

Email Marketing 201

How a SPAM Filter Works

Craig Stouffer

Pinpointe On-Demand

cstouffer@pinpointe.com

(408) 834-7577 x125

www.twitter.com/pinpointe

www.pinpointe.com/blog

Mark Feldman

NetProspex VP Marketing

mfeldman@NetProspex.com

(781) 290-5714

@netprospex

blog.netprospex.com

Like the Content? Please Share!

- Our webinars are free so please share!
- Tweet our tips: @Netprospex, @Pinpointe
- Share our blogs:
 - blog.pinpointe.com
 - blog.netprospex.com
- Slides, recording at: pinpointe.com/resources

Pinpointe Expertise

- **The Most Feature Rich Email Marketing Service**
- **Enterprise version: 5-250+ users, high volume**
- **Behavioral Targeting – Improves Results 35%+**
- **“Constant Contact on steroids!” – *Pinpointe customer***

What Sets NetProspex Apart?

- Augment Email Data
- 21 million decision makers
- User-generated contacts
- **Verified + guaranteed**
- Hard-bounce replacement
- All job titles & industries
- Thousands of new contacts per month
- Title, email address, direct dial, social media, URL
- Buy or trade

Gary Halliwell
Chief Executive Officer

Email available
ghalliwell@netprospex.com

Phone available
Direct: (781) 290-5716
Main: (888) 826-4877

Social Media
<http://www.linkedin.com/in/garyhalliwell>
<http://twitter.com/ceonetprospex>
<http://www.facebook.com/gary.halliwell>

NetProspex
318 Bear Hill Road
Waltham, MA 02451 [map](#)
<http://www.netprospex.com>

Estimated Accuracy: 84%
Verified on: 01/28/2010
[What does this mean?](#)

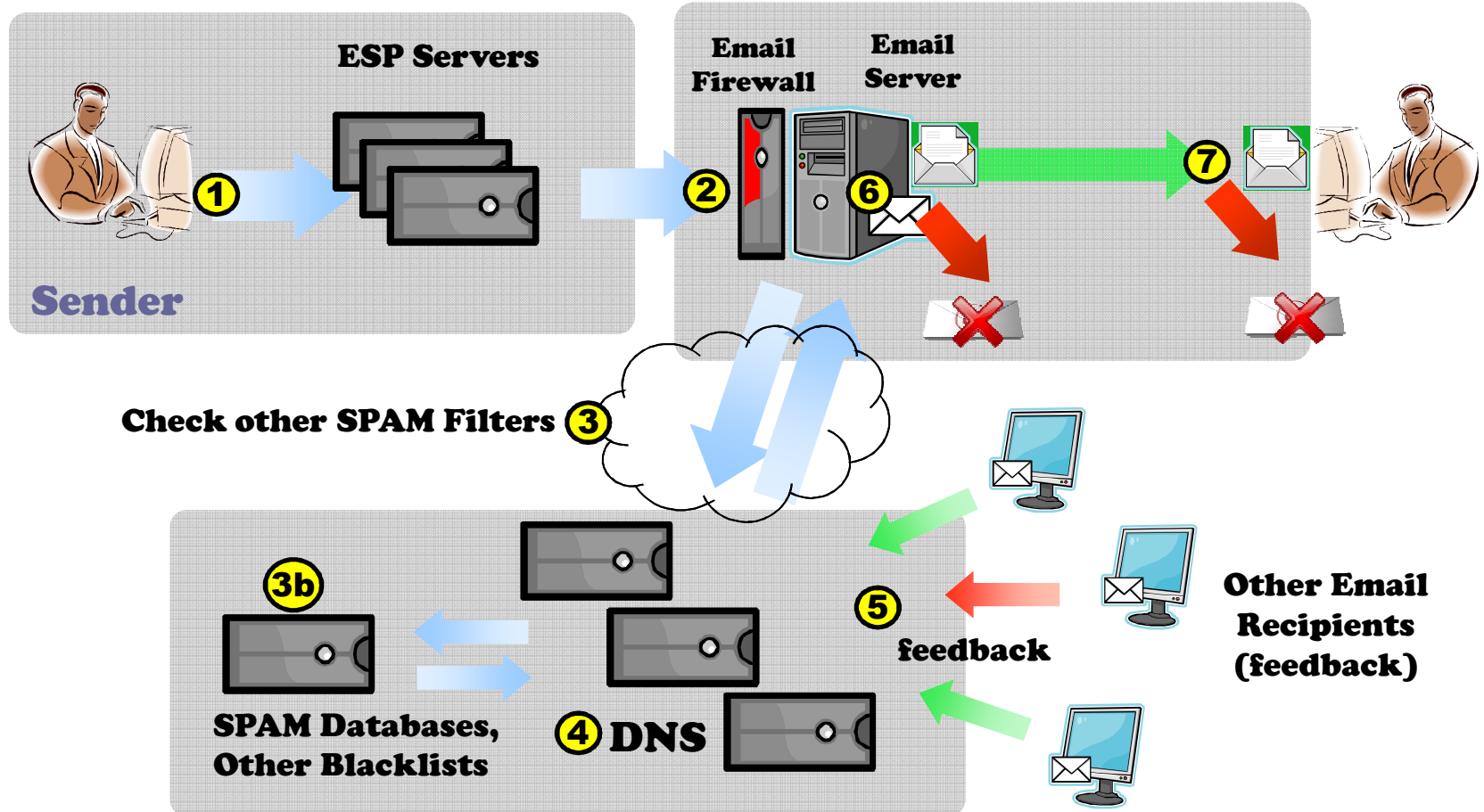
www.NetProspex.com
hello@netprospex.com
888-826-4877



Agenda

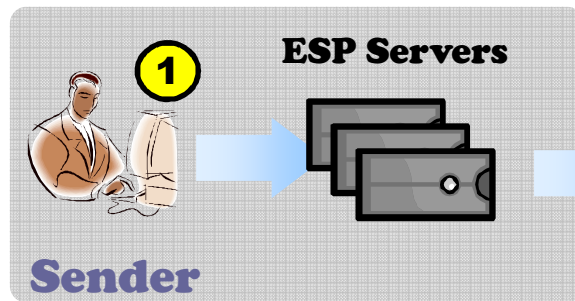
- **Overview: Email Delivery Architecture**
- **What Affects Email Delivery?**
 - Reputation
 - Authentication / Authorization
 - Sending Technology
 - Email Content

Email Delivery Architecture



Bet you thought it was simple!

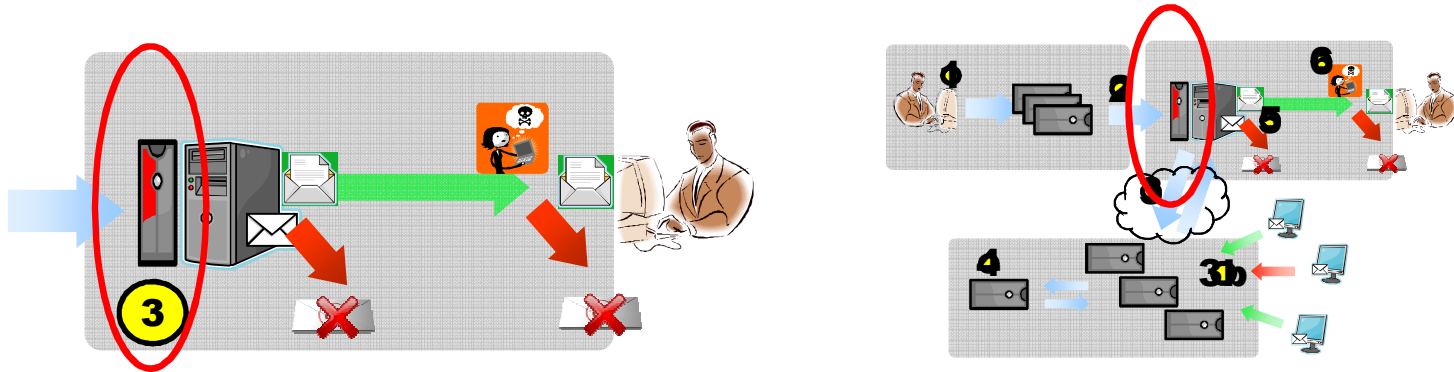
Create / Send Email (Using an ESP)



Tip: “MTA” means ‘Mail Transfer Agent – a fancy name for an email server (typically outbound)

- Create email w/ external HTML editor or online editor
- Best results: create “multi-part version” (Text + HTML)
- Run spam checker (Pinpointe feature)
- Use Pinpointe previewer to preview in various email clients (Outlook '03, Outlook '07, Yahoo, etc)
- Schedule / send away!
- Email merge occurs – emails sent from ESP mail servers

Email Received by Email Firewall



- Email received by recipient's corporate spam filter
- Spam filter (email firewall) checks:
 - Reputation of sending email server(s)
 - Sending mail server settings
 - Authentication (Are you who you say you are?)
 - Checks Authorization
 - Content filter / spam score (Spamassassin)
- If all tests pass → next step **(YEAH!)**

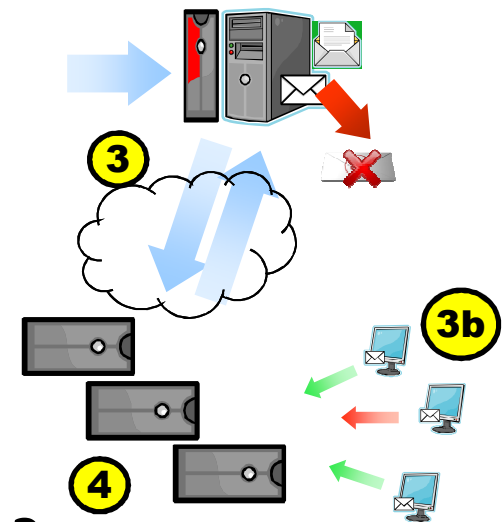
Importance of Email Reputation

- ReturnPath claims >70% of decision to forward is based on reputation
- SPAM filters are networked
- Accumulate history of email senders
- Accurate view of reputation over time
- Share reputation info to other filters
- Real-time!



Networked SPAM Filter Checks

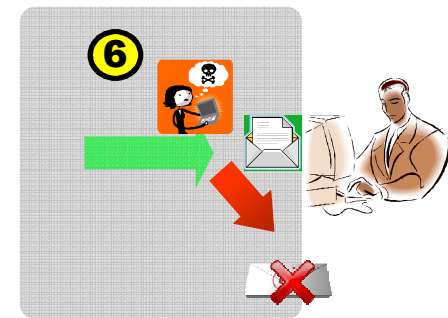
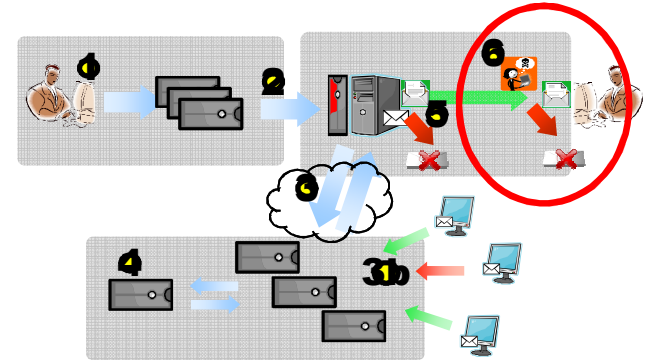
- Aggregated reputation information
- Email server IP history/reputation
- Is sender on global white-list?
- Blacklisted URLs? Domain? IPs?
- Any 'SPAM honeypot' hits?
- SPAM complaint rates? (<1:1000)
- Bounce / delivery rates against domain?
- Do reverse DNS entries match?
- How long has domain been registered?
- When does domain expire?
- If PASS -> Forward to local inbox **(YEAH!)**



Local SPAM Filter / Inbox (Finally!)

Local Inbox Filter

- Applies local / personal settings
- Is sender locally white-listed?
- ... In address book?
- Is sender /sending domain locally blacklisted?
- Have I marked previous emails from sender as SPAM?/not SPAM?
- Often runs a local content filter with local settings



If you pass all this... **You've made it to the in inbox!**

Email Delivery: Infrastructure

What is required by ESP servers?

- Proper IP address configuration
- DNS / Reverse DNS settings are correct
- Properly formed “envelope header”
From/Reply-to
- Rate limiting - match receiving domain’s limits
- IP classes of service / possibly dedicated IPs

- Errors cause emails to be filtered
- Spammers don’t do these right!

What is Email Authorization?

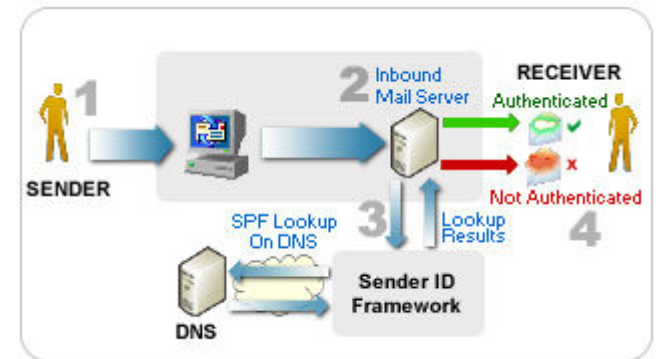
- Are the sending email servers authorized to send on behalf of your domain?
- Protects against email servers being ‘hijacked’ or “spoofed” for phishing attacks, scams etc
- Two standards:
 - Sender ID (Microsoft) and
 - ‘Sender Policy Framework’ (“SPF”)
- Different standards but use compatible format

Authorization – What SPF Does

- SPF is an open standard
- SenderID is ‘championed’ by Microsoft (msn, hotmail)
- Verifies servers sending email are authorized to send on behalf of the domain
- How?
 - Domain admin publishes SPF record in top-level-domain DNS record
 - DNS TXT Entry lists servers authorized to send
- For more information:
 - www.openspf.org
 - old.openspf.org
 - www.microsoft.com/senderid/wizard

SPF Authorization:

- Sender transmits email
- Receiver's mail server receives email.
- Server checks which domain claims to have sent the message
- Receiver checks if sender has permission to send for designated domain (via DNS)
- If PASS -> Allow



Authorization –SPF Example

- Domain = mycompany.com, registered w/GoDaddy.com
- Your ESP is Pinpointe (pinpointe.com)
- Go to old.openspf.org/wizard – SPF tool

The SPF record:

```
v=spf1 a mx include:pinpointe.com ~all
```

can be explained as:

v=spf1	<code>v=spf1</code>	This identifies the TXT record as an SPF string.
a	<code>a</code>	mycompany.com's IP address is 208.239.76.34. That server is allowed to send mail from mycompany.com.
mx	<code>mx</code>	mycompany.com has one MX server, filter.kcl.net. It is allowed to send mail from mycompany.com. If you add more MX servers in the future, they'll automatically be allowed, too.
include:	<code>include:pinpointe.com</code>	Any server allowed to send mail from <code>pinpointe.com</code> is also allowed to send mail from mycompany.com.
all	<code>~all</code>	SPF queries that do not match any other mechanism will return "softfail". Messages that are not sent from an approved server should still be accepted but may be subjected to greater scrutiny.

Email Authentication:

- Are you who you say you are?
- Protects against server hijacking/spoofing for phishing attacks, scams etc
- Crypto solutions:
 - Domain Keys (DK)
 - DKIM (www.dkim.org)
 - Requires storage of public/private “keys”
 - Public key -> DNS record (like SPF)
 - Private key -> sending email servers
- “Highly desired” by some domains today

Authentication/Authorization: Impact

- What is the impact of not doing these today?
- No absolute answer – many variables
- Imperially – 5% ~ 15% impact
- Enterprises implementing NOW
- Non-compliant systems will see dramatic fall-off in delivery
- Best to be prepared with an ESP that can help

Email Delivery: Content Filtering

- Covered in Email Marketing 101 Webinar:
 - www.pinpointe.com/resources
- Analyzes email content for “spammy” phrases
- Often based on spamassassin engine
- Examples and tips covered in previous webinar
- Link to spamassassin tests:
 - http://spamassassin.apache.org/tests_3_2_x.html
- Tip: Always use your ESP’s online SPAM checker

Summary

- Email delivery is more than **just** content filtering
- If you understand email delivery, you will:
 - Design better / more efficient emails
 - Select vendors more intelligently
 - Improve delivery / response rates / ROI
- Resources-
 - www.twitter.com/pinpointe
 - www.pinpointe.com/blog

Contact Information

Goto www.pinpointe.com/get-started

Use coupon code: PPTNPW100 for 1 FREE month

Join us for future webinars

For questions, or to request a trial account, please contact:

Craig Stouffer

Pinpointe (Email Marketing)

cstouffer@pinpointe.com

(408) 834-7577 x125

www.twitter.com/pinpointe

www.pinpointe.com/blog

Mark Feldman

NetProspex

mfeldman@NetProspex.com

(781) 290-5714

[@netprospex](https://twitter.com/netprospex)

blog.netprospex.com