



PacketSure Network Application Management Protocols & Applications in Default Rules Set and File Types Analyzed

Protocols and Applications

Out of the box, PacketSure can be set to monitor, block, or allow the following protocols and applications:

HTTP PROTOCOLS

Protocols that use the HTTP protocol to transfer files.

- **HTTP** HTTP (Hyper Text Transfer Protocol) is the underlying protocol of the World Wide Web.
- **HTTP-ACTIVEX** ActiveX controls are objects inserted into a Web page or other applications to reuse packaged programming functionality; because these controls execute on a user's computer, they may be a security and/or virus risk. This setting manages user attempts to transfer ActiveX controls through the HTTP protocol.
- **HTTP-AVI** Microsoft video format file transfers over HTTP.
- **HTTP-EXE** HTTP-EXE manages user attempts to transfer executable files through the HTTP protocol. Because these files execute on a user's computer, they may be a security and/or virus risk.
- **HTTP-Audio-MPEG** HTTP-Audio-MPEG manages user attempts to transfer MPEG audio files through the HTTP protocol.
- **HTTP-Video-MPEG** HTTP-Video-MPEG manages user attempts to transfer MPEG video files through the HTTP protocol.
- **HTTP-QuickTime** Manages user attempts to transfer Quick Time files through the HTTP protocol.
- **HTTP-RAR** RAR-format archive files transferred over HTTP.
- **HTTPS** HTTPS is a secure connection for the HTTP protocol; it uses port 443.
- **HTTP-SHOCKWAVE-FLASH** Shockwave allows users to view interactive Web content like games, business presentations, entertainment and advertisements from a Web browser. This setting manages user attempts to transfer Shockwave through the HTTP protocol.
- **HTTP-Zip** HTTP-Zip manages user attempts to transfer Zip files through the HTTP protocol. Because these files execute on a user's computer, they may be a security and/or virus risk.

HTTP INFORMATION

- **HTTP_Hosts** This rule matches host names in HTTP requests with host names in a list that you create. If a hostname in the list begins with a period (.), it is considered a domain name and all hosts in that domain will match.
- **HTTP_Servers** This rule enables the ability to capture data for the Web Monitor capability in TrendReporter and logs URLs and hosts in the URL Log. This rule, like LogUnmatched, does not match connections. It is used for data collection only, not for blocking or allowing. When adding this rule, some options in the Rule Properties window are unavailable. It is recommended that you place this rule near the top of the list so it captures information from all HTTP data.
- **HTTP_URLs** This rule matches URLs in HTTP requests with URLs in a list that you create.

WORM MITIGATION

The Palisade support team often adds new signatures to our web site for you to download. Many of these effect worms that may compromise your system. Check the signature page at <http://www.palisadesys.com/support/downloads/ PacketSure/sigupdates.shtml> for the most recently added signatures. Your Palisade web site user name and password is required.

INFORMATION SERVICES

- **AOL-TCP** Manages use of the AOL information service over the internet.
- **Compuserve-TCP** Manages use of the Compuserve information service over the internet.

VOICE OVER IP (VoIP)

- **SIP** is the signaling protocol used for Internet conferencing, telephony, presence, event notification, and instant messaging.
- **H.323** A real-time communication protocol used for VoIP and conferencing.
- **Q.931** A signaling protocol used by H.323 communications.
- **Skinny** A special-purpose protocol used for communication between VoIP handsets products and IP PBXs.

FILE SHARING APPLICATIONS

Applications that allow users to share files across the Internet.

- **AudioGalaxyWeb** This setting allows you to manage access to the AudioGalaxy web sites.
- **BitTorrent** BitTorrent is a tool for copying and sharing files. Files clients download are automatically copied onto client's machine and are made available for peer-to-peer sharing.
- **BlubsterXfer** A peer-to-peer file sharing application for MP3 files.
- **DirectConnectHub** Matches initial hub connection message.
- **DirectConnectXfer** A host-based synthesizer/sampler streaming tool.
- **EDonkey (including OverNet)** Peer-to-peer file-sharing application.
- **EDonkeyXfer** Peer-to-peer file-sharing application.
- **FiletopiaXfer** Filetopia is a free communications software that includes: instant messaging, chat, file sharing system with a search engine, online friends list and message boards.
- **FreeNet** A distributed, encrypted file sharing system used to anonymously share files. FreeNet nodes store encrypted pieces of files that are indexed by keys. As a result of its design, FreeNet can be used to anonymously and confidentially store and retrieve data, thus avoiding content filters and government limitations.
- **FurtherNetClient** A peer to peer file sharing system.
- **Gnutella** Gnutella is a file-sharing application that allows users to exchange any type of files by connecting them to a "daisy-chain" of other machines. PacketSure also manages these other applications that are based on the Gnutella protocol:
 - Bearshare
 - BearshareXferEnc
 - Bodetella
 - Cooltella
 - Furi Launcher
 - Furi Updater
 - Gnewtella
 - Gnewtella 2
 - GnOtella
 - GnuCache
 - Gnucleus
 - Gnujatella
 - Gnumm
 - Gnuspace
 - Gnutella for Mac
 - Gnut
 - Gnutella.it
 - Gobobo
 - GTK-Gnutella
 - Hagelslag
 - Limewire
 - Mactella
 - Morpheus
 - MyGnut
 - MyTella
 - N-Tella
 - Newtella
 - PeaGnut
 - Pi
 - Pygnut
 - Reflector
 - SeachLord
 - Shareaza
 - Gnute
 - Gnutmeg
 - Gnutella Crawler
 - Tellaseek
 - Toadnode
- **Gnutella2UDP** A UDP-only rule that matches UDP packets with Gnutella2 data that would not be matched by the Gnutella rules.
- **GnutellaXfer** GnutellaXfer matches file transfers between many Gnutella clients, including Bearshare, LimeWire, Gnotella, Gnutella, Gnucleus, and Morpheus.
- **IRC-DCC-Send Direct chat (DCC)** file transfers on Internet Relay Chat (IRC).
- **iTunes** A pay-per-song music download service. CAUTION: The signature matches after the user pays for the song.
- **KaZaA** (including Morpheus) KaZaA is a file-sharing service where users can trade audio, video, images, and other documents through a "daisy chain" connection.
- **KaZaAXfer** Blocks attempts to transfer files using the KaZaA protocol.
- **Napster** Napster is a central-server based file-sharing application that allows users to exchange MP3 music files. PacketSure also manages these other applications that are based on the Napster protocol:
 - Amster
 - BeNapster
 - Blazter
 - Capster
 - Console Napster CLT
 - DeWrapster
 - DiaRRIA
 - DJnap
 - Fanster
 - File Navigator
 - NapAmp
 - Napigator
 - Napkin
 - NapMan
 - Napsack
 - Napster for Beos.htm
 - Napster/2
 - Napsterminator
 - Napster - Linux
 - Napster Server Manager
 - Gnapster
 - Gnome-Napster
 - GTK-Napster
 - Hackster
 - iNapster
 - JNap
 - J Napster
 - Jnerve
 - KNapster
 - Koog Epsilon
 - Lopster
 - Macstar
 - Macstar
 - Macster
 - Music City
 - MyNapster
 - Napster Unban
 - Netstreak iAssimilator
 - N-Dream Plug-In for
 - Napster
 - OpenNap
 - Pakster
 - Rapster
 - Riscster
 - Snap
 - Socks2HTTP
 - Spyster
 - TekNap
 - TKNap
 - Unwrapper
 - Webnap
 - Wrapster
 - XMMap
- **Napster Xfer** This setting allows you to manage all Napster uploads, downloads, and hot list transfers.
- **SoulSeekLogin** File-sharing application known for exchange of rare music files.
- **SoulSeekXfer** Manages all SoulSeek transfers.

- **Twister** A free Internet program to find and download MP3 and other music files.

INSTANT MESSAGING

Applications that allow users to send and receive messages in real time.

- **AIMLogin** America Online Instant Messenger (AIM) is an instant message and file-transfer application that allows users to chat and share files. This setting allows you to manage user logins to AIM.
- **AIMMsg** This setting allows you to manage incoming and outgoing AIM messages.
- **AIMXfer** This setting allows you to manage AOL Instant Messenger file transfers.
- **GoogleTalk** This setting allows you to manage incoming and outgoing Google Instant Messages.
- **ICQLLogin** ICQ is an instant messenger and file transfer service that allows you to manage user logins to ICQ.
- **ICQMsg** This feature allows you to manage incoming and outgoing ICQ messages.
- **IRCLLogin** Matches logins to the Internet Relay Chat (IRC) protocol. IRC provides chat rooms, but is often used to share files in violation of copyright laws. Intruders will often set up IRC servers on compromised computers to assist their sharing of files.
- **MSNMessengerLogin** MSN Messenger is an instant messaging service provided by the Microsoft Network. This feature allows you to block your users from logging into MSN Messenger.
- **MSNMessengerXfer** This feature allows you to block users from transferring files through MSN Messenger.
- **YahooMsgLogin** Yahoo Messenger is an instant messaging service. This feature allows you to block your users from logging into Yahoo Messenger.
- **YahooMsgRMsg** This setting allows you to block Yahoo messages and file transfers.

FILE/PRINTER/OS

- **LPR** LPR is a BSD UNIX printing protocol that supports printing to network and local printers. It also acts as a print server. LPR uses port 515.
- **Microsoft-DS** Microsoft-DS is a file sharing application that allows users to share files through port 445.
- **NetBIOS-SSN** NetBIOS-SSN is a Microsoft File Sharing application that uses port 139.
- **NFS** A Network File System (NFS) provides remote access to shared file systems across networks, allowing them to be accessed as if they were local.

MULTI-MEDIA

Applications that allow users to stream audio and video to their desktops.

- **RealMedia 1, 2, and Multi Rate** RealAudio and RealVideo are streaming formats that many sites use to transfer audio and video; Real Networks use two different protocols, and we've included both separately for your convenience. To block *all* RealMedia, you must block both of these protocols.
- **ShoutCast** ShoutCast is a streaming media format that many sites use to transfer audio.
- **WindowsMedia** Windows Streaming Media is a streaming format that many sites use to transfer audio and video.

MAIL PROTOCOLS

Protocols used to transfer e-mail.

- **IMAP** IMAP (Interim Mail Access Protocol) is a mail protocol that uses port 143.
- **IMAPS** IMAPS allows users to access their mail through a secure SSL connection; it uses port 993.
- **POP** POP (Post Office Protocol) is a mail protocol that uses port 109/110.
- **POP3S** POP3S allows remote users to access their mail through a secure SSL connection; it uses port 995.
- **SMTP** SMTP (Simple Mail Transfer Protocol) is a mail protocol that uses port 25.

WEB-BASED MAIL

E-mail programs using standard HTTP.

- **AOLWebmail** Web access for AOL mail.
- **GoogleMailSend** An e-mail program by Google that provides web mail access from the Internet.
- **Hotmail** An e-mail program that provides e-mail access from any computer connected to the Internet.
- **YahooMail** Another e-mail program providing access to e-mail from the Internet.

FTP

File transfer protocol.

- **CVS-PServer** Concurrent Versions System (CVS) is an open-source change management system. This rule matches the protocol used to access files on the CVS server.



- **CVSup** Concurrent Version System Update (CVSup) is a high-performance protocol used to mirror changes in a file on the CVS server. This rule matches the protocol used by the client to access the server.
- **FTPActive** This setting allows you to block FTP active file transfers on Port 20.
- **FTPControl** This setting allows you to block the FTP control port (port 21).
- **FTPPassive** This setting allows you to block passive FTP file transfers.

REMOTE LOGIN

- **CitrixICA** Matches Citrix's Independent Computing Architecture (ICA) protocol, which is used for remote access to computers running Microsoft Windows applications.
- **GotoMyPCShare** Application that allows remote access to a user's computer.
- **RLogin** RLogin (Remote Login Protocol) allows users to log into the network remotely using port 513.
- **RExec** Allows remote execution of commands on UNIX hosts, or any other system with the RExec interface.
- **RSH** RSH (Remote Shell Protocol) allows users to execute shell commands remotely using port 514.
- **SSH** A secure shell protocol that provides connectivity, encryption, and authentication for servers using port 22.
- **Telnet** Telnet Remote Terminal Protocol allows users to login to other systems remotely. Telnet uses port 23.
- **VNC** Virtual Network Computing (VNC) is a remote display system allowing users to remotely view a desktop from anywhere on the Internet. VNC uses port 5190.
- **WindowsTerminalServer** Remote connections using Windows Terminal Server.
- **XWindows** Graphical user interface primarily for UNIX similar to Microsoft Windows.

DISTRIBUTED COMPUTING

These programs allow organizations to use your computer when it is idle.

- **BOINC** SETI@Home's new distributed computation protocol.

OTHER

Standard TCP/IP protocols and others you may wish to manage.

- **DNS Query** Manage activity on the domain name server (DNS).
- **Finger** Finger User Information Protocol is a UNIX command used to gather information about other Internet users. Finger uses port 79.
- **Gopher** Gopher is a system that pre-dates the World Wide Web for organizing and displaying files on Internet servers. Gopher uses port 70.
- **IDENT** UNIX-based protocol that looks up real user names when a user attempts to login to a server.
- **NetBIOS-SendMulti** Multi-packet NetBIOS user messages.
- **NNTP** NNTP (Network News Transfer Protocol) is a news service that transmits information through port 119.
- **Port** The Port setting allows users to specify a block of a specific TCP/IP port.
- **Socks4/5** Protocol that provides access to network services through a SOCKS proxy server. This may be used to hide a user's identity and evade network management systems like PacketSure.
- **SSL** Used to assist system administrators in determining how much encrypted traffic is running (aside from HTTPS and POP3S)
- **WakeOnLan** A UDP packet that can start a machine on the network that has been shut down.

SPECIAL RULES

- **Custom** This setting allows you to enter your own Custom Match String for a protocol that you've identified and wish to manage. This is recommended only for advanced users.
- **EthernetAddresses** This rule matches packets that have a source or destination Ethernet address that is in a user-created list.
- **Everything** This setting allows you to block, monitor, or ignore any connection by any of the protocols managed by PacketSure.
- **LogUnmatched** The LogUnmatched rule allows you to log all connections that do not match defined protocols.

File Types Analyzed

PacketSure analyzes many different types of files for private content. Metadata, text, and character sets are extracted for all types, except those marked with an asterisk (*). For these file types, only metadata (title, subject, author, etc.) is extracted. The following table lists the file types that are analyzed for private content

Format	Version	Extension
Archive Formats		
PKZIP	through 2.04g	unzip; zip
Computer Aided Design		
AutoCAD Drawing	R13, R14, 2000, 2004	DWG
AutoCAD Drawing Exchange	R13, R14, 2000, 2004	DLL
Microsoft Project*	98, 2000, 2002	MPP
Microsoft Visio	5, 6, 2000, 2002, 2003	VSD
Adobe Portable Document Format	1.1 to 1.6	PDF
Graphic Formats		
CorelDRAW (TIFF header)	through to 9.0 C	DR Y
DCX Fax System	TIFF/CCITT/DCX	DCX
Enhanced Metafile	n/a	EPS
Tagged Image File*	3.0 to 6.0	TIFF
Windows Metafile	3	WMF
Mail Formats		
Lotus Notes database	4, 5, 6.0, 6.5	NSF
Mailbox email ¹	Eudora 6.2	
Thunderbird 1.0	MBX	
Microsoft Outlook	97, 2000, 2002, 2003	MSG
Microsoft Outlook Express	n/a	EML
Microsoft Outlook Personal Folder (Windows only)	97, 2000, 2002, 2003	PST
Multimedia Formats		
MPEG-1 Audio layer 3 ID3*	versions 1 and 2	MP3
Presentation Formats		
Applix Presents ()	4.0, 4.2, 4.3, 4.4	AG
Corel Presentations	7, 9, 10, 11, 2000	SHW
Lotus Freelance Graphics	96, 97, 98, R9, 9.8	PRZ
Lotus Freelance Graphics 2	2	PRE
Microsoft PowerPoint Windows	97, 2000, 2002, 2003	PPT
Microsoft PowerPoint Windows	95	PPT
Microsoft PowerPoint	PC4	PPT
Microsoft PowerPoint Macintosh	98	PPT
Spreadsheet Formats		
Applix Spreadsheets	4.2, 4.3, 4.4	AS
Comma Separated Values ()	n/a	CSV
Corel Quattro Pro	5, 6, 7, 8	QPW WB3
Lotus 1-2-3	96, 97, R9, 9.8	123
Lotus 1-2-3	2, 3, 4, 5	WK4
Lotus 1-2-3 Charts	2, 3, 4, 5	123
Microsoft Excel Windows	2.2, through 2003	XLS
Microsoft Excel Charts	2, 3, 4, 5, 6, 7	XLS
Microsoft Excel Macintosh	98	XLS
Microsoft Works Spreadsheet	1, 2, 3, 4	S30 S40
Word Processing Formats		
Text and Markup		

¹ MBX files created by other common mail applications are typically filtered, converted, or displayed.

Format	Version	Extension
ANSI	n/a	TXT
ASCII	n/a	TXT
HTML	3, 4.0	HTM
MIME	n/a	EML
IBM DCA/RFT (Revisable Form Text)	SC23-0758-1	DC
Microsoft Excel Windows XML	2003	XML
Microsoft Word Windows XML	2003	XML
Microsoft Visio XML	2003	VDX
OpenOffice	1, 1.1	SXI; SXP; SXC; SXW
Rich Text Format	1 through 1.7	RTF
StarOffice	6, 7	SXI; SXP; SXC; SXW
Unicode Text	3, 4	TXT
XHTML	1.0	HTM
XML (generic)	1.0	XML
Word Processors		
Adobe Maker Interchange Format	5, 5.5, 6, 7	MIF
Applix Words	3.11, 4, 4.1, 4.2, 4.3, 4.4	AW
DisplayWrite	4	IP
Folio Flat File	3.1	FFF
Fujitsu Oasis	7	OA2
JustSystems Ichitaro	8, 9, 10, 12	JTD
Lotus AMI Pro	2, 3	SAM
Lotus AMI Professional Write Plus	2.1	AMI
Lotus Word Pro (Windows x86 only)	96, 97, R9	LWP
Lotus SmartMaster (Windows x86 only)	96, 97	MWP
Microsoft Word PC	4, 5, 5.5, 6	DOC
Microsoft Word Windows	1.0 and 2.0	DOC
Microsoft Word Windows	6, 7, 8, 95	DOC
Microsoft Word Windows	97, 2000, 2002, 2003	DOC
Microsoft Word Macintosh	4, 5, 6, 98	DOC
Microsoft Works	1, 2, 3, 4	WPS
Microsoft Works	6, 2000	WPS
Microsoft Windows Write	1, 2, 3	WRI
WordPad	through 2003	RTF
WordPerfect Windows	5, 5.1	WO
WordPerfect Windows	6, 7, 8, 9, 10, 11, 2000	WPD
WordPerfect Linux	6, 8	WPS
WordPerfect Macintosh	1.02, 2, 2.1, 2.2, 3, 3.1	WPS
XyWrite	4.12	XY4

* Metadata only (title, subject, author, etc.) is extracted.