



828 West Taft Avenue  
Orange, CA 92865  
714-282-6111  
714-282-6117 Fax  
[www.8e6.com](http://www.8e6.com)

## 8e6 3000 | Enterprise Filter



### **Instant Message Blocking and Filtering: The Requirement of Instant Message Blocking as a Crucial Part of any Instant Message Security Solution**

#### **Scope**

---

The scope of this white paper is to define and explain the fundamental differences between Instant Message Blocking and Filtering as well as the methodology 8e6 uses in its R3000 Enterprise Filter.

#### **Product Definition**

---

The 8e6 R3000 Enterprise Filter is a hardware-based appliance solution that allows users to monitor, filter and log an organization's Internet traffic. Through user-defined parameters based on 8e6's 75+ categories of Web content, an R3000 filter will help improve employee productivity, reduce liability and preserve network resources.

#### **Introduction**

---

*Many business people have chosen and accepted text-based IM over phone calls and e-mail — preferring its immediacy and streamlined efficiency...*

As a technology that was initially designed for conducting one-on-one personal chats, Instant Messaging (also referred to as IM), has made its way into the workplace. Many business people have chosen and accepted text-based IM over phone calls and e-mail — preferring its immediacy and streamlined efficiency in getting real-time information from partners, suppliers and colleagues both working internally and remotely.

Essentially, IM can be thought of as the text version of a phone call. Its popularity has grown to approximately 275 million users across Yahoo, MSN, AOL and other providers according to aggregate service provider estimates. "Instant messaging could well be the dial tone of the future — albeit a silent one," says The Wall Street Journal. In fact, technology consultant Gartner Group predicts that by 2005, instant messaging will surpass e-mail as the primary online communications tool.

IM is fundamentally different from other types of Internet applications in that it involves direct connections between workstations either locally or across the Internet. While it has gained acceptance as a popular and productive business tool to send text messages, files, audio, video, etc., IMs lack of basic security features needed to protect corporate networks opens the door to hackers and viruses not to mention the transfer of virtually any type of confidential company data between workstations located anywhere.

While IM is one of the most important applications to control, it is also one of the most difficult to control, and therefore the most often abused application in today's networks. Control is difficult because IM attempts to hide within other network services, borrowing assigned tcp port numbers for it's own communication. This stealthy approach makes traditional firewalling impractical and ineffective. Regaining control and security over this type of service requires a totally new approach to both filtering and blocking.

---

## What is “filtering” and what is “blocking”?

There is a fundamental difference between filtering and blocking, although the terms are often used interchangeably.

*There is a fundamental difference between filtering and blocking, although the terms are often used interchangeably.*

**Blocking refers to blocking the ability of a user to utilize an IM application or service.** All features of the application are simultaneously blocked, providing complete security for the network.

Blocking can only be provided through the use of “sniffing” or firewall technology or by application control on the end user PC. Traditional firewalling is ineffective in blocking IM since most IM applications do not utilize proper tcp port numbers and can float among many ip addresses. The best way to provide effective blocking is through sniffing the packets on a network.

**Filtering refers to “controlled use” of an IM application.** While the application can be used, it can only be used in certain ways to communicate with select individuals. It also often involves recording the conversations themselves.

Filtering can be provided a number of ways by the devices commonly referred to as a proxy, filter, or server. Instant message proxies and filters are essentially the same thing -- software or hardware designed to be compatible with several instant message applications and act as a login server for that application in place of the real server. A true instant messaging server refers to hardware or software that duplicate the full capability of one real instant messaging login server. This offers the same features as a proxy or filter, but only for a single instant messaging application.

---

## A Place for Filtering; A Place for Blocking:

*Filters and blockers are two totally separate devices used for distinct purposes.*

At first glance, it appears that there is a clear choice between installing a filter vs. a blocker. It even appears that a filter is simply more capable than a blocker. However, nothing is further from the truth. Filter's and blockers are two totally separate devices used for distinct purposes.

Filtering by itself, without blocking, will always be unsuccessful unless all participants agree to be filtered 100% of the time. It is blocking that enforces the use of the filtering server, thus preventing end users from completely bypassing filtering and logging.

Simply put, blocking is the enforcer, or the policeman and filtering is the inspector and recorder. The filter can only inspect and control what it is voluntarily handed. If an end user changes the local settings back to connect directly to the real IM server, all control and logging is lost unless a blocker is in place to prevent direct connection.

The end result is a collection of possible scenarios when both blocking and filtering components are installed. It is practical to use blocking without filtering, but not filtering without blocking.

## How do these two components work together?

---

The blocking device sits on the network at the Internet access point watching for any attempts to connect to the real IM servers. Any such attempts are blocked and logged.

The filtering device sits somewhere inside the network, and the client applications are set to use this device as their server.

### Scenario Matrix:

	Blocker	Proxy or Server
Stop all use of IM	•	
Log all attempts to run an IM client	•	
Allow use of any IM by only certain individuals	•	
Allow only a particular IM client	•	•
Allow IM to communicate internally but not externally	•	•
Allow IM but filter content for foul language	•	•
Allow IM but disable file transfers	•	•
Allow IM but log all conversations	•	•
Filter IM for virus	•	•

As you can see, blocking is required 100% of the time while filtering is required most of the time.

## Which does 8e6 provide?

---

8e6 provides Instant Message blocking on the R3000. The goal of the R3000 is to prevent the use of application and services that are not authorized. Instant messaging is one of those services controlled. The R3000 can block the use of instant messaging by unauthorized individuals, log attempts to run instant messengers and enforce the use of an IM filter or proxy.

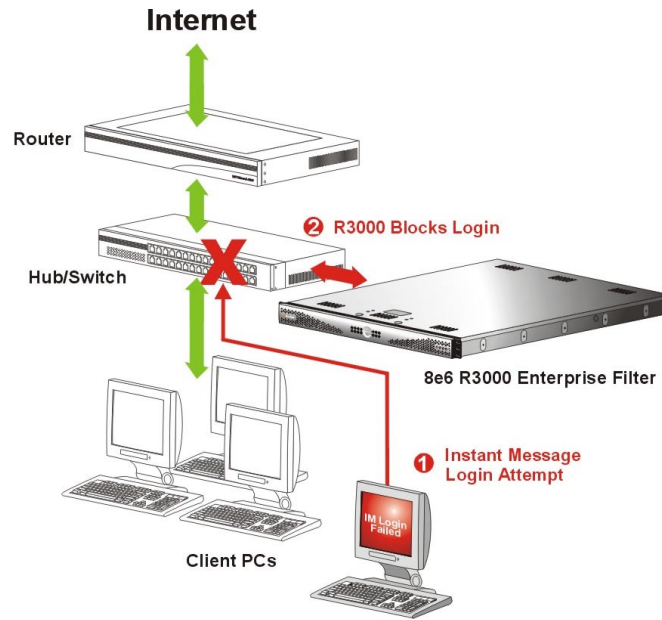
## The Average Installation

---

There are two primary installation methods. Example one discusses blocking instant messaging while the second is for filtering or allowing controlled use.

### Blocking Instant Messaging:

The R3000 is installed as it would be for web filtering. When this install is laid out, it is important to ensure that the R3000 can "see" all traffic regardless of port number. Routing or redirecting traffic based on port number should be avoided.

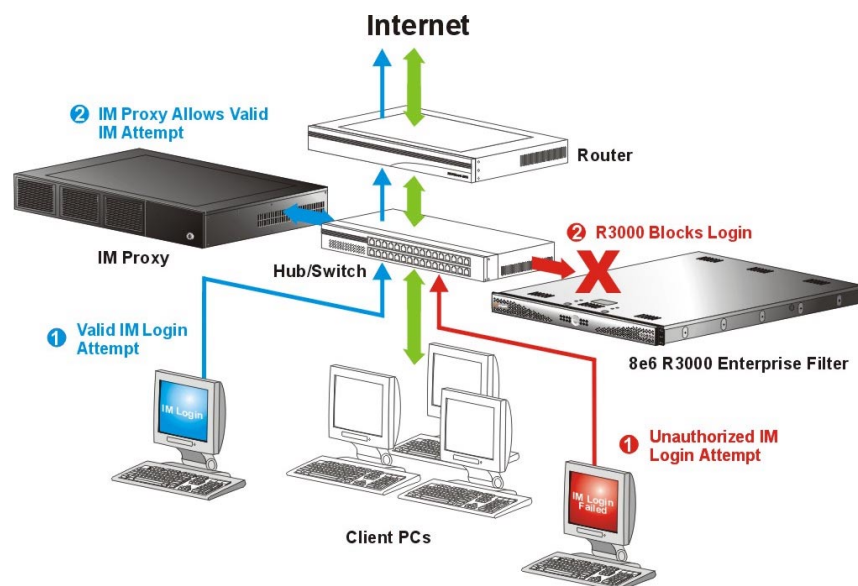


When a login is attempted to an instant messenger server, the attempt will be logged and stopped, causing an error in the instant messenger client. This normally shows up as a network error or a “failed to contact server” error.

It is possible in this scenario to allow or deny use of instant messaging per end user by making use of the R3000 individual user profiling abilities. This can be based on a personal login, NT Authentication, IP address, or Active Directory Authentication.

**Filtering or Controlled Use:**

In this case, the R3000 is installed in the same manner as above. In addition, an instant messaging proxy / filter / or server is installed internally. The R3000 is then configured to ignore login requests from the instant message server. The instant message filter / proxy / server is then configured to provide the features desired according to the manufacturer installation guide.



Next, the desired instant messenger client is installed on the workstations and configured to use the new filter / proxy / server as its login server.

In this scenario, all login requests first go to the filter / proxy / server and are checked against its rule set, and either allowed or not. Any attempts by the end user to bypass the filter / proxy / server are blocked and logged by the R3000. All use of the proper instant messenger is controlled and logged by the filter / proxy / server.