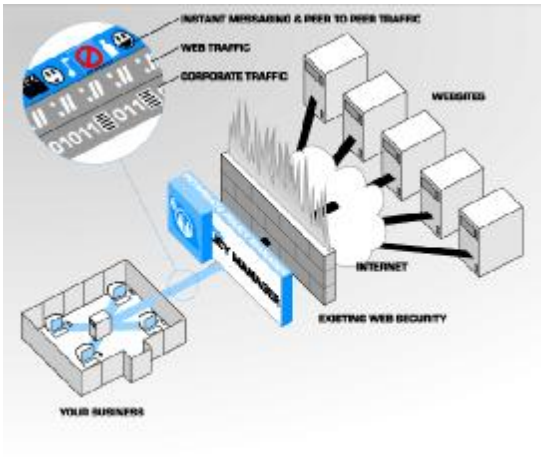
InterGate Intercept works together with InterGate Policy Manager to control the access of Instant Messaging, Peer-to-Peer and IP telephony applications.



InterGate Intercept lends administrators the ability to block or allow access to Instant Messaging 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.

InterGate Intercept provides signature-based blocking of multiple IM and P2P protocols. The module's deep stateful packet inspection makes sure that even applications that try to circumvent ordinary firewalls and web filters are blocked, as most IM and P2P applications will try to use a different connection method (i.e. via a proxy and/or using a different underlying protocol) if a firewall blocks their main method of communication.

Instant Messaging (IM)
Instant Messaging (IM) usage in the enterprise has its benefits but unsanctioned use of these applications raises many valid productivity and security concerns among Enterprise Executive, Technology and Security Officers.

IM protocols were designed to allow communication between consumers across the public Internet under any possible configuration and, therefore, are very difficult to control with existing network security products. IM applications treat network security as just another network problem to be circumvented. Furthermore, these public IM products generally contain no provisions for message logging, confidentiality or security.

InterGate Intercept's IM filtering recognises protocols of IM applications on a packet data level then applies pre-defined security policies when such protocols are detected.

Peer-to-Peer (P2P)
Peer-to-Peer (P2P) file sharing services allow an employee to circumvent corporate security measures. The very nature of the P2P client design is to evade firewalls and general network security. Additionally, blocking P2P at the firewall has proved to be extremely difficult because port blocking, as a means to controlling P2P, is very limited. P2P port usage can be dynamic and P2P protocols are not standards-based, making them very difficult for administrators to detect much less control. P2P packets cannot be classified simply by looking at packet headers such as IP address and port number. Deeper packet inspection is required for effective P2P control.

InterGate Intercept's P2P filtering is done by a deep packet inspection searching for known data patterns such as login requests from clients to P2P servers.

Skype
Skype is a proprietary peer-to-peer (P2P) voice over Internet protocol (VoIP) that intentionally evades network policies and may expose enterprises to security and liability risks. Its network is defined by all users of the free desktop software application. Skype users can speak to other Skype users, call traditional telephone numbers, receive calls from traditional phones, and receive voicemail messages. In addition, Skype allows its users to send instant messages and transfer files to other users in the Skype network. Because it was designed to work in overly restrictive environments, it is difficult to control via traditional means, such as firewalls.

InterGate Intercept Filters

InterGate Intercept's Skype detection depends on stateful inspection of transmitted Skype data taking into account connection endpoints, the timings between connections and the protocols used, as normal protocol examination for data patterns is not possible due to the encryption technology used by Skype.

US & Canada: 1 888-842-2608
UK & Europe: +44 (0) 1202 757560
www.vicomsoft.com