Perimeter Checks

The Hermes SEG Perimeter Checks page allows you to set settings for any incoming email before they are even processed by the SMTP server or the rest of the subsystems such as the virus and spam filters . You can think of perimeter checks as a type of "front door" checks before they are processed by the system.

NOTE: This section requires any changes to be applied by clicking the Apply Settings button on the bottom of the page.

Initial Connection Deep Protocol Tests

The Initital Connection Deep Protocol Tests are comprised of the following 3 tests:

- **Pipeline Detection** - Detects senders that send multiple commands, instead of sending one command at a time and waiting for Hermes SEG to reply.
- **Non SMTP Commands Detection** - Detects senders that try to use non-SMTP commands
- **Bare New Line Detection** - Detects usage of newline that are not proceded by carriage returns, e.g., a bare line.

If they are all enabled they are very useful in refusing SMTP connections by zombie senders. However, this setting introduces a delay (graylisting) in email delivery and certain legitimate but incorrectly configured email servers do not try to reconnect to deliver their email. If you have problems receiving emails from legitimate servers, you should first attempt to permit the sending email server(s) under **Content Checks --> IP & Network Override** which will configure Hermes SEG to bypass Initial Connection Deep Protocol Tests on the server(s) IPs you specify. Hermes SEG comes pre-configured to bypass Initial Connection Deep Protocol Tests on certain email services such as Exchange Online and Outlook.com.

Require HELO

If enabled, this setting requires for the incoming email system to start the SMTP session by first sending the HELO or EHLO command before sending the MAIL FROM or ETRN command. Set this setting to Disabled if it starts creating problems with certain homegrown email systems. Otherwise, it is recommended to be set to Enabled (Figure 2).

Reject Unauthorized Domain

If enabled, this setting will reject any incoming email that is destined for a recipient domain or subdomain thereof that the system does not handle i.e. any domain that is not listed in the Relay Domains (See General Options Above). It is recommended that this settings is set to Enabled.

Sender Policy Framework (SPF) Checks

Enable/Disable SPF checks on the system. When enabled the system will attempt to identify email spam by detecting whether or not the email is spoofed by verifying that the sender IP address is authorized to send email on behalf of the senders domain.

Reject Invalid HELO Hostname

If enabled, this setting will reject any incoming email from a mail server that sends the HELO or EHLO command along with a malformed hostname. It is recommended that this settings is set to Enabled. For best effect of this setting, ensure the Required HELO setting above is also set to Enabled.

Reject Pipelining

If enabled, this setting will reject any incoming email from a mail server that sends SMTP commands where it is not allowed or without waiting for confirmation that the system supports ESMTP commands. This is used by spammers in order to try to speed up delivery of spam email. It is recommended that you set this setting to Enabled.

Reject Non-FQDN Sender Domain

If enabled, this setting will reject any incoming email from a mail server without a FQDN (Fully Qualified Domain Name). Example of a Non-FQDN domain would be: domain.local. It is recommended that you set this setting to Enabled.

Reject Invalid Sender Domain

If enabled, this setting will reject any incoming email from a mail server whose domain as sent in the MAIL FROM command during the SMTP session does not have a DNS A or MX record or has an invalid MX record. It is recommended that you set this setting to Enabled.

Reject Non-FQDN Recipient

If enabled, this setting will reject any incoming email destined for a recipient without a FQDN (Fully Qualified Domain Name) as sent in the RCPT TO command of the SMTP session. It is recommended that you set this setting to Enabled.

Reject Invalid Recipient Domain

If enabled, this setting will reject any incoming email where this system is not the final destination and the email is destined for a recipient domain as specified in the RCPT TO command of the SMTP session that does not have a DNS A or MX Record or an invalid MX record. It is recommended that you set this setting to Enabled.

Realtime Block/Allow Lists Threshold Score

This is the score required for the system to block an incoming mail server’s IP address that has been listed on Real Time Block/Allow List(s). The final outcome of combining the weights of the Real Time Block/Allow Lists must be less than the number specified below in order for the incoming mail server to be allowed to deliver mail to this system. Realtime Block/Allow Lists are configured under **Content Checks --> RBL Configuration**.

Message Size Limit

Enter the maximum message size in MB (Megabytes) to be processed by the system. Please note, the larger the limit the more memory required by the system to process the e-mail. Extremely large message sizes can crash the system. Recommended size is 20 MB or lower.

Revision #1
Created 2021-01-02 13:58:12 UTC by Dino Edwards
Updated 2021-01-03 12:53:17 UTC by Dino Edwards