



MailDefender ...network level control of Spam and Viruses

Business Problem:

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

MailDefender is offered as a Hosted Service or as an on-site Appliance. Both solutions are “managed services” from xDefenders.

Firewall-Level Filtering:

With the *MailDefender* 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. *MailDefender* 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
- Policy-based filtering with web-based administration
- Mail filtering based in IP address checks, SMTP envelopes, 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.
- *MailDefender* 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!

Description:

Typically, *MailDefender* 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.

MailDefender 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 *MailDefender* database will be automatically updated every 10 minutes, from 3 different sources, so that inspection is timely and current.

The *MailDefender* 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
- 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 mail before a 35 day period. Valid mail always re-sends.
- Valid User Directories are checked to prevent Dictionary Attacks (LDAP)
- 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 scoring 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 Archiving (clean mail) can take place, at this time.

MailDefender® Features -***Business***

Hardware Appliance(s) Managed Services	Small, medium and large, HP servers offered Yes, by xDefenders, also Hosted in SAS 70 datacenter 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	Weekend nights @ xDefenders Data Center
New Software Uploads	Quarterly
Reports Package	Yes Daily, Weekly, Monthly, Annual Graphical Reports
Mail Server	Optional, Post Fix implementation
Mail Archive	Optional, software and appliance

MailDefender® 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
	Post-Fix Mail Transport
GreyListing	Optional (Opt In)
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 by checking first for valid users
Secure Web Mail	Yes
Encryption	Yes, by default
POP3, IMAP4 Filtering	Optional

MailDefender - Managed Security Appliance 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 included 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 or HP on-site contract
- Minimum HP appliance has Xeon Intel CPU, 1 GB ram, CD, 80 GB disk.
- Appliance has a Hardware Warranty from date of shipment
- SAS 70 Data Center with Redundancy

Jeff Thon, VP
xDefenders, inc.
1100 Pittsford Victor Rd
Pittsford, NY 14534
585-385-2770
<http://www.xdefenders.com>