

Cisco Spam & Virus Blocker



Ioan Stanciu

Cisco System Engineer – Logicom

Cisco Expo – 17.03.2010



Logicom in Romania

Member of Logicom Public Ltd Group



Cyprus Greece Italy United Arab Emirates Saudi Arabia Lebanon Jordan Turkey Qatar Pakistan Kuwait Oman Bahrain Malta Hungary Bulgaria Romania

Logicom Public Group

18 countries - 12 warehouses
5'000 customers in 25 countries



Cyprus Greece Italy United Arab Emirates Saudi Arabia Lebanon Jordan Turkey Qatar Pakistan Kuwait Oman Bahrain Malta Hungary Bulgaria Romania

About Logicom Public Ltd

- Started in 1987
- IT Distribution Group with HQ in Cyprus
- The biggest IT company in Cyprus
- **1997-1999 – EU Distribution contracts for: Cisco Systems, Intel, Microsoft**
- 2000 – listed on the Cyprus stock exchange and starts geographical expansion in 18 countries
- 2005 – member of FTSE CySE 20 Stock Exchange
- 2006 – presence in Turkey – after 1 year of operation, becomes no.1 Cisco Authorized Distributor
- May 2007 – presence in Romania, Bulgaria, Hungary



Logicom in Romania



Logicom in Romania

- May 2007 – start ops; **Cisco Systems Authorized Distributor**
- June 2008 – Intel Authorized Distributor
- July 2008 – No. 1 Cisco (revenue) on Ro Cisco Disti market
- Aug 2008 – Kingston Authorized Distributor
- Nov 2008 – Microsoft distributor based on EU contract (OEM, VL, retail)
- May 2009 – Linksys distributor
- June 2009 – new offices & own warehouse in Mogosoaia area
- Dec 2009 – MSI products in portfolio
- Feb 2010 – HP supplies based on EU contract



Market proposition (1)

- **Diversified stocks & financial strength**
 - Invest heavily in stock; various items; latest products
 - DHL delivery all over Romania
- **Optimized Logistics & Fast access** to products due to regional presence (Greece, Bulgaria, Hungary)
- **Transparency**
 - Product availability on stock/back-order, delivery terms, product life-cycle, price variation, new products
 - Correlate stocks with you needs (forecast)
 - Flexible payment terms ... for good payers and constant customers
- **Only distribution business**
 - no PC/network integration
 - no retail presence
 - No direct contact with end-users – we forward them to the resellers

Market proposition (2)

- **High quality products and support**
 - Extensive info about vendor's promotions and marketing programs
 - Technical and sales trainings
 - Road shows, promotions, sales contests etc
- **Fast(est) answer** to your orders/questions
- **Relationship oriented**
 - Attention to the resellers business needs, special projects etc.
 - Identify **profitable** business opportunities for the resellers & provide proper solution support
- Fast approval of **credit lines & payment terms** (depends on the financial situation of the company & history payment)
- **The product portfolio is expanding**



Cisco Spam & Virus Blocker





Business Challenge



“Spam, viruses, spyware, and phishing all have one thing in common—they make profitable businesses. And these profits create incentive for innovation on the part of the perpetrators.”

— Peter B. Danzig, Ph.D.
University of Southern California

http://www.messagingnews.com/magazine/2006/01/cover_story/changing_face_of_network_security.html



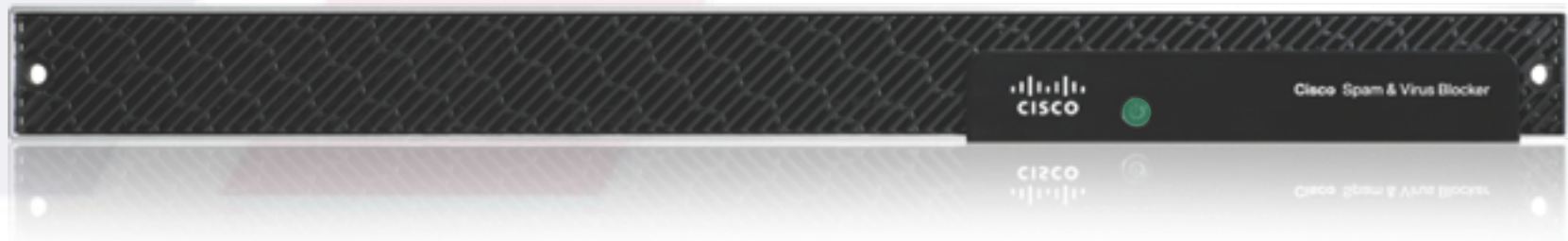


Product Overview



The Cisco Spam & Virus Blocker is a dedicated email security appliance for small business with up to 250 email users.

It provides powerful protection against spam, viruses and other email threats to secure your network and business data while improving productivity.





Benefit Highlight: Accuracy



- Virtually eliminate spam, viruses, and other email threats.
- Accurate protection immediately after setup.
- Block non-business email.
- Retains accuracy with continuous and automatic updates.
- Set it. Forget it. It just works.





Benefit Highlight: Easy Installation and Use



- Quick and easy installation into most networks within minutes.
- Provides immediate protection out of the box once installed in network.
- Automatic threat updates to the appliance with no intervention required.
- Simple browser-based wizards support management and reporting.
- Reduce operational costs of administration.



Email



Internet



Firewall



Cisco Spam &
Virus Blocker



Groupware
(Exchange, Notes,
Groupware)



Clients





Benefit Highlight: Simplified Single SKU Ordering



- Bundles include everything (hardware, software, support services for 1-3 years, for 50, 100, 250 users) to simplify ordering to just one SKU.
- Available only through distribution channel and competitive pricing.

Product Name	Product Description	
BLKR-SVB-50U-1Y	Cisco Spam & Virus Blocker - 50 User - 1 year	
BLKR-SVB-100U-1Y	Cisco Spam & Virus Blocker - 100 User - 1 year	
BLKR-SVB-250U-1Y	Cisco Spam & Virus Blocker - 250 User - 1 year	
BLKR-SVB-50U-3Y	Cisco Spam & Virus Blocker - 50 User - 3 year	
BLKR-SVB-100U-3Y	Cisco Spam & Virus Blocker - 100 User - 3 year	
BLKR-SVB-250U-3Y	Cisco Spam & Virus Blocker - 250 User - 3 year	
CON-BLK-BLKR50U	SW and Supp Subscr NBD Blocker 50 User (annual)	
CON-BLK-BLKR100U	SW and Supp Subscr NBD Blocker 100 User (annual)	
CON-BLK-BLKR250U	SW and Supp Subscr NBD Blocker 250 User (annual)	





Cisco Spam & Virus Blocker Technical Overview



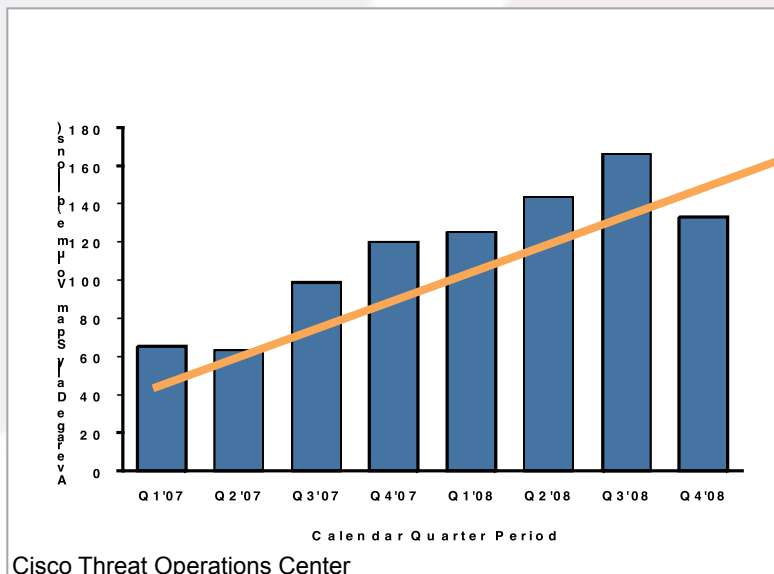


Email Security Threats More Spam and Spammers



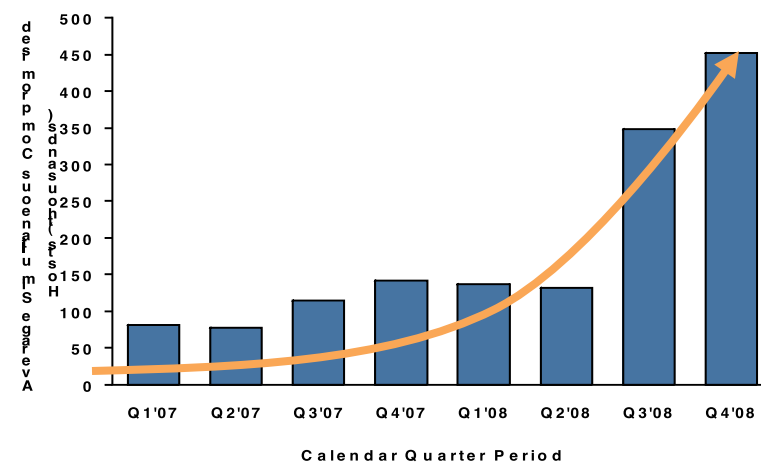
More Spam

- Daily spam volume doubles yearly
- Reaching 180 billion spam messages per day



Source: Cisco Threat Operations Center

Average # Compromised Hosts



More Spammers

- More Spammers with Botnet-compromised hosts send spam
- Malware sophistication increasing





Spam Sophistication Increasing



TEXT SPAM



ATTACHMENT SPAM
(PDF, EXCEL, MP3)

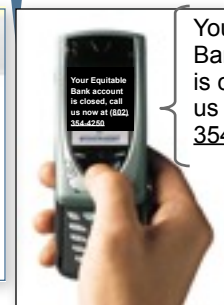
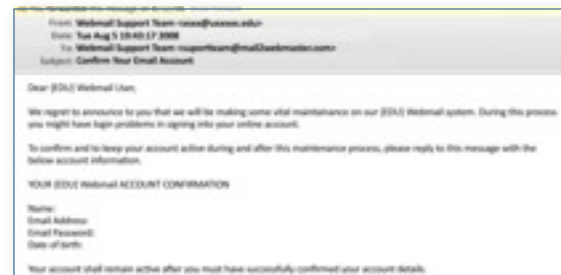


IMAGE SPAM

TARGETED ATTACKS

“Spam has undergone a significant evolution in 2008...sophisticated online criminals have been using smaller phishing campaigns aimed at more targeted groups of recipients – to great effect.”
- 2008 Internet Security Trends Report

Published By Cisco and IronPort

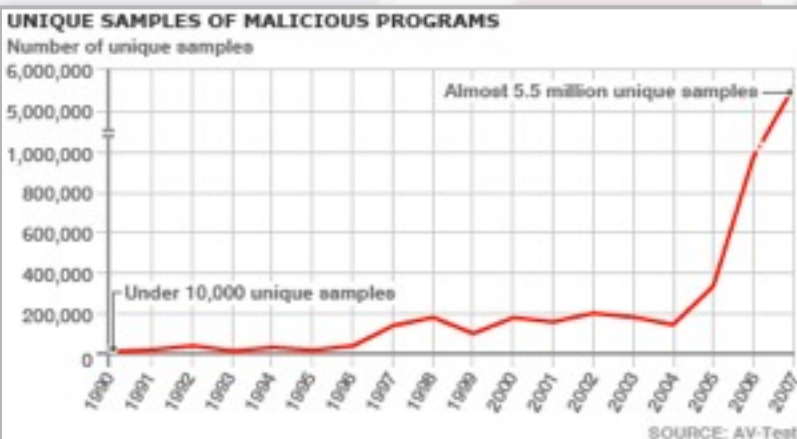
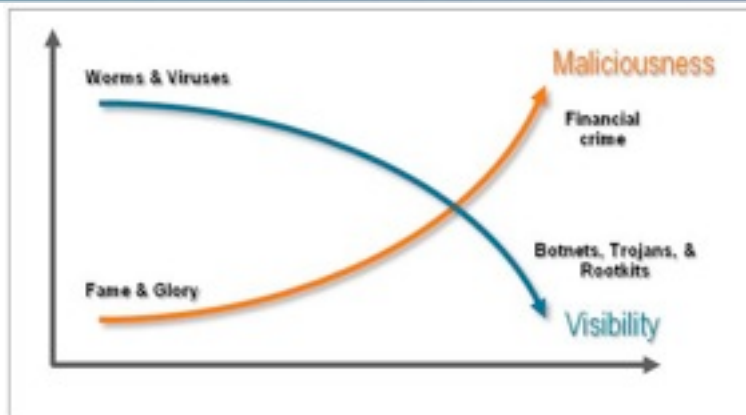


Your Equitable Bank account is closed, call us now at (802) 354-4250





Malware Is On The Rise Email is a Primary Medium





Net Admin's Frustrations

- Threat proliferation increases workload and demands increased expertise
- Thin administrator resources increasingly stretched with budget tightening





Cisco Spam & Virus Blocker Architecture

Inbound Security, Outbound Control



**INBOUND
SECURITY**

Spam and Virus Defense

**THE CISCO ASYNCOS™
EMAIL PLATFORM**

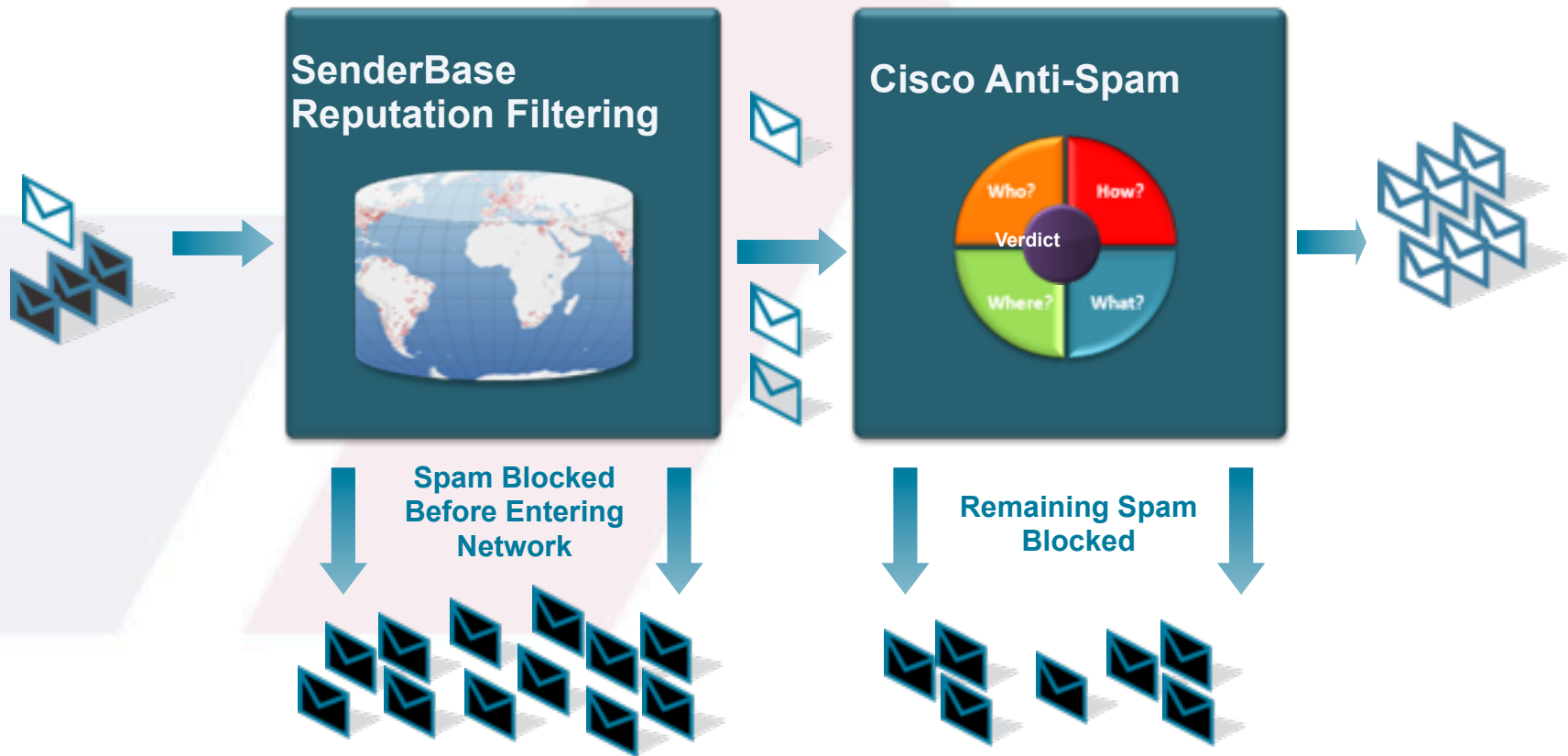
**OUTBOUND
CONTROL**

Highly Flexible Content Filtering





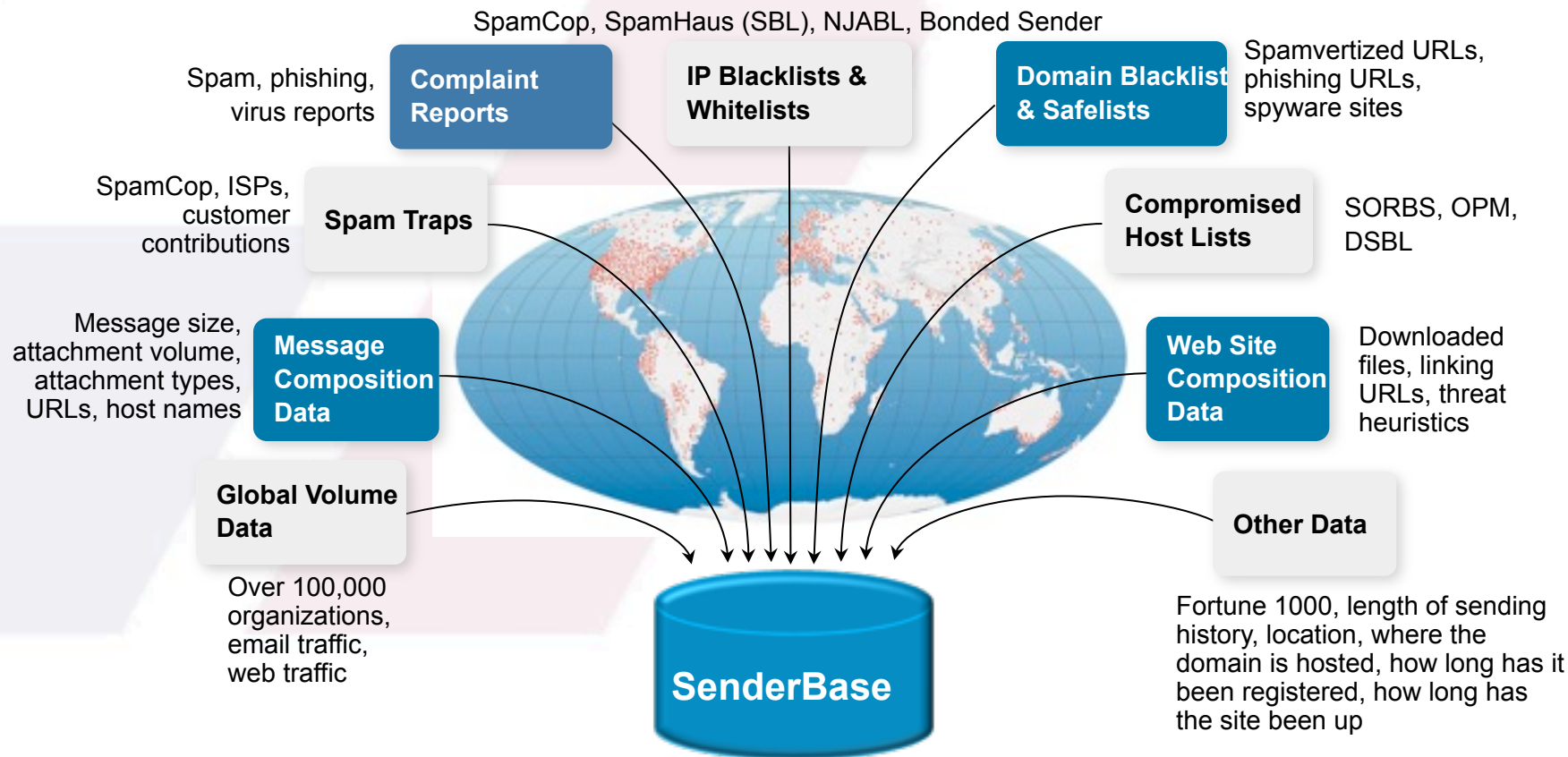
Anti-Spam Defense in Depth





SenderBase

Breadth & Quality of Data -> the Difference





Email Threat Operations Center Data, Research, Protection

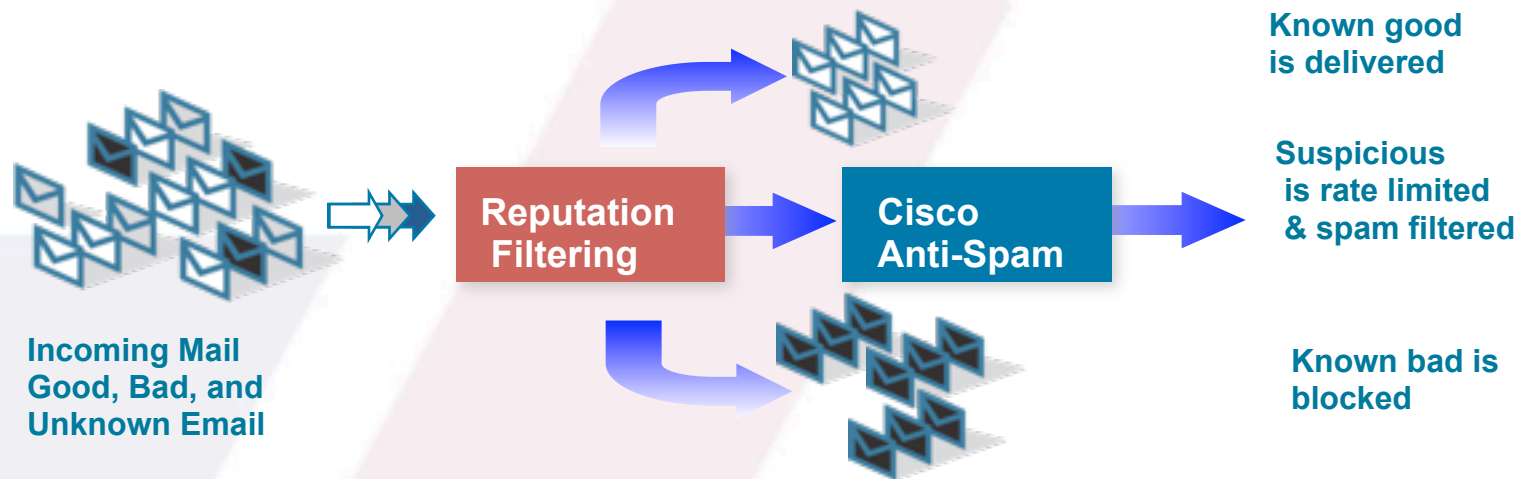


- 500 Threat Analysts worldwide
- 100+ Patents; 80+ Ph.D's
- 24 x 7 / 365 coverage
- Over 32 languages spoken





SenderBase Reputation Filtering Real Time Threat Prevention



Cisco's Internal Email Experience:

Message Category	%	Messages
Stopped by Reputation Filtering	93.1%	700,876,217
Stopped as Invalid recipients	0.3%	2,280,104
Spam Detected	2.5%	18,617,700
Virus Detected	0.3%	2,144,793
Stopped by Content Filter	0.6%	4,878,312
Total Threat Messages:	96.8%	728,797,126
Clean Messages	3.2%	24,102,874
Total Attempted Messages:		752,900,000





Cisco Anti-Spam Defense in Depth Spam Protection



- ✓ Spam Botnets
- ✓ Spammer Networks

EMAIL REPUTATION

- ✓ SMS Spam
- ✓ Attachment-based Spam

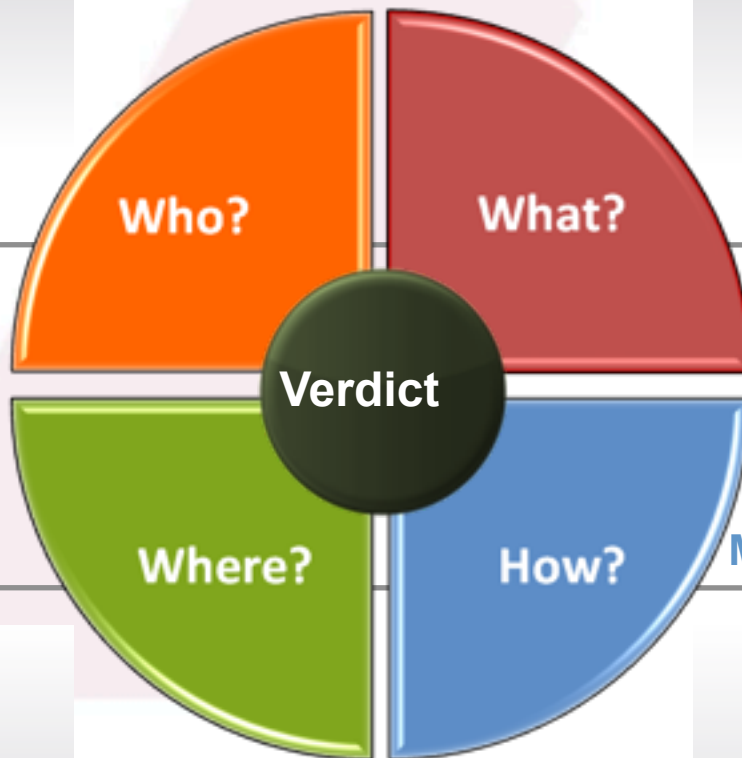
MESSAGE CONTENT

WEB REPUTATION

- ✓ Malware/Phishes
- ✓ Short-Texted Spam with URLs

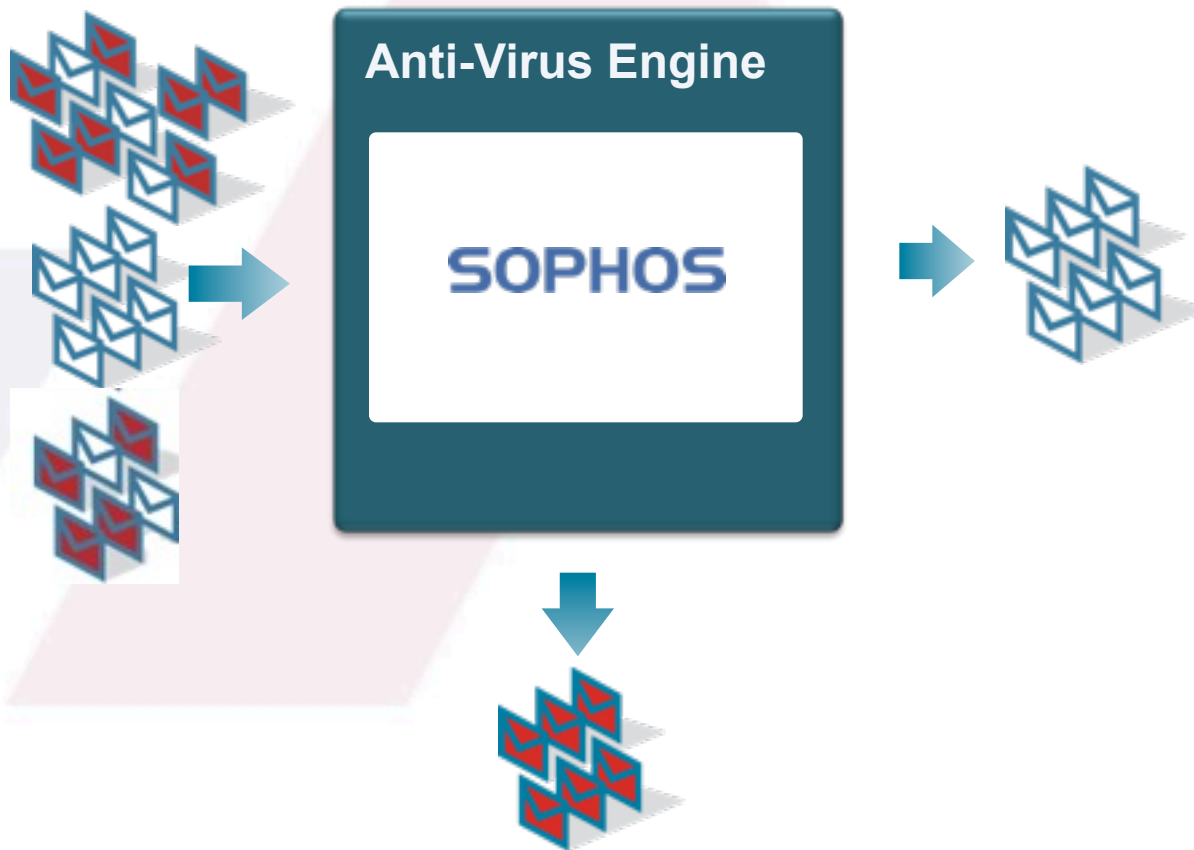
MESSAGE CONSTRUCTION

- ✓ Image Spam
- ✓ Spam created using Automation Tools





Anti-Virus Defense in Depth





Data Loss Prevention Simple Set Up



- Easy “3 click” set-up using content filters
- Use pre-defined content categories or create / customize your own
- Can be applied to specific users under specific conditions

☒ Import from local computer:

☐ Import from the *configuration* directory on your IronPort appliance:

- GLBA-Dictionary.txt
- HIPAA-Dictionary.txt
- PCI-Dictionary.txt
- README
- SOX-Dictionary.txt
- config.dtd

Message Body or Attachment

Does the message body or attachment contain text that matches a specified pattern?

- ☐ Contains text:
- ☒ Contains smart identifier:
ABA Routing Number
- ☐ Contains term in content dictionary:
HIPAA-Dictionary.txt

Number of matches required: (1-1000)

For content dictionaries, the number of matches is term weight.

Smart Identifiers: ?

Enable Smart Identifiers	Weight
<input checked="" type="checkbox"/> Credit Card Numbers	1
<input checked="" type="checkbox"/> Social Security Numbers	1
<input checked="" type="checkbox"/> ABA Routing Numbers	1
<input checked="" type="checkbox"/> CUSIPs	1





Data Loss Prevention Comprehensive Remediation & Reporting



- Multiple remediation actions – encrypt, quarantine, drop, bounce, BCC, strip content
- Offending content highlighted in quarantine for easy analysis
- Reporting on a per policy and per user basis

Quarantine
Strip Attachment by Content
Strip Attachment by File Info
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add Header
Encrypt and Deliver (Final Action)
Bounce (Final Action)
Deliver (Final Action)
Drop (Final Action)

Quarantine

Flags the message to be held in one of the areas.

Send message to quarantine: Policy

☐ Duplicate message

Send a copy of the message to the specified area. The original message will continue processing the original message actions will apply to the original message.





Spend Less Time Managing



Easy
Installation

Cisco Spam & Virus Blocker

Registration • Network Settings • Security Settings

You should receive a confirmation email within an hour of submitting your registration information (includes Internet connectivity). A 30-day evaluation license will activate with your registration is complete and device automatically updates with a permanent license.

Company Information

Company Name:
 Address:
 City: State/Province/Region:
 Postal Code: Country: United States

Primary Contact

First Name: Last Name:
 Email: No other Email:
 Business Phone: Home Phone:

More Information

Maximum Users: 10
 Maximum Mailbox Size: 10 MB
 Maximum Mailbox Count: 10
 Maximum Mailbox Size: 10 MB
 Maximum Mailbox Count: 10

Incoming Mail Policies

Find Policies

Email Address:

 Recipient

 Sender

Find Policies

Policies

[Add Policy...](#)

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	[? Staff]	QuarantineEXEs	(use default)	QuarantineEXEs	(use default)	
2	Sales	Import Positive; Deliver; Suspected; Deliver	(use default)	DelmgmtEXEs	(use default)	
3	Legal	(use default)	(use default)	Archival; QuarantineEXEs; SymphedEXEs	Enabled	
	Default Policy	Import Positive; Drop; Suspected; Deliver	Expanded; Deliver; Encrypted; Deliver; Unexpandable; Deliver; Virus Positive; Drop	QuarantineEXEs; SymphedEXEs	Enabled	

Key: Default Enabled Disabled

Email Security
Manager For
Configuration

Message Tracking

Search

No Tracking Data is currently available.

Envelope Sender: Date in time range: 10-25-2006

Envelope Recipient:

Subject:

Date and time range: and

Advanced

Sender IP Address:

Message Status:

☐ Search rejected connections only ☐ Search messages

Search multiple events will expand your search to include messages that report each event

☐ Virus Positive ☐ Spam Positive ☐ Suspicious ☐ Delivered

☐ Hard Bounced ☐ Soft Bounced ☐ Currently in Outbreak Quarantine

Message ID Number:

Default Action:

Import Mail:

Track All
Messages

Executive Summary



Real Time
Reporting



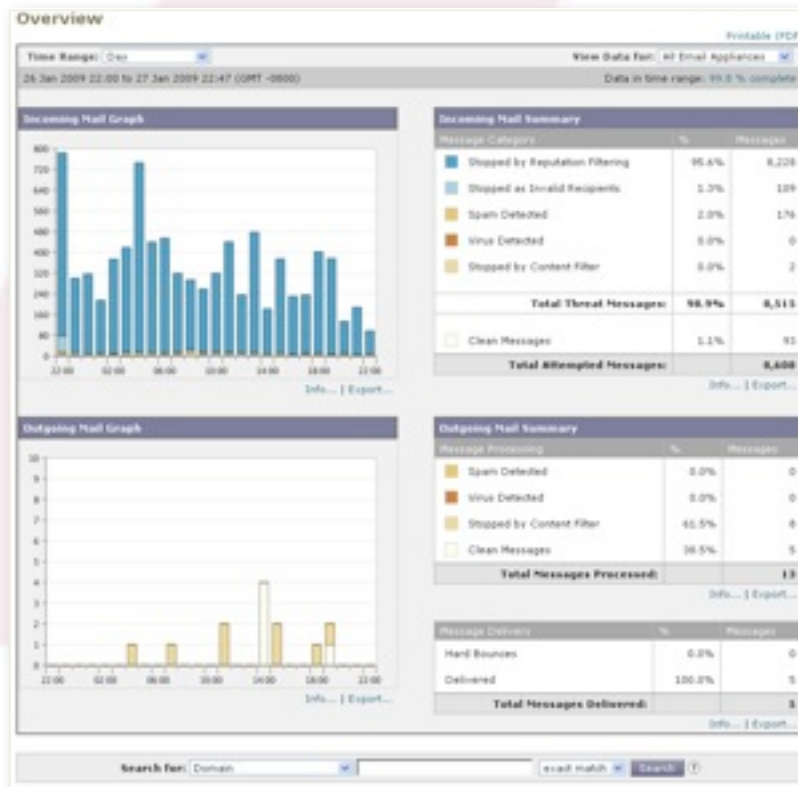


Comprehensive Insight Unified Business Reporting



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



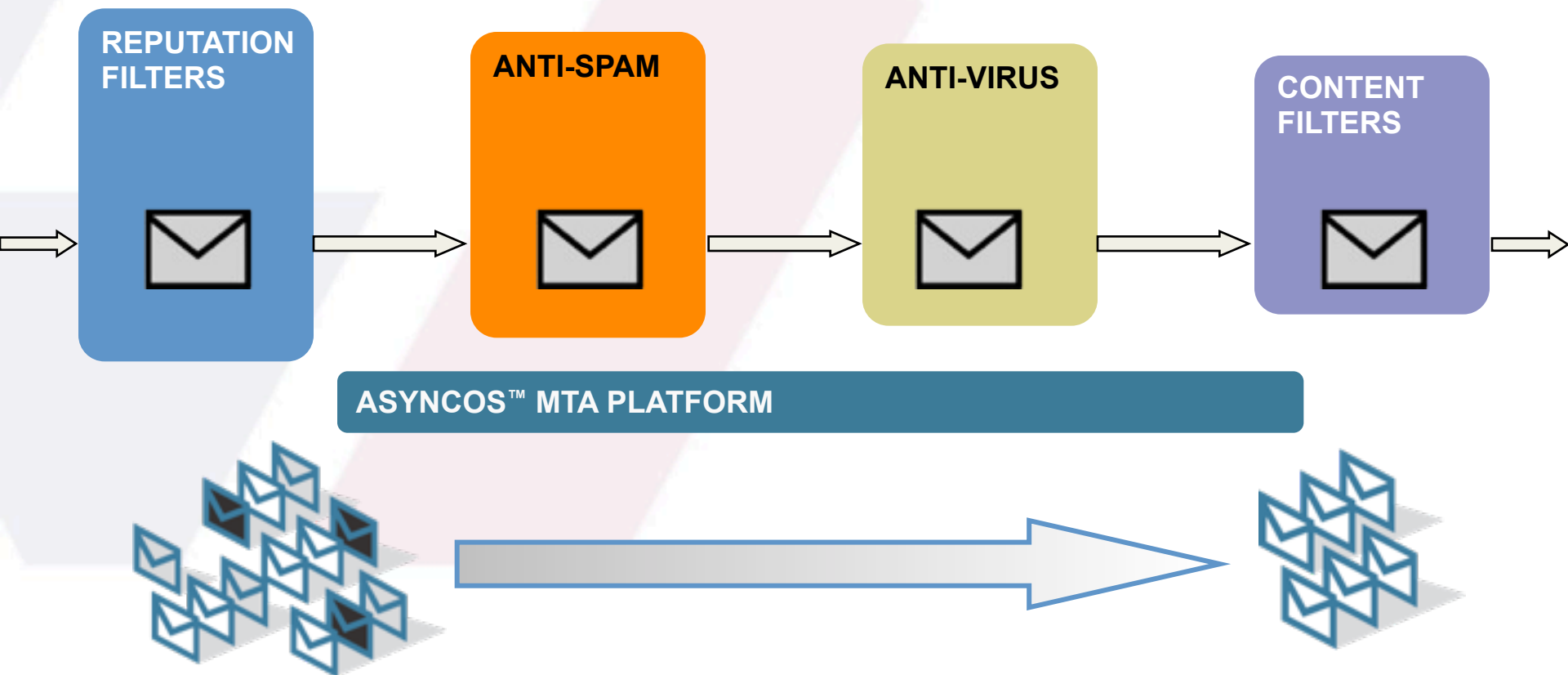


How Email Passes Through Blocker



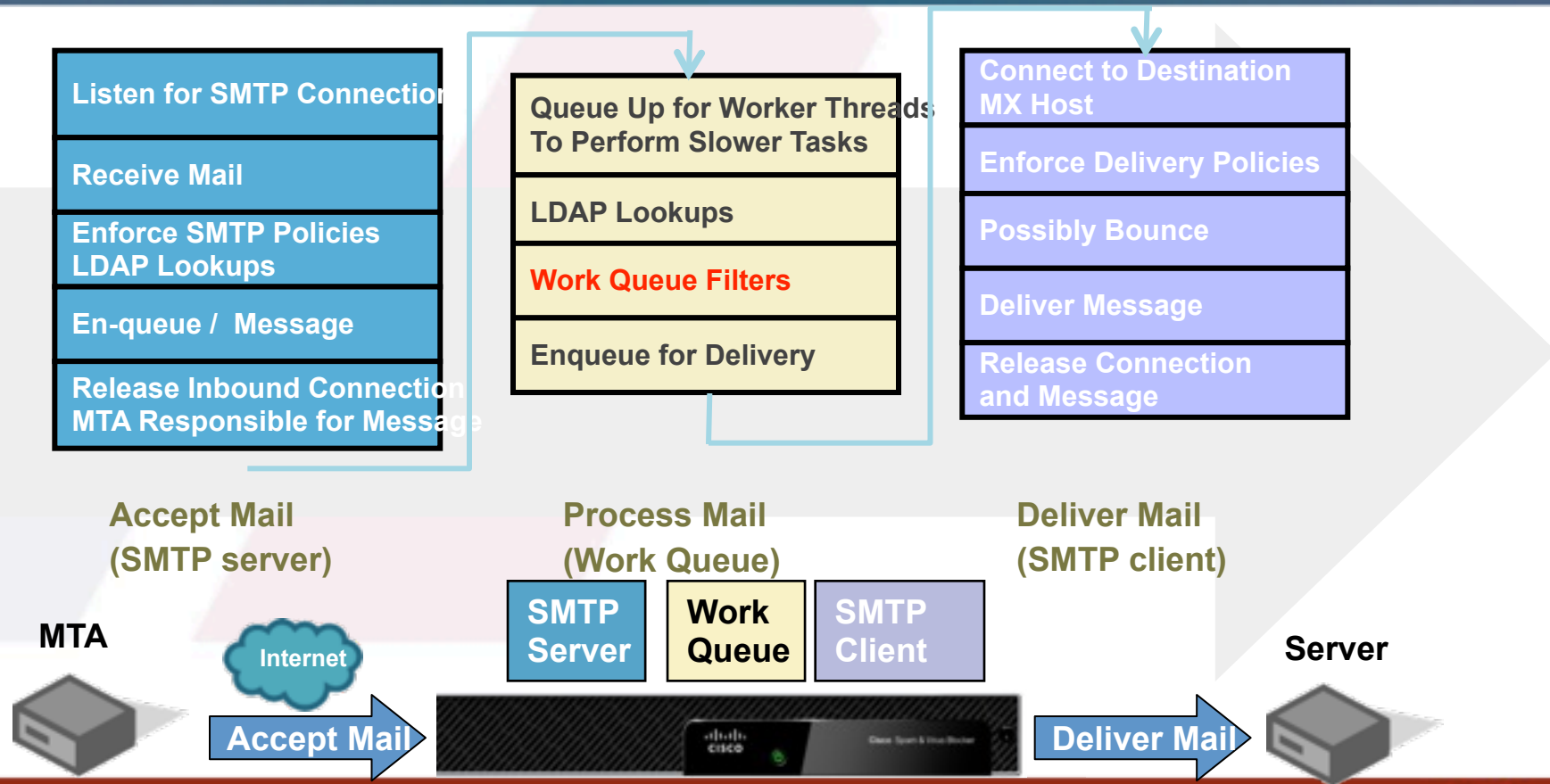


Understanding the Work Queue





Understanding the Email Pipeline



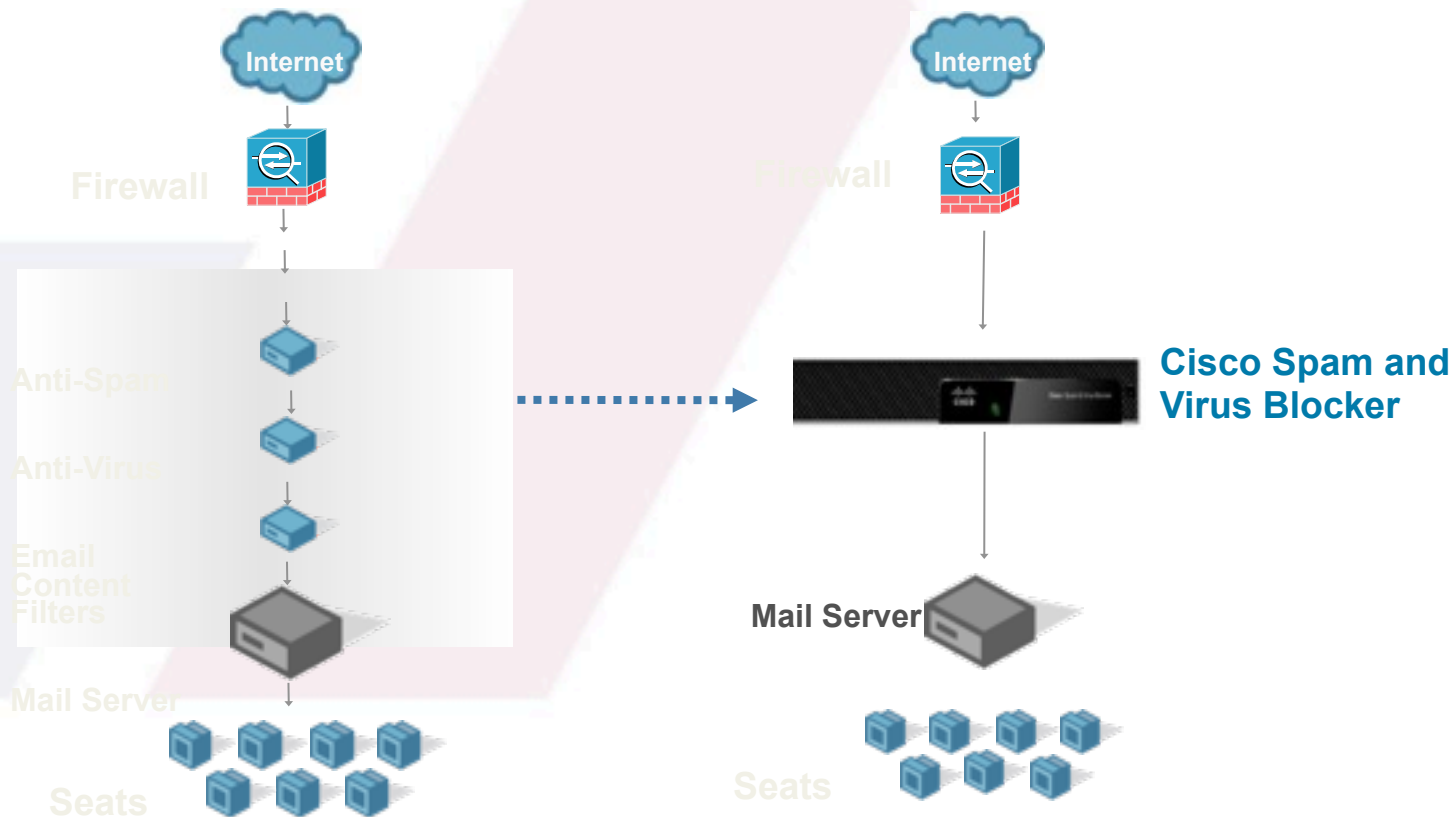


Installing Blocker





Cisco Spam & Virus Blocker Overview

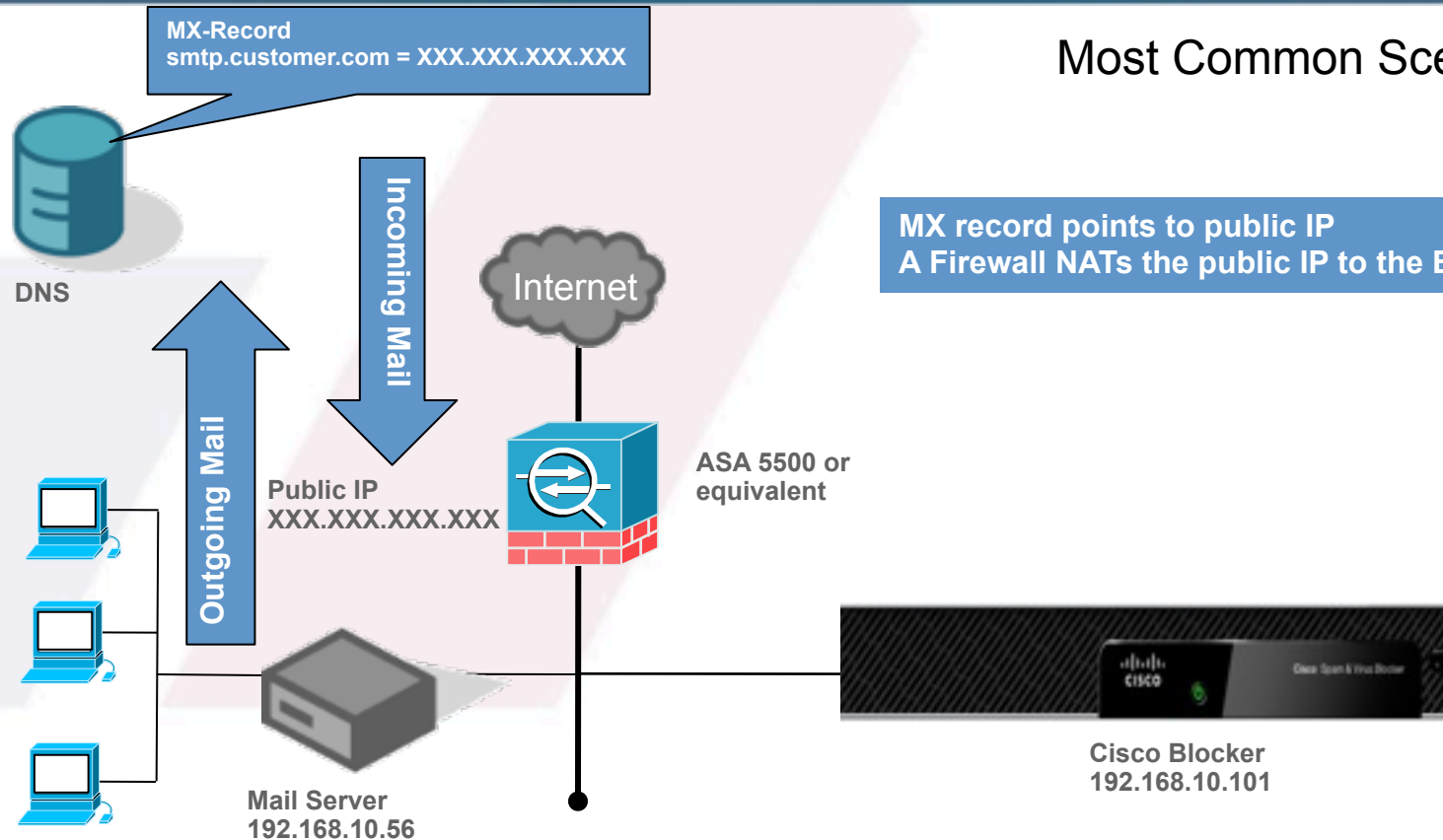




Blocker Connected to Inside (Intranet)



Most Common Scenario





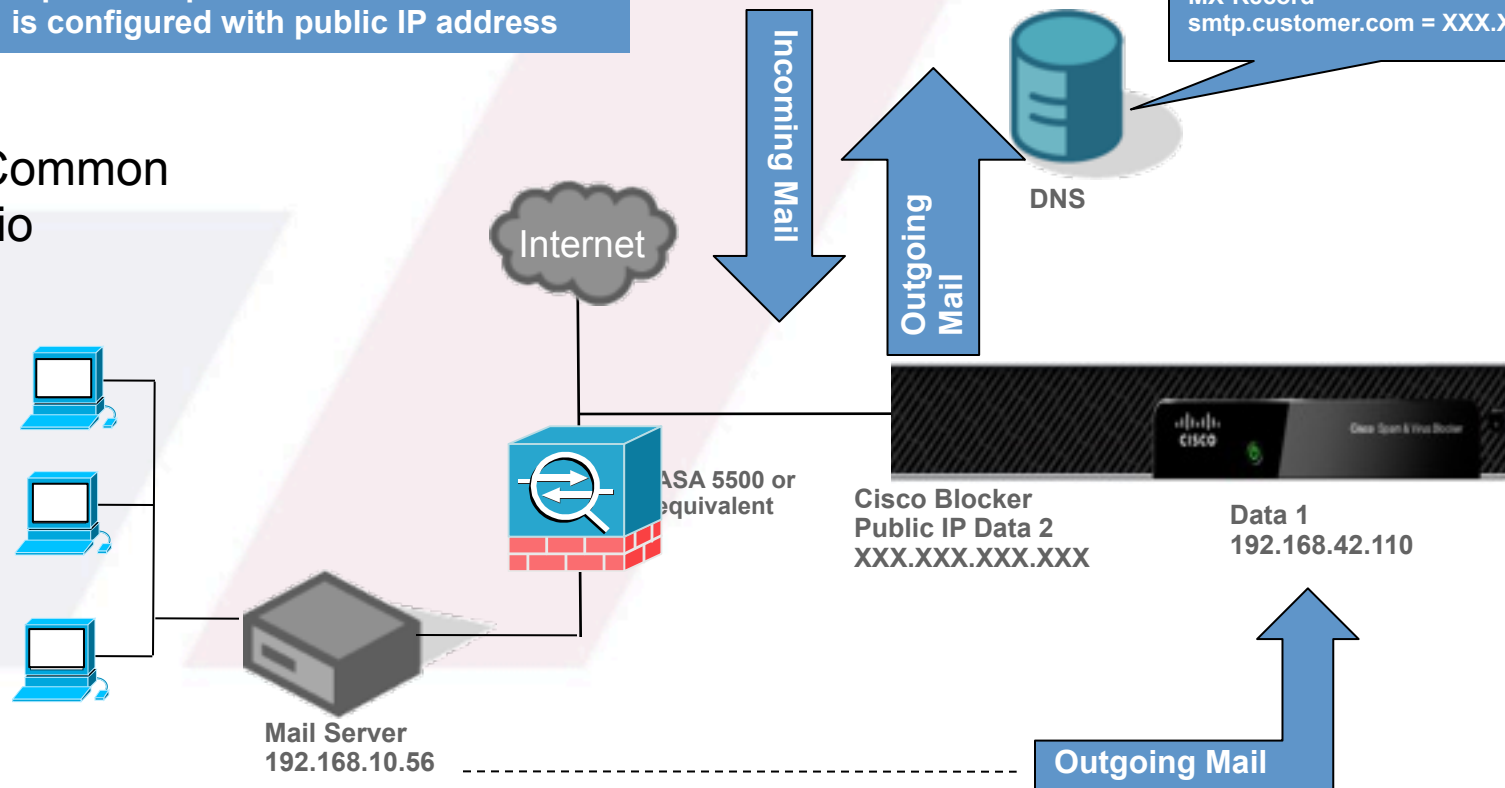
Blocker Connected to Outside (Internet)



MX record points to public IP
Blocker is configured with public IP address

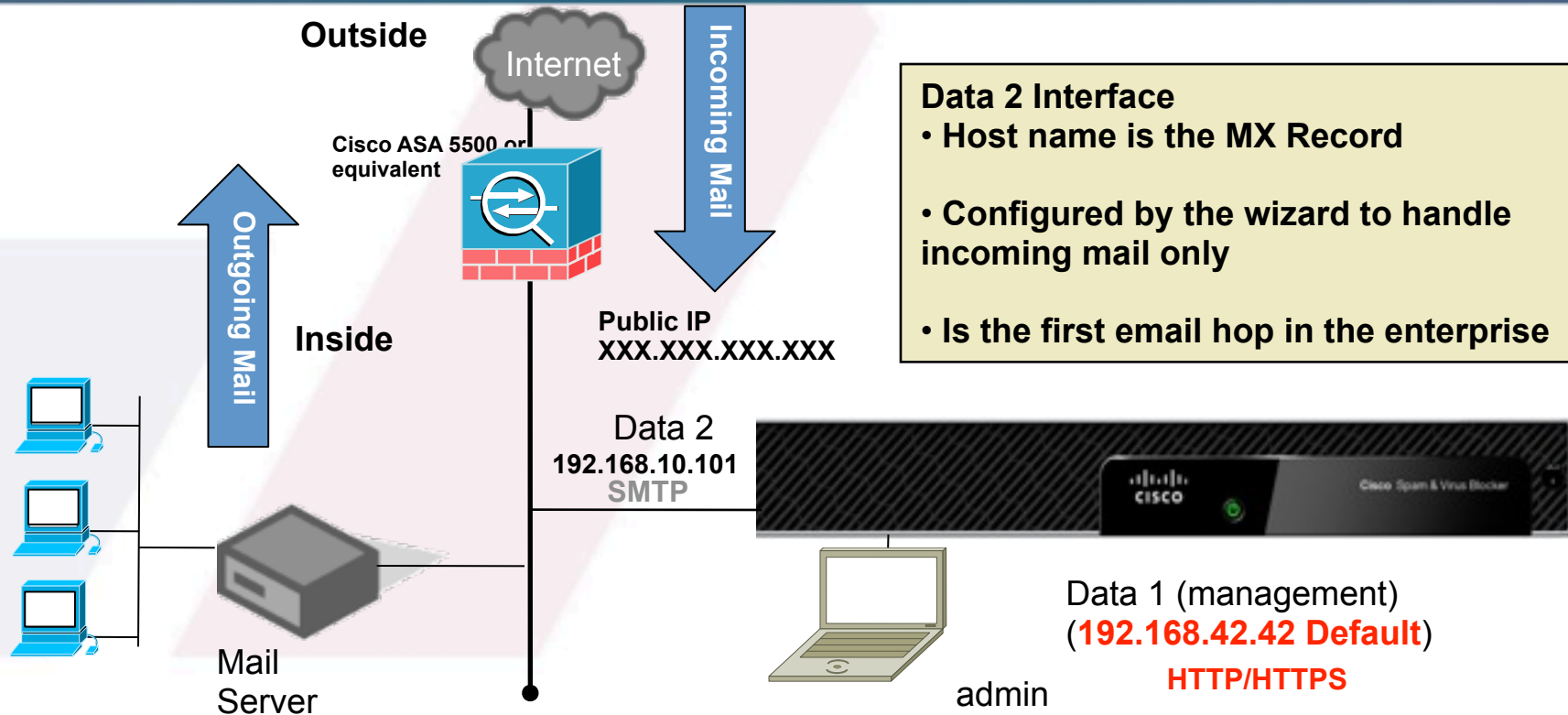
MX-Record
smtp.customer.com = XXX.XXX.XXX.XXX

Least Common
Scenario





Planning the Blocker Placement



Default: Cisco Blocker runs as an incoming mail gateway and Company mail server sends mail directly outbound

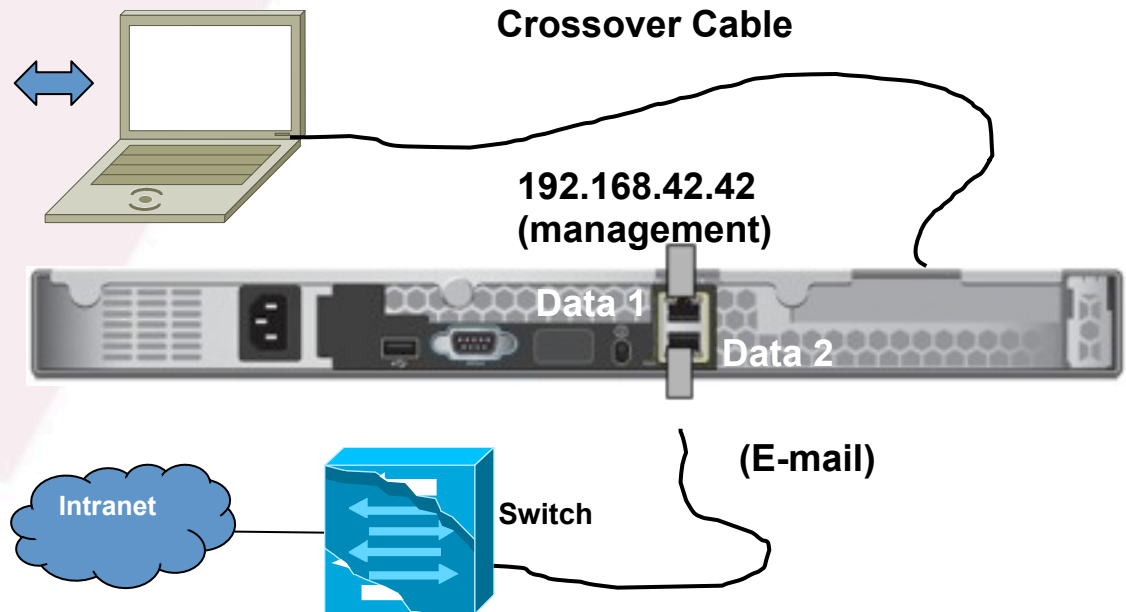




Accessing the Blocker



- Set your IP address up on the 192.168.42.0/24 subnet
- If auto-negotiation is not available, then use a cross-over cable between Blocker Data 1 and your Laptop





Running Setup Wizard



Ready to Stop Spam?

In minutes your company's
spam & virus problems will be solved.

Thank you for choosing the **Cisco Spam & Virus Blocker**
to protect your organization's email.

What you need to get started:

An Internet Connection

Your Quick Start Guide Out of the Box with Step 1 Filled Out

get started ▶





Running Setup Wizard (Cont.)



Cisco Spam & Virus Blocker

1 License 2 Registration 3 Network 4 Security 5 Review

A 30 day evaluation license is active until you complete the product registration. After you register, Blocker is automatically updated with a permanent license.

Company Information

Company Name:

Address:
(optional)

City: State/Province/Region:

Postal Code: Country:

Primary Contact

First Name: Last Name:

Email: Re-enter Email:

Business Phone: Mobile Phone: (optional)

Secondary Contact (optional)

First Name: Last Name:

Email: Re-enter Email:

Business Phone: Mobile Phone:

More Information

Mouse over fields to the left for additional notes.

Please enter your company's contact information and a primary point of contact so we may process your registration quickly. A valid email address is required for a permanent license.





Running Setup Wizard (Cont.)



Cisco Spam & Virus Blocker

License Registration **Network** Security Review

Data 1 (Default IP 192.168.42.42)

Data 2 (Incoming Mail)

Network Settings

Blocker Hostname: (Ex: blocker.example.com)

Blocker IP Address:

Subnet Mask:

Gateway IP Address:

Time Zone:

DNS: ☐ Use the Internet's Root DNS Servers
☒ Use the specified DNS Servers:

DNS Server IP Address:

DNS Server IP Address:

Help Fight Spam: ☒ I would like to help fight spam by sharing anonymized information with Cisco. [Learn what information is shared...](#)

Mail Configuration

Accept mail for these domain(s):

Exchange/Mail Server:

Administrator Settings

Administrator Email:

Your new administrator password:

Confirm your new password:

[Previous](#) [Next >](#)

**Data 2
Network
Settings**

Information from
Pre-install
checklist

**Alert
Recipient**





Running Setup Wizard (Cont.)



Cisco Spam & Virus Blocker

1 License

2 Registration

3 Network

4 Security

5 Review

Anti-Spam Policy

How would you like to handle spam?

☒ Block and Quarantine (recommended)
☒ and notify users with a daily digest.

☐ Quarantine All
☒ and notify users with a daily digest.

☐ Tag and Deliver

Anti-Virus Policy:

☒ Block Viruses

< Previous

Cancel

Next >

More Information

Mouse over fields to the left for additional notes.


Default
Security
Settings





Reviewing your System Setup Values



Cisco Spam & Virus Blocker

[1 License](#) [2 Registration](#) [3 Network](#) [4 Security](#) [5 Review](#)

Review Your Configuration

Please review your configuration. If you need to make changes, click the edit link to return to the page you'd like to edit.

Registration [Edit]

Company Information:

Juliet Engineering
5343 Technology Drive
San Jose, California 94493
United States

Primary Contact:

Joel Smith
Joel@exchange.juliet.com
Business: 408 239-2498

Secondary Contact:

N/A

Network [Edit]

Blocker Hostname:

smtp.juliet.com

Blocker IP Address (Data 1):

192.168.10.110

Subnet Mask:

255.255.255.0

Gateway IP Address:

192.168.10.1

Time Zone:

America/Tijuana

DNS:

192.168.10.200

Help Fight Spam:

Enabled

Accept Mail for these domains:

2
exchange.juliet.com

Exchange/Mail Server:

[172.20.0.32]

Administrator Email:

Joel@exchange.juliet.com

Administrator Password:

(Hidden)

Message Security [Edit]

Anti-Spam Policy:

Block and Quarantine and send daily digest

Anti-Virus Policy:

Enabled

[Previous](#) [Cancel](#) [Install Configuration](#)





Verifying the Installation



Cisco Spam & Virus Blocker

Monitor

Mail Policies

Security Services

Network

System Administration

Next Steps

Is Your Network Ready?



Confirm Firewall Settings.

Verify that you have opened all necessary ports in your firewall. For example, ensure you open port 25 on your firewall so Blocker can accept mail.

> See Blocker documentation for more information on firewall configuration.

Confirm NAT Settings.

If your network environment contains a NAT device, confirm it is configured for port forwarding to Blocker.

> See Blocker documentation for more information on NAT device configuration.

Confirm the MX Record configuration.

Your MX record is used to help route incoming mail to a mail server. You must change the MX record to point to Blocker.

> See Blocker documentation for more information on MX record configuration.

System Test

System Test

The system test checks Cisco Blocker for internet connectivity and basic mail handling.

Enter an email address that contains a valid recipient domain:

[Run System Test...](#)

Blocker is ready to receive email.

[Run System Test...](#)





Verifying the Installation



Subject: Welcome to Cisco Spam & Virus Blocker!
From: MAILER-DAEMON@alpha.com
Date: Fri, November 21, 2008 4:30 pm
To: alan@exchange.alpha.com
Priority: Normal
Options: [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#)

Congratulations, Blocker is successfully sending email!

As a final test, we recommend you send yourself a message to verify Blocker is receiving email traffic.

1. Send email to your company account from a personal account like Gmail or Yahoo!

2. Within a few minutes, you should receive your message. Confirm that Blocker processed this message by going to the https://mgmt.alpha.com/monitor/reports/incoming_mail. The email domain you used to send the test message should be listed.

Once you've completed this final test, you've confirmed Blocker is protecting your email systems--not only from today's threats, but from those certain to evolve in the future.

Incoming Mail: Domains

[Addresses](#) | [Domains](#) | [Network Owners](#)

[Printable \(PDF\)](#)

Time Range:

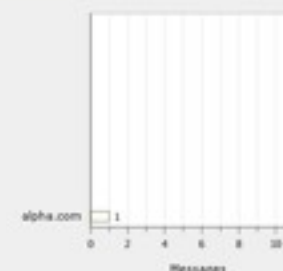
Nov 2008 21:00 to 21 Nov 2008 21:39 (GMT)

Data in time range: 99.92 % complete

Senders by Total Threat Messages

No data was found in the selected time range

Top Senders by Clean Messages



[Info...](#) | [Export...](#)

Incoming Mail Details

Summary

Sender	Messages							Clean
	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	
alpha.com	1	0	0	0	0	0	0	1

[Info...](#) | [Export...](#)





More Information



- Cisco Small Business Web Site: www.cisco.com/smallbusiness
- Cisco Partner Central – Security: www.cisco.com/go/smbpartner/security
- Cisco Spam & Virus Blocker: www.cisco.com/go/blocker





Logicom IT Distribution SRL

- Email: sales@logicom.com.ro
- Tel: (+4) 021 24 24 226
- Fax: (+4) 021 312 55 45
- Office and warehouse: Sos. Bucuresti – Targoviste, Nr. 12A, Corp A, et. 4, Mogosoaia, Jud. Ilfov



