xDefenders, inc.
1100 Pittsford-Palmyra Rd
Pittsford, NY 14534
585-385-2770
jthon@xdefenders.com
www.xdefenders.com

Defender*Wall*… *Managed Security Appliances*

Today, your business needs more than a network firewall. It needs **"Defense-In-Depth"** at the perimeter, the DMZ, the LAN and at the Host levels. This includes *"application-layer"* firewalls and filters and tools, because attacks have become more sophisticated and frequent.

Defender*Wall*™ Advantages:

- Network **and** Application-Level Protection
- Personalized, Professional Support
- Managed Services 24x7
- Best Value

The Defender*Wall*™ delivers network and application-layer, Intrusion Prevention (IPS) and Intrusion Detection (IPS) services on a hardened Linux-HP server. It is an Internet security appliance that integrates essential functions into a well-managed security solution.

Defender*Wall*™ Applications:

1. *App*Defender - Reverse Proxy - Web Server & DMZ Protection
2. *Mail*Defender® - Spam and Virus Filter
3. *Net*Defender IDS – Intrusion Detection System, Malware Detection, ARP watch
4. *Sys*Defender - Vulnerability Testing & Management
5. *Web*Defender - Forward Proxy - Web Content Filter, User Reporting

These Linux-based services are integrated into a security-hardened, high-performance, scalable HP appliance. For larger organizations, multiple appliances can be installed for distributed security services, supporting thousands of users.

xDefenders acts as your Security System Administrator and becomes a member of your Incident Response Team. We remotely manage and monitor the Defender*Wall*™ for you. Critical databases are automatically updated and timely software patches are applied. We perform daily and weekly remote backups and include hardware maintenance coverage.

As an option, **24x7 Management and Monitoring** is available to monitor for real-time intrusions and attacks. Our 24x7 Security Operations Center (SOC) is professionally staffed, around the clock, to support immediate escalation procedures, according to your Plan.

Sizing and Hardware Platforms

Small, medium and large rack-mount appliances are available to support a few users (small) to thousands of users (multiple large appliances). These **HP server-based** appliances can scale have up to multiple CPU, 8 GB memory, CD, multiple NIC's and multiple large disks. Multiple security software applications can reside on a single appliance, for example; a MailDefender with IDS. **Thousands of users** can be supported by dedicating multiple appliances to specific security applications. This creates a smart *"Defense-in-Depth"* security architecture. Contact the xDefenders Engineering Department at esupport@xdefenders.com to confirm your needs.

DefenderWall Managed Services

- Design, Deploy, Manage, Monitor, Maintain Services.
- Hardware, software support and installation assistance is included.
- Pre-Installation configurations are provided and delivered to the client.
- Automatic updates of critical knowledge databases and software updates.
- Daily and Weekly remote backups
- Next-day Hardware Replacement or HP Maintenance Contract
- Phone or on-site support is available Monday thru Friday from 8:30 am-7 pm EST.
- Firewall and IDS Managed Services is available 24x7x365.
- Custom support and fine-tuning is available from xDefenders.

Network and Security Operations Centers

- 24x7x365 staffed by CISSP professionals
- Data Center Quality, SAS 70 certified
- Network, Security and Systems Management and Monitoring
- Escalation Planning, Incident Response
- *"Bacon"* (correlation engine) escalates security alerts and alarms

Professional Security Services

- Network, Wireless, Web Application and Database Vulnerability Assessments
- Security Audits, Social Engineering, Gap Analysis,
- Security Policy Development, Employee Awareness Training
- Business Continuity Plans (BCP), Forensics

Company Background

Since 2003, xDefenders have focused exclusively on the deliver of Information Security Solutions. Our CISSP's have "Enterprise-Class" experience with firewalls, networking, web application development and Industry Security Standards. xDefenders is headquartered in Rochester, NY, with a large client base throughout most of the US. A Synergy Global Solutions Company.

Call (585) 385-2770 or email jthon@xdefenders.com or visit www.xdefenders.com

*App*Defender …*protecting your DMZ and web applications*

Business Problem:

Companies that deploy web-based applications and accept client information over the Internet are vulnerable to many exploits. Client-based (browser) software can't be trusted. Anyone can change data that is received from the web application and send back a command that could cause the application to misbehave or worse, open up the machine on system to more devious attacks.

The very nature of web applications – their ability to collate, process, and disseminate information over the Internet, exposes them in at least two ways. First, **they have total exposure by nature of being Internet accessible**. This makes security through obscurity impossible and heightens the requirement for hardened code. Second, and most critically from a penetration testing perspective, they process data elements from within HTTP requests – a protocol that can employ a myriad of encoding and encapsulation techniques – or **Vulnerabilities!**

Most web application environments including ASP and PHP, expose data elements to the developer in a manner that fails to identify how they were captured and hence what kind of validation and sanity checking should apply to them. Because the web "environment" is so diverse, and contains so many forms of programmatic content, input validation and sanity checking is the key to web applications security. This involves both identifying and enforcing the valid domain of every user-definable data element, as well as a sufficient understanding of the source of all data elements to determine what is potentially user definable.

Application security is a constant struggle to maintain balance between functional requirements and business drivers, deadlines, and limited resources. Smart security measures should not disrupt the development or performance of your applications – they should streamline them.

xDefenders offers (2) solutions; a **Security Appliance** and a **Vulnerability Management Service** (based on OWASP.org findings) to address the issue of web application security.

***App*Defender Appliance:**

As a hardened Linux Web Firewall appliance, ***App*Defender** provides network isolation, address translation (NAT) and HTTPS to HTTP conversion. This **Reverse Proxy** provides a *physical layer of security* in front of vulnerable, typically Microsoft-based, Web Applications. This Proxy can inspect and stop invalid or malicious web traffic. Additionally, the AppDefender can provide load balancing among multiple web servers, being a single point of access-control. There are overall performance advantages of this solution because the appliance does caching, handles SSL and compresses outbound traffic, and frees up web server resources.

*Mail*Defender …*network level control of Spam and Viruses*

Business Problem:

Most e-mail is Spam! Most viruses come through e-mail! The *Mail*Defender appliance filters out unwanted email and viruses at the firewall level. M*ail*Defender will protect the integrity of your corporate email system and network itself, by preventing dangerous penetrations and subsequent time-consuming responses to such incidents.

Firewall-Level Filtering:

With the *Mail*Defender gateway appliance or hosted service, you add another layer of physical security at your firewall level or in your DMZ (Demilitarized Zone). Most organizations have anti-virus on their desktops and mail servers. This gives you anti-virus at a ***third-level,*** the perimeter of your network. Trying to block spam at the mail server is not good enough. *Mail*Defender leverages Linux and open-source tools and services so your total cost of ownership is much lower than commercial software vendors and other appliance providers.

Benefits:

- Protects your organization from Viruses and Spam and employees from embarrassment and liability of offensive material
- Increases employee productivity and system availability
- Gives you a 3rd layer of protections…at the firewall level
- "Buys back" network bandwidth, computing resources and staff time for productive use

Features:

- Professional, Personalized Service and Support
- User or Group based Policy-based filtering with web-based administration
- Mail filtering based in IP address checks, SMTP envelops, headers and text of the message body. Eliminates spam, porn and other junk email
- Virus-filtering of SMTP traffic (HTTP optional)
- Real-time checks of known spam offenders and new viruses updates every 10 minutes from (3) sources are made to the MailDefender database
- Configurable, scalable platforms to fit your exact requirements, Load-sharing with multiple appliances.
- *Mail*Defender is offered as a Managed Service, so you do not have to administer the operating system, application software, databases and backups, or even monitor the operation of the appliance. xDefenders does that for you!
- Extensive Reporting and Diagnostic Tools

Description:

Typically, *Mail*Defender will be installed in your DMZ (or as a hosted service) and accepts all inbound and outbound Port 25 mail traffic. After inspection, it will route acceptable mail to your corporate internal mail system for final delivery.

It will filter out unwanted mail and forward acceptable mail, based on IP addresses of know spam senders, SMTP envelope, header and keyword checks. Confirmed SPAM mail will be deleted or routed to an administrators mailbox, which allows the suspected spam messages to be examined before deletion. Spam can be labeled as such and delivered to the intended recipient. You have the ability to override these automatic updates by "white-listing". Advanced, content filtering is performed by Spam-Assassin, a proven heuristic assessment tool, that you can regulate.

*Mail*Defender has a built-in Anti-Virus application to inspect mail messages and attachments. It will quarantine every email with a virus for manual inspection. An email will be sent to the offending sender indicating that they are sending viruses and an email will be sent to the intended recipient that a virus filled email arrived. The *Mail*Defender database will be automatically updated every 10 minutes, from 3 different sources, so that inspection is timely and current.

The M*ail*Defender appliance is offered in *small, medium, large* and *redundant* configurations, to accommodate any size business need.

Technical Features:

- GreyListing – qualifies mail to be valid before acceptance
- Supports Active Directory (LDAP) integration to prevent Dictionary Attacks
- RBL and *Heuristic* - Advanced Text Assessment Techniques
- Fail-over configuration using "Round Robin" technique
- Denial of Service Prevention, Intrusion Detection sensor optional
- Web-Based Administration Interface
- Complete Reports Package, Diagnostic Tools
- Encrypted SMTP optional, per domain, Supports multiple Domains

Filtering Process

- Internal and External e-mails arrive at port 25 (SMTP)
- Greylisting may be applied forcing a re-send from a valid sending server, if sender has not sent before a 35 day period
- Valid User Directories are checked to prevent Dictionary Attacks

- Mail:From address is being checked against a two, conservative Real-time Black-hole Lists. If found there, the IP connection is severed. Transaction logged. Most spam blocking occurs here.
- Mail:From address is checked for known spam senders. If found there, email is rejected with an error message back to the sender and an entry in the log.
- e-mail body is being checked for specific regular expressions that clearly classify the email as Spam. If detected, email is rejected with an error message back to the sender and an entry in the log
- All e-mail headers are being checked for specific regular expressions clearly classify the email as Spam. If detected, email is rejected with an error message back to the sender and an entry in the log e-mail is deposited into a queue
- If e-mail has progressed this far, it is pulled from the queue and checked for Spam using a dual-level scorng system. If Spam score reaches or exceeds set thresholds (user controlled), e-mail is tagged as Spam and either sent to the original recipient or re-directed to a specific mailbox (user defined process) or deleted outright.
- e-mail is being checked for viruses. If detected, email is being quarantined on the server along with a message back to the sender and a message to the system administrator (user defined process)
- Optional Mail Archiving (clean mail) can take place, at this time.

***Mail*Defender Features -**	***Business***
Hardware Appliance(s)	Small, medium and large, HP servers
Managed Services	Yes, by xDefenders, also Hosted in SAS 70 data center with redundancy OS, Applications and DB updates Remote Backup, Remote Monitoring
High Availability Configurations	Yes, via Load Sharing
User Controls & Options	Yes
Web-based Administration	Yes
Remote Control & Reboot	Yes
Real-Time Monitoring w/ Alerts	Yes
Disaster Recovery Method	Simple CD re-load, 1 hour
Hardware Maintenance Plan	Next Day Overnight Replacement or HP on-site
Remote Backups Made	Saturday nights @ xDefenders HQ
New Software Uploads	Quarterly
Reports Package	Yes Daily, Weekly, Monthly, Annual Graphical Reports
Mail Server	Optional, Post Fix implementation
Mail Archive	Optional, software or appliance

***Mail*Defender® Features –**	***Technical***
Architecture	Firewall Layer, Security Gateway
Protocol Filtered	SMTP
Viruses Filtered	SMTP (HTTP optional)
Firewall	Built-in for extra Security
Operating System	Hardened Linux
OS Reliability	Best of Breed
Applications	(3) Real-time Black-hole Lists Spam Assassin Scoring Filter FPROT, BDC and Clam AV's Post-Fix Mail Transport
GreyListing	Optional
Advanced Rule Base Filtering	Heuristic Algorithms
Anti-Virus Pattern Updates	Every Ten Minutes
Blacklist updates	Hourly
White Listing/ Overrides	Yes
Attachment Controls (ActX, Java)	Yes
MIME De-fang	Yes
Multi-Language Support	Yes (French, Port.
MS MMC Snap-In Support	No
LDAP Support	Yes, to block Dictionary Attacks by checking first for valid users
Secure Web Mail	Yes
Encryption	Yes, by default
POP3, IMAP4 Filtering	Optional
User or Group Set Policy	Yes
Reporting	Extensive
Diagnostic Tools for eMail	Yes

MailDefender - Managed and Hosted Services include:

- Appliance - Design, Deploy, Manage, Monitor, Maintain
- Hardware and software and services
- Pre-Installed Linux Configuration
- Turnkey Installation and basic fine-tuning of rules
- Escalation Plan Developed with I/T Staff.
- Online Documentation, Web Interface
- Technical phone and email support
- Databases updated, automatically (daily, MailDefender AV is every 10 minutes)
- Secure SSH connection to/from xDefenders Security Operations Center
- OS and Applications patched, enhanced, remotely
- Weekly local and remote backups
- Hardware maintenance is next day overnight, replacement
- Typical HP appliance has dual core Intel, 1 GB ram, CD, 80 GB disk.
- Appliance has a 1 Year Warranty from date of shipment
- SAS 70 Data Center with Redundancy

Mail*Defender® Features – *Technical

Architecture	Firewall Layer, Security Gateway
Protocol Filtered	SMTP
Viruses Filtered	SMTP (HTTP optional)
Firewall	Built-in for extra Security
Operating System	Hardened Linux
OS Reliability	Best of Breed
Applications	(3) Real-time Black-hole Lists Spam Assassin Scoring Filter FPROT, BDC and Clam AV's Post-Fix Mail Transport
GreyListing	Optional
Advanced Rule Base Filtering	Heuristic Algorithms
Anti-Virus Pattern Updates	Every Ten Minutes
Blacklist updates	Hourly
White Listing/ Overrides	Yes
Attachment Controls (AcX, Java)	Yes
MIME De-Fang	Yes
Message Parking	Yes
Multi-Language Support	Yes (French, Port.)
MS MMC Snap-In Support	No
LDAP Support	Yes, to block Dictionary Attacks checking for valid users
Secure Web Mail	Yes
Encryption	Yes, by default
POP3, IMAP4 Filtering	Optional

*Net*Defender … *Intrusion Detection System*

Business Problem:

Every business that leverages the Internet needs advanced security protections, otherwise business operations can be disabled! Organizations may not have the time, interest or technical expertise required to administer and maintain these essential security services. In addition, the cost of popular commercial security products can be prohibitive. The N*et*Defender appliance, with managed service solves these problems by delivering advanced intrusion detection, malware detection, ARP monitoring at all levels in your LAN and DMZ.

Description:

The *Net*Defender appliance provides robust, enterprise-class security services including a state-full inspection firewall, port-scan detection, standards-based **IPsec**, 3DES Virtual Private Networking (VPN), Intrusion Detection System that utilizes **Snort** for real-time alert detection, **ACID** for Reporting of the Snort Database and our own **"Bacon"** software for Correlation and Escalation of "New" or "Escalating" Critical Alerts. The Snort database is updated, automatically every day. xDefenders provides essential IDS tuning and training to eliminate false-positives.

The *Net*Defender IDS is a compact, plug-n-play rack-mount appliance that is managed and monitored by xDefenders. Built upon a hardened, Linux operating system. *Net*Defender provides the highest levels of Internal security and have incorporated industry standards.

Administrators can monitor the appliance with a Web-based management interface to centralize and control policy. xDefenders maintains a Secure Shell (SSH) to the appliance for periodic updates and monitoring purposes.

xDefenders has a 24x7x365 **Security Operations Center** that can manage and monitor firewalls and intrusion detection systems for clients. Escalation Planning and Incident Response is provided with the client.

Features:

- HoneyPot will automatically detect and alert based on the presence of MalWare
- ARP monitoring reports on changes, updates to prevent Man-in-the-Middle attacks, IP address and MAC address reconciliation
- Web GUI and extensive IDS and ARP Reporting
- Daily updates of Snort and Bleeding Edge signatures
- ACID or BASE Reporting of the MY/SQL Snort Database
- BACON checks every 5 minutes for NEW & Escalating Alerts

- Automatic IDS Escalation via email or text messaging
- Fine-Tuning by xDefenders to your environment

HoneyPot

There is a built-in HoneyPot function into the NetDefender IDS and it is designed to alert, immediately, based on the pressence of MalWare in the network. This means that root-kits, spyware, bots and other dangerous code will be identified and detected. The alert goes to the xDefenders SOC and the SOC staff will contact the customer.

ARP Monitoring

Man-in-the-Middle attacks are the latest attack that can affect the LAN. By watching for changes to the LAN and comparing IP address with MAC address, this kind of attack can be identified. ARP Reporting is extensive and valuable to a Security Administrator. These reports will allow them to identify strange behavior and unplanned or unwanted changes.

Network Intrusion Detection (IDS)

This risk management service incorporates real-time monitoring of malicious and suspicious electronic activity within your business. Every 5 minutes, the IDS checks for NEW or ESCALATING Events and alerts the client or the xDefenders **Security Operations Center (SOC)** in Rochester, NY, where a Trouble Ticket is created and available via the Client Portal. This service includes attack signature database updates, real-time correlation, real-time web reporting (see below), administration support and monitoring with custom escalation/notification procedures. A (6) Month Forensic Database is kept. Escalation Plans w/ Incident Response.

Snapshot Views of the IDS Database using ACID:

- Most recent Alerts: any protocol, TCP, UDP, ICMP
- Today's: alerts unique, listing; IP src / dst
- Last 24 Hours: alerts unique, listing; IP src / dst
- Last 72 Hours: alerts unique, listing; IP src / dst
- Most recent 30 Unique Alerts UDP

Most frequent 15 Alerts
Most Frequent Source Ports:
any , TCP , UDP
Most Frequent Destination Ports:
any , TCP , UDP
Most frequent 30 addresses:
source, destination
Last Source Ports: any , TCP , UDP
Last Destination Ports: any , TCP ,

*Sys*Defender … *Vulnerability Testing Service, Appliance*

Business Problem:

If your organization depends on the Internet to conduct business, you have to stay one step ahead of emerging hackers, viruses and threats. If you do not, your business will be disrupted and that could be very costly. It makes good business sense to frequently test then patch your Internet, I/T Technologies and Communications services for vulnerabilities and risks.

Types of Assessments:

1. *External Vulnerability Assessment* simulates a "hacker" trying to penetrate your firewall. www.modsecurity.org
2. *Internal Vulnerability Assessment* simulates a "disgruntled employee" and attempts to exploit vulnerabilities inside your firewall and on your LAN.
3. *CIS (Center for Internet Security) Benchmarks* provide a score from 0-100, grading your servers and databases for security competence against "best industry practices". www.cisecurity.org
4. *Social Engineering* attempts to gain access and vital knowledge by communicating with employees and business partners.
5. *Wireless Vulnerability Assessment* uses "drive-by and walk-by" attempts to gain access to private wireless networks and assets, using modern technology.
6. *Database and Web Application Assessment* to determine security protections at these levels of the business.

Description:

For External and Internal Vulnerability Assessments, xDefenders offers *SysDefender,* a hardened Linux based server with powerful open-source scanning (up to 65,000+ open ports) software. The appliance is updated periodically to stay current with known vulnerabilities and vendor patches. Thousands of built-in tests automatically interrogate IP based network devices and servers. A database of "findings" is created with severity/ risk levels assigned to help network and system administrators quickly identify and remedy vulnerable ports, operating systems and applications. An Executive Summary and Technical Report are created and findings are reviewed with the client.

Features:

- **Plug-in architecture**. Each security test is written as an external plug-in. This way, you can easily add your own tests without having to read the code of the testing engine.
- **ASL**. The Security Scanner includes an Attack Scripting Language, designed to write security tests easily and quickly. Security checks can also be written in C.
- **Up-to-date security vulnerability database**. We mainly focus on the development of security checks for **recent security holes**. Our security checks database is updated on a

daily basis, and all the newest security checks are available, including FTP servers and mirrors.

- **Client-server architecture**. The Security Scanner is made up of two parts: a server, which performs the attacks, and a client which is the front end. You can run the server and the client on different systems. That is, you can audit your whole network from your personal computer, whereas the server performs its attacks from the *Sys*Defender, which is in the data-center. There are several clients: one for X11, one for Win32 and one written in Java

- **Smart service recognition**. *Sys*Defender does not believe that the target hosts will respect the IANA assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (31337 say), or a web server running on port 8080

- **Multiples services**. Imagine that you run **two** web servers (or more) on your host, one on port 80 and another on port 8080. When it comes to testing their security, *Sys*Defender **will test both of them**

- **Tests cooperation**. The security tests performed by *Sys*Defender coordinate with your configuration so that useless tests are not performed. If your FTP server does not offer anonymous logins, then anonymous-related security checks will not be performed.

- **Complete reports**: *Sys*Defender will not only tell you what's wrong on your network, but will, most of the time, tell you how to prevent crackers from exploiting the security holes found and will give you the risk level of each problem found (from *Low* to *Very High*)

- **Exportable reports**: The Unix client can export *Sys*Defender reports as ASCII text, LaTeX, HTML, "spiffy" HTML (with pies and graphs) and an easy-to-parse file format.

- **Full SSL support**: *Sys*Defender has the ability to test SSLized services such as https, smtps, imaps, and more. You can even supply *Sys*Defender with a certificate so that it can integrates into a PKI-field environment

- **Smart plug-ins** (optional): *Sys*Defender will determine which plugins should or should not be launched against the remote host (for instance, this prevents the testing of SendMail vulnerabilities against Postfix or "optimizations")

- **Non-destructive** (optional): If you don't want to take the risk to bring down services on your network, you can enable the "safe checks" option of *Sys*Defender, which will make *Sys*Defender rely on banners rather than exploiting real flaws to determine if a vulnerability is present

- **Independent developers**. The *Sys*Defender developers are independent. We will not suppress vulnerabilities because we have a relationship with the authors.

*Web*Defender …*enforcing your Internet Acceptable-Use-Policy*

Introduction:

The *Web*Defender appliance with managed service restricts access to undesirable and unwanted web material by providing high performance URL filtering, using policies and a current database of restricted sites. It is completely configured and installed in your DMZ or LAN to control web access and log user activity.

Benefits:

- Protects your organization and employees from embarrassment and liability of offensive material
- Increases employee productivity and system availability
- "Buys back" network bandwidth, computing resources and staff time for productive use.
- Leverages Open-Source tools and services for Lowest Cost of Ownership available.

Features:

- Popular *SmoothWall* application software or Cymphonix Firewall Appliance
- Policy-based filtering to enforce your Policy
- Restrict Access to Web Sites based on Domain Name, URL and Expressions
- Filtering based on specific words and phrases written and by the overall rating of the content
- Web page cache to boost performance
- Timely updates of websites with questionable content, from critical knowledge databases
- LDAP interface (Active Directory integration)

Description:

Typically, *Web*Defender will be installed in your DMZ or LAN and accepts all outbound HTTP traffic. Web pages are cached, then inspected.

The *Web*Defender database is automatically updated each day with new, websites, so that inspection is timely and current. You have the ability to over-ride (White-List) and add-to (Black-List) these automatic updates.

Web caching enhances the web browsing experience by caching commonly accessed web content and serving subsequent requests for the same content locally rather than requesting it from the actual web site.

Technical Features:

1. Host-based Denial of Service Prevention
2. Web-Based Administration Interface
3. Restrict Access to sites with Viruses (HTTP traffic)
4. User Tracking via Login & Password
5. User Authentication via LDAP or user database
6. Time of Day, User Controls if #4 and #5 is utilized
7. User Groups are supported
8. Forward Proxy with Cache

Filtering Process:

1. Checks the website to see if it is a banned site or not. Automatic daily updates are made to the database. Blacklisting and White-listing of websites is possible.
2. Checks to see if specific URL's are banned. Daily updates are made to the database. Blacklisting and White-listing of URL's is possible.
3. Keywords and Expressions are checked to see if they should be banned. There are 25 categories and 21 user-definable categories for management controls. Black-listing and White-listing is possible.
4. Web pages of certain type can be blocked. User-defined Blacklist is maintained.

Reports:

Top User – A report for each user broken down by sites visited, connections, and other info each day.

Top Sites – Top 100 sites visited by the users sorted by number of connections. This is a daily report.

Top 20 URLs Blocked - Because of virus, mime type, or category per day.

Top 20 Users Blocked - Because of virus, mime type, or category per day. The ranking is by number of blocked attempts.

Sites & Users Report – All sites accessed during the day and who accessed them.

Site Guard – All site access attempts that were blocked on a daily basis. This report includes the offending site, the user who made the attempt, the time of day, and the rule, which was violated (ie: porn, news sites etc.).

Daily User – this shows how much time a user is spending on the web hour by hour each day.

Blocked by Category – This simple report shows the number of blocked attempts for each category per day. Categories include gambling, porn, ads, news, etc.

Blocked by Virus or Mime Type - This simple report shows the number of blocked attempts that were blocked because they contained viruses, blocked by category, or mime type violations per day.