# Filtratge de pàgines Web

**Jordi Mínguez Orozco**

**ETIS**

**Maria Isabel March Hermo**

**11 / gener / 2009**

# Agraïments

La realització del TFC, ha estat subjecte a ritmes i contratemps que ha alterat el dia a dia del meu entorn, laboral i familiar. Es per això que cal agrair a totes aquelles persones que han patit els meus mals de cap.

En primer lloc a la meva família, Jordi i Marta, que m'han suportat amb optimisme en aquesta etapa final de la meva carrera. A la Josephine, la meva parella, per haver aguantat els meus canvis d'humor i actituds, a vegades massa estressants.

La Maribel, la consultora, per la seva paciència i consells sobre tots els canvis de ritme que ha agafat la realització del projecte final.

Per últim a totes aquelles persones que sense nombrar-les han estat al meu costat i m'han animat a continuar.

# Resum

L'objectiu inicial d'aquest treball era la realització i el disseny d'una aplicació per fer un filtratge de pàgines web, i la seva posterior implementació.

Després de realitzar una gran recerca d'informació per a poder conèixer les diferents opcions de mercat, la primera decisió va ser utilitzar el filtratge web sota plataforma Linux amb les eines OpenSource, Iptables, Squid i SquidGuard

Actualment agradi o no, estem en un món on la majoria d'empreses utilitzen solucions Microsoft en les seves estacions de treball o en els servidors, per tant, a mitjans del treball es va decidir realitzar un canvi de plataforma i enfocar la implementació del Proxy i del *Firewall* utilitzant una de les solucions més populars de Microsoft actualment: *ISA* Server 2004. Per tant, implementar un *ISA* server en el nostra laboratori és una simulació molt acotada de la vida real.

Finalment el treball ha estat la realització del filtratge web utilitzant les eines de Microsoft *ISA* Server 2004, llur implementació, configuració i parametrització, en un escenari de treball domèstic o de petita empresa.

Per assolir aquest nivells de seguretat es va triar implementar un *Firewall* sota Windows Server 2003. Les funcions de *WebProxy*, *Firewall* i *SecureNAT* m'han permès crear regles que ofereixen la possibilitat de configurar la meva xarxa laboratori amb diferents politiques de seguretat: molt restrictives, o més permissives.

Es va configurar un escenari amb serveis de xarxa generalitzats i d'us amb molta difusió en àmbits empresarials. Els serveis triats han estat: DNS, Web, FTP, Correu, DHCP.

La política de seguretat del *Firewall ISA* Server 2004 és per defecte totalment restrictiva, bloquejant tot allò que l'administrador de sistemes no ha permès, mitjançant regles i politiques. La configuració pot arribar a ser força complexa, generant una regle per cada tipus de servei.

Cap *Firewall* proporciona una seguretat del 100%, ja que això implicaria el disposar d'una estació de treball totalment aïllada de la xarxa, sense cap tipus de connexió, garantint així una seguretat del 100% però amb la funcionalitat totalment restringida a nivell de connectivitat.

De les proves realitzades en cada una de les estacions de treball, es va poder observar que la seguretat per a us domèstic i presumiblement per a petita empresa és suficient.

Com a conclusió general podem dir que la utilització de *Firewalls* per a garantir la seguretat de la xarxa és imprescindible.

# Índex de Continguts

# Índex de Figures

# 1. Introducció

## 1.1 Motivació i Justificació

La implantació i popularitat creixent d'Internet, tant a l'entorn empresarial com per a usuaris particulars, gracies a la generalització de les connexions ADSL i a llur augment de qualitat, afavoreix l'expansió i la creixent manca de seguretat, ocasionant problemes que poden arribar a qüestionar la nostra privacitat.

A causa del creixent nombre d'atacs i de la seva complexitat tenim la necessitat d'oferir entorns de qualitat i segurs per a les empreses, i per tant l'estudi dels *Firewalls* és d'una manifesta importància. En aquest treball realitzarem un estudi i amb la seva respectiva implementació utilitzant una de les eines Firewall/Proxy més esteses en el mercat, ISA Server 2004. Aquesta tasca es realitzarà tot simulant una situació de xarxa real, on es realitzen un seguit de jocs de proves i configuracions per tal d'obtenir el nivell de seguretat desitjat i una correcte funcionalitat.

## 1.2 Objectius

L'objectiu d'aquest treball és la implementació i estudi d'una aplicació per al filtratge de pàgines web, realitzant una xarxa corporativa per a simular una situació real, i alhora analitzar com el filtratge pot millorar la nostra seguretat.

La idea és que l'aplicació de filtratge proporcioni tota la informació possible, com per exemple:

- Quins Usuaris han estat utilitzant les estacions de treball
- Les direccions IP de tots els clients del nostre *Firewall*.
- Les Pagines webs visitades, amb l'hora i data.
- Els Temps de connexió.
- Els protocols i ports que han estat utilitzats.
- Quines regles i politiques del Firewall han estat aplicades a cadascun dels clients.

Com a segon objectiu tenim el restringir l'accés a totes aquelles webs que per el seu contingut o perillositat, en quan a codi maliciós, sigui convenient evitar, i per tant, que els nostres clients no les puguin visitar. D'aquesta manera, per exemple, una empresa podria controlar que en hores productives un treballador no estigui realitzant tasques no laborals, o a un nivell més domèstic, evitar que els nostres fills visitin pagines web amb continguts per adults.

Per assolir els objectius s'ha realitzat:

- Realitzar tot el seguit de proves en la xarxa per a comprovar si el nostre sistema de seguretat esta funcionen correctament.
- Estudiar i configurar diferents servidors com *ISA* Server 2004 i utilitzar els clients amb plataforma Windows per a testejar la funcionalitat.
- Un diagrama gràfic per al disseny de la xarxa on es realitza l'estudi.

El fet de tenir tot el treball documentat ens permet analitzar d'una manera més senzilla la funcionalitat i configuració de la xarxa, per a poder comprovar la seva correcte implementació i fins hi tot, si s'escau, corregir i implementar millores per a nous reptes que haguem d'afrontar, ja que com tots sabem, la tecnologia avança ràpidament i com a conseqüència, la seguretat de les nostres xarxes també.

## 1.3 Enfocament i mètode del projecte

En quan a l'enfocament del projecte, s'ha centrat bàsicament en el funcionament d'un Firewall i un Proxy web per tal d'aprendre el seu funcionament i la seva correcte configuració depenen de l'escenari en el qual ens trobem.

El mètode seguit per a la realització del treball consisteix en que una tasca no comença fins que l'anterior ha estat finalitzada, tal i com varem aprendre en el curs, alhora de realitzar projectes en distribució en cascada.

En la primera etapa del projecte va haver un procés d'aprenentatge de les eines relacionades amb aquest, ja que inicialment no es coneixia el producte a implementar i mai havia realitzar cap tasca similar. A més a més es va haver de tornar a mirar els antics mòduls d'aquelles assignatures de Xarxes ja superades, amb la intenció de repassar coneixements i facilitar el disseny de l'escenari.

Un cop acabat el procés de recerca d'informació per tenir clar els conceptes teòrics es va prosseguir amb el muntatge físic de la infraestructura. El primer pas va ser aconseguir el software necessari per a la instal·lació de tots els ordinadors, així com l'adquisició dels ordinadors físics per tal de implementar la xarxa laboratori. Un cop la xarxa estava físicament implementada, es va començar amb la parametrització de les configuracions de cadascun dels elements.

Finalment, es pot veure la temporització del projecte en l'apartat que ve a continuació: La planificació.

## 1.4 Planificació del Projecte

Al inici del projecte es van marcar una sèrie de dates amb tot el seguit de diferents entregues previstes durant el semestre.

| Títol | Data |
|---|---|
| Pla de Treball | 28 de setembre |
| Lliurament quinzenal de progrés | 12 d'Octubre |
| Lliurament quinzenal de progrés | 26 d'Octubre |
| Entrega de la PAC 1 | 2 de Novembre |
| Lliurament quinzenal de progrés | 23 de Novembre |
| Lliurament quinzenal de progrés | 7 de Desembre |
| Entrega de la PAC 2 | 14 de Desembre |
| Lliurament quinzenal de progrés | 4 de Gener |
| Lliurament Final | 11 de Gener |
| Lliurament de la Presentació | 19 de Desembre |

**Figura 1 : Entregues Previstes inicialment**

Les tasques previstes al inici del projecte eren les següents:

## Tasca 1:

**Temporització:** 2 setmanes (28 de setembre al 12 d'octubre).
**Descripció:** Recollida i classificació de tota la informació que pugui ser rellevant per dur a terme el projecte:

- **1.1** - Temes relacionats amb aplicacions *OpenSource* per al filtratge web i la seguretat en un entorn corporatiu.
- **1.2** - Temes relacionats amb els servidors que s'han d'implementar per a la simulació de la xarxa, Apache2, etc.
- **1.3** - Temes relacionats amb l'anàlisi, el disseny i la implementació de com dissenyar les politiques de seguretat clients/servidor.

**Objectius:**

- Dissenyar la xarxa i preparar cadascun dels servidors i clients que participaran en el estudi.
- Tenir molt clar com s'instal·len i es configuren els servidors per al seu futur estudi.
- Començar a preparar com realitzarem el filtratge web i totes aquelles aplicacions que intervindran a nivell de la seguretat.

**Fites:**

- Document descriptiu del rol que faran cadascun dels servidors/clients.
- Resum de totes les funcions de filtratge que haurem d'implementar més endavant.

## Tasca 2:

**Temporització:** 4 setmanes (13 d'octubre al 2 de novembre).
**Descripció:** Implementació real de la xarxa corporativa amb totes les aplicacions i serveis que hauran de ser estudiats.
**Objectius:**

- Instal·lar els Sistemes operatius i aplicacions necessàries a cadascun dels servidors i clients.
- Realitzar les configuracions necessàries per aconseguir el nivell seguretat desitjat i el seu respectiu filtratge per a un posterior anàlisis.

**Fites:**

- Aconseguir que els servidors i els clients estiguin totalment operatius i configurats correctament, per a poder iniciar el procés de proves en la següent tasca.

## Tasca 3:

**Temporització:** 6 setmanes (10 de novembre al 21 de desembre).
**Descripció:** Anàlisis i joc de proves
**Objectius:**

- Generar els jocs de proves adients per garantir el correcte funcionament del filtratge web i totes les politiques de seguretat en la nostra xarxa. Les proves hauran de demostrar que hem assolit el nivell de seguretat desitjat.

**Fites:**

- Inici del procés de proves per a demostrar que la seguretat ha estat adequadament implementada. Comprovant que el filtratge web funciona correctament.
- Documentació sobre els jocs de proves realitzat.
-

| **Tasca 4:** |
|---|
| **Temporització**: 1 setmana (del 22 al 28 de desembre).<br>**Descripció:** Documentació del producte.<br>**Objectius:**<br>- Documentar la instal·lació del producte i la implementació de la política de seguretat estudiada, per a una futura aplicació en una xarxa real.<br>- Documentar l'ús de les diferents opcions de configuració que pugui tenir.<br>**Fites:**<br>- Documentació del filtratge de pagines web. |
| **Tasca 5:** |
| **Temporització:** 2 setmanes (del 29 de desembre al 9 de gener).<br>**Descripció:** Arranjaments finals de la memòria i preparar la presentació del filtratge de pagines web i el estudi realitzat.<br>**Objectius:**<br>- Síntesi de la memòria presa durant el projecte.<br>- Crear una presentació del treball.<br>**Fites:**<br>- Memòria del projecte.<br>- Presentació del filtratge web. |

**Figura 2 : Tasques Inicials**

A causa de la decisió d'implementar el filtratge web utilitzant Microsoft *ISA* server 2004 enlloc de les eines OpenSource que en un principi s'anaven a implementar, es van tenir que realitzar una sèrie de modificacions en el pla de treball.

La principal modificació va ser incorporar una tasca on es reflectís l'etapa de recerca i d'aprenentatge del nou producte, així com una lleugera desviació temporal en les tasques 2 i 3.

El canvis realitzats en la planificació han estat els següents:

| **Tasca 2:** |
|---|
| **Temporització:** 4 setmanes (13 d'octubre al 2 de novembre).<br>**Descripció:** Implementació real de la xarxa corporativa amb totes les aplicacions i serveis que hauran de ser estudiats.<br>**Objectius:**<br>- Instal·lar els Sistemes operatius i aplicacions necessàries a cadascun dels servidors i clients.<br>- Realitzar les configuracions necessàries per aconseguir el nivell seguretat desitjat i el seu respectiu filtratge per a un posterior anàlisis.<br>**Fites:**<br>- Aconseguir que els servidors i els clients estiguin totalment operatius i configurats correctament, per a poder iniciar el procés de proves en la següent tasca. |

| **Tasca X:** |
|---|
| **Temporització:** 4 setmanes (2 de novembre al 30 de novembre).<br>**Descripció:** Aprenentatge i investigació de com implementar *ISA* Server 2004<br>**Objectius:**<br>- Lectura de documentació per a poder conèixer el funcionament *ISA* Server 2004 en un dels servidors.<br>- Iniciar la implementació de *ISA* Server 2004 en un servidor Windows 2003.<br>- Configuració i creació de les politiques de Firewall en un entorn Microsoft.<br>**Fites:**<br>- Reestructurar la xarxa per a realitzar la funcionalitat amb Microsoft *ISA* Server 2004 |
| **Tasca 3:** |
| **Temporització:** 4 setmanes (30 de novembre al 21 de desembre).<br>**Descripció:** Anàlisis i joc de proves<br>**Objectius:**<br>- Generar els jocs de proves adients per garantir el correcte funcionament del filtratge web i totes les politiques de seguretat en la nostra xarxa. Les proves hauran de demostrar que hem assolit el nivell de seguretat desitjat.<br>**Fites:**<br>- Inici del procés de proves per a demostrar que la seguretat ha estat adequadament implementada. Comprovant que el filtratge web funciona correctament.<br>- Documentació sobre els jocs de proves realitzat.<br>- |

**Figura 3 : Tasques Modificades**

## 1.5 Infraestructura utilitzada

Tot seguit podem veure el hardware i software utilitzats en el projecte. El hardware utilitzat va ser utilitzat centrant-nos en la disponibilitat, en cap moment les especificacions físiques dels ordinadors utilitzats tenen relació amb com haurien de ser en una situació real el servidors. El programari al contrari, si que va ser seleccionat per acotar el millor possible una situació quotidiana. Ens els apartats posteriors podem veure les diferents raons de l'elecció de cadascun dels elements de software.

### 1.5.1 Hardware

| Nom: | **W2003** |
|---|---|
| Especificacions tècniques | • Compaq Evo D51C<br>• 2.0-GHz Pentium 4 CPU<br>• 256MB DDR |
| Sistema Operatiu | Windows Server 2003 |
| Serveis que ofereix | • DNS |

| | |
|---|---|
| | • DHCP<br>• Controlador de Domini |
| Utilització | Oferir servei a la Xarxa |

| Nom: | **Ubuntu** |
|---|---|
| Especificacions tècniques | • HP Compaq nx9110<br>• 3.06-GHz Pentium 4 CPU<br>• 512MB DDR |
| Sistema Operatiu | Linux Ubuntu 10.0 |
| Serveis que ofereix | • Correu<br>• Web<br>• FTP |
| Utilització | Oferir servei a la Xarxa |

| Nom: | **ISA04** |
|---|---|
| Especificacions tècniques | • Compaq Evo D510 Small Form Factor<br>• 2.53-GHz Pentium 4 CPU<br>• 512MB DDR |
| Sistema Operatiu | Microsoft Server 2003 - *ISA* Server 2004 |
| Serveis que ofereix | • *SecureNAT*<br>• *Firewall*<br>• Web Proxy |
| Utilització | Controlar la seguretat de la xarxa i fer de porta d'enllaç |

| Nom: | **Client1** |
|---|---|
| Especificacions tècniques | • HP DC7600 Desktop<br>• 2.8-GHz Pentium 4 CPU<br>• 512MB DDR |
| Sistema Operatiu | Windows XP Professional |
| Serveis que ofereix | Client |
| Utilització | Realitzar el joc de proves |

**Figura 4 : Hardware Utilitzat**

### 1.5.2 Software

Per la documentació i preparació del projecte faig servir el programari següent:

- Diagrames gràfics de la xarxa amb Microsoft Visio 2007.
- Per als documents Microsoft office (Word, Excel, PowerPoint) 2007

El programari dels Clients és:

- Sistema operatiu Microsoft Windows XP en els Clients
- Client Firewall del ISA server 2004

El programari necessari per a la implementació dels servidors és:

- Windows Server 2003 per a DNS, Controlador de Domini i DHCP
- Microsoft *ISA* Server 2004 en quan al Proxy/*Firewall*
- Distribució Linux "Ubuntu" per al servidor Web, FTP i Correu.
- Servidor Web "Apache"
- Servidor FTP "ProFTPd"
- Servidor de correu "Sendmail"


**Figura 5 : Programari utilitzat**

## 1.6 Producte Obtingut

Els productes obtinguts després de la realització del TFC són:

- ***La memòria***

En la memòria és reflecteixen els coneixements adquirits i tota la informació necessària per tal de fer possible la reproducció d'aquest TFC. Donant a conèixer la implementació i configuració de totes les eines necessàries pel nostre escenari, així com els passos seguits durant la seva realització; sempre amb la fita d'aconseguir una correcta funcionalitat de tots els elements de la xarxa.

- ***La Presentació***

La presentació es un fitxer PowerPoint on només s'exposen els punts més importants o destacats que s'han desenvolupat en l'elaboració del projecte, mentre que els detalls del mateix es troben reflectits en la memòria. En aquest producte és on hi ha una síntesi de les fases més importants del projecte: la de disseny i la d'implementació.

- ***El producte***

En aquest TFC no existeix un producte en forma de programa o aplicatiu com s'ha pogut observar anteriorment. El treball ha estat centrat en la parametrització i implementació d'un Firewall/Proxy amb llicencia privada: Microsoft ISA Server 2004. La utilització d'aquesta eina ha implicat el haver d'assolir inicialment uns coneixements sobre un producte que fins ara desconeixia.

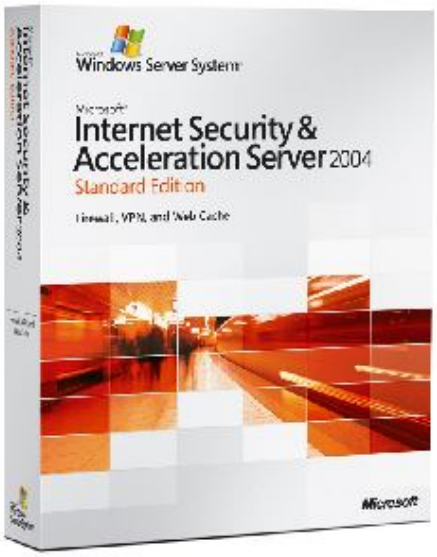


**Figura 6 : Microsoft ISA Server 2004**

## 1.7 Breu descripció dels capítols

**Proxy i Firewall**

En aquest apartat es descriurà el funcionament dels Proxys i Firewalls, amb els seus avantatges i desavantatges, així com també les diferents opcions de mercat que existeixen, incloent una breu comparativa entre elles.

**Escenari**

En el capítol de l'escenari es mostra gràficament a on s'ha implementat cadascun del elements del treball mitjançant un gràfic de tota la xarxa, així com tota la informació necessària per a recrear exactament l'escenari laboratori on ha donat lloc tot el TFC.

**El servidors**

Aquest apartat és on es mostra la configuració i implementació que s'ha dut a terme en cadascun dels servidors, per aconseguir la funcionalitat de la xarxa desitjada.

**Els clients**

El capítol dels clients ens dona a conèixer tot el seguit d'opcions i configuracions que els clients de la xarxa hauran de realitzar per a un correcte funcionament amb tot els altres elements prèviament implementats. També es mostra mitjançant imatges com la funcionalitat de la xarxa ha estat correcte.

**Conclusions**

Com es pot veure en el nom del capítol, aquí s'inclouen totes les conclusions, a nivell acadèmic i personal després de la realització del TFC

**Glossari**

El glossari és un breu capítol on es mostren tot un seguit de paraules tècniques amb les seves respectives explicacions, per afavorir l'entesa dels lectors.

# 2. Proxy i Firewall

## 2.1 Definició de Proxy

Un Proxy o servidor Proxy, és un ordinador que intercepta les connexions de xarxa que un client fa a un servidor. El servidor Proxy de web intercepta la navegació dels clients a pàgines web, els possibles motius són la seguretat, el rendiment, anonimat, etc. Podem definir un Proxy com un servei que permet als usuaris d'una xarxa realitzar connexions a Internet.

Un servidor Proxy es troba situat normalment entre el client i la connexió a l'exterior. El client es connecta al servidor Proxy i sol·licita un recurs d'Internet, el servidor com a conseqüència és l'encarregat de sol·licitar-ho a l'exterior, si s'escau, oferir-ho al client.

El Proxy pot emmagatzemar en el disc dur les pagines web visitades com a "cache" per a pròximes consultes dels seus clients.

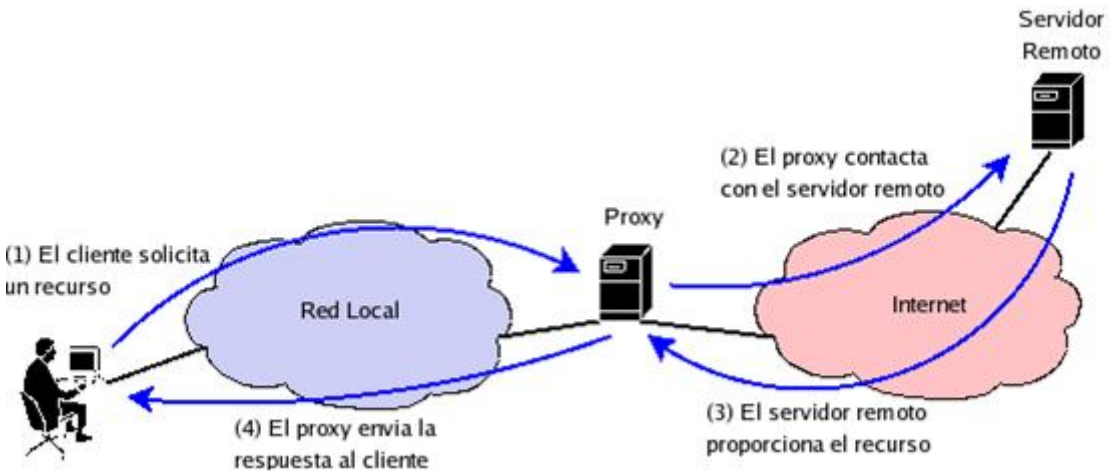


**Figura 7 : Funcionament d'una VPN**

### 2.1.1 Avantatges

- **Control**. Sòls l'intermediari fa el treball real, podem limitar i restringir els drets dels usuaris. Pot donar servei a un gran nombre d'usuaris.
- **Velocitat**. Si diferents clients demanen el mateix recurs, el Proxy pot fer de cache. Així per a les mateixes demandes no te que tornar a contactar amb el destí, i la resposta és més ràpida.
- **Filtratge**. El Proxy pot denegar la resposta a peticions si detecta que estan prohibides, basades en criteris establerts per l'administrador.
- **Modificació**. Un Proxy pot falsificar informació o modificar-la.
- **Anonimat**. Si els usuaris s'identifiquen com un sol, el recurs no pot diferenciar-los.

### 2.1.2 Desavantatges

- **Abús**. Ha de controlar qui te accés i qui no als serveis.
- **Sobre carrega**. Ha de fer el treball de molts usuaris.
- **Intromissió**. Poden existir usuaris que no vulguin passar pel Proxy si fa de cache i guarda copies de les dades, vulnerant la seva intimitat.
- **Incoherència**. Es possible que doni una resposta antiga, no actualitzada, existint una més nova.

### 2.1.3 Funcionament i tipologia

Un Proxy permet la connexió d'equips a una xarxa a través seu. És el Proxy qui realitza la comunicació i a continuació trasllada el resultat a l'equipo inicial. Disposem de diverses tècniques. Podem tenir Proxys funcionant com a Proxy web, Proxy cache, Proxy NAT (Network Adress Translation) fent funcions normalment de routers o servidors d'enroutament.

**Proxy web:**

El Proxy web és una aplicació específica per l'accés a la web. Proporciona una cache par a pàgines web i els continguts descarregats, que es compartida per tots els equ*ips* de la xarxa. El client realitza la petició d'un recurs d'Internet (una pàgina web o un altre arxiu) especificat per una URL.

**Proxy Cache:**

El Proxy cache rep la petició, cerca la URL al seu cache local. Si la troba, retorna el document, si no, la captura del servidor remot, la retorna a qui la va demanar i guarda una copia al cache per a futures peticions.

**Proxy NAT:**

La funció NAT (NAT, Network Address Translation), és coneguda com emmascarament d'IPs. Normalment en les xarxes corporatives aquesta funció la realitzen els routers. És una tècnica que reescriu les direccions origen i destini dels paquets IP i substituïdes per d'altres. Ens permet que més d'un usuari comparteixi una única connexió a Internet (IP publica) i disposin de diferents *IPs* privades. A una xarxa d'àrea local (LAN) els equ*ips* utilitzen adreces IP reservades per a us privat, el Proxy és l'encarregat de traduir les adreces privades a la única adreça pública per a realitzar las peticions, i distribuir les pàgines rebudes als clients de la xarxa interna.

Les adreces privades es troben als rangs prohibits per a us a Internet com són:

- 192.168.x.x
- 10.x.x.x
- 172.16.x.x - 172.31.x.x

## 2.2 *Firewall*

### 2.2.1 Definició de *Firewall*

Un *Firewall* és un sistema de seguretat de xarxes per a protegir una màquina o una subxarxa de serveis que puguin esser una amenaça des de l'exterior, es a dir és un sistema d'aïllament entre xarxes per evitar comunicacions no desitjades.

El *Firewall* filtra fent un examen de les capçaleres de tots i cada un dels paquets utilitzant unes regles fixades per l'usuari. Es a dir utilitza una política de seguretat que decideix quins paquets es poden acceptar, modificar o bloquejar.

Un *Firewall* no examina els paquets dintre de la mateixa xarxa, per això es important que una gran empresa disposi de diferents *Firewalls*, (per a departaments, ...), a fi de garantir un nivell de seguretat òptim.

Existeixen dos tipus de *Firewalls*:

- ***Firewalls* de programari**, que és una aplicació integrada o afegida al sistema operatiu. Les actualitzacions d'aquets *Firewalls* acostuma a ser manual i poc transparent.
- ***Firewalls* físics**, que és la combinació de maquinari i programari específic per a la funció i política de seguretat ja preconfigurats i les actualitzacions són automàtiques.

### 2.2.2 Tipus de filtratge

Els filtres són petits programes dissenyats per acceptar, modificar o bloquejar l'accés a continguts no desitjats d'Internet. Tenen dos components: la classificació i el filtratge.
Cal classificar el contingut abans d'aplicar un filtratge, d'aquesta manera podem establir que s'ha de fer.
La classificació dels filtres podem establir-la en:

- **Sistemes autònoms** (subministrats pel venedor de programari). Es a dir en els sistemes autònoms els criteris els fa el venedor. Aquests sistema s'instal·la com qualsevol aplicació o be a un equip personal, encara que també hi ha aplicacions de xarxa, amb la finalitat de bloquejar l'accés a determinats llocs web a tots els usuaris de la xarxa.
- **Sistemes basats en diferents protocols** (programari que no conté cap informació especifica sobre els llocs que seran bloquejats, i fa servir estàndards establerts per comunicar la informació a traves de Internet). Els sistemes basats en protocols saben com interpretar la informació. Els criteris els determinen estàndards establerts. Aquest mètode fa servir dos tipus de filtratge per bloquejar l'accés: les llistes negres (llista explicita dels llocs web no acceptats) i les cerques per paraules clau (si el sistema troba una paraula clau, bloqueja el lloc al que s'està intentant entrar).

### 2.2.3 Politiques de seguretat

Tots els *Firewalls* es regeixen per una política de seguretat definida prèviament. Quan parlem de política de seguretat estem fent referència a les accions que s'hauran de realitzar com a resposta a l'anàlisi de les capçaleres realitzades als paquets.

Es comparen els paquets un a un amb cada regle de la llista fins a trobar una coincidència. Si no es troba cap coincidència llavors s'aplica la directiva predeterminada.

Hi ha dues politiques de seguretat bàsiques:

- Denegar tot de forma predeterminada i permetre passar sols els paquets seleccionats de forma explicita.
- Acceptar tots els paquets i denegar que passin els paquets seleccionats de forma explicita.

La política de denegar tot és la proposta més segura i que implementarem generalment. Tindrem que habilitar cada servei coneixent el protocol de comunicacions.
La política d'acceptar tot ens fa inicialment la feina molt més senzilla, però ens obligarà a tenir la previsió d'imaginar tots els accessos que volem negar. El perill apareix si no som capaços de preveure un accés perillós i ens adonem quan ja és massa tard. Acceptar-ho tot ens pot facilitar la aparició d'errors.

La política que implantarem al nostre *Firewall* serà la de denegar tot, doncs aporta més seguretat, facilitat en la realització i menor numero de regles.
El filtratge web te les funcions següents:

- Bloqueig de finestres emergents i anuncis.
- Bloqueig de scripts.
- Protecció de privacitat

En el següent esquema podem veure un esquema de la funcionalitat d'un Firewall alhora d'acceptar o bloquejar el tràfic.

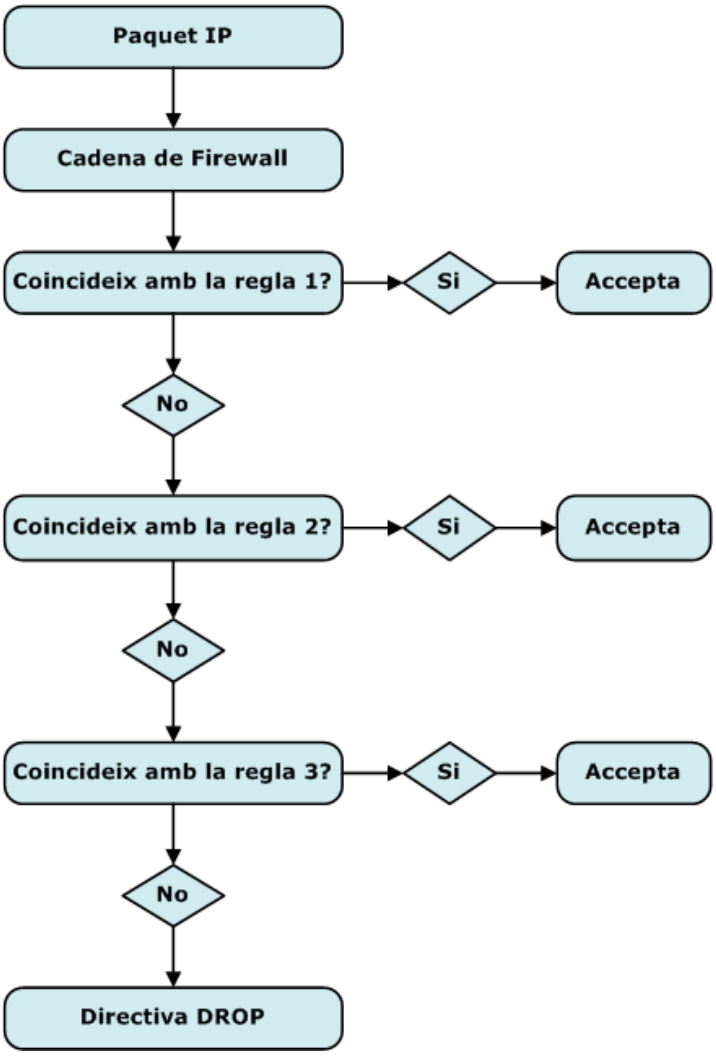


**Figura 8 : Esquema del Funcionament de les regles d'un Firewall**

### 2.2.4 Plataforma Linux

El S.O. Linux proporciona programes i eines suficients per a la gestió de filtres.

El programa que s'encarrega del filtratge s'anomena netfilter, i l'eina per a la gestió que proporciona les regles de filtratge s'anomena iptables. Les accions encarregades són dues drop (descarta i deixa que el paquet es perdi), i accept (deixa passar el paquet al seu destí).

Aquestes eines són molt amplies i de gran capacitat, permeten realitzar una gran quantitat de filtres. La dificultat per a la correcta utilització d'aquestes eines és molt alta. Les politiques de filtratge utilitzen Iptables per afegeix i eliminar regles de la taula de filtratge del nucli de Linux. "Squid + SquidGuard" és una aplicació que permet gestionar de forma senzilla llistes negres i denegar l'accés a llocs web coneguts.

### 2.2.5 Plataforma Microsoft

El S.O. Windows disposa de Microsoft *ISA* Server, un aplicatiu que sol funcionar sota Windows Server 2003 i que proporciona Proxy i Firewall en el mateix producte.

Normalment en les empreses s'utilitzen diferents sistemes de seguretat, compaginant cadascun d'ells per a una millor privacitat de la xarxa. Com si es tractes d'una ceba, cadascuna de les capes de la torre OSI es controlada per una gran varietat de sistemes de seguretat. En el nostre laboratori hem implementat la seguretat mitjançant *ISA* server, però hi ha una gran varietat de competidors en el mercat, que moltes vegades proporcionen ajudes complementaries a la seguretat.

A continuació resumiré breument les principals diferencies de ISA Server amb els seus principals competidors en el mercat.

- ***ISA* Server i Checkpoint**

Checkpoint és un dels grans del mercat a nivell de seguretat. Controlen el 48% de la distribució de *Firewalls* a nivell mundial. A diferencia de *ISA* Server, checkpoint funciona sota qualsevol Sistema Operatiu. Un dels principals inconvenients és el seu alt cost, ja que hem de comprar llicencies segons la quantitat d'*IPs* i cadascun dels extres que hi volem afegir comporta un cost afegit. Si volem incorporar VPN segura, o altres funcions com Web cache, hem de tornar a pagar llicencia per cadascun dels addons que afegim. *ISA* Server ja porta incorporat moltes d'aquestes aplicacions, sense cap extra cost.

- ***ISA* Server i Cisco PIX**

Un altre dels grans de la seguretat és Cisco. El 34% del mercat de *Firewalls* integrats amb el hardware els pertany. Cisco PIX té l'avantatge d'utilitzar el seu propi sistema operatiu, afegint un punt positiu a la seguretat, ja que només Cisco PIX utilitza aquest sistema, i per tant no estan tan exposats a problemes de seguretat com Windows. Un dels inconvenients de Cisco PIX és que malgrat tenen una interfase gràfica per facilitar la configuració, *ISA* server es molt més intuïtiu alhora de configurar, per exemple, les VPN. Una funcionalitat com Web cache, inclosa en *ISA* server, no esta inclosa en Cisco PIX i per tant implica un cost extra per a l'empresa.

# 3. L'escenari

En aquest apartat descriurem l'escenari proposat. Les màquines, aparells que en formen part i els serveis implementats.

En el nostre esquema hi ha dues xarxes molt diferenciades, la xarxa laboratori amb el domini uoclab.com i la xarxa domestica que normalment utilitzem a casa, tan jo com la meva família. Per a no comprometre la funcionalitat de la xarxa domestica en el moment de realitzar els jocs de proves, aquesta va estar quasi totalment al marge, per tant tot es va centrar en la xarxa laboratori. També cal destacar els usuaris VPN que externament s'associen a la xarxa laboratori (uoclab.com), simulant d'aquesta manera aquells treballadors que estan autoritzats a treballar des de fora de la nostra oficina fictícia. Aquests clients assoleixen les *IPs* com si estiguessin connectats directament a la Xarxa Laboratori.
Les principals característiques de les xarxes són:

- Les *IPs* son de classe C, ja que ens proporciona 65,536 hosts, els quals son més que suficients per al nostre laboratori, no necessitant d'aquesta manera, la utilització de classes B o A
- La mascara de la xarxa es 255.255.255.0, proporcionant 254 host utilitzables.

A continuació podem veure una taula resum amb les dues principals xarxes:

| ***Nom de la Xarxa*** | ***Rang d'ips*** | ***Funció*** |
|---|---|---|
| Xarxa No Laboratori | 192.168.1.0/24 | Ús Domèstic |
| Xarxa Laboratori | 192.168.2.0/24 | TFC |

**Figura 9 : Xarxes del treball**

A la xarxa No laboratori s'hi trobem els ordinadors d'ús domèstic que no han format part del laboratori directament, però si que d'una manera indirecta la xarxa a la qual pertanyen. En aquesta xarxa s'hi troba també el router, l'encarregat de donar accés a Internet a tots els Pcs de les dues xarxes. Una altre punt important és el nostre servidor *ISA, ja que* té connectada una de les NIC (Network Interface Card) a la xarxa domestica, per així poder encaminar els paquets de la xarxa laboratori que hagin de sortir a l'exterior, enviant-los al router i aquest últim a Internet.

Pel que fa a la xarxa Laboratori hi trobem en primer lloc un servidor anomenat W2003, el qual és el controlador del nostre domini uoclab.com. Totes les màquines estan associades al domini mitjançant Active Directory, per tant, es realitza una autentificació a nivell de AD cada vegada que un usuari accedeix a un ordinador utilitzant les seves credencials. El servidor W2003 també ens ofereix altres serveis com: servidor de noms o DNS i servidor d'assignació d'adreces IP automàtiques o DHCP. En aquesta xarxa també hi trobem el servidor Linux, el qual ens ofereix serveis com el Web a nivell intern i Correu, malgrat aquests serveis siguin més aviat secundaris en el nostre anàlisis.

El punt més important per al nostre treball és el servidor ISA04, funcionant sota Windows Server 2003 i utilitzant l'aplicació de Microsoft ISA Server 2004 com a Firewall i Proxy.

Finalment en la xarxa Laboratori hi trobem el Client1, un ordinador amb Windows XP que com tota la resta, forma part del domini i és l'encarregat de realitzar els jocs de proves, per a comprovar que la funcionalitat del Firewall i del Proxy.

Tot seguit podem veure una taula amb cadascuna de les màquines utilitzades i la seva respectiva informació:

| ***Xarxa*** | ***Host*** | ***Rang d'adreces*** | ***Sistema Operatiu*** | ***Funció*** |
|---|---|---|---|---|
| No Laboratori | Diversos | 192.168.1.x/24 | Diversos | Ús Domèstic |
| No Laboratori | ISA04 | 192.168.1.100/24 | Windows Server 2003 | Encaminar uoclab amb router |
| No Laboratori | Router | 192.168.1.1/24 | Firmware Propi | Porta d'enllaç |
| Xarxa Laboratori | ISA04 | 192.168.2.1/24 | Windows Server 2003 *ISA* Server 2004 | *Firewall*,Proxy,NAT |
| Xarxa Laboratori | W2003 | 192.168.2.2/24 | Windows Server 2003 | Controlador domini, DHCP, DNS |
| Xarxa Laboratori | Ubuntu | 192.168.2.3/24 | Ubuntu Linux | Web, Correu, FTP |
| Xarxa Laboratori | Client1 | 192.168.2.x/24 | Windows XP | Client |
| Xarxa Laboratori | Client VPN | 192.168.2.x/24 | Windows XP | Client VPN |

**Figura 10 : Ordinadors i maquinaria de les xarxes**

## 3.1 Esquema il·lustratiu

Visualitzem en modus gràfic l'escenari que es va implementar i l'esquema de direccions IP de les maquines.

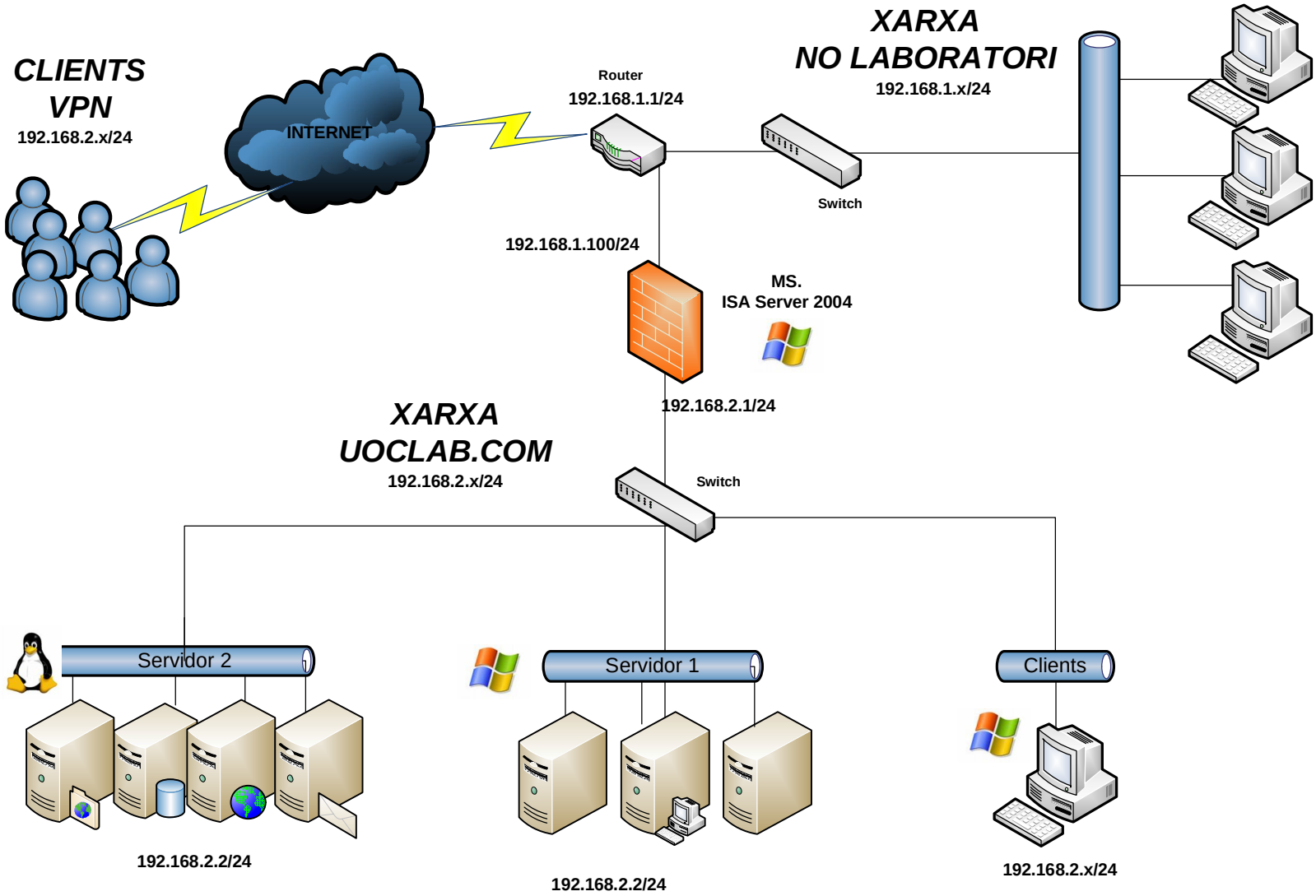


**Figura 11 : Esquema Il·lustratiu de la xarxa**

# 4. Els Servidors

Els apartats següents descriuen els serveis a utilitzar per la xarxa que podrem trobar a l'escenari proposat. Com en totes les distribucions Debian disposem de la instrucció:

*apt-get install nom_programa*

per descarregar, instal·lar i actualitzar el programari.

En quan als serveis que corren sota Windows Server 2003, l'activació es totalment gràfica. Cadascun dels servidors estan implementats en un servidor Ubuntu Linux i Windows Server 2003.

## 4.1 Servidor Controlador de Domini

Es el servidor encarregat de controlar el domini de la nostra xarxa i el respectiu arbre del Active Directory, en aquest cas, uoclab.com és el nostre domini. El controlador de Domini està funcionant amb Windows 2003 i el seu nom dins de la nostre xarxa és w2003.

## 4.2 Servidor de Noms DNS

Les màquines en una xarxa TCP/IP les podem identificar per la seva adreça IP de 32 bits. Com és molt més fàcil recordar el nom de la màquina, el servidor associa una IP amb un nom de màquina. Windows Server 2003 ja porta incorporat un servei de DNS. L'activem per a que comenci a respondre les peticions DNS de la nostra xarxa. Aquest servei utilitza el port 53.

Al voler automatitzar la configuració dels exploradors webs amb el Proxy s'ha afegit un CNAME en la llista del nostre servidor DNS, d'aquesta manera quan algú pregunti per WPAD (automatització d'opcions del proxy), el servidor DNS respondrà amb la direcció del ISA04 i a on estar el fitxer per l'automatització de les opcions del proxy.

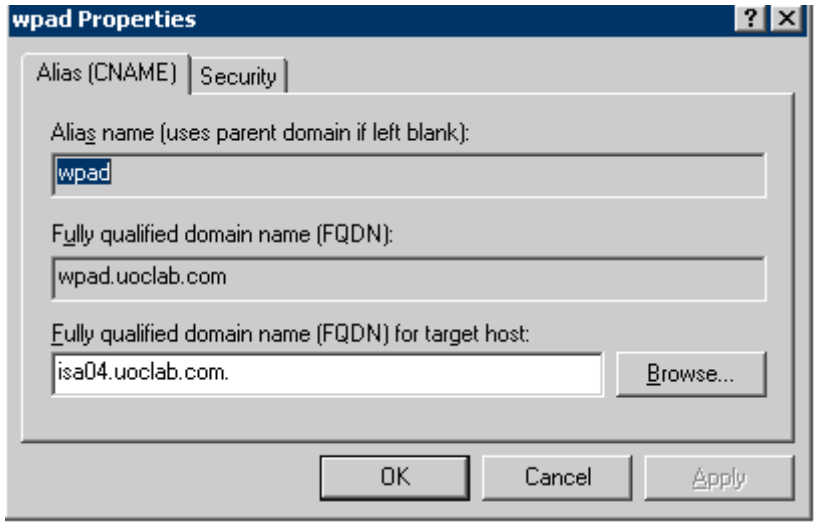


**Figura 12 : Propietats de l'entrada wpad en el servidor DNS**

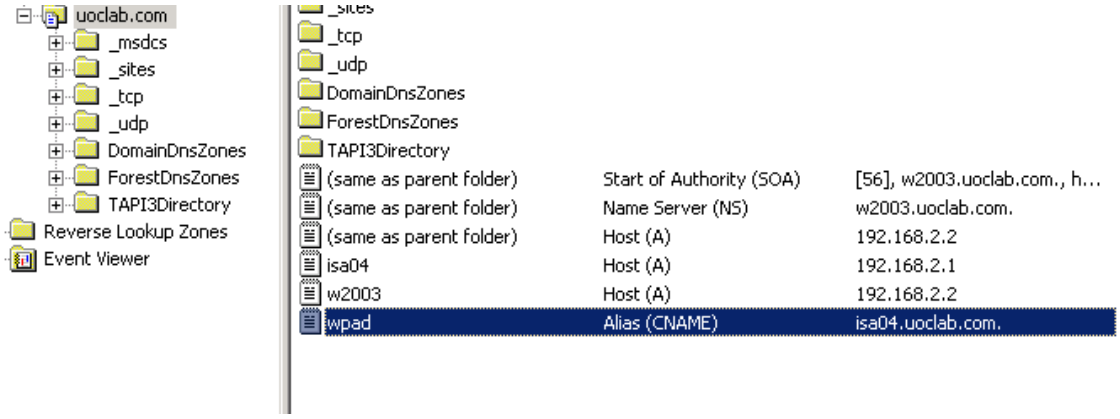


**Figura 13 : Llista de les entrades en el servidor DNS**

## 4.3 Servidor DHCP

El servei DHCP proporciona a les màquines de la nostra xarxa interna una adreça IP, una mascara, una porta per sortir a l'exterior i la direcció on es troba Wpad. Aquest servei utilitza el port 68.

Windows Server 2003 ja porta incorporat un servei de DHCP. L'activem per a que comenci a oferir *IPs* als nostres clients de la xarxa interna. El servidor DHCP en el nostre laboratori està oferint a més a més WPAD per automatitzar la configuració dels clients proxys, com anteriorment ha estat comentat en el servidor DNS. A continuació veiem com s'ha realitzat aquesta tasca de WPAD.

Com podem observar, el servidor DHCP quan assigna *IPs* està oferint alhora, quina és la porta d'enllaç (el ISA04), qui es el servidor DNS (w2003) i finalment qui es el que ofereix el fitxer Wpad. Per a realitzar aquesta tasca hem creat una nova opció i s'ha afegit wpad a les opcions de DHCP per a que tingui efecte. La opció Wpad utilitza el codi 252.

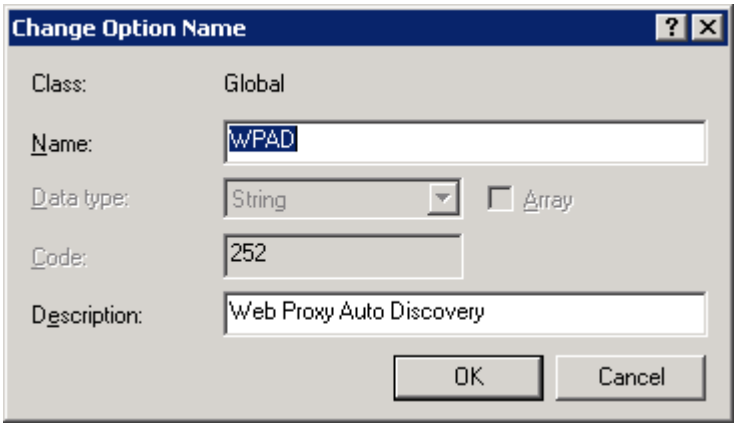


**Figura 14 : Propietats de l'opció creada WPAD en el servidor DHCP**

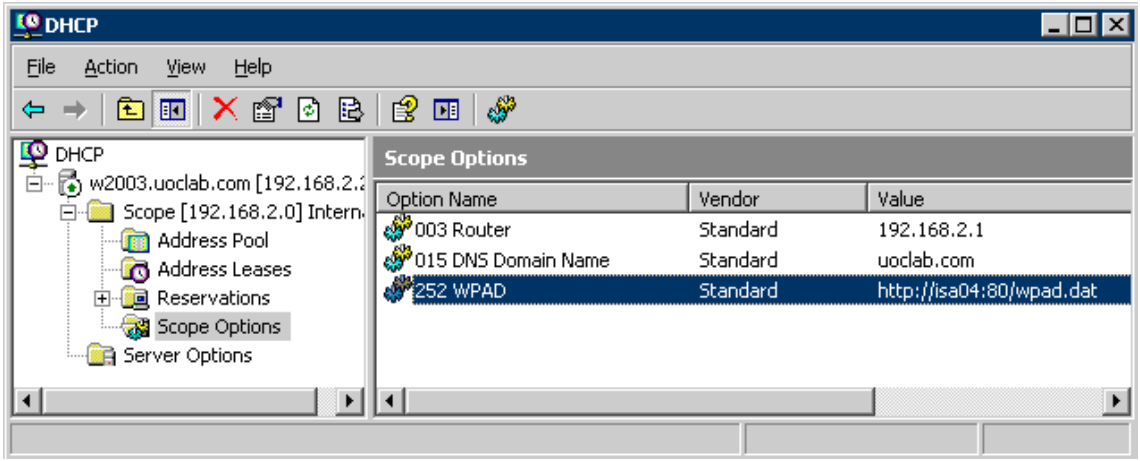


**Figura 15 : Visualització del servidor DHCP i de les opcions**

## 4.4 Servidor Proxy/*Firewall*: *ISA* Server 2004

Aquest servidor és l'encarregat de controlar la seguretat de la xarxa i el filtratge web dels clients associats. Funciona amb Windows Server 2003 i està dins del nostre domini uoclab.com. Està configurat per a utilitzar les tres opcions funcionals que *ISA* server ens ofereix, *SecureNAT*, Web Proxy i *Firewall*.

A nivell de hardware disposa de dues targetes Ethernet. La primera anomenada Externa, és la connexió que ens proporciona accés amb l'exterior de la nostre xarxa laboratori, permetent

accedir a la real xarxa domestica i al router que ens dona accés a Internet. La segona targeta Ethernet, anomenada Internal, és la connexió a la xarxa de laboratori on estem realitzen totes les proves.

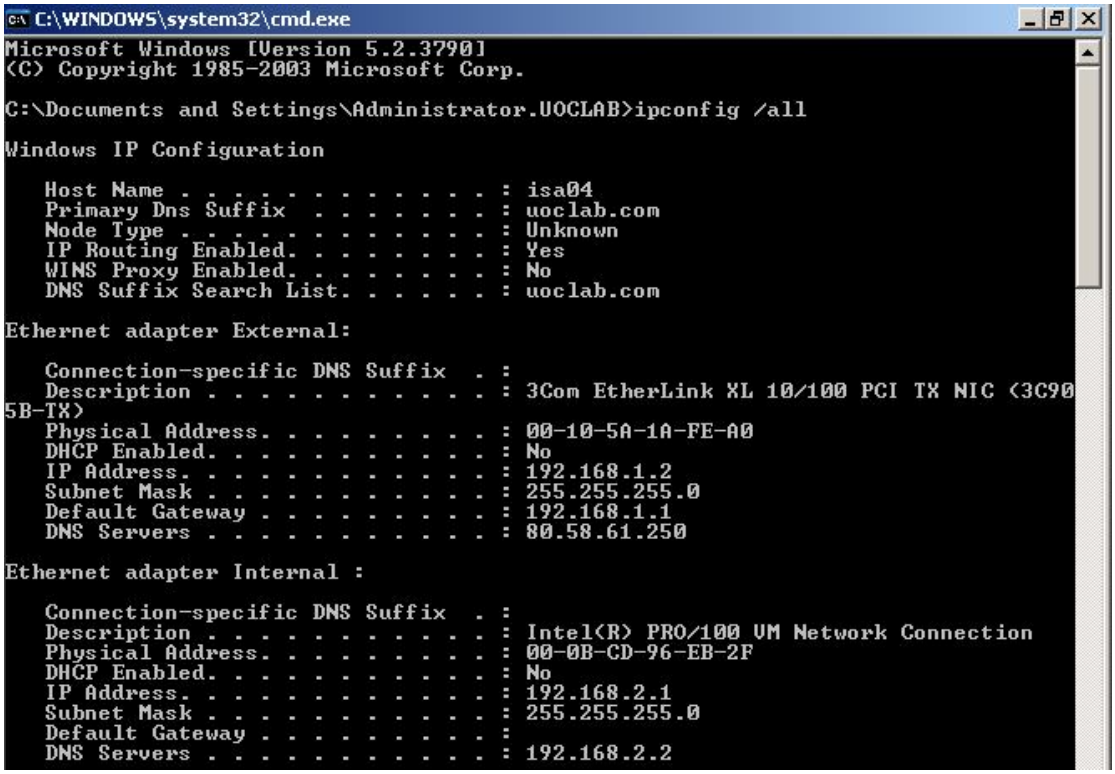


**Figura 16 : Imatge de la configuració del servidor ISA04**

Un punt important és veure que el primer adaptador de xarxa Internal no disposa de cap porta d'enllaç assignada per evitar problemes de redundància, ja que el mateix servidor és la seva pròpia porta d'enllaç. En canvi en l'adaptador de xarxa External, hem assignat la IP del router de Telefónica, per a permetre al *ISA* server encaminar totes les peticions am destinació Internet.

En el nostre *ISA* Server 2004 existeix per defecte una regla del *Firewall*, la qual denega tot el tràfic, d'entrada o sortida, amb destinació qualsevol, per tal de bloquejar tot allò que no estigui permès per una altre regla. Per tant, la política per defecte es la de bloquejar-ho tot.

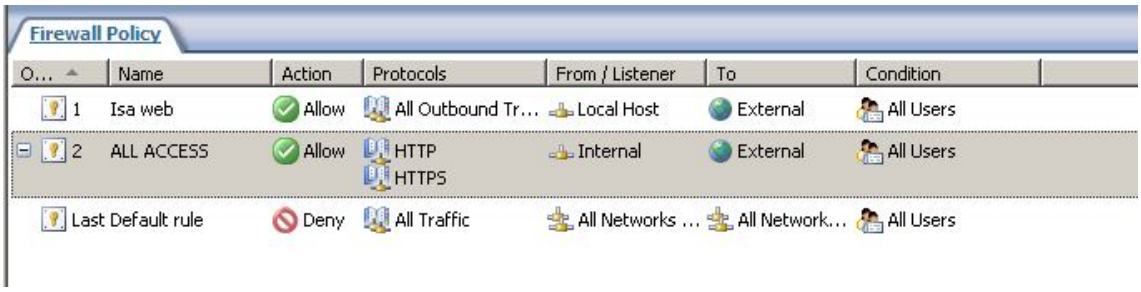


**Figura 17 : Politiques de Seguretat del Firewall**

La primera regla, anomenada *ISA* Web, es va implementar per tal de permetre al nostre *ISA04* la navegació web per Internet, malgrat no es una activitat normal utilitzar *ISA* Server per a navegar via web, a causa de la perillositat de comprometre tot el servidor a nivell de seguretat. Aquesta activitat també es podia haver realitzat sense la necessitat d'aplicar una regla nova, simplement activant el protocol http/https des de les politiques per defecte del servidor, la qual ens proporciona la mateixa funcionalitat. La raó principal d'habilitar la navegació web pel servidor ISA04 va ser la necessitat d'estar consultant informació contínuament a Internet per realitzar la correcta configuració del Firewall.

La segona regla es l'encarregada de permetre el tràfic web des de la xarxa interna a l'exterior, per tal de que els nostres clients puguin navegar via web, autoritzant els protocols http/https a sortir a l'exterior.

### 4.4.1 Bloqueig de Pàgines web

Un dels grans beneficis de *ISA* Server 2004 es l'habilitat de bloquejar accés a qualsevol web URL o domini que per politiques de seguretat, es cregui convenient bloquejar, ja sigui per evitar que els treballadors realitzin tasques no laborals o navegar per webs on puguin comprometre la seguretat de la xarxa, infectant les estacions de treball amb spyware o altres codis mal intencionats.

Un dels principals problemes alhora de configurar aquestes llistes estàtiques, es la dinamització de moltes webs a canviar el host en pocs períodes de temps. Avui un domini que es vol bloquejar anomenat www.sexe.com, potser demà s'anomenarà www.porno.es, per tant, la nostra llista ja no funcionaria alhora de denegar el nou dominiAmb això no es vol dir que sigui incoherent utilitzar aquest mètode de filtratge, simplement es vol deixar clar que ho hem d'aplicar com una eina complementaria per tal d'ajudar als administradors en la seguretat de la xarxa, però mai com a una solució única i definitiva.

Hi ha moltes llistes per Internet que podem utilitzar en els nostres *Firewalls amb* tot un seguit de webs a bloquejar. En la implementació del ISA04 es va decidir descarregar una llista qualsevol per a fer el joc de proves, per així disposar d'un exemple pràctic:
*http://www.tacteam.net/isaserverorg/download/blocklists.zip.*

Per a poder implementar aquesta regla de bloqueig web, el primer que es va realitzar és la importació dels arxius que ens hem descarregat a l'apartat de URL Sets, com podem veure a continuació:


**Figura 18 : Creació d'un Grup de URLs**

Un cop es troba l'arxiu *.xml simplement cliquem a importar, i ja tindríem la llista preparada per ser utilitzada. El fitxer BNSD es va utilitzar com a llista de dominis, i per realitzar aquesta tasca s'ha fet el mateix procediment anterior però enlloc d'importar-ho a URL Sets s'ha importat a Domain sets.

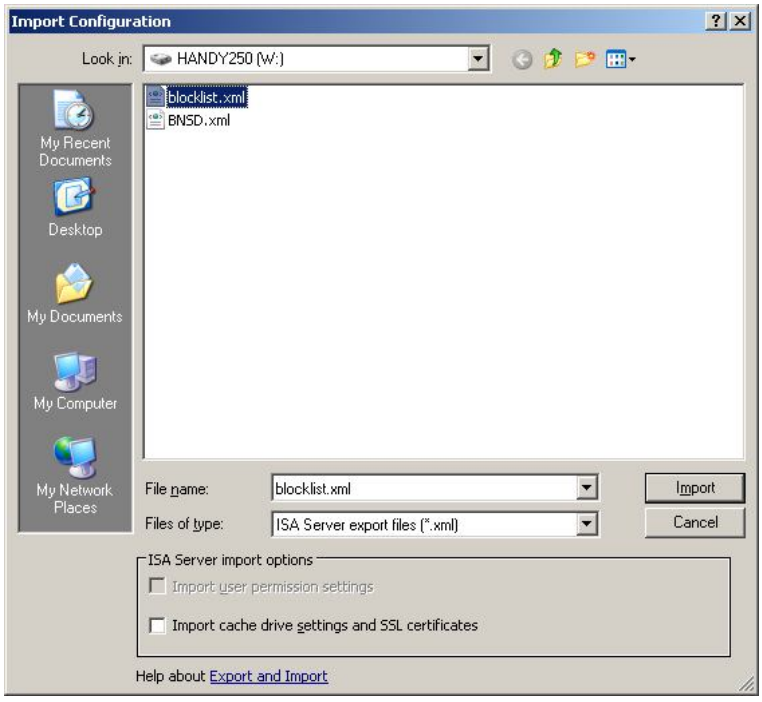


**Figura 19 : Localització de les llistes XML**

Ara bé, un cop es tenen les llistes en el nostre *ISA* es van definir les noves regles per a denegar-hi l'accés.

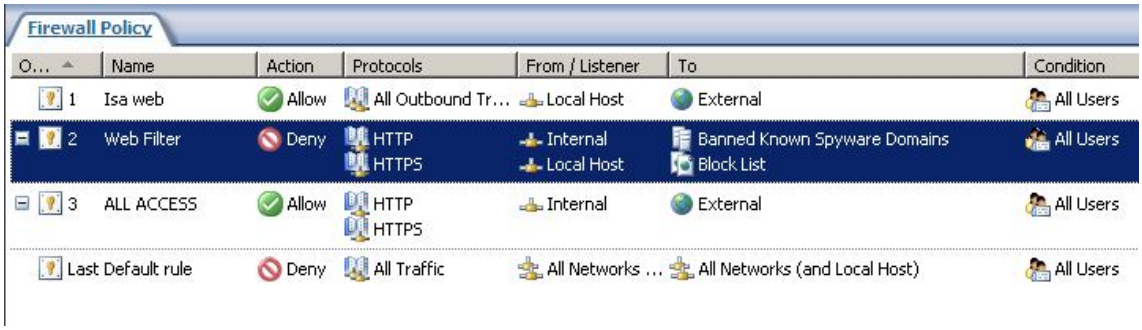


**Figura 20 : Llista de les politiques del Firewall**

La regla anomenada Web Filter es l'encarregada de bloquejar l'accés de tots els nostres clients cap a dominis i webs concretes que hem considerat perilloses o fora de l'ús corporatiu, anteriorment importades en arxius xml. Com es pot observar es va decidir col·locar la regla abans de la que permet l'accés web, ja que d'aquesta manera *ISA* processa primer les negacions i en cas de no estar en les llistes negres, decideix saltar de regla i permetre l'accés. Si s'hagués col·locat al invers, *ISA* server permetria l'accés abans que comprovar si l'ha de denegar, el qual no ens interesaria. Aquesta regla en concret esta bloquejant el tràfic procedent de la xarxa interna i del mateix *ISA* cap a qualsevol de les dues llistes que hem importat. Com la principal funció de la regla es bloquejar via web, es van triar els protocols HTTP i HTTPS, sense voler denegar tot el tràfic de sortida, evitant sobrecarregar d'aquesta manera que el *Firewall* estigui contínuament comprovant el tràfic de sortida que no és http/https.

### 4.4.2 Bloqueig d'aplicacions

Una altre de les regles que normalment s'apliquen en escenaris corporatius es el bloqueig d'aplicacions com emule, torrent o MSN Messenger. Aquestes eines abans eren molt senzilles de bloquejar, ja que només feia falta saber els ports on corrien i dir-li al *Firewall* que tanques aquests ports, per així evitar el seu ús dins de la nostra xarxa corporativa. Ara bé, tot això ha canviat lleugerament, les aplicacions van evolucionar i són capaces de realitzar una tecnica coneguda port tunneling. Aquesta técnica consisteix en canalitzar la seva informació via el port 80, el port web, el qual normalment sempre està obert, i per tant, permeten així esquivar la seguretat dels firewalls que es basaven en bloquejar els ports concrets. A dia d'avui això ha estat solucionat i es una de les regles es van decidir implementar en la xarxa laboratori.

Aquesta tasca consisteix en bloquejar el tràfic mitjançant les signatures o capçaleres dels paquets TCP. A continuació podem veure una taula de les aplicacions més comunes segons Microsoft i de la informació necessària per al bloqueig de cadascuna. La taula la podem trobar a *http://technet.microsoft.com/en-us/library/cc302520.aspx*.

| Application | Location | HTTP header | Signature |
|---|---|---|---|
| MSN Messenger | Request headers | User-Agent: | MSN Messenger |
| Windows Messenger | Request headers | User-Agent: | MSMSGS |
| Netscape 7 | Request headers | User-Agent: | Netscape/7 |
| Netscape 6 | Request headers | User-Agent: | Netscape/6 |
| AOL Messenger (and all Gecko browsers) | Request headers | User-Agent: | Gecko/ |
| Yahoo Messenger | Request headers | Host | msg.yahoo.com |
| Kazaa | Request headers | P2P-Agent | Kazaa<br>Kazaaclient: |
| Kazaa | Request headers | User-Agent: | KazaaClient |
| Kazaa | Request headers | X-Kazaa-Network: | KaZaA |
| Gnutella | Request headers | User-Agent: | Gnutella<br>Gnucleus |
| Edonkey | Request headers | User-Agent: | e2dk |
| Internet Explorer 6.0 | Request headers | User-Agent: | MSIE 6.0 |
| Morpheus | Response header | Server | Morpheus |
| Bearshare | Response header | Server | Bearshare |
| BitTorrent | Request headers | User-Agent: | BitTorrent |

| Application | Location | Type | Value |
|---|---|---|---|
| Kazaa | Headers | Request Header | X-Kazaa-Username:<br>X-Kazaa-IP:<br>X-Kazaa-SupernodeIP: |
| BitTorrent | Extensions | None | .torrent |
| Many peer-to-peer clients | Headers | Request Header | P2P-Agent |

**Figura 21 : Signatures de les Aplicacions més comunes**

Amb el botó dret del ratolí, sobre de la regla que permet l'accés http a Internet, veiem l'opció de configurar el protocol http. Si entrem en aquesta opció veurem el següent menú, on podrem configurar les diferents capçaleres i signatures per tal d'evitar la utilització d'aplicacions concretes.

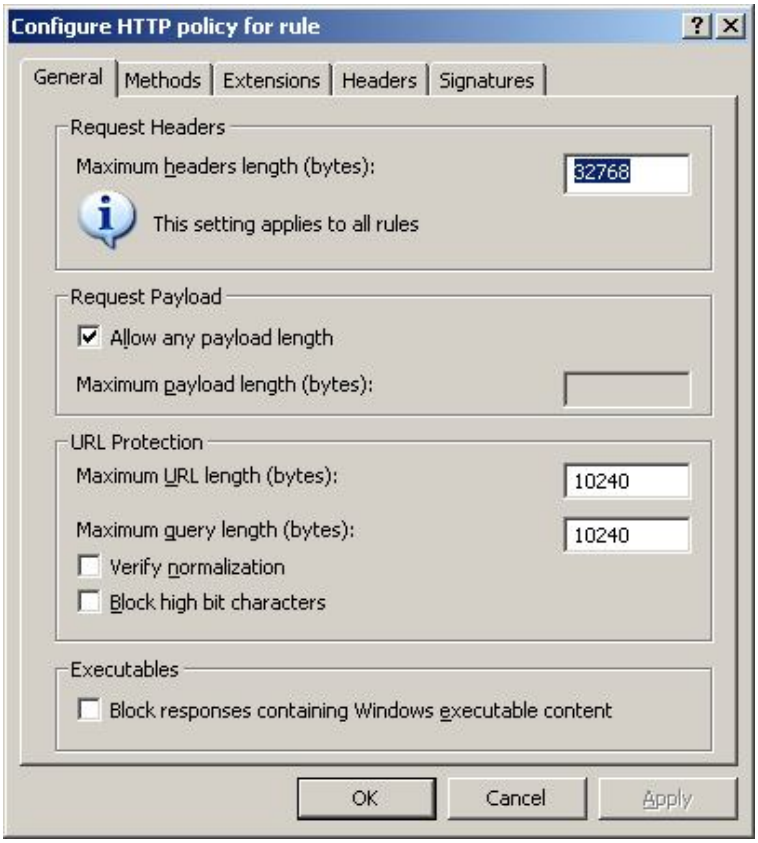


**Figura 22 : Configuracio de regles per al protocol HTTP**

El màxim de la capçalera veiem que hi ha posat per defecte un 32768 bytes, això ve per defecte, amb la finalitat d'evitar el conegut buffer overflow, una tècnica mal intencionada per tal de col·lapsar el sistema, utilitzant capçaleres que l'ordinador no pot processar i s'acabaria col·lapsant.

Finalment, un cop estem a l'apartat de signatures hi agreguem una nova enbtrada i la configurem amb la informació de la taula abans exposada, segons l'aplicació a bloquejar. En el nostre exemple tenim el bloqueig de MSN Messenger.

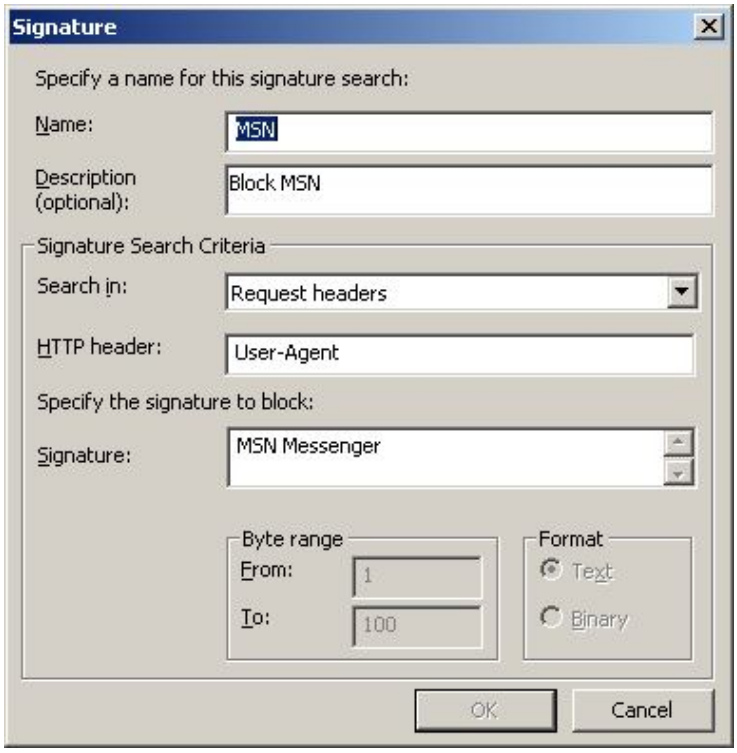


**Figura 23 : Signatures per a bloquejar MSN Messenger**

Per acabar, veiem el llistat de totes les signatures que es va creure oportú configurar per tal d'evitar l' utilització de l'aplicació. En el cas de que es volgués bloquejar aplicacions torrent, emule o d'altres, aquest procés seria el mateix però modificant les signatures a bloquejar

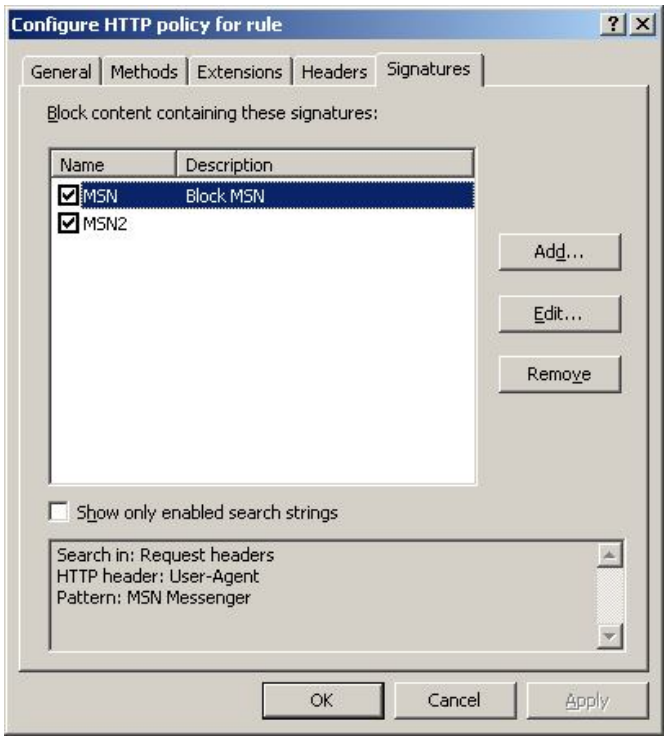


**Figura 24 : Llista de Signatures a bloquejar via HTTP**

### 4.4.3 Habilitar Terminal Server

Durant el treball es van utilitzar bastants ordinadors pel laboratori i va arribar un punt en el que no es disposava de mes cables per utilitzar l' intercanviador de pantalla, teclat i ratolí. A conseqüència d'això es va prendre la decisió d'habilitar una regla per a permetre l'ús de Remote Desktop per administrar els servidors sense necessitat de utilitzar l' intercanviador físic.

Per a crear la regla que ens oferís aquesta funcionalitat es va haver de realitzar una publicació de servidor. Aquesta tasca no es res més que un tipus de regla del Firewall on s'afecta directament a un servidor intern, el qual necessita ser accessible. La seva implementació va ser com totes les anteriors, però enlloc de triar una regla d'accés es va haver de triar una regla de publicació de servidors. Els passos son els mateixos que per a les regles d'accés, però amb la diferencia que s'ha d'especificar quin protocol és l'utilitza't. En el nostre cas va ser el RDP, com es pot observar en la figura 22.

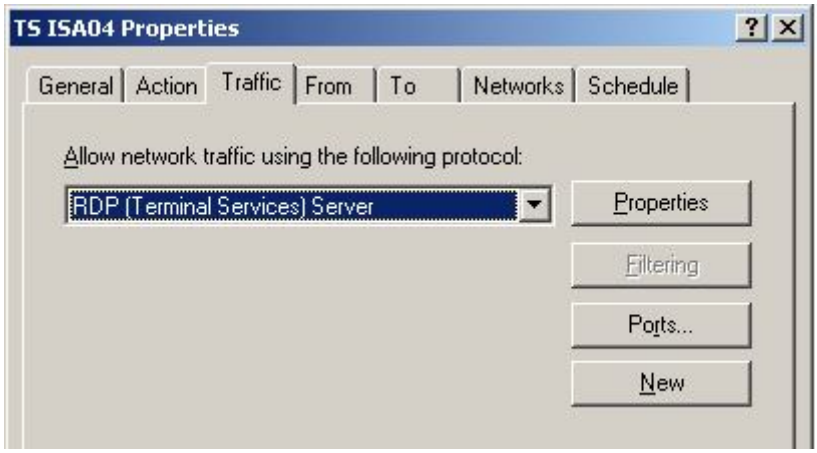


**Figura 25 : Acceptar connexions RDP per a Terminal Server**

Finalment es va assignar la IP del servidor on estàvem autoritzant les connexions RDP, la IP interna del nostra ISA04.

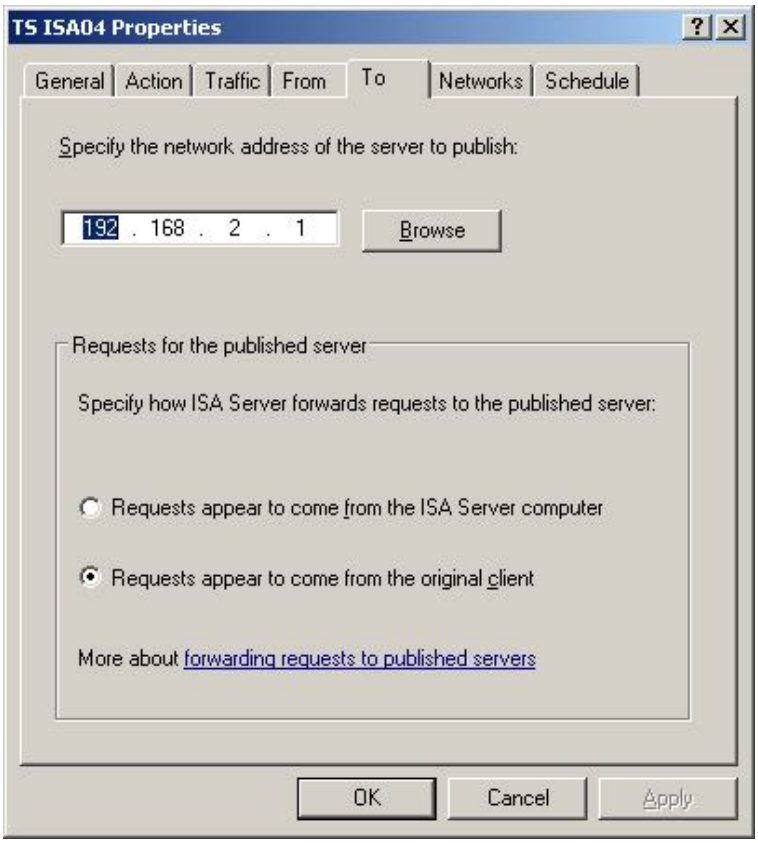


**Figura 26 : Publicació del servidor per a acceptar les connexions**

### 4.4.4 Habilitar VPN

La Xarxa Privada Virtual, en angles Virtual Private Network (VPN), es una tecnologia de xarxa que permet una extensió de la xarxa local sobre una xarxa publica, com per exemple Internet. Normalment s'utilitza per a connectar dues sucursals d'una mateixa empresa, realitzen la connexió a traves d'Internet. Això permet que un treballador, per exemple, pugui concertar-se a la xarxa de la feina, des de casa d'una manera totalment segura i controlada per nosaltres.

Un punt important sobre aquesta tecnologia es que ens permet evitar el alt cost de les xarxes WAN dedicades, fent així ús de les connexions d'Internet quotidianes.

Les principals característiques del funcionament de les VPN son:

- Identificació de l'usuari: les VPN han de verificar la identitat dels usuaris i restringir l'accés a aquells que no siguin autoritzats.
- Codificació de dades: les dades que es transmeten a través de la xarxa pública (Internet), abans han de ser codificades per evitar la seva intercepció i lectura. Aquesta

tasca la realitzen un conjunt d'algoritmes de xifratge, que només el receptor pot desxifrar.

- L'administració de les claus: Les VPN han d'actualitzar les claus de xifratge per als seus usuaris.

En la nostra xarxa laboratori es va implementar la simulació d'aquesta situació tan quotidiana en el món laboral. Les connexions dels clients VPN realitzen connexions directes a ISA04, el qual s'encarrega de sincronitzar la connexió i assegurar-se que els usuaris que han fet la petició de connexió formin part del grup de VPN Clients. Aquest grup d'usuaris són els que estan autoritzat per utilitzar la VPN.

A continuació es pot veure la elecció del tipus de protocols de connexió que activem en la nostra VPN. PPTP es el mètode més Standard per a les connexions VPN i L2TP/IPsec s'utilitza en el moment que implementem la seguretat i el xifrat.

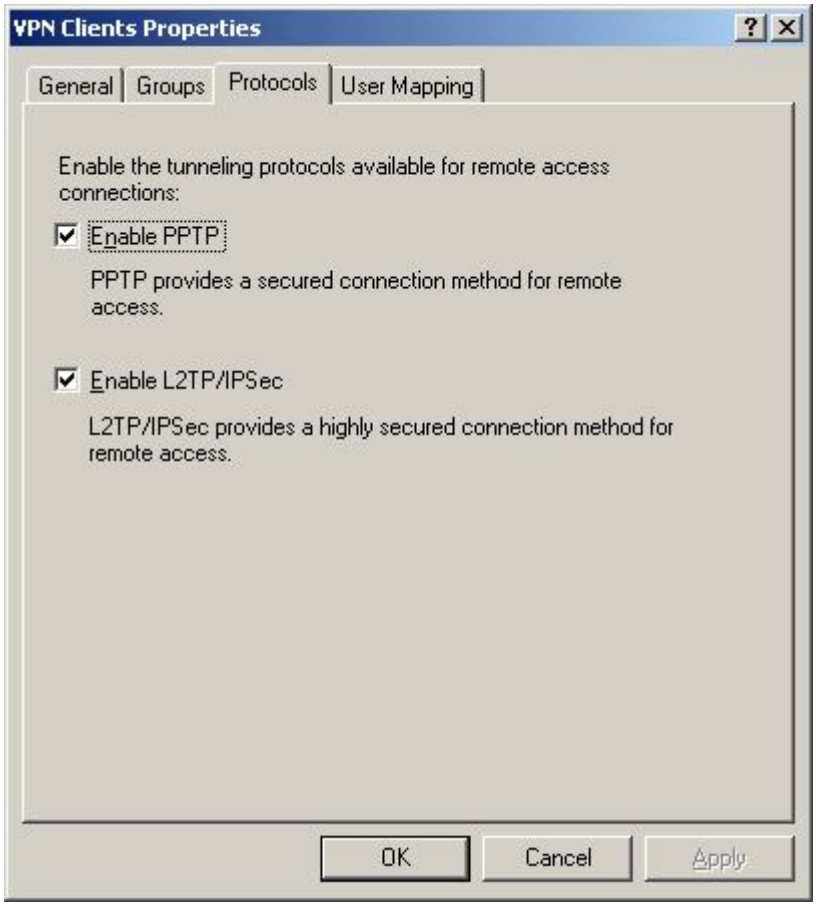


**Figura 27 : Tipus de protocols per a la VPN**

Posteriorment caldria limitar l'ús de connexions a la nostra VPN, per evitar qualsevol tipus d'ús mal intencionat. En el nostra laboratori, es va decidir restringir les connexions a 10 persones com a exemple, però en la vida quotidiana aquest nombre és mol més elevat, tot depenen de les necessitats de l'empresa.

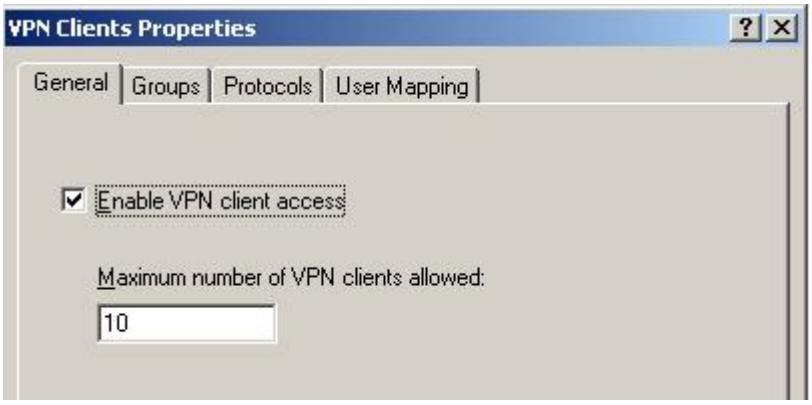


**Figura 28 : Màxim de connexions a la VPN**

Finalment l'últim punt a realitzar en la configuració de la VPN, és agregar al grup VPN Clients en les propietats de la connexió VPN. Ja que si no realitzéssim aquesta tasca, el servidor ISA no podria validar les credencials dels nostres usuaris autoritzats, perquè no hi constaria cap.

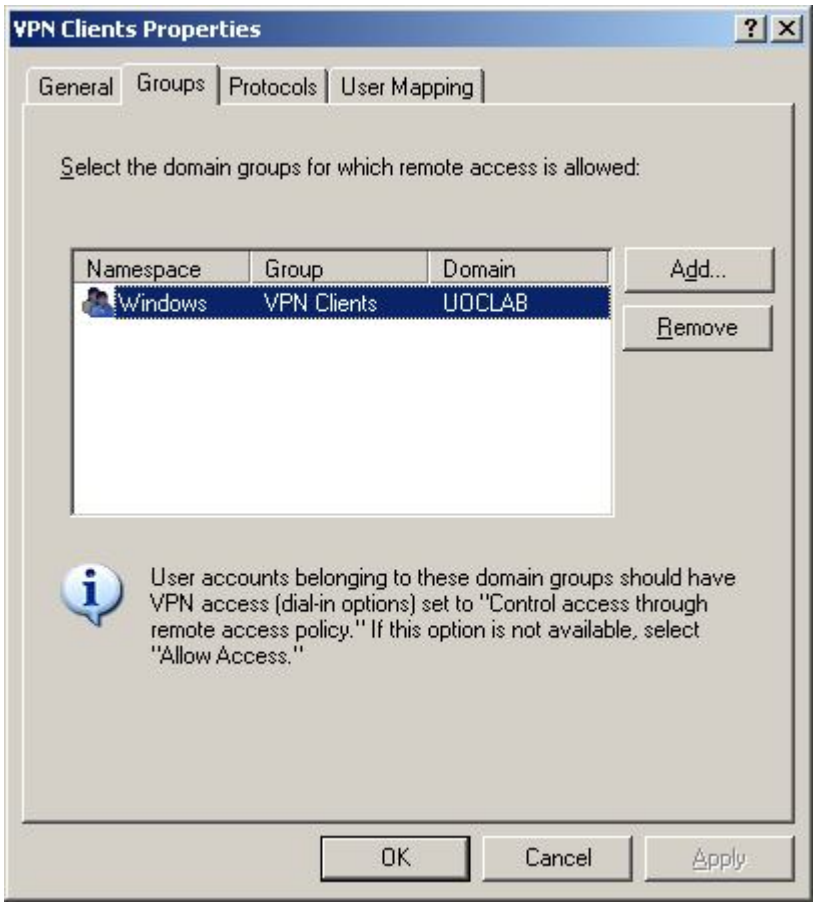


**Figura 29 : Grups autoritzats a utilitzar la VPN**

### 4.4.5 Informació en els fitxers Log

Isa Server 2004 ens proporciona una eina molt important, la coneguda monitorització. Aquesta eina ens permet analitzar visualment el que esta passant en el nostre Firewall en temps real i emmagatzemar-ho en uns fitxer coneguts com logs, els quals podem consultar per a un posterior analisi en cas de necessitat.

A l'inici del treball es comentava com mitjançant un proxy podiem visualitzar, per exemple, aquelles webs que un usuari havia estat visitant, o fins i tot aquells ports i protocols que han establert connexions amb l'exterior. Totes aquestes tasques d'analisi es realitzen mitjançant la visualització dels logs d'informació, utilitzant diferents consultes segons el filtratge que es vulgui realitzar.

Els logs del Firewall i del proxy emmagatzemen tota l'informació sense cap tipus de filtratge, per tant, no seria una tasca sencilla haver d'analitzar la totalitat del fitxer. Per evitar aquesta tasca tan complicada, Microsoft ens ha proporcionat una eina que realitza filtratges mitjançant una consulta (query) al fitxer log. Aquesta consulta diposa d' infinitat d'opcions per a filtrar l'informació segons ens interesi. Com es pot observar a la figura 27, el gran llistat d'opcions per a realitzar les regles de la consulta es variat i ens garanteix l'habilitat de filar molt prim en la nostra recerca d'informació.

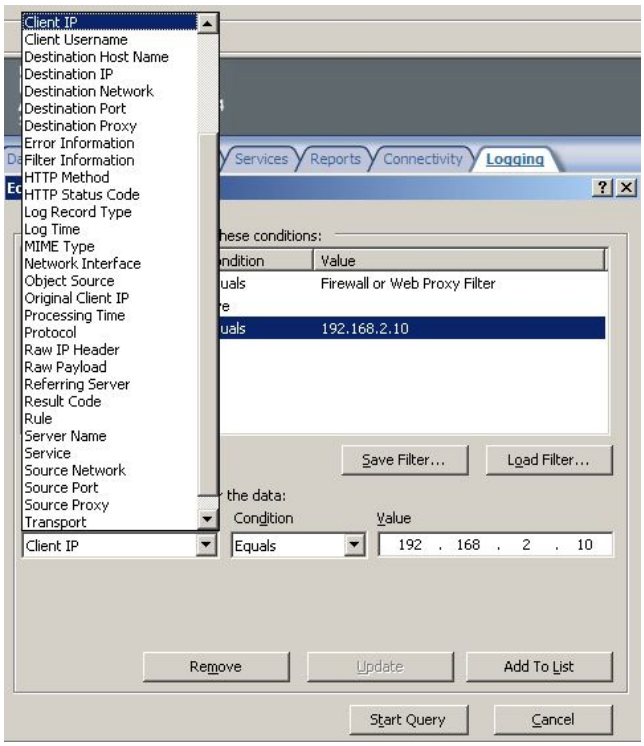


**Figura 30 : Opcions de filtratge de les Querys**

Tot seguit, tenim una imatge on es motra com ISA Server 2004 està mostrant en temps real les pagines web visitades per el nostre servidor W2003. En aquest cas es va realitzar la prova de visitar la uoc i observar com ISA04 ho estava monitoritzan en temps real i emmagatzeman-t'ho en un fitxer log.

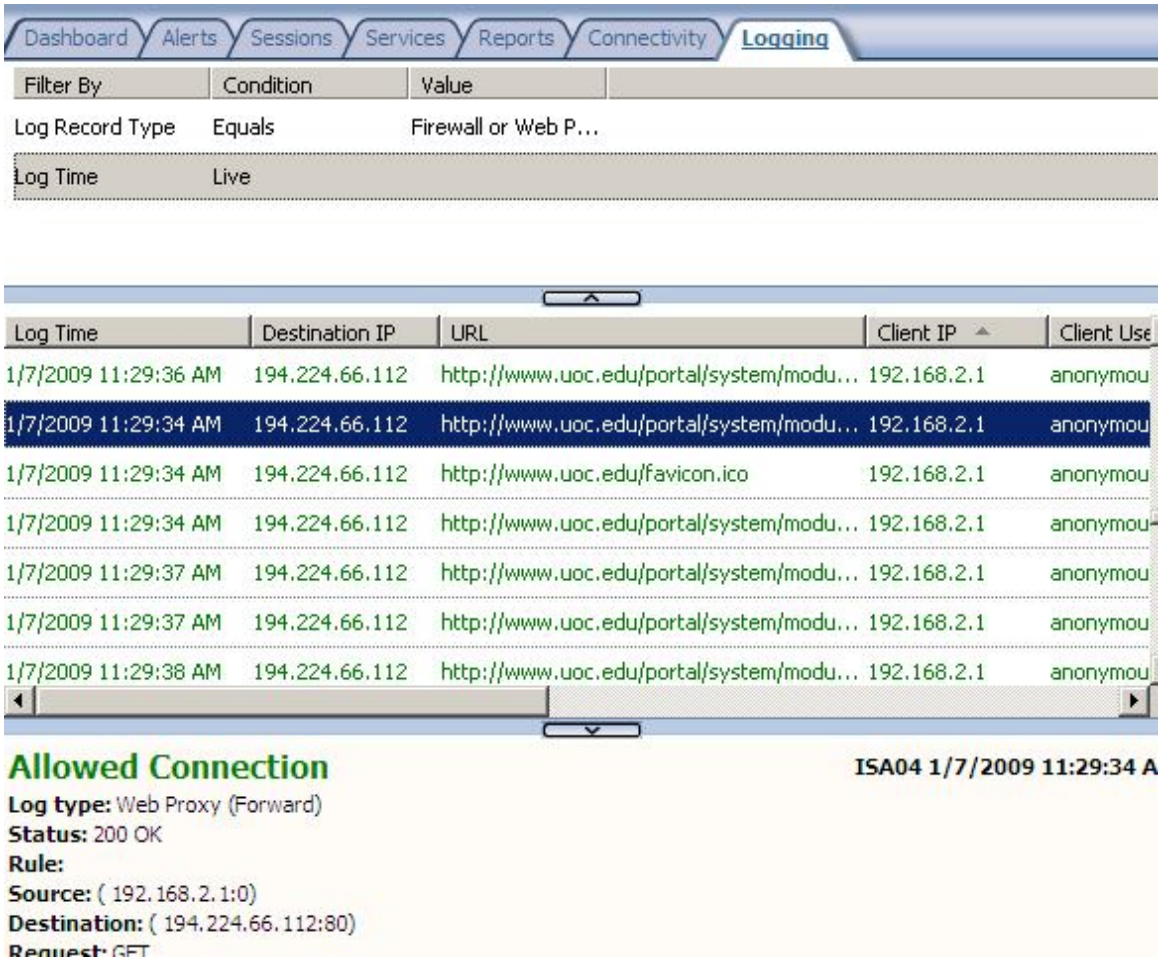


**Figura 31 : Monitorització de les URL visitades**

## 4.5 Servidor Web

El servidor Web més utilitzat a l'entorn empresarial és el servidor *Apache*, amb un us superior al 50%, i és de lliure distribució.

Una de les raons principals perquè APACHE es gratuït, és el ser totalment programat per un conjunt d'entusiastes i voluntaris, els quals sota la bandera de UNIX, el distribueixen amb una llicencia publica GNU. La filosofia dels seus programadors és la gratuïtat i la llibertat total de manipulació del seu codi. Aquest punt, permet per tant, a les empreses aconseguir un servidor

Web sense cost per a llicencies i alhora disposar de l'opció de personalitzar-lo. Els programadors de l'empresa, poden millorar o modificar la funcionalitat de l' Apache, segons les necessitats del negoci. Aquests factors el fan idoni per aquest treball i les nostres proves de laboratori.

*Apache* escolta pel port 80, port del servei Web.

Primer descarreguem i instal·lem el paquet amb la instrucció:

*apt-get install Apache2*

En segon lloc modifiquem el fitxer:

*/var/www/index.html*

Com podem veure a continuació, el arxiu predeterminat es el index.html, el qual esta a la carpeta var/www/index.html. En aquesta posició és on posaríem la nostra web. Tot seguit podem veure una imatge *des de Ubuntu, on es troba l'arxiu index.html.*

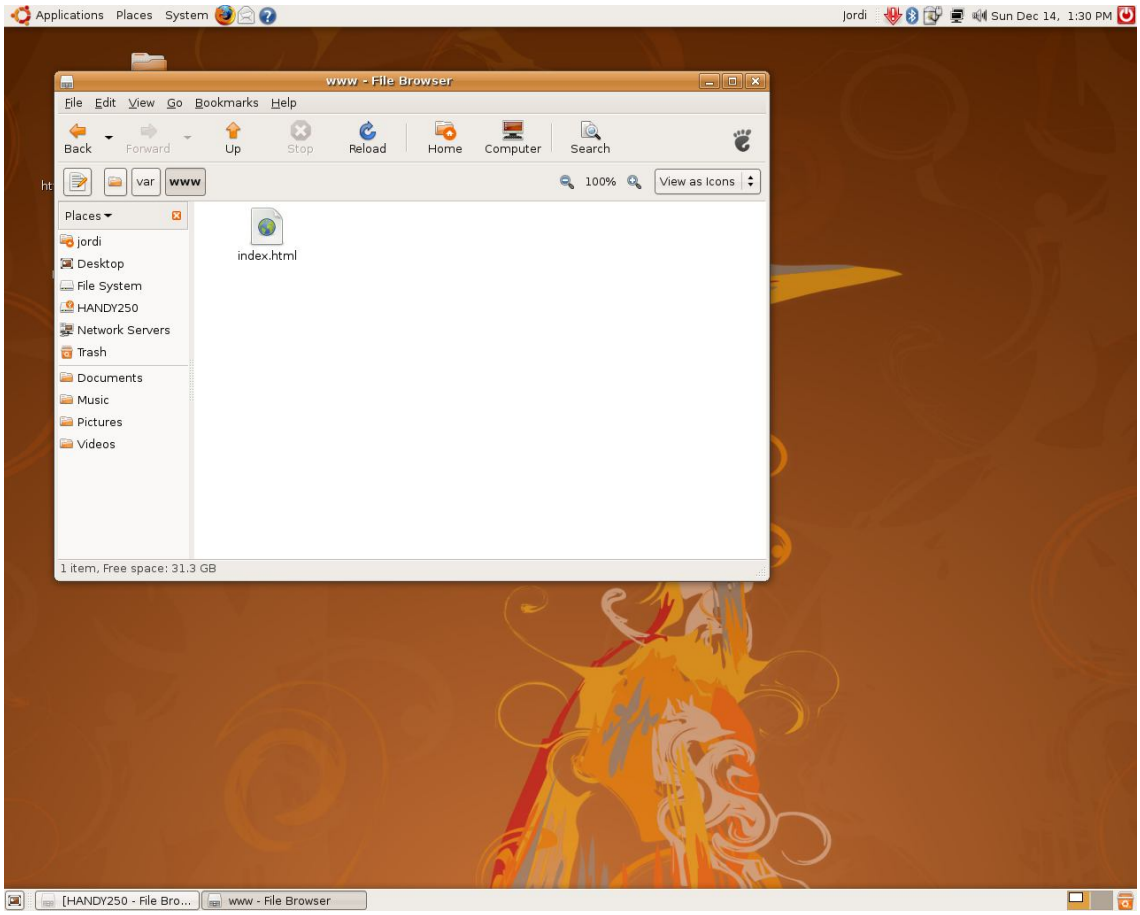


**Figura 32 : Fitxer index.html de Apache a Ubuntu Linux**

Per a concloure, a continuació podem observar una imatge on es mostra com el servidor web esta correctament funcionant a nivell intern (intranet). Si volguéssim que fos accessible per al exterior hauríem de configurar una regla en el *Firewall* per a la publicació d'un servidor web.

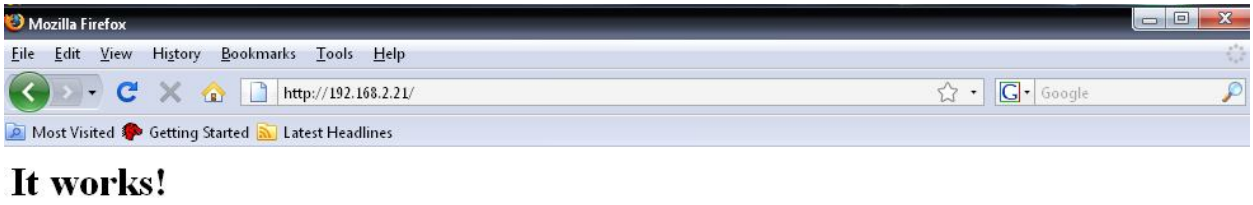


**Figura 33 : Demostració de la funcionalitat d'Apache**

## 4.7 Servidor de correu

Utilitzarem el servidor de correu *Sendmail*, que permet enviar i rebre correu SMTP. Sendmail és un popular agent de transport de correu (MTA - Mail Transport Agent) a Internet, el qual s'encarrega d'encaminar els missatges de correu per a que arribin al seu destí. És un dels més populars sota sistemes Unix, i alhora el responsable de la majoria de correu enviat a traves d'Internet. La raó principal és la mateixa que per al Apache, la lliure distribució i el codi obert.

*Sendmail* queda resident i escolta pel port 25.

Primer descarreguem i instal·lem el paquet amb la instrucció:

*apt-get install sendmail*

En segon lloc modifiquem els fitxers:

*/etc/sendmail.cf*

*/etc/mail/sendmail.mc*

*/etc/mail/local-host-names* #dominis a administrar

*/etc/mail/accés* #llista amb les IPs locals

*/etc/mail/alises*

Creem el fitxer:

*/etc/mail/relay-domains* #llista de dominis permesos

Per que els canvis siguin efectius cal compilar:

*/etc/mail*

Amb el comandament:

*make*

### 4.8 Servidor FTP

Disposem d'un servei de transferència de fitxers que ens permet descarregar i enviar arxius a l'ordinador amb el servei actiu. Utilitzarem el servidor *ProFTPd* per ser un dels més populars per a Linux i gracies a la no necessitat de llicencies el podrem fer servir com exemple en el nostre laboratori. Els ports 20 i 21 TCP són els utilitzats per aquest servei.

Primer descarreguem i instal·lem el paquet amb la instrucció:

*apt-get install proftpd*

Modifiquem el fitxer:

*/etc/proftpd/proftpd.conf*

D'aquesta manera es simula que els usuaris de la xarxa interna puguin accedir al servidor i pujar arxius en ell mitjançant el protocol FTP.

# 5. Els Clients

### 5.1 Client1 : Windows XP

A continuació podem veure com hauran d'estar configurats els clients per a poder entrar en domini i funcionar correctament segons el nostre disseny de la xarxa.

Al tenir un servidor DHCP que ens assigna *IPs* automàtiques, la nostra configuració de xarxa es totalment automàtica. Com hem pogut veure anteriorment, el servidor DHCP és també l'encarregat de donar-nos qui es el servidor DNS i a on anar quan el explorador busca WPAD per al seva auto-configuració de les opcions del Proxy.

Tot seguit veiem com les opcions de xarxa són totalment automatitzades

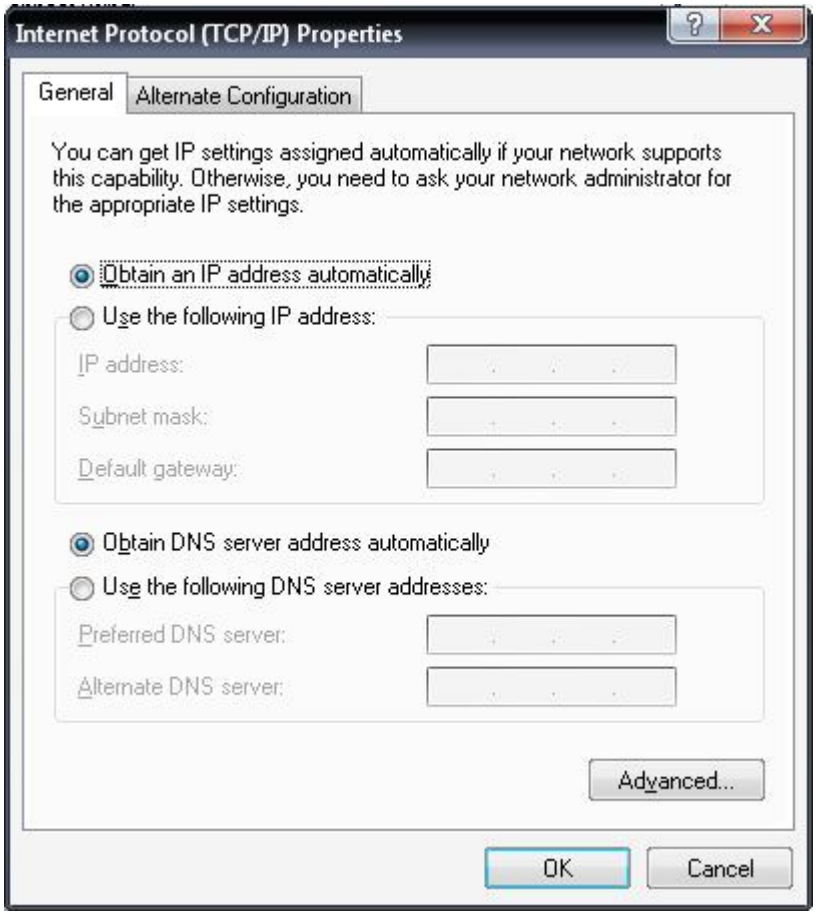


**Figura 34 : Propietats de la connexió xarxa del client**

Si des de el command de Windows realitzem un ipconfig /all podem veure com se'ns han assignat automàticament totes les *IPs* per a poder funcionar en xarxa i que formem part del domini uoclab.com.

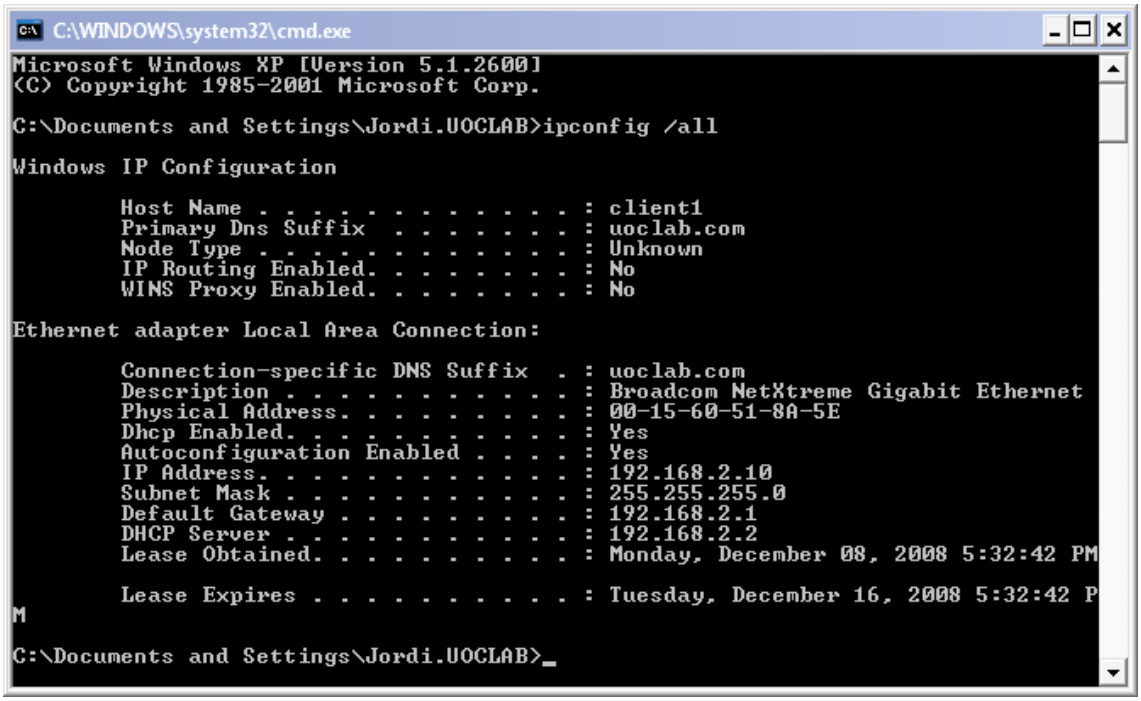


**Figura 35 : Configuració IP del client 1 des de Consola**

La configuració del nostre navegador també és totalment automàtica, ja que l'explorador realitza una consulta per aconseguir el fitxer wpad.dat al servidor ISA, i aquest contesta donant-li tots els paràmetres de les opcions per al seu correcte funcionament, com es pot apreciar en la següent imatge. En cap moment es van completar les opcions següents a mà, tot ha estat un procés automatitzat gracies a WPAD del ISA Server.

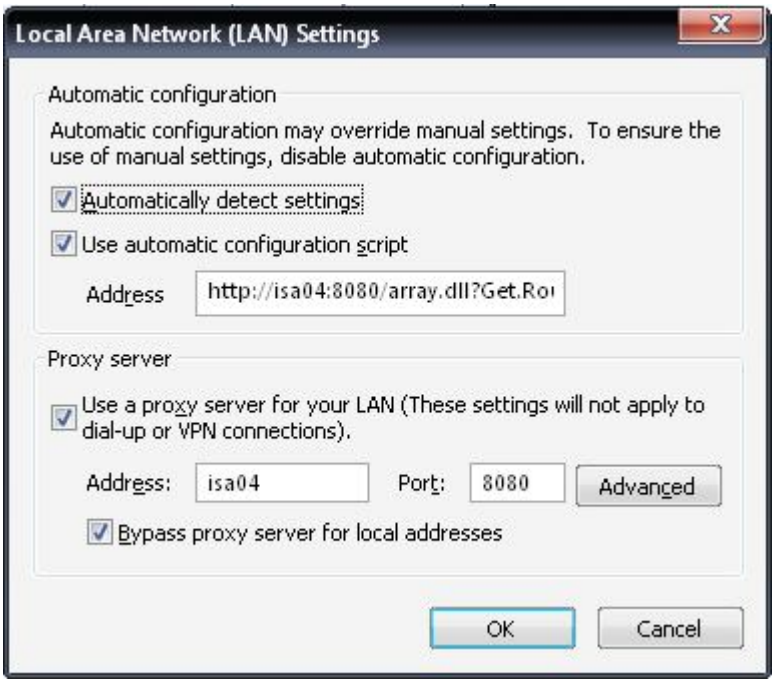


**Figura 36 : Configuració del explorador automatitzada**

Finalment per a poder tenir accés via web a Internet es necessari ser clients del *Firewall*, ja que al estar activat des d'un principi, s'ha de realitzar la instal·lació d'un petit software per a poder tenir funcionalitat en la xarxa o el nostre Firewall ISA bloquejarà la connectivitat de l'estació de treball. L'instal·lador el trobem en una carpeta compartida que esta en el nostre servidor isa04 (\\isa04\mspclnt). Un cop instal·lat client del Firewall , les politiques seran aplicades correctament i disposarem de connectivitat.

La instal·lació del client s'ha realitzat manualment seguint les pantalles visuals, ja que només va ser necessària per a un client. En cas de trobar-nos en una xarxa amb molts usuaris, seria convenient llençar la instal·lació mitjançant una GPO (política de grup) a l'Active Directory, automatitzant així la instal·lació i estalviant molt de temps.

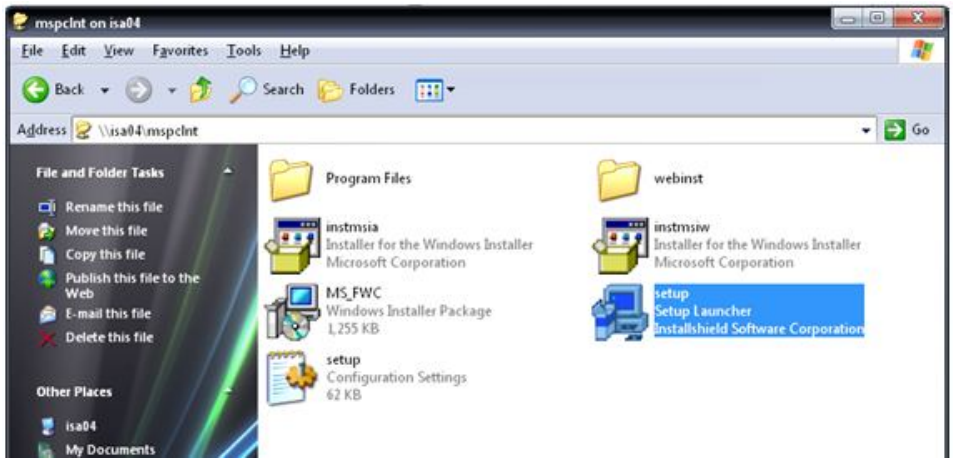


**Figura 37 : Localització del instal·lador del client Firewall (\\isa04\mspclnt)**

La següent imatge es mostra com el client del *Firewall* ha detectat automàticament el servidor ISA i ha automatitzat els paràmetres del client.

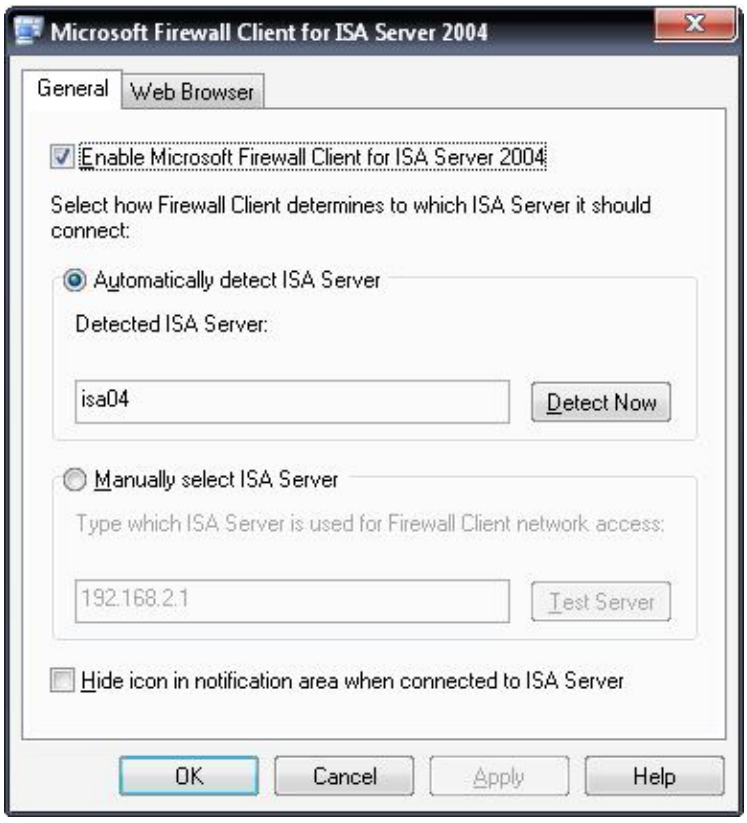


**Figura 38 : Configuració del Client Firewall**

Un punt important alhora d'obtenir una correcte funcionalitat en el nostre escenari, es assegurar que *ISA* Server 2004 té l'opció de publicar el servei WPAD activat. Aquest opció la podem trobar a les propietats de la nostra xarxa interna, des de la interfase gràfica del nostre servidor:


**Figura 39 : Xarxes configurades al servidor ISA Server**

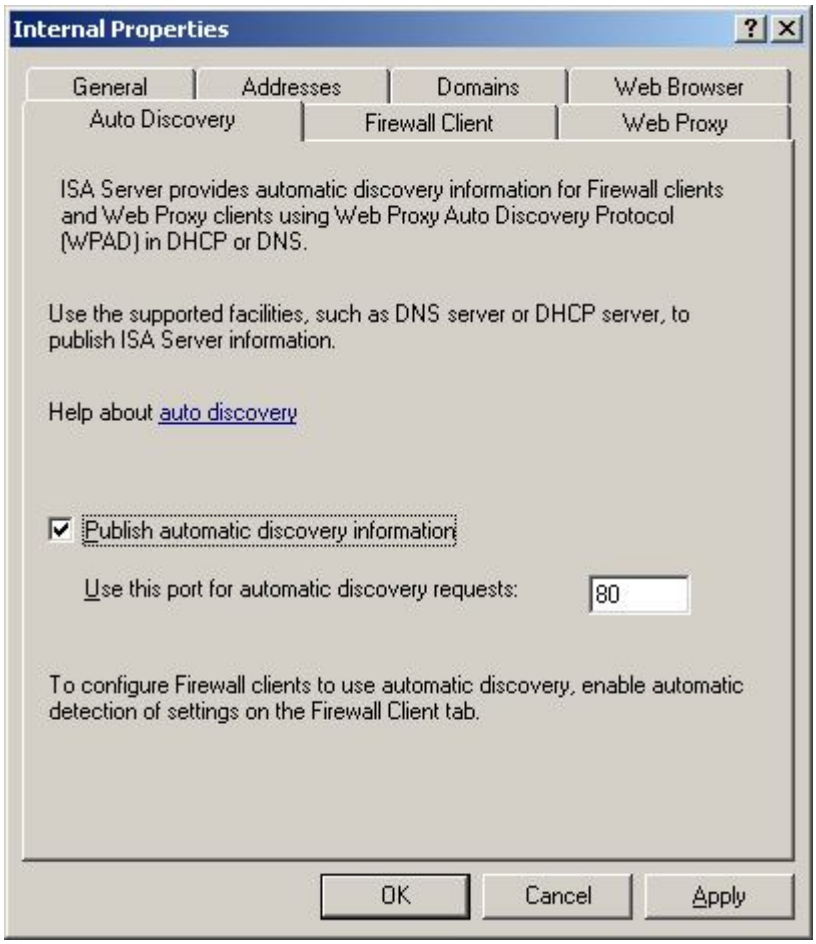


**Figura 40 : Opció de publicar l'auto configuració dels clients Proxy (WPAD)**

Com hem vist en la configuració de les polítiques del *Firewall*, amb *ISA Server* hem bloquejat certes pàgines webs i la famosa aplicació MSN Messenger. Això ens proporciona un exemple pràctic de com una xarxa corporativa pot censurà les webs que els seus treballador visiten i fins hi tot bloquejar certes aplicacions. La seva implementació ha estat detallada en apartats anteriors, però tot seguit podem veure els missatges que obtenim des de el client, confirmant que el *Firewall* esta funcionant correctament i aplicant les politiques de seguretat implementades.

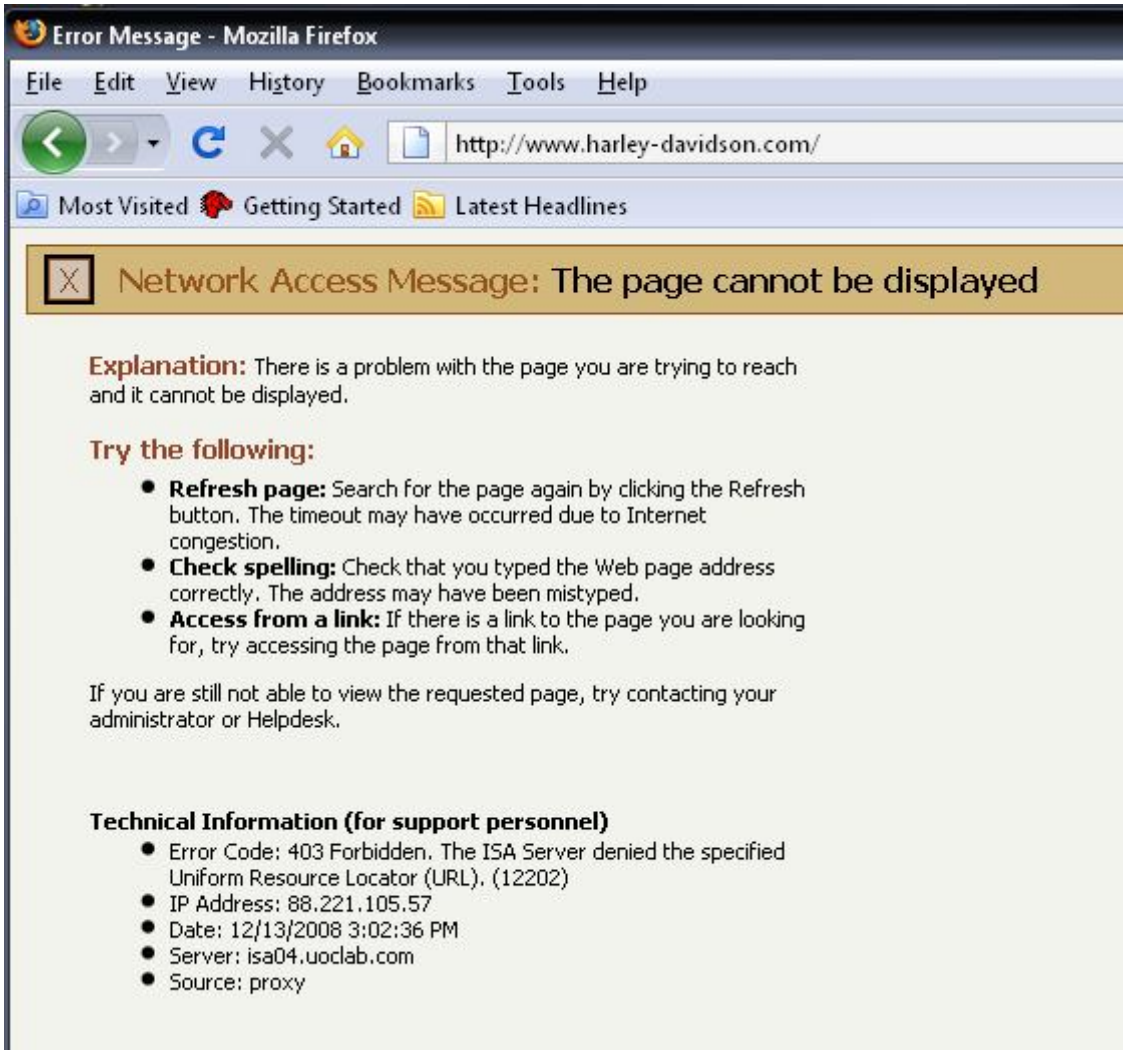


*Figura 41 : Missatge d'error de Pàgina web bloquejada*

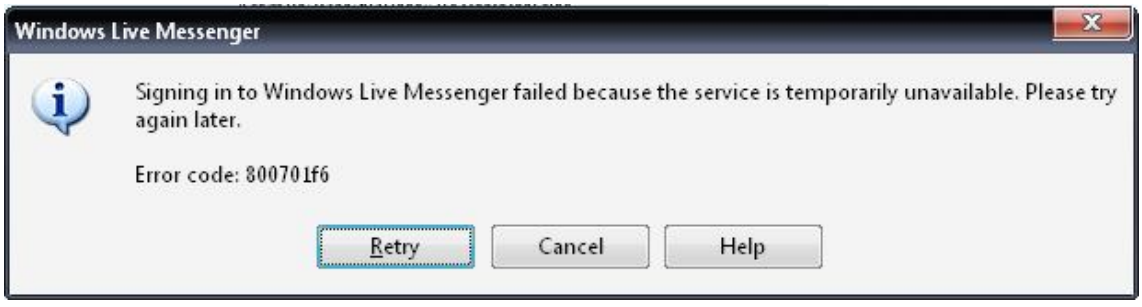


*Figura 42: Missatge d'error de MSN Messenger Bloquejat*

# 6. Conclusions aportades pel projecte

Un cop realitzat el TFC, cal fer allò que dona caràcter a l'estudi, treure'n conclusions que avalin l'esforç realitzat.

Crec que l'anàlisi del treball realitzat cal entendre'l en dos àmbits, un implícit al caràcter acadèmic de l'estudi, i un altre personal.

## 6.1 Conclusions generals:

Aquest treball ha proporcionat la possibilitat de millorar els nostres coneixements i la nostra comprensió sobre el mon de les amenaces electròniques i la seguretat informàtica. En un mon on les batalles entre administradors de xarxes y intrusos maliciosos esta a l'ordre del dia, tots estem sota l'amenaça real de que algú posi en perill els nostres sistemes de seguretat i envaeixi la nostra privacitat.

- La política de *seguretat* és, per defecte, de negació i bloqueig. Deixant que cap comunicació sigui possible fins que implementem les politiques i regles del Firewall.
- *Microsoft ISA Server 2004* té una configuració força visual però depenen de les necessitats de l'empresa pot arribar a ser molt complexa. L'inconvenient principal ha estat configurar una regla per cada tipus de servei que volem habilitar, això fa que s'hagi d'estar molt atén a quins serveis estem utilitzant en tot moment.
- ISA Server 2004 necessita d'actualitzacions periòdiques per a esser efectiu. Aquest fet ofereix vulnerabilitats importants si les actualitzacions no són possibles.
- El filtratge mitjançant llistes URL pot arribar a ser molt elevat i necessita un nivell elevat de hardware per assolir un rendiment òptim. ISA server cada vegada que rep una petició web comprova les llistes, línea per línea, i això requereix un nivell elevat de hardware.
- El filtratge que realitza ISA Server es a nivell de xarxa i d'aplicació, a diferencia d'altres eines com Cisco PIX, els quals son Firewalls de hardware normalment basats en un filtratge de xarxa i no d'aplicació. Això implica un major anàlisis dels paquets per part del nostre Firewall, disminuint la velocitat si no disposem de la maquinaria adequada.
- ISA Server 2004 disposa de la possibilitat de controlar VPN's, el qual el fa idoni per a grans empreses amb diferents seus.
- Cap *Firewall* proporciona una seguretat del 100%.

- De les proves realitzades per a cada una de les aplicacions, he observat que la seguretat per a us domèstic i presumiblement per a petita empresa és suficient.
- Com a conclusió general podem dir que la utilització de *Firewalls* per a garantir la seguretat de la xarxa és imprescindible.

## 6.2 Conclusions personals.

El primer objectiu ha estat acomplir la planificació temporal, una tasca molts cops complicada a causa de l'aparició d'inconvenients que sorgeixen de manera aleatòria i fortuïta, els quals molts cops no poden ser solucionats a priori, impliquen una recerca d'informació addicional a lo previst. L'escàs coneixement previ que tenia del tema ha fet canviar en algun moment la programació prevista. El no disposar del material i les condicions de treball optimes en començar el projecte ha provocat incertesa per a la finalització del termini establert, i la posterior posada en marxa del projecte.

El temps necessari per a la familiaritzar-me amb entorn de Windows Server 2003 i ISA Server 2004, ha estat superior al que en un principi s'havia estimat, a causa de que l'adquisició de coneixements sobre el tema ha estat paral·lela a la realització del TFC, i alhora em va motivar per a realitzar la Certificació de Microsoft MCSA, realitzant l'examen d'ISA Server 2004 unes setmanes abans de la finalització d'aquest treball.

L'escrit ha sofert canvis en la seva estructura inicial, i per tant es va haver de canviar l'enfocament d'alguns capítols.

La part més positiva és el alt nivell de coneixements adquirits en la realització del treball i que la necessitat d'un gran esforç.

Cal destacar els següents:

- L'estudi del concepte de Firewall i Proxy.
- Familiaritzar-me amb el sistema operatiu Windows Server 2003, i les principals opcions i configuracions segons el rol del servidor, així com la creació d'un domini.
- La configuració del *Firewall i Proxy ISA Server 2004,* sobretot *el que* ha portat més temps del previst, ja que es va haver d'estudiar la funcionalitat del producte abans d'intentar implementar-lo.

# 8. Glossari

- **DHCP**: DHCP és un protocol dissenyat per estalviar temps gestionant les adreces ip. Quan aquest servei esta actiu, el servidor assigna automàticament les adreces als clients, evitant així la configuració manual.

- **NAT**: "Network Address Translation" és un mecanisme utilitzat normalment per routers per permetre el intercanvi de paquets entre dues xarxes diferents.

- **WPAD**: The Web Proxy Autodiscovery Protocol (WPAD) és un mètode utilitzat pels clients per tal de localitzar el Proxy de la xarxa i auto configurar les opcions del navegador.

- **DNS**: El Domain Name System (DNS) és una base de dades distribuïda i jeràrquica on s'emmagatzema la informació associada als noms de domini de la xarxa.

- **Active Directory**: AD és el terme utilitzat per Microsoft quan ens referim a la seva implementació de servei de directori, en una xarxa distribuïda d'ordinadors. En l'AD és on s'emmagatzemen els usuaris, els computadors, politiques de grup, etc.

- **GPO**: Global Policy Object, política aplicada en l'Active Directory per tal de d'assolir una fita en un grup d'objectes.

- **OSI**: És un model per tal de diferenciar i entendre els diferents nivells del funcionament d'una xarxa, de més alt (aplicacions) fins els nivells més baixos (físics)

- **CNAME**: es un registre en la base de dades DNS que indica el veritable nom de host d'un ordinador. Bàsicament el registre CNAME permet que un ordinador sigui reconegut per un o més hosts.

- **Cisco PIX**: Firewalls realitzats per Cisco amb hardware dedicat.

- **Addons**: Petites aplicacions que s'afegeixen a un software ja existent per tal d'augmentar la funcionalitat d'aquest últim.

# 9. Bibliografia

**MCSA/MCSE Self-Paced Training Kit – Microsoft Press**

- *(Exam 70-350): Implementing Microsoft® Internet Security and Acceleration Server 2004*
- *(Exam 70-290): Managing and Maintaining a Microsoft® Windows Server(TM) 2003 Environment, Second Edition*

**Microsoft**:

- http://www.microsoft.com/spain/servidores/isaserver/info/features.aspx

**ISA Server 2004**:

- http://www.isaserver.org/

**CBT Nuggets (Video Training)** :

- *70-350*: ISA Server 2004
- *70-290: Microsoft Windows Server 2003*

**Wikipedia**:

- http://en.wikipedia.org/wiki/Proxy_server
- http://en.wikipedia.org/wiki/Squid_cache
- http://es.wikipedia.org/wiki/Red_privada_virtual

**Projecte GNU**:

- http://www.gnu.org/philosophy/free-sw.html
- http://www.gnu.org/copyleft/gpl.html