo se tienen que distribuir? Para solucionar este problema, se desarrolló un protocolo de intercambio de claves por Internet denominado protocolo de Internet de intercambio de claves o *Internet key exchange* (*IKE*), basado en dos fases. En la primera fase se autentica a los participantes de la comunicación y, en la segunda, se negocian las asociaciones de seguridad y se eligen las claves. Además, el protocolo IKE utiliza claves dinámicas.

Las claves dinámicas son una medida de seguridad añadida, puesto que las claves simétricas resultan fáciles de descifrar: solo es una cuestión de tiempo. Cuanto más tiempo utilicemos esta clave, más posibilidades hay de que la descifren. Por lo tanto, las claves dinámicas se basan en ir cambiando las claves simétricas que se utilizan de manera periódica, previa negociación en los dos extremos de la comunicación. De este modo, las claves se van renovando y, si utilizamos poco tiempo cada clave simétrica, nos aseguramos la confidencialidad de la comunicación.

Hemos visto que en la segunda fase del protocolo IKE se negocia una "asociación de seguridad". En una asociación de seguridad o *security association* (*SA*) se almacenan todos los parámetros que intervienen en una comunicación IPsec. Estos parámetros son los siguientes:

1) La dirección IP origen y destino de la cabecera IPsec.

2) El protocolo IPsec utilizado (AH o ESP).

3) Los algoritmos de clave dinámica que utiliza IPsec.

4) El índice de parámetro de seguridad o *security parameter index* (SPI). Es un número de 32 bits que identifica la asociación de seguridad.

Estas asociaciones de seguridad se almacenan en bases de datos de asociaciones de seguridad o *security association databases* (*SAD*). Algunas de estas bases de datos permiten almacenar más parámetros de las asociaciones (modo túnel o transporte, tamaño de la ventana deslizante y tiempo de vida de la SA).

Una SA solo protege un sentido de la comunicación; si queremos proteger la comunicación de manera bidireccional, necesitamos dos asociaciones de seguridad. Además, las SA solo especifican cómo se supone que IPsec tiene que proteger el tráfico, pero no definen qué tráfico se tiene que proteger y cuándo se debe hacer. Para definir estos casos, se requiere información adicional. Esta información adicional se almacena en la política de seguridad o *security policy* (*SP*). La información que se almacena en una SP es la siguiente:

1) Direcciones origen y destino de los paquetes que se protegerán. Si usamos el modo transporte, son las mismas direcciones que las almacenadas en la SA. Si utilizamos el modo túnel, puede que estas direcciones no coincidan con las almacenadas en la SA.

2) Protocolos y puertos que se tienen que proteger. Si la implementación de IPsec que utilizamos no es compatible con la definición de protocolos, se tiene que proteger todo el tráfico que circula entre las direcciones IP origen y destino.

3) La asociación de seguridad que se utiliza para proteger los paquetes. Las políticas de seguridad SP se almacenan en bases de datos de políticas de seguridad o *security policy databases* (*SPD*).

4.1. Instalación de IPsec en GNU/Linux

En este apartado, explicaremos cómo se instala y se configura IPsec en un sistema operativo basado en GNU/Linux. Tenemos que instalar las herramientas de espacio de usuario. Para hacerlo, ejecutamos la orden siguiente:

```
root# apt-get install ipsec-tools.
```

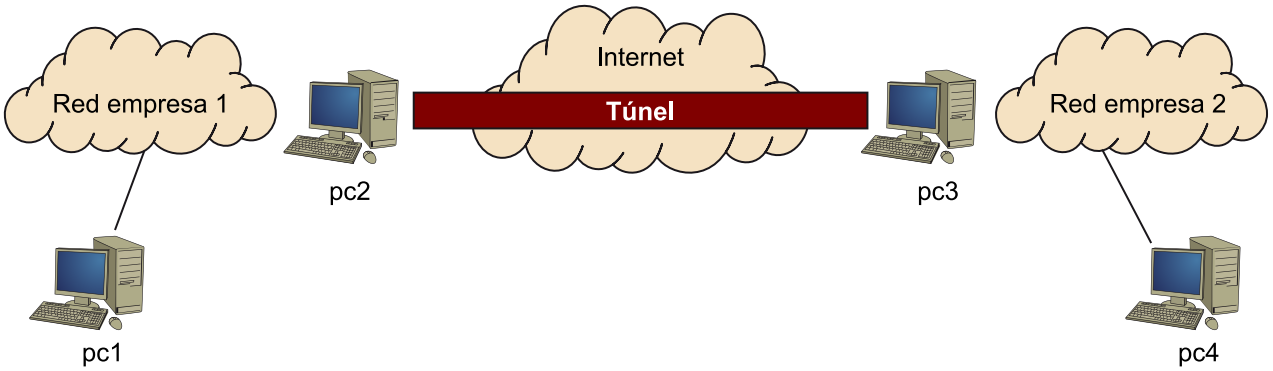
Una vez acabada la instalación, estamos en disposición de empezar la configuración de los archivos.

4.1.1. Modo túnel

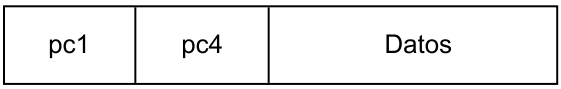
Antes de empezar con la configuración de IPsec en modo túnel, explicaremos un poco el concepto de túnel.

Imaginemos una empresa que tiene dos sedes, una en Barcelona y otra en Madrid, pero que solo dispone de un servidor para las dos redes. Para que los usuarios de las dos redes pudieran acceder a todos los servicios, solo había una solución: una línea telefónica dedicada entre las dos sedes (lo que implica unos gastos adicionales a la empresa). La idea de túnel apareció para solucionar este problema.

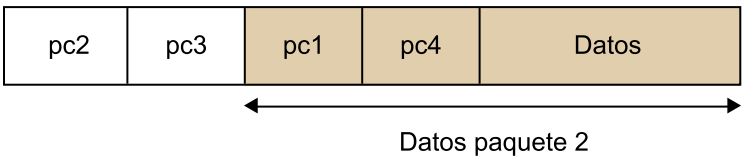
Para explicar qué es un túnel, nos basaremos en el esquema de red siguiente:



Imaginemos que el pc1 se quiere comunicar con el pc4. Entonces, genera un paquete IP cuyo origen es el pc1 y el destino, el pc4. Al paquete resultante lo denominamos paquete1, y es algo parecido a esto:



Cuando el paquete1 llega al pc2, este pc2 detecta que el pc4 es la red_empresa2. Entonces encapsula el paquete1 dentro de otro paquete (que denominamos paquete2), en el que pc2 es el origen y pc3 es el destino. El aspecto del paquete2 es algo parecido a esto:



Cuando el paquete2 llega al pc3, este pc3 detecta que se trata de un paquete del túnel. Desencapsula el paquete2 (es decir, recupera el paquete original, paquete1) y lo envía a la red_empresa2, en la que por funcionamiento IP llega al pc4.

El funcionamiento del túnel es completamente transparente a los usuarios de las dos redes de la empresa y para cualquier observador de Internet, que solo ve comunicación entre el pc2 y el pc3. El funcionamiento del túnel original

viaja plano, es decir, sin cifrar. Utilizando el protocolo IPsec conseguimos que los datos se codifiquen, de modo que la comunicación entre el pc1 y el pc4 es confidencial y segura puesto que está cifrada.

Para configurar el modo t¼nel, tenemos que configurar el fichero `/etc/ipsec-tools.conf`. A continuaci·n, mostramos un fichero `ipsec-tools.conf` adecuado al esquema de red que indica la figura, y que utiliza ESP como protocolo seguro. Hay que se¶alar que, para que el t¼nel funcione mediante IPsec, tenemos que configurar las dos m§quinas en los extremos del t¼nel.

```
#!/usr/sbin/setkey -f

# Flush the SAD and SPD
flush;
spdflush;

add address_pc2 address_pc3 esp 0x201 -m tunnel -E 3des-cbc \
0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831 \
-A hmac-md5 0xc0291ff014dccdd03874d9i8i4cdf3i6;

add address_pc3 address_pc2 esp 0x301 -m tunnel -E 3des-cbc \
0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df \
-A hmac-md5 0x96358c90783bbfa3d7b196ceabe0536b;

# Security policies
spdadd net_company 1 net_company2 any -P out ipsec
esp/tunnel/ address_pc2-address_pc3 /require;
spdadd net_company2 net_company1 any -P in ipsec
esp/tunnel/ address_pc3-address_pc2 /require;
```

En este archivo de configuración, vemos que no están puestas las direcciones IP de las máquinas encargadas de hacer el túnel (`address_pc2` y `address_pc3`), puesto que dependen del esquema de red que tengamos nosotros. Sucede lo mismo con las direcciones de las redes protegidas en las que se aplican las políticas de seguridad (`net_company1` y `net_company2`).

4.1.2. Modo transporte

Para poner un ejemplo de configuración del protocolo IPsec en modo transporte, utilizaremos el esquema de red entre dos puntos.

Al igual que en el caso anterior, en modo túnel el fichero de configuración que tenemos que editar es `/etc/ipsec-tools.conf`. En este caso, mostraremos el ejemplo mediante el uso del protocolo IPsec AH.

```
#!/usr/sbin/setkey -f
```

```
# Flush the SAD and SPD
flush;
spdflush;

add address_pc1 address_pc2 ah 0x200 -A hmac-md5 \
0xc0291ff014dccdd03874d9i8i4cdf3i6;
add address_pc2 address_pc1 ah 0x300 -A hmac-md5 \
0x96358c90783bbfa3d7b196ceabe0536b;

# Security policies
spdadd address_pc1 address_pc2 any -P out ipsec
ah/transport//require;
spdadd direccion_pc2 direccion_pc1 any -P in ipsec
ah/transport//require;
```

Este archivo configura IPsec en el pc1; si queremos configurar el pc2 tenemos que intercambiar `-P out` por `-P in`, y viceversa. En segundo lugar, y a modo de ejemplo, podemos utilizar las claves que hay en la definición de la asociación de seguridad (SA) del protocolo AH, pero conviene crear nuestras propias claves. Una vez tenemos configurados los dos extremos, lo ponemos en marcha mediante la orden:

```
root# setkey -f /etc/ipsec-tools.conf
```

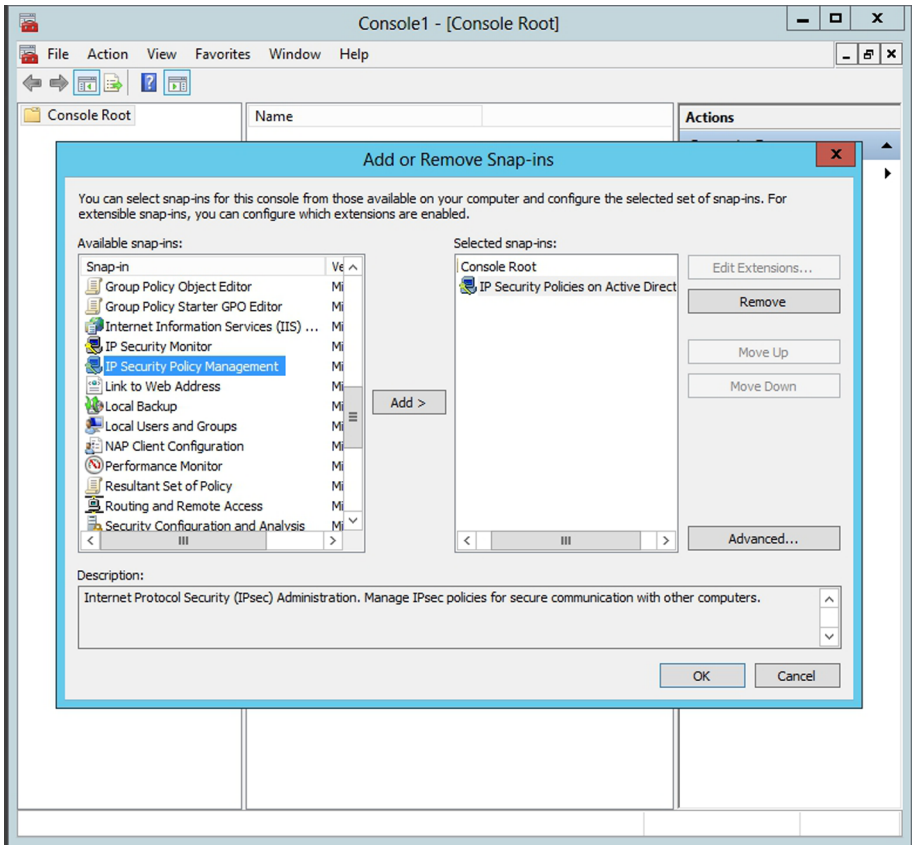
Para comprobar el funcionamiento de IPsec, podemos mostrar las diferentes bases de datos (SAD y SPD) mediante las órdenes siguientes:

```
root# setkey -D
root# setkey -DP
```

4.2. Herramientas de control de IPsec en Windows Server 2012

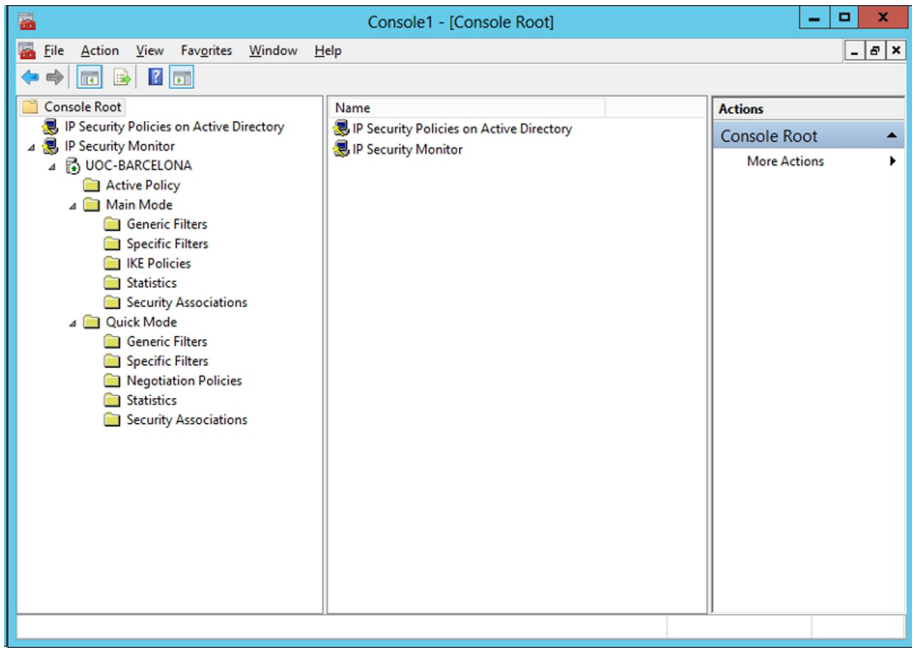
Para configurar IPsec, utilizamos el complemento "Directivas de seguridad local" de la consola de administración. Para abrir este complemento, en PowerShell escribimos `mmc.exe` para acceder a la consola. Para añadir el complemento, seleccionamos la opción "Agregar o quitar complemento" del menú "Acción". En la nueva ventana, hacemos clic sobre el botón "Agregar" y en la lista de elementos seleccionamos "Administración de las directivas de seguridad de IP" (figura siguiente). A continuación seleccionamos el equipo sobre el que queremos administrar las directivas IPsec, que podría ser el propio sistema en local o el directorio activo. Una vez hecho esto, se agrega el complemento al árbol de la consola de administración. Este complemento nos permite utilizar políticas de IPsec predefinidas o definir otras nuevas, como veremos a continuación.

Instalación IPSec



Otra herramienta que nos resulta útil para comprobar la seguridad IP del servidor y de los equipos en general del directorio activo es el monitor de seguridad IP, que se puede añadir como el complemento “Monitor de seguridad IP” a la consola que acabamos de crear. Por lo tanto, tendremos en la consola, o la máquina local, las políticas de seguridad del directorio activo –configuración que se tendrá que guardar en disco o se perderá– y el monitor de seguridad, tal y como muestra la figura siguiente.

Monitor de seguridad y políticas de seguridad en la consola



4.3. Utilización de directivas IPsec predefinidas

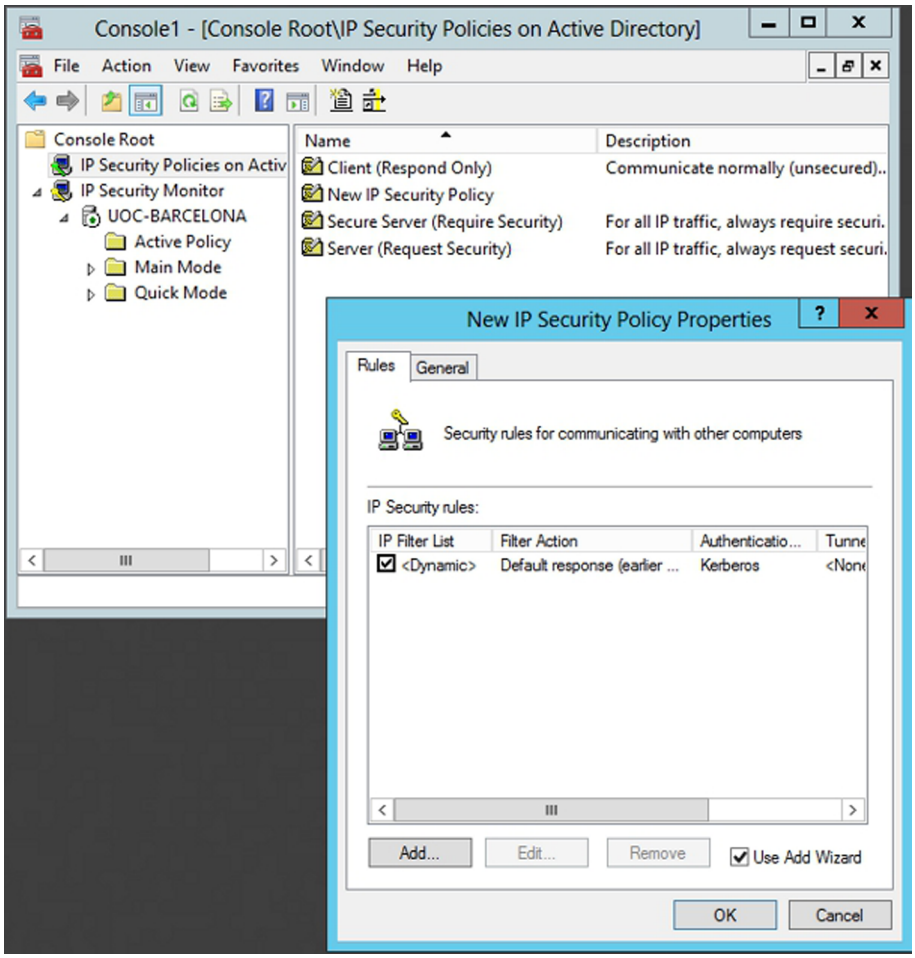
En la parte derecha del complemento de las políticas de IPsec vemos tres directivas predefinidas: cliente (solo responder), servidor (pedir seguridad) y servidor seguro (requiere seguridad). Estas tres directivas ya vienen activadas y, por lo tanto, si es necesario se pueden desactivar con las acciones asociadas a cada directiva.

4.4. Utilización de directivas IPsec personalizadas

Para crear una nueva directiva IPsec personalizada, seleccionamos la opción "Crear directiva de seguridad IP" del menú "Acción", y nos sale el asistente correspondiente. En la primera pantalla asignamos un nombre a la nueva directiva. En la segunda, tenemos que decidir si activamos la regla de respuesta predeterminada en caso de que no se pueda aplicar ninguna otra regla.

En la pantalla siguiente, seleccionamos el tipo de autenticación utilizado en la regla de respuesta predeterminada (si seleccionamos la opción de la ventana anterior). Esto se podría hacer si en el servidor se dispone de los certificados que se han mostrado con anterioridad.

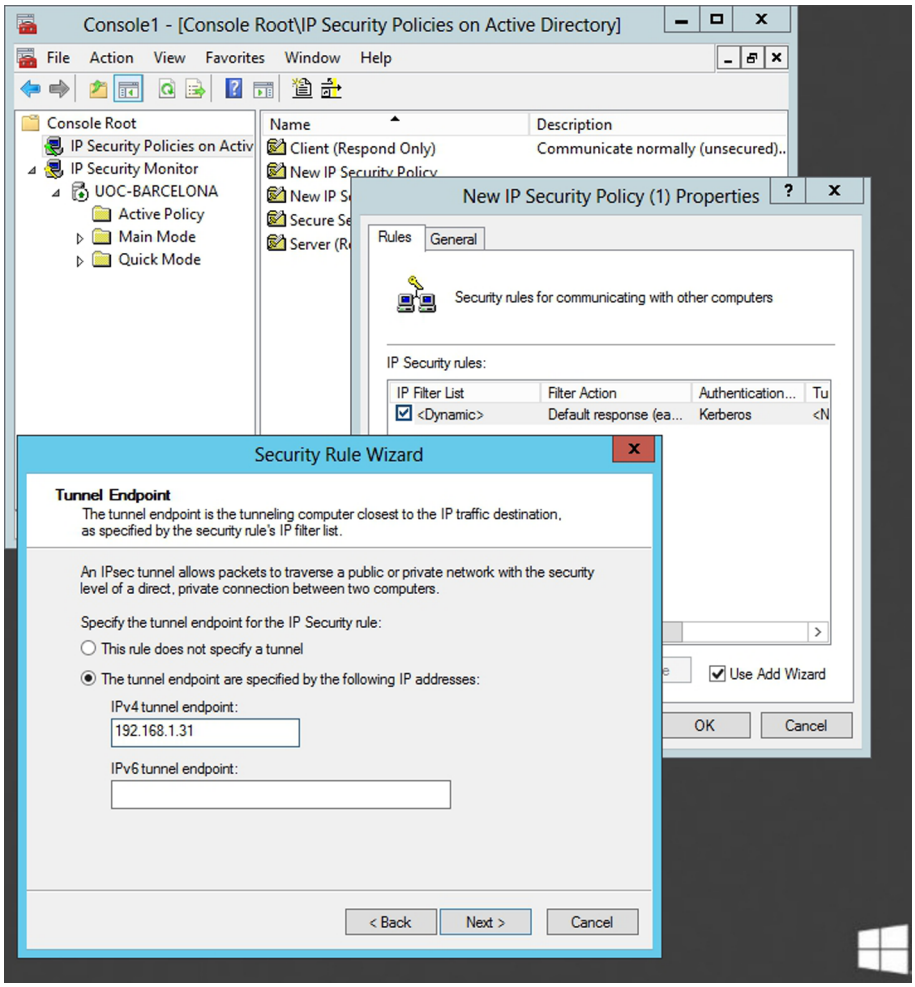
Nueva directriz de seguridad



Se acaba el proceso de crear la nueva directiva. Para modificar sus propiedades, a continuación se puede seleccionar la opción "Modificar las propiedades", que abre la ventana de propiedades de la directiva. En esta ventana vemos las reglas de la directiva. En principio solo está configurada la regla predeterminada, pero podemos añadir más reglas mediante la opción "Agregar". Al agregar una regla nueva dentro de la directiva, sale el asistente correspondiente que va guiando la instalación hasta conseguir lo que se quiere. Esta ventana de configuración del túnel permite, por ejemplo, especificar la IP del otro extremo de una conexión VPN, tal y como muestra la figura siguiente.

En la pantalla siguiente, especificamos el tipo de red a la que es aplicable esta regla: a toda la red, al área local o al acceso remoto hacia este servidor. A continuación, elegimos qué tipo de tráfico es el que se controlará. Podemos especificar con una nueva regla direcciones de IP específicas tanto de entrada como de salida, los protocolos, etc. para acabar marcando si se permite el tráfico o se bloquea, dependiendo de cómo se haya pensado aplicar la regla que se está configurando. Se podría bloquear el tráfico a todos los puertos y direcciones externas al mismo tiempo.

Asignación IP de la VPN en la directiva de seguridad



5. Redes privadas virtuales

Una red privada virtual o *virtual private network* (*VPN*) es un túnel de información privada que lleva datos de un extremo al otro y lo hace utilizando una red pública (como por ejemplo, Internet), sin que la comunicación de extremo a extremo se dé cuenta de que utiliza una red pública y sin que los nodos intermedios de la red pública se den cuenta de que los atraviesa un túnel de información privada. La gran ventaja de las VPN es que permiten construir redes privadas de una manera mucho más barata que implantando un enlace dedicado entre los diferentes extremos de la comunicación privada.

La implantación de VPN es una tarea compleja, puesto que hay muchos tipos de soluciones VPN. Además, cada solución se puede llevar a cabo de varias maneras y cada una de estas maneras puede utilizar, a su vez, más de un protocolo de comunicaciones. En este apartado veremos cómo hay que instalar y configurar VPN de diferentes maneras.

5.1. GNU/Linux

5.1.1. Secure Shell

Una primera manera muy sencilla de crear VPN consiste en utilizar el protocolo Secure Shell (SSH). Este método sustituye las aplicaciones Telnet y Rlogin con una aplicación similar (basada en un *shell*) pero que utiliza túneles encriptados para la comunicación. Además, con este protocolo podemos hacer transferencias de ficheros de manera segura (*secure file transfer protocol* o *SFTP*), lo que permite sustituir las transferencias de ficheros que usan canales no cifrados (*file transfer protocol* o *FTP*). Otra ventaja muy importante de este método de creación de VPN es que SSH ofrece más de un método de autenticación, entre los cuales encontramos el nombre de usuario con la contraseña correspondiente y la autenticación basada en certificados.

En general, las desventajas de SSH son, por un lado, la instalación –puesto que, como en la mayoría de las soluciones VPN, el cliente tiene que instalar una aplicación para usar la VPN– y, por otro lado, el protocolo en sí. SSH es un protocolo que ya hace años que está activo; esto ha repercutido en el hecho de que sea muy conocido y estudiado, de modo que se le han encontrado vulnerabilidades, la mayoría de las cuales están en lo que se denomina SSH1. Para solucionar estos problemas salió el denominado SSH2, que ofrece una protección del túnel cifrado mucho mejor que en el caso del SSH1. Por este motivo, nos tenemos que asegurar de que en nuestra máquina instalamos y configuramos solo SSH2.

Hasta ahora hemos visto el protocolo SSH en la forma de funcionamiento habitual, pero con SSH también tenemos la capacidad de crear túneles cifrados. Podemos crear los túneles SSH utilizando la funcionalidad de redirección de puertos o *port forwarding*. Este es su funcionamiento:

1) El servidor ofrece un servicio (inseguro) por su puerto habitual.

2) Mediante la redirección de puertos, redireccionamos el servicio a un túnel cifrado.

3) El cliente tiene instalado un cliente de redirección de puertos.

4) El cliente configura el servicio (inseguro) para utilizar el puerto local donde empieza el túnel cifrado, en lugar del puerto remoto donde se da el servicio inseguro.

5) El cliente envía una petición de servicio (inseguro).

6) Esta petición entra en el túnel cifrado.

7) Llega al otro extremo del túnel, donde la redirección de puertos lo descifra y lo entrega al servicio en su puerto estándar.

Mediante la utilización de esta funcionalidad, podemos redireccionar puertos locales para que utilicen un túnel cifrado. De este modo, podemos ofrecer a nuestros usuarios servicios en principio inseguros de una manera segura. No todas las comunicaciones utilizan el mismo túnel, sino que se crea un túnel cifrado para cada puerto que queremos redireccionar. Las limitaciones de la redirección de puertos son la capacidad de túneles que pueda redireccionar y que solo podemos redireccionar los protocolos que usan TCP.

Este método de generación de VPN es muy recomendable, puesto que podemos crear VPN de una manera muy rápida y a un coste muy bajo. El gran problema, no obstante, es que si trabajamos con redireccionamiento de puertos los clientes (los usuarios) tienen que configurar su máquina, y esto implica un nivel de conocimiento superior al de la mayoría de los usuarios.

La mayor parte de las distribuciones GNU/Linux ya vienen con los paquetes de SSH instalados. Sin embargo, si se tiene que instalar debemos hacerlo mediante la orden:

```
root# apt-get install openssh.
```

La configuración del servidor de esta aplicación está en el archivo `/etc/ssh/sshd_config`. Las opciones de configuración más destacadas del fichero de configuración de `sshd_config` son las siguientes.

- `AllowTCPForwarding`: esta opción está habilitada por defecto y permite hacer el redireccionamiento de puertos comentado en este apartado.

- `AuthorizeKeysFiles`: indica el directorio donde están almacenadas las claves públicas que se utilizan para autenticar el acceso de los usuarios.

- `DenyUsers`: lista de usuarios que, a pesar de que tienen cuenta en la máquina, no podrán acceder a la misma por SSH.

- `ListenAddress`: especifica en qué dirección local se encuentra el servidor SSHD.

- `PermitEmptyPasswords`: mediante esta opción, indicamos si permitimos que los usuarios tengan el campo de la contraseña vacío. Es muy recomendable que esta opción esté configurada siempre para que no permita contraseñas vacías.

- `PermitRootLogin`: esta opción nos indica si permitimos al usuario raíz entrar por SSH o no. Esto depende del servicio que demos y de la seguridad de red que tengamos. Por ejemplo, si tenemos SSH configurado para hacer SFTP y permitimos a nuestros usuarios entrar por SFTP desde cualquier sitio de Internet, es recomendable no permitir el acceso de raíz por SSH. Ahora bien, si utilizamos SSH solo para habilitar consolas interactivas en el entorno de la empresa, sí podemos permitir el acceso de raíz por SSH.

- `Port`: nos indica en qué puerto TCP está el servidor SSHD. Por defecto, es el puerto 22. Es recomendable cambiar el puerto por otro que no esté en uso. Si se trata de un número alto, mejor.

- `Protocol`: nos indica con qué versión de SSH es compatible el servidor. Debido a las vulnerabilidades conocidas en SSH1, es muy recomendable que solo utilicemos SSH2.

- `Subsystem`: configura el subsistema externo. Si ponemos la opción `sftp-server`, configuramos un servidor de SFTP en nuestro servidor.

5.1.2. *Secure socket layer*

Sin duda, el método de generación de VPN más extendido es el método basado en web + *SSL* (protección de capa de conexión segura o *secure socket layer*). A pesar de que la mayoría de la gente lo asocia a la página web, SSL también puede proporcionar encriptación a muchos protocolos (POP3, IMAP, LDAP, SMTP, NNTP, etc.).

Este cifrado de los diferentes protocolos es el método estándar de conexión SSL, pero al igual que en el apartado anterior, SSL también es compatible con soluciones basadas en túneles.

El funcionamiento del servidor de SSL se basa en los certificados digitales. Tenemos que hacer una petición de certificado a una CA, como ya se ha mostrado y, una vez obtengamos la respuesta con el certificado de la máquina, lo instalamos (cada protocolo lo instala de una manera concreta, y cuando expliquemos los servicios veremos cómo se configuran los servicios SSL). De este modo, ya tenemos el servidor que ofrece el servicio de manera segura.

En la parte del cliente, también se configura de manera muy simple; tan solo tenemos que habilitar SSL (en el caso de los navegadores web, ya lo tienen habilitado por defecto). Un ejemplo de aplicación en la que tenemos que habilitar la SSL es la mayoría de los clientes de correo electrónico. En las opciones de configuración de los servidores, normalmente encontramos una pestaña o una casilla de selección donde podemos habilitar conexiones SSL. Debemos tener presente que el uso de servicios con SSL implica un puerto de entrada diferente del correo electrónico normal. Debemos considerar esto si hay un cortafuego, para abrir los puertos necesarios para hacer la comunicación.

Para crear túneles con SSL en entornos GNU/Linux, tenemos que utilizar la aplicación Stunnel. Esta aplicación crea túneles de manera parecida a la redirección de puertos que utiliza SSH. Por lo tanto, será necesario instalar esta aplicación con el comando `apt-get`.

La ventaja de SSL es la sencillez de la configuración (apenas hace falta nada más que un certificado digital y un par de modificaciones en el fichero de configuración del servicio). La desventaja, sin embargo, es la lentitud a la hora de obtener el certificado: dependiendo de la CA que utilicemos, la obtención del certificado puede tardar más de una semana.

SSL proporciona una manera muy sencilla de dar a los clientes las funcionalidades de una VPN para ciertas aplicaciones y protocolos, sin tener que llevar a cabo ninguna instalación y con pocas modificaciones en las aplicaciones de los clientes.

5.1.3. IPsec

En el apartado anterior, ya hemos hablado del funcionamiento de IPsec. Este protocolo, sin embargo, también se utiliza para crear VPN. A pesar de que SSH, SSL o IPsec proporcionan unas funcionalidades de encriptación parecidas, estos métodos son diferentes desde un punto de vista funcional.

Mientras que SSH o SSL crean un túnel nuevo para cada aplicación que queremos que funcione de manera segura, IPsec solo crea un túnel y hace pasar por el mismo toda la información. Desde un punto de vista de seguridad pe-

rimetral (uso de cortafuego), la implantación de una VPN con IPsec en lugar de SSH o SSL tiene muchas ventajas, puesto que, para empezar, solo tenemos que abrir el cortafuego en un único puerto.

5.1.4. Otros sistemas

Como hemos dicho al principio de este apartado, la construcción de VPN se puede hacer mediante diferentes protocolos. A lo largo de este apartado, hemos mostrado algunas de las maneras de construir una VPN, pero hay muchas más.

Algunas de estas son propietarias de una empresa, y otras son de distribución libre. Algunas de las otras maneras utilizadas para construir VPN son estas:

1) PPTP es un protocolo propietario de Microsoft.

2) FWZ es un protocolo propietario de Check Point Software Technologies utilizado en sus productos Firewall-1.

3) FreeS/Wan es una implementación de IPsec + IKE para Linux.

4) OpenVpn es una implementación de un cortafuego con *iptables* + túneles SSL.

5) Ip Masquerade + IPforward.

Podemos hacer esta lista muy larga, puesto que actualmente encontramos en el mercado muchas aplicaciones que hacen VPN. Nuestro trabajo es evaluar estas herramientas e instalar la que se adapte más a la configuración o a las necesidades de nuestra empresa.

5.2. Windows Server 2012

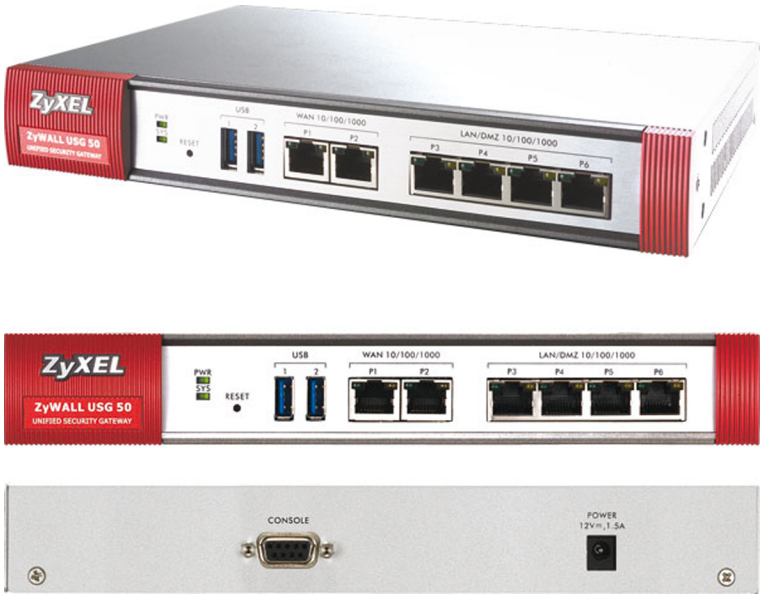
5.2.1. Configuración del servidor

El primer paso para configurar una red privada virtual consiste en configurar el servidor al que se quiere acceder para que permita conexiones entrantes, es decir, desde fuera incluso de la red interna. Para hacerlo, será necesario instalar un nuevo rol en el sistema, en este caso los servicios de acceso y directivas de red, que permita llevar a cabo conexiones entrantes remotas al servidor y que, además, cree las redes privadas virtuales implementadas directamente sobre el servidor.

Está claro que si se dispone de un cortafuego que permita crear estas redes virtuales, el sistema será mucho más seguro puesto que el mismo cortafuego se encargará de toda la gestión y, por lo tanto, el propio sistema operativo

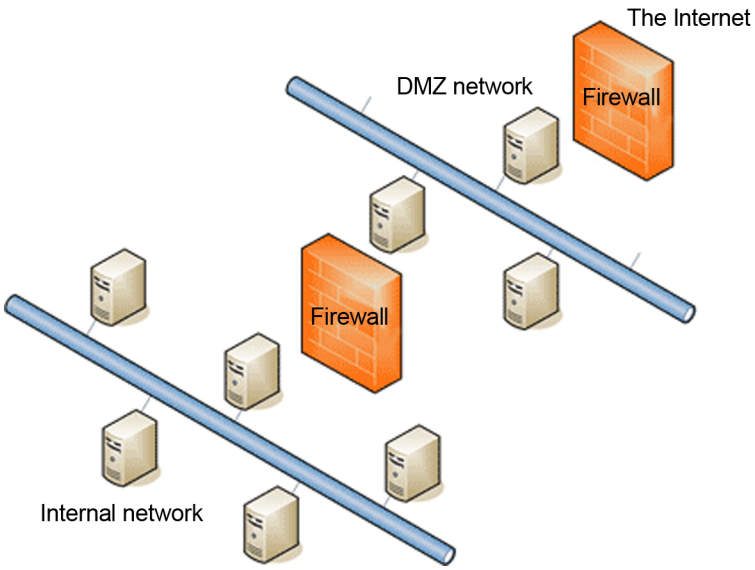
no será accesible desde fuera de la institución. La mayoría de los cortafuegos actuales, como por ejemplo el que muestra la figura siguiente, ya disponen de esta configuración y solo hay que activarla y configurarla de manera correcta.

Firewall Zyxel, Zywall USG 50



En este cortafuego tenemos una entrada que es la que se conecta directamente a Internet y otra entrada que se conecta a la red interna, donde están los servidores o la DMZ (figura siguiente), que separará con otro cortafuego el servidor que puede ser público de la parte de la organización que debe ser completamente privada. Por lo tanto, con estos aparatos las redes de las empresas o instituciones están mucho más securizadas, puesto que si no se dispone y se conecta directamente la red local interna al *router* y además hacemos que el propio servidor gestione las redes privadas, estamos provocando que el servidor se conecte directamente a Internet y además tenga abierto como mínimo el puerto para escuchar de las VPN, y posiblemente también los puertos de una página web, de los correos electrónicos, etc.

DMZ



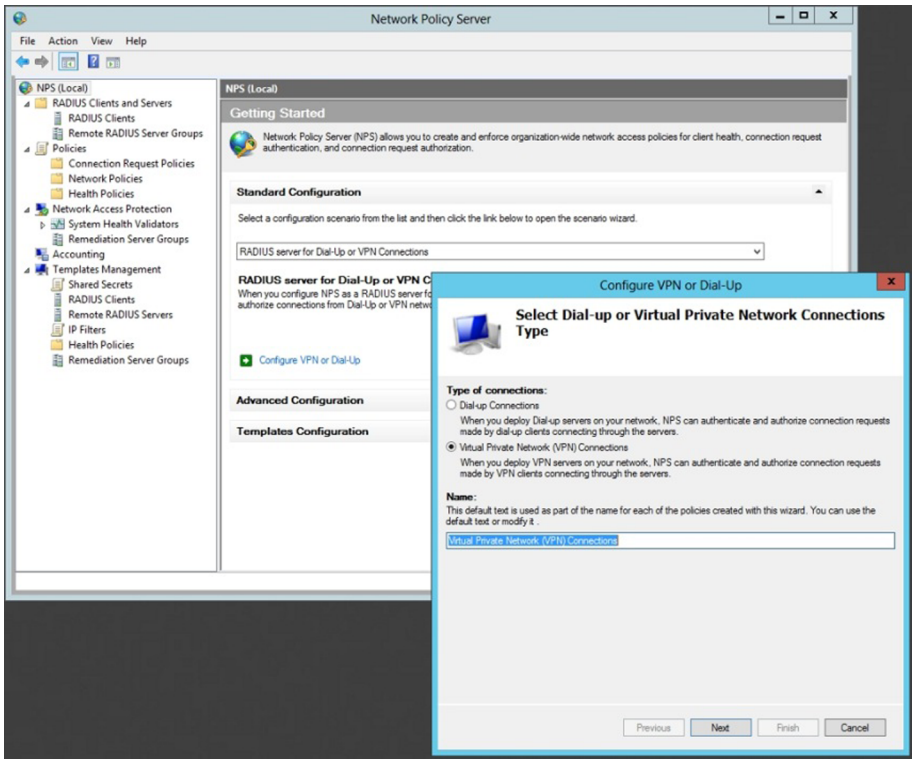
La configuración de cada uno de los cortafuegos es completamente distinta, pero normalmente estos aparatos permiten crear túneles permanentes entre dos equipos que tengan las mismas características. Esto permitirá crear túneles cifrados entre dos sedes, por ejemplo, de tal manera que la comunicación entre dos ADSL normales esté cifrada por completo y no se pueda escuchar la red pública entre estos puntos, además de crear una única red local entre todos los puntos ubicados a cada lado de las dos subredes (lo que crea una sola red local).

Sin embargo, en el caso de no disponer de este aparato, siempre se puede configurar el sistema operativo para crear una red virtual entre los equipos informáticos y el servidor donde esté instalado el rol de servicios de acceso y directivas de red.

Además de crear VPN, este rol nos permitirá crear políticas de conexión de los equipos clientes a partir de la "salud" que tenga cada ordenador; es decir, si se configura de modo que todos los ordenadores que se conecten a la red local deban tener instalado un sistema operativo, no dejará conectarse a aquellos que no dispongan de uno ya instalado. Se podría denegar el acceso a los servidores en la red o crear una subred donde únicamente tuvieran acceso a Internet, pero no a la red local. Pensemos en una empresa en la que los proveedores vienen a ofrecer los productos y disponen de portátiles que necesitan acceder a Internet, a alguna de las partes de la página web o al catálogo de productos propios.

En el momento de la instalación del rol, pedirá los servicios que se quieren instalar. Por defecto se instala el básico, pero es posible instalar también el registrador de salud, si se quiere utilizar esta característica concreta, y un módulo para integrar el proceso de autenticación de Microsoft (NAP) con el que dispone la empresa CISCO.

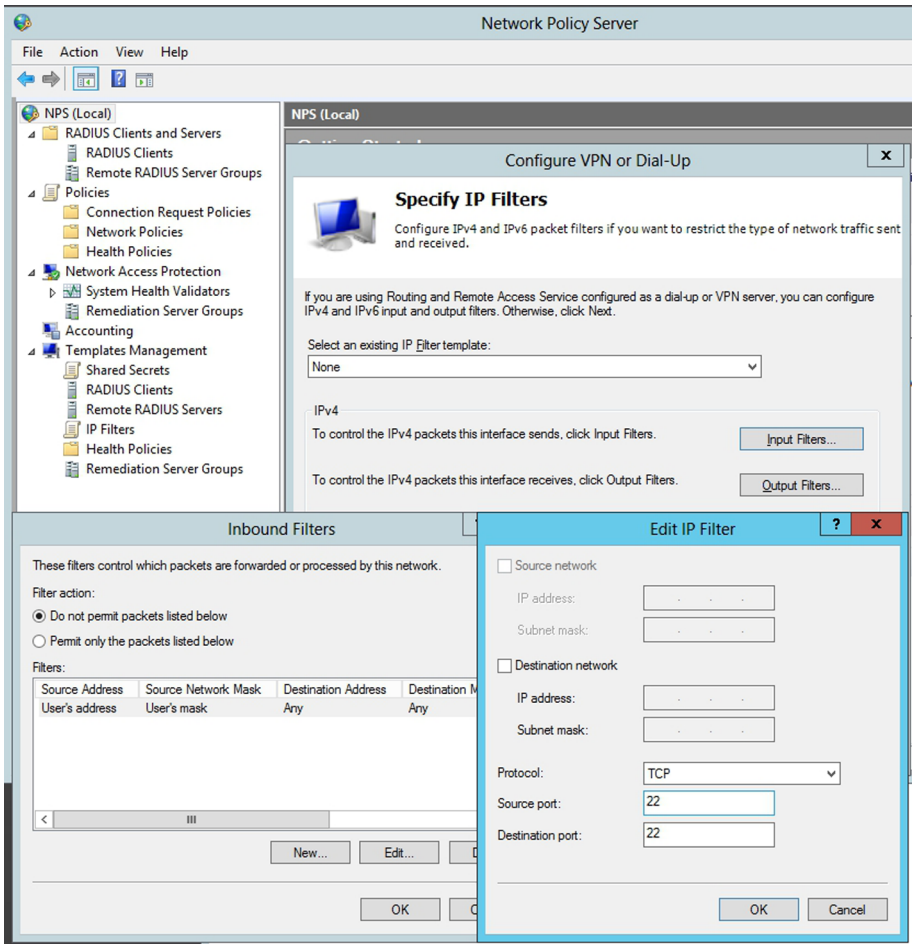
Configuración de VPN



Una vez instalado el rol, es preciso configurar el servidor para que acepte las peticiones de redes privadas. Esto lo podemos conseguir en el enlace de configuración estándar (figura siguiente), donde se puede decir que se quiere que actúe con redes VPN. A partir de aquí, hay que configurar el servidor RADIUS para los usuarios que se desee tener conectados, si es que se quiere utilizar esta característica o directamente la autenticación del propio servidor. Hay que configurar los protocolos de autenticación que se quiere tener en el servidor. Esto dependerá de qué equipos se conecten después a la VPN, que pueden tener o no unos protocolos determinados. Además, a continuación, y a partir de asignar un cierto grupo, se puede decidir qué usuarios del sistema tienen acceso a esta VPN, puesto que posiblemente no todos los empleados deben tener acceso a esta característica. Por lo tanto, se creará un grupo en el directorio activo que será el que se usará para incluir a todas aquellas personas que deban tener acceso a las VPN del servidor; por ejemplo el grupo `gVPN`.

A partir de aquí, se pueden incluir configuraciones para permitir o no ciertas IP internas o externas, protocolos, puertos, etc. de modo que la conexión VPN será mucho más segura si solo se permite el acceso a un determinado servidor donde esté la información que se quiere ofrecer, o el protocolo que se necesita (por ejemplo, el FTP, el de compartición de ficheros, etc.).

Configuración de los puertos, IP, protocolos, etc. permitidos de la VPN



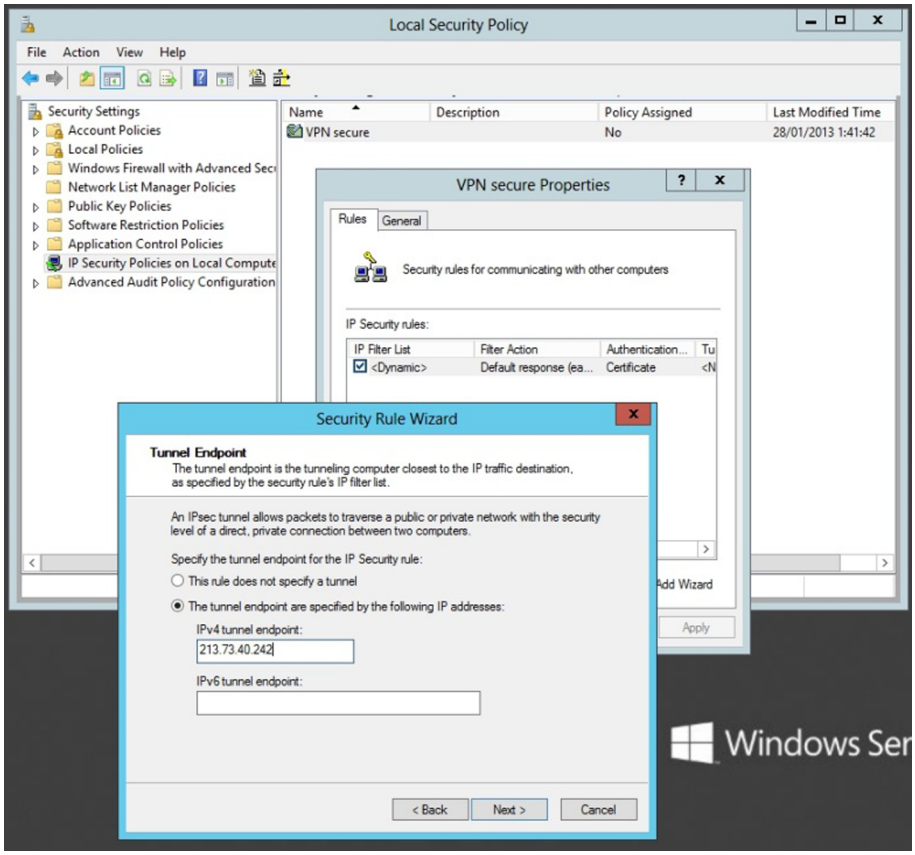
Podemos cambiar los protocolos de autenticación que tiene por defecto una vez instalado el rol de la conexión remota, directamente en las propiedades de los roles que se acaban de instalar.

En cuanto a la seguridad de las VPN, podemos definir una directiva de seguridad IP (IPsec) que permita cifrar los datos de la conexión y que obligue a los usuarios a autenticarse con un certificado digital expedido por una entidad de certificación propia. Para hacerlo, abrimos la herramienta Directiva de seguridad local del panel de control, luego Herramientas administrativas y, en el menú contextual del elemento Directivas de seguridad IP en equipo local, seleccionamos la opción Crear directiva de seguridad IP. Después de poner un nombre a la nueva directiva, deseleccionamos la opción Activar la regla de respuesta predeterminada. En la pantalla Tipo de red seleccionamos Acceso remoto y en la ventana Método de autenticación, la opción Usad un certificado de esta autoridad de certificados (CA), y pulsaremos el botón Examinar... para seleccionar el certificado de nuestra entidad de certificación o el de la entidad en la que confiamos, y se acaba el proceso de crear la directiva.

Después se muestran las propiedades de la directiva que se ha creado con el botón derecho del ratón. En la lista de reglas IP, hacemos clic sobre el botón Agregar... y aparece el asistente correspondiente. En la pantalla Punto final del túnel, y en el caso de que se trate de una dirección IP fija, se podrá bloquear

para que solo se pueda conectar desde esta IP (figura siguiente). Se selecciona la opción El extremo del túnel se especifica mediante la siguiente dirección IP y escribimos la IP de la VPN. Esto resulta muy útil, puesto que dejamos fijas las dos partes del túnel VPN y hacemos más difícil la intrusión en esta VPN de terceras personas. En el caso de que sea una IP variable, no se podrá fijar y se tendrán que asumir unos riesgos que minimizaremos un poco con los certificados, aunque no del todo.

Configuración del túnel VPN



Una vez creada la directiva IP, la tenemos que asignar con la opción Asignar del menú contextual correspondiente en la lista de directivas IP. A partir de este momento, los usuarios que quieren acceder vía VPN deben tener un certificado emitido por nuestra entidad emisora de certificados. Este certificado puede estar incluido en una tarjeta inteligente para aumentar la seguridad. Otra acción que podemos llevar a cabo para aumentar la seguridad de una VPN consiste en configurar un cortafuego para admitir acceso solo a las conexiones de las IP de los usuarios de la VPN, si bien esto restringe el hecho de que los usuarios puedan acceder desde diferentes lugares o que utilicen equipos con IP dinámica.

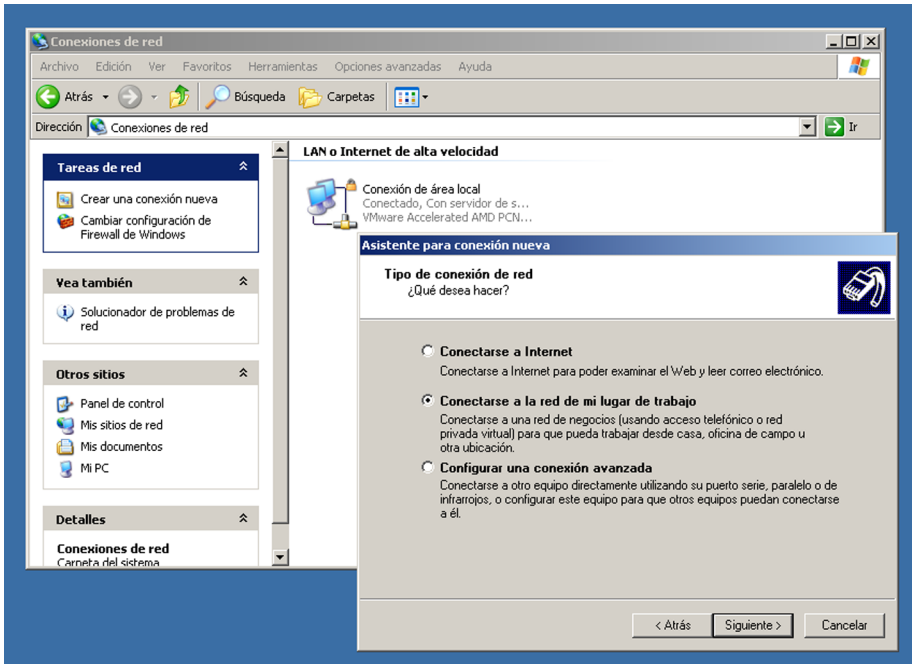
Hay otros mecanismos o herramientas más avanzados para mejorar la seguridad de la VPN –además de otros tipos de conexiones–, como por ejemplo Microsoft Internet Security And Acceleration Server (ISA Server), también conocido como Microsoft Forefront Threat Management Gateway y que, aparte

de facilitar la configuración y protección de redes VPN, lleva a cabo tareas de cortafuego, publicación web segura, autenticación segura, FTP seguro, monitorización, creación de informes, etc.

5.2.2. Configuración del cliente

Una vez configurado el servidor de la red VPN, configuramos los clientes desde los cuales queremos acceder al servidor. Para hacerlo desde los clientes, usamos la utilidad de creación de conexiones, dentro de la carpeta Conexiones de red y de acceso telefónico del panel de control (figura siguiente).

Creación de la VPN en el cliente Windows XP



En este caso, seleccionamos la opción Conectar a otra red privada mediante Internet. A continuación, el asistente nos pide el nombre del servidor o la dirección IP que tiene. Finalmente, antes de acabar, el asistente nos pregunta si la conexión está disponible para todos los usuarios del equipo o solo para la cuenta de usuario actual.

Antes de usar la nueva conexión, hay que configurarla. Vamos a la ventana de propiedades, seleccionamos el protocolo TCP/IP en la pestaña Funciones de red y hacemos clic sobre Propiedades. En la ventana de propiedades seleccionamos la opción de obtener una dirección IP de manera automática (salvo que no hayamos configurado el servidor para hacerlo), y modificamos las direcciones de DNS para que sean las mismas especificadas en el servidor. Hacemos clic en Avances y en la ventana que aparece deseleccionamos la opción Usar la puerta de enlace predeterminada en la red remota. Cuando intentamos conectarnos con la nueva conexión, nos sale una pantalla de identificación en la que tenemos que proporcionar nuestro nombre de usuario y contraseña.

Cuando un cliente se conecta al servidor de VPN, se enciende el icono de conexiones entrantes del servidor y muestra a los usuarios conectados en aquel momento.

6. Monitorización de la Red

La monitorización de la Red es un factor importante en la seguridad de nuestra empresa. Mediante la monitorización podemos saber cuál es el comportamiento (los hábitos de trabajo) de nuestra empresa, la cantidad de ancho de banda que consumimos en cada momento, etc.

Casi todos los sistemas operativos incluyen unos programas muy sencillos de monitorización. Estos programas solo permiten monitorizar diferentes parámetros del ordenador que los ejecuta (la Red, la memoria o el uso de CPU). Además, todas estas aplicaciones resultan muy sencillas, puesto que solo permiten la monitorización de cualquiera de estos programas siempre que el programa esté en ejecución y, por otro lado, solo nos dejan visionar lo que está pasando y un histórico de pocas horas.

Tenemos que ir con mucho cuidado cuando utilizamos herramientas de monitorización de la Red. Hay una ley de privacidad de datos que protege el tráfico por la Red. Si la finalidad de la monitorización de la Red es obtener estadísticas, podemos capturar paquetes IP para analizarlos en los casos siguientes.

1) Cuando no podamos capturar el contenido del paquete (de hecho, ni siquiera lo podemos ver mientras circula por la Red).

2) Cuando los resultados estén disociados, es decir, tenemos que enmascarar las direcciones IP ya sea trabajando en subredes, redes o superiores (sistemas autónomos).

6.1. Monitorización en GNU/Linux

En este apartado, comentaremos una aplicación de monitorización de la Red que tiene licencia GNU y que permite hacer una monitorización muy completa. Esta aplicación se denomina Multi Router Traffic Grapher (MRTG), y genera páginas de lenguaje de etiquetado de hipertexto o *hypertext markup language* (*HTML*) que contienen imágenes en formato gráfico de red portátil o *portable network graphics* (*PNG*), las cuales nos proporcionan una representación visual muy completa del tráfico de Red.

La aplicación MRTG consiste en una serie de *scripts* en lenguaje PERL que usan el protocolo simple de administración de redes o *simple network management protocol* (*SNMP*) para leer los contadores de tráfico que hay en los conmutadores (*switches*) o los enrutadores (*routers*). Mediante sencillos y rápidos programas escritos en lenguaje de programación C, crea imágenes en formato PNG que representan el estado del tráfico de nuestra red e inserta estos gráficos en

una página web que podemos consultar con cualquier navegador. Tenemos que hacer notar que para ver los resultados debemos tener instalado un servidor web en la máquina que tenga instalada MRTG.

Esta aplicación, además de ofrecernos una visión detallada del tránsito de la red local, también crea representaciones de tráfico de los últimos siete días, las últimas cinco semanas y los últimos doce meses. Esto es posible porque MRTG guarda en unos ficheros de *log* toda la información que ha ido pidiendo a los equipos de la red. Estos ficheros tienen la particularidad de que no aumentan su tamaño a lo largo del tiempo, lo que evita que se llene el disco y, por lo tanto, que se pueda parar el servidor. La monitorización de la red no es la única aplicación que podemos obtener de este programa. Puesto que MRTG usa SNMP, cualquier dato que seamos capaces de obtener mediante este protocolo es susceptible de ser monitorizado. Actualmente, la mayoría de los administradores que utilizan este programa supervisan otros parámetros aparte del tráfico de red (la carga del sistema, de los discos, etc.).

Antes de instalar esta aplicación, debemos asegurarnos de que tenemos instalados los requisitos de esta herramienta. Si necesitamos más información que la detallada en estas páginas, tenemos que consultar el manual de instalación de MRTG [Oet04].

Para instalar MRTG, necesitamos lo siguiente:

1) Un compilador de C. El más común es GCC (http://gcc.gnu.org/).
2) Una versión de PERL actualizada (http://www.perl.com/).
3) Las bibliotecas zlib (http://www.zlib.net).
4) Las bibliotecas libpng (http://www.libpng.org/pub/png/).
5) Las bibliotecas gráficas gd (http://www.boutell.com/gd/).

Como se ha indicado anteriormente, solo hay que utilizar la orden

```
root# dpkg -l gcc perl
```

para saber si tenemos estas herramientas instaladas. En el supuesto de que no lo estén, se tendrán que instalar con la aplicación `apt-get`. El resto de las librerías necesarias hay que bajarlas de la página web e instalarlas manualmente, por lo general mediante estos pasos:

```
root# ./configure
root# make
root# make install
```

A pesar de que las páginas de instalación de esta aplicación explican su instalación mediante el proceso de compilación de las fuentes de los diferentes requisitos, nosotros –dado que usamos una distribución de GNU/Linux basada en una Debian– podemos instalar esta aplicación con la orden siguiente:

```
root# apt-get install mrtg
```

Durante la instalación, nos advierte de que si el fichero de configuración es accesible por otros usuarios que no sean el usuario *root*, puede haber un problema de seguridad, puesto que en este fichero hay nombres de máquinas de la red que tendrían que quedar ocultas para personas ajenas a la compañía. Dejaremos de tener este problema únicamente haciendo que el propietario y el grupo sean un único usuario o el *root*.

Una vez tenemos instalada esta aplicación, ya la podemos configurar. Para hacerlo, es muy importante que conozcamos el entorno de red en el que trabajamos y que seamos administradores de la misma. Esto se debe de al hecho de que, puesto que utilizamos el protocolo SNMP, necesitamos las contraseñas (*community*) de acceso mediante este protocolo que hay definidas en los distintos equipos de red (conmutadores, enrutadores, etc.). La administración de estos equipos está a cargo del administrador de red.

Para configurar MRTG, utilizamos una herramienta de configuración que viene con la misma aplicación y que se denomina `cfgmaker`. Podemos ver los parámetros en el manual, pero un posible ejemplo de uso de esta herramienta es el siguiente.

```
root# cfgmaker -output /etc/mrtg.cfg --ifref=ip --ifdesc=name public@router
```

Las opciones más destacadas de `cfgmaker` son las siguientes.

1) `Ifref`: cómo referenciamos la interfaz. Los valores aceptados son número, IP, Ethernet, descripción, nombre y tipo.

2) `Ifdesc`: cómo describimos la interfaz. Los valores aceptados son los mismos que en el caso del parámetro `ifref`.

3) `Output`: tenemos que indicar el fichero donde se guarda la configuración.

4) `Dns-domain`: indicamos el dominio al que pertenecen las interfaces.

Una vez hemos ejecutado `cfgmaker`, tenemos que editar el fichero que acabamos de crear, en el caso del ejemplo `/etc/mrtg.cfg`, y modificar las líneas siguientes.

1) `Workdir`: especificamos el directorio de trabajo de MRTG.
2) `Htmldir`: especificamos en qué directorio se ponen los ficheros HTML.

3) `Imagedir`: especificamos en qué directorio se almacenan las imágenes.
4) `Logdir`: especificamos en qué directorio se guardan los *logs*.
5) `Icondir`: especificamos en qué directorio están los iconos MRTG.

No es preciso que todos estos directorios que hemos descrito aquí sean directorios distintos. Lo que sí debemos hacer es configurarlos todos para que MRTG funcione correctamente. Estos parámetros, si queremos, también se pueden pasar por línea de orden cuando ejecutamos `cfgmaker`. Para hacerlo, tenemos que ejecutar la orden con las opciones siguientes:

```
root# cfgmaker --global "Workdir: /var/www/mrtg" \
--global "htmldir: /var/www/mrtg" \
--global "ImageDir: /var/www/mrtg" \
--global "logdir: /var/log" \
--global "icondir: /var/www/icon" \
--output /etc/mrtg.cfg \
--ifref=ip \
--ifdesc=name \
public@router
```

Si queremos hacer la monitorización de más de una máquina, es aconsejable tener un único fichero de configuración. Para hacerlo, debemos añadir el par contraseña@máquina para cada anfitrión o *host* que queremos monitorizar en la ejecución de la orden `cfgmaker`. Para más información sobre las órdenes de la MRTG, ejecutad:

```
root# man cfgmaker
```

Una vez acabada la configuración de MRTG, tenemos que generar un índice. Para esto, ejecutamos la orden `indexmaker`. Un ejemplo de ejecución de esta orden es:

```
root# indexmaker -output /var/www/mrtg/index.html /etc/mrtg.cfg
```

Los parámetros que hemos puesto en el ejemplo de ejecución son los mínimos que necesita esta orden para hacer un índice. Esta orden, no obstante, tiene muchas más opciones. Ahora bien, todas estas opciones hacen referencia a la manera en que queremos que se visualice index.html: en una columna, en dos, en orden por dirección IP, por nombre, en orden ascendente, descendente, con qué tipo de letra, etc.

Para más información sobre estas opciones, tenemos que consultar el manual:

```
root# man indexmaker
```

Para acabar la configuración, debemos añadir el directorio `/var/www/mrtg` para que se visualice desde Internet. En el módulo siguiente, veremos todas las opciones de configuración de un servidor web. En este apartado nos limitamos a explicar las modificaciones necesarias para que funcione MRTG, y suponemos que nuestro servidor funciona de manera correcta.

```
<Directory "/var/www/mrtg">
Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

Una vez acabada la configuración, solo nos queda ejecutar la aplicación. Para hacerlo, utilizamos `crontab`, un fichero de sistema en el que se configuran todas las tareas de ejecución periódica que queremos hacer de manera automatizada. Para acceder al `crontab` de nuestra máquina, tenemos que usar la orden siguiente.

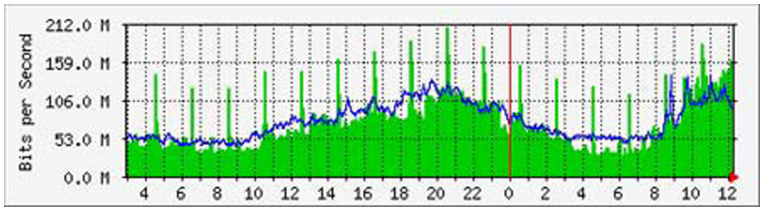
```
root# crontab -e
```

Una vez accedemos a `crontab`, añadimos la línea siguiente:

```
*/5 * * * * /usr/bin/mrtg /etc/mrtg.cfg -logging /var/log/mrtg.log
```

Mediante esta línea, suponemos que el ejecutable de MRTG está en `/usr/bin`; que el fichero de configuración lo tenemos en `/etc/mrtg.cfg`; y que los *logs* del sistema se encuentran en `/var/log`. Una vez funciona MRTG, si consultamos la página web de nuestra máquina en la que se muestran los resultados obtenemos gráficos semejantes al de la figura siguiente.

Ancho de banda monitorizado

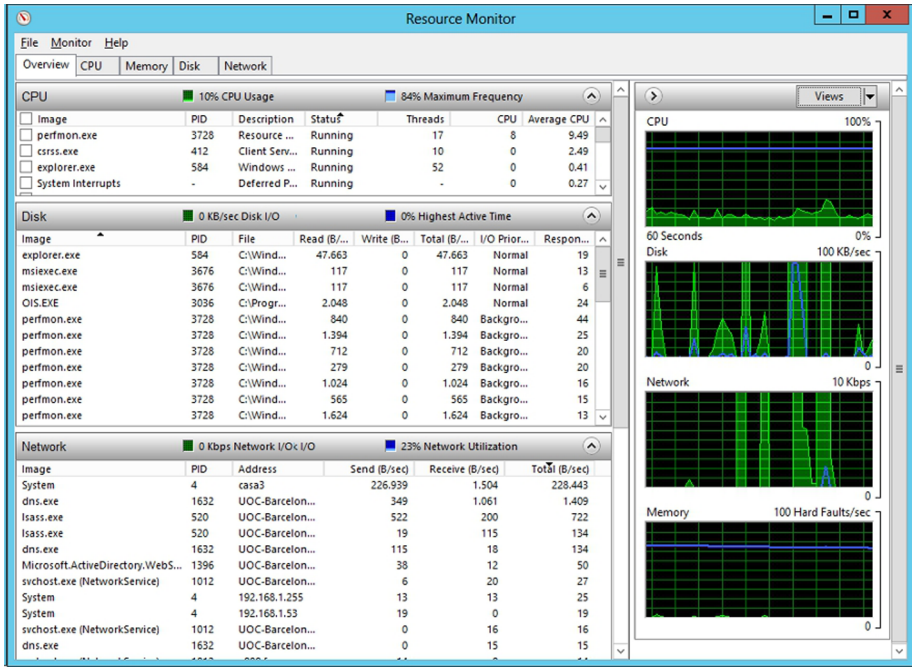


Estos gráficos nos muestran los volúmenes de información (tanto de entrada como de salida) que circulan por un equipo de red a lo largo de las últimas veinticuatro horas. La línea vertical de color rojo nos indica dónde se acaba el día. El color azul nos muestra la salida y el color verde, la entrada.

6.2. Monitorización en Windows Server 2012

Windows Server 2012 tiene incluida una utilidad para monitorizar en general los recursos del sistema: es el monitor de recursos, y se encuentra en la pantalla de administración del servidor, dentro del menú de herramientas. La figura siguiente muestra una captura con un comportamiento que *a priori* puede parecer extraño si el servidor está en unos momentos en los que no hay actividad.

Monitor de recursos

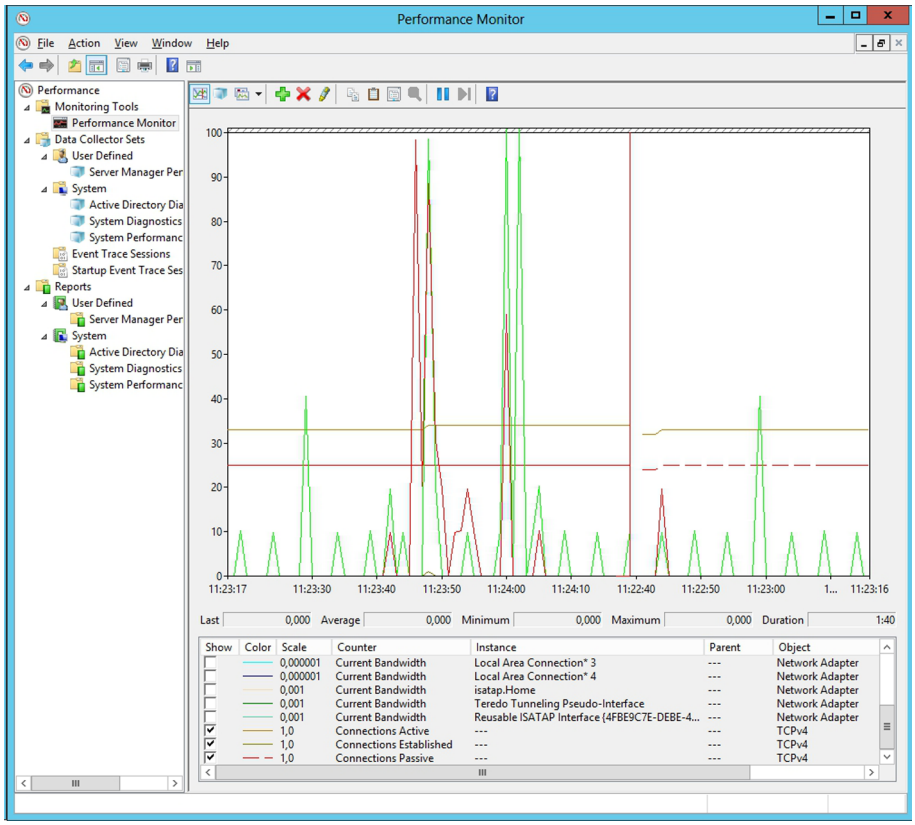


Podemos ver que el disco está en uso y que además, al mismo tiempo, se está utilizando la red, así como qué procesos la están usando. Este monitor de recursos nos da una información muy importante para controlar el comportamiento del servidor.

Sin embargo, además de este monitor, Windows Server 2012 también dispone de otro monitor del sistema que permitirá tener mucho más controlados ciertos elementos que con este primer monitor hayamos visto sospechosos. Esta otra herramienta es el monitor de rendimiento, que también se encuentra en el listado de las herramientas del administrador del servidor.

La figura siguiente muestra un instante de la monitorización del servidor. En esta herramienta todo es configurable: se puede monitorizar el número de conexiones establecidas con el servidor, los bytes que el servidor envía o recibe por IPv4 o por IPv6, el acceso a disco, los errores de paginación, etc. Hay una lista muy extensa de posibles variables para monitorizar.

Monitor de rendimiento en local

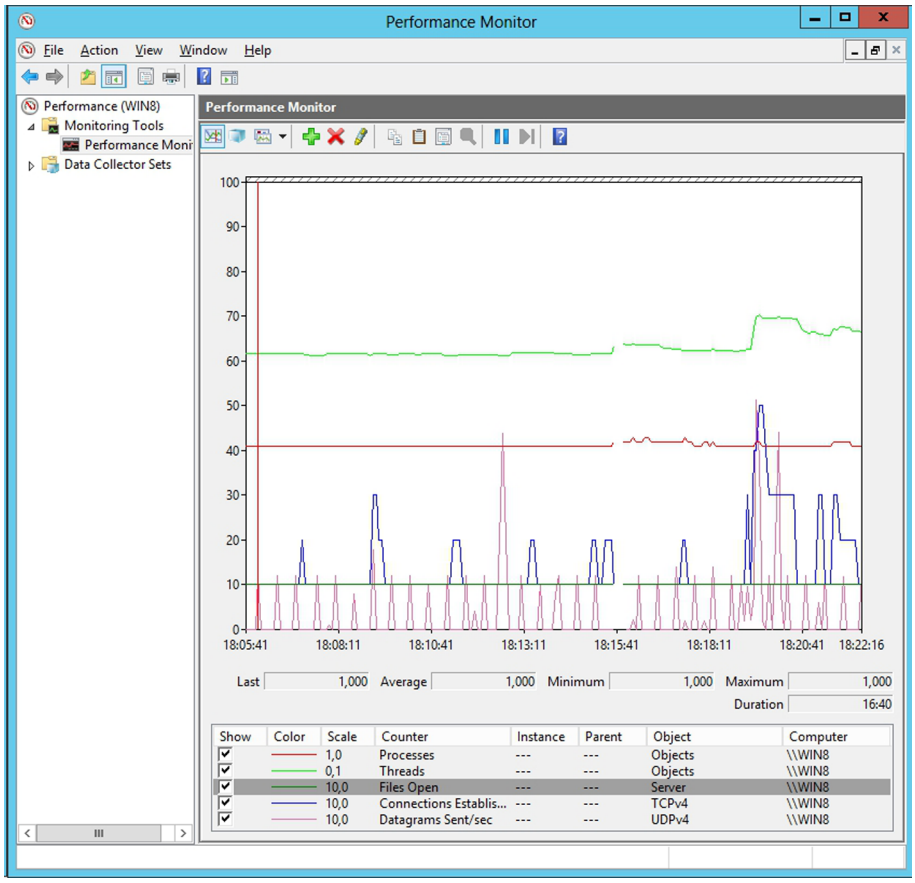


Permite monitorizar por medio de *active directory* las distintas estaciones de trabajo que están dentro del dominio. Solo hay que seleccionar el PC que se quiere seguir y elegir qué se quiere monitorizar en el momento de añadir el contador.

Para hacer esto, es preciso que en cada estación de trabajo en la que se quiera obtener los datos en remoto se haya activado el servicio de registro remoto. Esto se consigue abriendo la consola o el PowerShell del sistema –si la estación de trabajo tiene Windows 7 o Windows 8– y accediendo a la consola `services.msc`, que sirve para iniciar y parar los servicios. Se tienen que iniciar los servicios de registro remoto y de registro y alertas de rendimiento. El cliente ejecutará el servicio para tener accesibles los datos de manera remota.

Además, hay que tener en cuenta que es necesario habilitar el cortafuego para acceder de manera remota a estos servicios desde el servidor, y la configuración del acceso a los datos se tiene que hacer desde un usuario que pertenezca al grupo de usuarios de *log* y al de lectores de eventos de *log*. La figura siguiente muestra cinco contadores de un equipo remoto. De este modo, se puede controlar de manera mucho más cuidadosa y remota el comportamiento de un ordenador que se sospecha que tiene algún programa instalado ajeno a la compañía, como podrían ser programas de compartición de ficheros, troyanos, etc. Es posible monitorizar el uso de la red para aquel equipo en concreto, el número de sesiones abiertas que tiene, etc. Incluso permitirá controlar la "salud" del ordenador, con el estado del disco o del procesador.

Monitor de rendimiento de un equipo remoto



Además, permite crear informes de todo lo que se está monitorizando. La misma aplicación permite configurar los documentos de salida que se quieren producir. De este modo, se dispondrá rápidamente de sistemas de auditorías de los equipos internos de la organización.

7. Herramientas de comprobación

Pese a que la monitorización de la red es efectiva en muchos aspectos, dependiendo del tipo de análisis no es suficiente. Esto sucede cuando queremos descubrir las posibles vulnerabilidades de nuestra red. Mediante la monitorización solo vemos el uso que se hace de nuestra red, pero no vemos el uso de la red de manera detallada, como por ejemplo:

1) El porcentaje de tráfico TCP, UDP, ICMP o difusión (*broadcast*).

2) Cuáles son los protocolos más utilizados (HTML, FTP, SFTP, P2P, etc.).

3) Comprobar si nuestros servidores tienen puertos abiertos que no deberían estarlo.

La solución a este tipo de problemas nos la ofrecen las herramientas de comprobación.

Hay dos tipos de herramientas de comprobación: las pasivas y las activas. Las pasivas son las herramientas que no interfieren en la red, sino que se limitan a capturar paquetes y obtener resultados estadísticos de las capturas de las tramas que circulan por la misma. Por el contrario, las activas son las que, además de obtener estadísticas, son capaces de analizar la red mediante mecanismos intrusivos, es decir, pueden obtener información de las máquinas que hay enviando paquetes especiales que las máquinas destino contestan. De este modo, consiguen aún más información de cómo está configurada la red de ordenadores.

Tenemos que ir con mucho cuidado cuando utilizamos este tipo de herramientas, puesto que en algunas de las aplicaciones que tienen puede parecer que estemos haciendo un ataque a una máquina. Si la máquina no la administramos nosotros y no hemos avisado al administrador de que haremos este tipo de análisis, es posible que si se detecta el ataque tengamos algún problema con el administrador, pues en muchos casos se puede ver esta actividad como un ataque a los servidores a través de la red local.

También debemos tener mucho cuidado con los ámbitos en los que utilizamos este tipo de herramientas, puesto que cada país tiene su propia ley de protección de datos, en la que se describe en qué entornos se puede llevar a cabo un análisis, hasta dónde podemos analizar (cabecera IP, cabecera TCP, cabecera de aplicación y datos) y si hace falta o no algún tipo de autorización de conformidad de los clientes para analizar la red.

7.1. Herramientas de GNU/Linux

7.1.1. NMAP

Una aplicación típica y muy usada de la clase de las herramientas activas es la denominada Network Mapper (NMAP). Se trata de una herramienta GNU que se utiliza para explorar redes o hacer auditorías de seguridad. Esta herramienta está diseñada especialmente para hacer un análisis de grandes redes, pese a que solo está instalada en una única máquina.

La información que NMAP nos puede ofrecer es muy variada: qué máquinas hay activas, qué sistema operativo tienen, qué versión, qué puertos tiene abiertos cada máquina, etc. Además, hay versiones de NMAP para casi cualquier sistema operativo (Windows, Linux, FreeBSD, Mac OS X, etc.), con versión en modo texto o mediante entorno gráfico.

También encontramos versiones de NMAP para sistemas Debian. Para hacer la instalación, tenemos que ejecutar la orden siguiente:

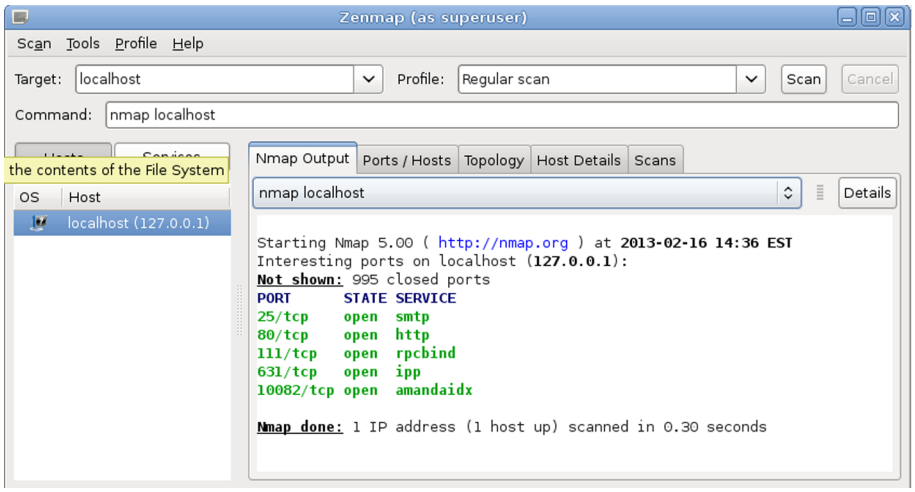
```
root# apt-get intall nmap.
```

Una vez tenemos instalada esta herramienta en modo consola, aparte de los ejecutables de la aplicación también tenemos instaladas las páginas de documentación del manual. La información de estas páginas es muy completa y nos detalla todas las opciones posibles; asimismo, al final de la documentación encontramos ejemplos de funcionamiento. Sin embargo, también hay la posibilidad de utilizar esta herramienta en un entorno gráfico. Tenemos que instalar el frontal o *front end* mediante la ejecución de la orden siguiente.

```
root# agt-get install nmapfe.
```

La visualización de esta herramienta en el entorno gráfico se muestra de una manera parecida a la figura siguiente.

Ejecución NMAP sobre *localhost*



Este entorno gráfico nos permite hacer todas las configuraciones posibles de la herramienta NMAP utilizando el ratón. Además, nos muestra (en la barra inferior, denominada *command*) la orden que tenemos que ejecutar para obtener el mismo resultado que lográbamos cuando utilizábamos esta herramienta sin entorno gráfico.

En la herramienta NMAP, los parámetros se dividen en dos partes: los escaneos y las opciones generales. Dentro del primer grupo de parámetros, encontramos las opciones siguientes.

1) `sS`: escaneo de TCP Syn. No establece una conexión completa TCP.
2) `sT`: escaneo de TCP. Establece una conexión completa TCP.
3) `su`: escaneo de UDP.
4) `sP`: escaneo PING. Encuentra máquinas accesibles en la red.
5) `sV`: intenta establecer qué versión de software hay en cada puerto activo.
6) `sR`: escaneo de RPC.

Los parámetros que afectan a las opciones generales de configuración de la herramienta NMAP son los siguientes.

1) `O`: uso de TCP/IP para identificar un sistema operativo remoto.
2) `p`: rango de puertos que se tienen que escanear.
3) `PO`: no hacer PING hacia las máquinas remotas.
4) `6`: uso de IP versión 6.
5) `v`: *verbose* (recursivo).

7.1.2. Snort

La herramienta Snort es una aplicación del tipo de las pasivas. Pese a que no resulta muy complicada de usar, esta herramienta puede ser un poco tediosa para los usuarios nuevos porque tiene muchos parámetros y tres maneras de configuración distintas:

1) Sniffer lee paquetes de la red y los muestra por pantalla.

2) Paquet Logger almacena los diferentes paquetes capturados en el disco para hacer un análisis de los mismos más adelante.

3) Network Intrusion Detection es un motor de comparación que intenta reconocer diferentes tipos de ataques de red.

Los primeros modos de configuración de esta herramienta están muy orientados a redes; por lo tanto, no entran dentro del temario de esta asignatura. Pese a que el tercer módulo también tiene mucho contenido de redes, en el mismo la mayoría de los ataques hacen referencia a los servidores que hay detrás. Por lo tanto, nos centraremos en la manera de configurar Snort para hacer la detección de intrusos.

Para instalar esta herramienta, tenemos que ejecutar la orden siguiente:

```
root# apt-get install snort
```

Una vez la hemos ejecutado, y antes de acabar la instalación, nos pide que configuremos algunos parámetros. Los parámetros que tenemos que configurar son los siguientes.

- El dispositivo utilizado por Snort: por defecto, `eth0` (tenemos que poner aquí el dispositivo que utilizaremos para examinar la red).

- El rango de red IP que queremos analizar: por defecto, 192.168.0.0/16 (debemos poner el rango IP que queremos analizar).

- El usuario que ejecutará Snort: por defecto, *root* (tenemos que cambiar este usuario por el de Snort y, si no se ha creado, hacerlo antes).

Para utilizar el modo Network Intrusion Detection, tenemos que ejecutar Snort con los parámetros siguientes:

```
root# snort -d -l /var/log/snort.log -h 192.168.1.0/24 -c snort.conf
```

El directorio de salida por defecto es `/var/log/snort.log`. Si no queremos especificar otro directorio, omitimos este parámetro. En este fichero quedará constancia de los ataques que hemos tenido. Por este motivo, lo tenemos que revisar con frecuencia. El fichero `snort.conf` tiene almacenadas las reglas de comportamiento de los ataques. Inicialmente no hay ninguno y, por lo tanto, no se puede hacer ningún tipo de ataque ya que hay muchos ataques posibles. Es preciso instalar otra herramienta que permitirá actualizar este conjunto de

reglas de manera automática. Conseguimos esto con la herramienta Oinkmaster, que se instala directamente con la herramienta Snort, pero si ocurre esto, solo hay que instalarla con el comando `apt-get`.

Para utilizar el programa Oinkmaster, se tiene que obtener acceso al mismo en la página web de Snort (www.snort.org) para configurar la herramienta de bajada de las reglas y, de este modo, tenerlas en local.

Una vez dados de alta, solo hay que llamar al comando Oinkmaster con el directorio donde se guardan las reglas de Snort, que por defecto es `/etc/snort` con el fichero `snort.conf` y un directorio denominado `rules` donde están todas las reglas.

De modo periódico, tenemos que actualizar el fichero de reglas puesto que van apareciendo nuevas reglas. Dado que este proceso no es automático, es preciso configurar `crontab` para que lo haga, por ejemplo ejecutando cada mañana la orden de actualización de las reglas de Snort. Podemos hacer que se ejecute cada mañana a la 1 de la madrugada:

```
0 1 * * * /usr/local/bin/oinkmaster.pl -o /etc/snort/rules
```

7.2. Herramientas de Windows Server 2012

7.2.1. Listas de comprobación de seguridad

Microsoft tiene una serie de listas de comprobación que indican los pasos que hay que seguir para comprobar que una funcionalidad del sistema operativo está bien configurada. Además, ofrecen información relacionada.

Encontramos listas de comprobación para distintos aspectos del sistema operativo, como *active directory*, gestión de usuarios, configuración de la red y configuración de dispositivos.

Esta lista de comprobación cubre aspectos como los siguientes.

- Definir una plantilla de seguridad para una directiva de grupo: ayuda a definir una plantilla de seguridad para una directiva de grupo. Una plantilla de seguridad consiste en un conjunto de reglas de seguridad que se tienen que comprobar para cualquier usuario que tenga asignada la directiva de grupo correspondiente.

- Definir una plantilla de seguridad para un equipo local: en este caso, las plantillas de seguridad definidas se asignan a equipos en vez de a usuarios.

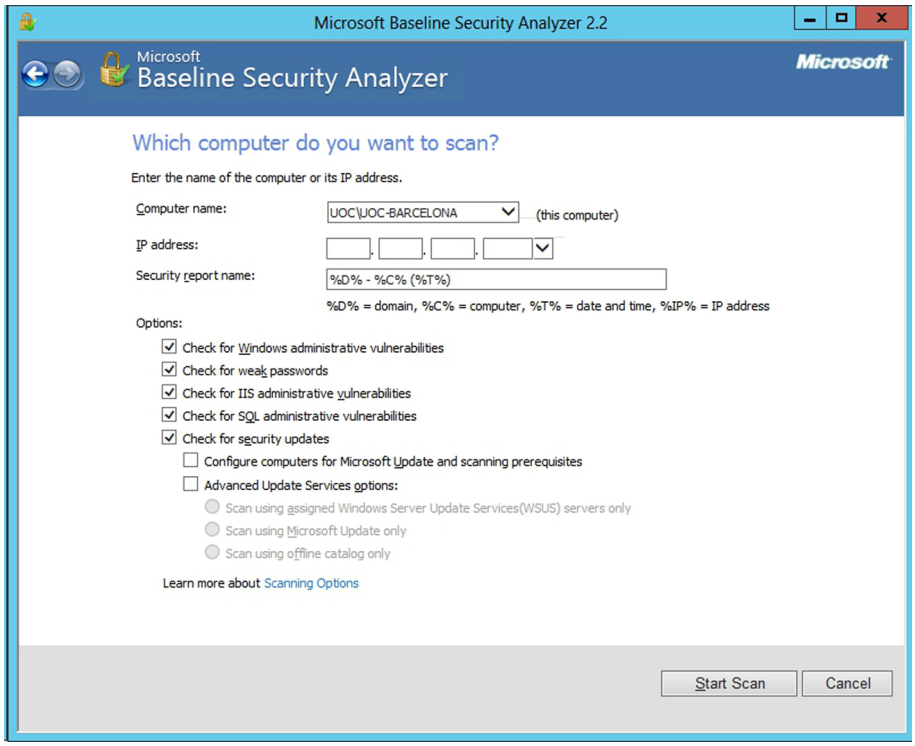
- Analizar la seguridad: ayuda a analizar el estado de la seguridad del sistema según la plantilla de seguridad elegida.

- Configurar la seguridad del sistema: ayuda a configurar la seguridad del sistema según una plantilla de seguridad.

7.2.2. Microsoft Baseline Security Analyzer

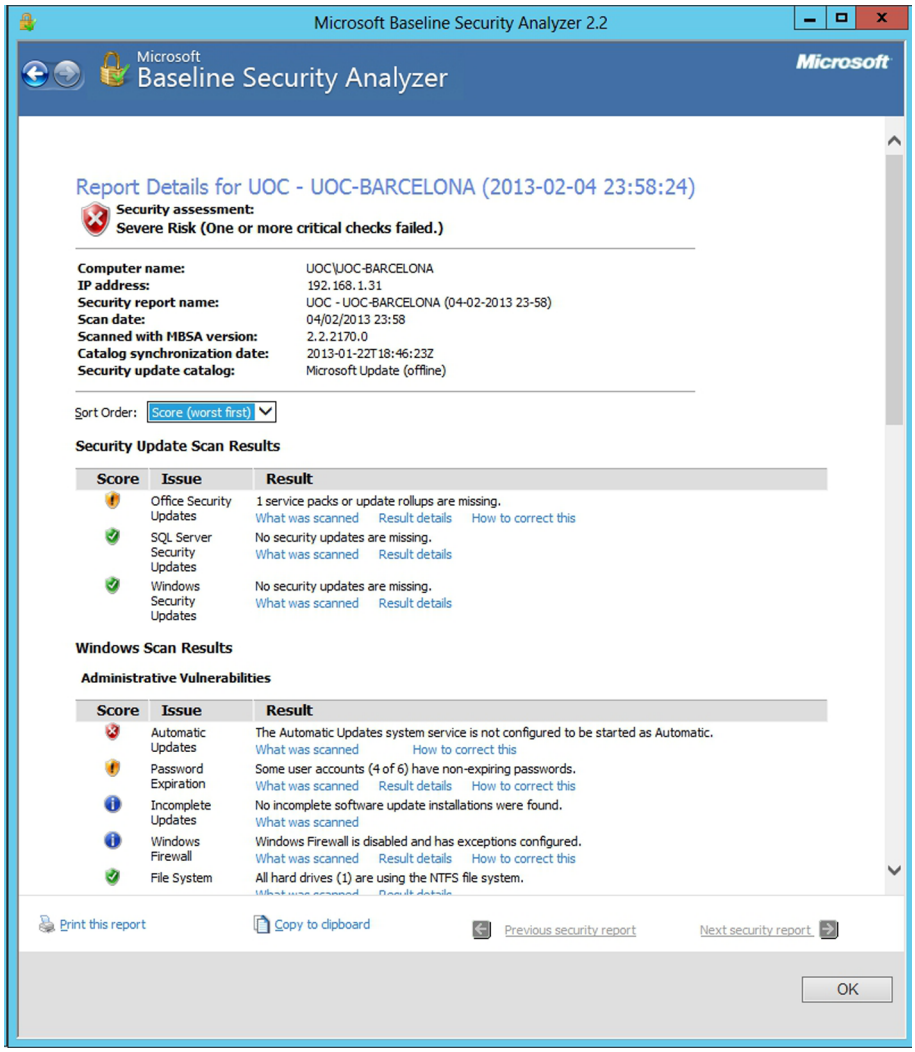
Microsoft Baseline Security Analyzer (MBSA) es una herramienta gratuita de Microsoft que permite hacer un análisis automático de la seguridad del sistema bastante completo y que, además, ofrece posibles soluciones a los problemas que encuentra. Permite determinar el estado de seguridad del equipo, según las recomendaciones de seguridad de Microsoft, y ofrece guías para corregir los fallos.

Configuración del escaneo de la seguridad de un servidor



La figura siguiente muestra la configuración por defecto del análisis que efectúa esta herramienta al servidor. El programa se conecta a Internet (a los servidores de Microsoft) para recuperar la última información sobre seguridad del sistema de Microsoft, y empieza a comprobar el ordenador seleccionado. Escanea todos los problemas conocidos y propone una solución, tal y como se puede ver en la siguiente figura, donde tenemos el resultado del escaneo de un servidor con Windows Server 2012.

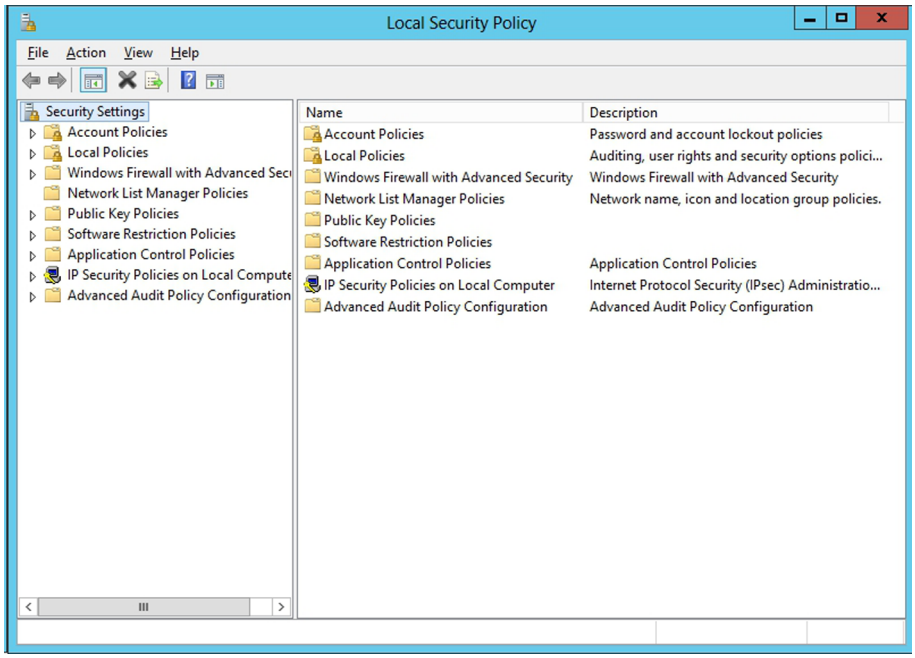
Resultado del escaneo de un servidor con MBSA



7.2.3. Configuración de seguridad local

La herramienta Directiva de seguridad local que está en el enlace de las herramientas dentro del administrador del servidor permite configurar los parámetros de seguridad para el equipo local.

Directivas de seguridad locales



En la parte derecha de la pantalla, como se puede ver en la figura anterior, encontramos las propiedades de seguridad que es posible modificar si hacemos doble clic encima de las mismas.

Desde aquí se puede acceder directamente a las políticas de grupo que están relacionadas con la seguridad, como por ejemplo las políticas de las cuentas de usuarios; las restricciones por las contraseñas; las políticas de bloqueo de los usuarios; la autenticación Kerberos; la configuración de las auditorías de los *logs*; las políticas del cortafuego de Windows; la criptografía con Bitlocker; restricciones del software que hay que instalar o usar; las VPN; etc. Se trata de un centro de control de todo lo relacionado con la seguridad del servidor.

7.2.4. Configuración y análisis de seguridad

La herramienta Configuración y análisis de seguridad permite analizar el estado de la seguridad del sistema según una plantilla de seguridad, y nos indica qué reglas o directivas de seguridad de la plantilla se cumplen y cuáles no. También permite modificar los parámetros de seguridad y configurar el sistema para cumplir todas las directivas de seguridad definidas en la plantilla.

Para ejecutar esta herramienta, tenemos que abrir la consola de administración del sistema con la orden `mmc.exe` y seleccionar la opción Agregar o quitar complemento del menú Archivo. Para añadir un elemento nuevo, hacemos clic sobre Agregar... y en la lista seleccionamos el componente Configuración y análisis de seguridad. Para empezar a trabajar, abrimos una base de datos de seguridad que ya exista o creamos una nueva. Una vez seleccionada la base de datos, salen los diferentes parámetros de seguridad definidos en la plantilla de seguridad elegida. En el caso de no tener ninguna plantilla de seguridad, será

necesario crear una a partir de la misma consola, añadiendo el componente Plantillas de seguridad. En esta plantilla, podremos definir todos aquellos parámetros que deseamos que el servidor tenga configurados.

Para cambiar la plantilla de seguridad, seleccionamos la opción Importar plantilla del menú contextual del elemento Configuración y análisis de seguridad de la lista de la izquierda.

Una vez seleccionada la plantilla, analizamos si el sistema cumple las directivas de seguridad definidas en la plantilla. Para esto, seleccionamos la opción Analizar el equipo del menú contextual del elemento Configuración y análisis de seguridad de la lista de la izquierda. Cuando acaba el análisis, se muestran los elementos que no cumplen la plantilla de seguridad y los que sí.

Para aplicar la plantilla de seguridad seleccionada en la configuración del equipo, seleccionamos la opción Configurar el equipo ahora del menú contextual del elemento Configuración y análisis de seguridad de la lista de la izquierda. El sistema llevará a cabo los cambios necesarios para satisfacer toda la plantilla de seguridad que se ha seleccionado.