InterGate POLICY MANAGER

IMPORTANT - Please Read First!

This document outlines the system requirements, installation and usage of InterGate Policy Manager for Windows, and it is highly recommended to read it in full before proceeding.

About InterGate Policy Manager Suite

The InterGate Policy Manager Suite offers unequalled flexibility and extensibility for the enterprise, small business or educational establishment, to manage and control user Internet activity. The deployment of InterGate Policy Manager Suite greatly increases productivity, enhances security, reduces legal liability and optimises the use of IT resources for any organization.

The suite includes InterGate Policy Manager, InterGate Inspect, InterGate Intercept and InterGate Intelligence. InterGate Policy Manager provides a comprehensive platform for seamless integration with the Inspect, Intercept and Intelligence components.

The Inspect web filter is founded in a database of over 100 million sites covering 80 well-organized categories which are continually updated.

The Intercept application filter has the ability to block or allow users from accessing applications such as Instant Messaging (IM) applications such as AIM (AOL Instant Messenger), ICQ, Yahoo Messenger, MSN Messenger; Peer-to-Peer applications like eDonkey, eMule, Kademlia, BitTorrent, Gnutella (Morpheus, LimeWire), Kazaa and the Internet telephony application, Skype.

The Intelligence logging and reporting tool presents fully drillable reports showing both summary and detailed information regarding the use of Internet resources on your network.

System Requirements

To use InterGate, the computer it is installed on must have access to the Internet, either directly via an account with an Internet Service Provider or as part of your organization’s network configuration. The computer must be able to connect and use the Internet before you install the software.

At a minimum, two separate Ethernet interfaces are required each of which must be on a separate physical segment. We recommend using two cards, as this will keep your Local Network physically separated from your Internet connection, offering you the greatest security for your local network.

InterGate will run on any PC running Windows 2000, XP, or 2003 Server, however for basic performance reasons we recommend at least:

Pentium 3 700Mhz, 512Mb memory, 80Gb free disk space

As the number of client computers increases and/or the configuration complexity increases, the processing capability, memory allocation and hard drive capacity must be increased appropriately: In high bandwidth requirement installations we recommend assigning the fastest available processor and more memory. For high traffic logging and reporting, we recommend installing an additional large hard drive, dedicated to the task of storing the data.

Installing InterGate

1. Double-click the InterGateInstaller.exe file and follow the on-screen instructions.

The InterGate software will have been installed into a folder named Vicomsoft, which is located in your Program Files folder on your Hard Disk

2. Double click the intergate.exe application icon in the installed folder, or use the Desktop shortcut if created.

3. If you already have a serial number (either full or demo), enter it into the box provided, and then click the Activate button

If you do not have a serial number to enter, click the Get Demo License button to apply for and activate a trial license and follow the on-screen instructions.

If you wish to purchase the software, click the Purchase Now button and follow the on-screen instructions.

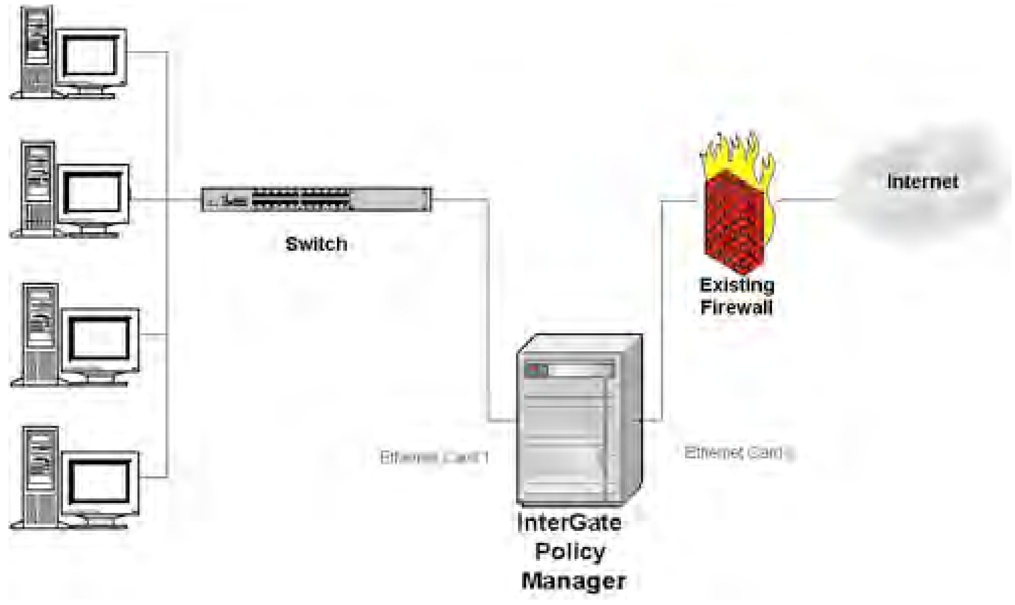
If you do not have a serial number and do not wish to proceed further, click the Quit button.

4. InterGate will now be automatically configured by Auto Setup. You may run this Auto Setup sequence at any time by selecting Auto Setup from the Network menu when InterGate is turned off.

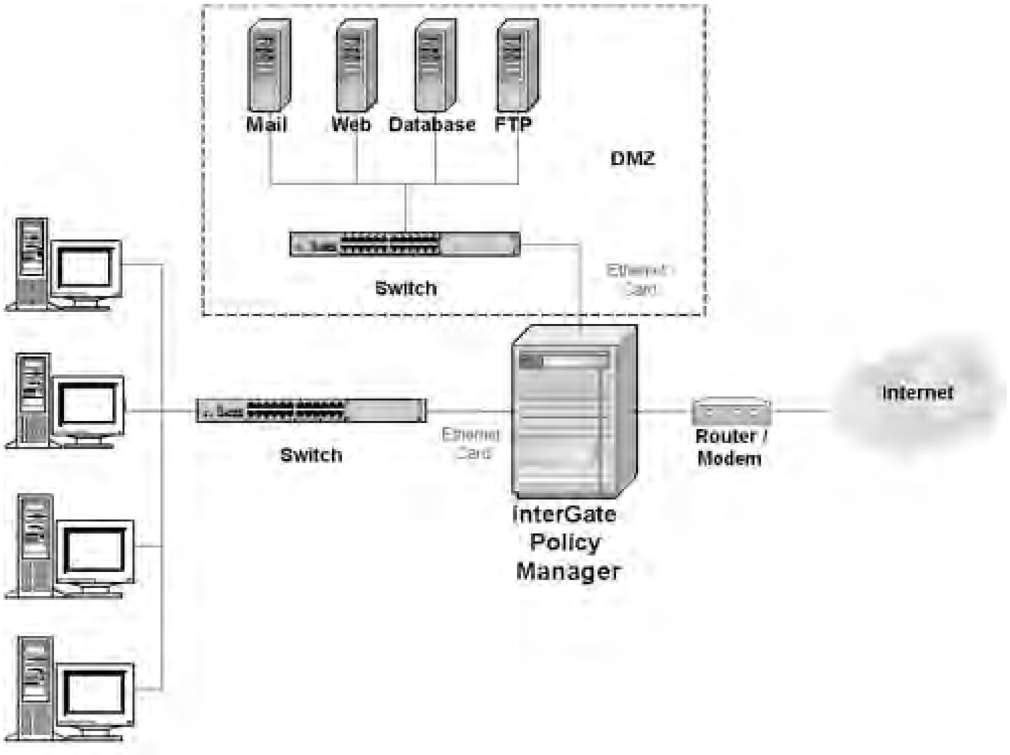
Auto Setup will use your machine's existing Internet configuration settings to configure InterGate.

- Select either a Router or Bridge setup

A Bridge setup will configure InterGate as a policy management device only, allowing it to be integrated into your existing network to give content filtering, application filtering, logging and reporting facilities where an existing firewall and/or router is in use. It is completely transparent and does not require you to change any network settings. The following shows InterGate being used for content filtering, logging and reporting where an existing firewall is already in place:



A Router / Firewall setup will configure InterGate as a firewall and router for all your machines on the network, in addition to providing content and application filtering, logging and reporting. You may have to change networking setup on your client computers, and possibly your servers, to operate in this mode. The following diagram shows InterGate being used as a firewall with content filtering etc. The DMZ is optional and its setup is dealt with in the Online Help.



5. Auto Setup will ask some basic questions about your network configuration requirements. It may also be necessary to enter one or more unused IP addresses in order to create the configuration, although Auto Setup will suggest IP addresses to use. You will have to select an “Internet” and a “Local” network card.

Please note that you can manually configure InterGate to have more than two network ports; this may be required if you have a large network or connectivity requirements not directly supported by Auto Setup. You can also change the settings of the ports at any time. Full details on this can be found in the Online Help.

6. Auto Setup will configure a default Internet Filtering policy for a typical installation and display it. This policy will apply to all computers connected to the network via InterGate, but not the InterGate machine itself. (Note that per-user / group policies can be configured once the initial installation is completed).

If you wish to make adjustments to this policy you may do so before proceeding, but in most cases simply click the ‘Install’ button to continue.

The Inspect filter controls access to web sites which are deemed unacceptable, such as those with sexually explicit or drug related content. Content is categorized, as indicated by the checkboxes shown. Enabling a checkbox will block access to that category of site. The default settings will be sufficient for most requirements.

The Intercept filter controls usage of Peer to Peer, Instant Messaging and Voice over IP applications, as indicated by the displayed checkboxes. Enabling a checkbox will block use of the selected application.

The User Defined Filters allow specific or wildcarded sites to be specifically allowed or prohibited, and act as a means to override the Inspect filter.

The Protocol Filters allow specific protocols, (ie FTP, News) to be blocked.

The Policy Manager enabled checkbox enables or disables filtering for all users.

7. InterGate is now ready to be used, and a Set Up Complete page will be displayed showing a summary of your configuration as well as resources to assist you in configuring client machines and other topics.

Help and Documentation

InterGate includes full documentation in the form of Online Help, which can be accessed from the Help option in the About menu.

Further help can be found via our support web site:

http://www.vicomsoft.com/support/