Seguretat activa

Jordi Serra Ruiz

PID_00200500

Universitat Oberta de Catalunya

Índex

Introducció

La seguretat activa de les organitzacions i empreses és de les més importants que s'han de tenir en compte, ja que ens hi protegim de tots els possibles atacs maliciosos que ens puguin venir bàsicament per la xarxa, i tenint consciència que es prenen mesures addicionals perquè els intrusos no tinguin accés a la informació de l'empresa.

Per a protegir-se de lectures no volgudes de la informació guardada en un fitxer o de les dades que circulen per Internet, n'hi ha prou de xifrar els missatges o arxius amb un parell de claus públiques i privades perquè ningú a qui no s'hagi donat permís exprés abans no pugui accedir a la informació.

En aquest mòdul mostrarem els conceptes de certificats en la informació i claus públiques i privades.

D'altra banda, totes les aplicacions que s'han d'executar per a tenir l'accés mitjançant la xarxa les podem autenticar. És a dir, podem demanar que l'usuari s'autentiqui per utilitzar aquestes aplicacions.

Per exemple, en comptes d'utilitzar el protocol HTTP d'intercanvi de fitxers per Internet, es pot fer servir el protocol HTTPS, que ha d'autenticar l'usuari que intenta accedir al servidor web per baixar-se la informació.

Una altra manera d'assegurar-nos que no s'accedeix a la informació privada són les extensions IPsec (seguretat del control d'Internet), canals segurs d'informació que viatja per Internet.

Una de les tasques d'un administrador, a part d'aquestes que hem indicat i de les que hem descrit en el mòdul de seguretat passiva, és el monitoratge de la xarxa. El trànsit d'informació de la xarxa dóna molta informació de la manera com es pot accedir a les dades i qui ha accedit a cadascun dels recursos compartits. Veurem com es pot obtenir aquesta informació.

Objectius

En aquest mòdul pretenem que conegueu els diferents mètodes de seguretat activa que es poden implantar en una màquina. Per a alguns d'aquests mètodes, com per exemple les eines de comprovació, faria falta un tema sencer per a arribar a veure totes les possibilitats que poden arribar a proporcionar aquestes eines; a més, es requereixen coneixements de xarxes bastant avançats, cosa que excedeix el temari de l'assignatura. Per tant, simplement pretenem explicar que hi ha aquestes eines, com s'instal·len i quins són els propòsits que tenen. Després, cada administrador pot estudiar amb més deteniment aquestes eines i de manera més avançada.

Els objectius d'aquest mòdul són els següents:

1. Conèixer l'ús de certificats i saber com els hem d'instal·lar en les màquines.

2. Conèixer el funcionament i la instal·lació d'IPsec.

3. Saber instal·lar i configurar VPN.

4. Conèixer les eines de monitoratge de la Xarxa.

5. Saber quines eines de comprovació hi ha.

1. Certificats i sistemes de clau pública i privada

Al llarg de la història, l'ésser humà ha desenvolupat sistemes de seguretat per determinar diversos factors que intervenen en una comunicació o en un contracte. En la llista següent hi ha enumerats uns quants d'aquests sistemes:

1) Identificar les identitats dels interlocutors, és a dir, comprovar que les persones que intervenen en la comunicació són les que diuen que són (documents d'identificació, signatura).

2) Cap de les dues parts no pot modificar la informació de manera arbitrària. És a dir, una vegada signat un contracte, no es poden canviar els acords que s'hi han descrit. Per a verificar aquests acords hi ha els notaris.

3) Cap de les dues parts no pot negar el fet que es va comprometre amb aquesta informació. Una vegada signat el contracte, no el podem incomplir.

4) En el cas concret de les comunicacions, hi ha el correu certificat, que serveix per a assegurar-nos que el destinatari ha rebut la informació.

En la majoria d'aquests casos, el sistema de seguretat es basa en la identificació física de la persona. Actualment cal traslladar aquests sistemes de seguretat a l'entorn de les comunicacions digitals a causa d'un augment de les activitats comercials per Internet.

El principal problema d'aquest tipus de comunicacions és que no tenim cap seguretat de la identitat de la persona o entitat que hi ha a l'altre extrem de la comunicació. La causa principal d'aquest problema és que no hi ha contacte directe entre les persones que hi ha implicades en la transferència d'aquesta informació. Necessitem, per tant, un document digital que ofereixi les mateixes funcionalitats que els documents que hi ha implicats en les transaccions presencials (identificació, integritat, no-repudi i confidencialitat).

Les solucions a aquests problemes són la signatura electrònica i el certificat digital. Abans d'entrar a explicar aquests punts, però, cal que comentem conceptes més bàsics sobre criptografia.

Curiositat criptogràfica

Per exemple, si desplacem totes les lletres dotze posicions en l'abecedari normal, la *a* passa a ser la *m*, la *b* la *n*, etc., i un missatge com *atacar avui* passa a ser *mfmomd mhgu*.

La criptografia té l'origen en l'Imperi Romà, en l'època de l'emperador Juli Cèsar, que utilitzava un esquema criptogràfic simple, però efectiu, per a comunicar-se amb els seus generals. El mètode consistia a desplaçar cada lletra de l'alfabet un nombre determinat de posicions.

Aquest mètode de xifratge tan simple ens introdueix en el concepte de clau criptogràfica: l'algorisme necessari per a codificar el missatge. En aquest cas l'algorisme és "desplaçar dotze posicions cada lletra en l'abecedari". En resum, el concepte de xifratge és molt simple: a un text sense xifrar hi apliquem un algorisme de transformació del missatge (xifrat) i obtenim un missatge xifrat que només poden saber les persones que saben la clau criptogràfica.

1.1. Clau simètrica

Diem que una clau és simètrica quan s'utilitza la mateixa clau criptogràfica per a xifrar i per a desxifrar, és a dir, que el receptor necessita tenir la clau per a poder descobrir el missatge codificat. El procés de xifrar un missatge amb la clau simètrica és molt senzill i el veurem amb un exemple de comunicació entre dos usuaris, com ara l'Albert i en David.

1) L'Alicia escriu un missatge en text pla.
2) L'Alicia aplica un algorisme de xifratge amb clau simètrica coneguda.
3) L'Alicia envia el missatge a en Bob.
4) En Bob, utilitzant la mateixa clau, desxifra el missatge.

El gran avantatge del xifratge amb clau simètrica és la velocitat i això fa que aquest tipus de xifratge sigui molt apropiat per a xifrar grans volums d'informació. El problema del xifratge amb clau simètrica és que el receptor ha de tenir la clau criptogràfica; per tant, cal distribuir la clau entre totes les persones o entitats entre les quals ens volem comunicar de manera xifrada. Si algú és capaç d'interceptar el missatge i interceptar la distribució de la clau, també serà capaç de desxifrar el missatge.

1.2. Clau asimètrica

Diem que una clau és asimètrica quan es fan servir claus diferents per a xifrar i per a desxifrar un missatge. Aquest mètode utilitza dues claus que estan lligades entre si: la clau privada i la clau pública. La clau privada només l'ha de saber el propietari de la clau, i la pública s'ha de distribuir de manera arbitrària per la Xarxa (més endavant veurem que el sistema de distribució de claus no és tan arbitrari, sinó que segueix uns passos molt concrets).

Aquesta parella de claus és complementària, és a dir, el missatge que xifra una clau només el pot desxifrar l'altra. Com que l'obtenció de les dues claus s'aconsegueix amb mètodes matemàtics molt complexos, és impossible (per raons de cost temporal) deduir la clau privada a partir de la clau pública. Costaria tants anys poder fer això que no surt a compte, i per tant es considera segur el mètode.

El funcionament de les comunicacions mitjançant aquest mètode el veurem amb un exemple. Imaginem-nos que l'Alicia es vol comunicar amb en Bob. Tots dos tenen una clau pública i una de privada. La clau privada només la sap el propietari, cadascú la seva, però les públiques les saben tots dos, ja que han accedit mitjançant la xarxa a la clau pública de l'altra persona.

Si l'Alicia vol enviar un missatge a en Bob i que només el pugui llegir ell, ha de seguir els passos següents:

1) L'Alicia escriu un missatge en text pla.

2) L'Alicia xifra el missatge fent servir com a clau criptogràfica la clau pública d'en Bob.

3) El destinatari (en Bob) rep el missatge xifrat i el desxifra amb la seva clau privada (que només sap ell i que és l'única que pot desxifrar el missatge).

Si en Bob vol respondre l'Alicia, ha de fer servir com a clau criptogràfica la clau pública de l'Alicia. D'aquesta manera s'assegura que la resposta només la podrà obrir ella. Mitjançant l'ús de les claus asimètriques obtenim molta més seguretat, ja que per a desxifrar una comunicació cal fer servir la clau privada, i aquesta clau no es distribueix. Per a generar un missatge cal especificar a qui es vol enviar i utilitzar la clau pública del destinatari, que només ell pot obrir amb la seva clau privada.

El desavantatge d'aquest mètode és que les claus asimètriques, per la complexitat que tenen, són molt lentes a l'hora de xifrar i desxifrar. I en el cas que una clau privada fos distribuïda s'hauria d'invalidar i crear una nova parella de claus asimètriques per a tornar a tenir seguretat en les comunicacions.

1.3. Clau de sessió

La clau de sessió és un ús combinat de les dues claus anteriors per a aprofitar la velocitat de la clau pública amb la seguretat de la clau privada. Ara, mitjançant un exemple de comunicació entre l'Alicia i en Bob, veurem el procés de xifratge d'aquest mètode.

1) L'Alicia escriu un text pla.

2) L'Alicia el xifra amb una clau simètrica generada de manera aleatòria, anomenada clau de sessió.

3) L'Alicia ja pot enviar el missatge a en Bob.

4) Per fer arribar la clau a en Bob, xifra la clau de sessió amb la qual ha xifrat el missatge amb la clau pública d'en Bob i la hi envia.

5) En Bob, amb la seva clau privada, desxifra el segon missatge amb la clau i, una vegada té la clau de sessió, pot desxifrar i xifrar els missatges, i per tant es pot comunicar amb l'Alicia de manera ràpida fent servir la clau simètrica que s'ha distribuït entre ells mitjançant una sola comunicació amb clau asimètrica, molt més lenta.

D'aquesta manera, fins que no tanquin la comunicació, o vulguin canviar la clau simètrica, el sistema farà servir la clau simètrica, que fa que la comunicació sigui molt més ràpida. Els portals web que fan servir protocols segurs fan servir tècniques semblants a aquesta.

Mitjançant aquest mètode aconseguim identificació i confidencialitat de la comunicació, i una velocitat de comunicació més ràpida que no pas utilitzant només les claus asimètriques. Si la comunicació s'estableix entre un client i un servidor, la negociació de les claus que es duu a terme entre l'un i l'altre es fa de manera transparent per a l'usuari (situat en el client). En aquests casos, les claus de sessió poden trigar fins a un dia a caducar. És a dir, si durant aquest dia fem unes quantes connexions amb el servidor, utilitzarem en totes les connexions la mateixa clau de sessió, sense haver de tornar a negociar l'intercanvi de claus.

1.4. Signatura digital

La signatura digital es fa servir amb el mateix fi que una signatura manuscrita. Per tant, l'objectiu és que el receptor sàpiga que l'emissor és qui diu que és, que el receptor i l'emissor sàpiguen que no s'ha modificat el contingut del missatge i que l'emissor no pugui repudiar un missatge enviat. La signatura digital funciona de la mateixa manera que les claus asimètriques, però en lloc de fer servir la clau pública del receptor fa servir la clau privada de l'emissor. Com que són claus complementàries, tot el que es xifra amb la clau privada es desxifra amb la pública, i viceversa.

No obstant això, ja hem vist que el principal inconvenient de les claus asimètriques és la lentitud que tenen, que augmenta segons la llargada del missatge que cal xifrar. Per a solucionar aquest problema, la signatura digital fa servir unes funcions *hash*.

Una funció *hash* és una operació que es fa sobre un conjunt de dades de qualsevol mida i que té com a resultat un subconjunt d'aquestes dades de mida fixa (anomenat *resum*), que té la propietat d'estar unit unívocament al text original. Com hem fet fins ara, veurem el procés d'una signatura digital amb l'exemple de comunicació entre l'Alicia i en Bob.

1) L'Alicia escriu un missatge original.

2) L'Alicia executa un *hash* sobre el missatge original i obté un resum.

3) L'Alicia xifra el resum amb la seva clau privada (d'aquest procés se'n diu signatura digital).

4) L'Alicia envia el missatge juntament amb la signatura a en Bob. (Noteu que no s'ha d'enviar la clau privada, només la signatura digital.)

5) En Bob, per assegurar-se que el missatge és de l'Alicia, n'ha de comprovar la signatura; per fer-ho, ha de desxifrar la signatura amb la clau pública de l'Alicia, i així obté el resum.

6) En Bob aplica un *hash* sobre el missatge original, i així obté un altre resum.

7) Finalment, compara els dos resums: si són iguals, pot estar segur que el missatge l'ha enviat l'Alicia i que no s'ha modificat des que s'ha generat.

1.5. Certificat digital

Els mètodes comentats fins ara, que es basen en les claus asimètriques, tenen una cosa en comú: l'èxit que tinguin depèn del fet que la clau privada dels usuaris només la sàpiguen aquests usuaris i que la clau pública sigui distribuïda per la Xarxa sense donar motiu a confusions entre les claus públiques dels diferents usuaris. Les claus privades solen estar integrades en targetes intel·ligents (són les targetes que porten un xip) o en un altre tipus de suport que impedeixi duplicar-les. Perquè hi hagi més seguretat, aquestes targetes també estan protegides amb contrasenyes numèriques que garanteixen que en cas de pèrdua no es puguin fer servir les claus.

Si la clau privada és per a una màquina (per a fer comunicacions segures per la Xarxa), ha d'estar en un directori només accessible per a l'usuari administrador i només amb permís de lectura per a aquest usuari. Les claus públiques estan associades als usuaris, però per a assegurar que una clau pública concreta pertany a un determinat usuari es fan servir els certificats digitals.

Els certificats digitals són documents electrònics que associen una clau pública amb la identitat d'un usuari. A més d'aquestes dades, un certificat digital pot contenir altres atributs, com són la data de principi i fi de validesa o l'àmbit en què es pot utilitzar aquesta clau pública.

Com sabem que és vàlid un certificat digital? Es pot donar el cas que algú falsifiqui el certificat digital d'en Bob; d'aquesta manera, quan l'Alicia consulti el certificat digital d'en Bob i n'obtingui la clau pública per poder-li enviar un missatge, en realitat ha obtingut la clau pública d'una tercera persona que vulgui conèixer la comunicació que mantenen ells. D'aquesta manera, quan l'Alicia enviï un missatge a en Bob, aquest no el podrà desxifrar, però sí que ho podrà fer la tercera persona que hi ha a l'escolta.

La validesa d'un certificat és molt important per a la comunicació, ja que mitjançant el certificat nosaltres confiem que la persona a qui identifica aquest certificat és la que esperem que sigui. La manera de confiar en un certificat digital d'una persona amb la qual fins ara no hem tingut cap relació és mitjançant l'ús del que s'anomenen terceres persones de confiança. La idea és que dos usuaris puguin confiar entre si, si tots dos tenen en comú una tercera persona que doni fe del procés. Aquesta idea no és nova: en l'àmbit comercial tradicional aquesta figura és el notari. En el cas concret del món electrònic, aquesta tercera persona és l'entitat certificadora o autoritat de certificació (CA).

Si un certificat l'avala una entitat certificadora reconeguda és de més confiança que si no l'avala ningú. Com sabem, però, que és reconeguda, aquesta entitat certificadora? La resposta la trobem en l'estructura de les entitats certificadores. Aquesta estructura és jeràrquica (semblant a l'estructura del servidor de noms de domini o DNS): hi ha una entitat certificadora a escala mundial que certifica les entitats certificadores principals de cada país, les quals, al seu torn, certifiquen les entitats certificadores de cada comunitat, i així successivament fins a arribar a les entitats que, com a usuaris, ens poden emetre un certificat digital. El model de confiança basat en tercers de confiança (TTP) és la base de la definició de la infraestructura de clau pública o *public-key infrastructure* (PKI). Una PKI és un conjunt de protocols, serveis i estàndards que són compatibles amb aplicacions basades en criptografia de clau pública. Aquest sistema es considera segur, tot i que hi ha hagut casos en què s'han vulnerat sistemes i han obtingut certificats vàlids terceres persones que els han fet servir per a "certificar" programes que eren maliciosos. La solució la dóna la revocació d'aquests certificats generals, i per tant tots els que puguin penjar d'aquests.

1.6. Petició d'un certificat

Un servidor també pot tenir un certificat. Aquests certificats s'utilitzen en la família de protocols anomenats segurs. Els passos que s'han de seguir són: primer demanar un certificat per a un servidor i després instal·lar aquest certificat. La instal·lació del certificat en la màquina és tan fàcil com posar-lo en un directori. Per a fer servir un certificat, però, no n'hi ha prou de tenir-lo a la màquina, sinó que hem de configurar els serveis que el volen utilitzar perquè puguin treballar amb certificats. En el mòdul següent explicarem com s'instal·len i es configuren la majoria dels serveis; per tant, és en aquell mòdul on comentarem els passos que s'han de seguir per a configurar els certificats en els diferents serveis.

2. Certificats en GNU/Linux

El primer pas és assegurar-nos que tenim instal·lat el paquet `openssl`. Per a saber si tenim instal·lat un paquet en el nostre servidor, hem de fer servir l'aplicació de gestió de paquets del Debian. D'aquesta manera, executem l'ordre següent:

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

Si el resultat és semblant a aquest:

```
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:~#
```

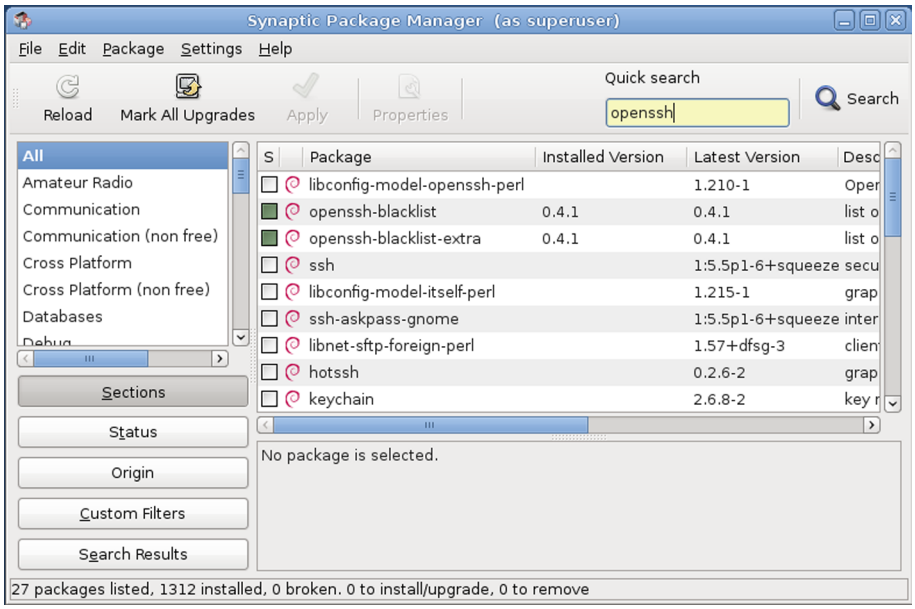
Ens indica que tenim aquest paquet instal·lat i, a més, quina versió fem servir. Si en el camp `version` surt `<none>` i la descripció del paquet no està disponible vol dir que no tenim el paquet instal·lat.

Per a solucionar-ho només cal instal·lar el paquet fent servir l'ordre `apt-get`:

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

o directament des del gestor de paquets Synaptic:

Gestor de paquets Synaptic



El pas següent és crear una clau privada per a la nostra màquina. Per a fer-ho només cal executar l'ordre següent:

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

Això genera una clau privada de 1.024 bits, amb el format de xifratge AES. La clau es crea en el directori en què som amb el nom `Server.key`.

També podem protegir la clau privada generada amb una contrasenya. Si no hi volem posar cap contrasenya, quan ens ho demani hem de prémer la tecla d'entrada. No passa res si després canviem d'opinió, ja que hi ha ordres per a canviar les contrasenyes de les claus privades.

Per canviar la contrasenya d'una clau privada, hem d'executar les ordres següents:

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

La primera ordre ens demana la contrasenya vella de la clau privada i després ens demana la nova, i escriu el resultat en un fitxer nou (`server.key.new`). L'últim pas sobreescriu el fitxer amb la clau vella. D'aquesta manera no cal canviar la configuració de cap aplicació que faci servir aquest nom de fitxer com a clau privada del servidor.

Un cop ja disposem de la clau privada podem generar la clau pública a partir d'aquesta. Per fer-ho, podem certificar nosaltres mateixos aquesta clau pública, cosa que no és gaire recomanable, ja que llavors ningú no confiarà en nosaltres

perquè no ens avalarà cap entitat certificadora, o podem fer una sol·licitud de certificat de signatura o *certificate signing request* (CSR) a una entitat certificadora avalada.

Evidentment us recomanem l'ús d'aquesta opció, ja que així les comunicacions amb terceres persones estaran més segures i es donarà més confiança a aquestes persones.

Per fer-ho, hem d'executar l'ordre:

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

Quan s'executa aquesta ordre, el primer que demana és la contrasenya de la clau privada amb la qual es vol crear la clau pública, després el país, l'estat o regió, la ciutat, l'organització o empresa, la secció de l'empresa, el nom de l'administrador de la màquina i una adreça de correu electrònic. Finalment, ens demana uns atributs addicionals; si no els hi volem posar, premem la tecla d'entrada.

Una vegada tenim la petició d'un certificat hem d'enviar aquesta petició (`server.csr`) a una entitat certificadora. Quan ens retornin la petició (`server.pem`) ja tenim un certificat real que podem fer servir per a configurar els serveis segurs que volem que tingui el servidor.

Aquest últim pas, el d'enviar el certificat a una entitat, varia una mica segons l'entitat que triem perquè ens certifiqui. A Internet hi ha unes quantes entitats que ho fan (Verisign, Thawte Consulting, BelSign, etc.), les quals ofereixen contractar la validació dels certificats anualment i també altres serveis per a fer més segura la comunicació per la Xarxa.

2.1. Creació d'una CA

La creació de la nostra pròpia CA és a vegades un procés innecessari, ja que els nostres certificats autenticats per nosaltres mateixos no tenen gaire credibilitat. Hi ha casos, però, en què aquest procés és molt útil; per exemple, casos en què només puguin accedir a la nostra intranet els usuaris que tenen un certificat avalat per nosaltres. Com els clients que s'han de connectar tant a la xarxa Wi-Fi com a la part segura de la intranet.

En primer lloc, hem de crear una clau privada per a la CA. Per fer-ho, executem l'ordre següent:

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

Igual que en els casos anteriors, hem de guardar molt bé aquest fitxer, ja que és la nostra clau privada de l'autoritat certificadora local que s'està creant.

En segon lloc, una vegada tenim la clau privada, l'hem de certificar amb el nostre propi certificat. Per fer-ho, executem l'ordre següent:

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

Que crearà un certificat (`ca.crt`) d'un any de validesa amb format x509.

Ara, en principi, ja estem en disposició de certificar els nostres propis certificats, però per fer-ho primer hem de tenir un *script* de certificació. Podem fer el nostre propi *script* o, si hem instal·lat el `mod_ssl` mitjançant la compilació del codi font, podem trobar un *script* de certificació en el directori `pkg.contri/sign.sh` de les fonts. En qualsevol cas, l'*script* ha de ser semblant a aquest:

```
#!/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 vegada tenim aquest *script* ja podem certificar. Imaginem-nos que tenim una petició d'una màquina que es diu `server.crt`. Per fer aquest certificat, hem d'executar l'ordre

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

2.2. Revocació d'un certificat

Les autoritats certificadores (CA) no solament avalen els certificats, sinó que també els administren. Administrar un certificat implica determinar-ne el període de validesa, renovar-lo o revocar-lo. La revocació d'un certificat és deixar-ne d'avalar un que fins ara era vàlid.

Exemples de revocació de certificat

1) Imaginem-nos que l'Alicia comença a treballar en una nova empresa, la qual li tramita un certificat personal en el moment d'entrar. El període de validesa d'aquest certificat és de dos anys, però al cap de sis mesos l'Alicia deixa l'empresa. El certificat de l'Alicia s'ha de revocar quan deixa l'empresa, ja que a partir de llavors no té cap vinculació amb l'empresa.

2) Un altre exemple de revocació d'un certificat és si detectem que la nostra màquina ha estat vulnerada, és a dir, s'hi han introduït intrusos i, a més, ho han fet amb privilegis d'administrador. En aquest cas, el certificat s'ha de revocar perquè tenim dubtes sobre la duplicació de la nostra clau privada. En aquest cas no val canviar la contrasenya de la clau privada, s'ha de revocar per a estar completament segur que no es farà servir en un altre lloc.

Els certificats que s'han revocat els publiquen les autoritats certificadores en unes llistes, que es *diuen llistes de revocació de certificats* o *certificate revocation lists* (CRL). Com que els certificats es distribueixen molt ràpidament, és impossible saber si l'han revocat mirant només el certificat.

Quan ens fixem en la validesa dels certificats, és quan hem de contactar amb una autoritat certificadora i comprovar a la seva llista de revocació si s'ha revocat el certificat. La majoria de les autoritats certificadores tenen una pàgina web on publiquen els certificats que s'han revocat.

Si nosaltres tenim la nostra pròpia autoritat certificadora i volem revocar un certificat perquè considerem que ha estat compromès, hem d'executar l'ordre

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

Després hem de regenerar la llista dels certificats revocats mitjançant l'ordre següent:

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

3. Certificats en el Windows Server 2012

Com s'ha explicat, una infraestructura de clau pública (PKI) consisteix en un conjunt de serveis, tecnologies, protocols i estàndards que permeten fer accions de manera segura en entorns distribuïts. La infraestructura de clau pública d'una xarxa, que necessitarem per al servidor Windows, consta dels elements següents:

1) Certificats digitals. Un certificat digital és una credencial electrònica que es compon d'una clau pública i una clau privada, i s'utilitza per a autenticar els usuaris.

2) Entitat emissora de certificats. Són entitats de confiança que creen certificats d'autenticació. Hi ha autoritats de certificació reconegudes mundialment, encara que es pot configurar un emissor de certificats propi per a propòsits específics.

3) Eines d'administració de claus i certificats. Són eines de gestió per a administrar certificats digitals en un servidor d'emissió de certificats.

4) Punt de publicació de certificats. Lloc on s'emmagatzemen i es publiquen els certificats. En el cas d'entitats emissores de certificats basades en Windows, els certificats s'emmagatzemen mitjançant l'Active Directory, en el mòdul addicional que ja s'ha instal·lat i que fa de gestor de certificats. L'AD-CS (Active Directory Certificate Services) és el que s'encarrega de la gestió dels certificats dins el directori actiu.

5) Aplicacions i serveis preparats per a l'ús de claus públiques. Perquè els certificats siguin útils, les aplicacions i els serveis de transferència d'informació han d'estar preparats per a fer-los servir. Uns exemples d'aplicacions preparades per a l'ús de certificats són el Microsoft Outlook i el Microsoft Internet Explorer. També són compatibles amb l'ús de certificats els serveis d'arxius xifrats o *encrypting file system* (EFS) i de seguretat del protocol d'Internet.

6) Llista de revocacions de certificat. Consisteix en una llista de certificats que s'han revocat (anul·lat) abans que no caduquessin.

3.1. Gestió de certificats

Per a gestionar els certificats locals disponibles en el sistema Windows mateix, utilitzem l'opció Certificats de la finestra Propietats d'Internet, que s'obre en seleccionar l'element Opcions d'Internet del tauler de control del sistema. En aquesta pantalla, en la figura següent, surten els certificats instal·lats en el compte local de l'equip, separats en diferents categories:

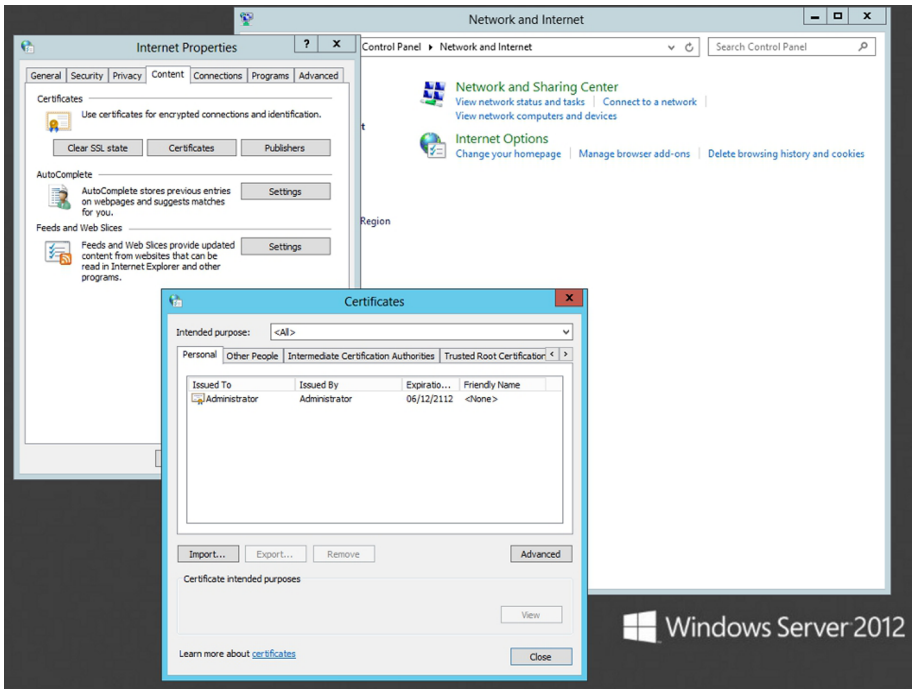
1) Personal: certificats personals amb una clau privada que hi està associada.

2) Altres persones: certificats d'altres persones amb les quals es comparteix l'accés a fitxers xifrats.

3) Entitats emissores de certificats intermèdies: certificats d'entitats de certificació que depenen d'altres entitats de certificació.

4) Entitats emissores de certificats arrel de confiança: certificats d'entitats de certificació que emeten certificats arrel de confiança (s'hi confia implícitament).

Certificats propis del sistema



En la llista de selecció Propòsit plantejat podem filtrar els certificats pel propòsit que tenen. Per tenir més informació sobre un certificat en concret, fem doble clic sobre l'element corresponent en la llista de certificats o sobre el botó Veure. Mitjançant el botó Modificar propietats podem modificar els propòsits per als quals s'utilitza aquest certificat digital. També podem modificar els propòsits del certificat seleccionat en la llista de certificats de la finestra Certificats, mitjançant el botó Avançades...

Hi ha diversos propòsits per a un certificat, entre els quals, l'autenticació d'usuaris que accedeixen al servidor, la signatura de codi (per a permetre l'execució en altres equips), la utilització del certificat en missatges de correu electrònic, la seguretat IP, el xifratge d'arxius i la signatura de documents. També és possible definir nous propòsits per a usos personalitzats dels certificats.

3.1.1. Importar i exportar certificats

Podem importar i exportar certificats amb els botons "Importar" i "Exportar" de la finestra "Certificats". També es pot eliminar un certificat mitjançant el botó "Treure". Importar un certificat afegeix un certificat a la llista de certificats que ja hi ha, ja sigui un certificat personal, un certificat d'una altra persona o un certificat d'una entitat emissora de certificats. Quan premem el botó Importar, comença l'assistent d'importació de certificats. Després de seleccionar l'arxiu que volem importar, hem de seleccionar també el magatzem de certificats en què el volem guardar. Podem deixar que el magatzem se seleccioni automàticament o seleccionar un magatzem concret. Un magatzem de certificats no és més que una petita base de dades en la qual s'emmagatzema un conjunt de certificats.

Finalment, l'assistent mostra un resum de la importació del certificat. Una vegada acceptem el resum, ens demana confirmació per fer l'operació d'importació del certificat en el magatzem especificat. L'exportació de certificats és útil per a transmetre una clau pública o com a mesura de seguretat. Quan premem el botó Exportar, comença l'assistent d'exportació del certificat seleccionat a la llista.

L'assistent ens demana si volem exportar també la clau privada (en cas de certificats personals que incloguin clau pública i privada), i el format de l'arxiu d'exportació. Finalment, hem de seleccionar la localització i el nom del fitxer on volem exportar el certificat. S'ha d'estar segur que es vol exportar també la clau privada, ja que si es perd i cau en mans d'una altra persona podrà fer absolutament tot el que vulgui amb el certificat. Per tant, si és necessari exportar la clau privada, per exemple per a tenir una còpia de seguretat del certificat per a poder-lo instal·lar en un altre ordinador, s'haurà de protegir amb una contrasenya suficientment segura.

3.1.2. Complement de certificats

A part de la finestra de certificats dins de la finestra de propietats d'Internet, hi ha un complement del gestor de consola, la Microsoft Management Console (MMC), per a gestionar certificats. Per instal·lar el complement a la consola, l'hem d'obrir, escrivint l'ordre `mmc.exe` en una finestra del PowerShell.

En la finestra de la consola que apareix, s'ha de seleccionar l'opció "Agregar o treure complements" del menú Consola. En la finestra d'agregar components, premem el botó Agregar per agregar el complement Certificats que hi ha en la llista de complements disponibles.

Si s'ha iniciat sessió amb un compte d'administrador, surten tres opcions sobre els certificats que es gestionaran:

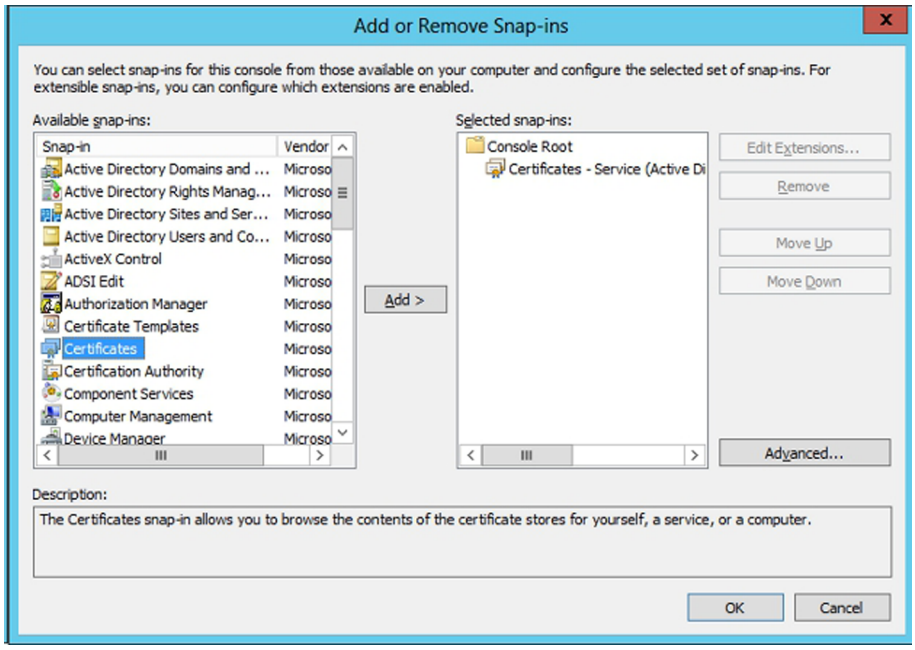
1) El meu compte d'usuari: permet gestionar els certificats del compte actual.

2) Compte de servei: permet gestionar els certificats d'un compte de servei del sistema.

3) Compte d'equip: permet gestionar els certificats d'un compte d'un altre equip. Podem instal·lar els certificats en altres equips.

Finalment, surt el nou complement a la consola, on veiem els certificats organitzats per tipus i on podem fer les accions que ja hem vist abans sobre certificats.

Complements per a la consola. Instal·lació de certificats



3.2. Utilització de certificats

Els certificats digitals es poden fer servir amb diverses utilitats per a garantir l'autenticitat de documents o autenticar usuaris. Entre aquestes utilitats, les més comunes són la de signatura electrònica, el xifratge d'arxius i l'autenticació de programari per Internet.

3.2.1. Signatura electrònica

Els programes de correu com l'MS Outlook permeten signar un missatge de correu electrònic, perquè el destinatari pugui comprovar que el missatge l'hem enviat nosaltres, i no un tercer en nom nostre.

Signatura en l'Outlook Express

Per a signar un missatge en l'Outlook Express, utilitzem l'opció Signar digitalment del menú Eines de la finestra de creació del missatge. Això fa que se signi el missatge amb el certificat digital associat al compte amb què hem iniciat sessió.

3.2.2. Xifratge d'arxius

El xifratge d'arxius serveix per a protegir documents, de tal manera que només els puguin llegir o modificar les persones autoritzades. Per xifrar un arxiu, obrim la finestra de propietats (opció Propietats del menú contextual que surt en fer clic amb el botó secundari del ratolí sobre la icona del fitxer) i premem el botó Avançades... En la finestra que surt seleccionem l'opció Xifrar continguts per a protegir dades, amb la qual cosa es xifra l'arxiu amb el certificat associat al compte amb què hem iniciat sessió. Quan acceptem ens demana si volem xifrar només l'arxiu seleccionat o també la carpeta que el conté.

Una altra opció molt més nova i completa és l'eina BitLocker, que es pot instal·lar com una característica més del servidor, i per tant per a fer-ho s'ha de fer a l'administrador del servidor. Aquesta eina està pensada per a entorns més empresarials i permet xifrar únicament fitxers separats o tota una unitat sencera. Aquesta eina permet gestionar tots els discos xifrats dels ordinadors de la xarxa i poder desxifrar-los remotament en cas necessari automàticament, i això és útil per a poder instal·lar algun programari de manera remota en el cas de tenir el disc completament xifrat en l'ordinador client. Aquesta característica s'ha d'instal·lar a part, és a dir, que no forma part de la característica del BitLocker, ja que és una altra que permet l'accés a aquests discos remotament.

A més permet xifrar tot un volum (un disc sencer), o únicament el contingut, cosa que farà que sigui molt més ràpid, i a més que la part que no està xifrada la puguin utilitzar altres persones. Per tant, es pot pensar que cada usuari pugui tenir una part del disc dur de l'ordinador, sobretot els portàtils, xifrada, i la resta no, i així aquest recurs pot ser compartit sense que la informació d'un usuari pugui ser vista per un altre usuari sense permís. Això es configura directament des de les polítiques de grup del directori actiu, i així es té molt més control sobre els ordinadors si cal. Es pot deixar que l'usuari decideixi què vol xifrar del seu disc dur, o decidir que s'ha de xifrar tot el volum o només la part amb dades i alliberar la resta del disc. Es pot trobar en la política de grup

```
\Configuració de l'equip\Directives\Plantilles administratives\Components de Windows\
Xifratge d'unitat BitLocker
```

Que apareixerà en el moment d'instal·lar la característica de xifratge amb el BitLocker.

3.2.3. Acceptació de certificats

Les aplicacions web tenen una sèrie d'accions restringides per a evitar que aplicacions malintencionades puguin danyar el sistema de l'usuari. A vegades hi ha pàgines web que requereixen alguns privilegis, en principi vetats, per a dur a terme l'activitat que han de fer, com per exemple accedir al disc dur. Per a això, se signa digitalment l'aplicació de manera que cada usuari pot decidir si confia o no en l'entitat que ha desenvolupat l'aplicació.

Certificat de Microsoft

La primera vegada que visitem el centre d'actualitzacions de Microsoft (Windows Update), ens demana la confirmació per executar el component necessari per a fer les actualitzacions. Si acceptem, s'instal·la el certificat de Microsoft, al qual es donen els privilegis necessaris per a fer les actualitzacions. També podem confiar sempre en el certificat de Microsoft (mitjançant la casella de selecció o *checkbox*), de manera que no ens torni a demanar confirmació per a instal·lar cap més component web desenvolupat i signat per Microsoft (s'instal·la directament).

3.3. Emissió de certificats

Tenim bàsicament dues maneres d'obtenir un certificat digital. Si necessitem el certificat per a fer operacions d'autenticació amb altres persones alienes a la nostra empresa, per a sol·licitar permisos en una pàgina web, per a executar codi no segur, etc., hem de sol·licitar el certificat a una entitat certificadora de confiança. En canvi, si el certificat és per a fer gestions dins de l'empresa mateixa, el més segur és que hi hagi un servidor de certificació que gestioni i emeti els certificats als treballadors.

3.3.1. Entitat certificadora de confiança

Hi ha entitats de certificació conegudes com Securenet (www.securenet.net), Verisign (www.verisign.com) o Thawte (www.thawte.com) que emeten certificats d'autenticació que són acceptats en la majoria de les aplicacions, ja que els certificats d'aquestes companyies estan inclosos en el magatzem de certificats predeterminat del sistema operatiu Windows.

Hi ha altres entitats de certificació amb propòsits més específics, com per exemple la Fàbrica Nacional de Moneda i Timbre a Espanya, que expedeix els certificats digitals que identifiquen els usuaris a l'hora de fer gestions amb l'Administració pública i Hisenda per Internet (www.cert.fnmt.es).

3.3.2. Servidor de certificació

La feina d'un servidor de certificació l'ha de dur a terme un servidor o més d'un servidor de l'empresa. La comesa que té és rebre sol·licituds d'emissió o renovació de certificats dels usuaris (treballadors o potser clients de l'empresa) que necessitin aquest certificat per a fer alguna gestió.

El Windows Server 2012, com s'ha indicat anteriorment, incorpora l'AD CS (Active Directory Certificate Server), que proporciona aquesta funcionalitat. Per a instal·lar aquest paper només s'ha de seleccionar en l'administrador del servidor, com s'ha indicat en el capítol de la instal·lació. A continuació, ens avisen que si instal·lem aquests serveis no podrem canviar el nom del servidor més endavant, ni afegir-lo a un domini, ni treure'l d'un domini, ja que els cer-

tificats pertanyen al servidor amb aquelles característiques. Abans d'instal·lar el paper també hem d'especificar el tipus de servidor de certificats que volem instal·lar, que dependrà del que es vulgui fer en cada cas. Podem fer:

Els tipus d'entitat emissora de certificats que es poden configurar són els següents:

1) Entitat emissora arrel de l'empresa: entitat principal, de màxima confiança en l'empresa.

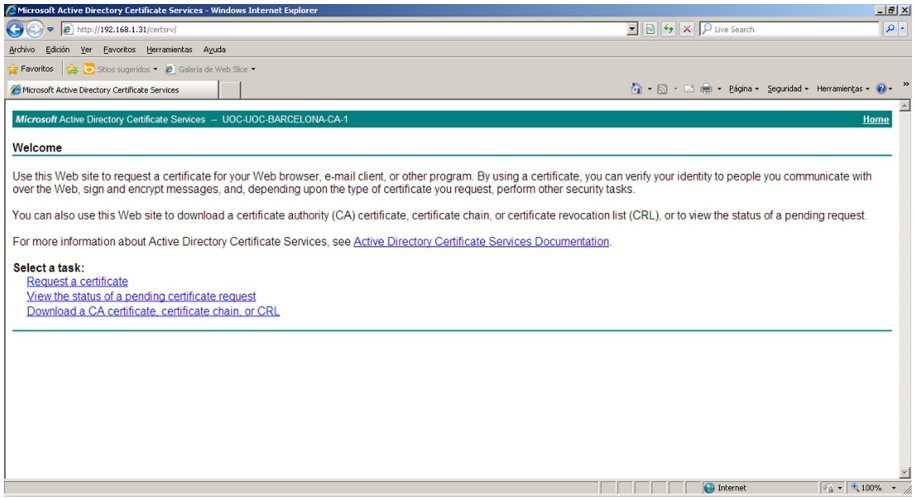
2) Entitat emissora subordinada de l'empresa: entitat secundària de certificació en l'empresa. Ha d'obtenir un certificat d'entitat emissora de certificats d'una altra entitat emissora de certificats de l'empresa.

3) Entitat emissora arrel independent: entitat principal, de màxima confiança en una jerarquia.

4) Entitat emissora subordinada independent: entitat secundària de certificació en una jerarquia. Ha d'obtenir un certificat d'entitat emissora de certificats d'una altra entitat emissora de certificats.

Una vegada introduïdes totes les dades, comença el procés d'instal·lació. En el cas de tenir també instal·lat el paper d'inscripció web (*web enrollment*) el procés d'instal·lació crea una sèrie de pàgines web que permeten als usuaris dels equips client, o des d'altres servidors, accedir al servidor emissor de certificats per a sol·licitar un certificat digital. L'adreça de la pàgina inicial de sol·licitud de certificats és `http://nomservidor/certsrv`, en què *nomservidor* és el nom del servidor d'emissió de certificats. Depenent de la configuració del servidor d'informació d'Internet (IIS), pot ser que ens hàgim d'autenticar abans d'accedir al lloc web, encara que una vegada validats hi podem accedir directament utilitzant les credencials de l'usuari amb el qual estem autenticats en la nostra estació de treball.

Pàgina web d'obtenció i renovació dels certificats



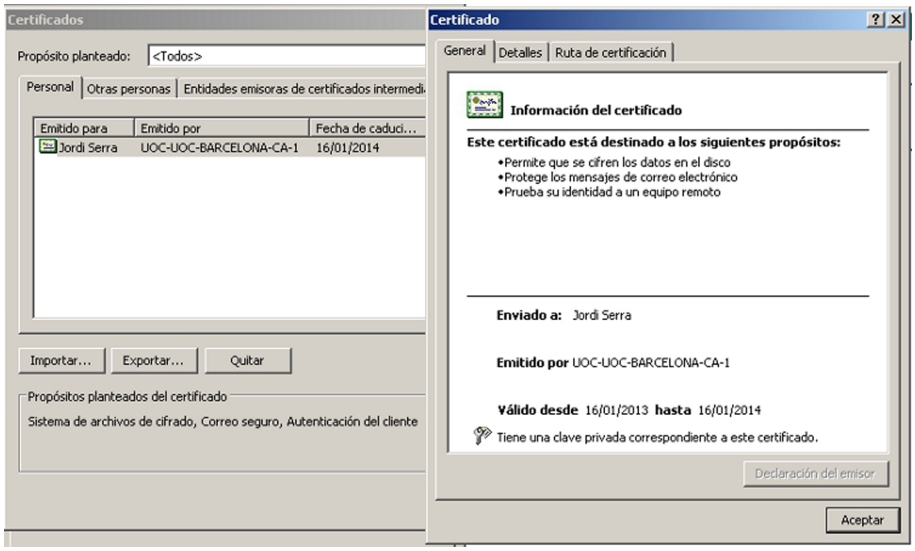
En la pantalla inicial d'aquesta pàgina web, en la figura anterior, hi trobem tres opcions:

1) Sol·licitar un certificat: permet sol·licitar un certificat a l'entitat de certificació.

2) Veure l'estat d'una sol·licitud de certificat: permet comprovar l'estat d'un certificat sol·licitat amb anterioritat.

3) Baixar un certificat d'entitat emissora, cadena de certificats o llista de revocació: permet recuperar el certificat de l'entitat emissora de certificats o la llista de certificats que ha revocat aquesta entitat.

Certificat instal·lat



Per sol·licitar un certificat, seleccionem la primera opció. En la pàgina següent seleccionem el tipus de certificat. En el cas d'una entitat emissora d'empresa, l'únic tipus de certificat disponible és el certificat d'usuari. En canvi, en una entitat emissora independent, podem sol·licitar certificats per a exploració web o de protecció de correu electrònic.

Si l'entitat de certificació és d'empresa, la informació de l'usuari es recupera automàticament i el certificat s'emet directament. En la pàgina següent es pot instal·lar el certificat.

Si anem a l'eina Entitat de certificació d'Eines administratives o a les propietats d'Internet, veiem el nou certificat emès, com es veu en la figura anterior. Des d'aquesta eina també podem revocar certificats emesos anteriorment, revisar peticions pendents de certificats, etc.

En canvi, si l'entitat de certificació és independent, cal introduir les dades de l'usuari o de l'equip per al qual demanem el certificat. La petició de la sol·licitud queda pendent en el servidor fins que un administrador confirmi l'emissió del certificat.

Si anem a l'eina Entitat de certificació, veiem que hi ha un certificat pendent. Mitjançant les opcions del menú Acció podem emetre el certificat sol·licitat o denegar-lo.

Per a comprovar l'estat de tramitació d'un certificat, podem utilitzar la segona opció de la pàgina web del servidor de certificació. Seleccionem el certificat sol·licitat i, en la pàgina següent, ens mostra l'estat del certificat, tant si està denegat com pendent de tramitació o concedit, cas en què ens permet baixar-lo i instal·lar-lo.

L'última de les opcions de la pàgina web del servidor d'emissió de certificats és recuperar el certificat de l'entitat de certificació, o la llista de certificats revocats, per a no confiar en aquests certificats d'ara endavant. Baixar el certificat de l'entitat emissora permet confiar en els certificats que ha emès l'entitat. Pel que fa a la ruta de certificació de l'entitat, no cal instal·lar-la si s'ha sol·licitat i instal·lat un certificat que ha emès aquesta entitat, ja que s'instal·la automàticament.

Si triem baixar la llista de revocació de certificats, obtenim un arxiu amb extensió . *clr*. Per instal·lar la llista, seleccionem l'opció Instal·lar CRL del menú contextual que surt en fer clic amb el botó secundari del ratolí sobre l'arxiu que hem baixat. A continuació comença l'assistent d'importació de certificats que ja hem vist abans per a importar la llista de certificats revocats al magatzem de certificats que seleccionem.

4. IPsec

IPsec és una extensió del protocol IP que proporciona seguretat al protocol IP i als protocols de capes superiors. L'arquitectura d'IPsec està descrita en l'RFC2401. En els paràgrafs següents veurem una petita introducció a aquest protocol i després veurem com es configura de manera bàsica en entorns GNU/Linux i en entorns Windows. Per a donar seguretat al protocol IP, IPsec fa servir dos protocols: l'autenticació de capçalera o *authentication header* (AH) i la càrrega de seguretat encapsuladora o *encapsulating security payload* (ESP). La funció d'aquests dos protocols és assegurar l'autenticació, la integritat i la confidencialitat de la comunicació. Pot protegir el datagrama IP complet (mode túnel) o només els protocols de capes superiors (mode transport). En el mode túnel, el datagrama IP és "encapsulat" dins d'un altre datagrama IP, amb una capçalera IPsec segura, mentre que en el mode transport només afegeix la capçalera IPsec al datagrama original. Com es mostra en la taula següent:

Estructura dels paquets TCP/IP

Paquet original	IP	TCP	Dades			
Paquet en mode transport	IP	AH	TCP	Dades		
Paquet en mode túnel	IP	AH	IP	TCP	Dades	

Per a assegurar la confidencialitat, IPsec utilitza claus simètriques, però com hem vist abans, tenen un problema: com s'han de distribuir? Per a solucionar aquest problema, es va desenvolupar un protocol d'intercanvi de claus per Internet anomenat *protocol d'Internet d'intercanvi de claus* o *Internet key exchange* (IKE), basat en dues fases. En la primera fase s'autentiquen els participants de la comunicació i en la segona es negocien les associacions de seguretat i es trien les claus. A més, el protocol IKE utilitza claus dinàmiques.

Les claus dinàmiques són una mesura de seguretat afegida, ja que les claus simètriques són fàcils de desxifrar, només és una qüestió de temps. Com més temps fem servir aquesta clau, més possibilitats tenim que la desxifrin. Per tant, les claus dinàmiques es basen a anar canviant les claus simètriques que es fan servir de manera periòdica, amb negociació prèvia en els dos extrems de la comunicació. D'aquesta manera, les claus es van renovant i, fent servir poc temps cada clau simètrica, ens assegurem la confidencialitat de la comunicació.

Hem vist que en la segona fase del protocol IKE es negocia una "associació de seguretat". Una associació de seguretat o *security association* (SA) és on s'emmagatzemen tots els paràmetres que intervenen en una comunicació IPsec. Aquests paràmetres són els següents:

1) L'adreça IP origen i destinació de la capçalera IPsec.

2) El protocol IPsec utilitzat (AH o ESP).

3) Els algorismes de clau dinàmica que utilitza IPsec.

4) L'índex de paràmetre de seguretat o *security parameter index* (SPI). És un nombre de 32 bits que identifica l'associació de seguretat.

Aquestes associacions de seguretat s'emmagatzemen en bases de dades d'associacions de seguretat o *security association databases* (SAD). Algunes d'aquestes bases de dades permeten emmagatzemar més paràmetres de les associacions (mode túnel o transport, grandària de la finestra lliscant, temps de vida de la SA).

Una SA només protegeix un sentit de la comunicació; si volem protegir la comunicació de manera bidireccional necessitem dues associacions de seguretat. A més, les SA només especifiquen com se suposa que IPsec ha de protegir el trànsit, però no defineixen quin trànsit s'ha de protegir i quan s'ha de fer. Per a definir aquests casos es requereix informació addicional. Aquesta informació addicional s'emmagatzema en la política de seguretat o *security policy* (SP). La informació que s'emmagatzema en una SP és la següent:

1) Adreces origen i destinació dels paquets que es protegiran. Si fem servir el mode transport, són les mateixes adreces que les emmagatzemades en l'SA. Si fem servir el mode túnel, aquestes adreces pot ser que no coincideixin amb les emmagatzemades en l'SA.

2) Protocols i ports que s'han de protegir. Si la implementació d'IPsec que fem servir no és compatible amb la definició de protocols, s'ha de protegir tot el trànsit que circula entre les adreces IP origen i destinació.

3) L'associació de seguretat que es fa servir per a protegir els paquets. Les polítiques de seguretat SP s'emmagatzemen en bases de dades de polítiques de seguretat o *security policy databases* (SPD).

4.1. Instal·lació d'IPsec en el GNU/Linux

En aquesta secció explicarem com s'instal·la i es configura IPsec en un sistema operatiu basat en GNU/Linux. Hem d'instal·lar les eines d'espai d'usuari. Per fer-ho, executem l'ordre

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

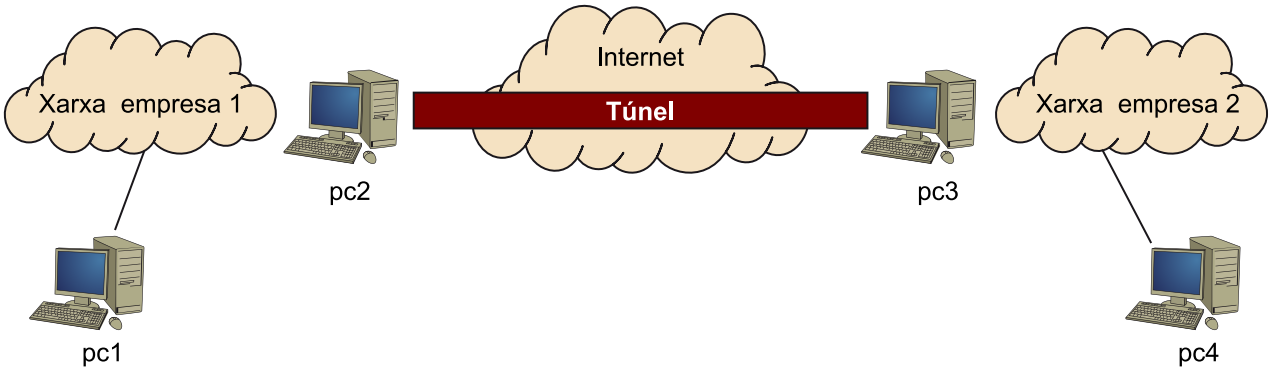
Una vegada acabada la instal·lació, estem en disposició de començar la configuració dels arxius.

4.1.1. Mode túnel

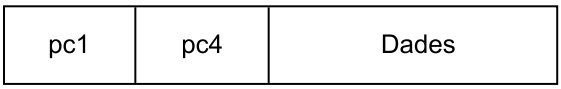
Abans de començar amb la configuració d'IPsec en mode túnel, explicarem una mica el concepte de túnel.

Imaginem-nos una empresa que té dues seus, una a Barcelona i l'altra a Madrid, però que només té un únic servidor per a les dues xarxes. Perquè els usuaris de les dues xarxes poguessin accedir a tots els serveis només hi havia una solució: una línia telefònica dedicada entre les dues seus (fet que implica unes despeses addicionals a l'empresa). La idea de túnel va aparèixer per a solucionar aquest problema.

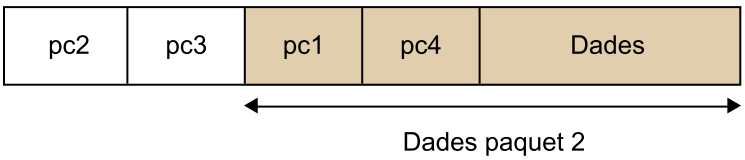
Per explicar què és un túnel ens basarem en l'esquema de xarxa següent:



Imaginem-nos que el pc1 es vol comunicar amb el pc4. Llavors genera un paquet IP en què l'origen és el pc1, i la destinació, el pc4. Del paquet resultant en diem *paquet1*, i és una cosa semblant a això:



Quan el *paquet1* arriba al pc2, aquest pc2 detecta que el pc4 és la *xarxa_empresa2*. Llavors encapsula el *paquet1* dins d'un altre paquet (que anomenem *paquet2*), en el qual el pc2 és l'origen i el pc3 és la destinació. L'aspecte del *paquet2* és una cosa semblant a això:



Quan el *paquet2* arriba al pc3, aquest pc3 detecta que es tracta d'un paquet del túnel. Desencapsula el *paquet2* (és a dir, recupera el paquet original, *paquet1*) i l'envia a la *xarxa_empresa2*, en què per funcionament IP arriba al pc4.

El funcionament del túnel és completament transparent als usuaris de les dues xarxes de l'empresa i per a qualsevol observador d'Internet, que només veu comunicació entre el pc2 i el pc3. El funcionament del túnel original viatja pla,

és a dir, sense xifrar. Utilitzant el protocol IPsec aconseguim que les dades es codifiquin, de manera que la comunicació entre el pc1 i el pc4 és confidencial i segura, ja que està xifrada.

Per configurar el mode túnel hem de configurar el fitxer `/etc/ipsec-tools.conf`. A continuació mostrem un fitxer `ipsec-tools.conf` adequat a l'esquema de xarxa que indica la figura, i que utilitza com a protocol segur ESP. Cal assenyalar que, perquè el túnel funcioni mitjançant IPsec, hem de configurar les dues màquines en els extrems del túnel.

```
#!/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 aquest arxiu de configuració veiem que no hi ha posades les adreces IP de les màquines encarregades de fer el túnel (`address_pc2` i `address_pc3`), ja que depenen de l'esquema de xarxa que tinguem nosaltres. Passa el mateix amb les adreces de les xarxes protegides en què s'apliquen les polítiques de seguretat (`net_company1` i `net_company2`).

4.1.2. Mode transport

Per a posar un exemple de configuració del protocol IPsec en mode transport, utilitzarem l'esquema de xarxa entre dos punts.

Igual que en el cas anterior, en mode túnel el fitxer de configuració que hem d'editar és `/etc/ipsec-tools.conf`. En aquest cas mostrarem l'exemple mitjançant l'ús del protocol 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 adreça_pc2 adreça_pc1 any -P in ipsec
ah/transport//require;
```

Aquest arxiu configura IPsec en el pc1; si volem configurar el pc2 hem d'intercanviar `-P out` per `-P in`, i viceversa. En segon lloc, i a manera d'exemple, podem fer servir les claus que hi ha en la definició de l'associació de seguretat (SA) del protocol AH, però convé crear les nostres pròpies claus. Una vegada tenim configurats els dos extrems, l'engeguem mitjançant l'ordre:

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

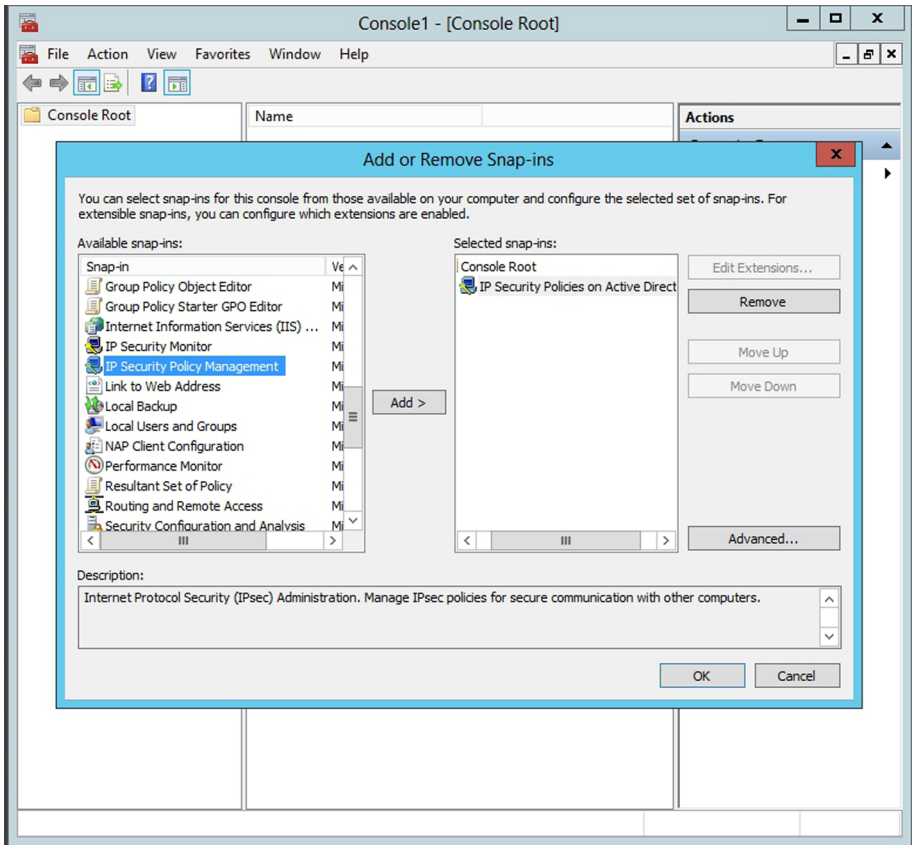
Per comprovar el funcionament d'IPsec podem mostrar les diferents bases de dades (SAD i SPD) mitjançant les ordres següents:

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

4.2. Eines de control d'IPsec en el Windows Server 2012

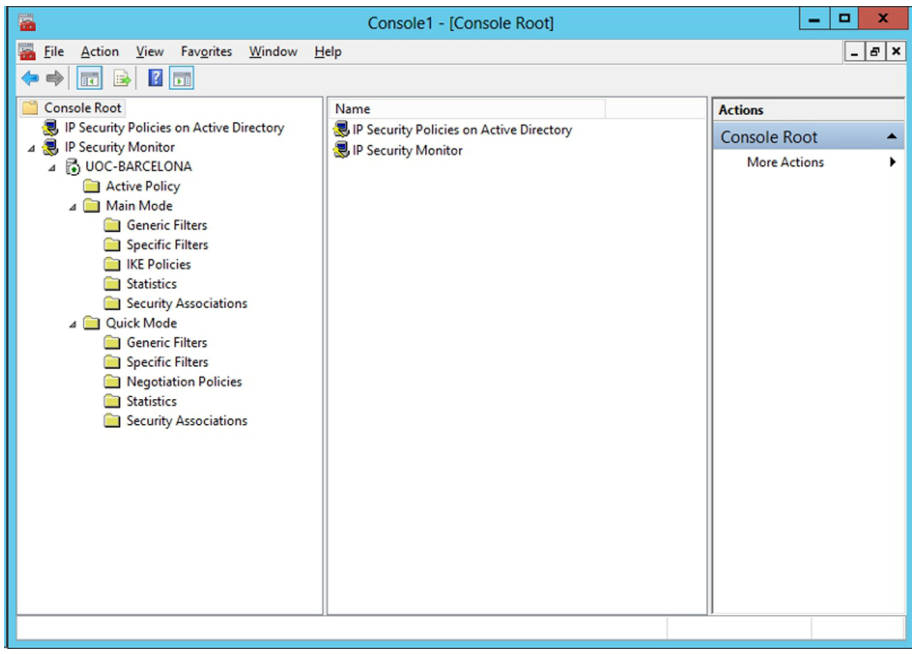
Per a configurar IPsec utilitzem el complement Directives de seguretat local de la consola d'administració. Per a obrir aquest complement, obrim el PowerShell i hi escrivim *mmc.exe*. Per afegir el complement, seleccionem l'opció Agregar o treure complement del menú Acció. En la nova finestra fem clic sobre el botó Agregar i en la llista d'elements seleccionem Administració de les directives de seguretat d'IP (figura següent). A continuació seleccionem l'equip sobre el qual volem administrar les directives IPsec, que podria ser sobre el sistema mateix en local o sobre el directori actiu. Una vegada fet això, s'agrega el complement a l'arbre de la consola d'administració. Aquest complement ens permet utilitzar polítiques d'IPsec predefinides o definir-ne de noves, com veurem a continuació.

Instal·lació d'IPSec



Una altra eina que ens és útil per a comprovar la seguretat IP del servidor i dels equips en general del directori actiu és el monitor de seguretat IP, que es pot afegir com el complement Monitor de seguretat IP a la consola que acabem de crear; per tant, tindrem en la consola, que s'haurà de guardar en el disc o es perdrà aquesta configuració, les polítiques de seguretat del directori actiu, o la màquina local, i el monitor de seguretat, tal com mostra la figura següent.

Monitor de seguretat i polítiques de seguretat en la consola



4.3. Utilització de directives IPsec predefinides

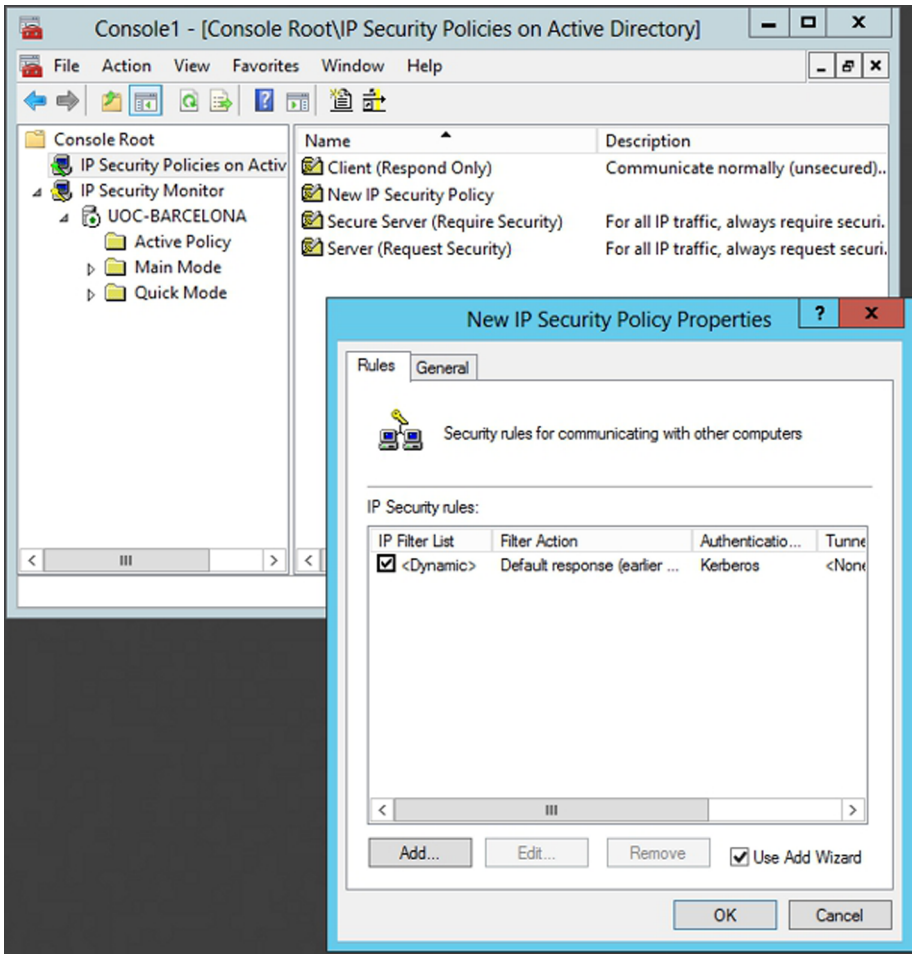
A la part dreta del complement de les polítiques d'IPsec veiem tres directives predefinides: client (només respondre), servidor (demanar seguretat), servidor segur (requereix seguretat). Aquestes tres directives ja estan activades, i per tant es poden desactivar si és necessari amb les accions associades a cada directiva.

4.4. Utilització de directives IPsec personalitzades

Per crear una nova directiva IPsec personalitzada, seleccionem l'opció Crear directiva de seguretat IP del menú Acció, i ens surt l'assistent corresponent. En la primera pantalla assignem un nom a la nova directiva. En la segona hem de decidir si activem la regla de resposta predeterminada en cas que no es pugui aplicar cap altra regla.

En la pantalla següent seleccionem el tipus d'autenticació utilitzat en la regla de resposta predeterminada (si seleccionem l'opció de la finestra anterior). Es podria fer si en el servidor es disposa dels certificats que s'han mostrat amb anterioritat.

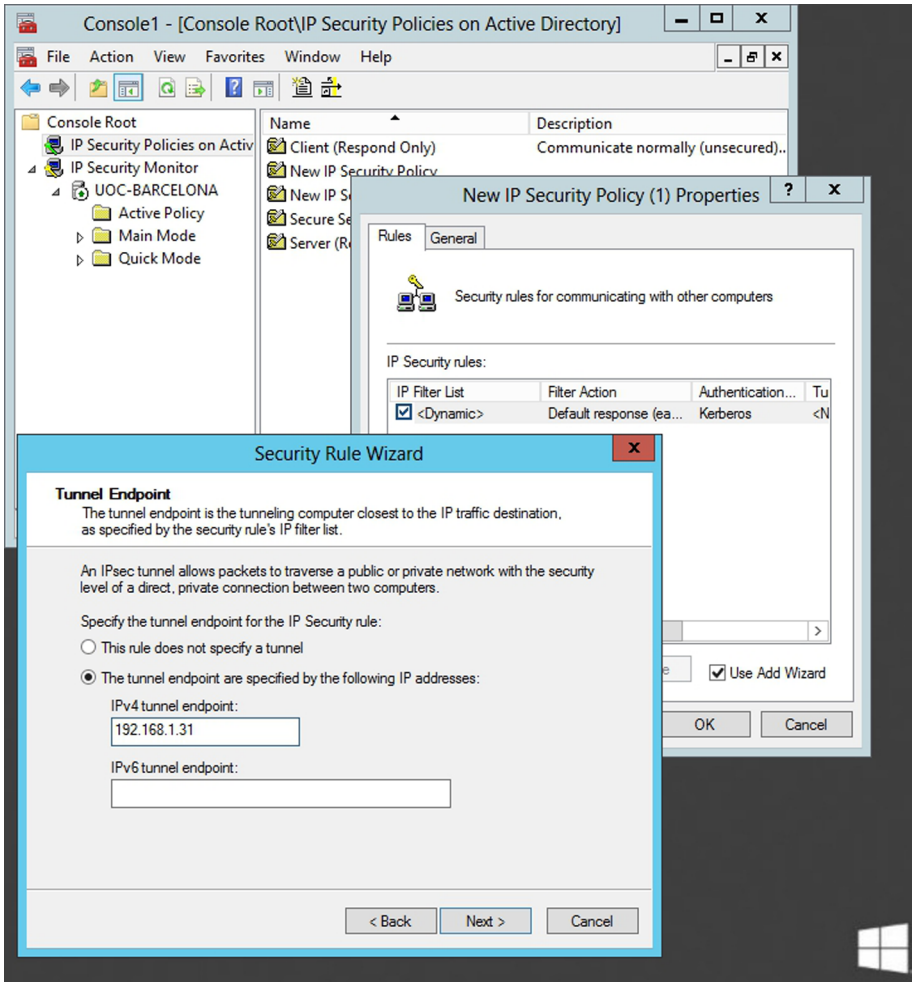
Nova directriu de seguretat



S'acaba el procés de crear la nova directiva. Per a modificar-ne les propietats, tot seguit es pot seleccionar l'opció Modificar les propietats, que obre la finestra de propietats de la directiva. En aquesta finestra veiem les regles de la directiva. En principi només hi ha configurada la regla predeterminada, però hi podem afegir més regles mitjançant l'opció Agregar. En agregar una regla nova dins la directiva surt l'assistent corresponent, que ens va guiant en la instal·lació fins a aconseguir el que es vol. Aquesta finestra de configuració del túnel permet, per exemple, especificar la IP de l'altre extrem d'una connexió VPN, tal com mostra la figura següent.

En la pantalla següent especifiquem el tipus de xarxa a la qual és aplicable aquesta regla: a tota la xarxa, a l'àrea local o a l'accés remot cap a aquest servidor. A continuació, triem quin tipus de trànsit és el que es controlarà, i podem especificar amb una nova regla adreces d'IP específiques tant d'entrada com de sortida, els protocols, etc. per acabar marcant si es permet el trànsit o es bloqueja, depenent de com s'hagi pensat d'aplicar la regla que s'està configurant. Es podria bloquejar el trànsit en tots els ports i adreces externes a la vegada.

Assignació IP de la VPN en la directiva de seguretat



5. Xarxes privades virtuals

Una xarxa privada virtual o *virtual private network* (VPN) és un túnel d'informació privada que porta dades d'un extrem a l'altre i ho fa utilitzant una xarxa pública (com, per exemple, Internet), sense que la comunicació d'extrem a extrem s'adoni que utilitza una xarxa pública i sense que els nodes intermedis de la xarxa pública s'adonin que els travessa un túnel d'informació privada. El gran avantatge de les VPN és que permeten construir xarxes privades d'una manera molt més barata que no pas implantant un enllaç dedicat entre els diferents extrems de la comunicació privada.

La implantació de les VPN és una tasca complexa, ja que hi ha molts tipus de solucions VPN. A més, cada solució es pot dur a terme de diverses maneres i cadascuna d'aquestes maneres pot utilitzar, al seu torn, més d'un protocol de comunicacions. En aquesta secció veurem com s'han d'instal·lar i configurar VPN de diferents maneres.

5.1. GNU/Linux

5.1.1. *Secure shell*

Una primera manera molt senzilla de crear VPN és utilitzant el protocol *secure shell* (SSH). Aquest mètode substitueix les aplicacions `telnet` i `rlogin` amb una aplicació similar (basada en un *shell*) però que utilitza túnels xifrats per a la comunicació. A més, amb aquest protocol, podem fer transferències de fitxers de manera segura (*secure file transfer protocol* o SFTP), cosa que permet substituir les transferències de fitxers que fan servir canals no xifrats (*file transfer protocol* o FTP). Un altre avantatge molt important d'aquest mètode de creació de VPN és que l'SSH ofereix més d'un mètode d'autenticació, entre els quals hi ha el nom d'usuari amb la contrasenya corresponent i l'autenticació basada en certificats.

En general, els desavantatges d'SSH són, d'una banda, la instal·lació, ja que, com en la majoria de les solucions VPN, el client s'ha d'instal·lar una aplicació per a fer servir la VPN, i d'altra banda, el protocol en si. L'SSH és un protocol que ja fa anys que és actiu; això ha repercutit en el fet que sigui molt conegut i estudiat, de manera que s'hi han trobat vulnerabilitats, la majoria de les quals són en el que s'anomena SSH1. Per a solucionar aquests problemes va sortir l'anomenat SSH2, que ofereix una protecció del túnel xifrat molt millor que en el cas de l'SSH1. Per això ens hem d'assegurar que en la nostra màquina instal·lem i configurem només l'SSH2.

Fins ara hem vist el protocol SSH en la forma de funcionament habitual, però amb l'SSH també tenim la capacitat de crear túnels xifrats. Els túnels SSH els podem crear utilitzant la funcionalitat de redirecció de ports o *port forwarding*, el funcionament de la qual és el següent:

1) El servidor ofereix un servei (insegur) pel seu port habitual.

2) Mitjançant l'adreçament de ports adrecem el servei a un túnel xifrat.

3) El client té instal·lat un client d'adreçament de ports.

4) El client configura el servei (insegur) per fer servir el port local on comença el túnel xifrat en lloc del port remot on es dóna el servei insegur.

5) El client envia una petició de servei (insegur).

6) Aquesta petició entra al túnel xifrat.

7) Arriba a l'altre extrem del túnel on l'adreçament de ports el desxifra i el lliura al servei en el seu port estàndard.

Mitjançant la utilització d'aquesta funcionalitat podem adreçar ports locals perquè facin servir un túnel xifrat. D'aquesta manera podem oferir serveis, en principi insegurs, als nostres usuaris d'una manera segura. No totes les comunicacions fan servir el mateix túnel, sinó que es crea un túnel xifrat per cada port que volem adreçar. Les limitacions de l'adreçament de ports són la capacitat de túnels que pugui adreçar, i que només podem adreçar els protocols que fan servir TCP.

Aquest mètode de generació de VPN és molt recomanable, ja que podem crear VPN d'una manera molt ràpida i a un cost molt baix. El gran problema, però, és que si treballem amb adreçament de ports els clients (els usuaris) han de configurar la seva màquina, i això implica un nivell de coneixement superior al de la majoria dels usuaris.

La majoria de les distribucions GNU/Linux ja vénen amb els paquets de l'SSH instal·lats. Però si s'ha d'instal·lar ho hem de fer mitjançant l'ordre:

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

La configuració del servidor d'aquesta aplicació és a l'arxiu `/etc/ssh/sshd_config`. Les opcions de configuració més destacades del fitxer de configuració `sshd_config` són les següents:

- `AllowTCPForwarding`: aquesta opció està habilitada per defecte i permet fer l'adreçament de ports comentat en aquesta secció.

- `AuthorizeKeysFiles`: indica el directori on hi ha emmagatzemades les claus públiques que es fan servir per a autenticar l'accés dels usuaris.

- `DenyUsers`: llista d'usuaris que, malgrat que tenen compte a la màquina, no hi podran accedir per SSH.

- `ListenAddress`: especifica en quina adreça local hi ha el servidor SSHD.

- `PermitEmptyPasswords`: mitjançant aquesta opció indiquem si permetem que els usuaris tinguin el camp de la contrasenya buit. És molt recomanable que aquesta opció estigui configurada sempre perquè no permeti contrasenyes buides.

- `PermitRootLogin`: aquesta opció ens indica si permetem a l'usuari arrel entrar per SSH o no. Això depèn del servei que donem i de la seguretat de xarxa que tinguem. Per exemple, si tenim l'SSH configurat per a fer SFTP i permetem als nostres usuaris entrar per SFTP des de qualsevol lloc d'Internet, és recomanable no permetre l'accés de *root* per SSH. Ara bé, si utilitzem l'SSH només per a habilitar consoles interactives en l'entorn de l'empresa, sí que podem permetre l'accés de *root* per SSH.

- `Port`: ens indica en quin port TCP hi ha el servidor SSHD. Per defecte, és el port 22. És recomanable canviar el port per un altre que no estigui en ús. Si és un número alt, millor.

- `Protocol`: ens indica amb quina versió de l'SSH és compatible el servidor. A causa de les vulnerabilitats conegudes en l'SSH1, és molt recomanable que només fem servir l'SSH2.

- `Subsystem`: configura en subsistema extern. Si hi posem l'opció `sftp-server`, configurem un servidor d'SFTP en el nostre servidor.

5.1.2. *Secure socket layer*

Sens dubte, el mètode de generació de VPN més estès és el mètode basat en Web + SSL (protecció de capa de connexió segura o *secure socket layer*). Tot i que la majoria de la gent l'associa al Web, SSL també pot proporcionar xifratge a un munt de protocols (POP3, IMAP, LDAP, SMTP, NNTP, etc.).

Aquest xifratge dels diferents protocols és el mètode estàndard de connexió SSL, però, igual que en la secció anterior, SSL també és compatible amb solucions basades en túnels.

El funcionament del servidor d'SSL està basat en els certificats digitals. Hem de fer una petició de certificat a una CA, com ja s'ha mostrat, i, una vegada n'obtenim la resposta amb el certificat de la màquina, l'instal·lem (cada pro-

tocol l'instal·la d'una manera concreta, i quan expliquem els serveis veurem com es configuren els serveis SSL). Així ja tenim el servidor que ofereix el servei de manera segura.

En la part del client també es configura de manera molt simple; tan sols hem d'habilitar SSL (en el cas dels navegadors web, ja el tenen habilitat per defecte). Un exemple d'aplicació en la qual hem d'habilitar l'SSL és en la majoria dels clients de correu electrònic. En les opcions de configuració dels servidors hi ha (normalment) una pestanya o una casella de selecció on podem habilitar connexions SSL. Hem de tenir present que l'ús de serveis amb SSL implica un port d'entrada diferent del correu electrònic normal. Aquesta consideració l'hem de tenir present, si hi ha un tallafoc (*firewall*), per obrir els ports necessaris per a fer la comunicació.

Per a crear túnels amb SSL, en entorns GNU/Linux, hem de fer servir l'aplicació `stunnel`. Aquesta aplicació crea túnels de manera semblant a l'adreçament de ports que utilitza SSH. Per tant, caldrà instal·lar aquesta aplicació amb l'ordre `apt-get`.

L'avantatge d'SSL és la senzillesa de la configuració (amb prou feines cal res més que un certificat digital i un parell de modificacions en el fitxer de configuració del servei). El desavantatge, però, és la lentitud a l'hora d'obtenir el certificat: depenent de la CA que fem servir, l'obtenció del certificat pot arribar a trigar més d'una setmana.

SSL proporciona una manera molt senzilla de donar als clients les funcionalitats d'una VPN, per a certes aplicacions i protocols sense haver de dur a terme cap instal·lació i amb poques modificacions en les aplicacions dels clients.

5.1.3. IPsec

En la secció anterior ja hem parlat del funcionament d'IPsec. Aquest protocol, però, també es fa servir per a crear VPN. Tot i que SSH, SSL o IPsec proporcionen unes funcionalitats de xifratge semblants, aquests mètodes són diferents des d'un punt de vista funcional.

Mentre SSH o SSL creen un túnel nou per a cada aplicació que volem que funcioni de manera segura, IPsec només crea un túnel i hi fa passar tota la informació. Des d'un punt de vista de seguretat perimetral (ús de tallafoc) la implantació d'una VPN amb IPsec en lloc d'SSH o SSL té molts avantatges, ja que per començar només hem d'obrir el tallafoc a un únic port.

5.1.4. Altres sistemes

Com hem dit al principi d'aquesta secció, la construcció de VPN es pot fer mitjançant diferents protocols. Al llarg d'aquesta secció hem mostrat alguna de les maneres de construir una VPN, però n'hi ha moltes més.

Hi ha algunes d'aquestes maneres que són propietat d'una empresa i n'hi ha d'altres que són de distribució lliure. Algunes de les altres maneres utilitzades per a construir VPN són aquestes:

1) PPTP és un protocol propietat de Microsoft.

2) FWZ és un protocol propietat de Check Point Software Technologies usat en els seus productes Firewall -1.

3) FreeS/Wan és una implementació d'IPsec + IKE per a Linux.

4) OpenVPN és una implementació d'un tallafoc amb *iptables* + túnels SSL.

5) IP Masquerade + IPforward.

Aquesta llista la podem fer molt llarga, ja que actualment en el mercat hi ha moltes aplicacions que fan VPN. És feina nostra avaluar aquestes eines i instal·lar la que s'adapti més a la configuració o a les necessitats de la nostra empresa.

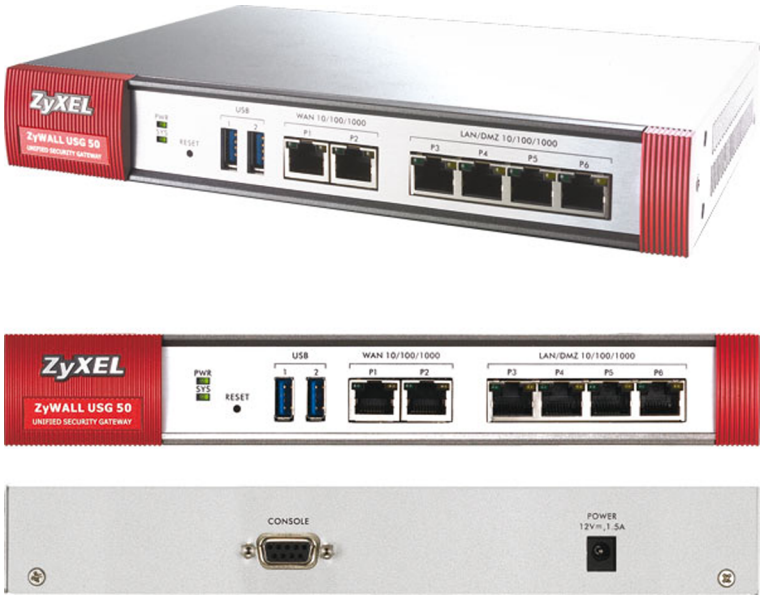
5.2. Windows Server 2012

5.2.1. Configuració del servidor

El primer pas per a configurar una xarxa privada virtual és configurar el servidor a què es vol accedir perquè permeti connexions entrants, és a dir, des de fora fins i tot de la xarxa interna. Per a fer-ho, caldrà instal·lar un nou paper en el sistema, en aquest cas el de serveis d'accés i directives de xarxa, que permet fer connexions entrants remotes al servidor i a més crea les xarxes privades virtuals implementades directament sobre el servidor.

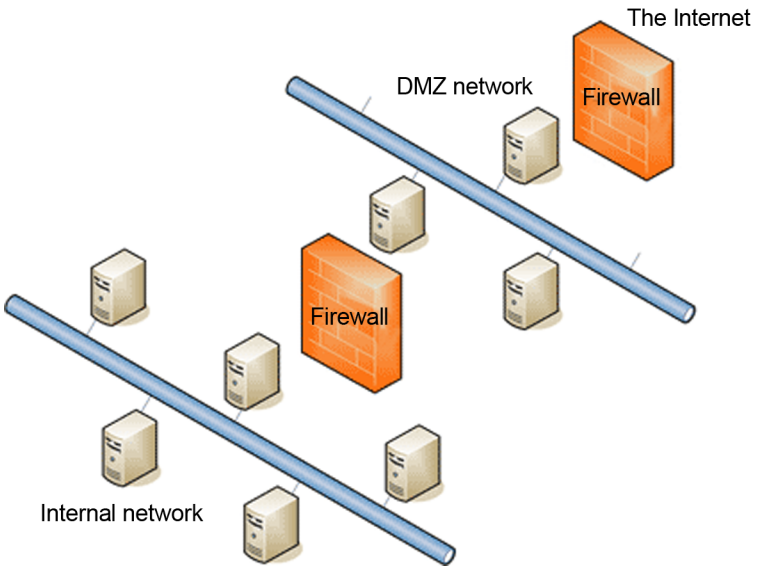
Està clar que si es disposa d'un tallafoc que permeti crear aquestes xarxes virtuals el sistema serà molt més segur, ja que s'encarregarà el tallafoc mateix de tota la gestió i per tant no serà accessible el sistema operatiu des de fora de la institució. La majoria de tallafocs actuals, com per exemple el que mostra la figura següent, ja disposen d'aquesta configuració i només cal activar-la i configurar-la correctament.

Tallafoc Zyxel, Zywall USG 50



En aquests tallafocs tenim una entrada que és la que es connecta directament a la xarxa Internet i una altra entrada que es connecta a la xarxa interna, on estan els servidors o la DMZ (figura següent), que separarà amb un altre tallafoc el servidor que pot ser públic de la part que ha de ser completament privada de l'organització. Per tant, amb aquests aparells, les xarxes de les empreses o institucions són molt més segures, ja que si no es disposa i es connecta directament la xarxa local interna a l'encaminador (*router*) i a més fem que el servidor mateix gestioni les xarxes privades, estem fent que el servidor es connecti directament a Internet i a més tingui obert com a mínim el port per a escoltar les VPN, i possiblement també els ports d'una pàgina web, del correu, etc.

DMZ



La configuració de cada un dels tallafocs és completament diferent, però normalment aquests aparells permeten crear túnels permanents entre dos equips que tinguin les mateixes característiques. Això permetrà crear túnels xifrats

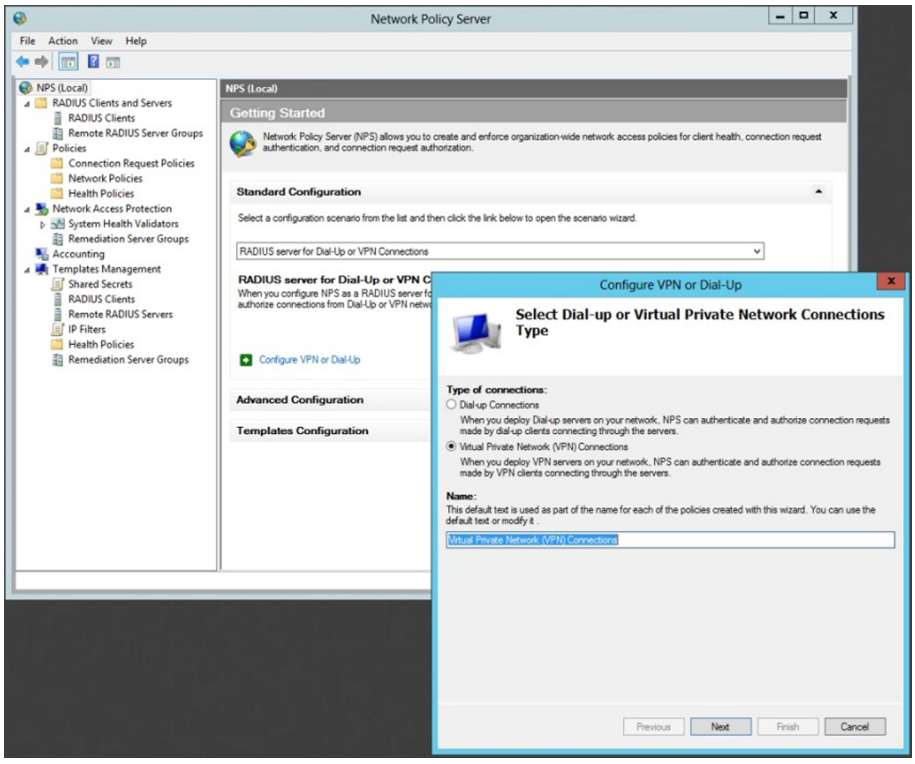
entre dos seus, per exemple, de tal manera que la comunicació entre dues ADSL normals estigui xifrada completament i no es pugui escoltar la xarxa pública entre aquests punts, a més de crear una única xarxa local entre tots els punts ubicats a cada costat de les dues subxarxes, per a crear una única xarxa local.

Però en el cas de no disposar d'aquest aparell, sempre es pot configurar el sistema operatiu per a crear una xarxa virtual entre els equips informàtics i el servidor on estigui instal·lat el paper de serveis d'accés i directives de xarxa.

A més de crear les VPN, aquest paper ens permetrà crear polítiques de connexió dels equips client a part de la "salut" que tingui cada ordinador, això és, que si es configura de manera que tots els ordinadors que es connectin a la xarxa local hagin de tenir instal·lat un sistema operatiu, no deixarà connectar-se aquells que no en disposin d'un ja instal·lat. Es podria denegar l'accés als servidors, a la xarxa o crear una subxarxa on únicament tinguessin accés a Internet, però no a la xarxa local. Pensem en una empresa en la qual els proveïdors vénen a oferir els productes i disposen de portàtils que necessiten accedir a Internet o a alguna de les parts de la pàgina web o al catàleg de productes propis.

En el moment de la instal·lació del paper demanarà quins serveis es volen instal·lar; per defecte s'instal·la el bàsic, però es poden instal·lar també el registrador de "salut", si es vol fer servir aquesta característica concreta i un mòdul per a poder integrar el procés d'autenticació de Microsoft (NAP) amb el que disposa l'empresa CISCO.

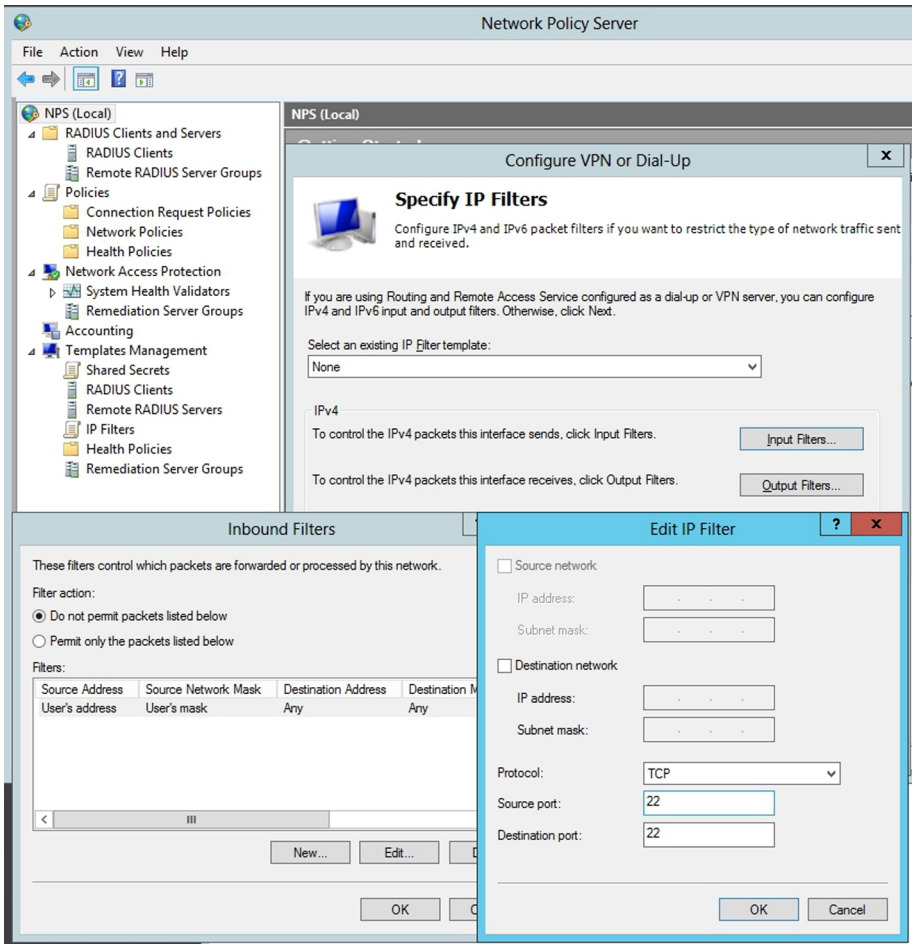
Configuració de la VPN



Un cop instal·lat el paper cal configurar el servidor perquè accepti les peticions de xarxes privades, i això ho podem aconseguir en l'enllaç de configuració estàndard (figura següent), on es pot dir que es vol que actuï amb xarxes VPN. A partir d'aquí cal configurar el servidor RADIUS per als usuaris que es vulguin tenir connectats, si és que es vol fer servir aquesta característica o directament l'autenticació del servidor mateix. Cal configurar els protocols d'autenticació que es volen tenir en el servidor, i depenent de quins equips es connectin després a la VPN poden o no tenir uns protocols determinats. A més es pot, a continuació, decidir quins usuaris del sistema, a partir d'assignar un cert grup, poden tenir accés a aquesta VPN, ja que possiblement no tots els empleats han de tenir accés a aquesta característica. Per tant, es crearà un grup en el directori actiu que serà el que es farà servir per a incloure totes aquelles persones que hagin de tenir accés a les VPN del servidor, com per exemple el grup `gVPN`.

A partir d'aquí es poden incloure configuracions per a permetre o no certes IP internes o externes, protocols, ports, etc., de manera que la connexió VPN serà molt més segura si només es permet l'accés a un determinat servidor on estigui la informació que es vol oferir, o el protocol que es necessita, com per exemple l'FTP, el de compartició de fitxers, etc.

Configuració dels ports, IP, protocols, etc. permesos de la VPN

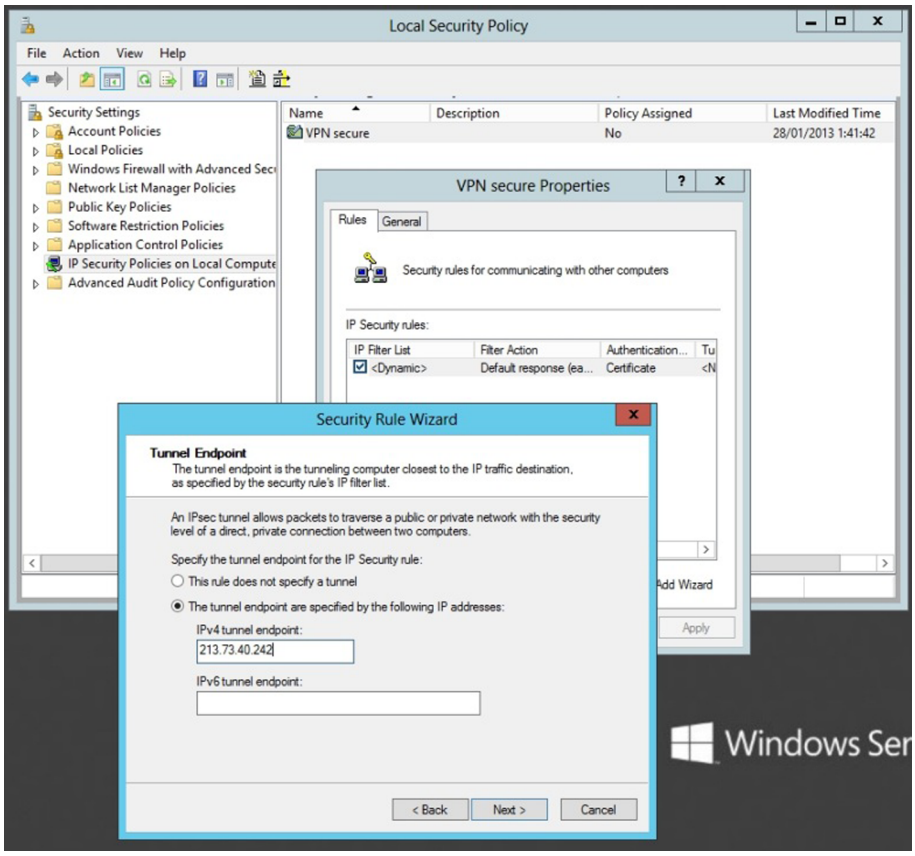


Podem canviar els protocols d'autenticació que té per defecte un cop instal·lat el paper de la connexió remota, directament en les propietats dels papers que s'acaben d'instal·lar.

Pel que fa a la seguretat de les VPN, podem definir una directiva de seguretat IP (IPsec) que permeti xifrar les dades de la connexió i que obligui els usuaris a autenticar-se amb un certificat digital expedit per una entitat de certificació pròpia. Per fer-ho, obrim l'eina de Directiva de seguretat local del tauler de control, Eines administratives, i en el menú contextual de l'element Directives de seguretat IP en equip local, seleccionem l'opció Crear directiva de seguretat IP. Després de posar un nom a la nova directiva, desseleccionem l'opció Activar la regla de resposta predeterminada, En la pantalla de Tipus de xarxa seleccionem Accés remot i en la finestra de Mètode d'autenticació seleccionem l'opció Useu un certificat d'aquesta autoritat de certificats (CA), i premem el botó Examinar... per seleccionar el certificat de la nostra entitat de certificació o el de l'entitat en què confiem, i s'acaba el procés de crear la directiva.

Després es mostren les propietats de la directiva que s'ha creat amb el botó dret del ratolí. En la llista de regles IP fem clic sobre el botó Agregar..., i ens surt l'assistent corresponent. En la pantalla de Punt final del túnel, en el cas que sigui una adreça IP fixa es podrà bloquejar perquè només es pugui connectar des d'aquesta IP (figura següent), se selecciona l'opció L'extrem del túnel s'especifica mitjançant l'adreça IP següent, i hi escrivim la IP de la VPN. Això és molt útil, ja que deixem fixes les dues parts del túnel VPN, i fem més difícil la intrusió en aquesta VPN de terceres persones. En el cas que sigui una IP variable aquesta no es podrà fixar i s'hauran d'assumir uns riscos, que amb els certificats minimitzarem una mica, tot i que no del tot.

Configuració del túnel VPN



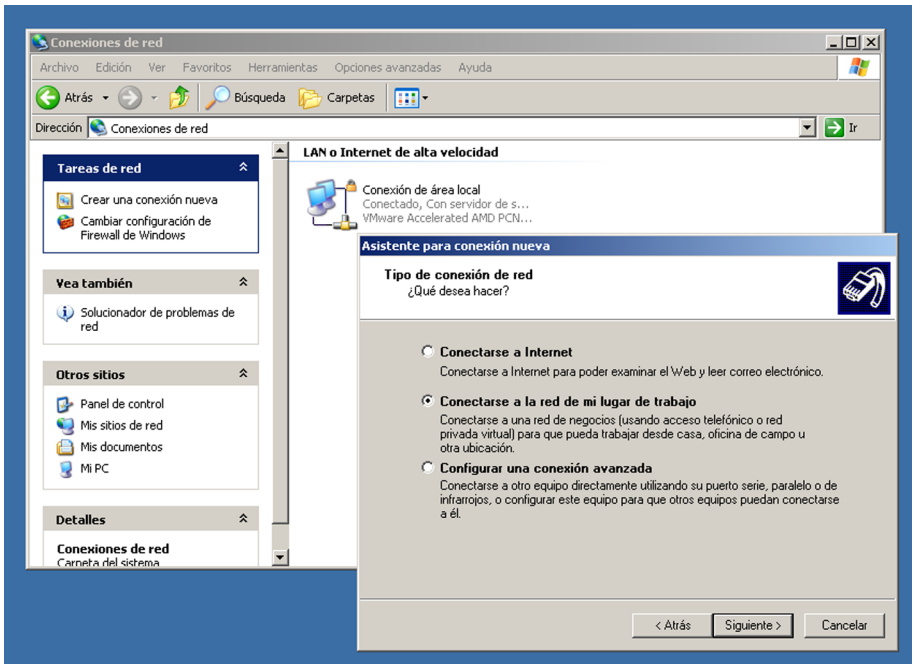
Una vegada creada la directiva IP l'hem d'assignar amb l'opció Assignar del menú contextual corresponent en la llista de directives IP. A partir d'aquest moment, els usuaris que volen accedir via VPN han de tenir un certificat emès per la nostra entitat emissora de certificats. Aquest certificat pot estar inclòs en una targeta intel·ligent per a augmentar la seguretat. Una altra acció que podem dur a terme per augmentar la seguretat d'una VPN és configurar un tallafoc per a admetre solament accés a les connexions de les IP dels usuaris de la VPN, si bé això restringeix que els usuaris puguin accedir des de diferents llocs o que utilitzin equips amb IP dinàmica.

Hi ha altres mecanismes o eines més avançades per a millorar la seguretat de VPN a més d'altres tipus de connexions, com per exemple el Microsoft Internet Security And Acceleration Server (ISA Server), també conegut com a Microsoft Forefront Threat Management Gateway, que, a part de facilitar la configuració i protecció de xarxes VPN, fa tasques de tallafoc, publicació web segura, autenticació segura, FTP segur, monitoratge, creació d'informes, etc.

5.2.2. Configuració del client

Una vegada configurat el servidor de la xarxa VPN, configurem els clients des dels quals volem accedir al servidor. Per a fer-ho, des dels clients, fem servir la utilitat de creació de connexions, dins de la carpeta Connexions de xarxa i d'accés telefònic del tauler de control (figura següent).

Creació de la VPN en el client Windows XP



En aquest cas seleccionem l'opció Connectar a una altra xarxa privada mitjançant Internet. A continuació l'assistent ens demana el nom del servidor o l'adreça IP que té. Finalment, abans d'acabar, l'assistent ens demana si la connexió és disponible per a tots els usuaris de l'equip o només per al compte d'usuari actual.

Abans de connectar amb la nova connexió, s'ha de configurar: anem a la finestra de propietats, seleccionem el protocol TCP/IP en la pestanya de Funcions de xarxa i fem clic sobre Propietats. En la finestra de propietats seleccionem l'opció d'obtenir una adreça IP automàticament (tret que no hàgim configurat el servidor per fer-ho), i modifiquem les adreces de DNS perquè siguin les mateixes especificades en el servidor. Premem Avançades, i en la finestra que surt desseleccionem l'opció Usar la porta d'enllaç predeterminada a la xarxa remota. Quan ens intentem connectar amb la nova connexió ens surt una pantalla d'identificació en què hem de proporcionar el nostre nom d'usuari i contrasenya. Quan un client es connecta al servidor de VPN, s'encén la icona de connexions entrants del servidor i indica els usuaris connectats en aquell moment.

6. Monitoratge de la xarxa

El monitoratge de la xarxa és un factor important en la seguretat de la nostra empresa. Mitjançant el monitoratge podem saber quin és el comportament (els hàbits de treball) de la nostra empresa, quina és la quantitat d'amplada de banda que consumim a cada moment, etc.

Gairebé tots els sistemes operatius inclouen uns programes molt senzills de monitoratge. Aquests programes només permeten monitorar diferents paràmetres de l'ordinador que els executa (la xarxa, la memòria o l'ús de CPU). A més, totes aquestes aplicacions són molt senzilles, ja que només permeten el monitoratge de qualsevol d'aquests programes, sempre que el programa estigui en execució, i d'altra banda, només ens permeten visionar el que està passant i un històric de poques hores.

Hem d'anar molt amb compte quan utilitzem eines de monitoratge de la xarxa. Hi ha una llei de privadesa de dades que protegeix el trànsit per la xarxa. Si la finalitat del monitoratge de la xarxa és treure estadístiques, podem capturar paquets IP per analitzar-los sempre que:

1) No puguem capturar el contingut del paquet (de fet, no el podem ni veure mentre circula per la xarxa).

2) Els resultats estiguin dissociats, és a dir, hem d'emmascarar les adreces IP, ja sigui treballant en subxarxes, xarxes o superiors (sistemes autònoms).

6.1. Monitoratge en el GNU/Linux

En aquesta secció comentarem una aplicació de monitoratge de la xarxa que té llicència GNU i que permet fer un monitoratge molt complet. Aquesta aplicació s'anomena Multi Router Traffic Grapher (MRTG) i genera pàgines de llenguatge d'etiquetatge d'hipertext o *hypertext markup language* (HTML) que contenen imatges en format gràfic de xarxa portàtil o *portable network graphics* (PNG) que ens proporcionen una representació visual molt completa del trànsit de xarxa.

L'aplicació d'MRTG consisteix en una sèrie de *scripts* escrits en llenguatge Perl que fan servir el protocol simple d'administració de xarxes o *simple network management protocol* (SNMP) per a llegir els comptadors de trànsit que hi ha en els commutadors (*switches*) o els encaminadors, i mitjançant senzills i ràpids programes escrits en llenguatge de programació C crea imatges en format PNG que representen l'estat del trànsit de la nostra xarxa. Aquests gràfics els insereix

en una pàgina web que podem consultar amb qualsevol navegador. Hem de fer notar que per veure els resultats hem de tenir instal·lat un servidor web en la màquina que tingui instal·lat l'MRTG.

Aquesta aplicació, a més d'oferir-nos una visió detallada del trànsit de la xarxa local, també crea representacions de trànsit dels últims set dies, les últimes cinc setmanes i els últims dotze mesos. Això és possible perquè l'MRTG desa en uns fitxers de registre (*log*) tota la informació que ha anat demanant als equips de la xarxa. Aquests fitxers tenen la particularitat que no augmenten la mida al llarg del temps, cosa que evita que s'ompli el disc i per tant es pugui aturar el servidor. El monitoratge de la xarxa no és l'única aplicació que podem obtenir d'aquest programa. Com que l'MRTG fa servir SNMP, qualsevol dada que siguem capaços d'obtenir mitjançant aquest protocol és susceptible de ser monitorada. Actualment, la majoria dels administradors que utilitzen aquest programa supervisen altres paràmetres a part del trànsit de xarxa (la càrrega del sistema, dels discos, etc.).

Abans d'instal·lar aquesta aplicació ens hem d'assegurar que tenim instal·lats els requisits d'aquesta eina. Si necessitem més informació que la detallada en aquestes pàgines, hem de consultar el manual d'instal·lació de l'MRTG [Oet04].

Per a instal·lar l'MRTG necessitem el següent:

1) Un compilador de C; el més comú és el GCC (http://gcc.gnu.org/).
2) Una versió de Perl actualitzada (http://www.perl.com/).
3) Les biblioteques *zlib* (http://www.zlib.net).
4) Les biblioteques *libpng* (http://www.libpng.org/pub/png/).
5) Les biblioteques gràfiques *gd* (http://www.boutell.com/gd/).

Com s'ha indicat anteriorment, només cal fer servir l'ordre

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

per a saber si tenim aquestes eines instal·lades. En el cas que no ho estiguin s'hauran d'instal·lar amb l'aplicació `apt-get`. La resta de biblioteques necessàries s'han de baixar de la pàgina web i instal·lar-les manualment, normalment fent els passos següents:

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

Tot i que les pàgines d'instal·lació d'aquesta aplicació n'expliquen la instal·lació mitjançant el procés de compilació de les fonts dels diferents requisits, nosaltres –com que fem servir una distribució de GNU/Linux basada en una Debian– podem instal·lar aquesta aplicació amb l'ordre següent:

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

Durant la instal·lació ens adverteix que si el fitxer de configuració és accessible a altres usuaris que no siguin l'usuari *root*, hi pot haver un problema de seguretat, ja que en aquest fitxer hi ha noms de màquines de la xarxa que haurien de quedar ocultes a persones alienes a la companyia. Únicament fent que el propietari i grup sigui un únic usuari o el *root* ja no tindrem aquest problema.

Una vegada tenim instal·lada aquesta aplicació, ja la podem configurar. Per a fer-ho, és molt important que coneguem l'entorn de xarxa en què treballem i que siguem administradors d'aquesta xarxa. Això es deu al fet que, com que fem servir el protocol SNMP, necessitem les contrasenyes (*community*) d'accés mitjançant aquest protocol que hi ha definides en els diferents equips de xarxa (commutadors, encaminadors, etc.). L'administració d'aquests equips és a càrrec de l'administrador de xarxa.

Per a configurar l'MRTG, fem servir una eina de configuració que ve amb la mateixa aplicació i que es diu `cfgmaker`. Podem veure els paràmetres en el manual, però un possible exemple d'ús d'aquesta eina és aquest:

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

Les opcions més destacades del `cfgmaker` són les següents:

1) `Ifref`: com referenciem la interfície. Els valors acceptats són número, IP, Ethernet, descripció, nom i tipus.

2) `Ifdesc`: com descrivim la interfície. Els valors acceptats són els mateixos que en el cas del paràmetre `ifref`.

3) `Output`: hem d'indicar el fitxer on es guarda la configuració.

4) `Dns-domain`: indiquem el domini a què pertanyen les interfícies.

Una vegada hem executat el `cfgmaker`, hem d'editar el fitxer que acabem de crear, en el cas de l'exemple, `/etc/mrtg.cfg`, i hem de modificar les línies següents:

1) `Workdir`: especifiquem el directori de treball de l'MRTG.
2) `Htmldir`: especifiquem en quin directori es posen els fitxers HTML.
3) `Imagedir`: especifiquem en quin directori s'emmagatzemen les imatges.
4) `Logdir`: especifiquem en quin directori es guarden els registres.

5) `Icondir`: especifiquem en quin directori hi ha les icones MRTG.

No cal que tots aquests directoris que hem descrit aquí siguin directoris diferents. El que sí que hem de fer és configurar-los tots perquè l'MRTG funcioni correctament. Aquests paràmetres, si volem, també es poden passar per línia d'ordre quan executem el `cfgmaker`. Per fer-ho, hem d'executar l'ordre amb les opcions següents:

```
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 volem fer el monitoratge de més d'una màquina, és aconsellable tenir un únic fitxer de configuració. Per fer-ho, hem d'afegir el parell *contrasenya@màquina* per cada amfitrió o *host* que volem monitorar en l'execució de l'ordre `cfgmaker`. Per a més informació sobre les ordres de l'MRTG, executeu:

```
root# man cfgmaker
```

Una vegada acabada la configuració de l'MRTG, hem de generar un índex. Per fer-ho, executem l'ordre `indexmaker`. Un exemple d'execució d'aquesta ordre és:

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

Els paràmetres que hem posat en l'exemple d'execució són els mínims que necessita aquesta ordre per a fer un índex. Aquesta ordre, però, té moltes més opcions. Ara bé, totes aquestes opcions fan referència a la manera com volem que es visualitzi `index.html`: en una columna, en dues, ordenats per adreça IP, ordenats per nom, en ordre ascendent, en ordre descendent, amb quin tipus de lletra, etc.

Per a més informació sobre aquestes opcions hem de consultar el manual:

```
root# man indexmaker
```

Per acabar la configuració hi hem d'afegir el directori `/var/www/mrtg` perquè es visualitzi des d'Internet. En el mòdul següent veurem totes les opcions de configuració d'un servidor web. En aquest apartat ens limitem a explicar les modificacions necessàries perquè funcioni l'MRTG i suposem que el nostre servidor funciona de manera correcta.

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

Una vegada acabada la configuració, només ens queda executar l'aplicació. Per a fer-ho, utilitzem el `crontab`, un fitxer de sistema on es configuren totes les tasques d'execució periòdica que volem fer de manera automatitzada. Per a accedir al `crontab` de la nostra màquina hem de fer servir l'ordre:

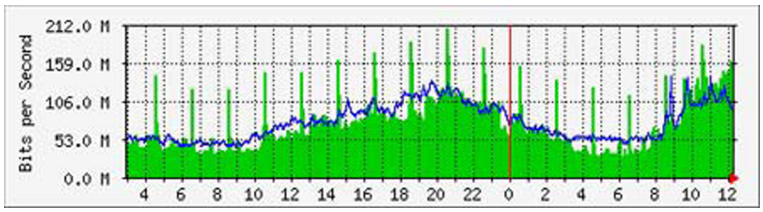
```
root# crontab -e
```

Una vegada accedim al `crontab` hi afegim la línia següent:

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

Mitjançant aquesta línia suposem que l'executable de l'MRTG és a `/usr/bin`, que el fitxer de configuració el tenim a `/etc/mrtg.cfg` i que els registres del sistema són a `/var/log`. Una vegada funciona l'MRTG, si consultem la pàgina web de la nostra màquina on es mostren els resultats, obtenim gràfics semblants al que ens mostra la figura següent:

Amplada de banda monitorada

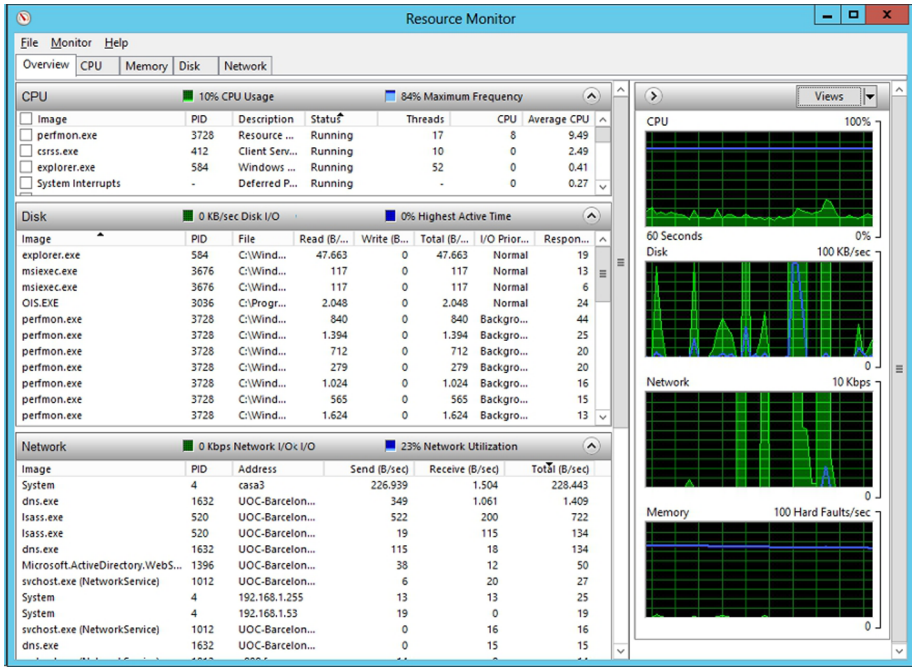


Aquests gràfics ens mostren els volums d'informació (tant d'entrada com de sortida) que circulen per un equip de xarxa al llarg de les últimes vint-i-quatre hores. La línia vertical de color vermell ens indica on s'acaba el dia. El color blau ens mostra la sortida i el color verd, l'entrada.

6.2. Monitoratge amb el Windows Server 2012

El Windows Server 2012 té inclosa una utilitat per a monitorar en general els recursos del sistema, que és el monitor de recursos, que es troba en la pantalla d'administració del servidor, dins el menú d'eines. La figura següent mostra una captura amb un comportament que *a priori* pot sembla estrany si el servidor està en uns moments en què no hi ha activitat.

Monitor de recursos

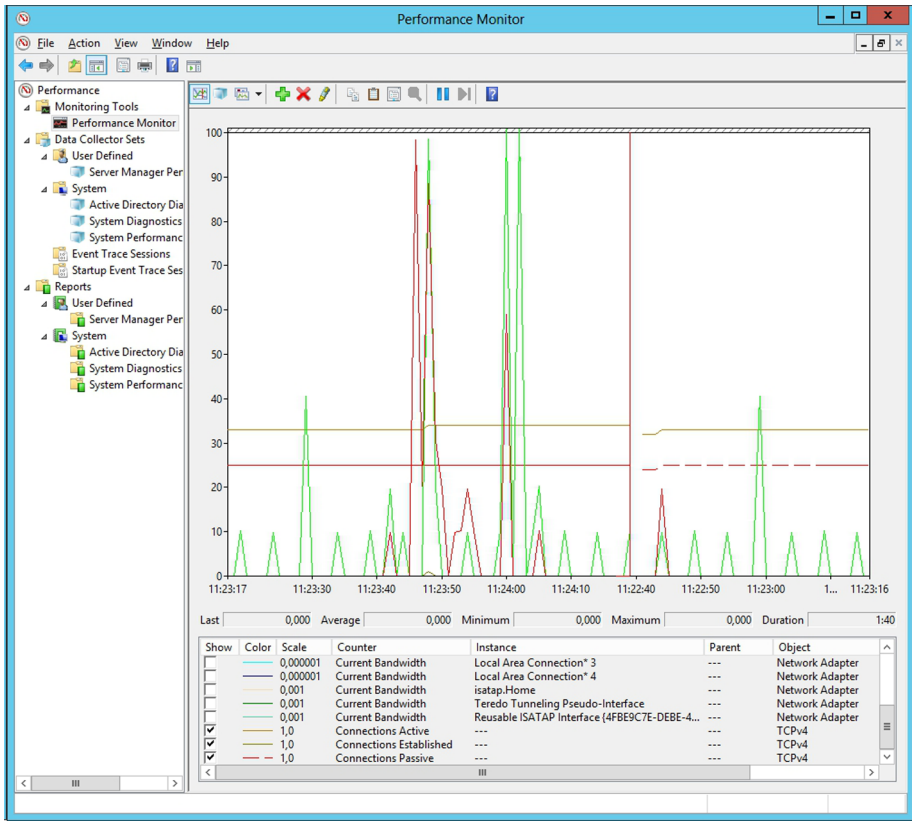


Podem veure que el disc està en ús i que a més, a la mateixa vegada s'està fent servir la xarxa, i quins processos l'estan fent servir. Aquest monitor de recursos ens dóna una informació molt important per poder controlar el comportament del servidor.

Però a més d'aquest monitor, el Windows Server 2012 també disposa d'un altre monitor del sistema que permetrà tenir molt més controlats certs elements que amb aquest primer monitor hàgim vist sospitosos. Aquesta altra eina és el monitor de rendiment, que també es troba en la llista de les eines de l'administrador del servidor.

La figura següent mostra un instant del monitoratge del servidor: en aquesta eina tot és configurable, es pot monitorar el nombre de connexions establertes amb el servidor, els bytes que el servidor envia o rep per IPv4, o per IPv6, l'accés a disc, els errors de paginació, etc.; hi ha una llista molt extensa de variables que es poden monitorar.

Monitor de rendiment en local

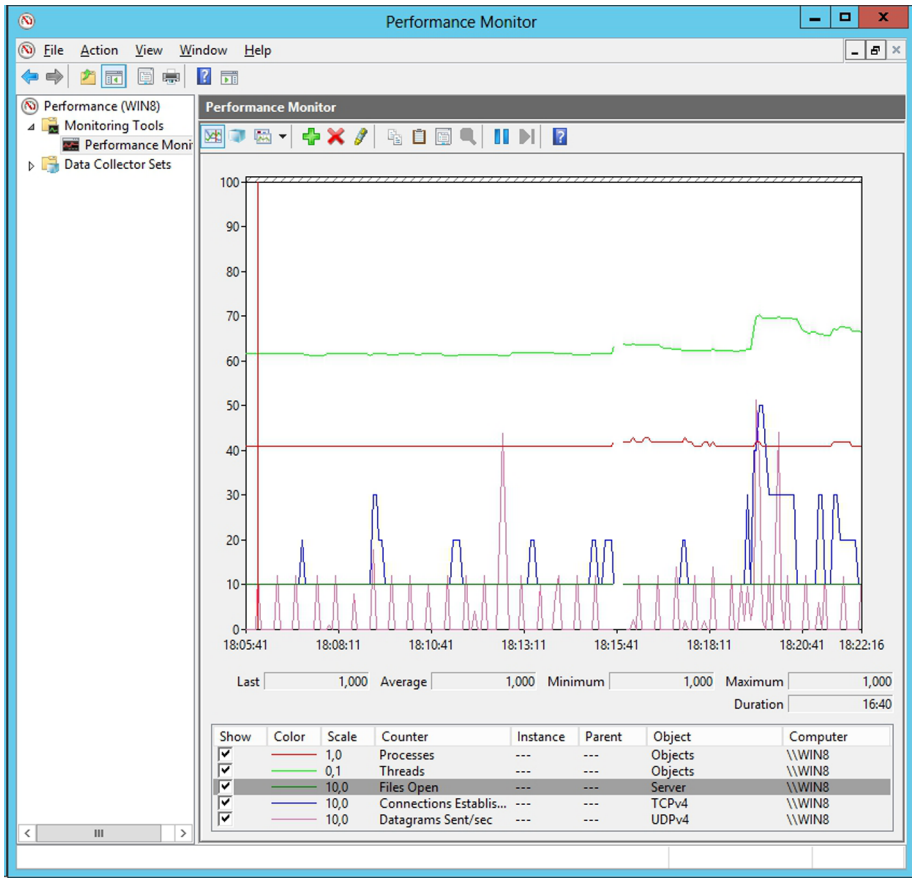


Permet monitorar per mitjà de l'Active Directory les diferents estacions de treball que estan dins el domini; només cal seleccionar el PC que es vol seguir, i escollir què es vol monitorar en el moment d'afegir el comptador.

Per a poder fer això, cal que en cada estació de treball en què es vulguin obtenir les dades en remot s'hagi activat el servei de registre remot. Això s'aconsegueix obrint la consola, o el PowerShell del sistema, si l'estació de treball té el Windows 7 o 8, i accedint a la consola `services.msc`, que serveix per a iniciar i parar els serveis. S'han d'iniciar els serveis de registre remot i el servei registre i alertes de rendiment, i així el client executarà el servei per tenir accessibles les dades remotament.

A més, s'ha de tenir en compte que s'ha d'habilitar el tallafoc per a poder accedir remotament a aquests serveis des del servidor i la configuració de l'accés a les dades s'ha de fer des d'un usuari que pertanyi al grup d'usuaris de *log* i al de lectors d'esdeveniments de *log*. La figura següent mostra cinc comptadors d'un equip remot. D'aquesta manera es pot controlar molt més acuradament el comportament d'un ordinador de manera remota en què se sospita que hi ha algun programa instal·lat aliè a la companyia, com podrien ser programes de compartició de fitxers, troians, etc. Es pot monitorar l'ús de la xarxa per a aquell equip en concret, el nombre de sessions obertes que té, etc. Fins i tot permetrà controlar la "salut" de l'ordinador, amb l'estat del disc o del processador.

Monitor de rendiment d'un equip remot



A més permet crear informes de tot allò que s'està monitorant. L'aplicació mateixa permet configurar els documents de sortida que es volen produir. D'aquesta manera es disposarà ràpidament de sistemes d'auditories dels equips interns de l'organització.

7. Eines de comprovació

El monitoratge de la xarxa, malgrat que és efectiu en molts aspectes, depenent del tipus d'anàlisi no és suficient. Aquest és el cas de descobrir les possibles vulnerabilitats de la nostra xarxa. Mitjançant el monitoratge només veiem l'ús que es fa de la nostra xarxa, però no veiem l'ús de la xarxa de manera detallada, com per exemple:

1) El percentatge de trànsit TCP, UDP, ICMP, o difusió o *broadcast*.

2) Quins són els protocols que es fan servir més (HTML, FTP, SFTP, P2P, etc.).

3) Comprovar si els nostres servidors tenen ports oberts que no ho haurien d'estar.

La solució a aquesta mena de problemes ens l'ofereixen les eines de comprovació.

Hi ha dos tipus d'eines de comprovació: les passives i les actives. Les passives són les eines que no interfereixen en la xarxa, sinó que es limiten a capturar paquets i obtenir resultats estadístics de les captures de les trames que circulen per la xarxa. Al contrari, les actives són les que, a més d'obtenir estadístiques, són capaces d'analitzar la xarxa mitjançant mecanismes intrusius, és a dir, que enviant paquets a la xarxa, són capaces d'obtenir informació de les màquines que hi ha enviant paquets especials que les màquines destinació contesten, i així obtenen encara més informació de com està configurada la xarxa d'ordinadors.

Hem d'anar molt amb compte quan fem servir aquest tipus d'eines, ja que en algunes de les aplicacions que tenen pot semblar que estiguem fent un atac a una màquina. Si la màquina no l'administrem nosaltres i no hem avisat l'administrador que farem aquest tipus d'anàlisi, és possible que, si es detecta l'atac, tinguem algun problema amb l'administrador, ja que en molts casos es pot veure aquesta activitat com un atac als servidors per mitjà de la xarxa local.

També hem d'anar molt amb compte amb quins àmbits utilitzem aquest tipus d'eines, ja que cada país té la seva pròpia llei de protecció de dades, en la qual es descriu en quins entorns es pot dur a terme una anàlisi, fins on podem analitzar (capçalera IP, capçalera TCP, capçalera d'aplicació i dades) i si cal o no algun tipus d'autorització de conformitat dels clients per a analitzar la xarxa.

7.1. Eines del GNU/Linux

7.1.1. NMAP

Una aplicació típica i molt usada de la classe de les eines actives és l'anomenada Network Mapper (NMAP). Es tracta d'una eina GNU que es fa servir per a explorar xarxes o fer auditories de seguretat. Aquesta eina està dissenyada especialment per a fer una anàlisi de grans xarxes, tot i que només estigui instal·lada en una única màquina.

La informació que ens pot oferir l'NMAP és molt variada: quines màquines hi ha actives, quin sistema operatiu tenen, quina versió, quins ports té oberts cada màquina, etc. A més, hi ha versions d'NMAP per a gairebé qualsevol sistema operatiu (Windows, Linux, FreeBSD, Mac OS X, etc.) amb versió en mode text o mitjançant entorn gràfic.

També hi ha versions d'NMAP per a instal·lar en sistemes Debian. Per fer la instal·lació hem d'executar l'ordre següent:

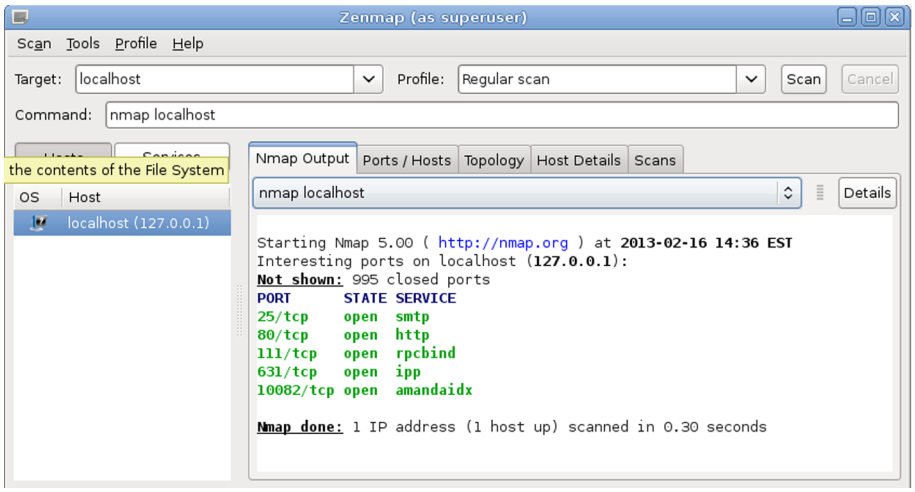
```
root# apt-get intall nmap.
```

Una vegada tenim instal·lada aquesta eina en mode consola, a part dels executables de l'aplicació, també tenim instal·lades les pàgines de documentació del manual. La informació d'aquestes pàgines és molt completa i ens detalla totes les opcions possibles; així mateix, al final de la documentació trobem exemples de funcionament. Però hi ha també la possibilitat d'utilitzar aquesta eina en un entorn gràfic; hem d'instal·lar el frontal o *front end* mitjançant l'execució de l'ordre:

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

La visualització d'aquesta eina en l'entorn gràfic es mostra d'una manera semblant en la figura següent:

Execució d'NMAP sobre *localhost*



Aquest entorn gràfic ens permet fer totes les configuracions possibles de l'eina `nmap` fent servir el ratolí. A més, ens mostra (a la barra inferior, anomenada *command*) l'ordre que hem d'executar per a obtenir el mateix resultat que si utilitzàvem aquesta eina sense entorn gràfic.

Els paràmetres en l'eina `nmap` es divideixen en dues parts: els escanejos i les opcions generals. Dins del primer grup de paràmetres trobem les opcions següents:

1) `sS`: escaneig de TCP Syn. No estableix una connexió completa TCP.
2) `sT`: escaneig de TCP. Estableix una connexió completa TCP.
3) `su`: escaneig d'UDP.
4) `sP`: escaneig *ping*. Troba màquines accessibles en la xarxa.
5) `sV`: intenta establir quina versió de programari hi ha en cada port actiu.
6) `sR`: escaneig d'RPC.

Els paràmetres que afecten les opcions generals de configuració de l'eina `nmap`:

1) `O`: ús del TCP/IP per a identificar un sistema operatiu remot.
2) `p`: rang de ports que s'han d'escanejar.
3) `PO`: no fer *ping* cap a les màquines remotes.
4) `6`: ús d'IP versió 6.
5) `v`: *verbose* (recursiu).

7.1.2. Snort

L'eina Snort és una aplicació del tipus de les passives. Aquesta eina, malgrat que no és gaire complicada de fer servir, pot resultar una mica tediosa per als usuaris nous perquè té molts paràmetres i tres modes de configuració diferents:

1) *Sniffer* llegeix paquets de la xarxa i els mostra per pantalla.

2) El paquet *logger* emmagatzema els diferents paquets capturats en el disc per fer-ne una anàlisi més endavant.

3) El *Network intrusion detection* és un motor de comparació que intenta reconèixer diferents tipus d'atacs de xarxa.

Els primers modes de configuració d'aquesta eina estan molt orientats a xarxes; per tant, no entren dins del temari d'aquesta assignatura. En el tercer mòdul, malgrat que també té molt contingut de xarxes, la majoria dels atacs fan referència als servidors que hi ha al darrere. Per tant, ens centrarem en la manera de configurar l'Snort per fer la detecció d'intrusos.

Per instal·lar aquesta eina hem d'executar l'ordre següent:

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

Una vegada l'hem executada, i abans d'acabar la instal·lació, ens demana que configurem alguns paràmetres d'aquesta eina. Els paràmetres que hem de configurar són aquests:

- El dispositiu utilitzat per l'Snort: per defecte, `eth0` (hi hem de posar el dispositiu que farem servir per a examinar la xarxa).

- El rang de xarxa IP que volem analitzar: per defecte, 192.168.0.0/16 (hi hem de posar el rang IP que volem analitzar).

- L'usuari que executarà l'Snort: per defecte, *root* (hem de canviar aquest usuari pel de *snort*, i si no s'ha creat, l'hem de crear abans).

Per executar en mode *Network intrusion detection*, hem d'executar l'Snort amb els paràmetres següents:

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

El directori de sortida per defecte és `/var/log/snort.log`. Si no volem especificar un altre directori, ometem aquest paràmetre. En aquest fitxer és on quedarà constància dels atacs que hem tingut. Per això l'hem de revisar sovint. El fitxer `snort.conf` és on hi ha emmagatzemades les regles de comportament dels atacs; inicialment no n'hi ha cap, i per tant no es pot fer cap tipus d'atac. Com que hi ha molts atacs possibles, s'ha d'instal·lar una altra eina que permetrà actualitzar aquest conjunt de regles automàticament. Això ho aconseguim amb l'eina Oinkmaster, que s'instal·la directament amb l'eina Snort, però si no és el cas, només cal instal·lar-la amb l'ordre `apt-get`.

Per tal de fer servir el programa Oinkmaster s'ha d'obtenir accés a la pàgina web de l'Snort (www.snort.org) per a poder configurar l'eina de baixada de les regles i així poder tenir-les en local.

Un cop donats d'alta només cal cridar l'ordre `oinkmaster` amb el directori on es guarden les regles de l'Snort, que per defecte és `/etc/snort` amb el fitxer `snort.conf` i un directori anomenat `rules` on hi ha totes les regles.

Periòdicament, hem d'actualitzar el fitxer de regles, ja que van apareixent noves regles. Com que aquest procés no és automàtic, s'ha de configurar el `crontab` perquè ho faci. Per exemple, executant cada matí l'ordre d'actualització de les regles de l'Snort. Es pot fer que s'executi cada matí a la una de la matinada:

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

7.2. Eines del Windows Server 2012

7.2.1. Llistes de comprovació de seguretat

Microsoft té una sèrie de llistes de comprovació que indiquen els passos que cal seguir per a comprovar que una funcionalitat del sistema operatiu està ben configurada; a més, ofereixen informació que hi està relacionada.

Hi ha llistes de comprovació per a diferents aspectes del sistema operatiu, com l'Active Directory, gestió d'usuaris, configuració de la xarxa i configuració de dispositius.

Aquesta llista de comprovació cobreix aspectes com els següents:

- Definir una plantilla de seguretat per a una directiva de grup: ajuda a definir una plantilla de seguretat per a una directiva de grup. Una plantilla de seguretat consisteix en un conjunt de regles de seguretat que s'han de comprovar per a qualsevol usuari que tingui assignada la directiva de grup corresponent.

- Definir una plantilla de seguretat per a un equip local: en aquest cas, les plantilles de seguretat definides s'assignen a equips en comptes de fer-ho a usuaris.

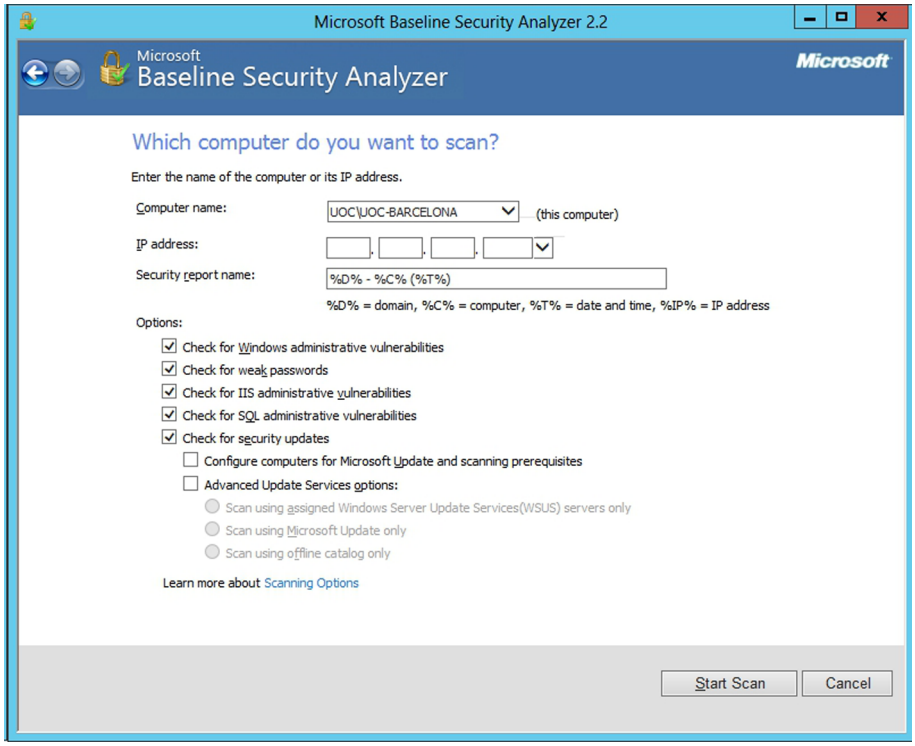
- Analitzar la seguretat: ajuda a analitzar l'estat de la seguretat del sistema segons la plantilla de seguretat triada.

- Configurar la seguretat del sistema: ajuda a configurar la seguretat del sistema segons una plantilla de seguretat.

7.2.2. Microsoft Baseline Security Analyzer

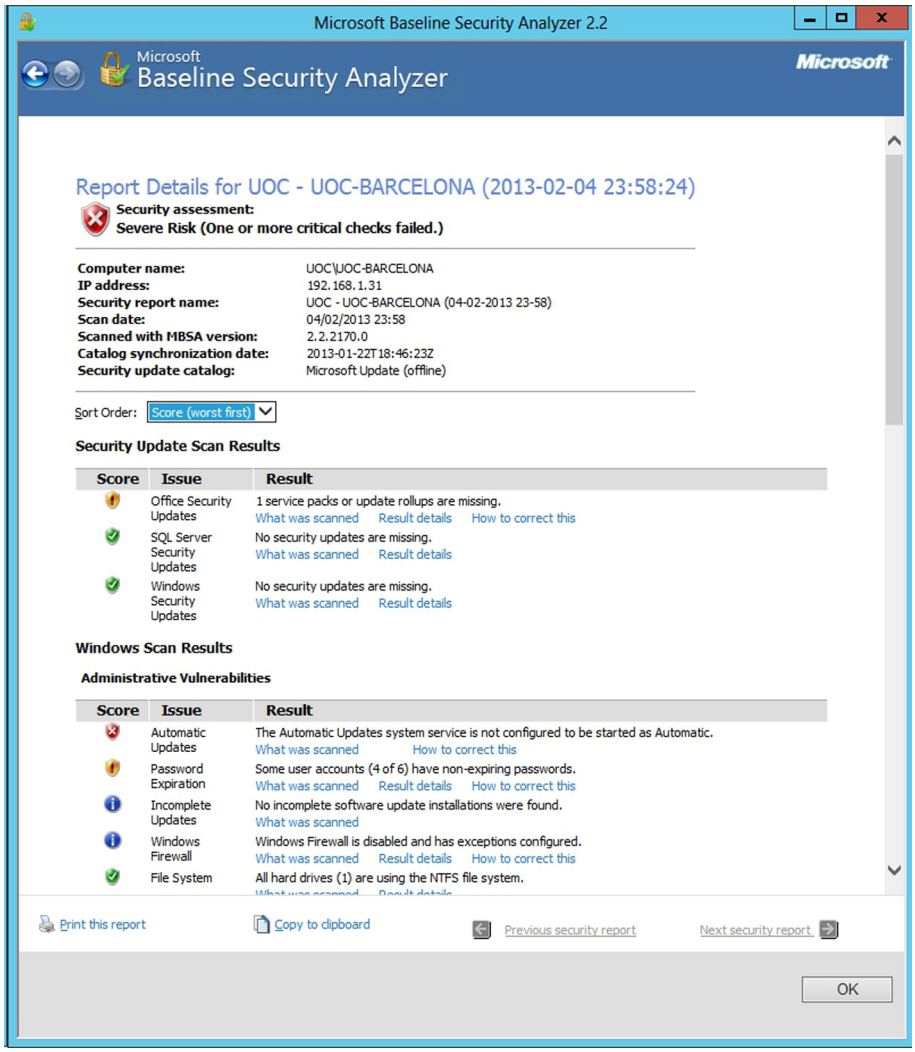
El Microsoft Baseline Security Analyzer (MBSA) és una eina gratuïta de Microsoft que permet fer una anàlisi automàtica de la seguretat del sistema força complet i que a més ofereix possibles solucions als problemes que troba. Permet determinar l'estat de seguretat de l'equip, segons les recomanacions de seguretat de Microsoft, i ofereix guies per corregir els errors.

Configuració de l'escaneig de la seguretat d'un servidor



La figura següent mostra la configuració per defecte de l'anàlisi que efectua aquesta eina en el servidor. El programa es connecta a Internet, als servidors de Microsoft, per a recuperar la darrera informació sobre seguretat del sistemes del Microsoft i comença a comprovar l'ordinador seleccionat. Escaneja tots els problemes coneguts i proposa una solució, tal com es pot veure en la figura següent, on tenim el resultat d'escanejar un servidor amb el Windows Server 2012.

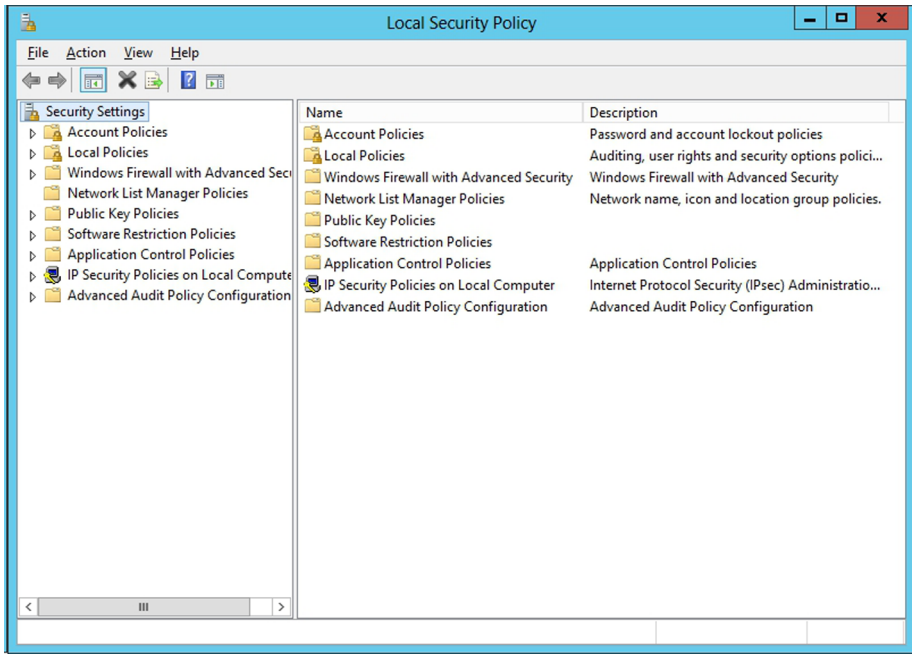
Resultat d'escanejar un servidor amb l'MBSA



7.2.3. Configuració de seguretat local

L'eina Directiva de seguretat local que hi ha en l'enllaç de les eines dins l'administrador del servidor permet configurar els paràmetres de seguretat per a l'equip local.

Directives de seguretat locals



A la part dreta de la pantalla, com es pot veure en la figura anterior, hi ha les propietats de seguretat que es poden modificar fent-hi doble clic a sobre.

Des d'aquí es pot accedir directament a les polítiques de grup que estan relacionades directament amb la seguretat, com per exemple les polítiques dels comptes d'usuari, les restriccions per a les contrasenyes, les polítiques de bloqueig dels usuaris, l'autenticació Kerberos, la configuració de les auditories dels registres, les polítiques del tallafoc de Windows, la criptografia amb BitLocker, restriccions del programari que es vol instal·lar o fer servir, les VPN, etc. És un centre de control de tot el que està relacionat amb la seguretat del servidor.

7.2.4. Configuració i anàlisi de seguretat

L'eina Configuració i anàlisi de seguretat permet analitzar l'estat de la seguretat del sistema segons una plantilla de seguretat, i ens indica quines regles o directives de seguretat de la plantilla es compleixen i quines no. També permet modificar els paràmetres de seguretat i configurar el sistema per a complir totes les directives de seguretat definides en la plantilla.

Per executar aquesta eina hem d'obrir la consola d'administració del sistema amb l'ordre `mmc.exe` i seleccionar l'opció Agregar o treure complement del menú Arxiu. Per afegir-hi un element nou, fem clic sobre Agregar... i en la llista seleccionem el component Configuració i anàlisi de seguretat. Per començar a treballar obrim una base de dades de seguretat que ja hi sigui o en creem una de nova. Una vegada seleccionada la base de dades, surten els diferents paràmetres de seguretat definits en la plantilla de seguretat triada. En el cas de no tenir cap plantilla de seguretat, se n'haurà de crear una a partir de la

consola mateixa afegint el component plantilles de seguretat i creant-ne una de nova. En aquesta plantilla es podran definir tots aquells paràmetres que es vol que el servidor tingui configurats.

Per canviar la plantilla de seguretat, seleccionem l'opció Importar plantilla del menú contextual de l'element Configuració i anàlisi de seguretat de la llista de l'esquerra.

Una vegada seleccionada la plantilla, analitzem si el sistema compleix les directives de seguretat definides en la plantilla, seleccionant l'opció Analitzar l'equip del menú contextual de l'element Configuració i anàlisi de seguretat de la llista de l'esquerra. Una vegada acabada l'anàlisi, es mostren els elements que no compleixen la plantilla de seguretat i els que sí.

Per aplicar la plantilla de seguretat seleccionada a la configuració de l'equip, seleccionem l'opció Configurar l'equip ara del menú contextual de l'element Configuració i anàlisi de seguretat de la llista de l'esquerra. El sistema farà tots els canvis necessaris per a poder satisfer tota la plantilla de seguretat que s'ha seleccionat.