Monitoring Microsoft Exchange Edge Transport Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

In Exchange 2007/2010, the Edge Transport server role is deployed in your organization's perimeter network as a stand- alone server or as a member server of a perimeter- based Active Directory domain. Designed to minimize the attack surface, the Edge Transport server handles all Internet-facing mail flow, which provides Simple Mail Transfer Protocol (SMTP) relay and smart host services for the Exchange organization. Additional layers of message protection and security are provided by a series of agents that run on the Edge Transport server and act on messages as they are processed by the message transport components. These agents support the features that provide protection against viruses and spam and apply transport rules to control message flow.

The message-processing scenarios that you can manage on the Edge Transport server role are described in the following sections.

- Internet Mail Flow

  Servers that run the Edge Transport server role accept messages that come into the Exchange 2007/2010 organization from the Internet. After the messages are processed by the Edge Transport server, they are routed to Hub Transport servers inside the organization. All messages that are sent to the Internet from the organization are routed to Edge Transport servers after the messages are processed by the Hub Transport server.

- Anti-Spam and Antivirus Protection

  In Exchange 2007/2010, the anti-spam and antivirus features provide services to block viruses and spam, or unsolicited commercial e-mail, at the network perimeter. Most viruses use spam-like tactics to gain access to your organization and to entice users to open an e-mail message. If you can filter out most of your spam, you are also more likely to capture viruses before they enter your organization.

  Spammers use a variety of techniques to send spam into your organization. Servers that run the Edge Transport server role help prevent users in your organization from receiving spam by providing a collection of agents that work together to provide different layers of spam filtering and protection.

- Edge Transport Rules

  Edge Transport rules are used to control the flow of messages that are sent to or received from the Internet. The Edge Transport rules help protect corporate network resources and data by

applying an action to messages that meet specified conditions. These rules are configured for each server. Edge Transport rule conditions are based on data, such as specific words or text patterns in the message subject, body, header, or From address, the spam confidence level (SCL), or attachment type. Actions determine how the message is processed when a specified condition is true. Possible actions include quarantine of a message, dropping or rejecting a message, appending additional recipients, or logging an event. Optional exceptions exempt particular messages from having an action applied.

- Address Rewriting

  You use address rewriting to present a consistent appearance to external recipients of messages from your Exchange 2007/2010 organization. You configure the Address Rewriting agent on the Edge Transport server role to enable the modification of the SMTP addresses on inbound and outbound messages.

If any of these critical services were to fail – for instance, say the Edge Transport server processes internet messages very slowly – it can cause significant delays in the delivery of important mails to specified recipients. In the world of business, such slip-ups are inexcusable, as prompt and effective email correspondence is essential to win orders and earn customer goodwill. Therefore, to prevent such adversities and their impact on corporate revenues, the Edge transport server will have to be monitored 24 x 7, and problems in its operations should be reported to administrators proactively. This can be achieved using eG Enterprise.

Chapter 2: How to Monitor Microsoft Exchange 2007/2010 Server with Edge Transport server role Using eG Enterprise

eG Enterprise adopts an agent-based approach to monitoring the Exchange 2007 and Exchange 2010 models and also those models that correspond to each of the Exchange 2007/2010 server with Edge Transport server role. The agent-based approach requires that you install and configure the eG agent on the Exchange 2007/2010 host (if one of the 'integrated' Exchange 2007 or Exchange 2010 models is being used) or on the host on which the server role to be monitored exists.

This internal agent, once started, periodically runs a wide variety of tests on the Exchange 2007/2010 server/server with Edge Transport server role to extract useful performance data. Some of these tests , namely – the Exchange Mailbox Status test, the Exchange Storage Group test, and the Exchange Queue Stats test – require **Exchange Administrator** privileges to execute. Therefore, prior to monitoring an Exchange 2007/2010 server/Edge Transport server role role using eG Enterprise, make sure that you configure the eG agent to run with the privileges of an **Exchange Administrator**. Once you assigned the privileges, manage the Microsoft Exchange Edge Transport Server using the eG administrative interface. The procedure for achieving this is discussed in Section **2.1**.

2.1 Managing the Microsoft Exchange Edge Transport Server

The eG Enterprise cannot automatically discover the Microsoft Exchange Edge Transport Server. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a Exchange Edge Transport Server component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Microsoft Exchange Edge Transport* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

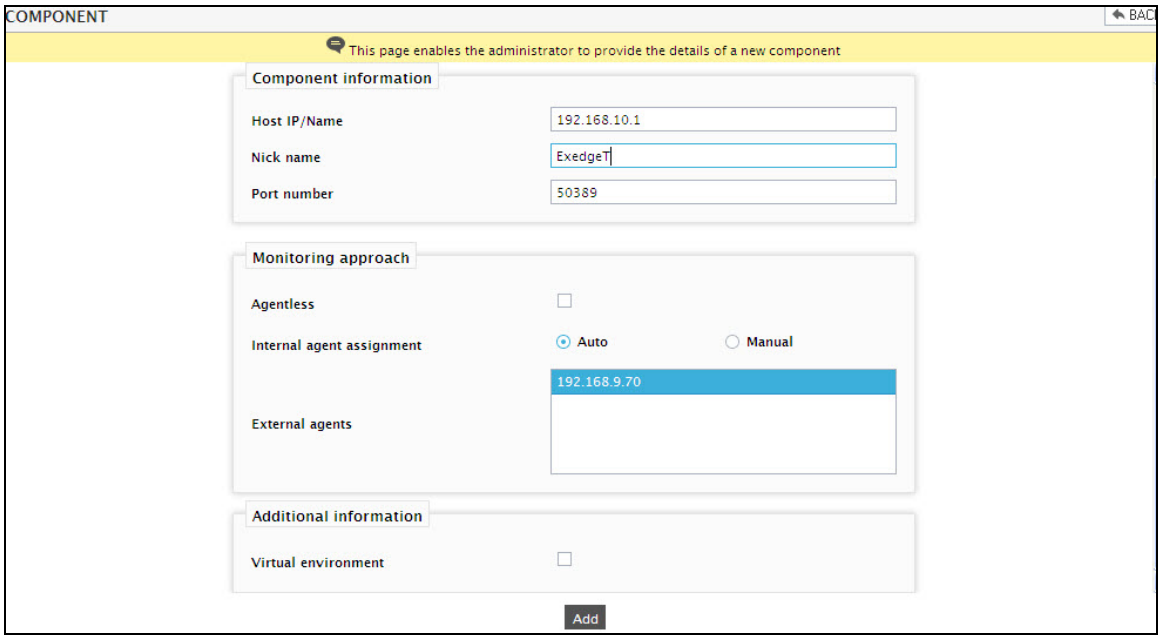

Figure 2.1: Adding an Exchange Edge Transport server

4. Specify the **Host IP** and the **Nick name** of the Exchange Edge Transport Server in Figure 2.1.
5. The **Port number** will be set as *50839* by default. If the server is listening on a different port in your environment, then override this default setting.
6. Now, click on the **Add** button in Figure 2.1 and sign out of the eG administrative interface.

Chapter 3: Monitoring the Microsoft Edge Transport Servers

eG Enterprise offers a specialized Microsoft Exchange Edge Transport model that provides real-time insights into the performance of Edge Transport servers.

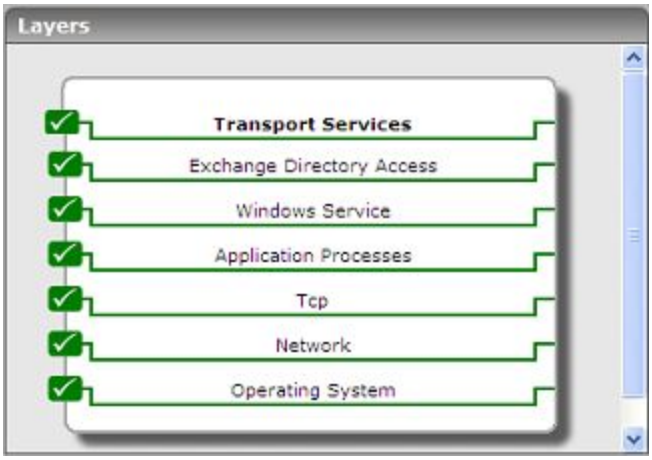

Figure 3.1: Layer model of the Microsoft Exchange Edge Transport server

Every layer of Figure 3.1 reports a wide variety of statistics that enable administrators to quickly find answers to the following critical performance queries:

- Is the Active Directory cache adequately sized to handle requests from the Edge transport server?
- search requests to any domain controller fail owing to a bad network link or the non-availability of the domain controller?
- Were any LDAP fatal errors experienced while communicating with a domain controller?
- Did too many bind calls to any domain controller fail?
- Is any domain controller responding too slowly to read and search requests?
- Is the server experiencing processing bottlenecks? Are there any lengthy message queues on the server? If so, which ones?
- How effective is the Recipient filter agent? How many requests per second were rejected by the Recipient Lookup and Recipient Block List data sources?
- How successful is the Sender Filter agent in evaluating and filtering out "suspect" senders?
- Is the Sender ID agent efficient?

- Has the Edge Transport server experienced latencies while connecting to the Exchange store? Which store interface can this delay be attributed to?
- How many messages are available in the delivery queue? Is the number very high?
- Do too many messages exist in the retry queue?
- Are too many messages awaiting delivery to an external recipient?
- Have messages been queued in the Unreachable queue?
- Does the poison queue contain messages?
- How efficient is Connection Filter agent? How many connection requests were rejected by the agent? Which data store used by the agent rejected the maximum requests - the IP Block list providers, IP allow list providers, or the IP Allow/Block lists defined by administrators?
- Were any spams detected by the content filter agent?
- Were any local/remote senders blocked by the Protocol Analysis agent?

The sections to come discuss the top 2 layers of Figure 3.1, as the remaining layers have already been dealt with in the *Monitoring Unix and Windows Servers* document.

3.1 The Exchange Directory Access Layer

The computer that has the Edge Transport server role installed does not have access to the Active Directory directory service. All configuration and recipient information is stored in the Active Directory Application Mode (ADAM) directory service. To perform recipient lookup tasks, the Edge Transport server requires data that resides in Active Directory. EdgeSync is a collection of processes that are run on a computer that has the Hub Transport server role installed to establish one-way replication of recipient and configuration information from Active Directory to the ADAM instance on an Edge Transport server. The Microsoft Exchange EdgeSync service copies only the information that is required for the Edge Transport server to perform anti-spam configuration tasks and the information about the connector configuration that is required to enable end-to-end mail flow. The Microsoft Exchange EdgeSync service performs scheduled updates so that the information in ADAM remains current.

The tests mapped to this layer measure the health of the interactions between the Active Directory and the Edge Transport server.

Figure 3.2: The tests mapped to the Exchange Directory Access layer

Both these tests have been dealt with elaborately in *Monitoring Microsoft Exchange Mailbox Server* document. Therefore, let us proceed to discuss the topmost layer – the **Transport Services** layer.

3.2 The Transport Services Layer

The tests linked to this layer monitor the effectiveness of the critical services offered by the Edge Transport server.

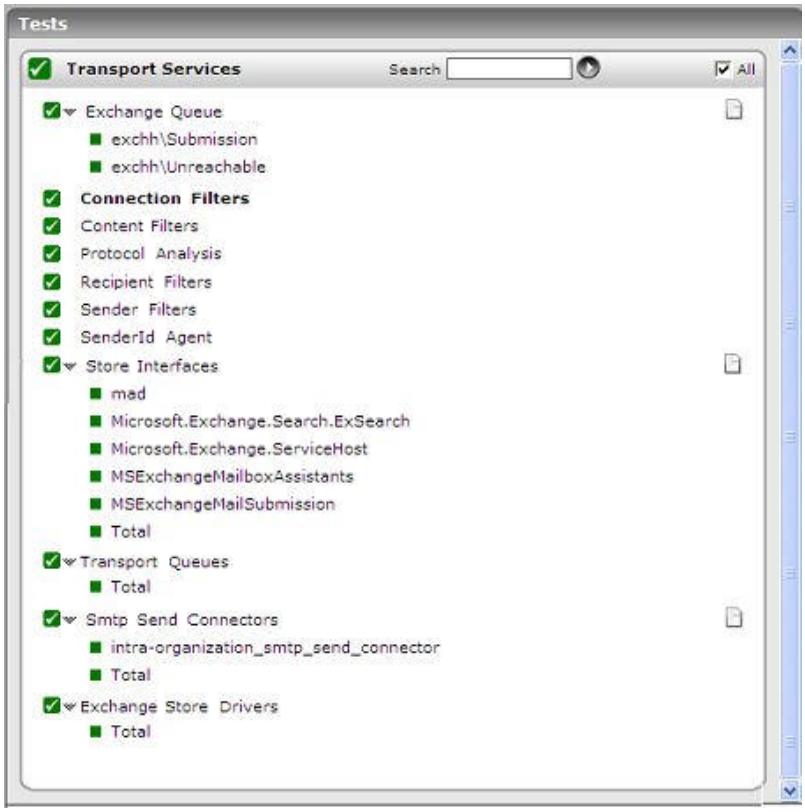

Figure 3.3: The tests mapped to the Transport Services layer

Since most of these tests are common to both the Edge Transport and Hub Transport servers, *Monitoring Microsoft Exchange Hub Transport Server* document provides the details of the common tests. The sections to come therefore, discuss the tests that are specific to the Edge Transport server alone.

3.2.1 Connection Filters Test

The Connection Filter agent is an anti-spam agent that is enabled on computers that have the Microsoft Exchange server 2007/2010 Edge Transport server role installed. The Connection Filter agent relies on the IP address of the remote server that is trying to connect to determine what action, if any, to take on an inbound message. The remote IP address is available to the Connection Filter agent as a by-product of the underlying TCP/IP connection that is required for the Simple Mail Transfer Protocol (SMTP) session

When you enable the Connection Filter agent, the Connection Filter agent is the first anti-spam agent to run when an inbound message is evaluated. When an inbound message is submitted to an Edge Transport server on which the Connection Filter agent is enabled, the source IP address of the SMTP connection is checked against any of the following data stores of IP addresses:

- Administrator-defined IP Allow lists and IP Block lists
- IP Block List providers
- IP Allow List providers

You must configure at least one of these data stores of IP addresses for the Connection Filter agent to be operational.

The source P address is first compared to the administrator-defined IP Allow list and IP Block list. If the IP address does not exist on either the administrator-defined IP Allow list or IP Block list, the Connection Filter agent queries the IP Block List provider services according to the priority rating that is assigned to each provider. If the IP address appears on the IP Block list of an IP Block List provider, the Edge Transport server waits for and parses the RCPT TO header, responds to the sending system with an SMTP 550 error, and closes the connection. If the IP address does not appear on the IP Block lists of any one of the IP Block List providers, the next agent in the anti-spam chain processes the connection.

This test monitors the connection filtering agent's activities to reveal the number of connection requests/inbound messages that are in various stages of filtering.

Target of the test : A server configured with the Edge Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Edge Transport server.
Port	The port number of the Edge Transport server. By default, this is *50389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Connections to IP block list providers	Indicates the number of connections to the IP Block List providers during the last measurement period.	Number	IP Block List provider services compile lists of IP addresses from which spam has originated in the past. Additionally, some IP Block List providers provide lists of IP addresses for which SMTP is configured for open relay. There are also IP Block List provider services that provide lists of IP addresses that support dial-up access. You can configure multiple IP Block List provider configurations by using the Exchange Management Console or the Exchange Management Shell. When you configure the Connection Filter agent to use an IP Block List provider, the Connection Filter agent queries the IP Block List provider service to determine whether a match exists with the connecting IP addresses before the message is accepted into the organization. The value of this measure indicates the number of connections that the filtering agent has established with the IP Block List provider service to perform such queries.

Measurement	Description	Measurement Unit	Interpretation
			When you use the Connection Filter agent, it is a best practice to use one or more IP Block List providers to manage access into your organization. However, there may be some disadvantages to using an IP Block List provider. Because the Connection Filter agent must query an external entity for each unknown IP address, outages or delays at the IP Block List provider service can cause delays in the processing of messages on the Edge Transport server. In extreme cases, such outages or delays could cause a mail-flow bottleneck on the Edge Transport server. The other disadvantage of using an external IP Block List provider service is that legitimate senders are sometimes added to the IP Block lists of IP Block List providers by mistake. Legitimate senders can be added to the IP Block lists that are maintained by IP Block List provider as the result of an SMTP misconfiguration, where the SMTP server was unintentionally configured to act as an open relay is an example of such a misconfiguration.
Connections to IP allow list providers	Indicates the number of connections on the IP Allow List providers during the last measurement period.	Number	IP Allow lists are sometimes referred to as IP safe lists or "white" lists elsewhere in the software industry. IP Allow List providers maintain lists of IP addresses that are definitively known not to be associated with any spam activity. When an IP Allow List provider returns an IP Allow match, which indicates that the sender's IP address is more likely to be a reputable or "safe" sender, the Connection Filter agent

Measurement	Description	Measurement Unit	Interpretation
			relays the message to the next agent in the anti-spam chain. The value of this measure indicates the number of connections the filtering agent has established with an IP allow list provider for checking whether the source IP address exists therein.
Connections to IP block list	Indicates the number of connections on the IP Block List during the last measurement period.	Number	By using administrator-defined IP Allow lists and IP Block lists, you can configure connection filtering to support the following scenarios: • To exempt IP addresses from the IP Block lists of IP Block List providers: You may have to exempt IP addresses from the IP Block lists of IP Block List providers when legitimate senders are unintentionally put on an IP Block List provider's IP Block list. For example, legitimate senders could be unintentionally put on an IP Block list when an SMTP server was unintentionally configured to act as an open relay. In this scenario, the sender will probably try to correct the misconfiguration and remove their IP address from the IP Block List provider's IP Block list. For more information about IP Block List providers, see "IP Block List Providers" later in this topic. • To deny access from IP addresses

Measurement	Description	Measurement Unit	Interpretation
			that are a source of unsolicited e-mail messages but are not found on an IP Block List provider's IP Block lists: Sometimes, you may receive a large quantity of unsolicited messages from a source that was not yet identified by a real-time block list (RBL) service to which you subscribe.
Connections to IP allow list	Indicates the number of connections on the IP allow list during the last measurement period.	Number	

3.2.2 Content Filters Test

Content filtering provides another tool to help manage the flow of messages entering and exiting your business's mail stream. Content filtering enables you to filter messages by using a variety of filtering tools. These include:

- **Sender-domains filtering (for Realtime and Manual scan jobs):** Sender-domains filtering enables you to filter messages from particular senders or domains.
- **Subject line filtering (for Realtime and Manual scan jobs):** Subject line filtering enables you to filter messages based on the content of the subject line of the message.
- **Filter set templates (simplify the creation and management of file and content filters on all scan jobs)**: Filter set templates can be created for use with any Forefront Security for Exchange Server scan job. A single filter set template can be associated with any or all of the scan jobs and administrators can also create multiple filter set templates for use on different servers or different scan jobs.

The Content Filter agent is the last filter to scan inbound messages. While doing so, the Content Filter agent uses Microsoft SmartScreen technology to assess the contents of the messages and to assign a **spam confidence level (SCL)** rating to each message. By comparing the SCL threshold configuration with the assigned SCL rating, the content filter feature takes a specific action on a specific message, such as rejecting a message or deleting a message.

This test monitors the operations of the Content Filtering agent, reports the count of messages that have been assigned various SCL ratings, and also reveals the action the filter has taken on the messages.

Target of the test : A server configured with the Edge Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Edge Transport server.
Port	The port number of the Edge Transport server. By default, this is *50389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Messages at Spam Control Level 0	Indicates the number of messages that were assigned a spam confidence level (SCL) rating of 0 during the last measurement period.	Number	Messages with an SCL rating of 0 are considered less likely to be spam.
Messages at Spam Control Level 1	Indicates the number of messages assigned a spam confidence level (SCL) rating of 1 during the last measurement period.	Number	Higher the SCL rating, greater is the likelihood of the message to be spam.
Messages at Spam Control Level 2	Indicates the number of messages assigned a spam confidence level (SCL) rating of 2 during the last measurement period.	Number	Higher the SCL rating, greater is the likelihood of the message to be spam.
Messages at Spam Control Level 3	Indicates the number of messages assigned a spam confidence level (SCL) rating of 3 during the last measurement period.	Number	Higher the SCL rating, greater is the likelihood of the message to be spam.
Messages at Spam	Indicates the number of	Number	Higher the SCL rating, greater is the

Measurement	Description	Measurement Unit	Interpretation
Control Level 4	messages assigned a spam confidence level (SCL) rating of 4 during the last measurement period.		likelihood of the message to be spam.
Messages at Spam Control Level 5	Indicates the number of messages assigned a spam confidence level (SCL) rating of 5 during the last measurement period.	Number	Higher the SCL rating, greater is the likelihood of the message to be spam.
Messages at Spam Control Level 6	Indicates the number of messages assigned a spam confidence level (SCL) rating of 6 during the last measurement period.	Number	Higher the SCL rating, greater is the likelihood of the message to be spam.
Messages at Spam Control Level 7	Indicates the number of messages assigned a spam confidence level (SCL) rating of 7 during the last measurement period.	Number	Higher the SCL rating, greater is the likelihood of the message to be spam.
Messages at Spam Control Level 8	Indicates the number of messages assigned a spam confidence level (SCL) rating of 8 during the last measurement period.	Number	Higher the SCL rating, greater is the likelihood of the message to be spam.
Messages at Spam Control Level 9	Indicates the number of messages assigned a spam confidence level (SCL) rating of 9 during the last measurement period.	Number	Messages with an SCL rating of 9 are considered more likely to be spam.
Messages quarantined	Indicates the number of messages that were quarantined during the last measurement period.	Number	Quarantined messages are typically sent to the spam quarantine mailbox that you specified.
Messages scanned	Indicates the number of messages that were scanned for viruses during the last measurement	Number	

Measurement	Description	Measurement Unit	Interpretation
	period.		
Messages rejected	Indicates the number of messages that were rejected during the last measurement period.	Number	If the connection filter rejects a message, it sends sends an SMTP error response to the sending server.
Messages deleted	Indicates the number of messages that were deleted during the last measurement period.	Number	For deleted messages, the computer that has the Edge Transport server role installed sends a fake "OK" Simple Mail Transfer Protocol (SMTP) command to the sending server and then deletes the messages. Because the sending server assumes that the message was sent, the sending server does not retry to send the message in the same session.
Messages with SCL unknown	Indicates the number of messages that could not be scanned by the filter during the last measurement period.	Number	Ideally, this value should be 0.
Messages that bypassed scanning	Indicates the number of messages that bypassed scanning during the last measurement period.	Number	Forefront Security for Exchange Server can be configured to only scan file attachments that are more likely to contain viruses. It does this by first determining the file type and then by determining whether that file type can be infected with a virus. Determining the file type is accomplished by looking at the file header and not by looking at the file extension. This is a much more secure method because file extensions can be easily spoofed. This check increases Forefront Security for Exchange Server performance while making sure that no potentially infected file attachments pass without being scanned. If you would like Forefront Security for Exchange Server to

Measurement	Description	Measurement Unit	Interpretation
			bypass scanning for file types that are not commonly known to be capable of carrying a virus, set the registry key ScanAllAttachments to 0.

3.2.3 Protocol Analysis Test

The Protocol Analysis / Sender Reputation agent is an anti-spam agent that is enabled on computers that are running Exchange 2007/2010 that have the Edge Transport server role installed. The Sender Reputation agent can block messages according to many characteristics of the sender. The Sender Reputation agent relies on persisted data about the sender to determine what action, if any, to take on an inbound message.

The **Sender Reputation Level (SRL)** is a number between 0 and 9 that predicts the probability that a specific sender is a spammer or malicious sender. A value of 0 indicates that the message is not likely to be spam. A value of 9 indicates that a message is likely to be spam. You can configure the threshold for sender blocking by SRL. This SRL block threshold defines the SRL value that must be exceeded for sender reputation to block a sender. If a message is equal to or greater than the SRL block threshold, that sender will be added to the IP Block list from 0 to 48 hours. The default is 24 hours.

This test monitors the activities of the Sender Reputation agent and reveals how many senders were blocked for what reason.

Target of the test : A server configured with the Edge Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Edge Transport server.
Port	The port number of the Edge Transport server. By default, this is *50389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Senders processed	Indicates the number of senders who were scanned for reputation level during the last measurement period.	Number	
Senders blocked due to a local open proxy	Indicates the number of senders who were blocked because of a open local proxy check during the last measurement period.	Number	One of the characteristics that sender reputation evaluates is the result of a test for open proxy servers. Frequently, spammers route messages through open proxy servers on the Internet. By routing spam through open proxy servers, spammers can send messages that appear to originate from a different server than their own. A non-zero value for this measure indicates that that one/more senders were blocked because a local open proxy server was detected.
Senders blocked due to a remote open proxy	Indicates the number of senders who were blocked because of a remote open proxy check during the last measurement period.	Number	One of the characteristics that sender reputation evaluates is the result of a test for open proxy servers. Frequently, spammers route messages through open proxy servers on the Internet. By routing spam through open proxy servers, spammers can send messages that appear to originate from a different server than their own. A non-zero value for this measure indicates that that one/more senders were blocked because a remote open proxy server was detected.
Senders blocked due to local sender reputation level	Indicates the number of senders who were blocked because of local sender	Number	A high value for this measure indicates that many local senders violated the

Measurement	Description	Measurement Unit	Interpretation
	reputation level (SRL) threshold violation during the last measurement period.		reputation level threshold. If the number is unreasonably high, you might want to review your SRL block threshold configuration. By default, the SRL threshold value is 7. Use caution when you set the SRL threshold. A threshold that is too low may unintentionally block legitimate senders. A threshold that is too high may not block malicious senders or spammers.
Senders blocked due to remote sender reputation level	Indicates the number of senders who were blocked because of remote sender reputation level (SRL) threshold violation during the last measurement period.	Number	A high value for this measure indicates that many remote senders violated the reputation level threshold. If the number is unreasonably high, you might want to review your SRL block threshold configuration. By default, the SRL threshold value is 7. Use caution when you set the SRL threshold. A threshold that is too low may unintentionally block legitimate senders. A threshold that is too high may not block malicious senders or spammers.

3.2.4 SMTP Send Connectors Test

SMTP Send connectors are configured on computers that are running Microsoft Exchange server 2007/2010 and that have Hub Transport and Edge Transport server roles installed. The Smtp Send Connector represents a logical gateway through which outbound messages are sent.

Using this test, you can periodically observe the traffic conducted by the Send connectors.

Target of the test : A server configured with the Edge Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each send connector supported on the Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Edge Transport server.
Port	The port number of the Edge Transport server. By default, this is *50389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current SMTP connections	Indicates the current number of outbound connections from the SMTP Send connectors.	Number	
Messages sent	Indicates the number of messages received by the SMTP Send connector each second.	Msgs / Sec	This is a good indicator of the load on the Send connector.
Data send in SMTP messages	Indicates the number of bytes sent per second.	KB/Sec	This is a good indicator of the load on the Send connector.
Recipients per message – average	Indicates the average recipients per message handled by this SMTP Send connector.	Recipients/Msg	
Data transferred per connection - average	Indicates the average number of bytes sent via this connector per connection.	KB/Conn	
Messages per connection – average	Indicates the average number of message bytes per outbound message sent.	Msgs/Conn	

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.