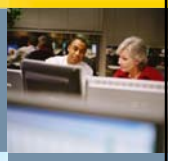
symantec.



Schutz vor Spam mit Traffic Shaping

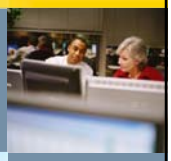
Patrick Heinen
Enterprise Technical Account Manager

symantec.

Agenda

- The email security problem
- Powerful email threat protection
  - Email Firewall
  - Antispam filtering
  - Antivirus scanning
  - Content compliance
  - Message integrity
- Spam best practices

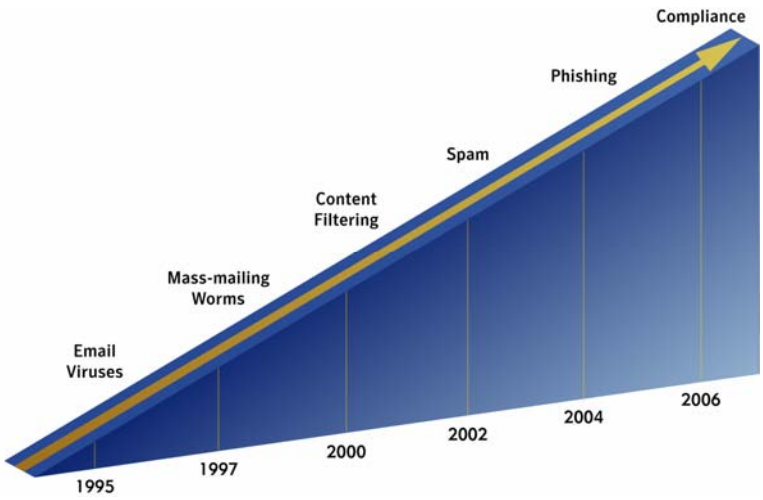
symantec.



The email security problem

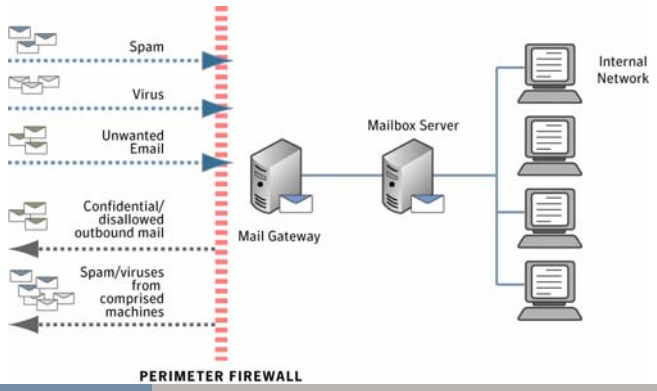
symantec.

Email threats are evolving



Email gateway is the primary conduit for threats

- Firewalls and most network security products ineffective against email threats
- Email flows freely through port 25



The impact of email security issues

Spam	Viruses and Malicious Content	Escalating Unwanted Traffic at Gateway	Content Control
▪ Lost productivity ▪ Resource drain ▪ False positives due to incorrect filtering	▪ System downtime ▪ Compromised machines	▪ Decreased bandwidth ▪ Overloaded server resources and mail storage space ▪ Increased resource cost	▪ Lack of policy enforcement ▪ Regulatory compliance vulnerability ▪ Danger of lawsuits

Administrator's Key Challenges

1. Safeguard organization from email threats
2. Preserve free flow of vital email from legitimate sources
3. Do this with as little administration as possible

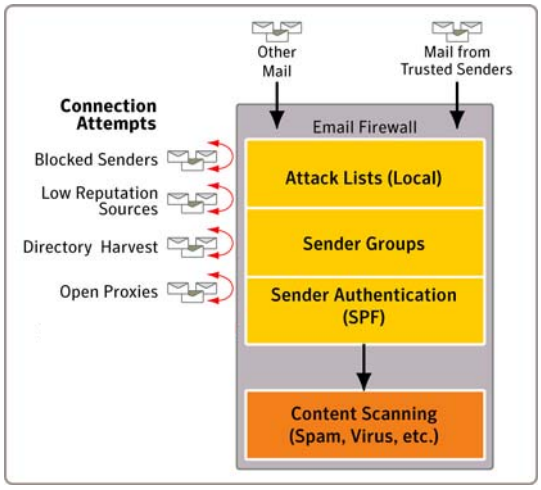
Critical elements for email security solutions

Email Firewall

Email Firewall: The first line of defense

- Feature overview
  - Controls which senders can connect to gateway MTA
  - Takes action before message proceeds further in filtering process
  - Denies access to malicious or unwanted senders
- Benefits
  - Reduces volume of mail that needs to be filtered
  - Saves resources and capacity
- Symantec Advantage
  - Leverages Sender Reputation Service to accurately characterize email sources
  - Patented TurnTide traffic shaping technology discourages spammers from targeting your site

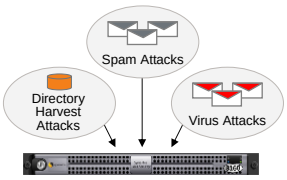
Typical threats addressed by Email Firewall



How the Email Firewall identifies abusive senders

Leveraging global data

- Check sender's global reputation



Analyzing local patterns

- Track how many times senders send spam, viruses, or other threats

Based on administrator lists

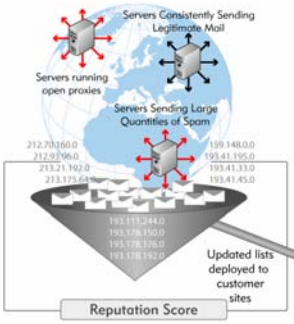
- Lists of blocked IP addresses
- Lists of allowed IP addresses

Leveraging global data: Sender reputation lists

Email Firewall accept or rejects message based on global Sender Reputation

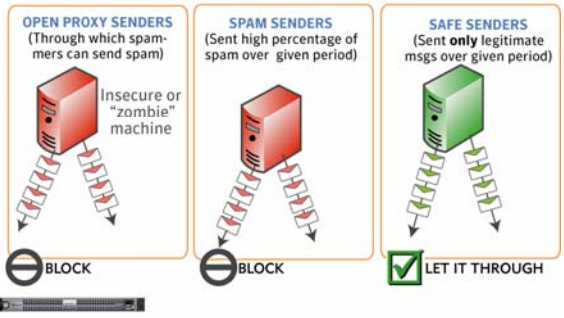
1 At Symantec

Symantec determines reputation for senders based on analysis of global email traffic



2 At Email Firewall

If incoming sender is on Sender Reputation List, Email Firewall takes action.



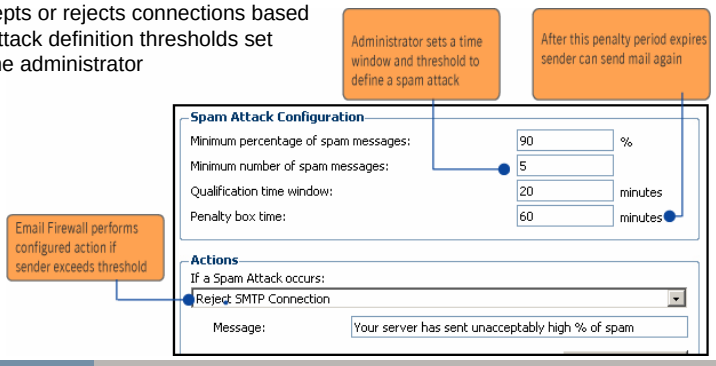
Sender Reputation Service vs. Other Reputation Approaches

- Tracks multiple dimensions of behavior with three lists
- Leverages Symantec's unprecedented visibility into email traffic
  - Filters over 106 billion messages/month
  - Filters over 15% of global Internet traffic
  - Filters mail for over 300 million users
- Ensures against misidentification/false positives
  - Dynamically rebuilds lists from scratch every hour to incorporate new changes
  - Lists are data-driven - no buy out!

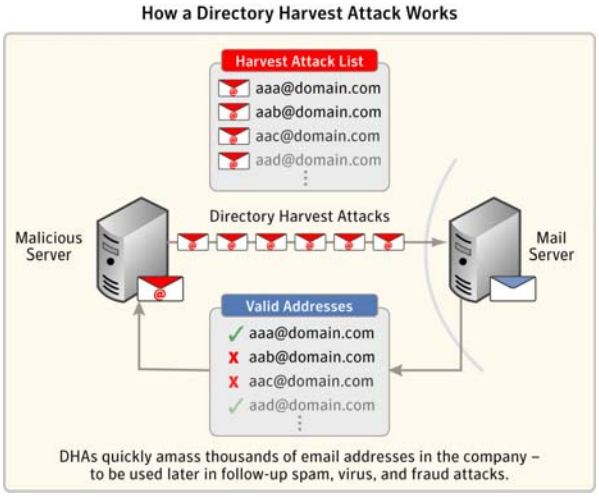
Dynamic analysis of local patterns

In addition to global analysis, the Email Firewall

- Dynamically analyzes **local traffic patterns**
- Performs frequency analysis, tracking how many times a specific sender (IP) sends spam, virus, directory harvest attempts, etc
- Accepts or rejects connections based on attack definition thresholds set by the administrator



Local attack example: directory harvest threat



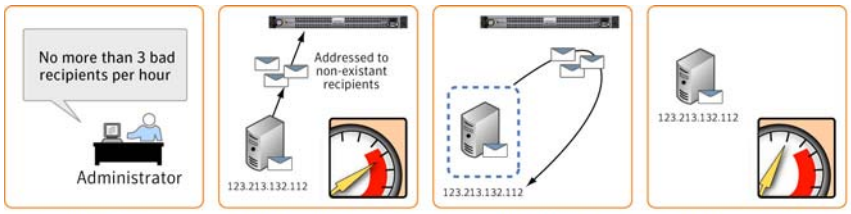
Impact

- Resource waste. Mail server must process all connection requests
- Theft of corporate data

The challenge

- Cannot address via content-based scanning
- Must pre-empt attack before the MTA accepts the message

How the Email Firewall stops directory harvest attacks



1. Administrator sets threshold.
To combat DHA, administrator specifies the maximum number of bad/unknown recipients that an IP address can target in a specified window of time.

2. Sender exceeds threshold.
The appliance will reject connections from the sender IP address for a configured period of time.

3. Sender lands in penalty box.
The administrator can configure how subsequent messages from this sender will be handled. In this case, messages are rejected before being accepted by the MTA.

4. Penalty period expires.
After the penalty period has expired, IP addresses are automatically removed and can send email.

Other Applications: Also works with spam and virus attacks

IPs and senders specified by Administrators or 3rd parties

- Email Firewall also recognizes senders specified by administrators:
  - IP addresses whom you never want to receive email
  - IP addresses from whom you always want to receive email
  - Third party lists of blocked and allowed IP addresses
- Create policies to control what happens to connection or message
  - E.g., reject messages from blocked IPs

Connection-level actions at the Email Firewall

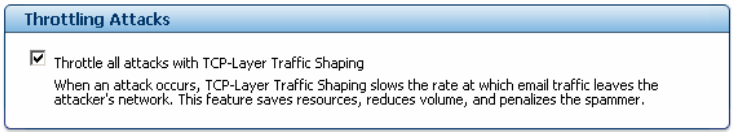
Defer SMTP connection
- MTA does not accept connection
- Sender receives temporary rejection
- Sender can “try again later”

Reject SMTP connection
- MTA does not accept connection
- Returns a permanent rejection to sending email server

Advantages of connection management: Dropping connection before mail is accepted results in a lower volume of spam or unwanted mail that needs to analyzed

Traffic Shaping option

- Available as an action for local attacks only
- How it works
  - Works at the network/TCP level
  - Uses TCP traffic shaping techniques to slow down (throttle) incoming connections from spam senders
  - Restricts ability of spammers to send high volume of messages
- Result
  - Spam backs up on spammers server, encouraging them to pick easier target
- Powered by unique, patent-pending technology acquired from TurnTide
- Full featured Traffic Shaping is available in Symantec Mail Security 8160



Antispam filtering

Antispam filtering powered by Brightmail

- Feature overview
  - Filtering powered by backed by Brightmail technology and infrastructure
  - False positive prevention
  - Gateway-based multilayered antispam engine
- Benefits
  - Restores employee productivity
  - Saves resources at groupware layer
- Symantec Advantage
  - Catches 95% or more of spam
  - Ensures that legitimate mail is untouched (99.9999% accuracy)
  - Turn on protection and walk away

Spam protection backed by the BLOC

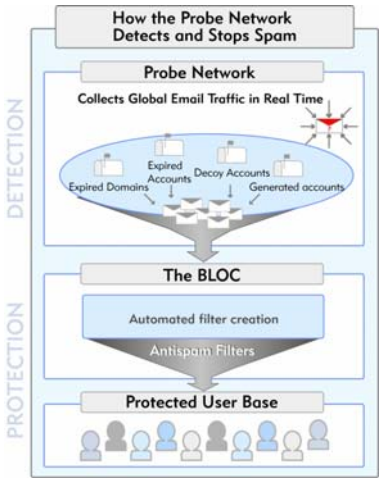
- Multiple, globally distributed response centers
- Analyzes and responds to the latest spam threats
- Transmits updated email security defenses every 10 minutes
- Removes the ongoing administration burden for spam defense

Some Facts About the BLOC

Spam defense coverage:	24x365
Languages spoken:	12
Decoy accounts monitored:	Over 2 million
Decoy (honeypot) spam processed/day:	Tens of millions
Countries represented by the Probe Network:	Over 20
Operation center locations:	San Francisco Dublin Sydney Taipei

Leveraging the unique Probe Network

- What it does
  - Collects large quantities of spam for analysis
  - Feeds spam to the BLOC for filter creation
- Why its important
  - Provides early warning of real-time spam attacks and other threats
  - Best infrastructure to track global sender reputation
- How its unique
  - **Patent-protected**
  - **Global coverage** with ISPs/Enterprise probes in North America, EMEA and APAC
  - **Widest reach** with over two million decoy email addresses and statistically representative of over 300 million more addresses



False positive prevention

- False positives (legitimate mail misclassified as spam) creates productivity and business loss
  - Sidelining of important mail (purchase orders, confirmations)
  - Users searching through quarantine
  - Admins responding to help desk tickets
- With Brightmail, you can “filter without risk”
  - Validated 99.9999% accuracy
  - Daily monitoring or filter accuracy by Symantec
  - Automatic review of all potential false positives

InfoWorld

Symantec Brightmail Anti-Spam 6.0

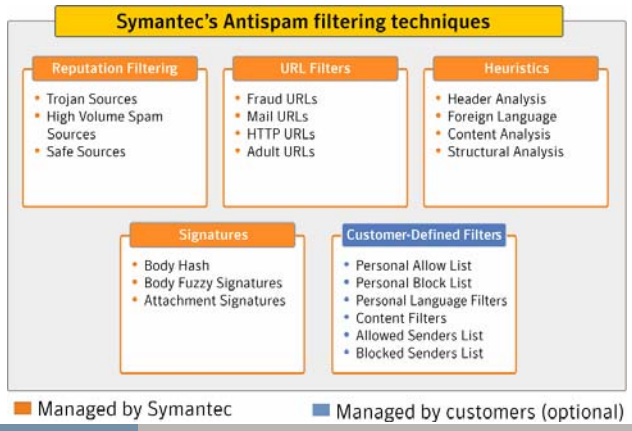
Symantec, symantec.com/

Excellent 9.1

criteria	score	weight
Accuracy	10.0	25.0%
Manageability	9.0	25.0%
Ease of use	9.0	20.0%
Setup	8.0	20.0%
Value	9.0	10.0%

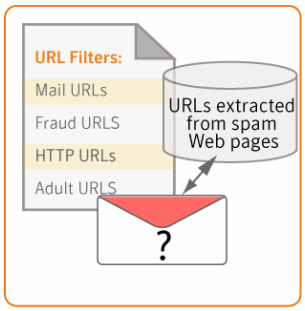
Multilayered antispam technologies

- There is no silver bullet anti-spam technology
- Different detection techniques are effective against different types of spam



Unique URL filters

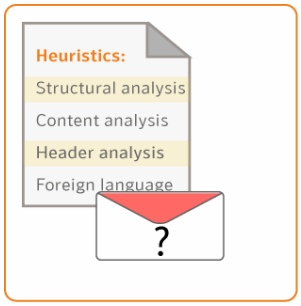
- Approach: Matches URL links in message against spam URL database maintained by Symantec
- Symantec URL filters
  - Based on dynamic and real-time data from Probe Network
  - Highly effective: responsible for over 70% of Symantec spam-catching
  - Optimized against obfuscation, disguised URLs, and redirects
  - Currently in forth generation
- Benefits
  - Updated URL lists deployed every 10 minutes
  - No administrator burden—Managed by Symantec
  - Provides added protection against phishing URLs used in fraudulent email



URL FILTERS
Does message contain an embedded link that leads to a spam Web page?

Heuristic filters

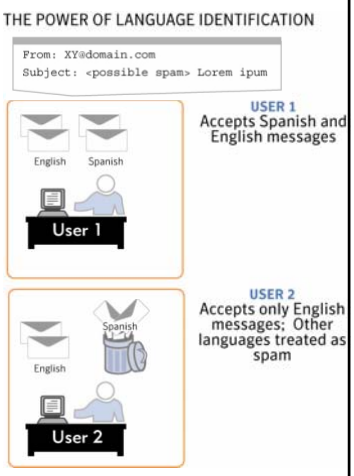
- Proactive approach designed to catch new spam
- Just one part of a multilayered arsenal
  - Not the primary antispam technology
  - Designed to capture the upper 5-10% of overall spam catching effectiveness
- Optimized for speed and accuracy
  - Uses compiled code that is 2-4x faster than interpreted implementations
  - Tested against legitimate mail before deployment
- No training required
  - Automatically trained and updated by Symantec using Probe Network data
  - Automatically updates incorporated every 10 minutes at customer site



HEURISTIC FILTERS
Does the message display common attributes of spam?

Language-based filtering

- Multilingual spam is a key pain point for international and global companies
- Symantec language identification ability
  - Identify language in which message is written
  - Support for 11 languages
  - Unique in the industry
- Benefits of language identification
  - Organizations can specify “approved” languages
  - Treat all other languages as spam
  - Allow end users to create own set of approved and blocked languages

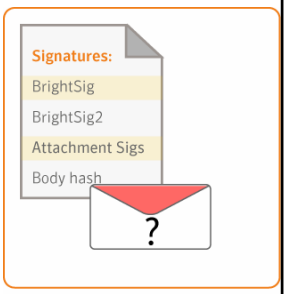


Language filtering abilities: the Symantec advantage

Technology	**Detection**	Identifies the language of a message in 11 languages
	Performance	Runs only the filters that apply to the message's language
	Filtering breadth	▸ Over 350 language-specific heuristics ▸ Other technologies (URL filters) are language-agnostic ▸ Geographically-based reputation filters
	User Preferences	▸ Users can define languages they want to receive messages in ▸ Treat others as spam
Resources	**Visibility**	▸ Probe Network attracts spam originating from over 20 countries ▸ Global BLOC coverage (US, EMEA, APAC) ▸ Probes from global ISPs
	Language Expertise	▸ Native language speakers in BLOCs (over 15 languages spoken) ▸ Translation tools for non-native speakers

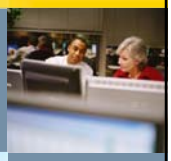
Third generation signature technology

- Approach: Distills specific spam attack down to essential fingerprint
- Symantec signatures
  - Based on real-time spam attacks
  - Optimized against spammer evasion techniques (randomization, HTML noise, obfuscation)
  - Updated signatures deployed every 10 minutes
- Benefits
  - Highly accurate: based on actual spam
  - Provides confidence level against false positives
  - No administrator burden—Managed by Symantec



SIGNATURES
Does message or its variants match a signature deployed by Symantec experts?

symantec.



Antivirus scanning

symantec.

Symantec AntiVirus

- Feature overview
  - Analyzes incoming and outgoing mail for viruses and mass-mailing worms
  - Based on Symantec Scan Engine
  - Mass-Mailer Cleanup
  - Supports optional Heuristic-based detection
  - Backed by Symantec Security Response
- Benefits
  - Prevents viruses and unwanted content from passing through the gateway
  - Reduces system downtime
- Symantec Advantage
  - Award-winning Symantec technology
  - Rapid and reliable virus scanning protection
  - Up-to-date protection automatically applied

Symantec Scan Engine technology

- Rapid, reliable scanning and repair engine
  - Multi-threaded scanning system for added performance
  - Repairs viruses within email attachments, including popular compressed file formats (zip, MIME/UU, etc)
  - 23 Virus Bulletin 100% awards
  - ICSA Product Certification
- Proven protection against the latest threats
  - Rapid Release definitions made available every hour
  - Designed to head off emerging threats
  - 99.98% success rate
- Maximum uptime during definition updates
  - Modular engine updates virus definitions and scan engines without having to redeploy the software or restart services
  - No interruption in virus scanning to get new definitions

DEFINITION-BASED AV SCANNING
Does the unpacked attachment match virus definitions deployed by Symantec experts?

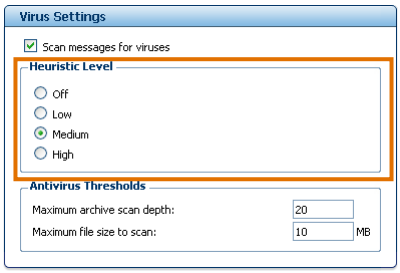
Mass-mailer cleanup

- Side-effects of mass-mailing worms
  - Unnecessary sender notifications
  - Multiple spawned emails that serve no purpose
  - Can number in the hundreds per recipient
- Mass-Mailer cleanup feature
  - Eliminates remnants of mass-mailer worm
  - Helps eliminate unnecessary calls to the helpdesk from concerned users and customers

MASS-MAILER CLEANUP
Automatically deletes unnecessary messages left behind in wake of mass-mailing worm attack

Heuristics-based antivirus scanning

- Detect “virus-like” behavior with optional heuristics
- Identify and repair unknown viruses
  - Detect up to 90 percent of new macro viruses
  - Detect up to 80 percent of new and unknown executable file viruses, including malicious mobile code
- Tailor aggressiveness based on performance needs



HEURISTICS-BASED SCANNING
Does the attachment “look like” a virus?

Content compliance

Content compliance

- Feature overview
  - Attachment blocking
  - Custom dictionaries
  - Custom filters
  - Annotations
- Benefits
  - Enforce corporate email policies
  - Reduce legal liability
  - Ensure compliance with regulatory requirements
- Symantec advantage
  - Easy to use
  - Integrated with spam and virus policies

Attachment Lists

- Control attachments that can be sent or received
  - Multimedia or executable files are typical
  - Applies to MIME-type, extension, or filename
- Flexible criteria
  - "is", "begins with", and others
- Multiple actions
  - **Strip** (remove) is most common
  - **Notify** can informs recipient of action taken
- Key benefits
  - Enhances employee productivity
  - Can reduce legal and human resource issues
  - Provides secondary line of defense to block viruses and malicious content
  - Protect confidential information from leaving the organization

ATTACHMENT LIST
Does message contain a restricted attachment type?

Custom Filters

- Create general purpose content filters
  - Applied globally for the organization
- Flexible criteria include
  - IP Address
  - Sender, Recipient, From, To, CC
  - Header Field
  - Body
  - Size
  - MIME Header
- Key benefits
  - Enforces a range of corporate policies

CUSTOM FILTERS
Does message trigger a custom content filter?

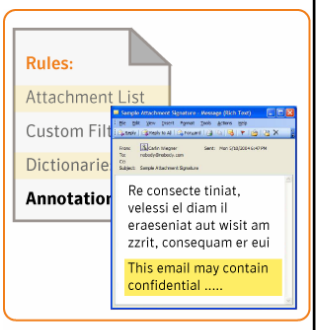
Dictionaries

- Specify lists of words to filter
- Seven pre-populated and editable lists
  - Profanity (Explicit/ Ambiguous)
  - Racial (Explicit / Ambiguous)
  - Sexual (Explicit / Ambiguous)
  - Sexual Slang
- Administrator defined lists
  - Internal code names, text such as "VPN password"
- Multiple actions
  - Examples include Quarantine or Forward to administrator for review
- Key benefits
  - Enforce corporate/HR policies regarding objectionable words
  - Prevent NDA, proprietary, or confidential material from leaving email gateway

DICTIONARIES
Does message contain restricted words or keywords?

Annotations

- Add customized annotations to messages
- Typical applications
  - Legal disclaimers
  - Virus warnings
- Supports plain or HTML text format
- Benefits
  - Add disclaimers to messages from specific departments (e.g., Legal)
  - Inform senders if message is out of compliance



ANNOTATION
Adds a custom disclaimer or text to inbound or outbound messages.

Message integrity

Message integrity

- Feature overview
  - Anti-forgery checks using SPF
  - Support for secure email using TLS
- Benefits
  - Reduces spoofing by ensuring that mail is coming from where it should be coming from
  - Promotes a higher level of security and privacy for email communications
- Symantec Advantage
  - Flexible configuration and actions

SPF authentication in the Symantec Mail Security 8200

- SPF is a global standard designed to reduce domain spoofing and forgery
- Optionally authenticates using SPF
  - If server is not listed in approved list for the domain, the message fails
  - If domain doesn't have SPF records, processing continues
- Apply SPF checks to the domains you want
  - Check for all incoming messages
  - Check only for specific domains
- Specify multiple actions based on authentication failure
  - Typical actions include Delete, Quarantine, Markup

Encryption support using TLS

- Optional TLS-based encryption between Symantec Mail Security 8200 and other MTAs
- How it works
  - Prior to transmitting or receiving any data, communications between Scanner and other MTAs are authenticated and then encrypted
  - Sent or received data is sent over an encrypted connection
- Flexible configuration for accepting TLS
  - For inbound—Can be globally enabled or disabled
  - For outbound—Can be globally enabled or disabled. If enabled, TLS can be required for a given set of domains.

Spam best practices

- Turn off automatic processing of meeting requests
- Limit where you post your e-mail address
- Disguise your e-mail address when you post it to public places
- Use multiple e-mail addresses for different purposes
- Review the privacy policies of Web sites
- Watch out for check boxes that are already selected
- Don't reply to spam
- Don't contribute to a charity based on a request in e-mail
- Don't forward chain e-mail messages


symantec.
SPAM
So good...