Securing Your E-mail Communication

T-SECB3&4

Hrvoje Dogan, Consulting Systems Engineer, Security
Prosíme, ptejte se nás

- **Twitter** [www.twitter.com/CiscoCZ](http://www.twitter.com/CiscoCZ)
- **Talk2cisco** [www.talk2cisco.cz/dotazy](http://www.talk2cisco.cz/dotazy)
- **SMS** 721 994 600
Cisco E-mail Security Consolidates the Network Perimeter
For Security, Reliability and Lower Maintenance

Before Cisco
- Encryption Platform
- MTA
- DLP Scanner
- Anti-Spam
- Anti-Virus
- Policy Enforcement
- Mail Routing

After Cisco
- Cisco E-mail Security Appliance
Email Security Architecture
Inbound Security, Outbound Control

INBOUND SECURITY

Spam Defense

Virus Defense

OUTBOUND CONTROL

Data Loss Prevention

Secure Messaging

THE CISCO ASYNCOS™ EMAIL PLATFORM
The Cisco AsyncOS
Robust — Tools to Protect Customers

**TLS Encryption**
Gateway to gateway encryption

**HTML Sanitization**
Eliminates spoofed URLs

**SPF Verification**
Verify mail is coming from servers designated to send on sender’s behalf

**DKIM Signing & Verification**
Sender verification

**Industry Leading LDAP Capabilities**
LDAP referrals, multiple LDAP servers, 3 step set up wizard

**Bounce Verification**
Eliminates mis-directed bounces

**End User Allow & Block Lists & Spam Quarantine**
End user controls

**Recipient Validation**
Eliminates messages sent to invalid email addresses
SenderBase Reputation Filtering
Real Time Threat Prevention

Incoming Mail
Good, Bad, and Unknown Email

Reputation Filtering
IronPort Anti-Spam

- Known good is delivered
- Suspicious is rate limited and spam filtered
- Known bad is blocked

Cisco on Cisco
Our Corporate Email Experience

<table>
<thead>
<tr>
<th>Message Category</th>
<th>%</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped by Reputation Filtering</td>
<td>93.1%</td>
<td>700,876,217</td>
</tr>
<tr>
<td>Stopped as Invalid recipients</td>
<td>0.3%</td>
<td>2,280,104</td>
</tr>
<tr>
<td>Spam Detected</td>
<td>2.5%</td>
<td>18,617,700</td>
</tr>
<tr>
<td>Virus Detected</td>
<td>0.3%</td>
<td>2,144,793</td>
</tr>
<tr>
<td>Stopped by Content Filter</td>
<td>0.6%</td>
<td>4,878,312</td>
</tr>
<tr>
<td><strong>Total Threat Messages:</strong></td>
<td>96.8%</td>
<td>728,797,126</td>
</tr>
<tr>
<td>Clean Messages</td>
<td>3.2%</td>
<td>24,102,874</td>
</tr>
<tr>
<td><strong>Total Attempted Messages:</strong></td>
<td></td>
<td>752,900,000</td>
</tr>
</tbody>
</table>
Cisco Email Encryption
Easy for the Sender. . .

- Automated key management
- No desktop software requirements
- Send to any email address seamlessly
Cisco Email Encryption
Easy for the Recipient. . .

1. Open Attachment
2. Enter password
3. View message
Cisco Email Security Manager
Single view of policies for the entire organization

### Incoming Mail Policies

<table>
<thead>
<tr>
<th>Order</th>
<th>Policy Name</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Content Filters</th>
<th>Virus Outbreak Filters</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IT Staff</td>
<td>(use default)</td>
<td>(use default)</td>
<td>QuarantineEXEs</td>
<td>(use default)</td>
<td><img src="image" alt="Delete" /></td>
</tr>
<tr>
<td>2</td>
<td>Sales</td>
<td>IronPort Positive: Deliver Suspected: Deliver</td>
<td>(use default)</td>
<td>DelMsgsWithEXEs</td>
<td>(use default)</td>
<td><img src="image" alt="Delete" /></td>
</tr>
<tr>
<td>3</td>
<td>Legal</td>
<td>(use default)</td>
<td>(use default)</td>
<td>ArchiveMailQuarantineEXEsStripMediaFiles</td>
<td>Enabled</td>
<td><img src="image" alt="Delete" /></td>
</tr>
<tr>
<td></td>
<td>Default Policy</td>
<td>IronPort Positive: Drop Suspected: Deliver</td>
<td>Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop</td>
<td>QuarantineEXEs StripMediaFiles</td>
<td>Enabled</td>
<td><img src="image" alt="Delete" /></td>
</tr>
</tbody>
</table>

**Policies: by Domain, Username, or LDAP**
Comprehensive Insight
Unified Business Reporting

Consolidated Reports

- Single view across the organization
- Real Time insight into email traffic and security threats
- Actionable drill down reports

Multiple data points

- Email Volumes
- Spam Counters
- Policy Violations
- Virus Reports
- Outgoing Email Data
- Reputation Service
- System Health View
Visibility Into Email Messages
Message Tracking

What happened to the email I sent 2 hours ago?
✓ Track Individual Email Messages

Who else received similar emails?
✓ Forensics to Ensure Compliance
Customizable E-mail Security Service Offerings
Provide Broad Protection and Control

**Anti-Spam**
- SenderBase Reputation Filtering
- IronPort Anti-Spam (IPAS)
- Outbreak Filters

**Anti-Virus**
- Virus Outbreak Filters
- McAfee Anti-Virus
- Sophos Anti-Virus

**DLP**
- Content Filters
- Smart Identifiers
- Weighted Content Dictionaries

**Encryption**
- Secure Message Delivery
- Transport Layer Security
Flexible Deployment Options
Same Market-Leading Email Security

Hosted Email Security (SaaS)
Hybrid Hosted Email Security
Cisco Security Operations Center
IN THE NETWORK

CUSTOMER PREMISE
Hybrid Hosted Email Security
Managed Email Security
Customer Premise Equipment (CPE)

Common Policy | Centralized Reporting | Consistent Protection
Gartner Magic Quadrant for Secure E-mail Gateway, 2011

The Magic Quadrant is copyrighted 2011 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Cisco.
Otázky a odpovědi

• Twitter  www.twitter.com/CiscoCZ
• Talk2Cisco  www.talk2cisco.cz/dotazy
• SMS  721 994 600

• Zveme Vás na Ptali jste se… v sále LEO
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00
Prosíme, ohodnoťte tuto přednášku.