Controlling spam: Advanced SMTP settings in Lotus Domino (Part 1)

Edmund Stanton

February 22, 2005
(First published October 04, 2004)

Find out how to control spam mail using the Configuration Settings document, server mail rules, and inbound SMTP commands and extensions in Lotus Domino 6 and later. This article is part one in a series about Lotus Domino methods of spam control.

In the ever-changing world of technology, the amount of spam mail is increasing faster than most email systems can handle or control. In 2004, almost nine billion dollars will be spent by all U.S. corporations to fight spam. Companies have dedicated products to identify and quarantine possible spam messages. Recent surveys have shown that over 40% of all email is considered spam with an average of six messages a day per email user. If you think that's bad, the estimated spam increase by 2007 is 63%. These statistics and more can be found at the Spam Filter Review Web site.

Starting in Lotus Domino 4, Lotus has been building ways to prevent spam email and to restrict Simple Mail Transfer Protocol (SMTP) messages. Lotus Domino 4 introduced multiple Notes.ini parameters to control relaying, inbound connections, and sendersâ## domains. Lotus Domino 5 introduced a Graphical User Interface (GUI) in which Domino administrators could list values within fields in the Configuration Settings Document. This made SMTP configurations easier for a Domino administrator and took some of the burden off Notes users.

Lotus Domino 6 has taken great steps to develop technology to integrate messaging with DNS blacklist (DNSBL) filtering and content filtering. This article series explores the multiple solutions that IBM has created to limit the amount of unsolicited email from the server as well as preview the spam controls in Lotus Domino 7. In part one of this series, we look at settings in the Configuration Server document and server mail rules to help control spam. In part two, we discuss settings in the Server document and Notes.ini variables that control spam. We'll also take a sneak peek at enhancements in Lotus Notes/Domino 7. This article series assumes that you are an experienced Domino administrator familiar with Lotus Notes and Domino 6.

SMTP settings in Domino

Most Notes users would prefer that their administrator prevent spam email instead of having to delete and filter out unwanted email themselves. The most effective way to prevent spam is to

stop the message from getting into your environment. This entails configuring SMTP and Router settings. You can configure both in the Configuration Settings document, Server document, and Domino server Notes.ini file.

The SMTP task controls the SMTP listener on the Domino server. By default, whenever you restart the SMTP service, and at two-minute intervals thereafter, the SMTP service automatically checks the Notes.ini file, Configuration Settings document, and Server document to see if any settings have changed. If the service detects that settings have changed, it rebuilds its internal configuration to incorporate the changes.

Configuration Settings document

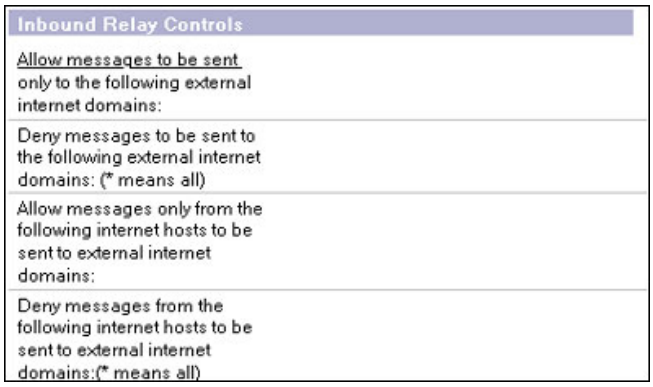
The most effective place to control SMTP traffic is through the Configuration Settings document. The Configuration Settings document has several tabs that allow you to filter SMTP email, therefore reducing the amount of spam. On the Configuration Settings document Router/SMTP - Restrictions and Controls - SMTP Inbound Controls tab, there are six additional sections to configure the SMTP protocol.

Inbound relay controls

This section allows you to populate Internet domains to which Domino will allow or deny relaying messages as shown in Figure 1. Not configuring your Domino server for relay settings can result in being blacklisted and unable to send outbound SMTP messages to domains that use blacklist services.

In the Deny fields, an asterisk (*) prevents Domino from relaying messages to an external Internet domain from any external Internet hosts or IP addresses. You can also use an asterisk (*) to represent a subnet of an IP address. Any IP address or host listed in the "Allow messages to be sent only to the following external internet domains" field takes precedence over the "Deny messages to be sent to the following external internet domains" field.

Figure 1. SMTP Inbound Relay Controls



Any value in the "Allow messages only from the following internet hosts to be sent to external internet domains" field will take precedence over the "Deny messages from the following internet hosts to be sent to external internet domains" field. In previous releases of Domino, entries in the

Deny fields of the inbound relay controls take precedence over those in the Allow fields when a conflict exists.

If you want to convert back to the algorithm that release 5 uses, you need to configure the Notes.ini variable SMTPRelayHostsandDomains=value. The default value is 0. This variable forces servers to abide by Domino 5 rules to resolve conflicts between Allow and Deny list entries in the SMTP inbound relay controls.

- 0 - Entries in the Allow field of the SMTP inbound relay controls take precedence over entries in the Deny fields when there is a conflict between them. For example, given the following entries the host mail.ibm.com can always relay to any destination, including destinations in the domain lotus.com

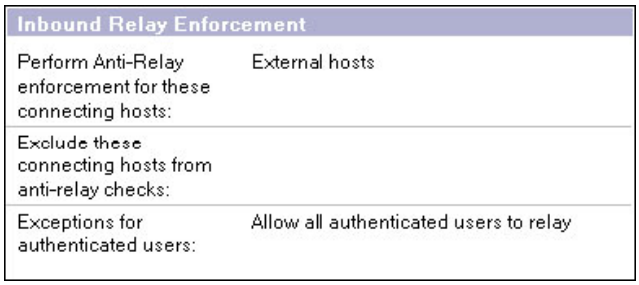
Deny messages to be sent to the following external internet domains	lotus.com
Allow messages only from the following internet hosts to be sent to external internet domains	mail.ibm.com

- 1 - Entries in the Deny fields of the SMTP inbound relay controls take precedence over entries in the Allow fields in the event of a conflict. Using the preceding example, if you deny relays to lotus.com, the host mail.ibm.com cannot relay to the denied domain.

Inbound relay enforcement

This section discusses advanced settings for relay controls. The following three fields specify additional SMTP relay settings shown in Figure 2.

Figure 2. SMTP Inbound Relay Enforcement



Perform Anti-Relay enforcement for these connecting hosts

This field specifies the connections for which the server enforces the inbound relay controls defined in the SMTP inbound relay controls shown in Figure 1. You need to choose one of the following settings:

- External hosts (default): The server applies the inbound relay controls only to hosts that connect to it from outside the local Internet domain. Hosts in the local Internet domain are exempt from anti-relay restrictions. The local Internet domain is defined by either a Global Domain document, if one exists, or as the Internet domain of the host server.
- All connecting hosts: The server applies the inbound relay controls to all hosts attempting to relay mail to external Internet domains.

- None: The server ignores the settings in the inbound relay controls. All hosts can always relay.

Exclude these connecting hosts from anti-relay checks
You can create an exceptions list containing the IP addresses or host names of systems that relay to any permitted domain. For each specified exception, the inbound relay controls are not enforced. Enter the IP addresses or host names of hosts to be exempted from the restrictions specified in the inbound relay controls section in Figure 1. When entering an IP address, enclose it within square brackets.

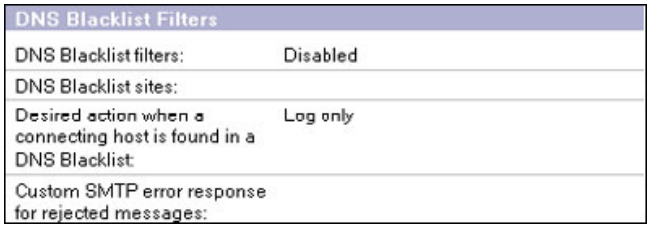
Exceptions for authenticated users
This field can be used to specify whether or not users who supply login credentials when connecting to the server are exempt from enforcement of the inbound relay controls. You must choose one of the following:

- Perform anti-relay checks for authenticated users: The server does not allow exceptions for authenticated users. Authenticated users are subject to the same enforcement as non-authenticated users.
- Allow all authenticated users to relay: Users who log in with a valid name and password are exempt from the applicable inbound relay controls. Use this to enable relaying by POP3 or IMAP users who connect to the network from ISP accounts outside the local Internet domain.

DNS blacklist filters

This section controls whether or not to use DNS blacklist filters as shown in Figure 3. If enabled, when Domino receives an SMTP connection request, it checks whether or not the connecting host is listed in the blacklist at the specified sites. If a connecting host is found on the list, Domino reports the event in a console message and in an entry to the Mail Routing Events view of the Notes Log. Both the console message and log entry provide the host name and IP address of the server as well as the name of the site where the server was listed. If Domino finds a match for a connecting host in one of the blacklists, it does not continue checking the lists for the other configured sites.

Figure 3. DNS Blacklist Filters



You can choose from a number of publicly available and private paid subscription services that maintain DNS blacklists. When using a public blacklist service, Domino performs DNS queries over the Internet. In some cases, it may take a significant amount of time to resolve DNS queries submitted to an Internet site. If the network latency of DNS queries made over the Internet results in slowed performance, consider contracting with a private service that allows zone transfer,

so that Domino can perform the required DNS lookups to a local host. During a zone transfer, the contents of the DNS zone file at the service provider are copied to a DNS server in the local network.

Each blacklist service uses its own criteria for adding servers to its list. Blacklist sites use automated tests and other methods to confirm whether a suspected server is sending out spam or acting as an open relay. The more restrictive blacklist sites add servers to their list as soon as they fail the automated tests and regardless of whether or not the server is verified as a source of spam. Other less restrictive sites list a server only if its administrator fails to close the server to third-party relaying after a specified grace period or if the server plays host to known spammers.

You can enter the text of the error message returned when denying a connection because it found the host in the DNS blacklist. The default error message indicates that the connection was denied for policy reasons. You can use the format specifier %s to specify the IP address of the denied host and the DNS blacklist site where Domino found the host listed.

For example, suppose you enter the following:

```
Your host %s was found in the DNS Blacklist at %s
```

When Domino denies a connection, it returns an error to the host in which it replaces the first %s with the IP address of the host and the second %s with the DNS blacklist site name. Thus, if you entered the text in the preceding example, a denied host receives an error such as:

```
Your host 127.0.0.2 was found in the DNS Blacklist at ibmdnsbl.mail-abuse.org
```

Desired action when a connecting host is found in a DNS blacklist
You must choose one of the following DNS blacklist settings:

- Log: When Domino finds that a connecting host is on the blacklist, it accepts messages from the host and records the host name and IP address of the connecting server and the name of the site where the server was listed in the server log.
- Log and tag message: When Domino finds that a connecting host is on the blacklist, it accepts messages from the hosts, the host name and IP address of the connecting server, and the name of the site where the server was listed and adds the note item, $DNSBLSite, to each accepted message. The value of a $DNSBLSite item is the blacklist site in which the host was found. Administrators can use the $DNSBLSite note item to provide custom handling of messages received from hosts listed in a blacklist.
- Log and reject message: When Domino finds that a connecting host is on the blacklist, it rejects the connection and returns a configurable error message to the host.

You can also gather statistics from the Domino Administrator or by using the SHOW STAT SMTP command from the server console. You can further expand the statistics to learn the number of times a given IP address is found on one of the configured DNSBLs. To collect the expanded information, you set the variable SMTPExpandDNSBLStats in the Notes.ini file on the server.

```
SMTPExpandDNSBLStats=value
```

Use this setting to generate DNS blacklist filter statistics for each connecting host found in a DNS blacklist site.

- 0 indicates that host-specific DNS blacklist filter statistics are not generated by the SMTP server.
- 1 indicates that the SMTP server generates host-specific DNS blacklist filter statistics that indicate the total number of hits per DNSBL site, per connecting host's IP address.

This Notes.ini setting applies to Domino servers. In the absence of this setting, the SMTP task maintains statistics that track the total number of connecting hosts that were found on the combined DNSBL of all sites combined as well as how many were found on the DNSBL of each configured site.

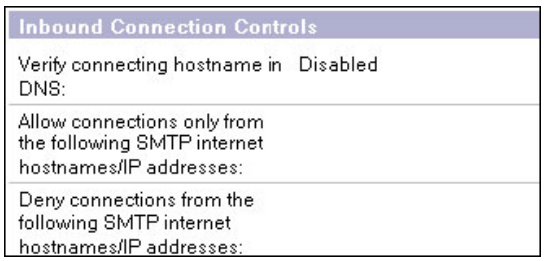
The variable `SMTPDebugSearchAllDNSBLSites=value` displays the total number of DNS blacklist hits for each site configured if you set the value to 1. The default value is 0. Do not leave this variable in all the time. It is good to calculate statistics against all configured blacklist sites.

Inbound connection controls

This section can be used to restrict hosts and IP addresses from connecting to your Domino server. You can configure Domino to do a reverse DNS lookup from any connecting host. This forces Domino to verify the name of the connecting host by performing a reverse DNS lookup. Domino checks DNS for a PTR record that matches the IP address of the connecting host to a host name. If Domino cannot determine the name of the remote host because DNS is not available or no PTR record exists, it does not allow the host to transfer mail.

You can also enter host names and/or IP addresses allowed to or denied from connecting to the SMTP service on this server as shown in Figure 4. Host name entries may be complete, as in the fully qualified host name of a particular server, or partial and imply the existence of a wildcard. For example, in the "Allow connections only from the following SMTP internet host names/IP addresses" field, if you enter ibm.com, Domino accepts only connections from mail hosts in the domains represented by *ibm.com, so it accepts all host names ending in ibm.com, including us.ibm.com and server.ibm.com. Domino rejects all other connection requests.

Figure 4. SMTP Inbound Connection Controls



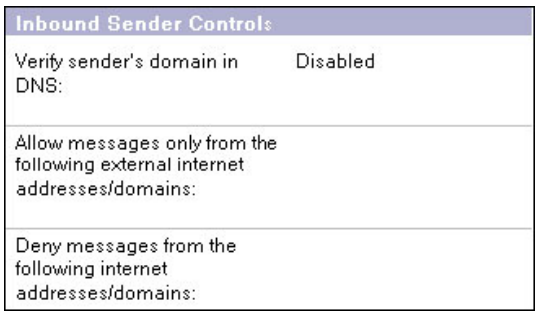
Inbound sender controls

This section is used to restrict the sender of inbound SMTP messages. You can enable reverse DNS lookups on the sender's domain as shown in Figure 5. If enabled, Domino verifies that the sender's domain exists by checking the DNS for an MX, CNAME, or an A record that matches the

domain part of the address in the MAIL FROM command received from the sending host. If no match is found, Domino rejects inbound mail from the host.

You can populate Internet addresses from which the server accepts or rejects messages. During the SMTP conversation, the Domino SMTP listener compares the address in the MAIL FROM command received from the connecting host with the entries in these fields.

Figure 5. SMTP Inbound Sender Controls



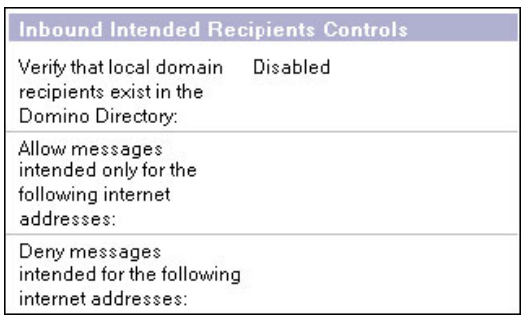
Inbound intended recipients controls

This section allows you to restrict the name of recipients for inbound SMTP messages. A very useful feature is the "Verify that local domain recipient exist in the Domino Directory" field. This specifies whether or not the SMTP listener checks recipient names specified in RCPT TO commands against entries in the Domino Directory. If enabled, the domain part of an address specified in an SMTP RCPT TO command matches one of the configured local Internet domains; the SMTP listener checks all configured directories to determine whether or not the specified recipient is a valid user. If all lookups complete successfully and no matching user name is found, the SMTP server returns a 550 permanent failure response indicating that the user is unknown:

```
550 bad_user@yourdomain.com ... No such user
```

Choosing this setting can help prevent messages sent to nonexistent users (for example, spam messages and messages intended for users who have left the organization) from accumulating in Mail.box as dead mail. To avoid messages from being rejected as a result of directory unavailability, Domino accepts messages when an attempted directory lookup does not complete successfully. Please refer to Figure 6 for more information.

Figure 6. SMTP Inbound Intended Recipients Controls



You can populate Internet addresses that are within the local Internet domain and that are allowed or denied the ability to receive mail from the Internet. You can also create a Notes group containing a list of addresses allowed to receive or reject mail from the Internet and enter the group name in this field.

NOTE: Some of the sections above have Allow messagesâ#¦ and Deny messagesâ#¦ fields. These fields are mutually exclusive. Any entry in the Deny messagesâ#¦ field will ignore the corresponding Allow messagesâ#¦ field.

Server mail rules

You can create content filtering rules for a server that define actions to take on certain messages. When a new message that meets a specified condition is deposited in Mail.box, Domino automatically performs the designated action. Rule conditions are based on content in the message headers or in the message body. By configuring a set of conditions and actions, you can customize rules to help block spam mail or intercept messages with questionable content. Except where a rule action explicitly indicates, Domino does not notify the sender or recipient if a rule prevents a message from reaching its destination.

If Mail.box receives an encrypted message (Notes encrypted, S/MIME, PGP, and so on), the server mail rules process any rule conditions that are based on unencrypted information in the message envelope, such as the sender, importance, and recipients, but do not process conditions based on the encrypted portion of the message body. Most rule conditions are based on information in the message envelope. The server does not log instances in which rules are unable to process a message.

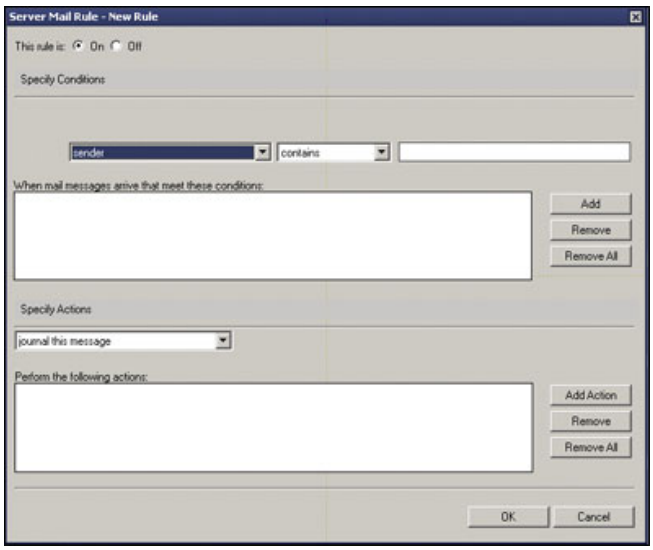
Domino stores the mail rules you create on the Configuration Settings document Router/SMTP - Restrictions and Controls - Rules tab. On startup, each server retrieves the mail rules from the appropriate Configuration Settings document and registers them as monitors on each Mail.box database in use. Whenever Mail.box receives a new message from any source, such as the SMTP process, the Router on another server, or a client depositing a message, the server evaluates the various message fields against the registered mail rules. Each message is evaluated only once.

Creating mail server rules

When you add a new rule, it takes effect only after the server reloads the mail rules. A reload is automatically triggered if the Server task detects a rule change when performing its routine check of the Configuration Settings document. This check occurs approximately every five minutes or can be reloaded from the Domino console.

When creating server mail rules, there are some factors that should first be considered. When multiple mail rules are enabled, you can set their relative priority by moving them up and down in the list. Try to place the most common words at the beginning of the rule so that if a condition is met it may not continue processing the remaining conditions in the rule. Don't search the body of the message unless it is really needed. Searching the body has the most impact on the server's CPU and memory and can cause undesired results on the performance of the Domino server. The maximum number of mail rules is 100, but can be adjusted with a Notes.ini variable.

Figure 7. New Rule dialog box



The first step in creating a server mail rule is to determine the message item to examine or to specify condition(s). You can choose from:

- Sender
- Subject
- Body
- Importance
- Delivery priority
- To
- CC
- BCC
- To or CC
- Body or subject
- Internet domain
- Size (in bytes)
- All documents
- Attachment name
- Number of attachments
- Form
- Recipient count
- Any recipient

Once you have the message item to examine, you need to set the logical operator or qualifier. You have the option to choose from:

- Contains (for text field values)
- Does not contain (for text field values)
- Is
- Is not
- Is less than (for numeric field values)

- Is greater than (for numeric field values)

You can also modify the server mail rule to add more conditions, such as And or Or. You can also add an exception to the server mail rule as an option.

The second step in creating a server mail rule is to specify the action to perform when a message arrives that matches the condition statement. Refer to Table A for the options to choose from.

Table A. Specify Actions for server mail rules.

Journal this message	The Router sends a copy of the message to the configured mail journaling database and continues routing the message to its destination. Journaling must be enabled on the Router/SMTP - Advanced - Journaling tab.
Move to database	The Router removes the message from Mail.box and moves it in the database specified in the accompanying text field, for example, junkmail.nsf. The specified database must already exist. The message is not routed to its destination. Placing messages in a junkmail database lets you examine them more closely for unwanted or other suspicious content.
Don't accept message	Domino rejects the message, but the Router does not generate a delivery failure report. Depending on the message source, the sender may or may not receive a nondelivery report (NDR) or other indication that the message was not sent. When Domino does not accept an incoming SMTP message, it returns an SMTP permanent error code to the sending server, indicating that the message was rejected for policy reasons. SMTP permanent errors (500-series errors) indicate error types that will recur if the sender attempts to send to the same address again Depending on the configuration of the sending client and server, the message originator may then receive a delivery failure report. For messages received over Notes routing, Domino returns a delivery failure report indicating that the message violated a mail rule. For messages deposited by a Notes client, the sending client displays an error indicating that the message violated a mail rule.
Don't deliver message	Domino accepts the message, but rather than sending it to its destination, it processes the message according to one of the following specified options: • Silently delete: Domino deletes the message from Mail.box with no indication to the sender or recipient. • Send NDR: Domino generates a nondelivery report and returns it to the sender. The MIME and Notes rich-text versions of messages sent from a Notes client result in separate delivery failure reports.
Change routing state	Domino accepts the message, but does not deliver it. Instead, it marks it as held, changing the value of the RoutingState item on the message to HOLD. This change to the routing state of the message causes the Router to retain the message in Mail.box indefinitely, pending administrative action to delete or release the held message.

Inbound SMTP commands and extensions

Lotus Domino supports some common ESMTP (Extended Simple Mail Transfer Protocol) commands and extensions. For the most part, most of these are configured through the Server Configuration Settings document under the Router/SMTP - Restrictions and Controls - Advanced - Commands and Extensions tab. Each ESMTP command is supported by a different Request For

Comment (RFC). Refer to Table B for the inbound ESMTP commands and extensions supported by the SMTP listener task.

Table B. Inbound SMTP commands and extensions

SIZE extension (RFC 1427)	• Enabled (default) - Domino declares its maximum message size to connecting hosts and checks the sending host's estimates of message size before accepting transfer. If the sender indicates that a message to be transferred is larger than the maximum size, Domino returns an error indicating that it will not accept the message • Disabled - Domino does not advertise its maximum message size or check inbound message size before transfer.
Pipelining extension (RFC 1854)	• Enabled (default) - Improves performance by allowing Domino to accept multiple SMTP commands in the same network packet. • Disabled - Domino does not accept multiple SMTP commands in a single packet.
DSN extension (RFC 3461))	• Enabled - Domino supports incoming requests to return delivery status notifications to the sender for failed, delayed, delivered, and relayed messages. Domino sends delay reports for low-priority messages held until the low-priority routing time to the sender of an SMTP message upon request. • Disabled (default) - Domino does not return delivery status notifications for SMTP messages. Domino will return failed DSNs.
8-bit MIME extension (RFC 1652)	• Enabled - Domino accepts 8-bit messages as is, allowing reception of unencoded multinational characters. • Disabled (default) - Domino requires inbound messages containing 8-bit characters to be sent using 7-bit ASCII encoding.
HELP command	• Enabled (default) - In response to the Help command, Domino displays a list of supported commands. • Disabled - Domino ignores the Help command.
VRFY command (RFC 821 section 3.3)	• Enabled - Domino accepts inbound requests to verify user names. • Disabled (default) - Domino denies requests to verify user names.
EXPN command (RFC 821 section 3.3)	• Enabled - Domino expands mailing lists or groups to show individual recipient names. • Disabled (default) - Domino does not expand lists and groups.
ETRN command (RFC 1985)	• Enabled - Domino accepts inbound "pull" requests from other SMTP hosts to transfer messages destined for the calling server. Enabling ETRN support allows for more efficient use of bandwidth resources by allowing a remote SMTP host to request pending messages at the same time it transfers messages to the Domino server. • Disabled (default) - Domino does not accept inbound "pull" requests from other SMTP hosts.
SSL negotiated over TCP/IP port (RFC 2487 and RFC 3207)	• Enabled - Domino supports the STARTTLS command, allowing it to create an encrypted SSL channel over the SMTP TCP/IP port. • Required - Domino accepts inbound SMTP connections over the TCP/IP port only from hosts that issue the STARTTLS command. • Disabled (default) - Domino does not allow secure SSL connections over the SMTP TCP/IP port. After accepting the STARTTLS command from a remote server, Domino uses settings for the server's SSL port to govern authentication for the sessions. For Domino to authenticate remote hosts that use the SMTP

	AUTH command, name and password authentication must be enabled for the Domino SSL port. We'll cover how to configure the server's SSL port in part two of this article series.

Conclusion

So far in this article series, we've covered SMTP settings in Domino that you can set in the Server Configuration Settings document, including inbound relay controls, blacklists, and inbound SMTP commands and extensions. We also discussed server mail rules and mail journaling, two more ways that you can weed out spam. In part two of our series, we cover Server document settings and Notes.ini variables that affect SMTP. Then we'll take a look at what you can expect in Lotus Notes/Domino 7.

Related topics

- Read Part 2 of this article series.
- For more about anti-spam controls, see the *LDD Today* articles, "Preventing spam mail in Notes/Domino 6" and "Notes spam mail filtering."
- You may also want to refer to the IBM Redbook, *Lotus Domino 6 spam Survival Guide*.
- Purchase Lotus books at discounted prices in the Lotus section of the Developer Bookstore.