FaceTime™

Integrated Management and Security for IM in the Enterprise:

A ‘Defense-In-Depth’ Approach

White Paper

Abstract

Instant Messaging (“IM”) is experiencing tremendous growth, becoming the fastest-growing communications medium in the history of communications. Although mature on the consumer side, the corporate IM market (the “enterprise”) is in its infancy and will continue to experience rapid growth during the next five years. Industry analyst firm Meta Group anticipates a broad adoption of IM in the enterprise with more than 90% of the Global 2000 workers having IM capabilities by 2007. IM users in the enterprise will increase from 20 million users in 2003 to 95 million users by 2007.

The increased use of IM in the enterprise is causing compliance and technology management challenges for Compliance Departments, Security Officers, IT Professionals and Regulators. In enterprises, including, but not limited to: energy companies, utility companies, communication companies and transportation-related industries, regulatory issues regarding the use of IM are increasingly appearing.

While other methods of communication are governed by IT policies and government regulation, IM has historically not. However, with the increased use of IM for critical real-time business communications, the management and control of IM in the enterprise can no longer be ignored. This paper explores FaceTime’s comprehensive and unique approach to IM management and security with added emphasis given to regulatory issues involved in using IM. The approach ensures end-to-end security for IM and provides a “defense-in-depth” approach – both IM user policy management and application behavior management.

Content

Explosive Growth of IM in Business

Gartner Group predicts that by 2004, 60% of real-time communication between users by any means, including voice, text or call-and-response will be driven by IM.

Business has always been about time and money- getting the right information to the right people at the right time to make the right decisions. This demand for business agility is driving the need for real-time communications in today's organizations. Access to instant information, collaborative groups, customers and partners, creates business efficiencies and sets the real-time organization above the rest. Instant messaging (IM) in the enterprise is a powerful communication technology that is breaking the barriers of cost while increasing employee productivity and information sharing.

The motivation for adoption of IM in business is the need to communicate and multi-task in real-time. Business users discovering the value of IM are having virtual conferences, collaborating on projects, augmenting phone conversations, and exchanging transaction instructions. Other benefits include community building and collaboration among multiple corporate locations, remote employees, telecommuters, vendors and customers, cost savings from reduced telephony costs, better accuracy of transactions via written communications, and increased business productivity by communicating in real-time.

What Is Defense-In-Depth?

IM creates and leverages a social network unlike any other application in the enterprise, presenting new and innovative channels for security threat propagation, including viruses, worms and malware. The pattern of use and behavior is significantly different then other forms of communication due to the synchronous and real-time exchange of signaling events and data.

Defense-in-Depth is a practical strategy for addressing these threats and behavioral differences to ensure network and information security in today's highly networked environments. FaceTime's approach to Defense-in-Depth for IM addresses the multiple layers in the network infrastructure which are at risk from use of IM and real-time communications technologies, specifically, the perimeter, enterprise IM host systems, and IM client applications on the desktop.

FaceTime's suite of solutions enable Defense-in-Depth by creating a framework for authorized access to services outside the perimeter, coupled with a mechanism for detecting and preventing rogue or unauthorized access. The result is comprehensive protection without compromise on cost, performance or operational considerations.

Regulatory Environment Recognizes Instant Messaging

The increased use of instant messaging ("IM") in enterprises that are either highly-regulated or increasingly regulated by the federal government can be analogized to the fable of the "tortoise and the hare." The hare represents the technology of IM dashing wildly out of the starting gate and moving quickly around the track. The hare enthralls the onlookers, who embrace the hare as all-important and not to be controlled by any other force of nature. The tortoise, on the other hand, is the government regulator that takes its time, slowly recognizes the issues (involving the hare), analyzes what needs to be done to understand and control the hare, and with time, catches up to the hare and at the end of the race manages to understand the hare's usefulness. The tortoise wins by determining a way to control the power of the hare.

This simplistic analogy reflects the current state of affairs with respect to the relationship of the various enterprises to regulators. Regulators and self-regulatory organizations are slowly issuing rules, regulations and interpretations that attempt to provide guidance and control over electronic communications.

Specifically, the federal government and various self-regulatory organizations have issued the following relevant rules, regulations and interpretations as follows for various enterprises:

Risks of Unsanctioned and Unmanaged IM in Business

IM growth in business is occurring along multiple dimensions. The vast majority of businesses use the public IM networks (PIM), such as AOL's AIM, Microsoft's MSN .Net Messenger, and Yahoo! Messenger, often in conjunction with enterprise IM servers (EIM), such as IBM/Lotus IM, Microsoft Exchange 2000 IM, Jabber, and Microsoft Office Live Communication Server (LCS). EIMs are on-premise servers that act as local exchanges for IM. In addition, industry specific IM communities such as Reuters Messaging, Instant Bloomberg, and Communicator are rapidly gaining popularity in the finance industry. Indeed, IM use in corporations is heterogeneous: different public and community network and enterprise server protocols are utilized with diverse clients from various vendors accessing them.

The diagram below shows the typical use of IM in business today, with no notion of management, security and access control authorization best practices, which are typically put in place by IT for all Internet and messaging systems. Peer-to-peer (P2P) file sharing, IM and Voice-over-IP (VoIP) applications like Kazaa and Skype have seen increased usage on enterprise networks and represent potential vulnerabilities on the network.

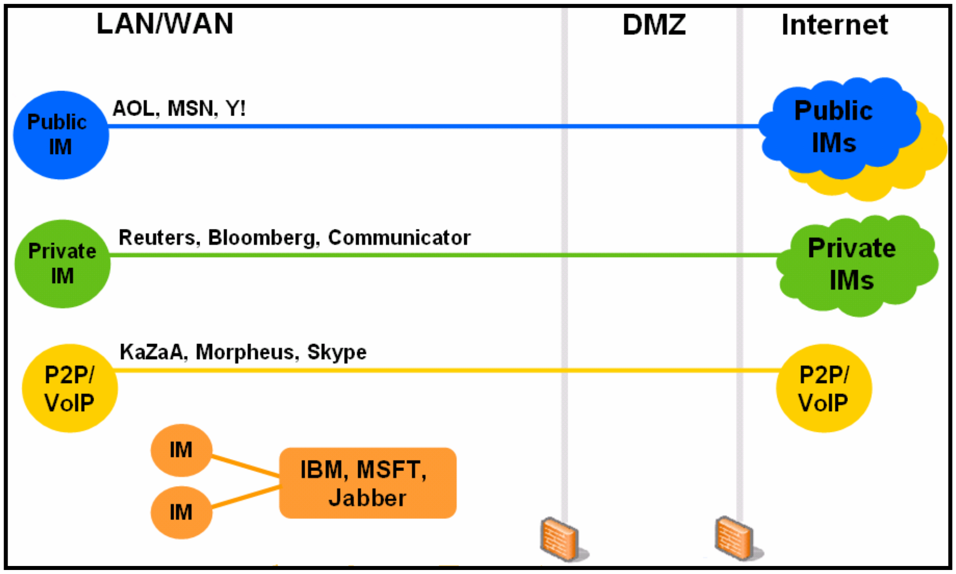


Figure 1: IM/P2P use in Business Today – Without any Management, Security and Access Control Authorization Policies

Unsanctioned and unmanaged use of IM and P2P creates tremendous risks, such as:

- Information security– not knowing what proprietary corporate information and intellectual property is being compromised
- Network security– exposing network information and being vulnerable to malicious attack
- Non Compliance–not providing a means to control and manage IM as an auditable means of electronic communications
- HR–lack of management and control of inappropriate and unprofessional conduct

- Legal– no control of downloads and sharing of copyrighted material

The risks described above arise because:

- The applications are downloaded and installed by employees without any IT involvement. The Internet acts as a perfect vehicle for rapid distribution and proliferation. IT organizations have no standard means of detecting the use and extent of use of these applications on the corporate network.
- The applications were designed to get around existing security mechanisms such as firewalls and web filtering proxies.
- Increasingly, the installed base of these applications makes them a natural target for exploiting their vulnerabilities by hackers, spreading of viruses and compromising enterprise network security.

Limitations of Firewalls and Web Proxies

Blocking IM

The first response of most companies is to try and block IM either implicitly by just issuing a notice to employees warning against use or explicitly by using current infrastructure such as firewalls and web filtering proxies.

Dissuading employees from using IM leads to dissatisfaction as employees have come to rely on IM not just for keeping in touch with friends and family members, but also for enhancing business potential by communicating with key partners, suppliers and even customers. IM has become a valid tool for fostering key business relationships. The scenarios of saved deals, nick-of-time solutions, and prevention of costly errors through rapid, real-time access to previously “unreachable” collaborators contain an implicit promise of productivity and competitive advantage.

An attempt to explicitly block IM using firewalls and web filtering proxies is manual, laborious and error-prone, besides the fact that it does not guarantee a blocking solution.

Port Crawling

Even though IM and P2P applications typically 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 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.

Changing IP Addresses

Every IM network provider has its own unique set of IP addresses that the clients can connect to. These IP addresses change frequently or at random without any notice. Firewalls and proxies apply blocking policies on the notion of a “black list” of IP addresses. The steps to block access at the firewall to every single IP address out of hundreds of potential IP addresses are extremely manual, laborious and error-prone, not to mention the fact that the firewall or proxy has to be touched and kept updated on a more frequent basis, which is also highly undesirable.

Constantly Evolving Proprietary Protocols

The rate of innovation for IM and P2P applications far exceeds the rate of innovation in firewalls and proxy infrastructure. The protocols are proprietary and evolve constantly to deliver newer and advanced features to the IM community. Firewalls and proxy vendors do not have the necessary relationships with IM providers to support the protocols. IT organizations typically prefer not to touch and constantly update the firewall with protocol signatures.

Application Intelligence

Some firewall and proxy vendors claim to support IM and P2P protocols, however, as the number and complexity of protocols increases, the firewall/proxy has to do more processing per packet resulting in potentially slowing down the network.

Also, the synchronous nature of real-time connections is much different from web browsing and email. And standard firewalls and proxies were not designed to inspect and analyze real-time communication traffic; they were primarily designed for asynchronous web traffic.

A standard firewall or proxy only offers a very cursory level of control and inspection of IM traffic. There is no ability to understand application behavior and context by understanding the proprietary application protocol. As a result it is not possible to distinguish between authorized IM and unauthorized IM connections. This is an important aspect of adopting IM in the workplace.

Complexity of Real-time Communications

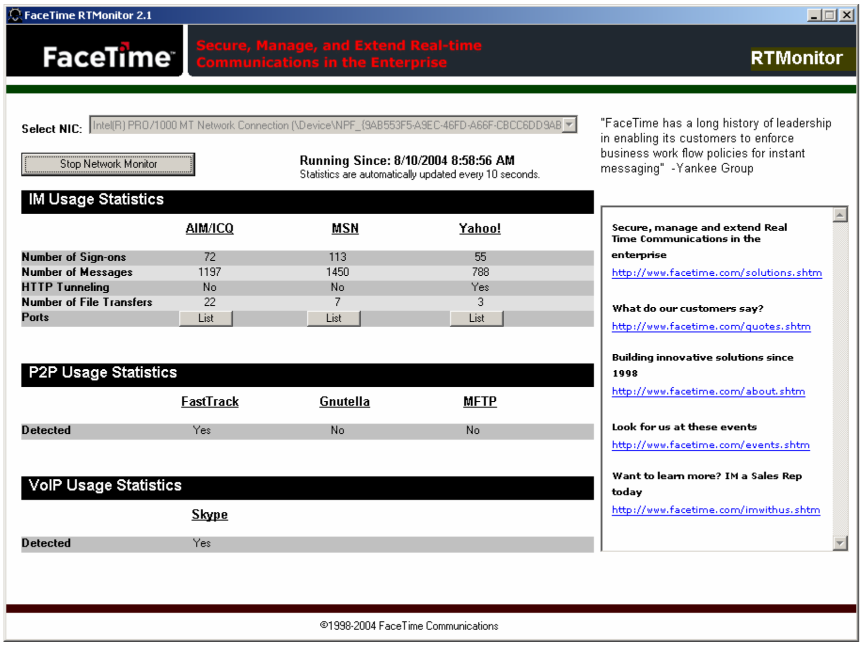
In the near future, as real-time communications expands to Voice over IP (VoIP), securing VoIP at the firewall would be even trickier. VoIP sessions use H.323 or Session Initiation Protocol (SIP). H.323 and SIP have separate connections for call control and actual media exchange. Call setup typically happens on one IP port, and then a random high-numbered port, usually above 1024, is selected for the media 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.

Best Practices Framework for IM

Rather than choosing to block IM, FaceTime advocates a more pragmatic approach of managing and securing IM use within the organization. This requires an understanding of how and why users use IM and also an understanding of how the IM application itself behaves behind-the-scenes on the corporate network.

Defining the Framework for Securing Employee Use

First and foremost it is important to assess the profile of existing usage. FaceTime provides a free download utility called RT Monitor™, which can be deployed in the network as the first step in assessing existing IM use within the company. It provides valuable information about the number of connection requests, messages, file transfers over IM, etc. Additionally it also reports on P2P and VoIP application usage.


FaceTime RTMonitor 2.1
FaceTime
Secure, Manage, and Extend Real-time Communications in the Enterprise
RTMonitor
Stop Network Monitor

Select NIC: Intel(R) PRO/1000 MT Network Connection (\Device\NPF_{9AB553F5-A9EC-46FD-A66F-CBCC6DD9AB

Running Since: 8/10/2004 8:58:56 AM
Statistics are automatically updated every 10 seconds.

"FaceTime has a long history of leadership in enabling its customers to enforce business work flow policies for instant messaging" -Yankee Group

IM Usage Statistics

	AIM/ICQ	MSN	Yahoo!
Number of Sign-ons	72	113	55
Number of Messages	1197	1450	788
HTTP Tunneling	No	No	Yes
Number of File Transfers	22	7	3
Ports	List	List	List

P2P Usage Statistics

	FastTrack	Gnutella	MFTP
Detected	Yes	No	No

VoIP Usage Statistics

	Skype
Detected	Yes

Secure, manage and extend Real Time Communications in the enterprise
http://www.facetime.com/solutions.shtm

What do our customers say?
http://www.facetime.com/quotes.shtm

Building innovative solutions since 1998
http://www.facetime.com/about.shtm

Look for us at these events
http://www.facetime.com/events.shtm

Want to learn more? IM a Sales Rep today
http://www.facetime.com/imwithus.shtm

©1998-2004 FaceTime Communications

Figure 2: FaceTime RT Monitor, a free utility to detect and assess IM, P2P and VoIP use

Requirements for securing user behavior require an understanding of:

- Who is using IM?
- Which external IM services are being accessed?
- What IM names do employees use while representing company interests?
- How can sensitive information be prevented from being disclosed over IM?
- Does the content of a message violate HR policy?
- How can messages be archived for regulatory record-keeping?
- Can users be subject to policies selectively based on which group or business unit they belong to?
- Are users being targeted and solicited by spam on IM (commonly known as *spim*)?
- Are users being asked to click on malicious URLs or accept virus-infected files?

A user policy framework that addresses the above requirements is best implemented by a dedicated IM proxy solution that provides native connection management for the respective proprietary protocols.

FaceTime IM Director™, IM Auditor™

FaceTime offers IM Director as an infrastructural foundation for defining user policies and proxying IM connections, either to enterprise IM systems or external IM services.

For companies facing regulatory mandates, FaceTime offers IM Auditor, to provide additional compliance capabilities for guaranteed message archiving, supervisor review and storage system integration.

IM Director and IM Auditor are built for high performance and scalable proxy connection management for IM.

Protecting the Framework by Securing Rogue Application Behavior

In order to understand application behavior, it is important to understand how the IM or P2P application connects and performs its operations.

The best practices framework defined for securing user behavior is only effective if this framework cannot be circumvented. Requirements for securing rogue application behavior require an understanding of the following:

- Are IM and P2P connections being established in an unauthorized manner outside the user policy framework?
- Are unsafe and unsanctioned IM features (e.g. games, webcam, image and file sharing) being used over these unauthorized connections?
- What ports are being misused?
- Are proxies being abused either within the corporate network or outside the corporate network?
- Are P2P applications being used?

It is a common misconception that P2P applications are only used for file sharing, however these applications also provide IM capabilities to send and receive messages, which violate the user policy framework described above and lead to compliance and information security risk.

FaceTime RTG500™

FaceTime offers RTG500 as a purpose-built and hardened network device that is the industry's first solution for securing real-time communications. RTG500 is based on FaceTime's award winning IM Guardian technology and performs deep packet inspection based on analysis of protocol patterns in the OSI model's application layer 7.

Figure 3: FaceTime RTG500 for Defense-in-Depth

RTG500 is built to offer non-intrusive network deployment, no performance impact for authorized application traffic and ability to block rogue and unauthorized IM and P2P connections.

RTG500 is validated with the Cisco AVVID framework and certified to interoperate with the Symantec SESA framework for enterprise security.

The Importance of 'Defense-in-Depth' for IM

As mentioned earlier, the user policy framework defined with FaceTime IM Director and IM Auditor is effective only as long as IM and P2P connections are established within this framework.

Any attempts, internal or external, to circumvent the framework and establish IM and P2P connections leads to policies being ineffective and creates a heightened sense of risk. Hence, it is important to distinguish between authorized and unauthorized connections at the network perimeter and make sure that only authorized connection requests are allowed to be established.

A two-pronged, layered, "Defense-in-Depth" approach is essential to proper management and security of all IM and P2P communications. Only FaceTime delivers this unique capability through an integrated trust relationship between IM Director/IM Auditor and RTG500.

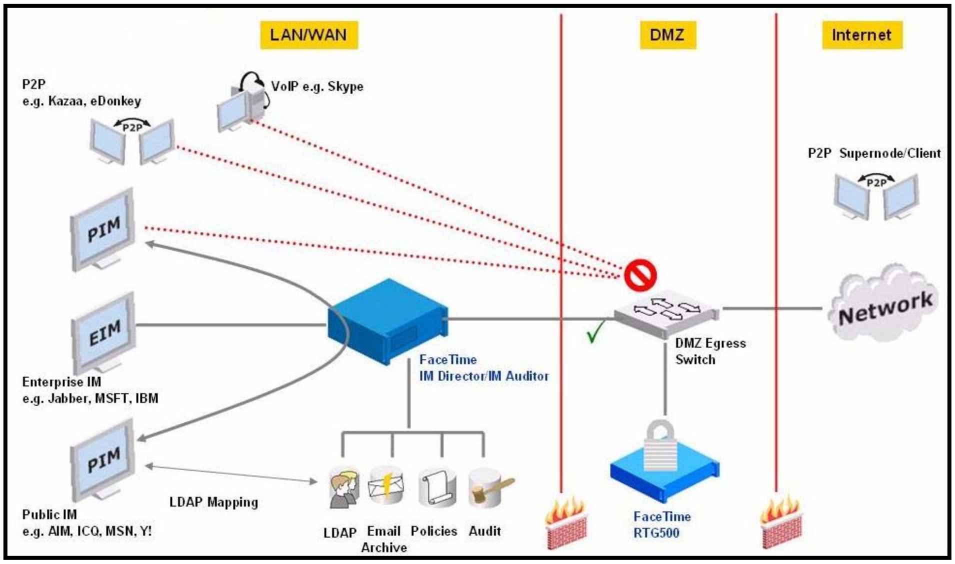


Figure 4: Integrated Management & Security for IM Defense-in-Depth

As shown in the figure above, the FaceTime "Defense-in-Depth" approach employs IM Director/IM Auditor for IM user policy management on the internal network with RTG500 at the network perimeter to manage application behavior through deep inspection of network traffic for protocol analysis that distinguishes between authorized and unauthorized use.

Through a built-in protocol handshake, RTG500 can automatically detect connection requests coming from IM Director/IM Auditor deployed anywhere within the company network, as well as rogue connection requests. Any IM traffic that does not flow through IM Director/IM Auditor is blocked by RTG500 to ensure all IM usage adheres to set policies.

This helps preserve the integrity of the rich user policy management and security framework that is defined by using IM Director and IM Auditor.

Summary

A revolution in the way people communicate has begun. The enthusiastic reception of IM for business communication marks the beginning of a new generation of communication.

This new channel of communication presents challenges to companies, specifically in the financial services, energy, insurance, healthcare industries, as well as others governed by stringent regulations, to manage, control and audit IM. However, it also presents a broader challenge of ensuring information and network security. These challenges are not effectively addressed by current security infrastructure comprising of firewalls and web proxies, as these solutions were not designed with real-time communications in mind. The pace of innovation for emerging IM and P2P technologies far exceeds the pace of innovation of traditional security solutions.

FaceTime provides companies with a dedicated and integrated defense-in-depth approach to managing and securing IM. This approach is unique and represents FaceTime's commitment to innovation for meeting customer requirements. The comprehensive approach also presents testimony to FaceTime's leadership in defining IM management and security solutions:

- IM Director™ gives IT professionals the ability to manage user policies and control the usage of IM, regardless of the network being used. Organizations have the freedom to choose the platforms, networks and applications with which to interface, without altering existing technologies and business workflow.
- IM Auditor™ addresses the regulatory compliance needs of today's businesses that must adhere to stringent government regulations. Organizations have the ability to log and review all real-time communications usage
- FaceTime RTG500™ controls rogue instant messaging and P2P file sharing. RTG500 can be deployed with other FaceTime solutions behind the firewall for a tightly integrated 'defense in depth' approach to managing both user and application behavior.

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