AccessEnforcer® Feature List

calyptix® SECURITY

Manage your small business network – simply & securely.

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]

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
- For failed logins into the GUI, SSH, and Calyptix VPN, automatic rate limited lockout of five minutes

Intrusion Detection & Prevention

- Detect and block malicious network traffic
- IDS/IPS engine powered by SNORT®
- Thousands of rules to detect and prevent network threats and undesirable traffic such as malware, ransomware, backdoors, exploits, botnet activity, adware, peer to peer, and much more
- Enable/disable rulesets and individual rules
- Additional rulesets available by entering an Oinkcode (available from Snort.org)
- Ruleset policies to prioritize connectivity, security, or balance both
- Notification of exposed RDP port forwarding rules
- Auto-enable new rule categories when downloaded
- Allow IDS/IPS engine to scan outbound connections
- Static CIDR whitelist and blacklist with import and export
- Define maximum limits to restrict services (such as guest wireless network)

Gatekeeper™

- Shield RDP, SSH, HTTPS, SFTP, VNC and other ports and systems from the public Internet
- Colored status check informs end user when desired host is reachable from AccessEnforcer®
- Provide zero trust secure authenticated access with 2FA and no client required with least privilege access
- No clunky VPN client eliminates your set up, patching and performance overhead
- Provide secure remote access to almost anything behind your AccessEnforcer® that has an HTTP HTTPS interface such as backup systems, NAS devices, webcams, switches, remote management systems, and more
- Eliminate exposure and dependency to third party hosted systems plagued by increasing vulnerabilities and breaches
- Identity management via Active Directory, LDAP systems or a local user directory
- Simple, secure and intuitive set up
- Enhance RDP user experience with configurable RDP options for connection speed, screen preferences, and more.
- Wizards to autodetect and activate highest TLS/ encryption settings for your AD server
- Implement Let's Encrypt™ SSL certificates (for free) with automatic renewal 30 days prior to expiry
- Integrate with leading identity providers that support LDAP, including JumpCloud

Geo Fence

- Allow or block traffic from selected countries
- Highly intuitive, interactive heat map for optimizing configuration
- Detailed alerts for monitoring, troubleshooting, and tightening the configuration
- Geographic database preinstalled by default
- Interactive logs
- Whitelist IP addresses from blocked countries
- Shrink your network attack surface
- Prevent persistent reconnaissance and probes
- Stop brute force and DOS attacks
- Stop zero day and pre-authentication attacks

Web Security

- HTTP & HTTPS web filter activation with one-click
- 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 filetype
- 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
- Web filter caching, cache management tools
- Blocked-access page customizable with HTML
- Static URL whitelist and blacklist web filter exemption list for devices and domains with import and export
- 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
- Access to curated external threat feeds from reputable external sources

Community Shield™

- Automated traffic correlation and protection from threat actors
- Threat information shared amidst all AccessEnforcer® units, blocking Internet threats and cyber attacks
- Identify and block destructive outbound connections, stopping the extraction of sensitive company information
- Nightly updates with the latest list of malicious and suspicious US and non-US based IP addresses
- Identification of failed login attempts in GUI, SSH and Gatekeeper logins
- Noise-reducing managed alerts, customizable for each customer
- Inclusion of curated external threat feeds from reputable external sources

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
- Supports automatic updates of Intel microcode firmware

Network Setup

- GUI-based console and point-and-click administration for fast deployment
- Supports Let's Encrypt certificates (free) for managed GUI, including automatic renewal 30 days prior to expiring
- Centralized notifications system to notify of informational and actionable messages on GUI

- VLAN for simple network management
- LAN LockdownTM for simple segmentation with optional pinhole exceptions
- Quality of service (QoS) for bandwidth management
- Multi-WAN with load balancing and failover
- Integration with Microsoft Active Directory(AD)
- Port forwarding rules with single click and drag-and-drop rule management, ICMP forwarding rules, and access control rules for source IP address/CIDR ranges
- Static and dynamic DNS settings
- SIP proxy server integration
- DHCP server with configurable ranges and one-click reservations for every LAN/VLAN
- Multiple network interface cards (NICs), which are physically separate for easy, secure segmentation and switching between LAN and WAN modes
- IP aliasing
- MAC address cloning
- PPPoE support (DSL)
- Automatically saved configuration files for rapid deployment of additional or replacement AccessEnforcer® devices

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, .csv, .xlsx
- Microsoft AD integration enables reports with AD usernames instead of IP addresses

Network Management

- Troubleshooter that tests 70+ network settings and services with one click
- WAN Activity Log tracks Internet outages and restoration
- System Status dashboard showing network statistics, enabled security settings, WAN/LAN status, system health, and charts of network traffic allowed and blocked
- Live Connections overview showing top users by bandwidth or connection count. Full dashboard shows all local hosts with corresponding bandwidth use, source, and destination. Click to terminate any or all connections
- Network Alerts dashboard showing the alert type, action taken, IP addresses, 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 top website visited and top web users by number of sites visited and bandwidth consumed
- Rejected Spam dashboard showing SMTP connections refused due to invalid sender or recipient, or failure to reverse-resolve to valid FQDN
- Login Attempts log showing failed and successful attempts, 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
- 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
- Access to curated external threat feeds from reputable external sources

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

Virtual Private Networks (VPN)

CalyptixVPN

- Securely connects remote users to the office network via an encrypted tunnel
- Unlimited VPN clients allowed (no license limits) 1
- 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
- KARL security feature generating randomized unique OpenBSD kernel on each boot
- Login attempts page showing CalyptixVPN logins, logouts, and timeouts, and the corresponding times and remote IP addresses (exportable via CSV)
- 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) 1
- Add and manage multiple IPsec policies
- Manual or automatic keying (IKE) options
- Security association lifetime configurable by admin
- Protocol options for Encapsulating Security Payload (tunnel mode) and Authentication Header (transport mode)
- Traffic encryption algorithms: AES-GCM, AES-CTR, AES 256, AES 192, AES 128, 3DES 168
- Traffic authentication algorithms: SHA512, SHA384, SHA256, SHA1, MD5
- Diffie-Hellman Group options: 8192-bit, 6144-bit, 4096-bit, 3072-bit, 2048-bit, 1536-bit, 1024-bit, 768 bit, Brainpool and X25519, as well as Elliptic Curve Groups

Email Security

- Block malicious and spam emails before they reach users
- SMTP email filter with optional DyVax dynamic filtering and custom spam-score thresholds
- Easy integration with Microsoft Exchange
- Multiple anti-virus and anti-spam engines used for filtering
- Sender IP addresses matched against realtime 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 nonexistent 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 environment 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

Quality of Service (QoS)

- Traffic prioritization on a scale of 0-7 to ensure most important traffic processed 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)
- 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)

Have questions about AccessEnforcer® features?

Get in touch to learn more about what AccessEnforcer® can do for your business.

800.650.8930
info@calyptix.com

calyptix® SECURITY