Basic description

AOL Instant Messenger connects to a group of central login servers which respond to just about any random TCP port. This is almost exactly the same way Yahoo messenger works. The data is then transferred from the servers on the streaming TCP connection.

Allowing this service inbound

If you wanted to have a AOL Instant Messenger server on your network, it would be *extremely* difficult to firewall, because it has to respond to *any* TCP port. This would basically negate most functions of a firewall.

Allowing this service outbound

If you would like to allow clients on your network to use the AOL Instant Messenger client, you can either employ an Outgoing service (see the In-Depth FAQ titled, "About the various Outgoing services," or create a custom packet filter with a specific TCP port and manually configure the AOL Instant Messenger clients to use this port.

Denying this service inbound

By default, this service will not be allowed inbound. No configuration changes should be necessary.

Denying this service outbound

Blocked Sites method

AOL Instant Messenger can use any TCP port (it most commonly begins on port 5190, then switches to 4101, and afterwards uses random ports) which makes it difficult to block (unless the Outgoing-TCP service is removed. Again, see the In-Depth FAQ titled, "About the various Outgoing services,"). The easiest way to block this traffic we have found thus far is to add the particular IP address ranges which make up the domain, "login.oscar.aol.com," to the blocked site list on the Firebox. This essentially tells the Firebox to discard any traffic from AOL's login servers. When the connection to login.oscar.aol.com fails, the client gives up. Therefore, it is only necessary to block the IP addresses of login.oscar.aol.com. This will probably change, so when setting up the policies to block AOL Instant Messenger it is important to do a current name lookup of login.oscar.aol.com.

Here is a list of the IP addresses comprised by the domain name "login.oscar.aol.com" as of August 15, 2001:

```
205.188.5.208, 205.188.7.164, 205.188.7.168, 205.188.7.172, 205.188.7.176,
205.188.3.160, 205.188.3.176, 205.188.5.204
```

The following provides step-by-step instructions on adding the AOL Instant Messenger login servers to the blocked site list:

1 Open Policy Manager with your current configuration file.

2 Select **Setup** ⇒**Blocked Sites**.
The Blocked Sites window appears.

3 Click the **Add** button. At the Type field, select **Host IP address**. Enter the first IP in the Value field.

4 Click **OK** to close the Add Site dialog box and store the first IP address.

5 Repeat step 3 to add the remaining IP addresses to the list.

6 When finished, click the **OK** button at the Blocked Sites window.

7 Save the new configuration file to the Firebox.

Bogus DNS blocking method

If you are using an internal DNS for your users, another blocking method would be to add the DNS records to your internal DNS server so that login.oscar.aol.com resolves to a bogus IP address. The client will attempt to look up this IP addresses but receive the wrong information. This would cause the client to timeout as it will not reach the correct IP addresses required for a successful connection. This method would require less maintenance as you would not have to worry about AOL adding IP addresses to the DNS names or rotating the IP addresses.