Email Migration Project Plan for Cisco Cloud Email Security

Overview

This document provides details about how to migrate your customer from another email security product that is either cloud based or on premise to the Cisco® Cloud Email Security (CES) solution. This is not to be used as a proof-of-concept (PoC) or competitive-product evaluation guide.

Audience

This guide is designed for Cisco Channel Partners and Cisco Sales Engineers who have experince in configuring Cisco's CES solution. It provides top level guidance that must be supported by the sales engineer's content security experience and the administration guide. It is assumed that acronyms and terminologies specific to content security are known.

Email migration project plan: Hosted

Supplemental reference: http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html.

Inbound

Infrastructure

- Mail Exchange (MX) records: Make sure Cisco Remote Operations Service (ROS) is notified to have the A record and Mail Exchange records to reference domain. iphmx.com.
  - Create and publish new Mail Exchange records at least 72 hours before cutting completely over to new systems. Most time-to-live (TTL) settings on DNS servers are 24 hours; 72 ensures that they are all updated by a cutover.
- Firewall rules: Are the necessary ports open between the hosted environment and the internal message transfer agent (MTA) and other devices?
  - Ports 25, 22, 636 (or 3269), and 443, 80 open to IP Range 68.232.128.0/19
  - Is the customer's mail server set to receive mail relayed from the Cisco CES solution?
  - Are there any other MTAs that will be upstream from the hosted ESA server? If yes, then follow the setup procedures for "incoming relay" in the admin guide.

  Note: This is by far not the best design because reputation filtering will no longer be applied during the initial Simple Mail Transfer Protocol (SMTP) connection.

Inbound Connection Control

- Transport Layer Security (TLS): Do you require TLS with any other domains? If so, you need to work with Cisco ROS to add a signed certificate to your devices.
  - Create sender groups for required for TLS domains. (If only opportunistic TLS, there's no need for new sender group.)
- Whitelists: New customers are encouraged to submit only mission-critical whitelists to begin with (payroll for instance). Do not copy whole lists because every product works differently, and adding too many whitelists can hurt spam efficacy.
  - Domain whitelists and blacklists are done in a Host Access Table (HAT), exceptions to Anti-spam for specific email addresses are made in the incoming mail policies
- Blacklists: We encourage you to move over all blacklists to the HAT, because you know these are unwanted senders regardless of other factors.

- Directory Harvest Attack Prevention (DHAP), Domain Key Identified Mail (DKIM) and Sender Profile Framework (SPF) validation: Enable these in the Security Features section of the Default Mail Flow Policy.
- Domains for which you receive mail: Make sure to include any and all subdomains (which can be done by changing “domain.com” to ”.domain.com” [notice leading period] where “domain.com” is the customers mail domain.) Set these domains in the Recipient Access Table (RAT).
- SMTP routes: Make sure that all mail servers are specified in the SMTP route table with either the customer’s fully qualified domain names (FQDN) or their IP addresses.

Note: Domains specified in the RAT, but not in the SMTP route table, may cause an email forwarding loop within the ROS ESA appliance.

Incoming Mail Policies

- End-user spam quarantine: Is the old solution using a spam quarantine? Users need to know what Cisco’s spam quarantine digest will look like, and details such as End User Quarantine password login, if needed, and Safelist/blocklist, if used. How are marketing messages handled? If spam and marketing messages are not quarantined, then skip this step.
- Policy for spam, antivirus function, and content: Do you have one company policy or more specific policies based on various groups?
  - Microsoft Internet Explorer: Marketing spam can be blocked for one group but allowed for another, or executives can have much more strict spam rules than the general population.
- Antivirus: Set up a policy for known viruses, encrypted messages, and unreadable messages, and determine what to do if a virus cannot be cleaned.
- Advanced malware protection: Do you have issues with Advanced Persistent Threats (APTs) and viral attachments typically missed by signature-based antivirus engines? Investigate enabling the advanced malware protection engine.
- Content Filter rules:
  - Attachment and/or file types to block or quarantine
  - Size limits for messages and attachments
  - Disclaimer to stamp messages
  - Other content rules such as blocking profanity, executable files, Web-Based Reputation Score (WBRS) filters, and the Web Category Analysis Tool (WebCAT).

Note: You can avoid Anti-Spam and Anti-Virus scanning of known file types that will be blocked in content Filters by instead blocking them with a message filter. Make sure the solution is completely tested.

- Outbreak filters: Do you have problems with phishing attacks? Is there a subset of emails with malicious URLs that take employees to malicious sites? If yes, then in Outbreak Filters, enable message modification.

Administrator

- Determine various levels of accounts needed: admin account, help desk, reporting, compliance, and so forth.
  - Help desk: Can the help desk access current system? Set up logins for help desk on new system.
  - Admin logins: Either tie in to an existing admin with external credentials, or set up local accounts with various levels of access.

Outbound

Note: The following guidance assumes that the outgoing mail flow is established through the Cisco CES infrastructure.

Infrastructure

- Firewall rules: Are the necessary ports open between the hosted environment and the internal sending mail transfer agent (MTA) and other devices?
  - Ports 25, 22, 389 (636 or 3269 for LDAP over SSL), and 443, 80 are open to IP range 68.232.128.0/19.
- Other devices: Are any other devices monitoring or sending mail other than the MTA? If so, make sure they are updated to reflect changes.

Outbound Connection Control

- Are you concerned with high-volume mail control? If so, do you need to make exceptions for marketing or bulk email?
- Do you have TLS policies to specific domains? What is the Service Level Agreement (SLA)?
- Is TLS required between your mail server and Cisco CES?
- Do you use Domain Key Identified Mail (DKIM) or (SPF) signing?

Outbound Mail Policies

- Do you want to check spam outbound?
  - For ISPs, have you discussed Intelligent Multi-Scan (IMS) licensing with the customer?
- Have you coordinated your antivirus function? Best practice is to match inbound and outbound antivirus policies to mimic one another.
- Are you using data loss prevention (DLP) software? If so, do the following:
  - Determine if you need DLP policies applied in the cloud or on premises? For on-premises situations, investigate the cloud hybrid solution.
  - Translate third-party DLP policies to the RSA DLP solution.
  - Verify real policy violations by sending them to a controlled outside destination.
- Are you using encryption?
  - Do you need encryption applied in the cloud or on premises? For on-premises situations, investigate the cloud hybrid solution.
  - Have you provided the encryption plug-in to your users?
  - Does DLP trigger encryption? Set up a connector to test.
  - Are you using the Microsoft Outlook encryption plug-in?
    - Desktop encryption
    - Set to encrypt by flag
  - Set up admin accounts in the Cisco Registered Envelope Service portal, so you can send a secure message to anyone internally who needs admin rights to the portal, and there is a user account connected to the admin account.

- Content filter rules:
  - Size limits on outgoing messages
  - File types to block and/or quarantine
  - Outgoing message disclaimer to add to messages
  - Any other outbound rules: recognizing profanity, WBRS filters, WebCAT, and so on.

Note: You can avoid Anti-Spam and Anti-Virus scanning of known file types that will be blocked in content filters by instead blocking them with a message filter. Make sure the solution is completely tested.

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 C96-731888-00 05/14