AccessEnforcer Version 4.0

Features List

AccessEnforcer UTM Firewall is the simple way to secure and manage your small business network. You can choose from six hardware models, each designed to protect networks of a different size. Each model has the same firmware and security features. [1]

Standard service includes the following

Network Security & Firewall

- Intrusion detection and prevention (IDS/IPS)
- SYN flood protection

Denial of service (DOS and DDOS) protection

- Anti-fragmentation
- ICMP packet blocking
- Outbound traffic filtering by protocol, source and destination IP address/CIDR range, and port number
- Spoofing and scan protection
- Firewall filter optimization with four settings: Normal, Aggressive, High-Latency (Satellite), and Conservative
- Firewall block policy to silently drop refused connections or notify the source

Intrusion Detection & Prevention

- Static CIDR whitelist and blacklist with import and export
- Dynamic blacklisting to block traffic from hostile source IP addresses
- Detect and block malicious network traffic
- IDS/IPS engine powered by SNORT®
- Thousands of rules to detect and prevent network threats such as malware, ransomware, backdoors, exploits, botnet activity, adware, and much more
- Enable/disable rulesets and individual rules
- Additional rulesets available by entering an Oinkcode (available for free at Snort.org)
- Ruleset policies to prioritize conectivity, security, or a balance of both
- Auto-enable new rule categories when downloaded
- Allow IDS/IPS engine to scan outbound connections

Quality of Service (QoS)

- Traffic prioritization on a scale of 0-7 to ensure the most important traffic is proccessed first
- Improve network performance with simple bandwidth management
- Bandwidth queues with optional minimum and maximum bandwidth limits
- Define minimum limits to ensure service quality (such as to ensure VoIP call quality)
- Define maximum limits to restrict services (such as guest wireless network)

calyptix® SECURITY

- Maximum upload and download speed configurable for any WAN
- Burst options to allow bandwidth queues to temporarily expand during times of high traffic
- Traffic assignment to bandwidth queues using any combination of IP address/CIDR range, ports, protocols, and direction (inbound or outbound)

Network Setup

- Accelerate deployment with a GUI-based console and point-and-click administration
- Quality of service (QoS) for bandwidth management
- Multi-WAN with load balancing and failover
- Dimilitarized zones (DMZs) with a single click
- Integration with Microsoft Active Directory (AD)
- Port forwarding rules with configurable source IP address/CIDR ranges
- Static routing and IP mapping (1:1 NAT)
- Static and dynamic DNS settings
- SIP proxy server integration
- DHCP server with configurable ranges and reservations
- Multiple network interface cards (NICs), which are physically separate for easy DMZ segmentation and switching between LAN and WAN models
- IP aliasing
- MAC address cloning
- PPPoE support (DSL)
- Automatically saved configuration files for rapid deployment of additional or replacement AccessEnforcer devices

Network Management

- Troubleshooter that tests 70+ network settings and services with one click
- System status dashboard showing network statistics, enabled security settings, WAN/link status, system health, and charts of current network traffic allowed and blocked
- Live connections dashboard showing local hosts with corresponding the bandwidth use and number of outbound and inbound connections
- Network alerts dashboard showing the alert type, action taken, IP addresses, the time, and more
- Select any network alert to blacklist or whitelist the source or destination IP address or disable the corresponding IDS/IPS rule
- Web traffic dashboard showing the top websites visited and top web users by number of sites visited and bandwidth consumed
- Rejected spam dashboard showing SMTP connections refused due to invalid sender, invalid recipient, or failure to reverse-resolve to a valid FQDN
- Login attempts log showing failed and successful attempts, the time, and source IP address
- System log showing events such as shutdown, boot, and restore
- IP conflicts dashboard showing local hosts configured with the same IP address
- User state dashboard showing current Microsoft AD users with the client, username, IP address, host name, and MAC address
- DHCP client dashboard showing current host IP addresses, hostname, network, manufacturer, start time, and stop time

- SNMP daemon to provide statistics to SNMP monitoring tools
- Best practice analyzer that reviews and suggest changes to improve network security and configuration
- Diagnostic tools including packet analyzer, ARP table, ping, DNS lookup, traceroute, telnet, CIDR calculator, route table, and whois lookup
- Microsoft AD integration automatically displays AD usernames with associated IP addresses throughout the management interface

Remote Management

- Single pane of glass (SPS) management dashboard showing all deployed AccessEnforcer devices with the corresponding customer name, IP address, firmware version, subscription status, configuration backups, and more [2]
- AccessEnforcer remote management interface accessible via web browser
- Configurable port number for remote management access
- Restrict remote management access for administrator to a list of IP address/CIDR ranges
- Restrict email quarantine access for administrator to a list of IP address/CIDR ranges
- Limit session time and idle time for remote management
- HTTPS SSL certificate for management console/email quarantine

Web Security

- Block access to malicious and distracting web content and services
- Define policies to allow or deny specified web traffic
- Block web traffic by topic, keyword, extension, and file-type
- Target policies by IP address/CIDR range and time of day
- Microsoft AD integration to web filtering policies by AD usernames and groups
- Exempt hosts from web filter policies by IP address/CIDR range and domain
- HTTPS web filter with one-click activation
- Web filter caching and cache management tools
- Blocked-access page customizable with HTML
- Static URL whitelist and blacklist with import and export
- Import and export web filter exemptions list
- Enable monitor mode to test web filter policies before they are enforced
- Blocked domain testing tool to check if a site is still accessible
- Block all web access except that which is explicitly allowed (default deny) or allow all web access except for what is explicitly blocked (default allow)

Email Security

- Block malicious and spam emails before they reach users
- SMTP email filter with optional DyVax dynamic filtering
- Easy integration with Microsoft Exchange
- Multiple anti-virus and anti-spam engines used for filtering
- Sender IP addresses matched against real-time DNS blacklists

- Daily updates for spam and virus definitions
- Multiple, selectable spam DNS blacklists
- Configurable spam filter sensitivity
- Filter and bypass by geography, keyword
- Exempt admin-provided email addresses from filter
- Fully qualified domain name (FQDN) check
- SMTP rate limiter with auto-blacklisting (spammers who send to more than 10 non-existent users are automatically blacklisted for three days)
- Allowed recipient list
- Allowed outbound sender list (listed by IP address)
- Inbound sender whitelist, blacklist, and domain whitelist
- Email visibility and control with mail bagging, search, recovery, and forwarding
- Email filter bypass for SMTP
- Email quarantines for a safe enviromnment in which end-users can review suspicious messages and see all messages allowed, blocked, and deleted
- View spam score, country of origin, and content analysis for any email ("See Why" link)
- Automated quarantine alert emails

Virtual Private Networks (VPN)

CalyptixVPN

- Securely connects remote users to the office network via an encrypted tunnel
- Unlimited VPN clients allowed (no license limits)
- Simple VPN client generation
- Unique SSL certificate for each VPN client
- Auto-backup of VPN clients with easy restoration
- Support for iOS, Android, Windows, OS X, Linux, and Chrome OS
- Connections from VPN clients to AccessEnforcer encrypted using 2048-bit RSA
- Key exchange using unique 4096-bit Diffie-Hellman groups
- Data channel encrypted using AES256-GCM
- Encrypted TLS control channel authenticates using HMAC-SHA256
- VPN server uses OpenBSD pseudorandom number generator (PRNG) based on ChaCha20 cipher
- Login attempts page showing CalyptixVPN logins, lougouts, and timeouts, and the corresponding times and remote IP addresses
- Automated notification emails sent to users when a new client is available for download
- Microsoft AD integration for easy VPN client generation for AD users

IPsec VPN

- Securely connects a remote location to the network via an encrypted tunnel
- Unlimited VPN tunnels allowed (no license limits)
- Add and manage multiple IPsec policies
- IPsec wizard for simple policy generation
- Manual or automatic keying (IKE) options
- Security association lifetime configurable by admin
- Compatible with many IPsec-based VPN services

- Protocol options for Encapsulating Security Payload (tunnel mode) and Authentication Header (transport mode)
- Traffic encryption algorithms: AES 256, AES 192, AES 128, 3DES 168
- Traffic authentication algorithms: SHA512, SHA384, SHA256, SHA1, MD5
- Deffie-Hellman Group options: 1536-bit, 1024-bit, 768-bit, and none

Network Reports

- Automatically generate daily, weekly, and monthly reports of important network events
- Overview reports showing network alerts, IDS/IPS rule alerts, IP addresses creating alerts, allowed and blocked web traffic, email filter activity, and user activity
- Detailed reports showing web traffic for one to 150 targets specified by the administrator
- Target reports by IP address/CIDR range or Microsoft AD username
- Customize report design with logo and text
- Automatic report archiving
- Automatic emailing of reports
- Export as .pdf or .csv
- Microsoft AD integration enables reports with AD usernames instead of IP addresses

Automated Administration

- Daily virus and security updates
- Daily configuration backup
- Daily backup of CalyptixVPN clients
- Daily backup of SSL certificates for admin interface
- Daily checks for firmware updates
- Firmware updates applied automatically without downtime
- Daily checks for web filter category updates
- Daily, weekly, and monthly reports on traffic and security
- Hardware health and integrity checked every 10 minutes

[1] Model AE800-R is designed for small satellite networks up to 10 active users. It does not include spam filtering and is limited to two IPsec VPNs and two Calyptix VPNs. All other security features are included.

[2] SPS licensed separately. Ask for details.

Questions about AccessEnforcer features?

Contact us:

704.900.0422 | www.calyptix.com

calyptix® SECURITY