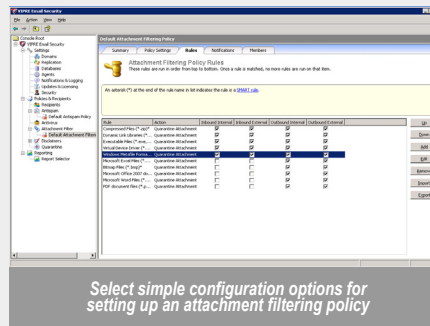


VIPRE Email Security for Exchange is an advanced, powerful, policy-based email security product that provides you as a system administrator the weapon to enforce email policies that protect your network against spam, phishing, viruses and other messaging security threats. VIPRE for Exchange provides a layered security approach for email inspection, cleansing and management. By using multiple scanning engines for antispam and antivirus, while integrating other email security rules, all treatment of messages occurs at the server, not at your end users' workstations - no client software needed.

Policy-based plug-in management

The plug-in architecture of VIPRE for Exchange was designed with flexibility and extensibility in mind. That way you get a robust product that enables you to comprehensively manage your email security. You can create customizable policies using VIPRE's integrated plug-in management. VIPRE for Exchange includes plug-ins for antispam, antivirus, attachment filtering, and disclaimers.

With extensive policy creation capabilities, you can create custom policies for groups of users or a single user using Active Directory. You can set parameters based on user and/or organizational requirements. If you wish, you can simply associate all users with VIPRE's default plug-in policies and have a powerful messaging protection solution in place in just a few minutes. You can also create separate policy templates for different groups or individuals. And, you don't have to set up and maintain lists of blocked IP addresses and constantly create all sorts of custom rules. You have the flexibility to fine tune the aggressiveness of detection for all messaging plug-ins.



Select simple configuration options for setting up an attachment filtering policy

Fast deployment in Exchange 2000-2010 environments

The VIPRE for Exchange management console enables you to install, configure, and manage your full email security from one central location. Designed as an MMC snap-in, deployment is simple with a minimum of configuration effort needed. VIPRE Email Security integrates tightly with Microsoft® Exchange and provides excellent spam and virus protection, file attachment inspection, and disclaimers. Additionally, VIPRE for Exchange makes it easy to create policies across multiple messaging plug-ins.

Multiple scanning engines for higher detection and protection

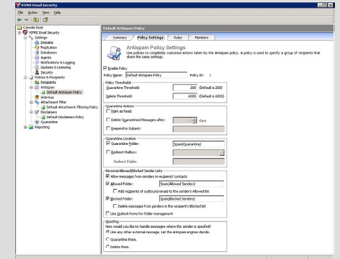
VIPRE for Exchange is designed to meet both the spam and virus protection needs of your organization. With multiple spam and virus scanning engines, you automatically receive higher detection rates and a more accurate response to the messaging threats that attempt to enter your network. VIPRE for Exchange is an integrated antispam and antivirus solution, eliminating viruses, malware, and other dangerous message content, while also filtering attachments at the Exchange server, before they reach your users.

Server-based antispam filtering

For its antispam capabilities, VIPRE for Exchange includes the Cloudmark™ antispam engine, Sunbelt's own antispam engine and support for Real-time Blackhole Lists (RBLs). This plug-in delivers superior spam detection against both standard and image spam using heuristic functionality and spam signature technology. Configure VIPRE for Exchange to delete, centrally quarantine, add Subject line identification, or send messages to a custom folder in the end-user's Exchange mailbox.

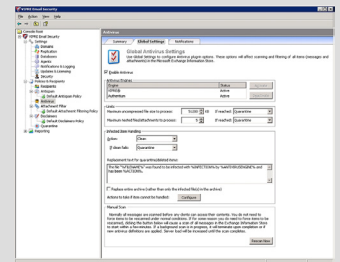
Custom rules capabilities give you the ability to control spam and any other kind of email. You can supplement the spam detection engine with a variety of rules created on a number of email message properties such as body, sender IP, header, or subject. With the ability to strip HTML content prior to scanning, as well as an option to add cumulative points for words or phrases that appear multiple times in a single message, you can control how VIPRE for Exchange scores the message based on your custom rule selections.

Also, using regular expressions for custom rules allows for even more powerful filtering. With the increasing number of phishing attacks, identifying legitimate email addresses from spoofed addresses is important. Using the Sender Policy Framework (SPF), users are able to test whether a specific email originated from its claimed domain. VIPRE for Exchange allows users to participate in SPF, helping reduce the risk of phishing and fraudulent email.



Antispam Policy Settings:

Diverse Antispam Policy settings for all needs



Antivirus Settings:

Multiple Antivirus engines for better protection



Sunbelt Software
we keep the bad guys out™



VIPRE Email Security for Exchange Requirements

Processor

Requirement

Intel Pentium or compatible 1 GHz or higher processor

Recommendation

Intel Pentium or compatible 2.4 GHz

Operating System and Software

Requirement

Windows 2000 Server family with SP3 through Windows Server 2008

Windows XP Professional SP1 for client tools

.NET Platform 2.0

MDAC 2.8 SP1

Microsoft Exchange 2003 SP1 through 2010

Recommendation

Windows Server 2003 R2

Windows XP Professional SP2 for client tools

Memory and Other Requirements

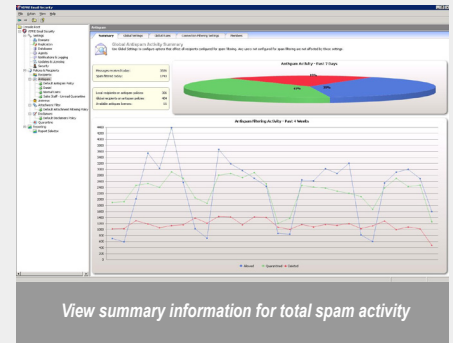
Requirement

Please visit www.sunbeltsoftware.com for memory requirements

Aggressive virus detection and elimination

VIPRE for Exchange uses multiple industrial strength antivirus engines to scan inbound and outbound email, including Sunbelt's own VIPRE antivirus engine. The engine is a comprehensive antivirus engine that merges the detection of all types of malware into a single, efficient, and powerful system. The technology was exclusively built by Sunbelt, without building on older generation antivirus engines and addresses the performance and resource headaches associated with traditional enterprise antivirus products.

You can set scanning parameters which include enabling or disabling individual scan engines as well as the desired action on detected infections. This allows you to disinfect and/or quarantine pieces of an email, essentially breaking apart the email message and only quarantining infected files instead of stripping all attachments. With this layered approach, VIPRE for Exchange not only quarantines and cleans viruses but also blocks potentially hazardous file attachments and looks for common virus signatures during the scanning process, including inspection within compressed ZIP files received in emails. VIPRE for Exchange automatically checks for updates to the virus definition files ensuring the best possible virus protection.

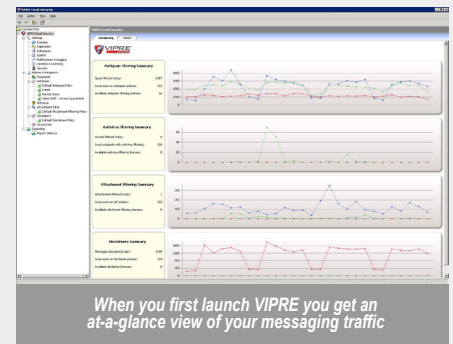


Email and attachment filtering on a per-policy basis

With powerful policy-based attachment filtering capabilities, VIPRE for Exchange enables you to configure inspection and filtering on a per-policy basis. The intelligent Suspicious Mail Attachment Removal Technology (S.M.A.R.T.) filter scans the content of a file to verify that an attachment is what it says it is; no more renaming .exe files to get around the filters. Set rules based on users and file types enabling you to quarantine potentially harmful content or attachments by file extension including .doc, .exe, .dll, .pdf, graphic files and more. For example, allow specified users to send .exe files internally while blocking them externally. No other email security solution in the industry uses policies to manage your attachment filtering!

Global and policy-based disclaimers

VIPRE for Exchange allows you to configure global disclaimers for all outbound email. Add disclaimers to every email using the global disclaimer configuration. Or if you prefer, configure policies to add disclaimers to emails from specific users, groups, domains or public folders. VIPRE for Exchange also prevents multiple disclaimers when replying or forwarding and gives you the ability to allow users to bypass the disclaimer on a per email basis. Additionally, disclaimer templates are included that allow you to easily set up disclaimers using HTML or plain text. Template samples include legal disclaimers, virus warning disclaimers, copyright disclaimers, and more.



Powerful reporting options for all plug-ins

VIPRE for Exchange delivers system reporting for all plug-ins using a set of pre-defined reports with the ability to customize reports based on individual needs. The database-driven reporting engine can generate reports with information at the system, group, and/or user level. You can choose reporting options to show the number of inbound mail messages scanned, number of spam deleted or marked, number of viruses intercepted, number of filters triggered, percentage of viruses by name, disclaimers used, and more.

