How to Most Effectively Filter Spam in Email Security Gateway

A vital component of any email security system is the effective prevention of spam from entering your network. Websense Email Security Gateway includes several tools that together provide effective spam filtering in email messages. This article describes these tools and how to use them to optimize Email Security antispam scanning functions.

The following Email Security Gateway tools may be used for preventing spam:

- *Websense email spam filter*
- *Hybrid service scanning*
- *Connection control settings*
- *Global always block/always permit lists*
- *Data Security email DLP policy attributes*

For optimal antispam scanning, we recommend you use all these tools.

Spam that still bypasses a fully configured email deployment is likely the result of a new spamming strategy. We encourage you to forward a copy of that spam to Websense for analysis and possible inclusion in the anti-spam database (spam@websense.com).

You can also use the Trusted IP Address Group component to tune Email Security Gateway email filtering. See *Trusted IP address group* for more information.

Websense email spam filter

Topic 70016 / Updated: 04-October-2011

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

The Websense email spam filter is an important tool for preventing spam from invading your email system. The following components are combined in the spam filter. They are enabled by default on the **Main > Policy Management > Filters** page for adding or editing a spam filter type.

- URL scanning, which accesses the Websense Web Security URL scanning database for accurate URL spam detection
- Digital Fingerprint scanning, which checks email content for any digital fingerprints of known spam
- LexiRules scanning, which analyzes email content for word patterns commonly found in spam
- Heuristics scanning, which checks message headers and content for spam characteristics.

The URL scanning option on the Add/Edit Filter page allows you to select the URL categories you want detected. Four categories are selected by default (Adult/Sexually Explicit, Gambling, Websense Security Filtering, and Hacking). We recommend you select all categories for maximum antispam scanning.

You can also set the sensitivity level for heuristics scanning. Default setting is Medium, the recommended setting for this option.

To optimize scanning, you should ensure all these tools are enabled.

Making sure the antispam databases are up-to-date is a critical consideration. You should verify that regular spam filtering database downloads are scheduled in the **Settings > General > Database Downloads** page. You can also force an immediate update on this page by clicking **Update Now** for the listed antispam databases.

Hybrid service scanning

Topic 70017 / Updated: 04-October-2011

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

The email hybrid service performs in-the-cloud message scanning to prevent spam from entering your email system. Hybrid service analyzes all incoming email and blocks any message that it recognizes as spam.

Hybrid service must be registered and running before you activate its antispam filtering capabilities. Register the hybrid service via the configuration wizard at **Settings > General > Hybrid Configuration**. After a successful hybrid service registration, ensure that the **Use hybrid service scanning results** option is selected on the **Main > Policy Management > Filters** page for the Websense antispam filter type.

Mail that hybrid service allows into the system for processing includes a header that contains a scanning result score. If the **Use hybrid service scanning results** check box is marked (**Main > Policy Management > Filters**, Spam Filter page), Email Security uses this score to determine how to handle the message. If that score exceeds a specified spam threshold, Email Security treats the message as spam and handles it according to applicable policy. In this case, Email Security Gateway does not perform its own, separate antispam scanning.

Connection control settings

Topic 70018 / Updated: 04-October-2011

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

The Connection Control page in the Email Security Gateway management server interface contains options that can help to filter email spam: real-time blacklist (RBL) and Websense reputation service. An RBL is a third-party published list of IP addresses that are known sources of spam. When RBL checking is enabled, messages from a sender listed on a user-specified RBL are prevented from entering your system. The Websense reputation service classifies email senders based on past behavior and allows Email Security to block mail from known spam senders.

Ensure that the RBL option is enabled on the **Settings > Inbound/Outbound > Connection Control** page, and specify up to 3 RBLs you want Email Security Gateway to use. This option is not enabled by default.

Enable the Websense reputation service on the **Settings > Inbound/Outbound > Connection Control** page, and select the scanning level for blocking email messages. This option is enabled by default, with a scanning level setting of "conservative" (block mail from addresses that send spam 100% of the time).

Global always block/always permit lists

Topic 70019 / Updated: 04-October-2011

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

Maintaining lists of IP and email addresses that are either always blocked or always permitted can contribute to the efficiency of your Email Security Gateway system. Bandwidth and time can be saved when known spam-sending addresses can be blocked and trusted mail can bypass the system's spam and virus scanning features.

Maintain the Email Security Gateway global Always Block and Always Permit lists on the **Main > Policy Management > Always Block/Permit** page. Add addresses of known spammers or other sources whose email you do not want in your system to the Always Block List. Known legitimate addresses that might otherwise be blocked as spam can be included in the Always Permit List.

Data Security email DLP policy attributes

Topic 70020 / Updated: 04-October-2011

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

Data Security email data loss prevention (DLP) policy settings can enhance antispam scanning in Email Security. Email DLP policy's acceptable use attribute provides various dictionaries against which message content can be scanned (Data Security module **Main > Policy Management > DLP Policies > Email DLP Policy** page**)**. If any message content matches an unacceptable use dictionary entry, the mail is blocked.

You can use the Data Security **Main > Policy Management > Content Classifiers > Patterns & Phrases** attribute to modify dictionary entries if necessary by excluding terms and phrases from policy detection.

Trusted IP address group

Topic 70021 / Updated: 04-October-2011

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

Trusted IP addresses can be added to the Trusted IP Addresses default group, which allows mail from those addresses to avoid some inbound email filtering. Specifically, mail from trusted IP addresses bypasses the following Email Security filtering:

- All message controls except message size limitations (**Settings > Inbound/Outbound > Message Control**)
- Recipient validation (**Settings > Users > User Authentication**)
- All connection controls (**Settings > Inbound/Outbound > Connection Control**)
- Directory harvest attacks (**Settings > Inbound/Outbound > Directory Attacks)**
- Relay controls (**Settings > Inbound/Outbound > Relay Control**)

By default, a Trusted IP Addresses group is defined in the Email Security management server interface, but it contains no entries (**Settings > Inbound/Outbound > IP Groups)**.