v7.6 Release Notes for Websense Email Security Gateway

Topic 70005 / Updated: 28-Apr-2011

Applies To:	Websense Email Security Gateway v7.6 Websense Email Security Gateway Anywhere v7.6

This release of Websense® TRITON™ Enterprise introduces Websense Email Security Gateway, an important addition to the Websense Web, Data, and Email Security solution set. Email Security Gateway provides maximum protection for email systems to prevent malicious threats from entering an organization's network and protect sensitive data from unauthorized email transmission.

Email Security Gateway provides comprehensive on-premises email security hosted on a Websense V-Series appliance (V10000 G2 and V5000 G2). Each email message is scanned by a robust set of antivirus and antispam filters to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email. Inbound, outbound, and internal email policies can be applied to specified sets of senders and recipients. Data loss prevention policies are used to scan mail and attachments so that valuable company data is not mishandled.

The value of Email Security Gateway is apparent as soon as the module is opened. A Today page displays data collected since midnight of the current day, showing the total message volume processed and the number of messages blocked by Email Security. System alerts covering the same period of time are readily available. Up to 4 status charts may be selected for display, summarizing email activity at a glance. The History page provides similar statistics for the previous 30-day period.

A subscription to Websense Email Security Gateway Anywhere adds support for a hybrid service pre-filtering capability "in the cloud," which scans incoming email against a database of known spam. This feature can save network bandwidth and maintenance costs by dropping spam before it ever reaches an organization's network.

Integration with Websense Data Security provides valuable protection for an organization's most sensitive data. Policies configured in the Data Security module can detect the presence of sensitive data and block the release of that data. Data Security can also determine whether a message should be encrypted and pass the message to an encryption server.

A URL scanning capability is added to the Email Security filtering arsenal if you include integration with Websense Web Security.

Logging and reporting capabilities allow a company to view system status and generate reports of system and email traffic activity.

A Personal Email Manager facility allows authorized end users to manage email messages that Email Security policy has blocked but that may be safe to deliver. End users can maintain individual Always Block and Always Permit lists of email addresses to simplify message delivery.

For instructions on downloading the TRITON - Email Security management server software, see the TRITON Unified Security Center online Help.

Access the following Deployment and Installation Center locations for instructions on installing and deploying Websense Email Security v7.6 in your network:

Click here for information about Websense V10000 G2 installation.

Click here for information about Websense V5000 G2 installation.

Use these Release Notes to find information about Version 7.6 Email Security Gateway features and system support. For a detailed description of Email Security functions, see the TRITON - Email Security Online Help. Personal Email Manager User Help contains the information end users need to manage their blocked email.

Contents

Features

Topic 70006 / Updated: 28-Apr-2011

Applies To:	Websense Email Security Gateway v7.6 Websense Email Security Gateway Anywhere v7.6

The following Email Security Gateway features are described in this section:

- *Appliance clustering*
- *Personal Email Manager*

TRITON integration

With this release, Email Security Gateway joins a suite of Web and Data Security modules in Websense TRITON Enterprise. The Web Security, Data Security, and Email Security modules are displayed in a single user interface, the TRITON Unified Security Center console. Appliance management, LDAP user directory specification, and administrator creation are controlled in the TRITON console. Availability of individual Web, Data, and Email Security modules depends on the subscription key used.

Users access the TRITON console with a single login to manage the functionality provided by the Web Security, Data Security, and Email Security modules. For information on the TRITON console, see the TRITON Unified Security Center Help.

Hybrid service integration

A subscription to Email Security Gateway Anywhere includes the hybrid service "in the cloud" pre-filtering capability. The hybrid service prevents malicious email traffic from entering a company's network by:

- Dropping a connection request based on the reputation of the IP address of the request
- Scanning inbound email against a database of known spam and viruses, and dropping any message that matches a database entry

The hybrid service may also share spam and virus detection information by writing extended headers in the mail it sends to Email Security Gateway. The additional header information includes a spam/virus detection "score," which Email Security then uses to determine message disposition.

You must mark the **Use hybrid service scanning results** check box on the **Main** > **Filters** > **Add Filter** or **Edit Filter** page to enable hybrid service spam/virus scoring. This option is visible only when the hybrid service is configured and running. When hybrid service spam/hybrid scoring is not enabled, Email Security Gateway performs its own antispam and antivirus scans.

The hybrid service does not provide a detailed log of the messages it drops. However, users can generate reports in Email Security Gateway showing the total number of messages processed and dropped by the hybrid service (**Main** > **Status** > **Presentation Reports**). Today and History page charts (**Main** > **Status** > **Today** or **History**) summarize hybrid service message volume and size.

Data Security integration

Integration with Websense Data Security ensures that Data Security email policies for acceptable use, data loss prevention, and encryption of sensitive information are enforced. Email Security Gateway is a control point for policies that are configured and managed by the Data Security module. See TRITON - Data Security Online Help for information about configuring Data Security policies.

Acceptable use policies ensure compliance with corporate rules for business and appropriate language and data content in email. Email Security Gateway uses the acceptable use policies to block or quarantine email based on content. Data loss prevention policies detect and secure sensitive data that may be transmitted in email.

Data Security policies can detect email that should be encrypted and return that information in the message header to the Email Security Gateway encryption server.

Reliable policy-based message routing

Email Security Gateway delivers a feature-rich content-filter framework for on-premises email scanning and routing capabilities. Use Email Security Gateway to designate IP addresses of trusted clients whose mail is not subject to some scanning operations. Define domains and IP address groups, and configure policy-based routing for email traffic.

Domain and IP address groups can be used in other Email Security functions like user authentication and message encryption options.

Email Security Gateway lets you define policies that are applied to specified sets of email senders and recipients. You can create policies for different sets of users in your organization and apply a different set of rules in each policy. Data Security acceptable use and data loss prevention policies are defined in the Data Security module.

Policy rules comprise the filters and filter actions that determine how a message that matches a policy's sender/recipient conditions is handled. Filters provide the basis for email scanning for viruses and spam, and filter actions determine the final disposition of a message that triggers a particular filter.

An email content policy configured in the Data Security module may specify that a message should be encrypted for delivery. Users can specify 1 of the following types of encryption for Email Security Gateway to use:

- Transport Layer Security (TLS) negotiated between a client and server
- Third-party application encryption. Third-party encryption software must support the use of x-headers to communicate with Email Security.

A third encryption option, using the hybrid service, may be selected in the **Settings > General > Encryption** page, but this service will not be available until later in Spring 2011. This option can only be selected if the hybrid service is configured and enabled.

Email Security Gateway also uses a comprehensive set of inbound and outbound configuration settings to determine how messages and connections are handled. Configuration settings include effective inbound connection control, directory harvest attack detection and blocking, appropriate mail relay definitions, and delivery control. Messages that Email Security cannot process due to processing errors can be held in a delayed messages queue for subsequent delivery attempts.

Antivirus and antispam filters

When the hybrid service is not configured as a pre-filter, Email Security Gateway antivirus scanning analyzes all email content and attachments for the presence of viruses and threats. The antivirus filter is a combination of Websense content classification analytics and an Authentium antivirus engine.

The antispam filter is composed of a collection of tools. Digital fingerprinting scans email against a database containing the latest digital fingerprints unique to spam. Email Security Gateway also uses the LexiRules antispam filter to analyze email for the words, phrases, and patterns commonly found in spam. Heuristics scanning can identify possible characteristics of spam in message headers and content.

Email Security Gateway can use Websense Web Security URL scanning for more accurate and efficient spam detection. In order to block email messages that contain URLs or IP addresses relating to, for example, a gambling Web site, Email Security Gateway relies on the Web Security module, which maintains an updated URL database from the Websense download server.

A message that triggers an antivirus or antispam filter is handled based on the action defined for the individual filter. The message may be delivered, dropped, or isolated in a specific quarantine folder based on the filter action configuration. Blocked messages are held in quarantine queues to await administrator or end-user action. Email Security provides default quarantine queues, along with the capability for an administrator to define new queues.

Reporting and logging

The Email Security Gateway log database receives system health and message traffic data, which it uses to generate reports. The Today and History dashboards display this information in system and email status and activity charts, providing a graphical picture of the value of Email Security Gateway to users. Users can select up to 4 summary charts for display on either the Today or History dashboard screen.

The **Main** > **Status** > **Presentation Reports** page enables users to generate various reports of system and email activity from predefined report templates. Some of these reports can be customized to suit specific needs. For example, message data may be sorted by hour, day, week, month, or calendar quarter. Generate a report immediately or schedule it to be automatically generated and delivered at specified intervals. Reports can be generated in PDF, HTML, or Excel formats.

The Email Security report catalog includes the following general report types:

- Overall message summary
- Inbound message summary
- Outbound message summary
- Data Security message summary
- Spam and virus summary
- Message transfer summary
- System capacity

In addition, Email Security Gateway provides the following logs on the **Main** > **Status** > **Logs** page:

- Message log for a running record of received email messages
- Audit log to record any administrator changes to Email Security Gateway configuration settings
- System log to record system level events such as a reboot or database update
- Console log to record Email Security Gateway changes in the TRITON Unified Security Center

Appliance clustering

Email Security Gateway offers support for multiple-appliance clusters, each of which has 1 primary appliance and 1 or more secondary, or auxiliary, appliances. The Email Security Gateway cluster provides real-time synchronization between the primary appliance and all secondary appliances in a cluster. Configuration settings for a secondary appliance can be accessed only from its designated primary appliance.

Log events for a cluster are centrally stored and reporting is aggregated across all machines. All quarantined email messages can be stored locally in each Email Security Gateway appliance or remotely on an external storage device. Either way, the data can be accessed from the same interface(s).

Appliances in a cluster must all be of the same platform: all V10000 G2 or all V5000 G2, not a mix of the 2 platforms. Platform versions must also match in a cluster.

Applications deployed on appliances in a cluster must be the same. For example, all appliances in a cluster are Email Security only appliances, or they all have Websense Web Security Gateway in addition to Email Security.

Appliances in a cluster should also have the same message queue configurations. Messages in a secondary appliance queue may be lost if that queue is not configured on the primary machine before the cluster is created.

Personal Email Manager

Email Security Gateway includes an effective tool for end-user email management. Personal Email Manager enables designated end users to manage their own blocked email. Authorized users can choose to deliver, delete, forward, or view blocked email messages. A user may also add the sender's address to a personal Always Block or Always Permit list to control access from those senders. See Personal Email Manager User Help for information about this end-user facility.

Personal Email Manager end-user control is configured the Email Security Gateway management interface. An administrator can determine the contents of the message notifying an end user about blocked mail, and control whether that user can maintain personal lists of email addresses that are either always blocked or always permitted.

Operating tips

Topic 70007 / Updated: 28-Apr-2011

Applies To:	Websense Email Security Gateway v7.6 Websense Email Security Gateway Anywhere v7.6

This article includes some operating tips for TRITON - Email Security.

Network date/time

Email Security Gateway components must all be located in the same time zone and be synchronized to the same time. The affected components include:

- Email Security Gateway V-Series appliance
- Email Security Gateway management server
- Email Security Gateway log server
- SQL Server database

Hybrid service registration

Hybrid service registration needs to be completed on a single Email Security appliance. The registration process cannot be started on 1 appliance and continued on another appliance.

After you have completed the registration on 1 appliance, that registration is applied to all other appliances listed with the Email Security management server.

Data Security registration in a cluster

The following tips apply if you want to deploy data loss prevention policies in an Email Security appliance cluster:

- Before you deploy Data Security policies, ensure that the Email Security cluster is established and that all the appliances are registered with the Data Security management server. If you deploy Data Security policies while an appliance registration is in progress, the registration will not complete.
- Ensure that all cluster appliances are configured to use the same communication IP address for Data Security registration.

Requirements

Topic 70008 / Updated: 28-Apr-2011

Applies To:	Websense Email Security Gateway v7.6 Websense Email Security Gateway Anywhere v7.6

Email Security Gateway is supported on the Websense V-Series appliance only (V10000 G2 or V5000 G2). The TRITON management server and Email Security Log Server are hosted on a separate Windows Server machine. Microsoft SQL Server is used for the Email Security log database. Click here for a detailed list of TRITON system requirements.

Embedded Help updates

Topic 70009 / Updated: 28-Apr-2011

Applies To:	Websense Email Security Gateway v7.6 Websense Email Security Gateway Anywhere v7.6

This article contains late-breaking additions and clarifications to the TRITON - Email Security online Help.

Delayed messages queue

The Explain This Page option in the Help menu displays the “Viewing a blocked message in a queue” Help topic for the Delayed Messages queue page. For information about viewing a message in the Delayed Messages queue, see the TRITON - Email Security Online Help topic titled “Viewing a delayed message.”

Known issues

Topic 70010 / Updated: 28-Apr-2011

Applies To:	Websense Email Security Gateway v7.6 Websense Email Security Gateway Anywhere v7.6

A list of known issues for Websense Email Security Gateway is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, the link above takes you to a login prompt. Log in to view the list.