

# The Barracuda IM Firewall: Enabling Corporate Compliance

## Corporate IM Growth

Instant messaging (IM) is quickly becoming the medium of choice for rapid business communications and its use is growing at an astounding rate. In a recent study, the Radicati Group, a technology market research firm in Palo Alto, Calif., projected that the number of business IM accounts will grow beyond 300 million by 2007. Most companies, however, remain vulnerable to prying eyes and in violation of government regulations because they rely on public IM networks.

## Regulations Regarding Electronic Messaging

Since the rapid growth in popularity of email in the mid-1990s the government has been regulating the use of electronic communications in various industries. Although originally designed to log and manage email communications, these regulations now require the logging and management of all IM communications.

There are currently numerous regulations which apply to instant messaging:

Regulation	Logging	Encryption
Sarbanes-Oxley	IM logs must be kept for no less than three, but up to seven years	Not Required
HIPAA	IM messages must be logged and stored for several years	Any information regarding patient information or diagnosis must be encrypted
CIPA	Communications should be monitored to ensure child safety	Not Required
Gramm-Leach-Bliley	Not Required	Customer financial data and information must be protected (i.e., encrypted)

## Descriptions of the Regulations

### Sarbanes-Oxley

The Sarbanes-Oxley Act requires companies to implement policies and systems to monitor and prevent fraudulent activities. Financial controls must be verified and documented by independent auditors. Penalties for non-compliance include fines of up to \$5 million and up to a 20-year prison term.

### HIPAA

The Health Insurance Portability and Accountability Act requires that all healthcare and insurance providers determine who has access to health information and ensure that the information is inaccessible to unauthorized users. Transmission of health information must be protected (i.e., encrypted). A solution must be in place to alert administrators if a violation occurs. Penalties for non-compliance include fees of up to \$250,000 and up to a 10-year prison term.

### CIPA

The Child Internet Protection Act (CIPA) requires that schools ensure the safety and security of minors using electronic communications. The penalty for non-compliance is the loss of Federal Universal Service funding (more commonly referred to as E-Rate funding), which is provided to schools by the federal government for computer and networking equipment.

### Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act requires that financial records and non-public personal information be kept private and safeguarded until it is eventually destroyed. Penalties of non-compliance can be as high as \$500,000 and up to a 10-year prison term.

### SEC Rules 17a and 17a4

The SEC mandates that companies must preserve copies of all electronic communications including instant messages for three years, two years of which must be in an easily accessible location. Penalties of non-compliance are determined on a case-by-case basis.

RELEASE 1

OCTOBER 2006

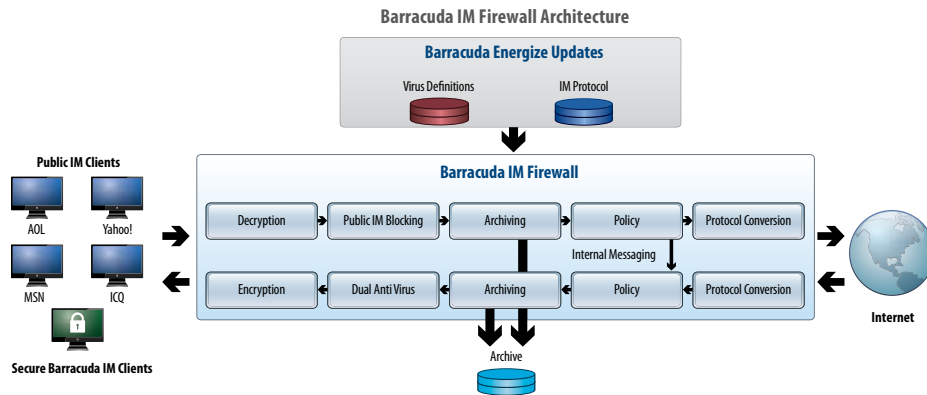
## Compliance Options

Compliance can be achieved in one of two ways:

- Gateway solutions must capture IM traffic and log it to a database.
- Server solutions must provide an IM infrastructure as well as message encryption.

In most cases both solutions are needed to ensure compliance. The Barracuda IM Firewall combines these two approaches to provide the tools that enable compliance with government regulations, in a single easy-to-use appliance.

The Barracuda IM Firewall provides organizations with a way to enable compliance and mitigate the risk of penalties through its logging, auditing, encryption, and policy tools.



## Enabling Compliance

The Barracuda IM Firewall was designed with compliance in mind. Compliance can be achieved using the logging, auditing, encryption, and management tools available on the appliance.

Regulation	Logging	Encryption
Sarbanes-Oxley	The Barracuda IM Firewall provides up to five years of logs on the appliance. Logs can be exported and backed up. Fraudulent activities can be identified by keyword notification tools and log audits.	Not Required
HIPAA	The Barracuda IM Firewall provides up to five years of logs on the appliance. Violation alerts are achieved using keyword notification and content filtering tools.	Using the Barracuda IM Firewall Client, communications are encrypted to secure patient data. IM communications can be limited to the secure channel, public (unencrypted) IM can be blocked.
CIPA	Not Required	Not Required
Gramm-Leach-Bliley	The Barracuda IM Firewall provides up to five years of logs on the appliance. Logs can be exported and backed up. Auditors can search and view logs and specify which messages have been audited.	Using the Barracuda IM Firewall Client, communications are encrypted to secure customer data. IM communications can be limited to the secure channel, public (unencrypted) IM can be blocked.

## Message Logging and Auditing

*Sarbanes-Oxley, HIPAA, CIPA, SEC*

The ability to log and audit instant messaging traffic on the corporate network has become a necessity, not an option. HIPAA and Sarbanes-Oxley dictate that messages must be stored and easily retrievable in the event of an audit. The Barracuda IM Firewall sits inline, so all network traffic can pass through it and IM traffic is easily identified and logged. These logs can be audited and searched as required by SEC and Sarbanes-Oxley regulations. The auditing capabilities of the Barracuda IM Firewall, which allow auditors to view logs and identify which messages have been audited, are important for SEC compliance.

The Barracuda IM Firewall logs all instant messages, whether internal or on the public IM networks, to a relational database where the messages are archived and can be searched and audited, meeting the requirements for message archiving as mandated by the Center for Medicare and Medicaid (CMS) in HIPAA. Additionally, the Barracuda IM Firewall provides a variety of tools for parsing the data within the logs. Data can be managed through a number of customizable search and filtering tools allowing for common searches to be saved for reuse.

## Encryption

### *HIPAA and Gramm-Leach-Bliley*

Security has been, and shall remain, a primary concern in all IT systems, regardless of the type or purpose. Instant messaging can be no exception. In fact, both HIPAA and Gramm-Leach-Bliley require all electronic communications that may contain patient, customer, or financial data, to be encrypted. Many employees believe that if they are sending an IM to someone in the next office, that message travels from their computer to the person's computer in the adjacent office. This is not true. In fact, that message travels out of the organization to the servers administered by the public IM network, then back to the person in the nearby office, the whole time as unencrypted text.

Any proprietary or confidential information can be viewed in transit by anyone with the skill to do so. This security hole has led many IT managers to either disable IM for employee use, or take the risk of compromising private information. The Barracuda IM Firewall provides a low cost solution for ensuring that customers' private data remains private.

The Barracuda IM Firewall provides an internal IM server boasting 256-bit default encryption on its internal instant messaging network. To provide maximum connectivity between coworkers and customers, the Barracuda IM Firewall maintains compatibility with the popular public IM networks yet it cannot provide encryption on these channels. Ensuring that confidential internal communications are channeled over the internal network only can be achieved through effective IM policy management.

## The Barracuda IM Firewall

Compliance has become a thorn in the side of many organizations over the past several years. Barracuda Networks recognizes and appreciates this, and as such it has designed a product that will enable IM compliance with one powerful, easy-to-use, and affordable solution.

### Powerful

The Barracuda IM Firewall provides everything a firm needs to comply with government regulations in an easy to install and administer, plug-and-play hardware appliance. The Barracuda IM Firewall is the only fully featured, complete IM solution on the market that can allow organizations to tailor the product to its needs, rather than bend requirements to meet the limited capabilities of competing solutions. The Barracuda IM Firewall provides a high level of encryption, logging and auditing capabilities, as well as instant messaging policy creation and management tools, all on a hardware platform that has been optimized for speed and stability at an affordable price.

### Easy-to-Use

The Barracuda IM Firewall is designed to be up and running in under 30 minutes. Simply install the product inline, on a Span port, or within the DMZ and the product will begin logging all traffic on the network including the popular AOL, MSN, and Yahoo! IM networks.

### Affordable

Barracuda Networks goal is to provide its customers with the highest quality product at a price that will deliver a rapid return on investment. In fact, the Barracuda IM Firewall can save customers between 50 and 80 percent of competing solutions. There are no per user licensing fees, no hardware issues to attend to, no expensive operating system to install and configure, no database integration headaches, and no security holes to patch.

*For questions about the Barracuda IM Firewall, please visit <http://www.barracuda.com/im> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.*

## Resources and Links

### HIPAA

<http://www.cms.hhs.gov/HIPAAGenInfo/>

### CIPA

<http://www.fcc.gov/cgb/consumerfacts/cipa.html>

### Sarbanes-Oxley

[http://www.sarbanesoxley.com/section.php?level=1&pub\\_id=Sarbanes-Oxley](http://www.sarbanesoxley.com/section.php?level=1&pub_id=Sarbanes-Oxley)

### Gramm-Leach-Bliley

<http://banking.senate.gov/conf/>

### SEC Rules 17a & 17a4

<http://www.sec.gov>



### Barracuda Networks

3175 S. Winchester Boulevard  
Campbell, CA 95008  
United States  
+1 408.342.5400  
[www.barracuda.com](http://www.barracuda.com)  
[info@barracuda.com](mailto:info@barracuda.com)