

Feature  
Brief

# NetEnforcer AC-400/800 Supported Applications and Protocols

© 2006 Allot Communications Ltd. Allot Communications, NetEnforcer and the Allot logo are registered trademarks of Allot Communications. NetXplorer is trademark of Allot Communications. All other brand or product names are trademarks of their respective holders. All information in this document is subject to change without notice. Allot Communications Ltd., and/or its affiliates (collectively "Allot Communications") assume no responsibility for any errors that appear in this document.

## Identifying Layer 7 Protocols with the NetEnforcer® AC-400/800

The NetEnforcer uses deep packet inspection (DPI) technology for identifying applications and protocols, including Layer 7 application signatures and patterns, user-defined content inspection and well known ports.

### Background

Distinguishing between different applications plays a major role in traffic monitoring and management. Allot's DPI offers sophisticated methods for classifying, analyzing and managing network applications and protocols up to Layer 7 (the "application layer").

### Well-Known Ports

In the past, each significant application had an official fixed port number (TCP or UDP) and applications were easily recognized by identifying the application's port number. When a network administrator needed to block the use of a certain application, access was blocked to the appropriate port using a router access list or a simple firewall.

Although virtually any port could be blocked, some ports had to be left open for the network to function. For example, even the most restrictive networks would leave port 80 unblocked, since as the "official" port for HTTP traffic, it was required to be open to enable basic Web access via HTTP. However, this also enabled many "unwanted" applications such as Napster and Kazaa to bypass network restrictions and use port 80 (or revert to it when other ports were blocked). Consequently, determination of application type solely by its port number was no longer sufficient for controlling network traffic.

### Application Signatures

Since applications could no longer be identified solely by their port numbers, an application's signature could be recognized by examining the data transferred above the transport layer (TCP/UDP). This method required special support of many application protocols while the well-known port method still used by many simple network devices requires only TCP/UDP support. Furthermore, many applications employ special techniques to bypass network policies. In addition to using port 80, they also use the actual HTTP protocol as the underlying method for transferring information.

To make traffic classification even more challenging, many standard protocols such as FTP frequently employ "port hopping", in which they initiate communication over a fixed, well-known port but hop to another random port quite quickly. Identification and control of network traffic has thus become quite a complex task.

## Content Inspection

Differentiating one application protocol from another is not always sufficient for managing network traffic. Sometimes it is necessary to distinguish between different types of traffic belonging to the same application. For these types of protocols, a special rule is applied for inspecting the content of the traffic (“content inspection”). For example, a network administrator may need to differentiate between different types of files that are downloaded via HTTP. With HTTP, he may want to block zip files that may contain hidden viruses while permitting HTML.

## Application and Protocol Support

The terms *applications* and *protocols* are often confused. An *application* usually refers to the actual software used, while *protocol* refers to the language the application uses to communicate with peers on the network. For example, two separate applications, Kazaa and Grokster, both use the Kazaa protocol. The NetEnforcer® uses a variety of methods for identifying Layer 7 protocols, including well known ports, application signatures and content inspection.

The following list represents the most common protocols and services supported by the NetEnforcer AC-400/800 series of devices. These protocols are available in the default Service Catalog database. Thousands of other protocols supported by the NetEnforcer can be found in the Advanced Service Catalog or manually defined.

<b>Email</b>	SUNRPC	Ultima
BIFF	SYSLOG	Unreal Tournament
ccMAIL	TFTP	Znes
IMAP	Thunder	
IMAP2		<b>IM/Chat</b>
IMAP3	<b>Games</b>	AOL
IMAPS (Secure IMAP)	Aliens	AOL - Chat
Lotus Notes	Asheron's Call	AOL - File Transfer
MS Exchange	Black and White	AOL - Client
Passive/Active RPC	Counterstrike	AOL - Express
POP2	Dark Reign	Camfrog
POP3	Diablo	Eyeball
SMTP	Doom	ICQ - Chat
SMTP by Sender Domain	Elite Force	ICQ - File Transfer
<b>File Transfer</b>	F22 Simulator	IRC
<b>File System</b>	Fightrace	MSN
CMD	Guild Wars	Chat
FTP	Hexen	File Transfer
FTP – File Names	Kali	Audio
FTP – Passive/Active	Kohan Immortal	Video
FTP – Method	Sovereigns	Qnext
Kontiki	Motorhead	QQ
NetBIOS (IP)	MSN Game	QQ-Audio
SMB	Myth	QQ-Video
NFS	Need For Speed	QQ-Chat
PRINTER	Operation Flash Point	QQ-File Transfer
PRINT-SRV	Outlaws	Trillian
RCP	Quake	
	Swat3	

<p>                     Yahoo                      Yahoo - Chat                      Yahoo - File Transfer                      Yahoo - Voice                 </p> <p> <b>Legacy</b>                      AppleTalk                      AppleTalk Over IP                      DECnet                      Finger                      Gopher                      I-NLSP                      IPX                      IPX Over IP                      MS-IPX                      NetBEUI                      NetWare                      SNA                      Who                      Whois                 </p> <p> <b>Network Infrastructure</b>                      ARP                      AUTH                      BGP                      BOOTP (DHCP)                      BOOTP-CLIENT                      BOOTP-SERVER                      CHARGEN                      CMIP                      CMIP-AGENT                      CMIP-MAN                      DNS                      ECHO                      EGP                      ICMP                      IGMP                      Local MGMT                      NPP                      NTP                      OSPF                      PPPoE                      PPPoE-CONTROL                      PPPoE-DISCOVERY                      RADIUS                      RADIUS-AUTH                      RADIUS-ACCT                      RIP                      RMON                      SNMP                      SNMP-TRAP                      SNMP-Mon                      SYSLOG                      TACACS                      TIMESERVER                 </p>	<p>                     TIME                 </p> <p> <b>P2P</b>                      Ants                      Ares                      BitTorrent (encrypted and non-encrypted)                      Azureus BitTorrent                      BitComet                      G3 Torrent                      µTorrent                      Direct Connect                      DC++                      BCDC++                      Opera's DC (oDC)                      RevConnect                      Earthstation V                      eDonkey                      eMule                      xMule                      ExoSee                      FastTrack                      Diet Kazaa                      Download Accelerator Pro                      Grokster                      Kazaa (v1/v2/v3)                      PeerEnabler                      Poisoned                      FileTopia                      Freenet                      Frost                      Furthur                      Gnutella                      giFT                      Acquisition                      Ares                      Bearshare                      FreeWire                      Gluz                      Gnucleus                      Gtk-Gnutella                      KCeasy                      LimeWire                      LordofSearch                      NEOFnapster                      Nova                      Phex                      Shareaza                      XoloX                      Hopster                      HotLine                      Jabber                      Madster-Aimster                      Mercora                 </p>	<p>                     MP2P                      Manolito                      Blubster                      Piolet                      RocketNet                      Multi-Network                      Epicea                      iMesh                      Morpheus                      Morpheus w/NEONet                      Mute                      Napster2                      Overnet                      Poco                      Share                      Soribada                      SoulSeek                      Warez                      Waste                      WinMX                      Winny (1 &amp; 2)                      Zultrax                 </p> <p> <b>P2P (Asian)</b>                      100BAO                      Baidu                      Kamun                      Kuro                      Real Link                      Sougood                      100GP2P                      KuGoo                 </p> <p> <b>Security</b>                      GRE                      IPIP                      IPSEC                      IPSEC-AH                      IPSEC-ESP                      L2TP                      PPTP                      SUGP                      swipe                      TrendMicro Updates                 </p> <p> <b>Streaming</b>                      Abacast                      Coolstream                      DIGStream                      iTunes                      MMS                      MSplayer                      Napster                      NetShow                      Player365                 </p>
---	--	---

Quicktime	Oracle-VP1, VP2
RealAudio	SAP
RealOne	SAP-DIALOGSERVICE
RTP	SAP-INFOSERVICE
RTSP	SAP-ROUTER
Interleaved	SAP-To-Adabas
RTP/AVP	SAP-To-Informix
Streaming	SQL
RDT	MS-SQL Server
X-PN-TNG	SQL*NET
WeatherBug	SQLSERVICE
Winamp	LDAP
PPLive	LDAPS
HTTP Streaming	
PodCast	<b>VoIP</b>
	GoogleTalk
<b>Terminals</b>	H.323
CITRIX	MGCP
Citrix Datacollec	NetMeeting
Citrix-ICA	Net2Phone
Citrix IMA Client	RTP
Citrix MgmtConsole	SIP
Citrix Nfuse	Skype
Citrix User Name	Skype In/Out
Citrix Published	Skype
Applications	T.120
Citrix Priority (Print)	Vonage
Citrix Web	VocalTec- IPhone
MS-RDP-CLIENT	Ventrilo
pcAnywhere	
RLOGIN	<b>Web Protocols</b>
RTELNET	HTTP
SSH	Host Names
TELNET	Method e.g., GET,POST
TELNETS	Mime Types
X11	URL e.g., File Types
	HTTP-PROXY
<b>Transaction/Database</b>	HTTP Tunnel
CORBA	NNTP
CORBA-IIOP	Socks (4, 5)
CORBA-IIOP-SSL	Socks2HTTP
CyberCash	SoftEther
EXEC	SSL (HTTPS)
Oracle	
Oracle Service	
name/DB name	
Oracle User name	
Oracle-Coauthor	
Oracle-EM1	
Oracle-EM2	
Oracle-Net8cman-Admin	
Oracle-Net8cman	
Oracle-ORASRV	
Oracle-Remote-Database	
Oracle-TLISRV	