

AccessEnforcer™ All-in-One Security Appliance



Anti-Spam

- SMTP filtering
- POP3 filtering
- Individual end-user email quarantines
- Safe message preview in email quarantine
- One-click email release from quarantine
- Quarantine summary scheduling
- Personal email address whitelists
- Global sender whitelists
- Global sender blacklists
- Automatic population of global sender whitelist
- Automatic deletion of obvious spam
- Active Directory integration
- Spam tagging
- Anti-phishing
- Real-time URL checking via SURBLs
- Connection management
- Strict email recipient checking
- DNS real-time blacklists (RBLs)
- Custom DNS real-time blacklists
- DNS real-time whitelists
- Spam sensitivity adjustment
- Sender Policy Framework (SPF)
- Collaborative hash systems
- Domain reputation
- Geographic email policies
- Mailbagging

Anti-Virus

- DyVax™ signature-less antivirus engine for zero-day threats
- Deep scanning of executable attachments
- Deep scanning of Microsoft Office attachments for zero-day exploits

Anti-Spyware

- Spyware Blocking via URL Blocking
- Spyware Blocking via IPS signatures

Web Filtering

- Monitoring mode
- Enforcement mode
- URL blacklist categories
- Custom URL blacklists
- URL whitelists
- Positive enforcement (restrict to whitelist)
- Extension blocking
- File Type blocking, including ActiveX
- Spyware blocking
- Antivirus scanning
- Content filtering by keywords
- Caching for faster downloads

IM Blocking

- AOL Instant Messenger (AIM)
- ICQ
- Jabber
- MSN
- Yahoo! Messenger
- Google Talk
- Internet Relay Chat (IRC)

P2P Blocking

- Ares
- BitTorrent
- Manolito
- Direct Connect
- eDonkey
- Kaaza
- MS Foldershare
- GnucDNA
- IRC Bots
- Gnutella
- LimeWire
- Morpheus
- Napster
- Overnet
- Phatbot

AccessEnforcer™ Features

VPN

- IPSec VPN
- Gateway-to-gateway
- Gateway-to-host
- AES / 3DES / Blowfish encryption
- SHA1, SHA256, SHA384, SHA512, MD5 authentication
- Static Keying
- Automatic Keying
- IPS enforcement within VPN tunnels
- Friendly IPsec wizard
- PPTP passthrough

Firewall

- High-quality PF firewall
- Stateful packet inspection
- SYN Flood DoS protection
- DDoS protection
- Anti-Fragmentation
- ICMP blocking
- Attack reconnaissance blocking
- IP whitelisting
- IP blacklisting

Intrusion Detection and Prevention

- Snort®, the same IDS/IPS engine used by government and military organizations
- Over 4,000 high-quality signatures
- IP whitelisting
- IP blacklisting
- Rule management and exceptions
- Dynamic blacklisting of offenders
- Denial of service protection
- Bots
- Exploits

- Adware
- Downloader
- Spyware
- Trojans
- Cross-site scripting attempts
- VoIP attacks

Network Management

- Friendly web-based interface
- Static IP Mapping (1:1 NAT)
- Port forwarding
- Static routes
- Static IP addressing
- DHCP IP addressing
- IP aliases
- Individual subnets (LANs)
- NAT
- DHCP server for each subnet
- DNS server for each subnet
- Fixed MAC-IP address mapping
- MAC address cloning/spoofing
- Secure HTTPS remote management
- Automatic maintenance-free updates
- Diagnostic tools
- Backup/restore
- Highly secure OpenBSD platform

Reporting

- Firewall and IPS network alerts
- Live connection monitoring
- Traffic usage graphs
- Email quarantine reports
- Web traffic reports
- Syslog
- Daily administrator PDF reports

Corporate Headquarters
8701 Mallard Creek Rd
Charlotte, NC 28262
United States
704.971.8989 p
704.971.8990 f
sales@calyptix.com
www.calyptix.com

calyptix™
SECURITY

AccessEnforcer™



© 2008 Calyptix Security Corporation. All rights reserved. Information subject to change without notice. Calyptix Security, the Calyptix Security logo, AccessEnforcer, DyVax, DyVax Protected, and the DyVax Protected logo are trademarks of Calyptix Security Corporation. Snort® is a registered trademark of Sourcefire, Inc.

Updated: February 19 2008