White Paper

Using Email Security to Protect Against Phishing, Spam, and Targeted Attacks: Combining Features for Higher Education

Online criminals are constantly looking for new ways to reach their targets—for instance, hijacking an organization's email accounts and cloaking themselves behind the host's good reputation, then using those phished credentials to create mass spam campaigns and steal users' account, financial, and personal information. Although there are a number of important security concerns for Higher Education, this is a common concern in higher education. Although data breaches are on a downward trend for higher education, they can be costly. The data breach at the Virginia Commonwealth University (VCU) in November 2011 compromised 176,567 records and could cost the university nearly $20 million.[1] Targeted attacks can lead to such breaches or worse. Institutions often find themselves under credential-phishing attacks and fighting blacklisting. This paper details the security features that can be combined to fight this serious problem.

Background

Students and faculty have a wide variety of experience when it comes to email and online security, making it difficult to provide a consistent level of education around identifying authentic communications from the institution. A higher level of protection is needed to keep phishing and directed or targeted attack messages out of users' inboxes, and a secondary set of features is needed to limit the damage from future attacks and from credentials that attackers already have.

A comprehensive email security solution should:

- Prevent incoming phishing attacks
- Help educate end users so they can recognize spam or phishing email
- Stop outbound spam
- Rate-limit outbound email without impacting systems and faculty members who send large volumes of email as part of their job duties
- Alert email administrators when rate limits are hit to allow for early investigation and remediation

The features in Cisco Email Security needed are:

- Outbreak filters
- Prepended disclaimers for outbreak filters
- Outbound anti-spam scanning

[1] Daily Open Source Infrastructure Report, U.S. Department of Homeland Security, March 14, 2012.

- Rate limit per mail-from
- Administrative alert messages

Combining these features allows the organization to create layered protection, including reinforcement of policies with end users around what the organization does and does not do via email.

Feature Descriptions

Outbreak Filters, new in Cisco AsyncOS® 7.5 for Cisco Email Security, combat low-volume directed and/or targeted attacks. They can rewrite URLs in suspicious emails and redirect the URLs through a Cisco Internet proxy server backed by the power of Cisco. Cisco Email Security also includes the ability to prepend customizable disclaimers above the body text of an email to remind users of the organization's email policy—for example, never asking for user IDs or passwords via email.

Outbound Anti-Spam Scanning in the Cisco Email Security Outbound software subscription allows administrators to filter spam being sent from compromised accounts. Cisco's flexible licensing allows user licenses for anti-spam scanning to be used to scan both inbound and outbound email flows.

Rate Limiting per Mail-From, new in AsyncOS 7.6, sets limits to the number of emails a user can send over a specified time period. Once the limit is hit, the outbound flow of messages is stopped; a hard stop is also placed on compromised accounts flooding spam outbound. An **alert message** can also be configured to be sent to a specific administrator or helpdesk email account once the limit is hit. An **Exception List** allows certain senders, whether human or automated systems, to bypass the rate limiting—for example, to send necessary bulk emails.

Large Spam Message Scanning, new in AsyncOS 7.5, raises the limits on what can be scanned to detect and stop spam. One way spam authors try to circumvent anti-spam scanning is by creating large messages. The Large Spam Message Scanning feature raises the default limit for "Always Scan" to 512 KB and sets an upper maximum of 1 MB for "Never Scan." Messages between these two size limits are partially scanned by Cisco Anti-Spam.

Task 1: Configure Outbreak Filters on the Incoming Mail Policy

These settings are configured on the incoming mail policies.

1. Log on to the Email Security Appliance using an account with the appropriate permissions.
2. Click *Mail Policies* > *Incoming Mail Policies*.
3. Under the desired policy, click the hyperlink *Retention Time*: *Virus 1 day*.

This will bring up the page for configuring Outbreak Filters settings.

4. Check the box for *Enable Message Modification*.

Note: If the Enable Message Modification box is not checked, then only the Virus Outbreak Filter functionality will be enabled. This box MUST be checked for the new URL rewrite capabilities to be enabled.

5. Click *Enable only for unsigned messages*.

This is purely a policy decision, but be aware that if you enable URL rewrite for all messages, then you will break signatures on signed messages.

6. In the *Bypass Domain Scanning* box, enter any domains that URL rewriting should be bypassed for. This could include business partners.

Be careful when using this feature. Bypassing URL rewriting for a domain could result in malicious messages from compromised machines coming into your network.

7. Choose the *System Generated* threat disclaimer and click to preview it.

Using custom threat disclaimers is a policy decision. These disclaimers can be created using the *Mail Policies > Text Resources* configuration option. Variables that pull information from the email can be added to the custom disclaimer to make a more powerful impact on the end user. Language and URLs can be added to bring the disclaimer in line with your corporate policies.

8. Click to *Submit*, then to *Commit* the changes.

Task 2: Verify Large Spam Message Scanning

Verify that the defaults for Large Spam Message Scanning have not been changed. Lowering these defaults could have a negative effect on efficacy.

1. Open *Security Services > Cisco Anti-Spam*
2. Verify the following *Message Scanning Thresholds*:
   a. Always scan messages smaller than: 512 KB.
   b. Never scan messages larger than: 1 MB.

The system will partially scan messages that are between the Always Scan setting (512 KB by default) and the Never Scan setting (1 MB by default).

Task 3: Configure Outbound Anti-Spam Scanning

Cisco's flexible licensing allows for Anti-Spam scanning (and Cisco Virus Defense, along with others) to be used for inbound scanning, outbound scanning, or both, without the customer incurring additional licensing costs. While most customers would not use outbound scanning, it is useful for contractual obligations such as not sending spam to business partners, as well as for keeping infected machines from causing your organization to be placed on email blacklists.

This should be modeled in a lab environment first; at a minimum, you should review the loading on the appliances before configuring Outbound Anti-Spam Scanning to ensure the devices are not overloaded. A message filter can be used to send a partial copy of production email flows to a lab environment and then slowly ramp up to understand the impact.

1. Open *Mail Policies > Outgoing Mail Policies*.
2. Under the appropriate policy, click to modify the *Anti-Spam* settings.
3. Enable *Anti-Spam Scanning for This Policy: Use Cisco Anti-Spam service*.

There are some additional controls that you will need to set according to your policy needs. This includes what to do with Positively-Identified Spam and Suspected Spam.

4. Click *Submit* and *Commit* your changes. The Outgoing Mail Policy page should now show Cisco Anti-Spam as being configured on the chosen policy.

Task 4: Enable Rate Limit per Mail-From and Create Both an Exception List and an Administrative Alert for the Limiting

The Rate-Limit per Mail-From feature allows you to configure time-range-based limits on the number of emails users may send. Using the Exception List feature, exceptions can be made for users that send out large amounts of email based on job requirements. This enables outbound marketing, customer support, and other parts of the organization to do their work without being limited while monitoring and catching anomalies that are signs of compromised hosts.

To minimize the configuration time this takes, the Exception List should be created before setting any limits on email senders.

1. Open *Mail Policies* > *Address Lists*.
2. *Add Address List* using the email addresses or wildcard addresses you wish to not have rate-limited.

These addresses can be a complete address or a partial one (@.example.com, for example, which would match for all subdomains such as @dc1.example.com, but not match on @example.com). Another good example of email addresses to exclude would be for the organization's executives.

3. Click *Submit*, but do NOT click *Commit*.

Once the Exception List(s) have been created, the rate limiting can be configured.

4. Open *Mail Policies* > *Mail Flow Policies*.
5. Click to open *RELAYED*.

Many different settings can be changed on this page. Please refer to the product documentation to understand what each setting does. Do not change anything on this page without the proper understanding, as it can have a negative effect on the organization's mail flow.

6. Scroll down to the Mail Flow Limits section and click to expand *Rate Limit for Envelope Senders*.
7. Set the *Max. Recipients Per Time Interval* to the desired number of recipients in 60 minutes.

This is the number of emails you wish to allow users to send outbound in a 60-minute period. Setting this too low could impact user productivity. Too high would allow too many unwanted emails to be sent if an account was compromised.

Note: Changing the time period is done under the Default Policy Parameters. The default for this and for the entire predefined policies list is *Unlimited*. If the time period is changed under the Default Policy, it will be changed for ALL policies in the Host Access Table (HAT); this may impact mail flows. If you wish to change the rolling time period on the default policy, you should ensure that the other mail flow polices that were previously set to Unlimited by default before are reset to it afterwards.

8. Under Exceptions, choose the configured Address List from under the *Ignore Rate Limit for Address List*: pull-down menu.

9. *Submit* the changes, but do not *Commit* them yet.

The next steps are to configure the administrative alert. This alert will be sent if the configured rate limit has been reached. If it has, you will need to investigate to determine if a machine is compromised and sending spam, or if a user has hit the limit but should be excluded based on job duties.

10. Open *System Administration* > *Alerts*.
11. *Add* an Alert Recipient's email address and set the alert type of *System* with a level of *Info*.

> Quick Tip: Set up a mailbox that is monitored by the helpdesk or that opens a trouble ticket automatically through the helpdesk software. This would allow for tracking and further alerting of the appropriate personnel.

12. *Submit* and *Commit* the changes.

Task 5: Verifying the Configured Features

The features are now configured and the changes to the email security device(s) have been committed. The data around these features is available in Reporting, in the Outbreak Filters Quarantine, and in both Message Tracking and System Logs. Also, depending on your configuration, you might have messages in the Cisco Anti-Spam Quarantine.

A report on Rate Limiting per Mail-From is available at *Monitor* > *Rate Limits* showing Top Offenders by Incident and Top Offenders by Rejected Recipients.

A count of messages caught by Cisco Anti-Spam rules can be found in the *Monitor* > *Overview* report or the *Monitor* > *Outgoing Senders* report.

Outbreak Filters uses a temporary quarantine to hold messages that are suspect. When released, the messages are rescanned by Cisco Anti-Spam using any updated anti-spam rules that have arrived since the email was quarantined. To access this Quarantine, open *Monitor* > *Quarantines*, then click to open the *Outbreak* Quarantine.

To access the Outbreak Filters Report, click *Monitor* > *Outbreak Filters*.

Message Tracking is available and will show the disposition of messages, including if caught by Outbreak Filters, Anti-Spam, or Rate Limiting.

The *mail_logs* log files will also contain information on message disposition.

Examples of log entries are:

```
Outbreak Filters: Fri Apr 20 09:02:09 2012 Info: MID 2099 quarantined to
"Outbreak" (Outbreak rule: Phish: Phish)
Rate Limiting per Mail From:  Mon Jul 2 15:38:12 2012 Info: MID 2219 To:
<user2@example.com> From: <user1@internal.com> Rejected by Rate Limiting per
Envelope Sender
```

Conclusion

Using a combination of configured features provides the greatest protection against incoming spam attacks. Additional reporting, log entries, and alert emails help institutions resolve problems quickly and stay off the email blacklists.

For more information about Cisco Anti-Spam or Cisco Email Security, please visit www.cisco.com/go/emailsecurity.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-720311-01 11/12