Whitelist in CISCO Secure Email Gateway

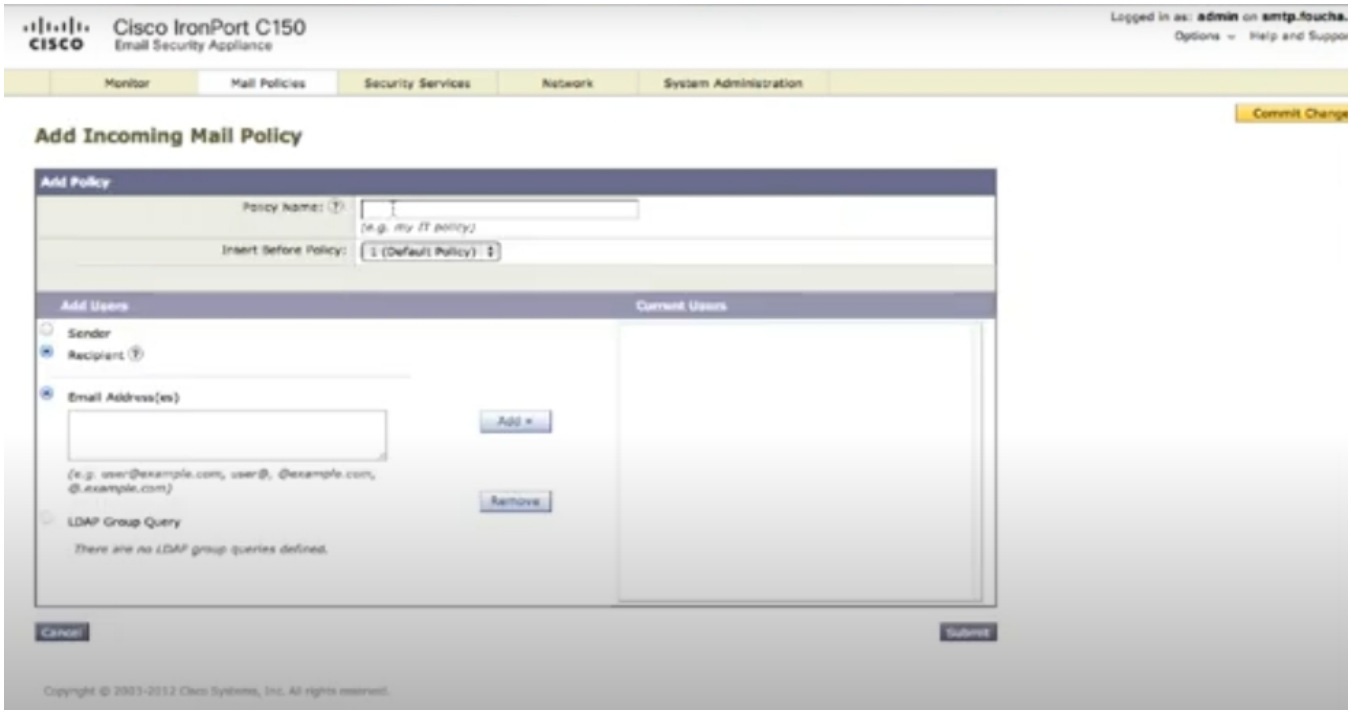
If you're using Cisco Secure Email Gateway spam filtering, you can whitelist CyTech to allow our simulated phishing test emails and training notifications through to your end users.

The instructions below include information from the Cisco whitelisting article. If you run into issues whitelisting CyTech in Cisco Secure Email Gateway, we recommend reaching out to Cisco for specific instructions. You can also contact our support team whenever you need assistance.

Whitelisting Cisco Secure Email Gateway

To whitelist CyTech in Cisco Secure Email Gateway, do the following:

1. From the Cisco Secure Email Gateway admin console, navigate to the **Incoming Mail Policies** tab.

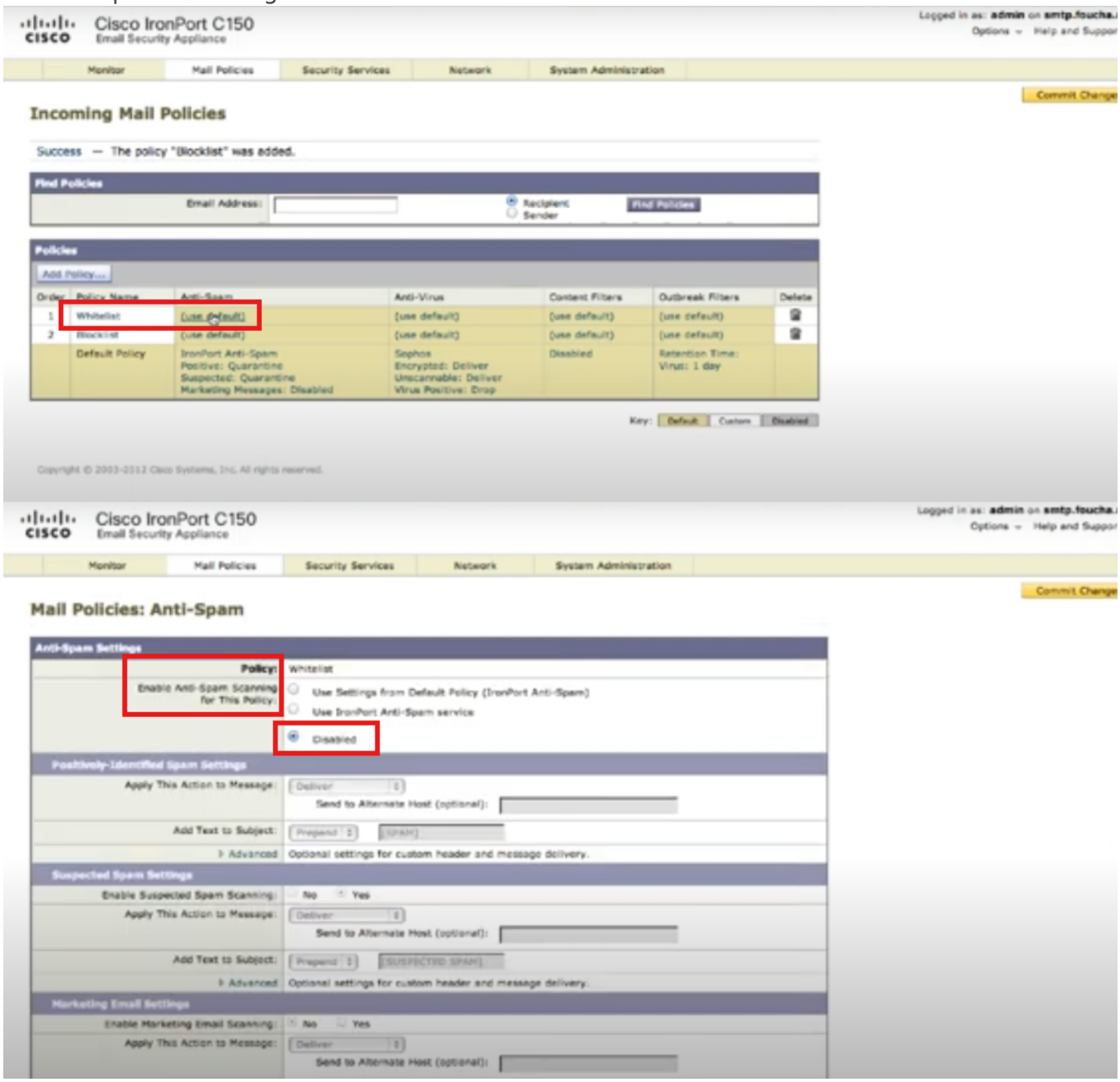


2. Select **HAT Overview**. Please ensure that **InboundMail lister** is selected.
3. Click **WHITELIST**. If you do not see **WHITELIST**, you can create your own group named "WHITELIST".
4. Click **Add Sender** and add our domains. **Note:** Contact CyTech for the list of domain names.
5. Click **Submit** and then **Commit Changes**.

Note: After following this article, we recommend setting up a test phishing campaign to 1-2 users to ensure your whitelisting was successful. As a last resort, we suggest reaching out to your service provider for assistance.

Disable Spam Scanning

To disable spam scanning in Cisco Secure Email Gateway, do the following:

1. From the Cisco Secure Email Gateway admin console, navigate to the **Incoming Mail Policies** tab.
2. Click **WHITELIST**. If you do not see **WHITELIST**, you can create your own group named "WHITELIST".
3. Disable Spam Scanning for the whitelisted
4. 

Skipping Outbreak Filter Scanning

The instructions above for whitelisting Cisco Secure Email Gateway do not prevent Secure Email Gateway's Outbreak Filter from scanning emails from our IPs or domain names. If you are experiencing issues with our emails being quarantined, you may also need to set our IPs or hostnames to bypass this filter.

To skip Outbreak Filter Scanning, do the following:

1. From your Cisco Secure Email Gateway admin console, navigate to the **Incoming Mail Policies** tab.
2. Under the **Message Modification** section, enter our IP addresses or domain names in the **Bypass Domain Scanning** table. **Note:** Contact CyTech for the list of IPs or domain names.
3. Click **Submit** and then **Commit Changes**.

Troubleshooting

If Cisco Secure Email Gateway is flagging CyTech's simulating phishing emails as spam or removing attachments from these emails, you may need to troubleshoot further in Cisco Secure Email Gateway.

For a potential troubleshooting method, see the steps below. If you don't see the solution you're looking for, we recommend reaching out to Cisco Ironport for assistance.

1. Create an individual **HAT Mail Flow Policy** specifically for CyTech.
2. In this policy, disable **Spam Detection** and **Virus Protection**. For more information, see Cisco Ironport's Mail Flow Policy documentation.
3. Add a sender group for our IP addresses or hostnames. **Note:** Contact CyTech for the list of IPs or hostnames.
4. Apply the policy to the sender group. For more information, see Cisco Ironport's Message Handing documentation.

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #6
Created 5 December 2024 07:17:11 by David Napoleon Romanillos
Updated 11 December 2024 13:06:16 by Aldion Pueblos