Understanding Microsoft Proxy Server 2.0

By NeonSurge
Rhino9 Publications

Preface-

This documented was not made for people who have been working with Microsoft Proxy Server since its beta (catapult) days. It is made for individuals who are curious about the product and security professionals that are curious as to what Microsoft Proxy Server has to offer. This document is also being written for individuals have a general idea of what a Proxy Server does, but wants to know more. This paper goes into discussion of Proxy Server Features and Architecture, Access Control, Encryption, and Firewall Strategies (which I have been getting a lot of requests for).

The second part of the documentation goes into Firewall types and strategies, so if that's the reason you downloaded the documentation, go straight to page 8 I believe.

What is Microsoft Proxy Server?

Microsoft Proxy Server is a "firewall" and cache server. It provides additional Internet security and can improve network response issues depending on its configuration. The reason I put the word firewall in quotes is because Proxy Server should not be considered as a stand-alone solution to a firewall need. When you are done reading this document, you will have an advanced understanding of the Proxy Server product and also understand firewall techniques and topologies.

Proxy Server can be used as an inexpensive means to connect an entire business through only one valid IP address. It can also be used to allow more secure inbound connections to your internal network from the Internet. By using Proxy Server, you are able to better secure your network against intrusion. It can be configured to allow your entire internal private network to access resources on the Internet, at the same time blocking any inbound access.

Proxy Server can also be used to enhance the performance of your network by using advanced caching techniques. The can be configured to save local copies of requested items from the Internet. The next time that item is requested, it can be retrieved from the cache without having to connect to the original source. This can save an enormous amount of time and network bandwidth.

Unlike Proxy Server 1.0, Proxy Server 2.0 includes packet filtering and many other features that we will be discussing.

Proxy Server provides it functionality by using three services:

* Web Proxy: The web proxy service supports HTTP, FTP, and Gopher for TCP/IP Clients.

* WinSock Proxy: The Winsock proxy supports Windows Sockets client applications. It provides support for clients running either TCP/IP or IPX/SPX. This allows for networks that may be running more of a Novell environment to still take advantage of Proxy Server.

* SOCKS Proxy: The SOCKS Proxy is a cross-platform service that allows for secure communication in a client/server capacity. This service supports SOCKS version 4.3a and allows users access to the Internet by means of Proxy Server. SOCKS extends the functionality provided by the WinSock service to non-Windows platforms such as Unix or Macintosh.

Proxy Servers Security Features

In conjunction with other products, Proxy Server can provide firewall level security to prevent access to your internal network.

* Single Contact Point: A Proxy Server will have two network interfaces. One of these network interfaces will be connected to the external (or "untrusted") network, the other interface will be connected to your internal (or "trusted") network. This will better secure your LAN from potential intruders.

* Protection of internal IP infrastructure: When IP forwarding is disabled on the Proxy Server, the only IP address that will be visible to the external environment will be the IP address of the Proxy Server. This helps in preventing intruders from finding other potential targets on your network.

* Packet Layer Filtering: Proxy Server adds dynamic packet filtering to its list of features. With this feature, you can block or enable reception of certain packet types. This enables you to have a tremendous amount of control over your network security.

Beneficial Features of Proxy

* IIS and NT Integration: Proxy Server integrates with Windows NT and Internet Information Server tighter than any other package available on the market. Proxy Server actually uses the same administrative interface used by Internet Information Server.

* Bandwidth Utilization: Proxy Server allows all clients in your network to share the same link to the external network. In conjunction with Internet Information Server, you can set aside a certain portion of your bandwidth for use by your webserver services.

* Caching Mechanisms: Proxy Server supports both active and passive caching. These concepts will be explained in better detail further into the document.

* Support for Web Publishing: Proxy Server uses a process known as reverse proxy to provide security while simultaneously allowing your company to publish on the Internet. Using another method known as reverse hosting, you can also support virtual servers through Proxy.

Hardware and Software Requirements

Microsoft suggests the following minimum hardware requirements.

* Intel 486 or higher. RISC support is also available.
* 24 MB Ram for Intel chips 32 MB Ram for RISC.
* 10 MB Diskspace needed for installation. 100 MB + .5 MB per client for Cache space.
* 2 Network interfaces (Adapters, Dial-Up, etc)

Following is the suggested minimum software requirements.

* Windows NT server 4.0
* Internet Information Server 2.0
* Service Pack 3
* TCP/IP

It is highly recommended that it be installed on an NTFS partition. If an NTFS partition is not used, not only are you losing NTFS's advanced security features, but also the caching mechanisms of Proxy Server will not work.

It is also recommended that your two network interfaces be configured prior to installation. On interface configured to the external network, and one

configured for the internal network. (Note: When configuring your TCP/IP settings, DO NOT configure a default gateway entry for your internal network interface.)

* Be sure that "Enable IP Forwarding" is not checked in your TCP/IP settings. Thi

What is the LAT?

This is probably one of the most common questions I am asked as a security professional. The LAT, or Local Address Table, is a series of IP address pairs that define your internal network. Each pair defines a range of IP addresses or a single pair.

That LAT is generated upon installation of Proxy Server. It defines the internal IP addresses. Proxy Server uses the Windows NT Routing Table to auto-generate the LAT. It is possible that the when the LAT is auto-generated, that errors in the LATs construction will be found. You should always manually comb through the LAT and check for errors. It is not uncommon to find external IP addresses in the LAT, or entire subnets of your internal IP addresses will not appear on the LAT. It is generally a good idea to have all of your internal IP addresses in the LAT.

* NO EXTERNAL IP ADDRESSES SHOULD APPEAR IN YOUR LAT.

Upon installing the Proxy Server client software, it adds a file named msplat.txt into the \Mspclnt directory. The msplat.txt file contains the LAT. This file is regularly updated from the server to ensure that the LAT the client is using is current.

What is the LAT used for?

Every time a client attempts to use a Winsock application to establish a connection, the LAT is referenced to determine if the IP address the client is attempting to reach is internal or external. If the IP address is internal, Proxy Server is bypassed and the connection is made directly. If the IP address the client is attempting to connect to DOES NOT appear in the LAT, it is determined that the IP address is remote and the connection is made through Proxy Server. By knowing this information, someone on your internal network could easily edit his or her LAT table to bypass Proxy Server.

Some Administrators may not see this as a problem because the LAT is regularly updated from the server, so any changes the user made to his or her LAT will be overwritten. However, if the user saves their LAT with the filename Locallat.txt, the client machine will reference both the msplat.txt and the locallat.txt to determine if an IP address is local or remote. So, by using the locallat.txt method, a user can, in theory, permanently bypass Proxy Server. The locallat.txt file is never overwritten unless the user does so manually.

What changes are made when Proxy Server is installed?

Server side changes:

* The Web Proxy, Winsock Proxy, and SOCKS Proxy services are installed and management items are added into the Internet Service Manager.

* An HTML version of the documentation is added into the %systemroot%\help\proxy\ directory.

* A cache area is created on an NTFS volume.

* The LAT table is constructed.

* Proxy Server Performance Monitor counters are added.

* Client installation and config files are added to the Msp\Clients folder. This folder is shared as Mspclnt and by default has the permissions set to Read for Everyone.

Client side changes:
* The LAT (msplat.txt) file is copied to the clients local hard drive.

* A WSP Client icon is added to control panel on Win3.X, Win95 and WinNT clients.

* A Microsoft Proxy Client Program Group is added

* The winsock.dll file is replace with Remote WinSock for Proxy. The old winsock file is renamed winsock.dlx.

* Mspclnt.ini file is copied to the client machine.

Proxy Server Architecture

To understand the architecture of Microsoft Proxy Server, you must first have a basic grasp of how Proxy works for outbound client requests. Here is a simple example:

Joe opens his browser to visit his favorite news site on the net. He types in the sites IP address which he has memorized because his visits often, instead of doing his job. The client compares the IP address Joe entered to the LAT table. Because the IP address is not found on the LAT, it is considered external. Since the client has determined that the IP address is external, it knows it must process the request through Proxy Server. The client hands Joe's request to Proxy Server. Proxy Server then checks the IP address against the access control applied by the Administrator. The Administrator has the ability to stop internal employees from visiting certain sites. Since Joe's request is not on the forbidden list applied by the Administrator, Proxy Server executes the request. Proxy contacts the website and requests the document Joe wanted. After Proxy server has received the information it requested, it stored a copy in its cache for later use and hands the request to the client machine. The website pops-up on Joe's browser.

Proxy Server Services: An Introduction

* WebProxy: Web Proxy normally functions with both clients and servers. As a server, it receives HTTP requests from internal network clients. As a client, it responds to internal network clients' requests by issuing their requests to a server on the Internet. The interface between the client and server components of the Web Proxy service provides chances to add value to the connections it services. By performing advanced security checks, the Web Proxy does more than relay requests between an internal client and a server on the Internet. The WebProxy service is an extensions of Internet Information Server 3.0. It consists of two following components: The Proxy Server ISAPI Filter and the Proxy Server ISAPI Application. The Web Proxy service is implemented as a DLL (dynamic link library) that uses ISAPI (Internet Server Application Programming Interface) and therefore runs within the IIS WWW process. The WWW Service must installed and running in order for proxy requests to be processed.

* WinSock Proxy: WinSock Proxy provides proxy services for windows sockets applications. WinSock Proxy allows winsock applications to function on a LAN and to operate as if it is directly connected to the Internet. The client app uses Windows Sockets APIs to communicate with another application running on an Internet computer. WinSock Proxy intercepts the windows sockets call and establishes a communication path from the internal

application to the Internet application through the proxy server. The process is totally transparent to the client. The WinSock Proxy consists of a service running on Proxy Server and a DLL installed on each client. The DLL it relies on is the Remote Winsock DLL that replaced the normal winsock.dll. WinSock Proxy uses a control channel between the client and the server to manage the ability of Windows Sockets messages to be used remotely. The control channel is set up when the WinSock Proxy client DLL is first loaded, and it uses the connectionless UDP protocol. The Winsock Proxy client and the WinSock Proxy service use a simple ack protocol to add reliability to the control channel. The control channel uses UDP port 1745 on the proxy server and client computers.

* SOCKS Proxy: Proxy Server supports SOCKS Version 4.3a. Almost all SOCKS V4.0 client applications can run remotely through SOCKS Proxy. SOCKS is a protocol that functions as a proxy. It enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of a SOCKS server, without requiring direct IP access. (To learn more about SOCKS, visit http://www.socks.nec.com/index.html).

Understanding components

This area will attempt to better define to the components of the architecture that we have used, but may not have defined.

ISAPI Filter

The ISAPI Filter interface is one of the components of the web proxy service. The interface provides an extension that the Web server calls whenever it receives an HTTP request.

An ISAPI Filter is called for every request, regardless of the identity of the resource requested in the URL. An ISAPI filter can monitor, log, modify, redirect and authenticate all requests that are received by the Web server. The Web service can call an ISAPI filter DLL's entry point at various times in the processing of a request or response. The Proxy Server ISAPI filter is contained in the w3proxy.dll file. This filter examines each request to determine if the request is a standard HTTP request or not.

ISAPI Application

The ISAPI Application is the second of the two web proxy components. ISAPI applications can create dynamic HTML and integrate the web with other service applications like databases.

Unlike ISAPI Filters, an ISAPI Application is invoked for a request only if the request references that specific application. An ISAPI Application does not initiate a new process for every request. The ISAPI Application is also contained in the w3proxy.dll file.

Proxy Servers Caching Mechanism

Microsoft Proxy Server handles caching in two different ways, Passive and Active

* Passive Caching: Passive caching is the basic mode of caching. Proxy Server interposes itself between a client and an internal or external Web site and then intercepts client requests. Before forwarding the request on to the Web server, Proxy Server checks to see if it can satisfy the request from its cache. Normally, in passive caching, Proxy Server places a copy of retrieved objects in the cache and associates a TTL (time-to-live) with that object. During this TTL, all requests for that object are satisfied from the cache. When the TTL is expired, the next client request for that object will prompt Proxy Server to retrieve a fresh copy from the web. If the disk space for the cache is too full to hold new data, Proxy Server removes older objects from the cache using a formula based on age, popularity, and size.

* Active Caching: Active Caching works with passive caching to optimize the client performance by increasing the likelihood that a popular will be available in cache, and up to date. Active caching changes the passive caching mechanism by having the Proxy Server automatically generate requests for a set of objects. The objects that are chosen are based on popularity, TTL, and Server Load.

Windows Sockets

Windows Sockets is the mechanism for communication between applications running on the same computer or those running on different computers which are connected to a LAN or WAN. Windows Sockets defines a set of standard API's that an application uses to communicate with one or more other applications, usually across a network. Windows Sockets supports initiating an outbound connection, accepting inbound connections, sending and receiving data on those connections, and terminating a session.

Windows socket is a port of the Berkeley Sockets API that existed on Unix, with extensions for integration into the Win16 and Win32 application environments. Windows Sockets also includes support for other transports such as IPX/SPX and NetBEUI.

Windows Sockets supports point-to-point connection-oriented communications and point-to-point or multipoint connectionless communications when using TCP/IP. Windows Socket communication channels are represented by data structures called sockets. A socket is identified by an address and a port, for example;

131.107.2.200:80

Access Control Using Proxy Server

Controlling Access by Internet Service

Proxy Server can be configured to provide or restrict access based on Service type. FTP, HTTP, Gopher, and Secure (SSL) are all individually configurable.

Controlling Access by IP, Subnet, or Domain

Proxy allows an administrator to control access based on IP Address, Subnet or Domain. This is done by enabling filtering and specifying the appropriate parameters. When configuring this security, you need to decide if you want to grant or deny access to an IP address, subnet, or domain. By configuring Proxy Server correctly, you can also set it up to use the internet as your corporate WAN.

Controlling Access by Port

If you are using the WinSock Proxy service, you can control access to the internet by specifying which port is used by TCP and UDP. You can also grant or deny, activate or disable certain ports based on your needs.

Controlling Access by Packet Type

Proxy Server can control access of external packets into the internal network by enabling packet filtering on the external interface. Packet filtering intercepts and evaluates packets from the Internet before they reach the proxy server. You can configure packet filtering to accept or deny specific packet types, datagrams, or packet fragments that can pass through Proxy Server. In addition, you can block packets originating from a specific Internet host.

The packet filtering provided by Proxy Server is available in two forms, Dynamic and Static.

Dynamic packet filtering allows for designed ports to automatically open for transmission, receive, or both. Ports are then closed immediately after connection has been terminated, thereby minimizing the number of open ports and the duration of time that a port is open.

Static packet filtering allows manual configuration of which packets are and are not allowed.

By default, the following Packet settings are enabled on Proxy Server (by default, ALL packet types are blocked except the ones listed below, known as Exceptions):

Inbound	ICMP ECHO (Ping)
Inbound	ICMP RESPONSE (Ping)
Inbound	ICMP SOURCE QUENCH
Inbound	ICMP TIMEOUT
Inbound	ICMP UNREACHABLE
Outbound	ICMP ANY
Inbound	TCP HTTP
In/Outbound	UDP ANY (dns)

Logging and Event Alerts

Events that could affect your system may be monitored, and, if they occur, alerts can be generated. The items listed below are events that will generate alerts:

Rejected Packets: Watches external adapter for dropped IP packets. Protocol Violations: Watches for packets that do not follow the allowed protocol structure. Disk Full: Watches for failures caused by a full disk.

When any of the events above occur, an alert is sent to the system log in the NT Event Viewer, or can be configured to e-mail a pre-defined person.

When the system logs information concerning Access Control, it does so to a log file stored in the %systemroot%/system32/msplogs/ directory. The log file itself is named Pfyymmdd.log (Where yy=Current year / mm= Current Month / dd= Current day).

The Packet log records information related to the following areas:

Service Information (Time of Service, Date and Time)

Remote Information (The Source IP Address of a possible Intruder, along with port and protocol used)

Local Information (Destination IP Address and port)

Filter Information (Action taken and what interface (network adapter) issued the action)

Packet Information (Raw IP Header in Hex and Raw IP Packet in Hex)

Encryption Issues

Proxy Server can take full advantage of the authentication and security features of Internet Information Server and SSL tunneling.

SSL supports data encryption and server authentication. All data sent to and from the client using SSL is encrypted. If HTTP basic authentication is used in conjunction with SSL, the user name and password are transmitted after

the client's SSL support encrypts them.

If your are wanting to take advantage of PPTP to provide additional flexibility and security for your clients, you can configure Proxy Server to allow these packets (GRE) to pass through.

Other Benefits of Proxy Server

RAS

Proxy Server can take full advantage of Windows NT Remote Access Service (RAS). Proxy can be configured to dial on demand when an internal client makes a request that must be satisfied from the external network. The RAS feature can be configured to only allow connectivity during certain hours. The Dial-Up Network Scripting tool can aslo be used to automate certain process using Proxy Server and RAS. For company's who have a standard constant connection (ISDN, T1, T3) to the Internet, the RAS ability provided by Proxy Server can be used as a back-up should your constant connection fail.

IPX/SPX

Microsoft Proxy Server was developed with support for Internet Packet Exchange/Sequenced Packet Exchange or IPX/SPX. IPX/SPX is a transport protocol group somewhat similar to TCP/IP.

There are many situations when a client computer may have both IPX/SPX and TCP/IP protocols installed although the company's internal network may only use IPX/SPX. Simply disabling aTCP/IP while on the LAN will not get the IPX/SPX component of the Proxy client software working. You will need to go into Control Panel, open the Wsp Client icon and check the box that reads "Force IPX/SPX protocol". This must be done because even though the TCP/IP protocol was disabled, the WinSock Proxy Client still detects its presence and will attempt to create a standard IP socket. By enabling the "Force IPX/SPX Protocol" option, this problem should disappear.

Firewall Strategies

A firewall is a system that enforces access control policies. The enforcement is done between an internal, or "trusted" network and an external, or "untrusted" network. The firewall can be as advanced as your standards require. Firewalls are commonly used to shield internal networks from unauthorized access via the Internet or other external network.

Logical Construction

The single basic function of a firewall is to block unauthorized traffic between a trusted system and an untrusted system. This process is normally referred to as Filtering. Filtering can be viewed as either permitting or denying traffic access to a network.

Firewalls know what traffic to block because they are configured with the proper information. This information is known as an Access Control Policy. The proper approach to an access control policy will depend on the goals of the network security policy and the network administrator.

Exploring Firewall Types

In the origins of firewalls, there were two types. These two types have now grown and overlapped each other to the point where distinction is hard. We will explore the differences between these two types and discuss Firewall building topologies.

Network Level Firewalls

Network level firewalls operate at the IP packet level. Most of these have a network interface to the trusted network and an interface to the untrusted network. They filter by examining and comparing packets to their access control policies or ACL's.

Network level firewalls filter traffic based on any combination of Source and Destination IP, TCP Port assignment and Packet Type. Network Level firewalls are normally specialized IP routers. They are fast and efficient and are transparent to network operations. Todays network level firewalls have become more and more complex. They can hold internal information about the packets passing through them, including the contents of some of the data. We will be discussing the following types of network level firewalls:

* Bastion Host
* Screened Host
* Screened Subnet

Bastion Host Firewall

Bastion host are probably one of the most common types of firewalls. The term bastion refers to the old castle structures used in europe, mainly for draw bridges.

The Bastion host is a computer with atleast one interface to the trusted network and one to the untrusted network. When access is granted to a host from the untrusted network by the bastion host, all traffic from that host is allowed to pass unbothered. In a physical layout, bastion hosts normally stand directly between the inside and outside networks, with no other intervention. They are normally used as part of a larger more sophisticated firewall.

The disadvantages to a bastion host are:

- After an Intruder has gained access, he has direct access to the entire network.
- Protection is not advanced enough for most network applications.

Screened Host Firewall

A more sophisticated network level firewall is the screened host firewall. This firewall uses a router with at least on connection to trusted network and one connection to a bastion host. The router serves as a preliminary screen for the bastion host. The screening router sends all IP traffic to the bastion host after it filters the packets. The router is set up with filter rules. These rules dictate which IP addresses are allowed to connect, and which ones are denied access. All other packet scrutiny is done by the bastion host. The router decreases the amount of traffic sent to the bastion host and simplifies the bastions filtering algorithms.

The physical layout of a Screened Host is a router with one connection to the outside network, and the other connection with a bastion host. The bastion host has one connection with the router and one connection with the inside network.

Disadvantages to the Screened Host are:

- The single screen host can become a traffic bottleneck
- If the host system goes down, the entire gateway is down.

Screened Subnet Firewalls

A screened subnet uses on or more addition routers and on more additional bastion hosts. In a screened subnet, access to and from the inside network

is secured by using a group of screened bastion host computers. Each of the bastion hosts acts as a drawbridge to the network.

The physical layout of a Screened subnet is somewhat more difficult, but the resu

Disadvantages to using this type of firewall are:

- The can be two or three times more expensive than other types of firewalls
- Implementation must be done by some type of security professional, as these types of firewalls are not for the un-initiated.

Application Level Firewalls

Application level firewalls are hosts running proxy server software located between the protected network and the outside network. Keep in mind that even though Microsofts product is called Proxy Server 2.0, it is actually a stand alone Bastion Host type of system. Microsoft Proxy Server can also, single-handedly, disguise your internal network to prevent mapping. Microsoft Proxy Server 1.0 did not have many of the advanced features presented in version 2.0. The 1.0 version can definitely be called a true proxy server, while the 2.0 version is more of a firewall.

Viewed from the client side, a proxy server is an application that services network resource requests by pretending to be the target source. Viewed from the network resource side, the proxy server is accessing network resources by pretending to be the client. Application level firewalls also do not allow traffic to pass directly between to the two networks. They are also able to use elaborate logging and auditing features. They tend to provide more detailed audit reports, but generally, as stand alone security unites, do not perform that well. Remember that an Application level firewall is software running on a machine, and if that machine can be attacked effective and crashed, in effect, youre crashing the firewall.

You may wish to use an application level firewall in conjunction with network level firewalls, as they provide the best all around security.

That's it for now.

NeonSurge
The Rhino9 Team.
http://rhino9.abyss.com