

Proxy Server Components

Components of firewalls provide different functions that correspond to layers of the DOD (Department of Defense) networking model. Table 1 shows how the components of Microsoft Proxy Server compare to the DOD model.

	Web Proxy	Winsock Proxy	Socks Proxy	IP Packet Filtering
Process/ Application	x	x	x	
Host-to-Host	X	x	x	
Internetwork	X	x	x	x
Network Interface				x

Table 1 DOD and Proxy Components

Three basic services provide Internet access for proxy clients: Web Proxy, WinSock Proxy and Socks Proxy. Each of these services has individual configuration options while some settings apply to all three. Packet filtering can be configured for the public interface attached to the server. This feature controls what types of packets can pass through the server in each direction. All of these components provide different levels of security and can be customized for each situation.

Packet Filtering

Packet filtering works at the lower levels of the DOD model and does not provide authentication or security for sessions. The role of packet filtering in a firewall environment is simply to deny or allow packets on the physical network. Four variables control the filtering:

- Source IP
- Source Port
- Destination IP
- Destination Port

This occurs at the network level, typically as a list of rules that allow and deny packets. Table 2 below shows an example of a packet filtering rule list:

Protocol Type	Source IP	Source Port	Destination IP	Destination Port	Action
*	*	*	*	*	Deny
TCP	*	*	198.209.250.221	80	Allow
TCP	*	*	198.209.250.225	25	Allow
TCP	*	*	198.209.250.225	110	Allow

Table 2 Packet Filter Rules

The rules in this table deny all packets except those destined to a Web server and a mail server. Packet filters do not examine the data portion of the packet and cannot prevent “unauthorized” use of specific ports.

WinSock Proxy Server and Client

WinSock Proxy provides a transparent, circuit-level gateway to Windows platform clients. WinSock proxy is a proprietary set of protocols developed by Microsoft to provide secure network communications between Windows clients and the Microsoft Proxy Server. The idea of a “socket” Application Programming Interface (API) was originally developed for BSD UNIX. A socket basically opens a connection between a server and a client and allows for the transfer of information. The WinSock Proxy client specifically allows Windows clients to establish a connection with the Microsoft Proxy Server to authenticate and perform such transactions as are allowed. WinSock proxy supports UDP (connectionless) and TCP (connection-oriented) protocols. WinSock Proxy works with the LAT (Local Address Table) to determine whether or not a host is on the local network. It supports many protocols that are based on both TCP and UDP, like VdoLive, AOL, IRC, NetShow#153 server, and RealAudio. WinSock proxy also supports IPX clients.

The current version of WinSock is 1.1. Windows NT4 and Windows 98 can both support WinSock 2 that has many enhanced features. For more information on WinSock 2, refer to: <http://www.sockets.com/winsoc2.htm>

Socks Proxy Server and Client

The Socks Proxy Service provides a similar type of socket API to that described above for Macintosh and other clients. The SOCKS protocol provides a nontransparent (applications must be built with SOCKS support in mind) circuit level gateway. SOCKS Proxy Service only allows TCP sessions and does not support UDP (VDOLive, NetShow, etc.). Applications must support SOCKS version 4.5 or greater to work with the SOCKS

Proxy Server. The SOCKS Proxy service uses IP addresses and the identd protocol that must be installed on the MS Proxy Server for SOCKS to work properly.

Web Proxy Server and Client

The Web Proxy Server is an application proxy that provides access for clients through Web browsers for the following protocols: HTTP, FTP and Gopher. The client can be Netscape or Internet Explorer and is enabled by simply pointing the browser to the IP number of the proxy server. This service needs to be tightly controlled for access since, theoretically, anyone on the Internet can use your proxy server by default. The Web Proxy Server has a built-in reverse Web proxy that allows the Proxy Server to protect a Web server on the private network.

Plan for Implementation

Prior to the installation of Proxy Server a plan for implementation should be developed. Factors to be considered include the physical layout of the network, NT Domain model, services required on both public and private networks and the level of security required. In general, only authorized traffic should be passed through the firewall and all else should be denied. The firewall itself must also be secure--in this case means the NT operating system and the physical location of the server.

1) Physical Network

The physical network primarily determines how many Proxy Servers are needed and what class of IP addresses should be used. Proxy Server was designed to work with private IP addresses on the intranet for optimum security. Private addresses are specific TCP/IP networks that have been reserved for use on intranets. These addresses are not routed over the intranet and can be used by anyone behind a "firewall". The addresses that can be used are:

10.0.0.0/8	mask=255.0.0.0
172.16.0.0/12	mask=255.255.0.0
192.168.0.0/24	mask=255.255.255.0

For more detailed information please refer to <http://sunsite.auc.dk8/RFC/rfc/rfc1918.html>

During the planning stage you should determine which addresses you will use, based on your network design and total number of workstations.

Example 1: An organization has one site with approximately 150 workstations and connects via one router to the Internet. One Proxy Server would be adequate and the class C network of 192.168.1.0/24 would provide plenty of addresses.

Example 2: An organization has one router that goes to the Internet. The router goes to a switch that has approximately 5 class Cs mapped to it. In this case one Proxy Server

would probably be adequate (placed between the router and the switch). If the configuration of the switch remains the same, 5 private class Cs would simply replace the class C networks. Everything else should stay the same. Another alternative would be to disable routing and use a class B address of 172.16.0.0.

Example 3: An organization has 3 sites separated by a 56 K Frame Relay WAN, each site has about 1,000 users. Although one Proxy Server will support over 1,000 users in this case it would be wise to have a Proxy Server at each site. Communications to and from a Proxy Server over a 56K line is not advisable. Each site could have its own class B address.

2) NT Domain Model

Proxy Server was not intended to run on an NT workstation or an NT Workgroup server. The Proxy Server should be installed on an NT Member Domain Server and not as a Primary Domain Controller or a Backup Domain Controller. This is primarily due to security issues associated with NT Directory Services. The firewall should not sit on the same machine that stores user information. Advanced Network Administrators may want to put the Proxy Server in its own domain, establishing a one-way trust with the organization's domain. This complicates the model and makes troubleshooting much more difficult.

3) NT Services on Network

Necessary services need to be determined for both the public and private networks. In general WINS servers will only be needed on the private network. Non-authoritative DNS services on the private network can facilitate the location of servers behind the firewall for local users. DHCP services can be run on the private network while all public addresses are statically assigned. A demilitarized zone (DMZ) can exist on a third network card to provide some security though it is not as secure as having servers completely behind the firewall. E-mail and Web Servers can be in public, private or DMZ portions of the network. MS Proxy Server has a built in reverse proxy component for an internal web server but setting up an internal mail server is a little more complicated.

Microsoft Proxy Server 2.0 supports "Server Proxying" (the proxy server forwards appropriate packets to servers behind the firewall). This involves configuring E-mail Servers, Web Servers, etc. behind the firewall and allowing secured public access. Instructions for setting up server proxying will be addressed in a future document.

4.) Proxy Services

Once the network design and positioning of services has been determined, the network administrator can determine which proxy services are needed. The client operating systems combined with required protocols and services determine which proxy services are needed. For example, if clients only need Web access on the Internet, the Web Proxy

Service may be adequate. If all clients are Windows-based and non-Web services are required such as POP3, SMTP, Telnet, then Winsock Proxy Server and client will be required. If non-Web services are required for non-Windows-based machines such as Macintosh or UNIX, then the SOCKS Proxy Server may be required.

Once the design of the firewall system has been determined, the next step is to make sure the NT Server meets the minimum requirements and to configure TCP/IP on the server for the public and private networks.

Installation Requirements

For optimal performance of Proxy Server 2.0 the Proxy Server should be a domain server and not a primary or backup domain controller. It is recommended that the server have the following configuration:

Hardware

- Minimum of 128MB RAM,
- 4GB hard disk space
- Pentium II (or higher) processor.
- At least two Network Interface Cards (NICs)

The server should be dedicated to Internet Services and should not be used for application serving or file and print sharing. No critical data should be stored on this server and backup implementation can be minimal (primarily for log files). Drives used for caching must be formatted as NTFS and should be prepared before installation. Both network cards must be configured with the TCP/IP protocol and no other protocols if possible.

TCP/IP Configuration

Proxy Server is designed to work with public and private IP addresses by default. Private IP addresses are not routable on the Internet but they follow the same rules of TCP/IP networking. To configure TCP/IP for both cards do so in the Control Panel of the NT Server under Network. The card that is directly connected to the private network should have a private address and no default gateway. The public card should have a default gateway = to the next router on the network (typically the MOREnet node router). Do not enable routing for TCP/IP protocol.

In the simplest configuration one public address would be assigned to the NIC directly connected to the Internet and one private address would be assigned to the NIC directly connected to the Local Area Network. In some cases a third NIC may be added for what is commonly called a "DMZ" or "Demilitarized Zone". The demilitarized zone has public addresses and is typically established for services that cannot be established with server proxying. This will be discussed in more detail later. In the Local Address Table (LAT) all private networks will automatically appear after installation as well as public networks defined by public NICs in the server.

Make a table of your public and private addresses for your records.

PUBLIC	PRIVATE
207.160.134.35 (Proxy)	192.168.1.1 – 192.168.1.253
207.160.134.46 (DMZ Mail Server)	

Software Requirements

Before you install Proxy Server you should also have the following software installed in the order listed below. Service packs, Option packs and Internet Explorer can be downloaded directly from Microsoft at [ftp:// ftp.microsoft.com](ftp://ftp.microsoft.com)

- NT Server 4.0 with IIS2.0
- Windows NT Service Pack 4 or 5
- MS Internet Explorer 4.0 or greater with SP1 or greater
- Windows NT Option Pack 4 and choose “Upgrade Plus” (to upgrade IIS 2.0 to IIS4.0)
- Reapply Service Pack 4 or 5
- Install Proxy Server 2.0

Step by Step Installation

1. Insert the Proxy Server CD into your NT server and run the `setup.exe` program.

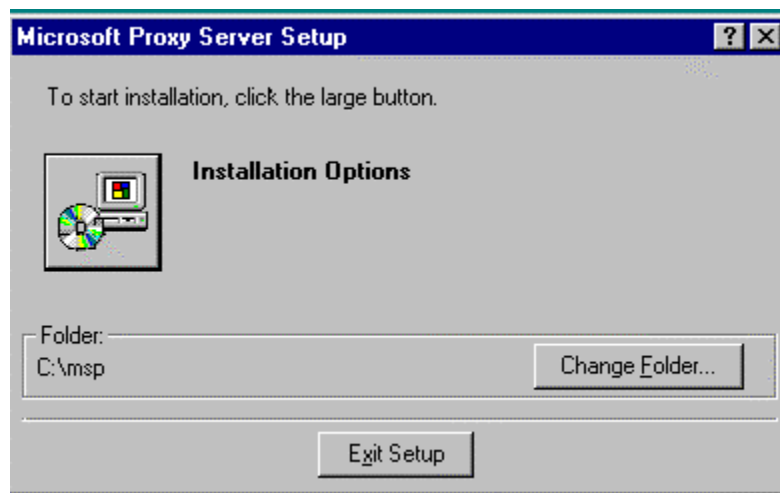


Figure 2 Server Setup

2. Click on the installation button on the left-hand side.

Choose the default for all three options which requires about 10MB of available space. This will install the server and create the share “msp clients” which stores the Winsock proxy client installation files.

Note: As you are installing you may get a setup warning “SAP Agent” not installed machines using only IPX networking protocol will not be able to access the proxy. This is only for networks that run IPX protocol and do not use TCP/IP. A SAP (Service Advertisement Protocol) agent is required for IPX to work with the Winsock Proxy Client. If you require this for some reason you will need to install the SAP agent on Windows NT.

3. Enable Caching. Determine the drive or drives for the web caching directories. The drives must be formatted as NTFS and must physically reside on the Proxy Server; network drives may not be used. The maximum size of your cache depends on what is available on your server (default is 100MB). In general, Microsoft recommends that you allow a minimum of 10MB base and .05MB per each user.

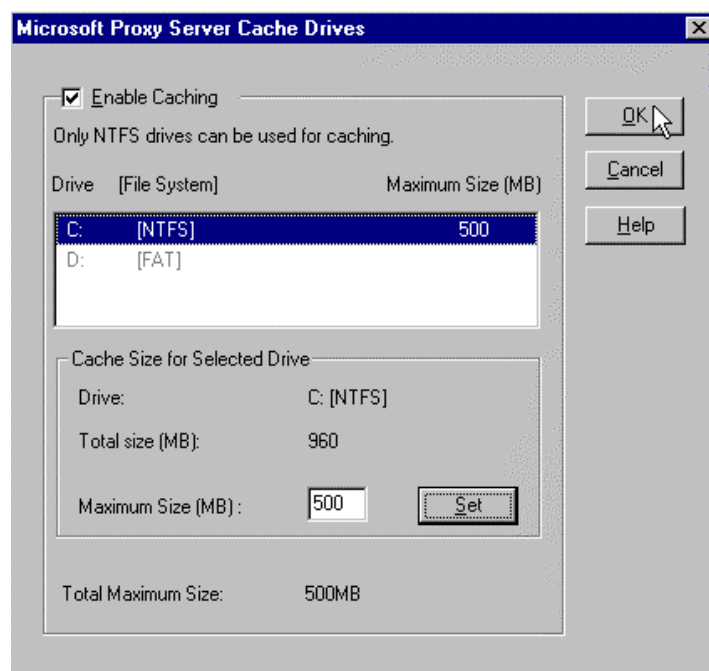


Figure 3 Default Components

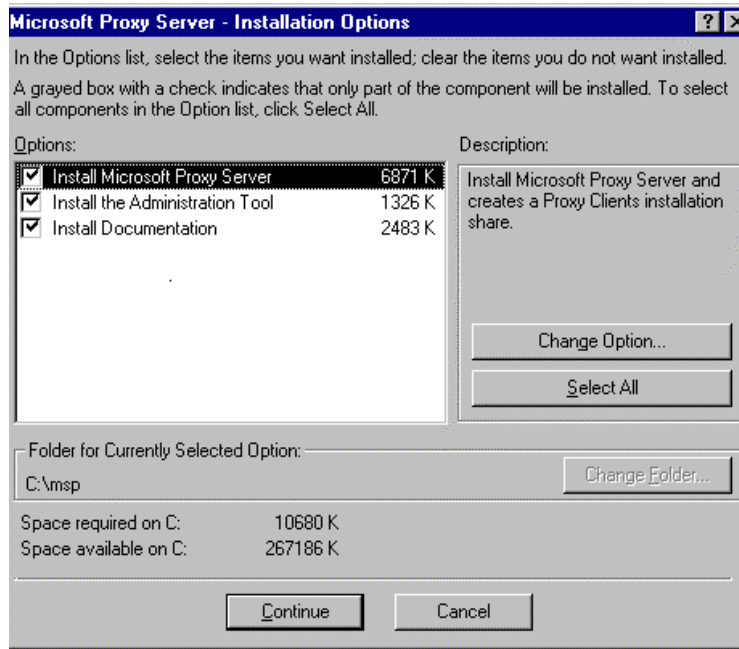


Figure 4 - Installation Options

Figure 4 shows the cache directory to be set at 500MB. Note that this is a maximum value and therefore should not cause problems with filling up the drive. Multiple NTFS drives may be used for caching.

4. Configure the Local Address Table. The next screen you see should be an empty LAT table as shown in Figure 5. Click on construct table.

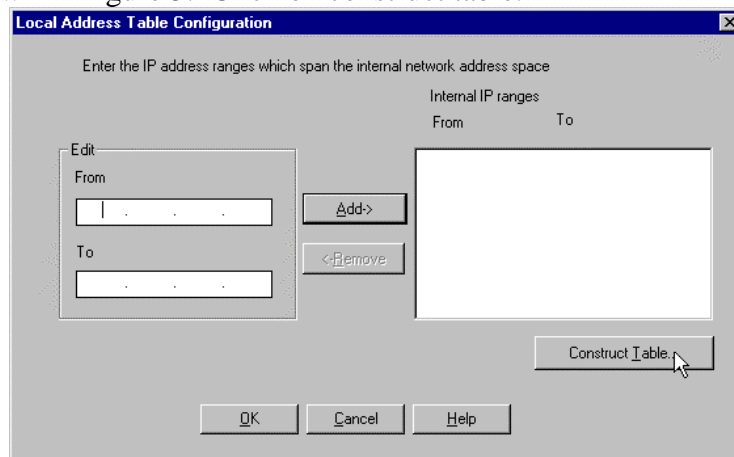


Figure 5 Empty LAT Table

5. A screen will appear with several options. Check load from NT internal routing table and load from specific IP interfaces. Then choose the network interface card with your private address as shown in Figure 6.

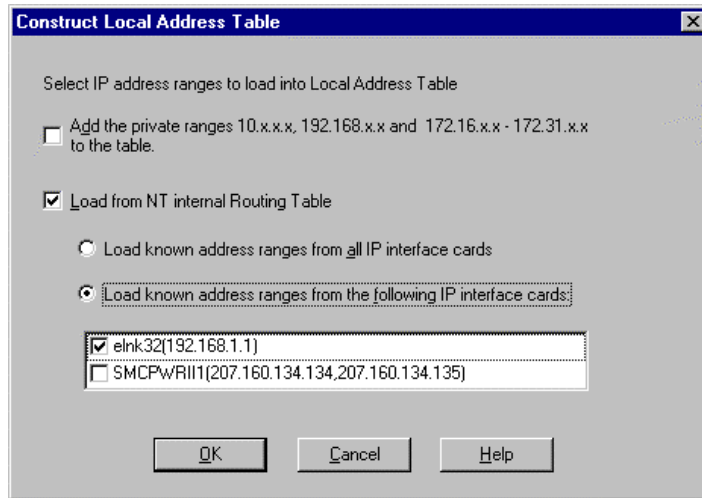


Figure 6 Choose Private Interface

A table should now appear that includes the networks bound to your private interface. If necessary you can manually edit the table to include additional networks. For example if you have a downstream router attached to your network that includes the network 192.168.2.0 you could manually add that network to the table.

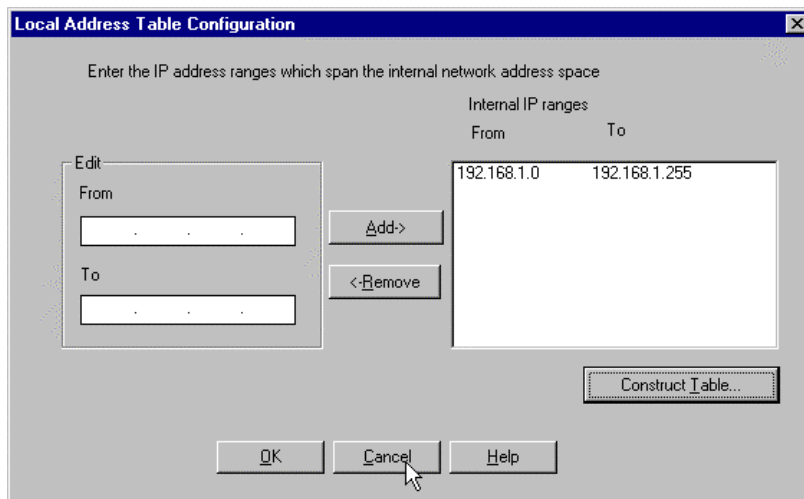


Figure 7 Local LAT Table

Note: Do not include addresses from the public interface in the LAT table!

6. Configure the settings for client connections. In general, choose connect by computer name. Some configurations such as setting up a mail server behind the Proxy Server may require a connection by IP address.

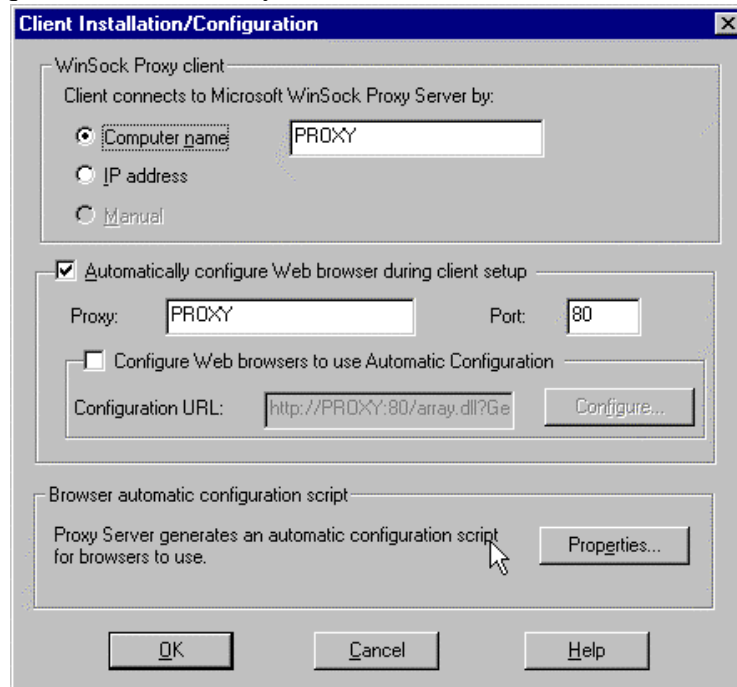


Figure 8 Client Options

7. Choose automatically configure Web browser during client setup so that when you install the Winsock Proxy client on each workstation it will look for a browser and configure it at the same time.
8. Enable access control. This is checked by default but once this is enabled everyone will be locked out until you configure the access control lists (discussed in next section).

Note: You should see a dialog box when Proxy Server is finished installing. It is not necessary to restart the NT Server.



Configuration

1. From the Program Menu on the Proxy Server choose Microsoft Management Console. A list of IIS and Proxy Services should appear.

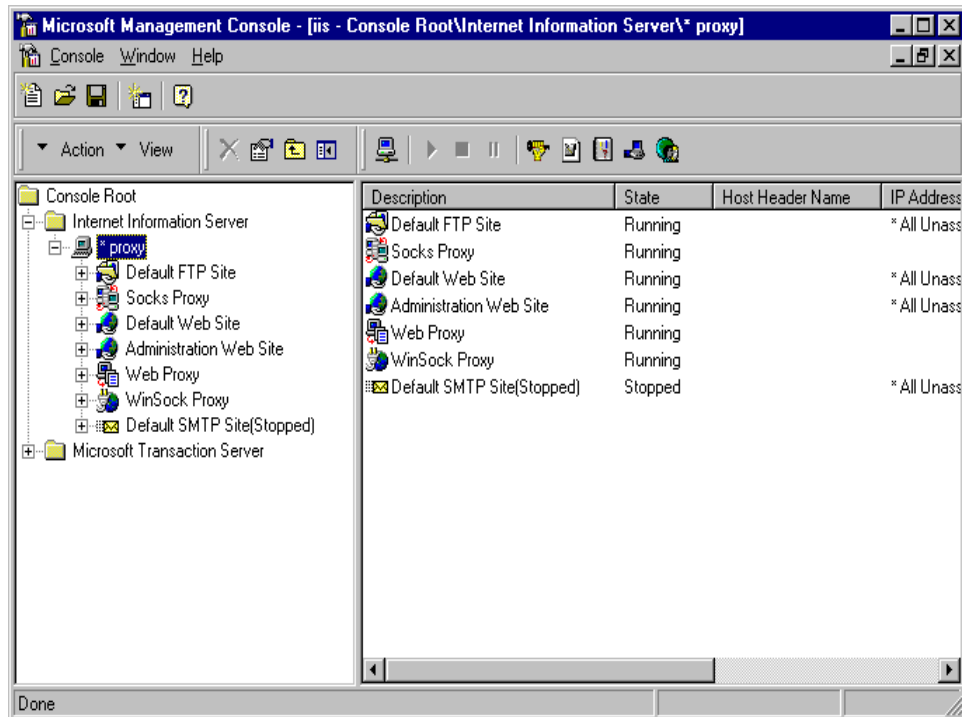


Figure 10 Proxy Services

Note: To configure services either double-click on the service or highlight the service and right click to properties. Some properties of each service overlap such as packet filtering and the LAT table. Each service also has unique properties such as reverse Web proxy, etc.

Configure Web Proxy Service

1. Double click on the Web Proxy Service.
2. The Web Proxy Service provides many functions for Microsoft Proxy Server including caching, authentication and reverse web proxy (pointing external requests to an internal web server. Figure 11 shows the general Properties page for the Web Proxy Service.

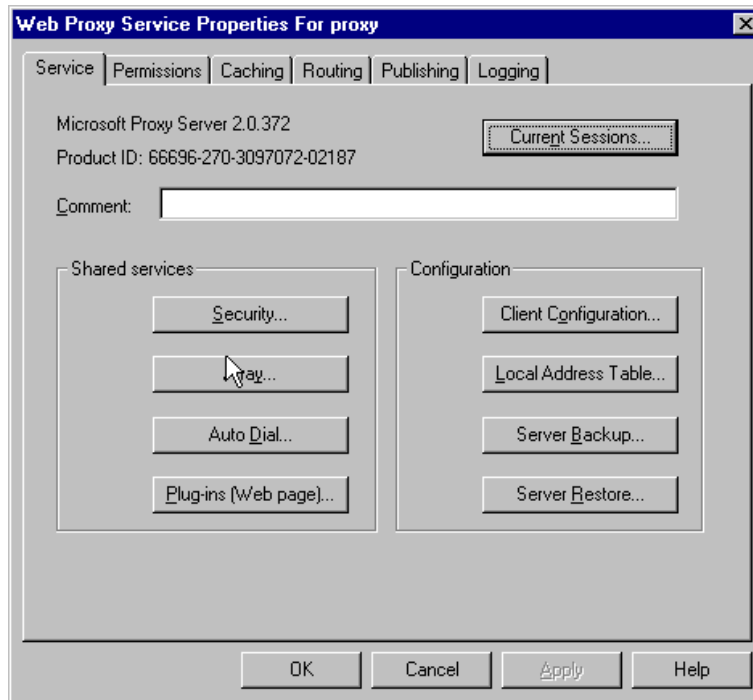


Figure 11 Web Proxy Properties

3. On the General Properties page of the Web Proxy Service, click on caching.

- The cache size was determined initially during installation. To change the size and/or location of the cache directories, use the cache size button to display options.

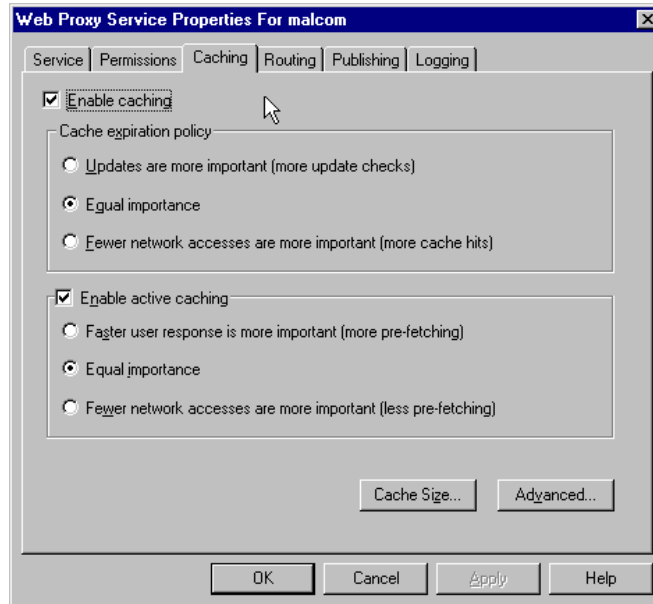


Figure 12 Caching Defaults

- Save the caching information and click on the Publishing tab as shown in Figure 12.

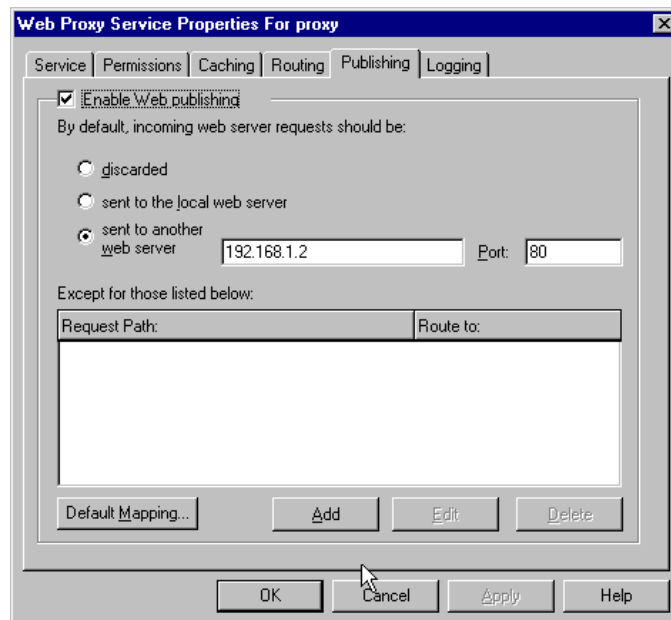


Figure 13 Web Publishing

6. The Publishing tab on the Web Proxy Service determines what types of Web services your Proxy Server will provide to the Internet.

- A. If no services will be provided check **discarded**.
- B. If you Web server will reside on the same machine as the Proxy Server, check “**sent to the local Web server.**”
- C. If your web server is on a private IP number behind the firewall, check “**sent to another Web server**” and provide the private IP address of the Web server.

Note: In cases B and C, the DNS name of the Web server should be registered to a public IP number bound to the Proxy Server

Configure Access Control for Web Proxy Service

Access can be enabled for each proxy service and defined for individual protocols. The protocols will vary depending on which one each service supports. Access can be granted to individuals or groups.

- 6. Click on the permissions tab of the Web Proxy Service.
- 7. Make sure that “enable access” is checked. In the protocol box choose WWW.
- 8. Click on the edit button. An empty box should appear, click on the add button at the bottom of this page. A list of domain users and groups will appear. Choose the groups and/or users that you wish to have access to WWW services through the Proxy Server. It is recommended that you do not give access to the groups “everyone” or “guests”. This service is for outgoing WWW requests. Figure 16 shows WWW access granted for all domain users.

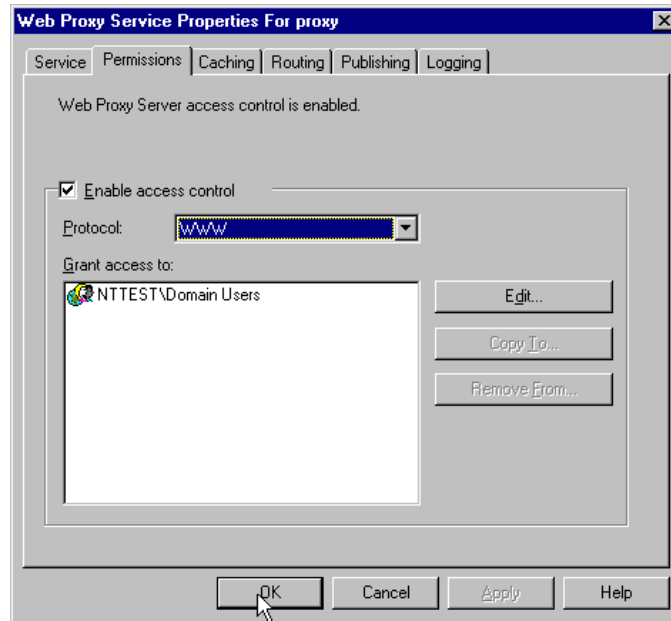


Figure 14 WWW Access Control

Configure Winsock Proxy Service

1. Double-click on the Winsock Proxy Service.
2. Click on the Protocols tab to show all the protocols that Winsock Proxy supports. You can add or remove any from this list. For example, if you don't want any access to Real Audio you can simply remove it here. The purpose of this tab is to remove protocols completely so that no one on the network can use these protocols. If you wish to control protocol access by group, do this in permissions.

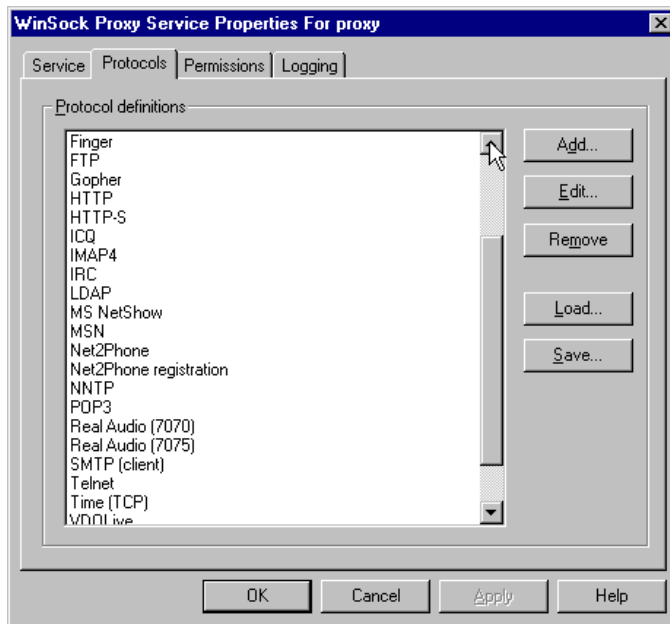


Figure 15 Winsock Proxy Protocols

3. Click on the Permissions tab. You can set permissions for users and groups for each protocol. In Figure 16 the only groups allowed to use FTP are administrators and server operators.

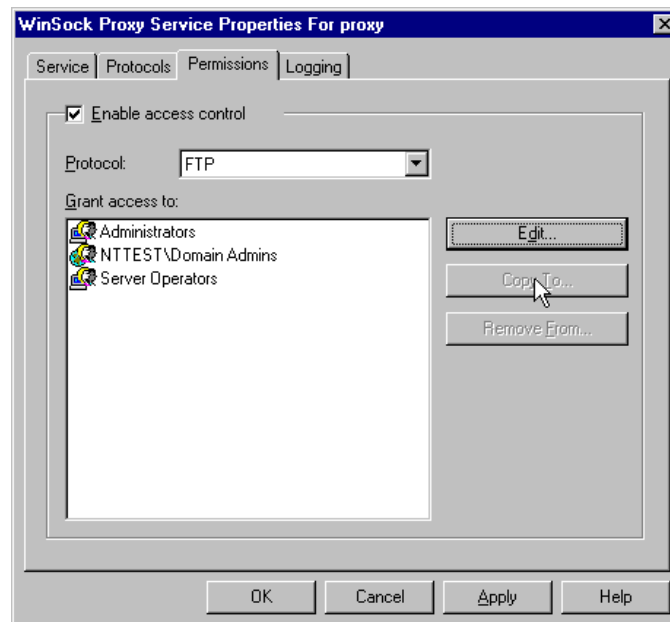


Figure 16 Permissions

Note: Once permissions have been defined for the Winsock Proxy Service and the Web Proxy Service you are ready to install the Winsock Proxy Client.

Install Winsock Proxy Client

During installation MS Proxy Server created a share on the NT server to store common client files. The default path for this directory is c:\msp. Client installation can be run from this directory on the server or it can be done from a browser. This documentation details the shared directory option.

1. From a Windows-based workstation log into the domain.
2. From the start menu choose Programs, Windows Explorer.
3. Double click on the shared directory c:\mspc\nt and then double-click on i386.
4. Double-click on setup.exe, an installation screen should appear.

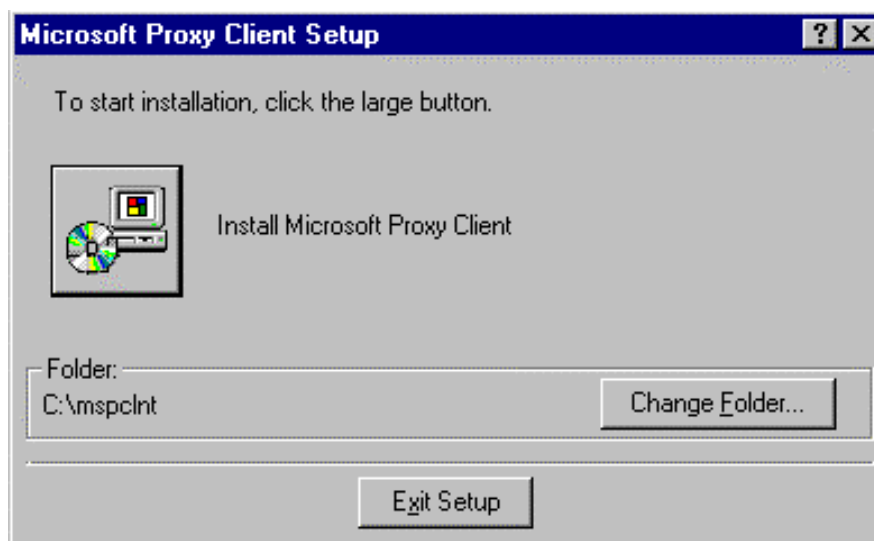


Figure 17 Client Install

5. Click on the large button to the left. The installation is very simple and just takes a few minutes while some files are copied. When finished you will be prompted to restart your computer.
6. After restarting, an icon will appear in your control panel labeled WSP client. Double click on this icon and you should see a configuration screen.

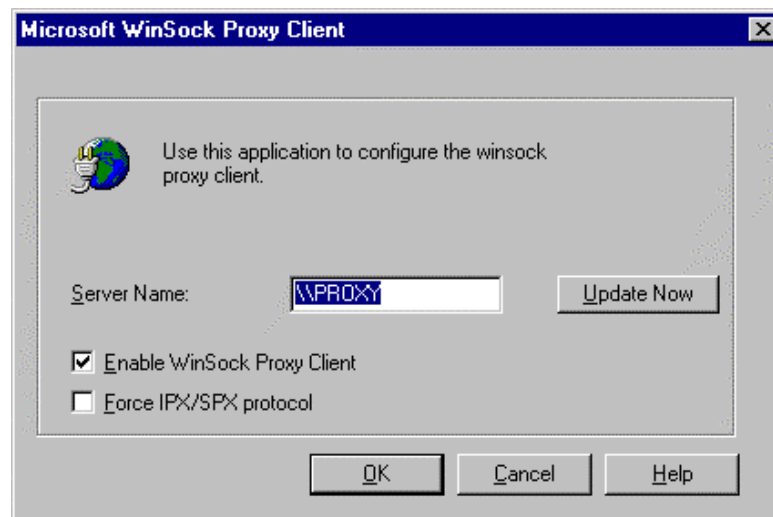


Figure 18 Client Update

The only options available on the client configuration are enable and disable the Winsock Proxy Client and force to IPX only. Every time you click on update now the client connects with the server and refreshes client configuration files from the server. Two files are automatically updated from the server, the `m脾clnt.ini` and the `msplat.txt`.

There is one file for local client configuration, the `w脾cfg.ini` file. This file is not updated from the server and can be used for specific client needs.

7. Click on update now to make a connection with the server. You will be notified if the connection was successful.
8. Test your connection. Go to the Proxy Server Management Console and double click on Winsock Proxy Server. You should see your connection information in the window.