FaceTime™

FaceTime RTG500™

Real-time Security for the Real-time Enterprise

White Paper

WP0104-0405

Content

Introduction

The Real-time Enterprise

Business has always been about time-sensitivity and speed in communications—getting the right information to the right people at the right time to be able to make the right decisions. Innovations in computing and communication technologies have been largely responsible for doing business faster, and better. Instant Messaging (IM) and Peer-to-Peer (P2P) networking represent the next generation of powerful communication technologies that are breaking cost barriers while increasing employee productivity and information sharing.

Growth of IM and P2P

IM is everywhere – on desktops, PDAs, cell phones, pagers, etc. According to International Data Corporation (IDC), the rapid consumer adoption of IM networks makes IM the fastest growing communication channel in history. In 2001, the public IM networks, AOL, Microsoft MSN and Yahoo! accounted for over 100 million users, growing to 400 million users by 2004. Meta Group predicts that the number of IM users in North American businesses will grow from 12 million in 2002 to 95 million in 2007. Gartner expects IM to surpass e-mail in worldwide traffic by 2006.

P2P applications, like Kazaa and Morpheus, are also deeply entrenched inside corporate networks. In a recent study spanning 560 companies, ranging from 10 to 45,000 employees, P2P applications were found installed in 77 percent of the companies. The survey found that every company in its sample with more than 500 employees had at least one installation of a P2P application.

The motivation for adopting of IM in business is the need to communicate and multi-task in real-time. Business users have discovered the value of instant messaging – they have virtual conferences, collaborate on projects, augment phone conversations, and exchange transaction instructions. Other benefits of IM include community building and collaboration among multiple corporate locations, remote employees, telecommuters, vendors and customers, and cost savings from reduced telephony costs, better accuracy of transactions via written communications, and more efficient markets by communicating in real-time.

IM and P2P: The Good, The Bad and the Ugly

While most people accept the enterprise productivity benefits of using IM, the mention of P2P usually conjures up images of music and video file sharing and misuse of network bandwidth. This narrow view, however, ignores the real promise of P2P technologies. P2P computing holds the promise for efficiencies in content distribution and service delivery without the need for centralized servers.

Today, the risks associated with use of IM and P2P applications stem from the following facts:

- The applications are downloaded and installed by employees without any IT involvement
- The applications were designed to get around existing security mechanisms such as firewalls
- Increasingly, the installed based of these applications makes them a natural target for exploiting their vulnerabilities by hackers, spread of viruses and compromising enterprise network security

- IT organizations have no means to detect the presence of these applications, how they are being used and how they bypass security mechanisms, including breaching firewalls through random port crawling, intrusion detection systems and anti-virus scanners.

Benefits aside, enterprises are wary of adopting IM because of the many unknown business and security issues that result from illegitimate use and social engineering attacks as well as from exploiting actual architectural vulnerabilities of the applications. P2P applications have recently come under a lot of attack from the RIAA (Recording Industry Artists Association) and the MPAA (Motion Picture Association of America) for fostering copyright violation from illegal sharing of copyrighted material resulting in untold losses to the music and film industries. Enterprises whose employees use these applications are also being issued warnings that they could be held liable for these copyright infringements.

Having a clear understanding of the technology and its most common applications best prevents illegitimate use and social engineering attacks. Enterprises should create a set of best practices and use policies that act as recommendations for proper use.

The design vulnerabilities of IM and P2P applications are open to exploitation by hackers and other malicious code writers propagating viruses, trojans and worms. This can potentially result in serious compromise of network infrastructure and bring the business to a grinding halt causing huge financial losses.

Safe Adoption of Disruptive Technologies

Most companies today are attempting to prevent the use of IM and P2P applications from within their corporate networks. However, these are fundamentally disruptive technologies, just like the PC, email, and the Internet, and truly hold the potential for significant benefits to business from lowering the cost of communications and information sharing to increasing productivity.

Realizing the growing need of companies to embrace these new forms of real-time communications, yet manage and control their use, FaceTime provides RTG500, the industry's first security gateway for real-time communications, designed with the goal of enabling companies to safely adopt and embrace these emerging technologies.

This white paper provides detailed information on the security issues of IM and P2P applications, and how RTG500 addresses these issues and helps make these applications safe for business.

Application Architectures

IM

IM applications use a client-server architecture. The most popular public IM clients, e.g. AIM from America Online, MSN and Windows Messenger from Microsoft, and Yahoo! Messenger from Yahoo!, communicate with a set of servers managed by the respective IM provider, using a proprietary non-standard protocol. The IM network servers not only manage the exchange of messages back and forth between two or more users on the network, but also perform authentication and manage online presence status of the users. The IM clients have a buddy list or a contact list showing presence of other users on the same network.

The figure on the next page shows the flow of communications between AIM clients and the AIM network. This is typical of most public IM applications.

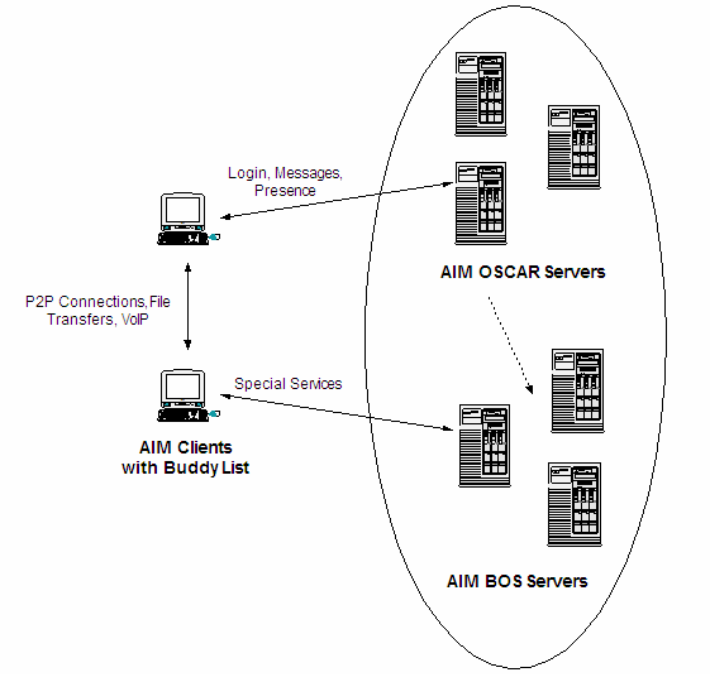

Figure 1: Client-server architecture of AIM

The AIM client signs on to the AIM OSCAR servers at login.oscar.aol.com. Upon successful login, OSCAR issues a session cookie to the client so that the client can use special services, e.g. advertisements, buddy-search, etc., that are provided by the AIM BOS servers. For certain non-text functions, the AIM clients can connect to each other directly as peers and exchange content, such as files, images, etc.

P2P

P2P applications on the other hand do not have a centralized server model. The client machines connect to each other directly without need for any central servers. Some client machines can be setup to function as supernodes. Supernodes store information where the most requested content resides making searches as fast as possible.

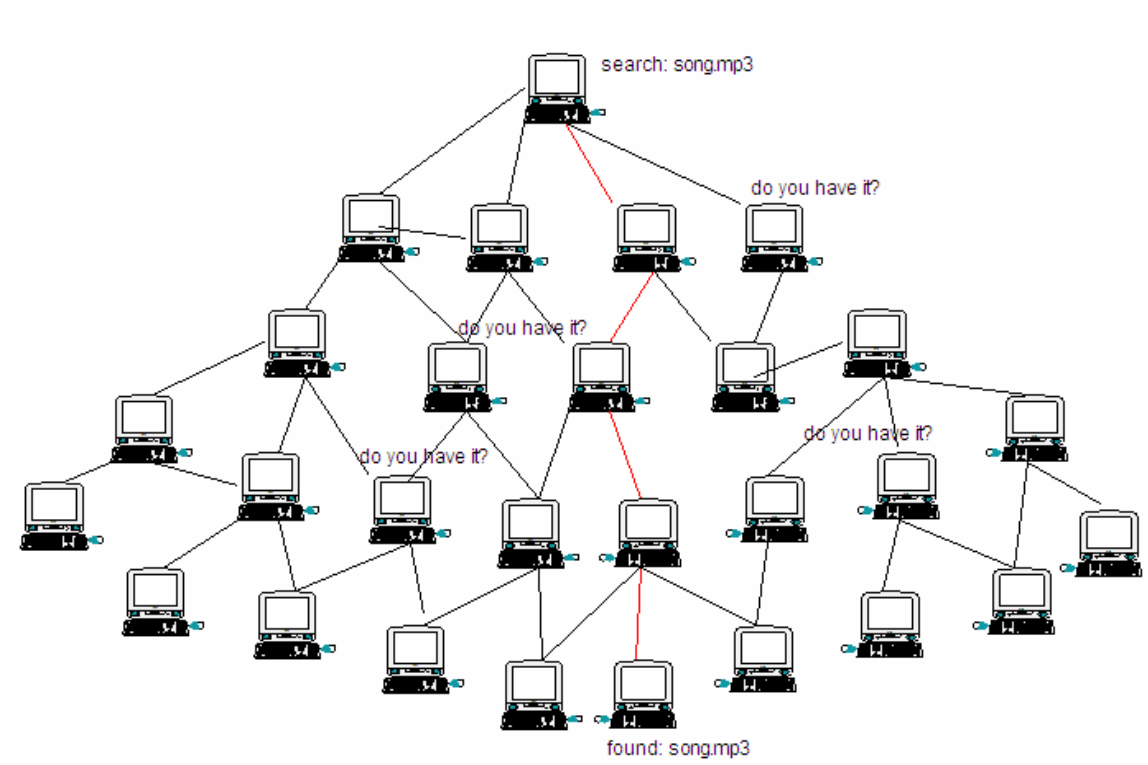

Figure 2: P2P application architecture

Kazaa has a layered architecture and implements a notion of supernodes. All Kazaa clients upload the information on which files they are sharing to their nearest supernodes. Supernodes help to speed up searches and help in locating peers for efficient downloads. In the Gnutella architecture, a Gnutella client sends a ping request to another client, which then gets forwarded from one client to another. The ping request also includes a "time-to-live" (TTL), which controls how deep in the hierarchy the ping is forwarded. Typically it is set to 7. The ping is answered by a pong from the other client, which includes information such as IP address and the files that are being shared.

Security Challenges of IM and P2P

Penetrating Firewalls

Even though IM and P2P applications each have a well-publicized port to use, e.g. 5190 for AIM, 1863 for MSN, 5050 for Yahoo, 1214 for Kazaa, it is not as straightforward to block these applications at the firewall. That is because all of these applications have the capability to exploit any open port on the firewall, frequently tunneling out through ports primarily designated or intended for use by other applications, such as port 80 (primarily used for HTTP), port 25 (primarily used for email), port 23 (primarily used for telnet) and port 21 (primarily used for ftp). When these applications exchange content directly with each other in peer modes, they negotiate ports randomly. This is commonly known as 'port-crawling behavior' and is highly undesirable.

In addition, each IM network provider has its unique set of IP addresses that the clients can connect to and these IP addresses change frequently or at random. This presents a two-fold problem for IT organizations: not knowing which IP addresses to block, and not knowing which ports to block. Thus any attempts to block IM and P2P are not 100% guaranteed to be effective,

as applications can always tunnel through other commonly used ports. Moreover, the steps to block access at the firewall are extremely manual and error-prone.

In the future, as Voice over IP (VoIP) becomes mainstream, securing VoIP at the firewall will be even trickier. VoIP sessions use H.323 or Session Initiation Protocol (SIP). H.323 and SIP have separate connections for call control and actual media exchange. Call setup typically happens on one IP port, and then a random high-numbered port, usually above 1024, is selected for the data portion of the call. IT administrators simply cannot decide on configuring firewalls with some ports open and some closed because it is not possible to predict which ports may be requested for the connection.

This requires a real-time communications security gateway like RTG500 that understands the real-time protocols well enough to authorize data connections when they have been negotiated and close the ports when the sessions are over.

Application Vulnerabilities

IM and P2P applications have been the target of recent attacks by hackers and other malicious code writers. These attacks exploit the vulnerabilities in the application's design and internal execution path to compromise security.

All the IM and P2P applications have demonstrated vulnerabilities whereby programming flaws such as buffer overflows or boundary condition errors have been exploited to spread viruses, worms, or in some cases even distributed denial-of-service (DDoS) attacks. Buffer overflows allow arbitrary and potentially malicious code to be injected into a system through a carefully crafted, malformed data entry. Generally, this input is much longer than the application expects, causing code to overflow the memory buffer, crash a process and enter parts of a system where it may be subsequently executed.

Some examples are enumerated below to indicate the way these applications are abused and the damage that they can create.

AOL Instant Messenger

- **Remote Buffer Overflow:** The AIM client v4.3 had vulnerability with the way it parsed game requests with a TLV (type-length-value) type of 0x2711. This type of game request is prone to a buffer overflow, which could allow a remote user to obtain the same privileges as the user who is currently logged on. AOL addressed this vulnerability by filtering such requests on its AIM network servers. Reference: http://www.securityfocus.com/bid/3769

- **%s DoS:** The AIM client v4.1 could be subjected to denial of service (DoS). By transferring a file consisting of an unusual number of '%s' to a user running Windows NT or Windows 2000, AIM crashed when attempting to reveal the filename in the IM window. Reference: http://www.securityfocus.com/bid/1747

- **Buddy Icon Buffer Overflow:** This vulnerability affected AIM clients v4.0 through v4.2 on Windows and MacOS platforms. When AIM is installed, by default it configures the system so that aim: URL protocol connects aim:// URLs to the AIM client. A buffer overflow existed in the parsing of aim:// URL parameters. The buffer overflow has to do with the parsing of parameters associated with the "Buddy Icon" option. A stack overflow will occur if the "Source" parameter is more than 3,000 characters in length. It may also be possible to execute arbitrary code. It is only sufficient to have AIM installed on the machine and the exploit can occur even if the AIM client is not running and the user clicks a malicious aim:// URL. AOL addressed

this vulnerability in AIM client v4.3.2229. Reference: http://www.securityfocus.com/bid/2122

MSN Messenger

- **Chat Control Buffer Overflow:** A buffer overflow existed in the "ResDLL" parameter of the MSN Chat ActiveX control that could permit a remote attacker to execute arbitrary code on the system with the privileges of the current user. This vulnerability affected some versions of MSN Messenger and Exchange Instant Messenger. Microsoft addressed this by providing updated versions of the Chat Control, and updated versions of MSN Messenger and Exchange Instant Messenger with the corrected control. Reference: http://www.kb.cert.org/vuls/id/713779

- **Malformed Invite Request DoS:** Vulnerability was reported in some versions of MSN Messenger, whereby it was possible to crash the remote client by sending a malformed invite request such as an invite for Remote Assistance using Messenger. The malformed invite request included a number of HTML encoded space characters (%20) in the Invitation-cookie field. Reference: http://www.securityfocus.com/bid/4827

Yahoo! Messenger

- **Script Injection:** With Yahoo! Messenger v5.0, it is possible to use a URL beginning with ymsgr:addview? to point the Yahoo! Messenger to a web page containing a script that will in turn be rendered by Yahoo! Messenger. If this page contains Javascript or Visual Basic script, the Yahoo! Messenger will execute the script, causing malicious code to be executed on the remote machine. Yahoo! addressed this vulnerability in build 1065. Reference: http://www.securityfocus.com/bid/4838

Kazaa

- **Advertisement in Local Zone:** A vulnerability has been reported in Kazaa Media Desktop 2.0 related to the displaying of advertisements. Kazaa advertisements are rendered in the MSIE local zone. This presents a security risk as it is possible for malicious advertisement content to execute arbitrary commands on client systems or disclose the content of system files. Reference: http://www.securityfocus.com/bid/6543

IM and P2P applications aggregate names and information such as email addresses, IP addresses of other people, and as such are a natural target for hackers and virus writers for attacks.

Bypassing Anti-Virus Scanners

IM and P2P applications can sneak files past perimeter security devices as attachments. Since the P2P tunnel goes directly to the desktop, infected files riding on IMs do not get subjected to gateway AV scanners. Unless the desktops have active scanning and updated signatures, IM and P2P can easily introduce viruses, worms and Trojans to the network.

In a recent survey by Central Command, an anti-virus developer, 48% of respondents said they have accepted and downloaded a file transfer using their IM software within the last six months. Thirteen percent said those transfers came from a friend(s), while 20% said they came from a co-worker(s). Six percent reported accepting transfers from families. 15% of all IM users said they

accepted file transfers from unknown parties. Aside from the risk of viruses, intensive file sharing can also negatively impact the performance of the network due to abuse of bandwidth.

There have been numerous instances of viruses and worms spreading over the popular IM networks and through P2P applications:

- W32.AimVen.Worm used AIM to spread itself, by modifying the AIM program itself.
- Backdoor.Cigivip, a backdoor Trojan, gave an attacker unauthorized access to an infected computer and also attempted to send IM usernames and passwords to a hacker.
- PWSteal.Snatch, a Trojan horse program, mimicked the AIM client for the purpose of stealing passwords.
- W32.HLLW.Kamesh is a worm that spreads using the Kazaa and iMesh file-sharing programs. The worm copies itself into a folder on your computer and modifies the Kazaa and iMesh configuration settings so that their download folder is the one that contains the worm.

To prevent the risks of virus and worms spreading through IM and P2P programs, IT administrators need a security gateway like RTG500 that either disables file transfer activity completely or ensures a gateway approach for authorizing file transfers and ensuring that the files are subjected to AV scanners.

IP Address Exposure

Direct connections between IM and P2P clients also mean that the IP addresses of employees' machines are exposed to the external users. This increases the vulnerability to hacking risks. Although some IM clients like ICQ allow individual users to control the exposure of IP address information, not all IM and P2P applications provide this capability. Moreover, IT organizations cannot rely on individual employees to make the appropriate client configurations.

Despite firewalls, NATs and network monitoring, IM and P2P products are designed to make firewalls transparent. However RTG500 disables any direct connections between client applications thus eliminating IP address exposure.

Use of Unauthorized Proxies

Almost all of the IM and P2P applications support the use of proxy servers. As a result, IM clients such as AIM can be configured to use any TCP port and connect through HTTP, HTTPS or SOCKS proxy servers. Any savvy user can build a proxy server accessible over the Internet at some remote location and configure his or her IM client to communicate on any open port on the corporate firewall to establish an outbound connection.

RTG500 is designed to prevent IM protocols from being tunneled through HTTP, HTTPS and SOCKS proxies.

Manually Blocking at the Firewall

Many companies are attempting to restrict use of unsanctioned IM and P2P applications by configuring their firewall to block the well-known ports that these applications use. However this is not an effective mechanism because legitimate applications that need to use that port also get blocked. In addition, the IM and P2P clients are capable of port-crawling and penetrating firewalls through other well-known ports.

As a result, it becomes essential to find out the external IP addresses that the IM and P2P applications are attempting to contact and block access to these IP addresses across all ports. For IM, these external IP addresses are the IP addresses of the IM network servers. However, for P2P, this is potentially the universe of IP addresses out on the Internet.

The IM network DNS names frequently resolve to multiple IP addresses, and IM network providers such as Yahoo! have multiple DNS names that the IM client can contact. The whole process becomes manual, time-consuming, laborious and error-prone and is not guaranteed to work.

The following table gives a list of DNS entries that would need to be resolved to IP addresses one by one and manually blocked on the firewall. However, it is important to note that this list may not be exhaustive and may not result in actually preventing IM usage. This underscores the need for RTG500 as a specialized security gateway for IM and P2P.

RTG500 is designed to automatically detect the IP addresses contacted from the IM and P2P applications and prevent unauthorized connections to these IP addresses through the firewall.

IM Network	DNS entries to block across all ports
AOL Instant Messenger (AIM)/ICQ	login.oscar.aol.com aimexpress.oscar.aol.com login.icq.com bucp1-vip-m.blue.aol.com java-aim-vip-m.blue.aol.com
Microsoft MSN Messenger	messenger.hotmail.com messenger.msn.com bavm-cs100.msgr.hotmail.com
Yahoo! Messenger	pager.yahoo.com scs-fooa.yahoo.com scs-foob.yahoo.com scs-fooc.yahoo.com scs-food.yahoo.com scs-fooe.yahoo.com scs-foof.yahoo.com

Table 1: A sample list of IM network DNS entries

RTG500: Application Security Gateway for IM, P2P, and Real-time Communications

To address the growing need to secure IM and P2P usage in corporations, FaceTime offers RTG500, a specialized application security gateway for real-time communications that protects corporate networks and end-user desktops from the security threats, risks and vulnerabilities of emerging IM and P2P applications. Existing traditional firewalls offer stateful packet analysis and filtering, but are not aware of new and emerging applications and protocols. Attempts to block IM and P2P with traditional firewalls are futile as explained in the section above. RTG500 performs non-intrusive detection of IM and P2P network traffic based on knowledge of protocols and patterns in the OSI model's application layer (layer 7). The advantage of RTG500 as a security gateway is that it can support multiple real-time application protocols on a single gateway.

Features and Functionality

RTG500 provides the following features and functionality:

Detection of IM and P2P Use

- Non-intrusive monitoring of all incoming and outgoing IM and P2P traffic
    - RTG500 monitors the following IM protocols:
        - AIM/ICQ Oscar for AOL Instant Messenger (AIM) and ICQ IM clients, as well as AIM connectivity from Lotus Sametime
        - AIM-TOC for web-based AIM Express application
        - MSNP for Microsoft MSN Messenger and Windows Messenger IM clients, as well as MSN connectivity from Microsoft Exchange 2000 IM client
        - Yahoo! Messenger for the Yahoo! Messenger IM client as well as the web-based Yahoo! WebMessenger application
    - RTG500 monitors the following P2P protocols:
        - FastTrack used by FastTrack, KaZaA, KaZaA Lite
        - Gnutella used by BearShare, Gnutella, Gnucleus, Grokster, iMesh, LimeWire, Morpheus, Shareaza and Xolox
        - MFTP used by the P2P application eDonkey
    - RTG500 also detects and monitors the VoIP application called Skype. Use of Skype on the enterprise network consumes network bandwidth and also exposes the network to unforeseen risks due to IP address exposure. The text messaging aspect of Skype can prompt rogue usage circumventing best practices and compliance policies.
    - RTG500 performs highly optimized deep packet inspection and protocol pattern matching analysis
- Detailed reports that provide insight into IM and P2P activity, network bandwidth usage, application behavior and security policy enforcement
- Automatic detection of IM network IP addresses and ports used by IM applications. This report can be used as an access list to manually block IP addresses on the firewall as an added security measure.

Security Policy Filters

- Automatic recognition of FaceTime® IMAuditor™ as an authorized source for IM usage.
- Allow/block IM and P2P usage based on specific source IP address/subnet
- Allow/block IM based on ports requested by IM client, thereby controlling port crawling
- Automatic detection of protocol tunneling via use of unauthorized HTTP, HTTPS or SOCKS proxy servers
- Allow or block IM file transfers and direct connections between IM clients

Deployment and Administration

- Seamless deployment within existing network topologies. RTG500 can be deployed securely in the DMZ as well as on internal networks.
- Option to deploy in "Discovery" mode, in which usage is detected and network activity is logged, or in Policy Enforcement mode, in which policies are enforced in addition to detecting use and logging network activity
- Web-based console for configuring security policies and viewing reports
- Automated product updates for updated protocol signatures and patterns
- Support for Internet Content Adaptation Protocol (ICAP) internally, and in the future will work with other ICAP-enabled devices in the network

Deployment

RTG500 can be deployed securely in the DMZ as a perimeter security gateway for IM and P2P. It can non-intrusively monitor traffic off the span port of most switches in the network, thus inspecting the traffic flowing in and out from the exit point of the network. A typical DMZ deployment is shown below.

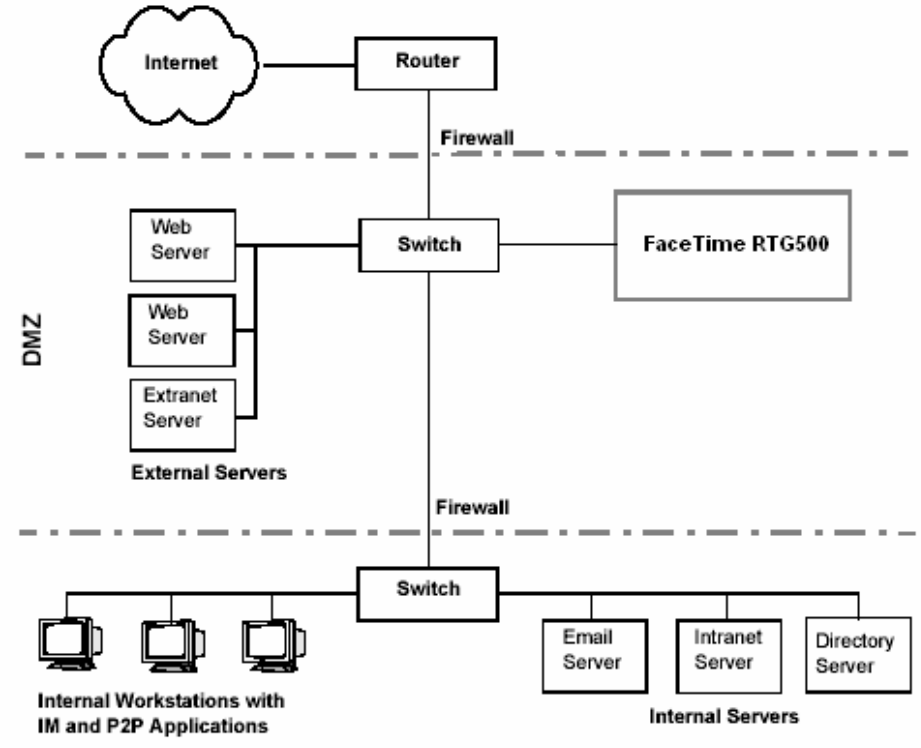

Figure 3: Secure DMZ deployment as a perimeter security gateway

RTG500 can also be deployed on the internal network, and is capable of being placed at any layer of the security infrastructure, as long as it is a peer of the chokepoint selected as the point of inspection for traffic. A typical internal LAN deployment is shown below.

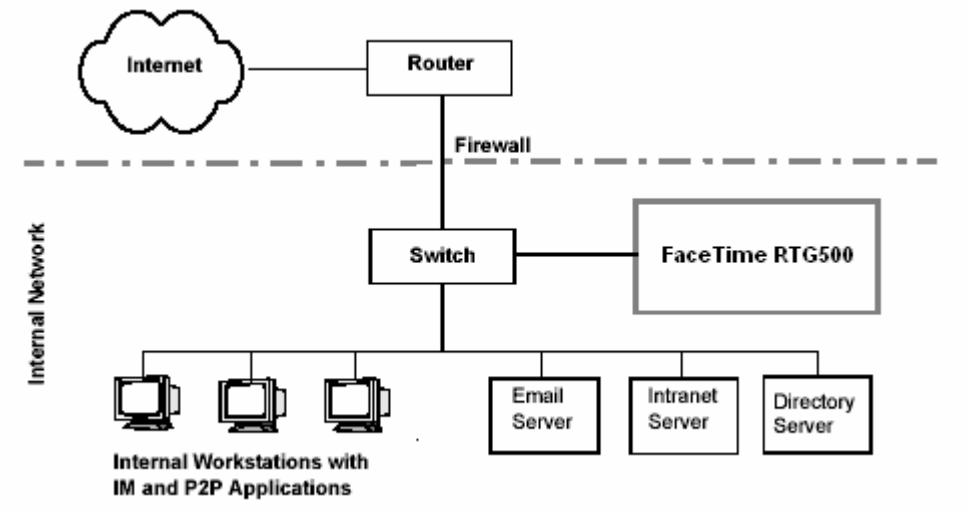

Figure 4: Typical LAN deployment of RTG500

Architecture & Functional Design

The basic RTG500 architecture is illustrated in the diagram below.

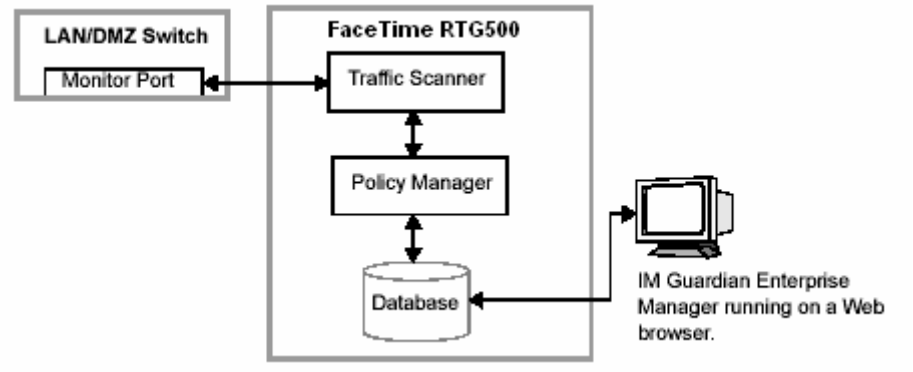

Figure 5: RTG500 functional components

The RTG500 functional components are described in the table below.

Component	Description
Traffic Scanner	The component that performs tight-loop pattern analysis and matching for IM and P2P protocols, sends suspicious packets and statistical information to the Policy Manager using ICAP, and resets source and destination connections for unauthorized connections
Policy Manager	The component that performs deep protocol analysis, enforces security policy filters and logs statistics for reports
Database	An embedded mySQL database that stores configuration information, security policies and statistical information
IM Guardian Enterprise Manager	A Web-based console that allows a network administrator to configure RTG500, define security policies, and generate and view reports of network usage

Table 2: RTG500 functional components

FaceTime Enterprise Edition: Best Practices for IM Adoption

FaceTime Enterprise Edition provides companies with a comprehensive solution for adopting IM in a cost-effective, safe, secure and manageable way, and further leverages it for integration into business processes.

If not managed, use of IM in the enterprise leads to two broad types of security risks:

- Information Security Risk – resulting from employee use and content of messages
- Network Security Risk – resulting from application behavior on the network

It is important to secure both employee behavior as well as application behavior for ensuring complete control over IM.

Information security-related risks run the gamut from inappropriate disclosure of sensitive and confidential information to information that's being transmitted in an unencrypted manner and susceptible to snooping attacks. However, this is no different from use of other electronic means of communication such as e-mail, for instance. To address the growing need of companies to embrace the use of IM, yet have the ability to manage and control employee behavior and mitigate network security risks, FaceTime provides a solution called FaceTime Enterprise Edition that includes:

- IMAuditor™ – Set user policy, manage and control usage, and archive and log IM for corporate and regulatory compliance
- RTG500™ – Secure real-time communications, block viruses, spIM and unauthorized IM and P2P use

RTG500 can be deployed standalone, or in combination with IMAuditor as part of an Enterprise Edition implementation to create a comprehensive defense-in-depth strategy for managing and securing IM usage.

Summary

FaceTime Communications has a mission of helping companies embrace emerging real-time communication communications technologies such as IM, while ensuring appropriate controls are in place to ensure security. FaceTime RTG500 addresses the growing need for preventing unauthorized usage of IM and P2P applications. RTG500 is a specialized application security gateway for real-time communications. It eliminates the need to manually change configurations on the firewall as a way of implementing security policies. FaceTime also provides a suite of Enterprise IM Management applications to enable companies to adopt IM in a strategic manner across the enterprise.

For More Information

For more information about FaceTime Communications and FaceTime solutions please visit http://www.facetime.com

FaceTime Communications
1159 Triton Drive
Foster City, CA 94404

Phone: (650) 574-1600
Email: info@facetime.com