Employing VisNetic MailServer Security Features

VisNetic MailServer

powerful email server

VisNetic MailServer Security Features

VisNetic MailServer includes a sophisticated and broad array of security features. A step-by-step guide to configuration of each follows.

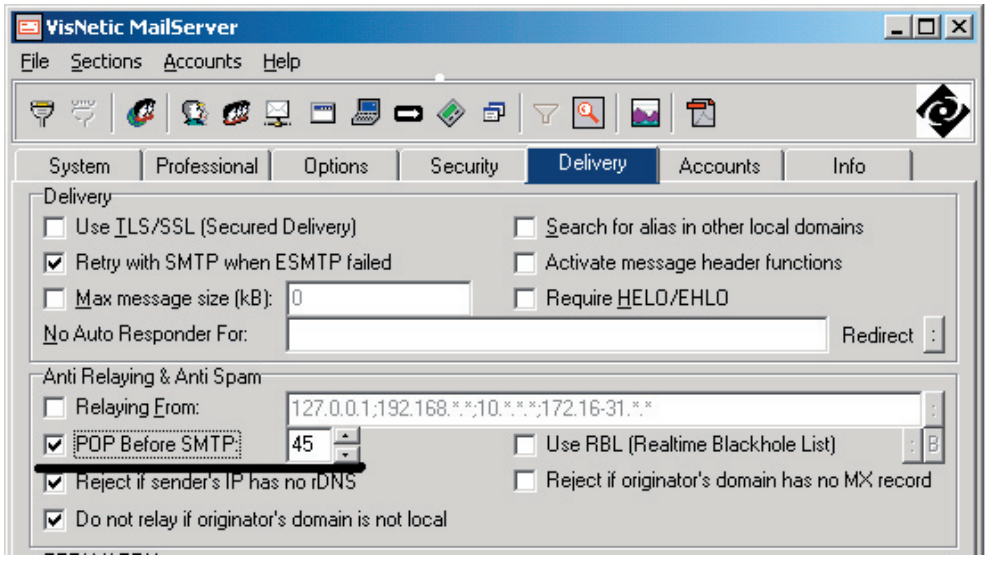
Prevent Open Relaying

An “Open Relay” server allows anyone, anywhere to connect and send mail through it. If your mail server is used as an open relay, your IP address may be black listed by Spam-blocking databases and by other mail servers on the Internet, reducing your ability to communicate via email with your customers, vendors and partners. Additionally, your bandwidth and resources are used to send the messages and that drain may negatively impact critical business operations.

POP Before SMTP

VisNetic MailServer’s POP before SMTP feature prevents open relaying by ensuring that all mail sent originates from a valid user account. When this feature is activated, VisNetic MailServer will require each user to check their mail or issue their POP login before sending email. The server then records the user’s IP address and, for a designated period of time, allows that IP address to send mail.

To activate this feature, select the Delivery tab in the VisNetic MailServer configuration window.



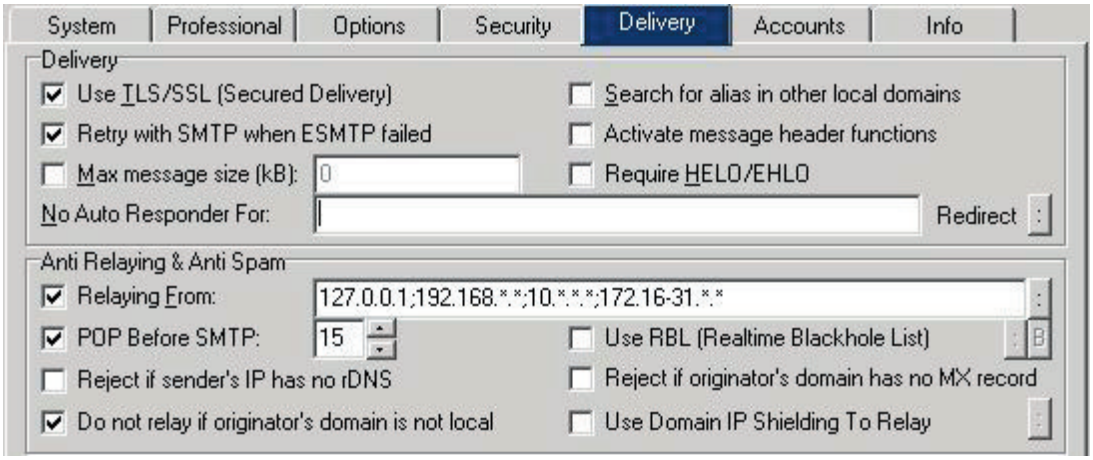
Enable “POP before SMTP” and specify the time interval. This is the amount of time (in minutes) VMS will allow a user to send mail before they are required to authenticate again.

SMTP Auth

VisNetic MailServer can be configured to allow external users or applications that do not have accounts on the server to send email. This is useful for individuals using email clients (e.g. IMAP) that do not POP before retrieving email from the server. The SMTP Authorization option, enabled by default, allows these users to send mail after proper authentication.

For proper authentication, the email clients of each external user must be configured to authenticate during SMTP sessions.

If you choose to disable the SMTP Auth feature, depress the Security tab and select Disable SMTP AUTH.

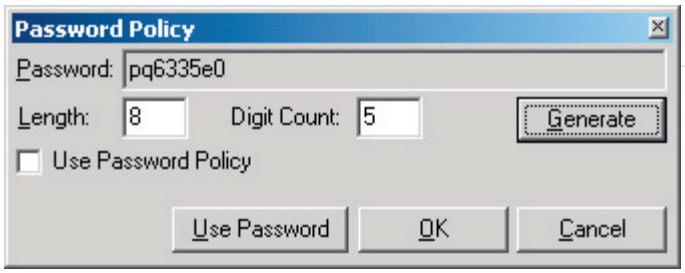


Avoid Account Hijacking

Account hijacking occurs when an unauthorized third party uses a valid user's login to send email through your server. This is possible when a login and password is compromised.

VisNetic MailServer's Password Policy option is designed to reduce the risk of unauthorized access to login and password information. The Password Policy option will automatically create random character passwords for user accounts. These passwords, by definition, are more difficult to hack.

To utilize this option, select the colon button in the user field, with the Accounts tab. Specify password length—8 to 15 characters is the standard recommendation—and number of numeric characters to be included in the password. Depress the Generate button and select Use Password.



Protect against Email-bourne Viruses

Integrated Antivirus

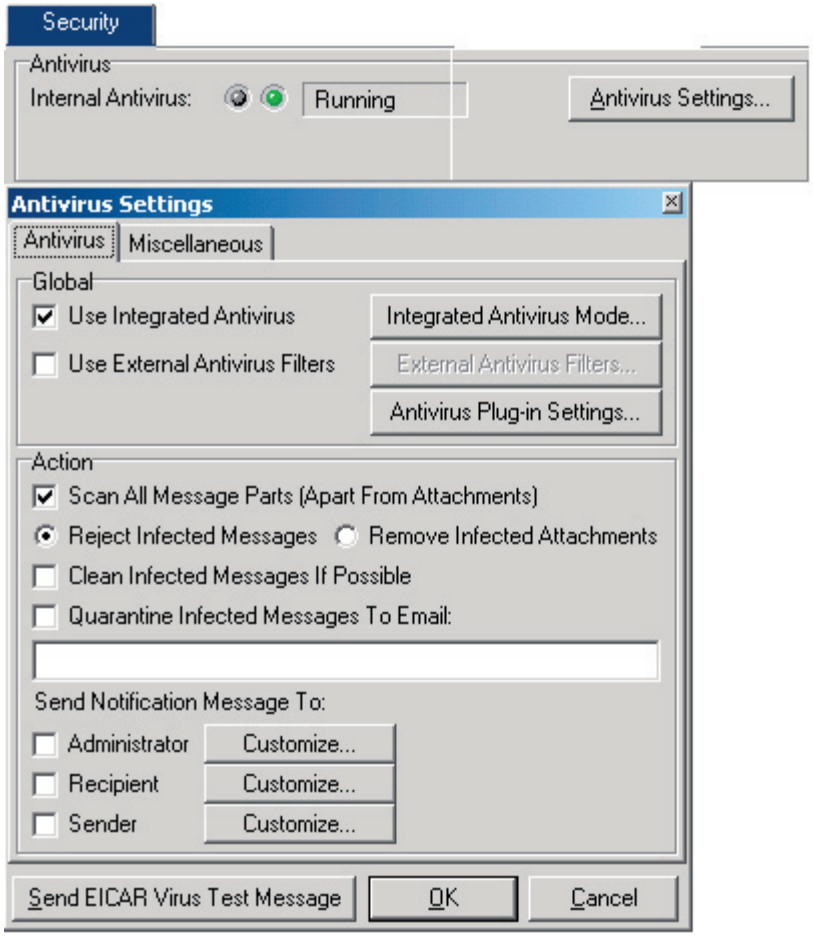
VisNetic MailServer includes support for integrated antivirus protection. The VisNetic AntiVirus Plug-in for MailServer resides on the email server and protects your entire network from email-bourne viruses. It features a powerful, multi-threaded scanning engine and SMTP-based virus update notifications.

The VisNetic AntiVirus Plug-in scans all inbound and outbound email traffic for viruses. Once identified and detained, infected email can be deleted, quarantined or forwarded to the administrator for further action.

The plug-in is supported by Kaspersky's continually updated virus signature list and is designed to automatically download only the necessary update information in a small download. Consequently, VisNetic AntiVirus is able to update quickly, with minimum bandwidth requirements.

Once the VisNetic AntiVirus Plug-in is installed, you must enable it from the Security tab in the VisNetic MailServer configuration window. Simply select the 'Use Integrated AntiVirus' field. To specify scanning criteria for domains, user accounts and messages, depress 'Integrated AntiVirus Mode'.

A green light on the Security tab in the AntiVirus filed indicates VisNetic AntiVirus is running and protecting your system from email-bourne viruses.



Learn more about the VisNetic AntiVirus Plug-in at http://www.deerfield.com/products/visnetic_mailserver/antivirus/ .

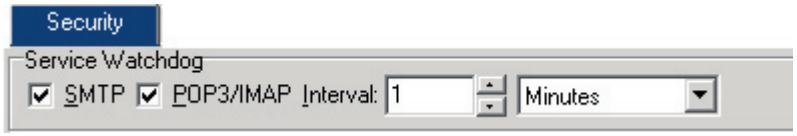
Learn more about email-bourne viruses at http://www.viruslibrary.com.

Protect against DoS attacks

Denial of service (DoS) attacks can occur when one or more third parties send large amounts of otherwise legitimate requests to your mail server, swamping the server process. The goal of this type of attack is to prevent other users from accessing the service by forcing the server to fulfill an excessive number of requests.

To protect against DoS attacks, VisNetic MailServer administrators can set the maximum number of allowed connections for a service. If your SMTP service is being DoS'd, it will only accept the number of connections set in this dialog and will then return a message to the sending server that the service is not available. This will prevent further connections from being accepted until the number of connections decreases to below the threshold. This will allow the service to continue to operate (it won't crash), until the attack subsides.

Additionally, VisNetic MailServer features a Service Watchdog that will check the SMTP and/or POP3/IMAP services periodically. In the event the monitored service is stopped, the Watchdog will attempt to restart it. This feature can be enabled under the Security tab.



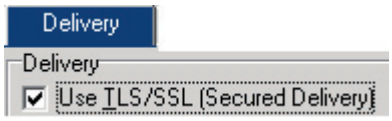
Secure Connections

VisNetic MailServer supports Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. Using these protocols, transmitted data is rendered indecipherable.

Applied to email, these protocols work in the following manner. Messages sent between two or more mail servers, or between a mail server and a mail client using SSL/TLS, acknowledge use of the protocol and negotiate or decide upon an encryption method. Messages to be sent are then encrypted and sent over the Internet in the same manner as standard email messages. Upon receipt, the messages are decrypted at the server level.

VisNetic MailServer allows direct SSL/TLS connections using POP3, SMTP, IMAP4 or LDAP protocols between 2 or more email servers. TLS/SSL support is enabled by default upon installation. Secure connections are initiated automatically when messages are sent to or received from an email server that supports these same protocols. If the email server that is being connected to does not support SSL or TLS, messages will be sent or received directly through the non-secure POP3 or SMTP protocols. This security check is transparent and will not interrupt the flow of email traffic.

This option is located under the Delivery tab within the configuration window.

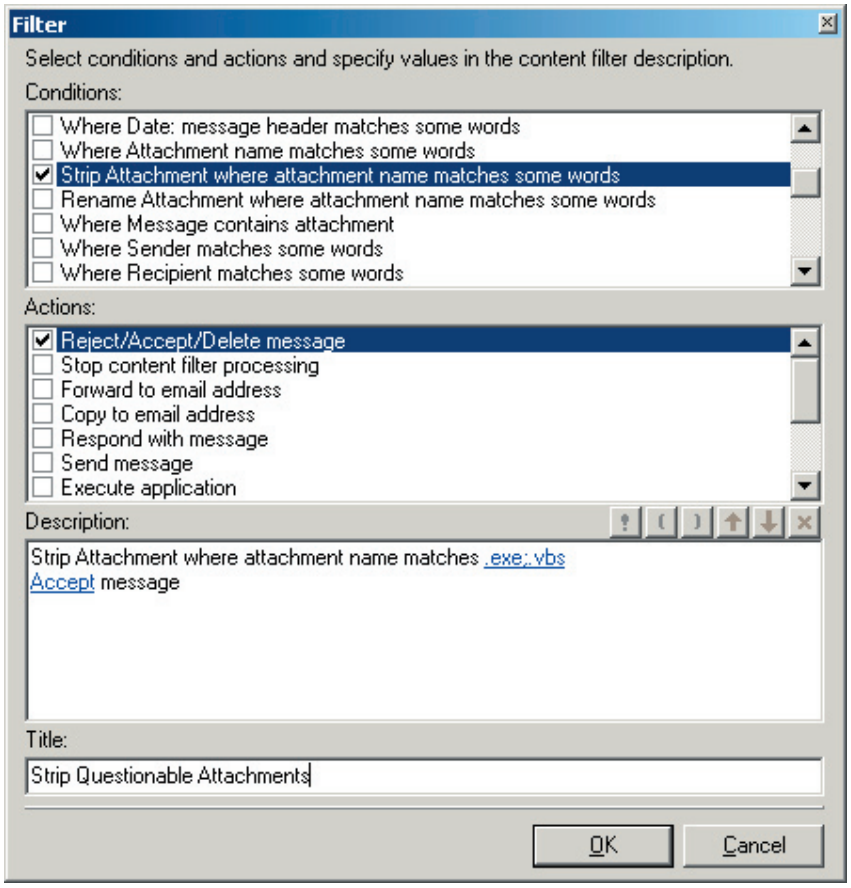


Filter Hazardous Attachments

VisNetic MailServer's mature content filtering capabilities allow administrators to block specific types of email attachments (e.g. .exe, .vbs), protecting your network and workstations from files potentially designed to alter computer settings or open ports to unauthorized traffic.

Enable VisNetic MailServer's Content Filter by placing a check mark in the Content Filter field within the Security tab in the VMS configuration window. To create a filter by attachment type, depress the 'Content Filter' button. In the following example, the filter is set up to strip .exe and .vbs attachments from email before delivery.

- Begin by selecting the Add button.
- In the Conditions field, select Strip Attachment where attachment name matches some word.
- In the Action field, select Reject/Accept/Delete message.
- In the Description field, select Some Words (highlighted) and specify the following string: .exe;.vbs. Depress OK.
- Also in the Description field, select Reject and change it to Accept the message. Depress OK.



Additional Security Options

Protecting User Account Information

Administrators can minimize access to user account information by activating the Deny VRFY and Deny Telnet features in VisNetic MailServer. Both commands may be utilized by third parties to harvest email addresses.

When the Deny VRFY feature is enabled, VisNetic MailServer will return a 'not supported' error to VRFY commands issued by a remote server. When the Deny Telnet feature is activated, a third party will be able to establish a connection using telnet, but VisNetic MailServer will not accept any commands once the session is established.

Protecting Server Information

Additionally, administrators can limit the amount of information about the server contained in email transmissions using VisNetic MailServer's option to hide the IP address from each message's "Received**:** MIME header".

Guarding Web Access

Organizations may also choose to deny web access to the mail server, locking everyone out. Administrators can disable web access but still modify server configuration via the remote console.

Alternatively, organizations that wish to allow web access (web mail, web administration) can deploy VisNetic ActiveDefense, an intrusion detection solution designed to monitor ports left open to this access for malicious activity.

Additional Resources

Setup Guides: http://www.deerfield.com/support/visnetic_mailserver/setup/
Knowledge Base: http://www.deerfield.com/support/visnetic_mailserver/kb/
FAQ: http://www.deerfield.com/support/visnetic_mailserver/faq/
Release Notes: http://www.deerfield.com/support/VisNetic_MailServer/releasenotes/

Free Support via Forum: http://webboard.deerfield.com/login

Contact

Deerfield Communications, Inc.

P.O. Box 851

Gaylord, MI 49735

USA

Telephone 989.732.8856

Fax 989.731.9299

www.deerfield.com

sales@deerfield.com
feedback@deerfield.com