An Internet Security Systems
White Paper

INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.

Controlling the Use of Instant Messaging and Peer-to-Peer Applications with the Proventia™ Intrusion Prevention Appliances

Updated August 2004

Controlling the Use of Instant Messaging and Peer-to-Peer Applications with the Proventia™ Intrusion Prevention Appliances

6303 Barfield Road • Atlanta, GA 30328 Tel: 404.236.2600 • Fax: 404.236.2626

Use of instant messaging applications—like AOL Instant Messenger, Yahoo! Messenger, MSN Messenger and ICQ—and peer-to-peer applications has grown significantly. Although the benefits of real-time communication offer a productivity benefit to corporate environments, instant messaging and peer-to-peer applications add significant vulnerabilities and risks to an enterprise's security posture. New security risks include bandwidth misuse, additional vectors for virus and worm attacks, the ability to transfer files and the ability to take control of other machines. For additional information regarding risks involved with instant messaging and peer-to-peer applications, view the Internet Security Systems (ISS) whitepaper, *Risk Exposure Through Instant Messaging and Peer-To-Peer (P2P) Networks*: http://documents.iss.net/whitepapers/X-Force_P2P.pdf.

This paper identifies the techniques that can help businesses block, control and tailor the use of instant messaging applications and peer-to-peer applications with Internet Security Systems' ***Proventia™*** Intrusion Prevention Appliances.

Overview

The appropriate instant messaging and peer-to-peer events are described in the following sections, which include a short description of what each event consists of. Detailed step-by-step instructions that describe how to enable in-line blocking for peer-to-peer and instant messaging events using the Proventia Intrusion Prevention Appliances are also included.

The events in this document are categorized in two groups: Instant messaging (IM) events and peer-to-peer events. In ISS' SiteProtector™ centralized management system, events may be grouped and located in different areas of the configuration menu based on the type of event. Events can also be located under the IM, File Sharing and Audits categories, as well as under the X-Press Update™ (XPU) tab.

There are five common steps to enable protection from instant messaging and peer-to-peer threats in the Proventia Intrusion Prevention Appliance:

1. *Enable In-Line Blocking mode*
2. *Create a new blocking policy in the Proventia Intrusion Prevention Appliance*
3. *Enable the desired event to block*
4. *Assign the appropriate blocking response (i.e., drop connection with reset)*
5. *Set the appropriate priority for the events selected*
6. *Apply the policy*

Important note: As with any signature, Internet Security Systems always monitors real-world events and customer feedback to determine if an event is generating false positive or false negative instances. Some signatures may display these anomalies. Descriptions of these instances can be seen in the event help window which is displayed when selecting an event. Events marked with an asterisk (*****) throughout this document are known to have false positive/negative instances and should be reviewed in your environment before implementing.

Enabling Simulation mode in Proventia Intrusion Prevention Appliances allows for the testing of new policies prior to implementing them.

Instant Messaging Events

AOL Instant Messenger (AIM)

AOL Instant Messenger (AIM) has had several security-related issues, including a buffer overflow in the game request parsing engine, which was reported on January 2, 2002 by Internet Security Systems: http://xforce.iss.net/xforce/alerts/id/advise107. This issue included a certain type of specially-crafted game request that could be made to an AIM user causing an area in memory to be overwritten with arbitrary data supplied by an attacker. This data could then be coerced into executing on the remote user's computer, thus enabling an attacker to take control. AOL has patched this bug, but this is not the first vulnerability to affect AIM. These security threats are becoming more prevalent as the code for these clients become more complex.

The events in the section below allow administrators to tailor how AIM is used on their enterprise's network. Administrators can completely block the use of AIM or tailor a policy which would allow its use but not allow file transfers or encrypted dialogue. Internet Security Systems recommends blocking of all exploit events.

Events to Block AIM

- *AOLIM_Message*
  - OSCAR "instant message" detected
- *AOL_Instant_Messenger_Overflow*
  - AOL Instant Messenger add buddy
- *AOLIM_Login*
  - Login detected to OSCAR Instant Messaging server
- *AOLIM_Password_Change*
  - AOL/ICQ2000 "instant messaging" client password change request

Events to Block AIM encrypted traffic

- *AOLIM_Trillian_Encrypt_Handshake*
  - Trillian instant messaging startup activity

Events to Block AIM File Transfer

- *AOLIM_File_Xfer*
  - AOL/ICQ2000 "instant messaging" network file transfer attempt

Events to Block AIM Exploits

- *AOLIM_GameRequest_Overflow **
  - AOL/ICQ2000 "instant messaging" game buffer overflow
- *AOLIM_AddExternalApp_Overflow*
  - AOL Instant Messenger external application request buffer overflow
- *AolAdmin_Response*
  - AOL Admin backdoor for Windows and AOL

MSN Messenger

MSN Messenger (also known as .NET Messenger and Windows Messenger) is the fastest growing instant messaging service. Much of this growth is a result of Microsoft automatically shipping MSN Messenger with Windows XP, as well as the integration of MSN Messenger with Microsoft Office and Microsoft's Hotmail service.

The events in this section allow administrators to block the use of MSN Messenger on the network. Internet Security Systems will add additional events specific to MSN Messenger in the future as they become available.

Events to block MSN

- *MsmsgrMessage*
  - MSN Messenger "instant messaging" service message
- *MsmsgrLogin*
  - MSN Messenger "instant messaging" service login

Events to Block MSN File Transfer

- *MSMessenger_FileXfer*
  - Reports the contents of Microsoft Messenger file transfer requests.

Yahoo! Messenger

Yahoo! Messenger has the weakest security features of the major instant messaging platforms. Its protocol does not encrypt usernames and passwords, making it risky to even log into the system. Also, the usernames and passwords are sent via HTTP which allows this information to be stored in HTTP proxy logs.

The following events allow administrators to tailor how Yahoo! Messenger is used on their networks. Administrators can completely block the use of Yahoo! Messenger or tailor a policy which would allow its use while not allowing file transfers. Internet Security Systems recommends blocking of all exploit events.

Events to block Yahoo!

- *YahooMSG_Message*
  - Yahoo! Instant Messenger service text message
- *YahooMSG_Login*
  - Yahoo! Instant Messenger service user login
- *YahooMSG_PeertoPeer*
  - Yahoo! Messenger has entered a peer to peer communication mode

Events to block Yahoo! File Transfer

- *YahooMSG_File_Transfer*
  - Yahoo! Instant Messenger service file transfer request

Events to block Yahoo! Exploits

- *YahooMSG_URL_Handler_Overflow*
  - Yahoo! Messenger ymsgr: protocol multiple function call buffer overflow

- *YahooMSG_AddView*
  - Yahoo! Messenger script injection using a ymsgr:addview? URL
- *YahooMSG_Filename_Overflow*
  - Detects an overflow attempt in a file transfer filename field.
- *HTTP_Yahoo_YAutoDLL_BO*
  - Detects html content that attempts a buffer overflow of the ActiveX object.
- YahooMSG_UserID_Overflow
  - This signature detects an overflow attempt in a user ID.

ICQ

Time Warner now owns ICQ. However, it currently still maintains a separate database of users from the AOL Instant Messenger service.

The events in this section allow administrators to block the use of the ICQ Application on the network. Internet Security Systems will add additional events specific to ICQ Application in the future as they become available.

Events to block ICQ

- *HTTP_ICQ_Pager*
  - Use an ICQ pager detected

Peer-to-Peer Events

Gnutella

The architecture for the Gnutella network is decentralized and is a true peer-to-peer network involving no central server for authentication, indexing, etc. To connect to the Gnutella network, it is necessary to connect to several pre-determined IP addresses, which are able to relay information about other systems' IP addresses to a newly connected one. After the system identifies IP addresses of nearby systems, searching through the network of identified systems and downloading shared files becomes possible.

The following events allow administrators to block the use of the Gnutella protocol on the network:

Events to block Gnutella

- *Gnutella_Connect* *
  - Gnuttella connection attempt
- *TCP_Probe_Gnutella*
  - TCP connection to default Gnutella port
- *Gnutella Download* *
  - Gnutella file download attempt
- *Gnutella_Worm* *
  - Gnutella download containing a worm detected
- *Gnutella_BearShare*
  - Connection made by the Gnutella client BearShare
- *Gnutella_Limewire*
  - Connection made by the Gnutella client Limewire

Kazaa

Since it still relies on a central server for user information, Kazaa is not strictly a peer-to-peer network. The central server allows users to sign up for the service, assigns the user a username and password, is responsible for authenticating users and assists in locating peers necessary for available downloads.

The following events allow administrators to block the use of the Kazaa application on the network:

Events to block Kazaa

- *FastTrack_Download **
  - FastTrack File transfer detected
- *HTTP_Kazaa **
  - *Kazaa Initial startup HTTP request detected*

eDonkey

eDonkey is a file searching and sharing application that is quite popular in Europe and has a growing user base in the United States. The architecture for the eDonkey network is semi-centralized and relies on servers set up by users of the service.

The following events allow administrators to block the use of the eDonkey application on the network:

Events to block eDonkey

- *HTTP_EDonkey*
  - eDonkey Initial startup HTTP request detected

BitTorrent

BitTorrent is a protocol and peer-to-peer system for distributing files. It identifies files by URL and is designed to work well with Web browsers.

The following events allow administrators to block the use of the BitTorrent application on the network:

Events to block BitTorrent

- *TCP_Probe_BitTorrent*
  - Attempts to connect to one of the default Bit Torrent ports detected
- *BitTorrent_Response*
  - TCP traffic indicative of BitTorrent peer is present
- *BitTorrent_Get_Request*
  - Detection of a BitTorrent GET request from a peer detected

SoulSeek

SoulSeek claims to be an ad-free, spyware-free peer-to-peer application. The application generates a random listening port number when it first starts to avoid detection by ISPs.

The following events allow administrators to block the use of the SoulSeek application on the network.

Events to block SoulSeek

- *Soulseek_Login_Detected*
  - Detects a Soulseek P2P client logging onto a SoulSeek server.

DirectConnect

DirectConnect is an older file sharing community that has evolved into a peer-to-peer player. This centralized network supports the directconnect, dc++ and bcdc++ clients.

The following events allow administrators to block the use of the SoulSeek application on the network.

Events to block DirectConnect

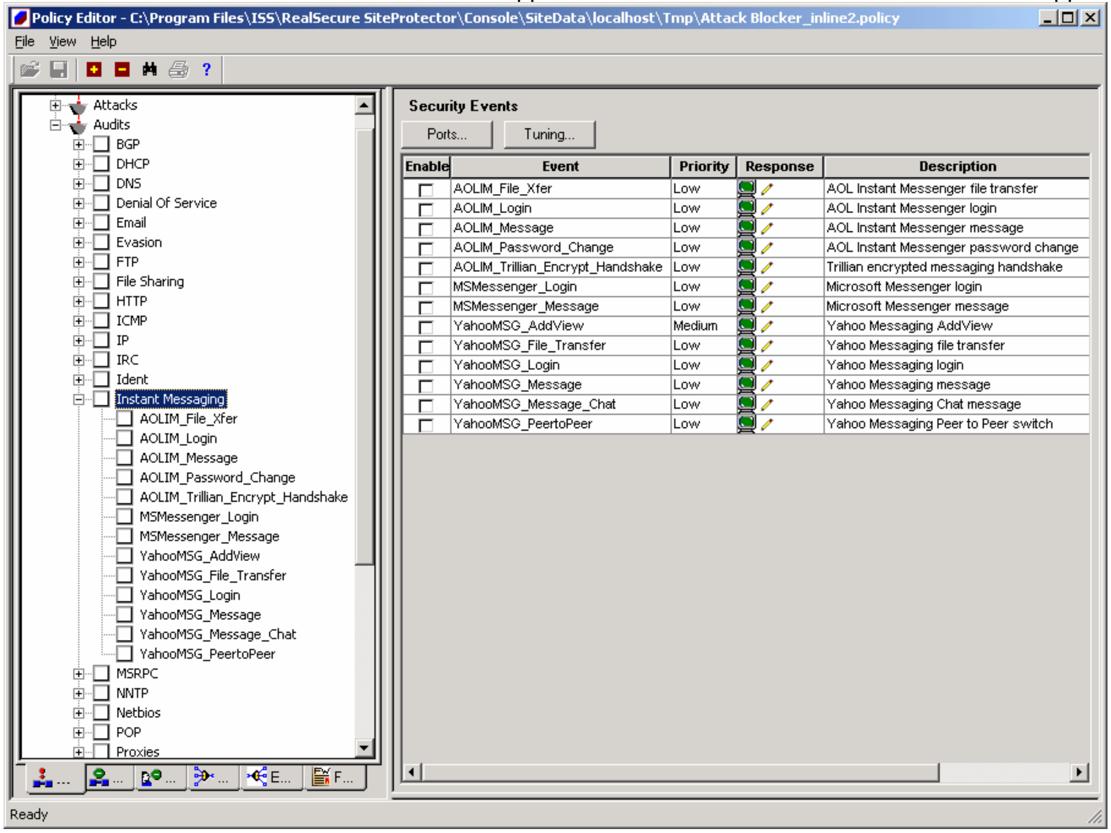
- *DirectConnect_Connect*
  - Detects a connection between a DirectConnect client and server.

Blocking Peer-to-Peer or Instant Messaging Events with Proventia Intrusion Prevention Appliances

With peer-to-peer or instant messaging events actively being monitored and blocked, administrators can feel confident that they are increasing not only their network bandwidth, but the overall security posture of the enterprise.

It is necessary to open the policy editor in the Proventia Intrusion Prevention Appliances to block any peer-to-peer or instant messaging events found (Figure 1). Create a new policy or incorporate the events you want into an existing policy. Pick your existing policy, “derive new policy”, and add the desired peer-to-peer and/or Instant Messaging events. It may be necessary to name the new policy similarly to the old policy name with a “2” or some other differentiator, which ensures that others will not reset the policy back to the old one.

Figure 1 - Policy Editor


Policy Editor - C:\Program Files\ISS\RealSecure SiteProtector\Console\SiteData\localhost\Tmp\Attack Blocker_inline2.policy
File View Help
Ready

Attacks
Audits
□ BGP
□ DHCP
□ DNS
□ Denial Of Service
□ Email
□ Evasion
□ FTP
□ File Sharing
□ HTTP
□ ICMP
□ IP
□ IRC
□ Ident
□ Instant Messaging
□ AOLIM_File_Xfer
□ AOLIM_Login
□ AOLIM_Message
□ AOLIM_Password_Change
□ AOLIM_Trillian_Encrypt_Handshake
□ MSMessenger_Login
□ MSMessenger_Message
□ YahooMSG_AddView
□ YahooMSG_File_Transfer
□ YahooMSG_Login
□ YahooMSG_Message
□ YahooMSG_Message_Chat
□ YahooMSG_PeertoPeer
□ MSRPC
□ NNTP
□ Netbios
□ POP
□ Proxies

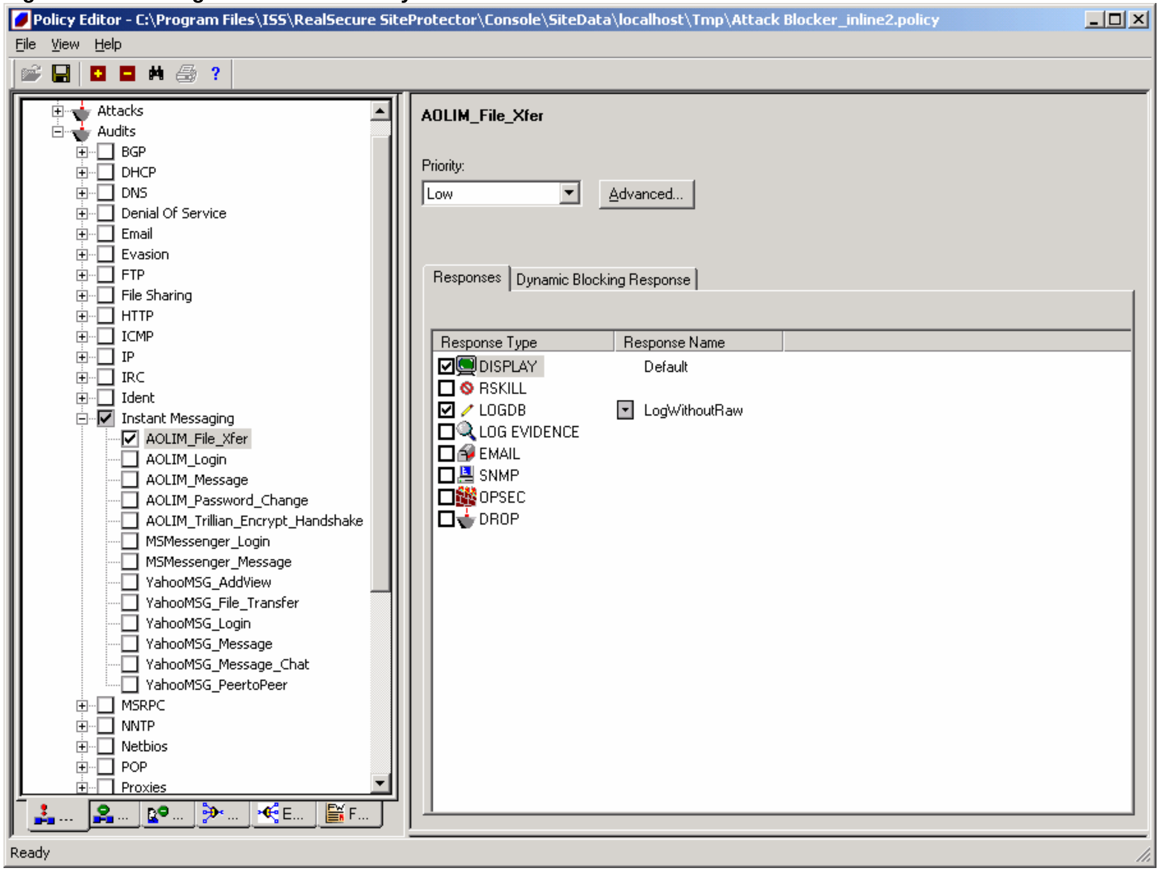
Security Events

Ports... Tuning...

Enable	Event	Priority	Response	Description
□	AOLIM_File_Xfer	Low		AOL Instant Messenger file transfer
□	AOLIM_Login	Low		AOL Instant Messenger login
□	AOLIM_Message	Low		AOL Instant Messenger message
□	AOLIM_Password_Change	Low		AOL Instant Messenger password change
□	AOLIM_Trillian_Encrypt_Handshake	Low		Trillian encrypted messaging handshake
□	MSMessenger_Login	Low		Microsoft Messenger login
□	MSMessenger_Message	Low		Microsoft Messenger message
□	YahooMSG_AddView	Medium		Yahoo Messaging AddView
□	YahooMSG_File_Transfer	Low		Yahoo Messaging file transfer
□	YahooMSG_Login	Low		Yahoo Messaging login
□	YahooMSG_Message	Low		Yahoo Messaging message
□	YahooMSG_Message_Chat	Low		Yahoo Messaging Chat message
□	YahooMSG_PeertoPeer	Low		Yahoo Messaging Peer to Peer switch

Select the events you want to block by checking the corresponding checkbox (Figure 2).

Figure 2 – Selecting Events in the Policy Editor



Policy Editor - C:\Program Files\ISS\RealSecure SiteProtector\Console\SiteData\localhost\Tmp\Attack Blocker_inline2.policy

- Attacks
- Audits
  - □ BGP
  - □ DHCP
  - □ DNS
  - □ Denial Of Service
  - □ Email
  - □ Evasion
  - □ FTP
  - □ File Sharing
  - □ HTTP
  - □ ICMP
  - □ IP
  - □ IRC
  - □ Ident
  - ☑ Instant Messaging
    - ☑ AOLIM_File_Xfer
    - □ AOLIM_Login
    - □ AOLIM_Message
    - □ AOLIM_Password_Change
    - □ AOLIM_Trillian_Encrypt_Handshake
    - □ MSMessenger_Login
    - □ MSMessenger_Message
    - □ YahooMSG_AddView
    - □ YahooMSG_File_Transfer
    - □ YahooMSG_Login
    - □ YahooMSG_Message
    - □ YahooMSG_Message_Chat
    - □ YahooMSG_PeertoPeer
  - □ MSRPC
  - □ NNTP
  - □ Netbios
  - □ POP
  - □ Proxies

AOLIM_File_Xfer

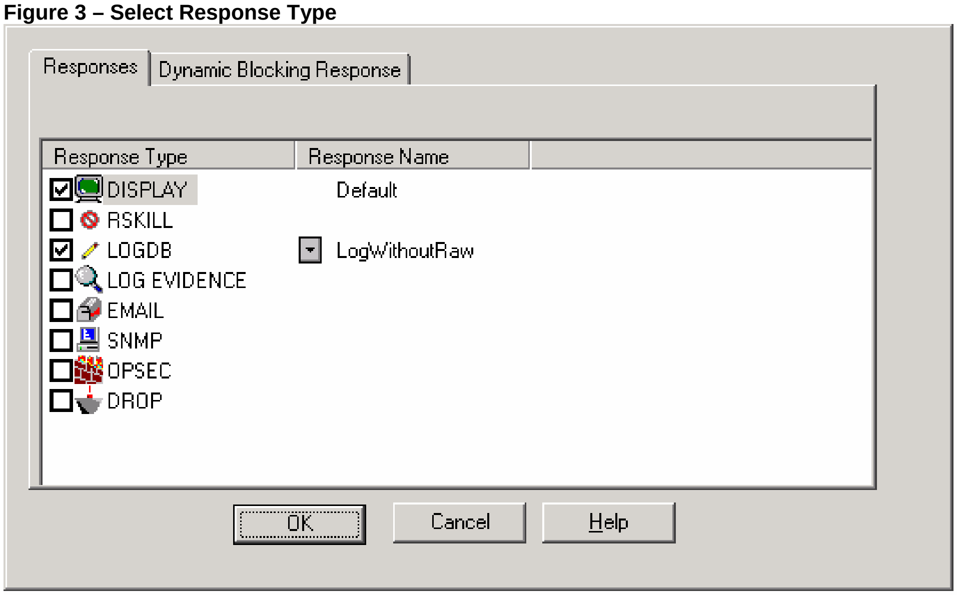
Priority: Low

Response Type	Response Name
☑ DISPLAY	Default
□ RSKILL	
☑ LOGDB	LogWithoutRaw
□ LOG EVIDENCE	
□ EMAIL	
□ SNMP	
□ OPSEC	
□ DROP	

Ready

After selecting an event, select the appropriate response for the event in your environment (Figure 3).

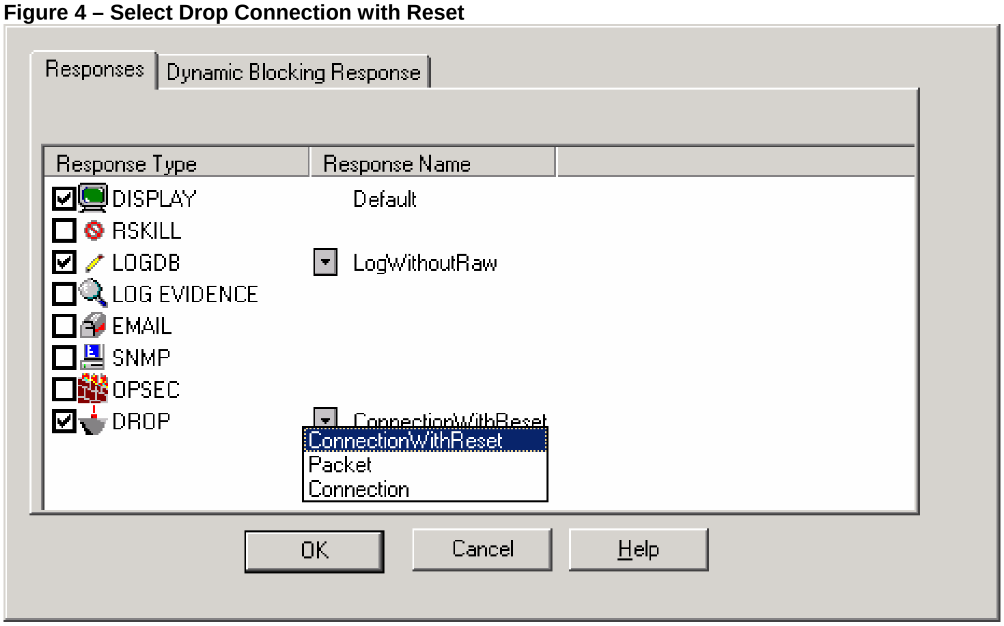
Figure 3 – Select Response Type



Response Type	Response Name
☑ DISPLAY	Default
☐ RSKILL	
☑ LOGDB	LogWithoutRaw
☐ LOG EVIDENCE	
☐ EMAIL	
☐ SNMP	
☐ OPSEC	
☐ DROP	

Based on the type of traffic (predominantly TCP) Internet Security Systems recommends using the “drop connection with reset” response for all signatures (Figure 4). UDP and ICMP Packets associated with selected signatures will be dropped by default with the “drop connection reset” response.

Figure 4 – Select Drop Connection with Reset

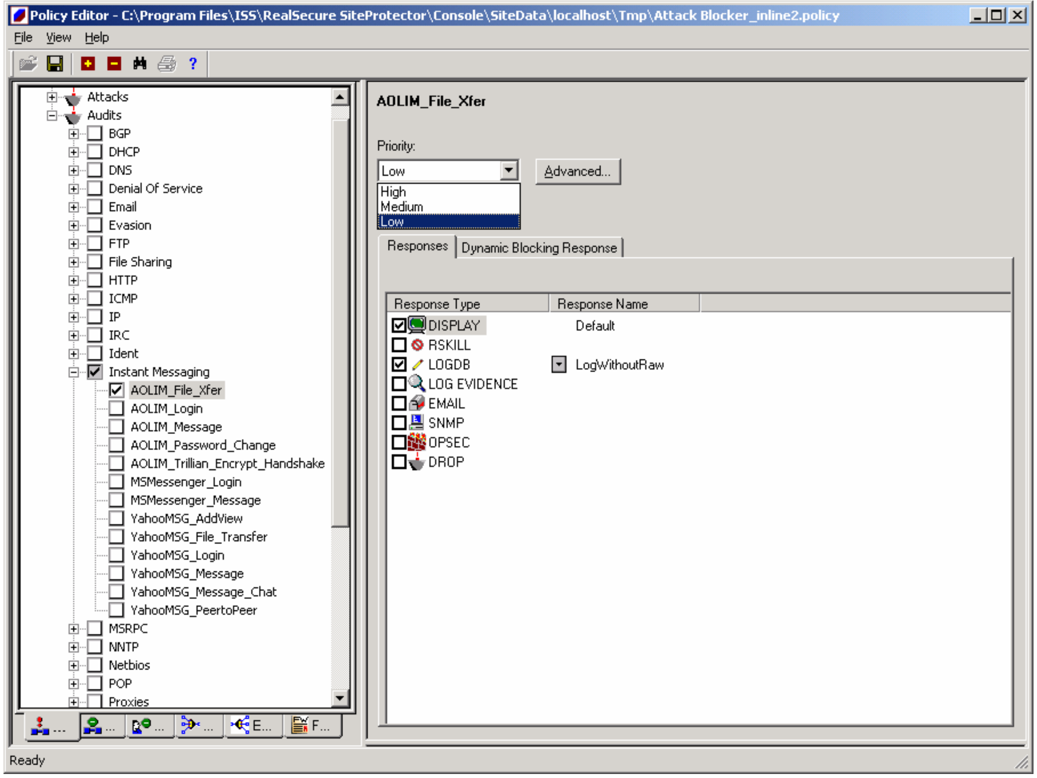


Response Type	Response Name
☑ DISPLAY	Default
☐ RSKILL	
☑ LOGDB	LogWithoutRaw
☐ LOG EVIDENCE	
☐ EMAIL	
☐ SNMP	
☐ OPSEC	
☑ DROP	ConnectionWithReset

ConnectionWithReset
Packet
Connection

Set the priority that you want to associate with the newly added signatures (Figure 5).

Figure 5 – Select Priority



Policy Editor - C:\Program Files\ISS\RealSecure SiteProtector\Console\SiteData\localhost\Tmp\Attack Blocker_inline2.policy

- Attacks
- Audits
  - □ BGP
  - □ DHCP
  - □ DNS
  - □ Denial Of Service
  - □ Email
  - □ Evasion
  - □ FTP
  - □ File Sharing
  - □ HTTP
  - □ ICMP
  - □ IP
  - □ IRC
  - □ Ident
  - ☑ Instant Messaging
    - ☑ AOLIM_File_Xfer
    - □ AOLIM_Login
    - □ AOLIM_Message
    - □ AOLIM_Password_Change
    - □ AOLIM_Trillian_Encrypt_Handshake
    - □ MSMessenger_Login
    - □ MSMessenger_Message
    - □ YahooMSG_AddView
    - □ YahooMSG_File_Transfer
    - □ YahooMSG_Login
    - □ YahooMSG_Message
    - □ YahooMSG_Message_Chat
    - □ YahooMSG_PeertoPeer
  - □ MSRPC
  - □ NNTP
  - □ Netbios
  - □ POP
  - □ Proxies

AOLIM_File_Xfer

Priority: Low

High
Medium
Low

Response Type	Response Name
☑ DISPLAY	Default
□ RSKILL	
☑ LOGDB	LogWithoutRaw
□ LOG EVIDENCE	
□ EMAIL	
□ SNMP	
□ OPSEC	
□ DROP	

Ready

Source: comSource Media Metrix,

March 2003

Appendix

The Threat Matrix table below identifies the applicable risks associated with peer-to-peer and instant messaging applications.

Threat Matrix

Application	Un-encrypted	File Transfer	Known Buffer Overflows	Remote Control	Known Worms	Spy-ware	Social Engineering	Misuse of Bandwidth/ Copyright Issues	Targeted by Known Viruses
AIM	X	X	X				X	X	X
MSN	X	X	X	X	X		X	X	X
Yahoo!	X	X	X				X	X	
ICQ	X	X	X		X		X	X	X
Trillian		X	X				X	X	
KaZaA	X	X	X		X	X		X	X
gnutella	X	X						X	X
eDonkey	X	X	X		X			X	X
SoulSeek	X	X						X	X
DirectConnect	X	X						X	X

The Port Information matrix below shows ports associated with peer-to-peer and instant messaging applications.

Port Information

Application	Messaging/ Connect	Video	Voice	FileXfer	Images/ Direct Connect	App Sharing
AIM	5190	n/a	5190 Range	5190	4443	n/a
ICQ	5190	n/a	5190 Range	3574/7320	n/a	n/a
MSN	1863	5004, Range	6901	6891-6900	n/a	1503
Yahoo!	5050, 80, Range	5100, Range	5000, Range	5010, Range	n/a	n/a
KaZaA	1214	n/a	n/a	1214	n/a	n/a
gnutella	6346	n/a	n/a	80	n/a	n/a
eDonkey	4661, 4665	n/a	n/a	4662	n/a	n/a
SoulSeek	2234,5534	n/a	n/a	2234,5534	n/a	n/a
DirectConnect	411	n/a	n/a	1025-32000	n/a	n/a

About Internet Security Systems (ISS)

Internet Security Systems, Inc. (ISS) is the trusted expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 11,000 customers worldwide. ISS products and services are based on the proactive security intelligence conducted by ISS' X-Force® research and development team— the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at http://www.iss.net or call 800-776-2362.