Secure Gateway

Micro Focus® Secure Gateway monitors and blocks illicit images, pornographic images, and inappropriate videos on your messaging system. This solution is an add-on for Micro Focus Secure Gateway that scans the actual composition of images and videos to ensure accuracy. Its sophisticated probability engine scans incoming and outgoing images, reliably distinguishes between pornographic and non-pornographic content, and stops the inappropriate content from entering or leaving your messaging system.

The Problem

Inappropriate email communications, including pornography and other explicit content, continue to be a major problem in many organizations. This content is often found in unsolicited spam, but it is more commonly generated from employee communications, both inside and outside of the workplace. If these messages go unchecked, organizations could face a number of devastating consequences that can cost time and money:

- Sexual harassment lawsuits
- Criminal charges
- A hostile work environment
- Reputation damage

The Micro Focus Solution

Organizations must address this inappropriate behavior through corporate policies and through the use of technology. Secure Gateway gives you the ability to monitor and block pornographic images, which addresses the primary issue of inappropriate communications.

Secure Gateway screens images before they pass through your email system and takes action when offensive material is detected. It uses sophisticated analytical processes consisting of multiple detection methods to reliably distinguish between pornographic and non-pornographic content, without having to rely on a signature database of pre-categorized content. These processes ensure that pornography is prevented from entering or leaving your messaging system.

CONFIGURE IMAGE ANALYSIS AUDITING

Follow these instructions to set Secure Gateway into an audit mode. In audit mode, you will locate the images that are passing through your email system. You can use audit mode without interfering with the mail flow.

PREREQUISITES

To use Secure Gateway, you must have the following items:

- A pre-installed Micro Focus Secure Gateway server that is configured and actively scanning email
- An Secure Gateway license key. Either a full license or trial key will work. (Contact your Micro Focus representative for your evaluation key.)

Step 1: Install the License Key

To install the Secure Gateway license key:

1. Browse to the Licensing section of the administration console.
2. Click Browse to locate and select the license file.
3. Click Install. Once the license is installed, you can start to use the image analysis tools.
**Step 2: Enable Secure Gateway**
The option you choose to enable for the Secure Gateway depends on the complexity of your Secure Gateway installation. In the example below, the Secure Gateway server has been configured to scan inbound and outbound mail with separate policies. If you want to audit more than one policy, complete these steps for each policy that needs to be monitored.

**ENABLE SECURE GATEWAY FOR INBOUND MAIL**
1. Browse the Scanner Management tree to locate your policy.
2. Open up the Scanning Configuration options to locate the Secure Gateway page.
3. Select Enable Image Analysis.
4. Select Quarantine for Administrator.
5. Leave all of the other settings at their default values.
6. Save your changes.

By setting these options, images that have strong indicators of offensive material (Threshold=75) will trigger the scanner to perform the defined actions. In the case of auditing, the message won’t be blocked, but the system will keep a copy for the administrator to review.

It’s also worth noting the image size settings of 100x100 pixels. This sets the minimum size of images that will be scanned. Anything below this size is unlikely to contain objectionable content and should be ignored to prevent a reduction in system performance (images below this size are generally going to be content such as email signature images).

**Step 3: Collect Data**
Your Secure Gateway server will now be collecting data for review. Depending on your system, you may want to give Secure Gateway a few days to collect enough data to be useful. To verify that the system is working, you can either send a message through the system with an image that would be considered objectionable, or you can temporarily adjust the Threshold to zero (0) and send an image through. Once you’ve sent an image, check the results as defined in the next section.

**Step 4: Review Data**
Once Secure Gateway has collected messages that exceed the Secure Gateway threshold, review the data.
1. Open the Secure Gateway Quarantine and log in as the System Administrator.
2. In the Search panel, click Show Advanced.
3. Select the following options from the search panel:
   - **Block state**: Blocked flag not set
   - **Limit to these events**: Secure Gateway
   - **Message age**: Adjust this as necessary

By selecting these options, messages that were not delivered to the end users due to other filters such as the anti-spam scanner will be ignored during the search. You will be reviewing only the messages that ended up in the recipients’ mailboxes.
4. Click Search to list the items that were detected with Secure Gateway. This action generates a results list of all of the captured items and the basic details of each item to determine the senders and recipients of the potentially offensive material.

**Getting Results**
Secure Gateway helps ensure that your organization is protected from inbound and outbound pornographic images.