UserGate Proxy Server for Windows

Windows Strengths and Weaknesses   The overwhelming majority of computers, both personal and corporate, use Microsoft Windows, which has included Internet access for well over a decade and as Windows became more complex, so has its Internet connectivity software. Windows 98 Second Edition introduced Internet Connection Sharing (ICS) to provide group access to the Internet from a local network. More complexities were added with the outbreak of Routing and Remote Access Service in Widows 2000 Server with its Network Address Translation (NAT) functions.   It took awhile before experts noticed that ICS has specific shortcomings. ICS changes network card addresses, which can cause problems on intranets. Because of this, ICS can only be used in small office or home networks and even then, ICS in office networks is not recommended, because there is no user authorization or validation with ICS. Even using it on a home network makes any connection to the Internet insecure, since it is so easy for criminals to gain access to your computers by falsifying where they are coming from (their IP and MAC addresses).

Some Help is Needed   Windows can organize Internet sharing, but security has never been a strong point. In practice either hardware or software solutions from other companies are generally purchased to provide the security solutions needed. One of the more important of these is UserGate Proxy Server.   UserGate Proxy Server provides local network users with a secure Internet access by defining policies of this access, forbidding particular Internet resources, and limiting traffic or time of a user's work on the Internet. Additionally, UserGate can keep distinct traffic calculations of users and of protocols, which greatly simplifies Internet traffic cost control. Lately, among Internet Service Providers (ISP) there has been a tendency towards unlimited traffic and for that purpose, UserGate Proxy Server provides a very flexible system of rules.   UserGate Proxy Server with NAT support works on Windows 2000/2003/XP with the Internet (using the standard TCP/IP protocols). UserGate can also work on Windows 98 and Windows NT 4.0, but without NAT support. UserGate does not require any special resources for its operation; it simply needs a relatively small amount of hard drive memory for its cache and log files. UserGate can also be installed on a dedicated computer to maximize your network's resources.

Proxy Servers   Your web browser (whether it is Internet Explorer, Firefox, Safari, Netscape, Opera or Mozilla to name the most popular) is already able to cache documents. However, significant disk space is not reserved for these purposes if the Internet connection is shared by an entire office. The reason for this is that the probability of one person visiting the same web pages is far less than if dozens or hundreds of people are sharing the connection. Creating a common cache for a company can greatly decrease bandwidth waste as well as make almost instantaneous the receipt of documents that are commonly accessed by employees. UserGate Proxy Server can also link with the external cascade proxy servers (of your Internet Service Provider) to increase the speed of receiving data and reduce your Internet bills (traffic costs for a provider are usually less when a proxy server is used).

Program Configuration   Configuring the cache settings is done from the «Services» page. The first step is to enable the cache, then you can set its separate options, which include caching of POST requests, dynamic objects, cookies, and FTP content. You can also set the size of the disc space for the cache and the time-to-live of cached documents.   Other options must also be set before you can start working with the program. As a rule, this task is completed in the following order: 1. Create users of the program.   2. Configure DNS and NAT on the UserGate server. At this stage you can configure NAT using the wizard.   3. Set parameters of the various protocols (HTTP, FTP, SOCKS), the intranet interface on which they will be listened for, and whether cascading will be done. All of these can be set at their&nbsp;&nbsp; corresponding pages of service settings.   4. Configure the network connection on each client computer, including gateway and DNS in TCP/IP in network connection properties, which must be set.   5. Create an Internet access policy.

Modules to Make Things Easier   To make the program more user-friendly, we divided it into several modules: &nbsp;   The Server module is started at a computer that has Internet access. This module controls the execution of all tasks.   &nbsp;   &nbsp;   UserGate administration is performed with the help of a special module: UserGate Administrator, which handles all server settings.   &nbsp;   &nbsp;   UserGate Authentication Client is a client application installed on each user's computer. This module monitors and controls user authorization to the UserGate server, if you choose an authorization independent of IP or IP+MAC.   &nbsp;

Security and Permissions   UserGate Proxy Server locks out unauthorized access. Each user can be authorized automatically by their IP address alone or by a correct combination of IP and hardware (MAC) address. Each user can be assigned specific permissions   To make it easy to add users and to quickly assign the same permissions to a group of similar users a separate page is provided for the managing of users and groups. Groups make it easy to manage users that should have common settings, including network access and rates. You can create as many groups as you need. Groups are usually created based on company structure and hierarchy.   Each group can be given its own rate that is used to manage Internet access expenses. A default rate can be set or left empty, in which case the connections of all users in a group are not paid unless a different rate is set in a user's own properties.   There are a number of default NAT rules provided in the program. These are access rules through Telnet, POP3, SMTP, HTTP, ICQ and other protocols. While setting group properties you can identify which rules will be applied to the group and its users.   A dial on demand option can be used when an Internet connection is through a modem. In this case the modem dials up the connection only when it is requested. Dial on demand can also be used with ADSL, if in order to get connected to the Internet provider it is necessary to dial up a VPN connection. In this case the VPN connection can be set as dial on demand.   If a computer with UserGate is in an Active Directory domain, users can be imported to it and then divided into groups that need similar access rights: authorization type, rate, NAT rules (if group rules do not fully meet the user's needs).

Authorization Types and Rules   UserGate Proxy Server supports several authorization types, including authorization through Active Directory and Windows Login, which allows integrating UserGate into existing network infrastructures.   UserGate uses its own client authentication module for some types of authorization. Depending on the type of authorization you choose it is necessary to indicate, in user options, either the user’s IP address (or IP address range), assign a login (username and password) or assign just a username. If you want to send to a user, reports of their Internet traffic use you can enter the user’s e-mail here.   UserGate rules can be more flexibly configured than RRAS Remote Access Policy. Using rules you can lock access to specific URLs, limit traffic on certain protocols, set time limits, set a maximum file size that a user can download, etc. Windows does not provide the functionality needed to fulfill these tasks.   Rules can be created with the help of the wizard provided. Each rule has application conditions and an object it is executed when one or more conditions are met. For examples, close a connection, assign a rate or speed, etc. Conditions include protocols used, time of work, a user’s traffic limits (incoming and outgoing), money remaining on account, as well as, IP address list and URL list. Settings also allow the specifying of any file extensions that users cannot download.   In a number of organizations the use of instant messengers, such as ICQ, is prohibited. This is easy with UserGate. To prohibit ICQ you simply create a rule, locking out any connection with the host ‘*login.icq.com*’ and apply it to all users.   UserGate Proxy Server provides rules to allow varying rates for day or night time access, to local or common resources (if such variations are offered by your Internet provider). For instance, for switching between day and night rates two rules are created: one that performs the switching at a fixed time from day to night rate and the other that switches back to the day rate.

DNS and NAT Settings   DNS (Domain Name System) is what is used on the Internet so you don’t have to remember a site’s numbers (its real Internet address), such as 53.128.182.67), but instead you can just remember its name, such as www.famatech.com. One of the controlling parts of the Internet’s DNS is the DNS server, which is a computer (there are many DNS servers) on the Internet that translates the names of sites to their numbers, so when your browser goes to www.famatech.com, the DNS server knows the correct IP number to send the browser request to.   The DNS setting in UserGate Proxy Server is simply the locations (IP addresses) of one or two of these DNS servers (the closer the DNS server is to your ISP’s physical location, generally the better), where each client’s DNS requests will be forwarded to. It is necessary to indicate the IP address in your network interface of UserGate Proxy Server as the gateway and DNS in the TCP/IP properties of each user’s network connection on their local computer.   There is another way to set the DNS. You can add a new NAT rule, in which the IP receiver (the internal interface) and the IP sender (the external interface) are set to port 53 and the protocol to UDP. If you use this method, this rule must be applied to all users. In connection settings of each local computer, the IP address of the ISP’s DNS servers must be set as the DNS and the IP address of UserGate Proxy Server set as the gateway on each local computer.   Mail clients can be set either through port mapping or through NAT. If instant messengers are allowed to be used in the organization, the network settings must be changed for them: both user firewall and proxy, the IP address of the internal network interface of UserGate Proxy Server must be indicated, and the protocol HTTPS or SOCKS needs be selected. If you use Yahoo Messenger, you should keep in mind that when you work through a proxy server, Yahoo’s chat rooms and video chats are unavailable.   Statistics for each user are recorded in a log. These include data on the time each connection started, its duration, total cost, the URLs and IPs visited, the number of bytes received and bytes sent. It is impossible to cancel or falsify the recording of any of this information about user connections in UserGate Proxy Server’s statistics file. The statistics can be viewed either from the Server Administrator or from a special module Statistics. Statistics data can be filtered by user, protocol and time period; and these stats can be exported to Microsoft Excel for further processing.   The early versions of UserGate Proxy Server cached only HTTP (web) pages. The latest version introduced new components designed to guarantee information security. Now UserGate users can take advantage of the built-in firewall and Kaspersky Antivirus modules. The firewall can control (permit or block) specific TCP ports and can also publish a company’s resources on the Internet. UserGate Proxy Server processes all packets received from the network. Every port that is open in the program, for example HTTP, SOCKS and others, are either selected by the administrator or can be opened in the firewall automatically. You can see which ports are open in the auto rules table on the Firewall Rules page.   Future development plans for UserGate Proxy Server include creation of its own VPN server—so you have an alternative VPN solution to that offered by Windows—an introduction of a mail server that has its own antispam support and the development of an intelligent firewall at the application level.

About the Author

Entensys Corporation   http://www.entensys.com

Source: http://americanahost.com