

Feature
Brief

NetEnforcer AC-1000 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-1000

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-1000 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.

Email

BIFF
ccMAIL
IMAP
 IMAP2
 IMAP3
 IMAPS (Secure IMAP)
Lotus Notes
MS Exchange
POP2
POP3
SMTP

File Transfer

File System
CMD
FTP
Kontiki
NetBIOS (IP)
SMB
NFS
PRINTER
PRINT-SRV
RCP
SUNRPC
SYSLOG
TFTP
Thunder

Games

Aliens
Asherons Call
Black and White
Counterstrike
Dark Reign
Diablo
Doom
Elite Force
F22 Simulator
Fighterace
Hexen
Kali
Kohan Immortal
Sovereigns
Motorhead
MSN Game
Myth
Need For Speed
Operation Flash Point
Outlaws
Quake
Swat3
Ultima
Unreal Tournament
Znes

IM/Chat

AOL
 AOL - Chat
 AOL - File Transfer
 AOL - Client
 AOL - Express
ICQ
 Chat
 File Transfer
IRC
MSN
 Chat
 File Transfer
Qnext
QQ
 QQ-Audio
 QQ-Video
 QQ-Chat
 QQ-File Transfer
 QQ Live
Trillian
Yahoo
 Yahoo - Chat
 Yahoo - File Transfer

Legacy

AppleTalk
AppleTalk Over IP
DECnet
Finger
Gopher
I-NLSP
IPX
IPX Over IP
MS-IPX
NetBEUI
NetWare
SNA
Who
Whois

Network Infrastructure

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
RADIUS
 RADIUS-AUTH
 RADIUS-ACCT
RIP
RMON
SNMP
 SNMP-TRAP
 SNMP-Mon
TACACS
TIMESERVER
TIME

P2P

Ares
BitTorrent (encrypted
and non-encrypted)
 Azureus BitTorrent
 BitComet
 G3 Torrent
 µTorrent
Direct Connect
 DC++
 BCDC++
 Opera's DC (oDC)
 RevConnect
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
 NEoNapster
 Nova
 Phex
 Shareaza
 XoloX
Hopster
HotLine
Jabber
Madster-Aimster
MP2P
 Manolito
 Blubster
 Piolet
 RockitNet

Multi-Network

Epicea
iMesh
Morpheus
 Morpheus w/NEOnet
Mute
Napster2
Overnet
Poco
Share
Soribada
SoulSeek
WareZ
Waste
WinMX
Zultrax

P2P (Asian)

100BAO
Baidu
Kamun
Kuro
Real Link
Sougood
100GP2P

Security

GRE
IPIP
IPSEC
 IPSEC-AH
 IPSEC-ESP
L2TP
PPTP
SUGP
swIPe
TrendMicro Updates

Streaming

Abacast
Coolstream
DIGStream
iTunes
MMS
MSPlayer
Napster
NetShow
Player365
Quicktime
RealAudio
RealOne
RTP
RTSP
WeatherBug
Winamp
PPLive
YouTube
Tioti
Veoh
HTTP Streaming

Terminals

CITRIX
Citrix-ICA
Citrix IMA Client
Citrix MgmtConsole
Citrix Nfuse
pcAnywhere
RLOGIN
RTELNET
SSH
TELNET
TELNETS
X11

Transaction/Database

CORBA
CORBA-IIOP
CORBA-IIOP-SSL
CyberCash
EXEC
SAP
SAP-DIALOGSERVICE
SAP-INFOSERVICE
SAP-ROUTER
SAP-To-Adabas
SAP-To-Informix
SQL
MS-SQL Server
SQL*NET
SQLSERVICE
LDAP
LDAPS

VoIP

H.323
T.120
NetMeeting
SIP
Skype
Skype In/Out
Skype
VocalTec- iPhone

Web

HTTP
HTTP-PROXY
HTTP Tunnel
Socks (4, 5)
Socks2HTTP
NNTP
SSL (HTTPS) - All