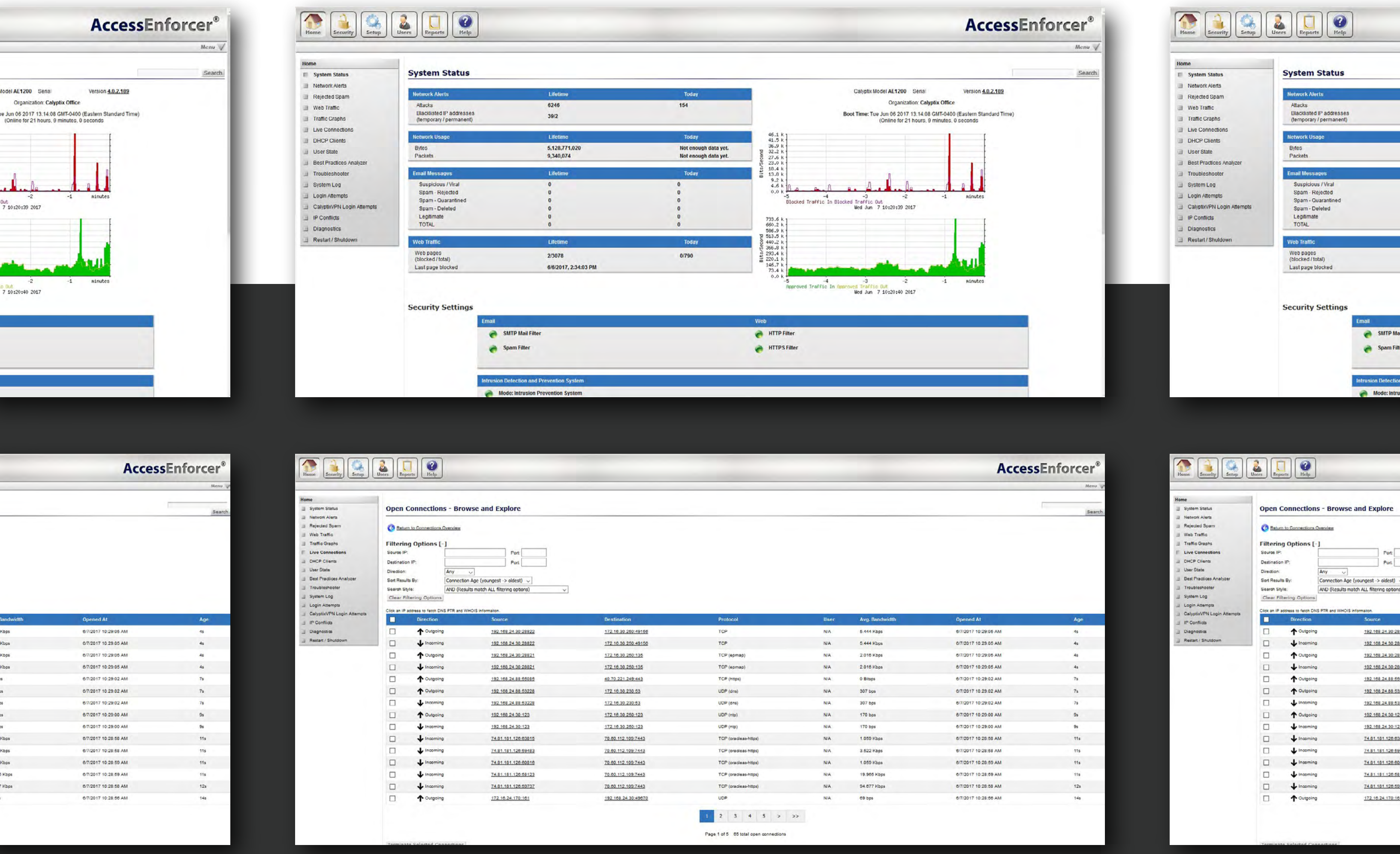
# AccessEnforcer Version 4.0

# *New Features and Improvements*



Home

- System Status
- Network Alerts
- Rejected Spam
- Web Traffic
- Traffic Graphs
- Live Connections
- DHCP Clients
- User State
- Best Practices Analyzer
- Troubleshooter
- System Log
- Login Attempts
- CalyptixVPN Login Attempts
- IP Conflicts
- Diagnostics
- Restart / Shutdown

**System Status**

| Network Alerts | Lifetime | Today |
|---|---|---|
| Attacks | 6246 | 154 |
| Blacklisted IP addresses (temporary / permanent) | 39/2 | |

| Network Usage | Lifetime | Today |
|---|---|---|
| Bytes | 5,128,771,020 | Not enough data yet. |
| Packets | 9,340,074 | Not enough data yet. |

| Email Messages | Lifetime | Today |
|---|---|---|
| Suspicious / Viral | 0 | 0 |
| Spam - Rejected | 0 | 0 |
| Spam - Quarantined | 0 | 0 |
| Spam - Deleted | 0 | 0 |
| Legitimate | 0 | 0 |
| TOTAL | 0 | 0 |

| Web Traffic | Lifetime | Today |
|---|---|---|
| Web pages (blocked / total) | 2/3078 | 0/790 |
| Last page blocked | 6/6/2017, 2:34:03 PM | |

Calyptix Model AE1200 Serial Version 4.0.2.189

Organization: Calyptix Office

Boot Time: Tue Jun 06 2017 13:14:08 GMT-0400 (Eastern Standard Time)
(Online for 21 hours, 9 minutes, 0 seconds

**Security Settings**

| Email | Web |
|---|---|
| ● SMTP Mail Filter | ● HTTP Filter |
| ● Spam Filter | ● HTTPS Filter |

Intrusion Detection and Prevention System

● Mode: Intrusion Prevention System

**Open Connections - Browse and Explore**

Return to Connections Overview

**Filtering Options [-]**

Source IP: ____ Port: ____
Destination IP: ____ Port: ____
Direction: Any
Sort Results By: Connection Age (youngest -> oldest)
Search Style: AND (Results match ALL filtering options)
Clear Filtering Options

Click an IP address to fetch DNS PTR and WHOIS information.

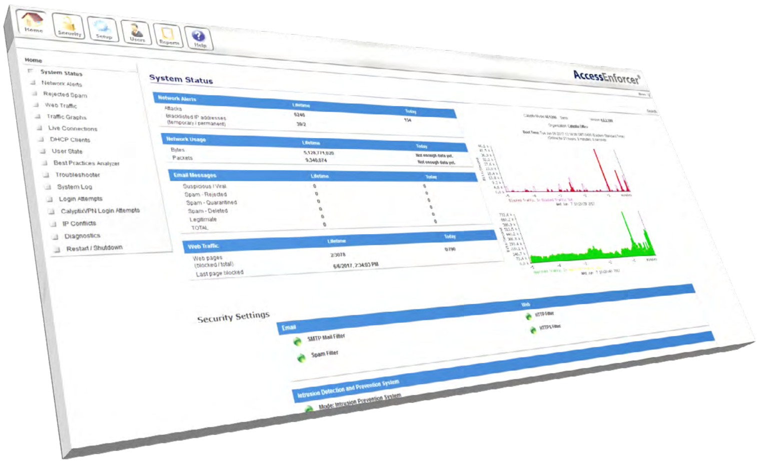
| □ | Direction | Source | Destination | Protocol | User | Avg. Bandwidth | Opened At | Age |
|---|---|---|---|---|---|---|---|---|
| □ | ↑ Outgoing | 192.168.24.30:28822 | 172.16.30.250:49156 | TCP | N/A | 5.444 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↓ Incoming | 192.168.24.30:28822 | 172.16.30.250:49156 | TCP | N/A | 5.444 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↑ Outgoing | 192.168.24.30:28821 | 172.16.30.250:135 | TCP (epmap) | N/A | 2.016 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↓ Incoming | 192.168.24.30:28821 | 172.16.30.250:135 | TCP (epmap) | N/A | 2.016 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↑ Outgoing | 192.168.24.88:55085 | 40.70.221.249:443 | TCP (https) | N/A | 0 Bitsps | 6/7/2017 10:29:02 AM | 7s |
| □ | ↑ Outgoing | 192.168.24.88:53228 | 172.16.30.230:53 | UDP (dns) | N/A | 307 bps | 6/7/2017 10:29:02 AM | 7s |
| □ | ↓ Incoming | 192.168.24.88:53228 | 172.16.30.230:53 | UDP (dns) | N/A | 307 bps | 6/7/2017 10:29:02 AM | 7s |
| □ | ↑ Outgoing | 192.168.24.30:123 | 172.16.30.250:123 | UDP (ntp) | N/A | 170 bps | 6/7/2017 10:29:00 AM | 9s |
| □ | ↓ Incoming | 192.168.24.30:123 | 172.16.30.250:123 | UDP (ntp) | N/A | 170 bps | 6/7/2017 10:29:00 AM | 9s |
| □ | ↓ Incoming | 74.81.181.126:63815 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 1.059 Kbps | 6/7/2017 10:28:58 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:59483 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 3.622 Kbps | 6/7/2017 10:28:58 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:60816 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 1.059 Kbps | 6/7/2017 10:28:59 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:58123 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 19.965 Kbps | 6/7/2017 10:28:59 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:59737 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 94.677 Kbps | 6/7/2017 10:28:58 AM | 12s |
| □ | ↑ Outgoing | 172.16.24.170:161 | 192.168.24.30:49670 | UDP | N/A | 69 bps | 6/7/2017 10:28:56 AM | 14s |

Page 1 of 5 65 total open connections

Terminate Selected Connections

# New Features and Improvements

## // AccessEnforcer Version 4.0



System Status

| Network Alerts | Lifetime | Today |
|---|---|---|
| Attacks | 6246 | 154 |
| Blacklisted IP addresses (temporary / permanent) | 39/2 | |

| Network Usage | Lifetime | Today |
|---|---|---|
| Bytes | 5,128,771,020 | Not enough data yet. |
| Packets | 9,340,074 | Not enough data yet. |

| Email Messages | Lifetime | Today |
|---|---|---|
| Suspicious / Viral | 0 | 0 |
| Spam - Rejected | 0 | 0 |
| Spam - Quarantined | 0 | 0 |
| Spam - Deleted | 0 | 0 |
| Legitimate | 0 | 0 |
| TOTAL | 0 | 0 |

| Web Traffic | Lifetime | Today |
|---|---|---|
| Web pages (blocked / total) | 2/3078 | 0/790 |
| Last page blocked | 6/6/2017, 2:34:03 PM | |

Security Settings

Email
- SMTP Mail Filter
- Spam Filter

Web
- HTTP Filter
- HTTPS Filter

Intrusion Detection and Prevention System
- Mode: Intrusion Prevention System

AccessEnforcer 4.0 is here. The most significant update to the UTM Firewall in nearly a decade, it brings vast improvements in speed, simplicity, and security for Calyptix reseller partners and their clients.

New features are combined with a clean and simple layout for easy configuration. Look for blue header rows used throughout the interface to indicate a device is running AccessEnforcer version 4.0 firmware.

The number of improvements could fill a small book, so please allow us to share the highlights in this document.

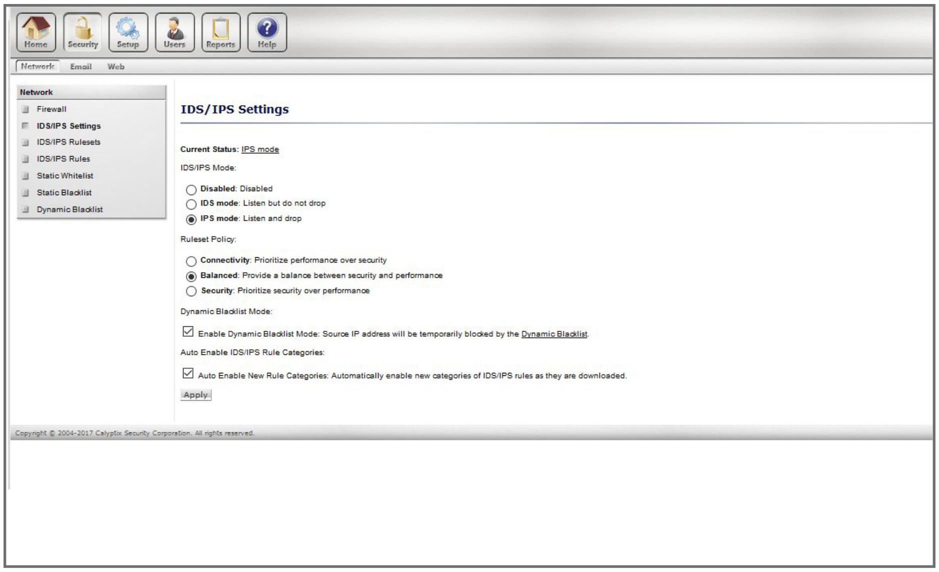
*Note:* the features marked "All New" have been redesigned and recoded from scratch.

calyptix® SECURITY

# Table of Contents

# Intrusion Prevention (IDS/IPS)

## // ALL NEW



**IDS/IPS Settings**

**Current Status:** IPS mode

IDS/IPS Mode:

○ **Disabled**: Disabled<br>
○ **IDS mode**: Listen but do not drop<br>
● **IPS mode**: Listen and drop

Ruleset Policy:

○ **Connectivity**: Prioritize performance over security<br>
● **Balanced**: Provide a balance between security and performance<br>
○ **Security**: Prioritize security over performance

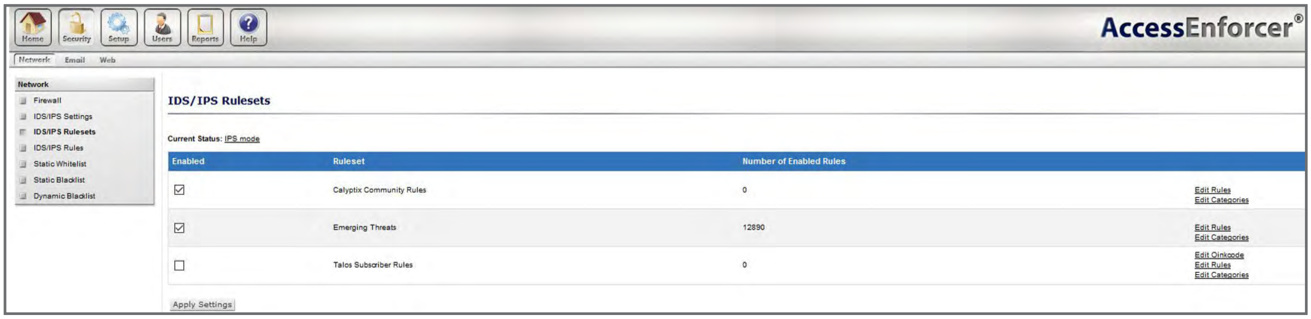
Dynamic Blacklist Mode:

☑ Enable Dynamic Blacklist Mode: Source IP address will be temporarily blocked by the Dynamic Blacklist.

Auto Enable IDS/IPS Rule Categories:

☑ Auto Enable New Rule Categories: Automatically enable new categories of IDS/IPS rules as they are downloaded.

Copyright © 2004-2017 Calyptix Security Corporation. All rights reserved.



**IDS/IPS Rulesets**

**Current Status:** IPS mode

| Enabled | Ruleset | Number of Enabled Rules | |
|---|---|---|---|
| ☑ | Calyptix Community Rules | 0 | Edit Rules<br>Edit Categories |
| ☑ | Emerging Threats | 12890 | Edit Rules<br>Edit Categories |
| □ | Talos Subscriber Rules | 0 | Edit Oinkcode<br>Edit Rules<br>Edit Categories |

The Intrusion Detection and Prevention engine has been completely rewritten with many new features:

### Stronger security

- Thousands of new IDS/IPS rules to detect and block threats such as malware, backdoors, exploits, server attacks, and more

### Flexible controls

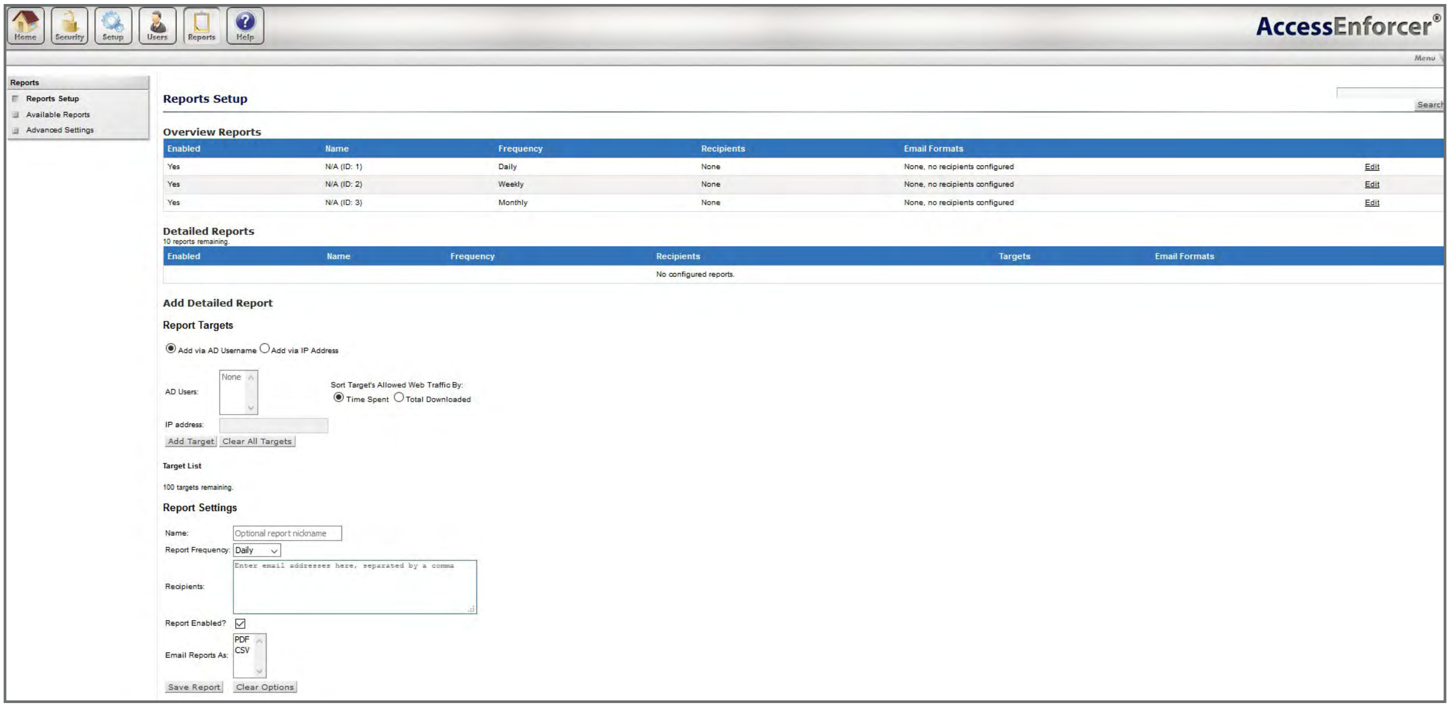
- Choose from multiple rulesets, including Calyptix Community Rules and Emerging Threats
- Enter a Talos Subscriber Oinkcode to apply the latest Snort rules to the system (sign up for a free subscription to Snort rules at snort.org)
- Within rulesets, activate and deactivate categories and individual rules for granular control over the system's security and performance
- Choose from one of three Rule Policies – Connectivity, Security, or Balanced – to automatically tailor the active rules to the administrator's priority

### Faster performance

- Revamped back end provides greater efficiency in how the IDS/IPS engine processes traffic and enforces rules

# Reporting

## // ALL NEW



**Reports Setup**

**Overview Reports**

| Enabled | Name | Frequency | Recipients | Email Formats | |
|---|---|---|---|---|---|
| Yes | N/A (ID: 1) | Daily | None | None, no recipients configured | Edit |
| Yes | N/A (ID: 2) | Weekly | None | None, no recipients configured | Edit |
| Yes | N/A (ID: 3) | Monthly | None | None, no recipients configured | Edit |

**Detailed Reports**

10 reports remaining.

| Enabled | Name | Frequency | Recipients | Targets | Email Formats |
|---|---|---|---|---|---|
| | | | No configured reports. | | |

**Add Detailed Report**

**Report Targets**

● Add via AD Username ○ Add via IP Address

AD Users: None

Sort Target's Allowed Web Traffic By:
● Time Spent ○ Total Downloaded

IP address:

Add Target | Clear All Targets

**Target List**

100 targets remaining.

**Report Settings**

Name: Optional report nickname
Report Frequency: Daily
Recipients: Enter email addresses here, separated by a comma
Report Enabled? ☑
Email Reports As: PDF CSV

Save Report | Clear Options

The reporting service is redesigned and recoded from scratch. New and improved features include:

### Faster performance

- Faster page load times
- Greater storage efficiency
- Seamless report dispatching
- Simple report handling
- Simplified layout for clean and clear analysis
- Downloadable as .pdf or .csv
- Customize with logo and "prepared by" text automatically
- Archive reports automatically

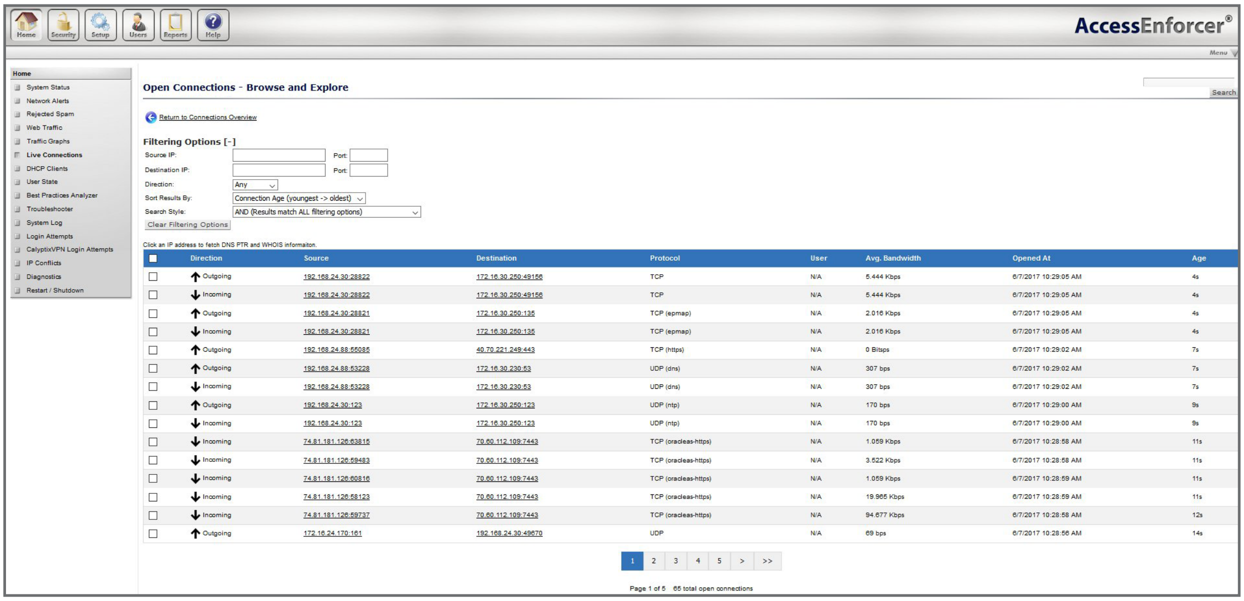
### New report types

*Overview Report* – reviews network alerts, IDS/IPS rule alerts, IP addresses creating alerts, allowed and blocked web traffic, email filter activity, and user activity

*Detailed Report* – reviews web traffic for one to 150 targets specified by the administrator. Targets can be entered by IP address, IP range, or Active Directory username

# Live Connections

## // ALL NEW



Open Connections - Browse and Explore

Filtering Options [-]

Source IP: Port:
Destination IP: Port:
Direction: Any
Sort Results By: Connection Age (youngest -> oldest)
Search Style: AND (Results match ALL filtering options)

Click an IP address to fetch DNS PTR and WHOIS informaiton.

| □ | Direction | Source | Destination | Protocol | User | Avg. Bandwidth | Opened At | Age |
|---|---|---|---|---|---|---|---|---|
| □ | ↑ Outgoing | 192.168.24.30:28822 | 172.16.30.250:49156 | TCP | N/A | 5.444 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↓ Incoming | 192.168.24.30:28822 | 172.16.30.250:49156 | TCP | N/A | 5.444 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↑ Outgoing | 192.168.24.30:28821 | 172.16.30.250:135 | TCP (epmap) | N/A | 2.016 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↓ Incoming | 192.168.24.30:28821 | 172.16.30.250:135 | TCP (epmap) | N/A | 2.016 Kbps | 6/7/2017 10:29:05 AM | 4s |
| □ | ↑ Outgoing | 192.168.24.88:55085 | 40.70.221.249:443 | TCP (https) | N/A | 0 Bitsps | 6/7/2017 10:29:02 AM | 7s |
| □ | ↑ Outgoing | 192.168.24.88:53228 | 172.16.30.230:53 | UDP (dns) | N/A | 307 bps | 6/7/2017 10:29:02 AM | 7s |
| □ | ↓ Incoming | 192.168.24.88:53228 | 172.16.30.230:53 | UDP (dns) | N/A | 307 bps | 6/7/2017 10:29:02 AM | 7s |
| □ | ↑ Outgoing | 192.168.24.30:123 | 172.16.30.250:123 | UDP (ntp) | N/A | 170 bps | 6/7/2017 10:29:00 AM | 9s |
| □ | ↓ Incoming | 192.168.24.30:123 | 172.16.30.250:123 | UDP (ntp) | N/A | 170 bps | 6/7/2017 10:29:00 AM | 9s |
| □ | ↓ Incoming | 74.81.181.126:63815 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 1.059 Kbps | 6/7/2017 10:28:58 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:59483 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 3.522 Kbps | 6/7/2017 10:28:58 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:60816 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 1.059 Kbps | 6/7/2017 10:28:59 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:58123 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 19.965 Kbps | 6/7/2017 10:28:59 AM | 11s |
| □ | ↓ Incoming | 74.81.181.126:59737 | 70.60.112.109:7443 | TCP (oracleas-https) | N/A | 94.677 Kbps | 6/7/2017 10:28:58 AM | 12s |
| □ | ↑ Outgoing | 172.16.24.170:161 | 192.168.24.30:49670 | UDP | N/A | 69 bps | 6/7/2017 10:28:56 AM | 14s |

Page 1 of 5 65 total open connections

The Live Connections service is also redesigned and recoded from scratch. In addition to a simplified layout, here are more improvements:

### Enhanced performance

- Page load time roughly 10-times faster

### Simple analysis

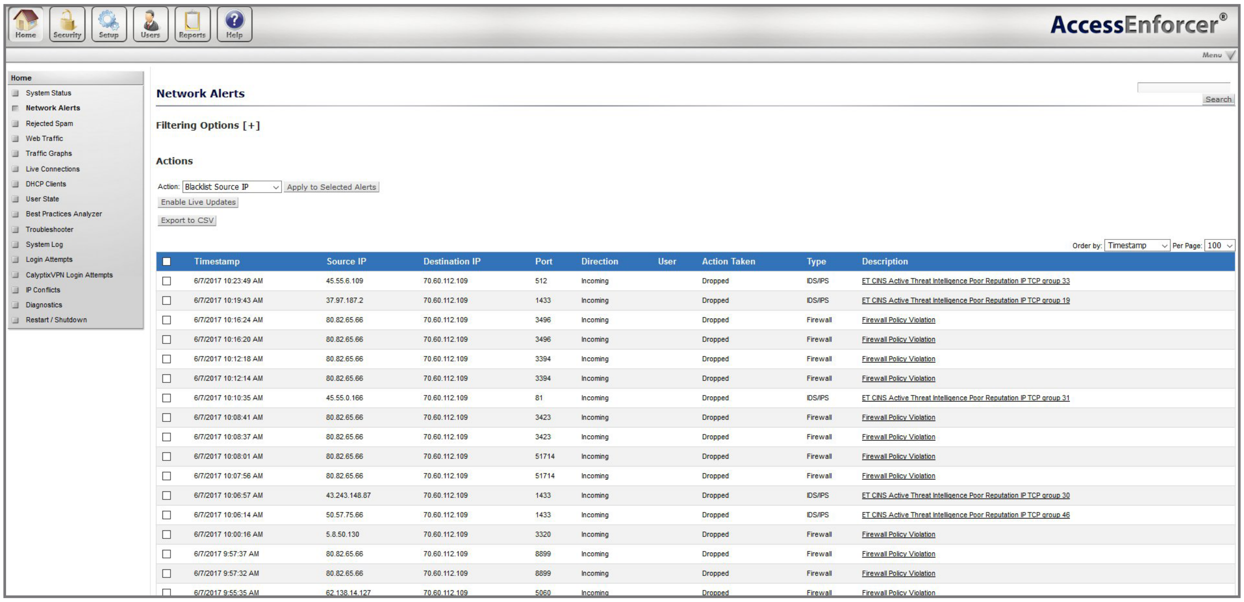
- Quickly view the top 50 bandwidth users and the top 50 users of open connections
- Search and sort the connections table for fast and granular review

### Dive into data

- Click an IP address to view its current connections
- Sort and filter the connections table
- Terminate selected connections
- View Whois and DNS information by clicking any IP

# Network Alerts

## // ALL NEW



Network Alerts

Filtering Options [+]

Actions

Action: Blacklist Source IP

Order by: Timestamp  Per Page: 100

| ☐ | Timestamp | Source IP | Destination IP | Port | Direction | User | Action Taken | Type | Description |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | 6/7/2017 10:23:49 AM | 45.55.6.109 | 70.60.112.109 | 512 | Incoming | | Dropped | IDS/IPS | ET CINS Active Threat Intelligence Poor Reputation IP TCP group 33 |
| ☐ | 6/7/2017 10:19:43 AM | 37.97.187.2 | 70.60.112.109 | 1433 | Incoming | | Dropped | IDS/IPS | ET CINS Active Threat Intelligence Poor Reputation IP TCP group 19 |
| ☐ | 6/7/2017 10:16:24 AM | 80.82.65.66 | 70.60.112.109 | 3496 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:16:20 AM | 80.82.65.66 | 70.60.112.109 | 3496 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:12:18 AM | 80.82.65.66 | 70.60.112.109 | 3394 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:12:14 AM | 80.82.65.66 | 70.60.112.109 | 3394 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:10:35 AM | 45.55.0.166 | 70.60.112.109 | 81 | Incoming | | Dropped | IDS/IPS | ET CINS Active Threat Intelligence Poor Reputation IP TCP group 31 |
| ☐ | 6/7/2017 10:08:41 AM | 80.82.65.66 | 70.60.112.109 | 3423 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:08:37 AM | 80.82.65.66 | 70.60.112.109 | 3423 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:08:01 AM | 80.82.65.66 | 70.60.112.109 | 51714 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:07:56 AM | 80.82.65.66 | 70.60.112.109 | 51714 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 10:06:57 AM | 43.243.148.87 | 70.60.112.109 | 1433 | Incoming | | Dropped | IDS/IPS | ET CINS Active Threat Intelligence Poor Reputation IP TCP group 30 |
| ☐ | 6/7/2017 10:06:14 AM | 50.57.75.66 | 70.60.112.109 | 1433 | Incoming | | Dropped | IDS/IPS | ET CINS Active Threat Intelligence Poor Reputation IP TCP group 46 |
| ☐ | 6/7/2017 10:00:16 AM | 5.8.50.130 | 70.60.112.109 | 3320 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 9:57:37 AM | 80.82.65.66 | 70.60.112.109 | 8899 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 9:57:32 AM | 80.82.65.66 | 70.60.112.109 | 8899 | Incoming | | Dropped | Firewall | Firewall Policy Violation |
| ☐ | 6/7/2017 9:55:35 AM | 62.138.14.127 | 70.60.112.109 | 5060 | Incoming | | Dropped | Firewall | Firewall Policy Violation |

Also redesigned and recoded from scratch, Network Alerts has many new features:

### Enhanced performance

- Page load time roughly 10-times faster

### Apply bulk actions

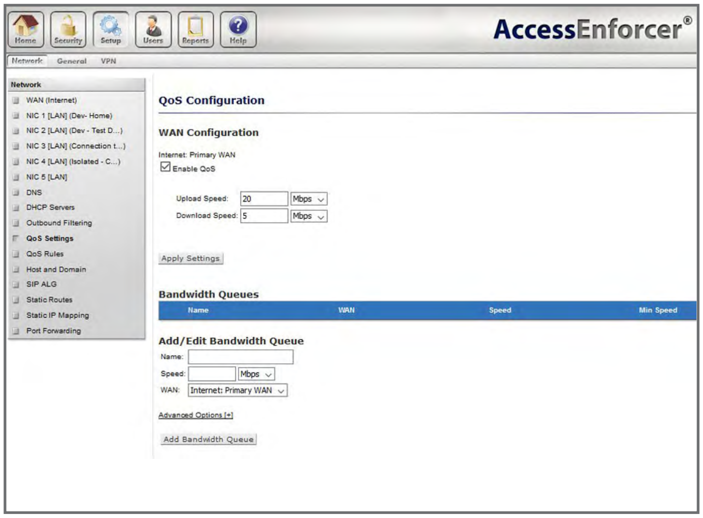
- Select one or more alerts and click to blacklist or whitelist the source, blacklist or whitelist the destination, or disable the corresponding IDS/IPS rule

### Quickly and easily review alerts

- Sort by timestamp, source, destination, user, or another factor
- Filter by address, port number, or string
- Monitor new alerts as they are recorded by enabling live updates

# Quality of Service (QoS)

## // ALL NEW



**QoS Configuration**

**WAN Configuration**

Internet: Primary WAN
☑ Enable QoS

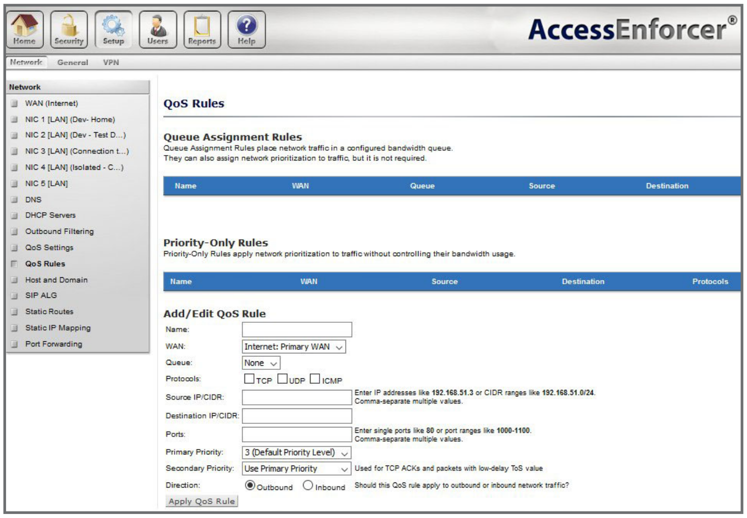
Upload Speed: 20 Mbps
Download Speed: 5 Mbps

**Bandwidth Queues**

| Name | WAN | Speed | Min Speed |
|---|---|---|---|

**Add/Edit Bandwidth Queue**

Name:
Speed: Mbps
WAN: Internet: Primary WAN



**QoS Rules**

**Queue Assignment Rules**

Queue Assignment Rules place network traffic in a configured bandwidth queue.
They can also assign network prioritization to traffic, but it is not required.

| Name | WAN | Queue | Source | Destination |
|---|---|---|---|---|

**Priority-Only Rules**

Priority-Only Rules apply network prioritization to traffic without controlling their bandwidth usage.

| Name | WAN | Source | Destination | Protocols |
|---|---|---|---|---|

**Add/Edit QoS Rule**

Name:
WAN: Internet: Primary WAN
Queue: None
Protocols: □ TCP □ UDP □ ICMP
Source IP/CIDR: Enter IP addresses like **192.168.51.3** or CIDR ranges like **192.168.51.0/24**. Comma-separate multiple values.
Destination IP/CIDR:
Ports: Enter single ports like **80** or port ranges like **1000-1100**. Comma-separate multiple values.
Primary Priority: 3 (Default Priority Level)
Secondary Priority: Use Primary Priority Used for TCP ACKs and packets with low-delay ToS value
Direction: ● Outbound ○ Inbound Should this QoS rule apply to outbound or inbound network traffic?

The QoS service (or "bandwidth management") is also completely rewritten. The service is simpler, more efficient, and has new features:

### Prioritize traffic

- Group traffic into bandwidth queues and prioritize them on a scale of 0-7 to ensure the most important traffic is processed first
- Assign traffic by protocol, IP address, ports, and/or port ranges

### Burst options

- Allow a bandwidth queue to expand during times of high traffic
- Set a burst length, after which the burst will expire and return to normal size

### Bandwidth limits

- Set upload and download bandwidth for any queue
- Set minimum and maximum limits on any bandwidth queue

### New algorithm

- Now using the Hierarchical Fair Service Curves (HFSC) algorithm, which is a significant improvement over the previous Alternate Queueing (ALTQ) system

# Multi-WAN

## // ALL NEW

The Multi-WAN and LAN/WAN management systems have been completely rewritten for improved efficiency and stability. New and improved features include:

### Easier configuration

- Configure any WAN interface without reinitializing all other WAN interfaces or restarting the device
- Add or delete outbound filtering rules without reinitializing WAN interfaces
- Change DNS settings without restarting the device

### More compatible

- Greater stability when operating alongside other AccessEnforcer features, including IDS/IPS and HTTPS Web Filtering
- DHCP client works with more DHCP servers

### More reliable

- Improved detection and faster reaction to WAN status changes
- Improved load balancing, especially when more than two WANs are specified
- Greater stability for WAN failover

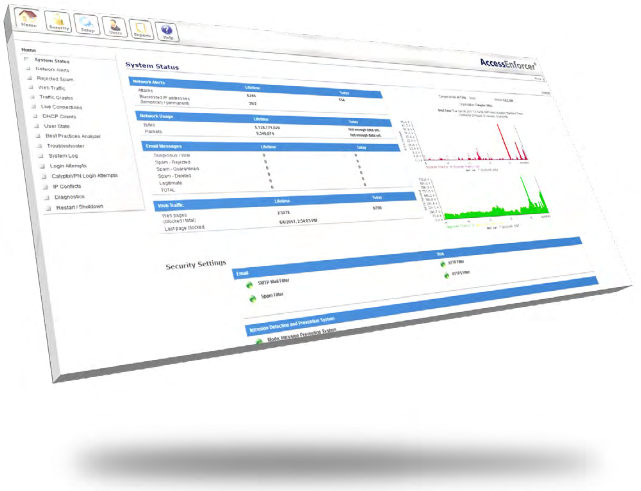
# HTTP/HTTPS Web Filter

## // ALL NEW

The backend of the Web Filter has been completely revamped for better security, reliability, efficiency, logging, and integration with the new reporting system.

### More compatible

- Web filtering now works on most websites, including join.me, logmein.com, bankofamerica.com, aws.amazon.com, and office365.com
- Handles HTTP/1.1 connections



System Status

| Network Alerts | Lifetime | Today |
|---|---|---|
| Attacks | 6246 | 154 |
| Blacklisted IP addresses (temporary / permanent) | 39/2 | |

| Network Usage | Lifetime | Today |
|---|---|---|
| Bytes | 5,128,771,020 | Not enough data yet. |
| Packets | 9,340,074 | Not enough data yet. |

| Email Messages | Lifetime | Today |
|---|---|---|
| Suspicious / Viral | 0 | 0 |
| Spam - Rejected | 0 | 0 |
| Spam - Quarantined | 0 | 0 |
| Spam - Deleted | 0 | 0 |
| Legitimate | 0 | 0 |
| TOTAL | 0 | 0 |

| Web Traffic | Lifetime | Today |
|---|---|---|
| Web pages (blocked / total) | 2/3078 | 0/790 |
| Last page blocked | 6/6/2017, 2:34:03 PM | |

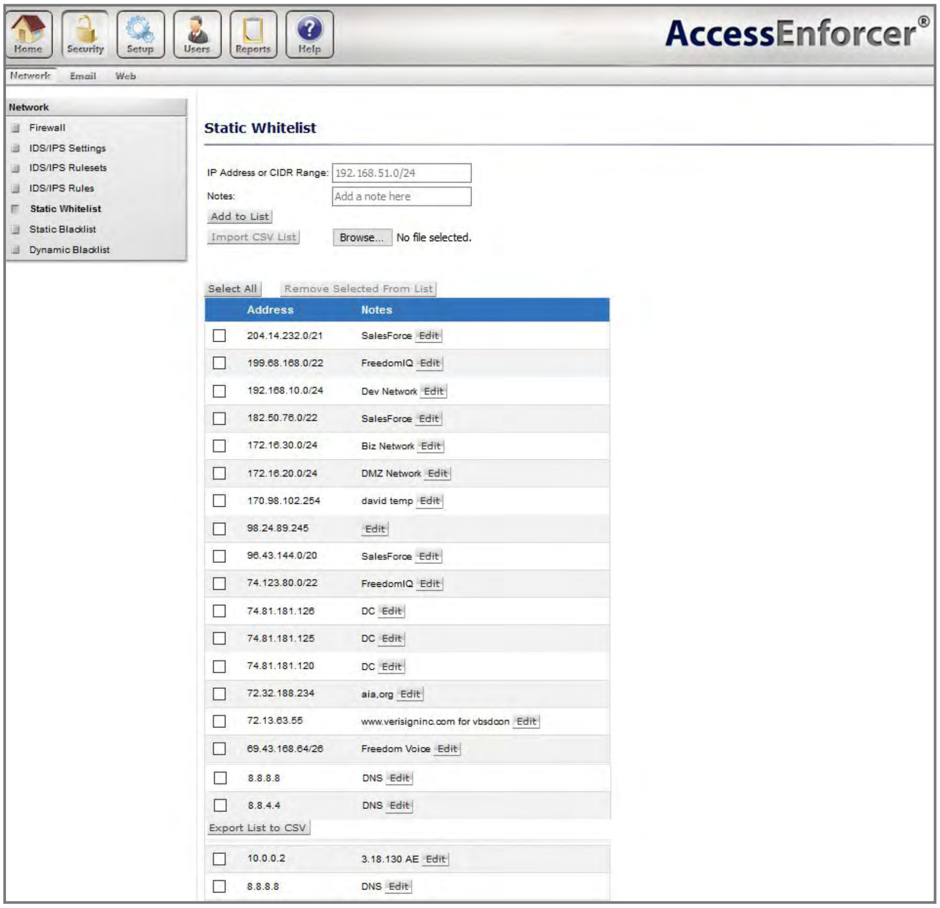
Security Settings

Email
SMTP Mail Filter
Spam Filter

Web
HTTP Filter
HTTPS Filter

Intrusion Detection and Prevention System
Mode: Intrusion Prevention System

# *Static Whitelist, Static Blacklist, & Dynamic Blacklist*



Static Whitelist

IP Address or CIDR Range: 192.168.51.0/24

Notes: Add a note here

No file selected.

| | Address | Notes |
|---|---|---|
| □ | 204.14.232.0/21 | SalesForce Edit |
| □ | 199.68.168.0/22 | FreedomIQ Edit |
| □ | 192.168.10.0/24 | Dev Network Edit |
| □ | 182.50.76.0/22 | SalesForce Edit |
| □ | 172.16.30.0/24 | Biz Network Edit |
| □ | 172.16.20.0/24 | DMZ Network Edit |
| □ | 170.98.102.254 | david temp Edit |
| □ | 98.24.89.245 | Edit |
| □ | 96.43.144.0/20 | SalesForce Edit |
| □ | 74.123.80.0/22 | FreedomIQ Edit |
| □ | 74.81.181.126 | DC Edit |
| □ | 74.81.181.125 | DC Edit |
| □ | 74.81.181.120 | DC Edit |
| □ | 72.32.188.234 | aia,org Edit |
| □ | 72.13.63.55 | www.verisigninc.com for vbsdcon Edit |
| □ | 69.43.168.64/26 | Freedom Voice Edit |
| □ | 8.8.8.8 | DNS Edit |
| □ | 8.8.4.4 | DNS Edit |

| | | |
|---|---|---|
| □ | 10.0.0.2 | 3.18.130 AE Edit |
| □ | 8.8.8.8 | DNS Edit |

New features added to the whitelist and blacklists will help administrators save time:

### Bulk imports

- Import .csv files to quickly add thousands of hosts to a list
- Export entries for easy back up and sharing

### Add notes

- Apply comments (such as “Bob’s VoIP” or “DMZ Network”) to any entry for easy reference

### Filter and search

- Type any string to quickly filter the table of entries

# *see for yourself.*

Contact us to see the new features in AccessEnforcer Version 4.0. You will get a live demo with a Cayptix representative who will walk you through the interface and answer any questions you have.

See how AccessEnforcer will help your IT business secure networks and save time.

**Contact us today:** sales@calyptix.com