Internet Management Through WinGate

WinGate contains all of the necessary tools to track Internet activity and allows you to take appropriate actions to safeguard against identified abuse. Managing Internet usage is a necessity in today's workplace. When your employees use the Internet for non-business related activity while on the job, the result is a loss in productivity, reduced bandwidth available to customers trying to reach you online, and in some cases, legal penalties. WinGate contains a variety of features and plug-ins designed to assist administrators to ensure that Internet usage is not abused, and that users comply with company policies.

WinGate's log files contain all of the information needed to monitor Internet traffic on the network. WinGate creates a log file that displays all Internet traffic, as well as logs specific to certain protocols (WWW - browsing, FTP - file transfer, etc.). This gives administrators the ability to view specific Internet activities. Administrators are also able to view Internet traffic in "real time" within the WinGate interface (GateKeeper), letting you see user activity live.

To prevent unauthorized Internet traffic, WinGate allows the creation of policies/black or white lists. These lists can be enforced network wide, or specific to users and groups. This means that you can deny one or a select group of employees' access to unapproved web sites. Users and groups can be imported from an NT user database, and authentication for users can be accomplished through a user name and password, IP address, or computer name.

WinGate offers a wide variety of criterion to scale Internet access rights, including:
Website - what websites can or cannot be accessed
Time - define specific timeframe users are allowed to access the Internet
Application - what applications (e.g. IE, Outlook) are permitted to access the Internet

The Transparent Redirection (TR) feature in WinGate ensures that Internet requests made through the WinGate Internet Client (WGIC) or Network Address Translation (NAT) are routed through the proxy level of communication with no special configurations required. TR allows administrators to create policies in a centralized location, and benefit from applications that require proxies, such as the WinGate plug-ins: PureSight Content Filter and Kasperksy AntiVirus Plugin.

For additional protection, the PureSight for WinGate plug-in is available. PureSight for WinGate, a content filtering solution, utilizes a primary Internet filter technology based on AI (Artificial Intelligence), which previews the content of a website, determines if it is inappropriate, and blocks the site if necessary. PureSight for WinGate separates itself from other filtering solutions because it is dependant upon its own ability to determine if the content of sites is suitable for users, as opposed to the imperfect science of regularly updating and maintaining lists of unacceptable sites.

Though WinGate is widely recognized as the preeminent Internet sharing/firewall solution, it also provides a comprehensive solution for maintaining the integrity of the Internet connectivity that it provides.

PHONE: (519) 633-9551   E-MAIL: sales@ccsoftware.ca   WEB SITE: www.ccsoftware.ca