TOMORROW starts here.

CISCO

Cisco live!

Advanced Email Security with ESA

BRKSEC-3770

Raymond Jett

Technical Marketing Engineer

Agenda

- IPv6 support for ESA
- Specifics of Cloud/Hybrid Cloud E-mail Security and migration from on-prem
- How Message Filters can help your mail flow
- Anti-phishing technologies: Outbreak Filters, DKIM and SPF; why and how to implement them
- Q&A

Abstract

This technical session will tackle several advanced topics of e-mail security with a focus on Cisco's solution.

We shall begin by describing the level of IPv6 support in newer versions of AsyncOS, and what changes this brings to traditional e-mail processing.

Second part of the session will talk about recent trends of migrating towards the Cloud or Hybrid Cloud e-mail security solution, and what are the challenges and migration consideration.

This will be followed by a section on Message Filters, a powerful mechanism of mail flow filtering which was deliberately neglected out of caution.

Several Anti-phishing techniques will be laid out in the remainder of the session, outlining Cisco's Outbreak Filters, and providing insight into DKIM and SPF deployment considerations.

Prerequisites for this session are acquaintance with SMTP and e-mail security technologies; experience with Cisco E-mail Security products is desirable.

The target audience are security and email administrators of the enterprise email gateway. The audience will also benefit from following the session BRKSEC-3771 "Advanced Web Security Deployment with WSA" and BRKSEC-2695 "Embrace Cloud Web Security with your Cisco Network"

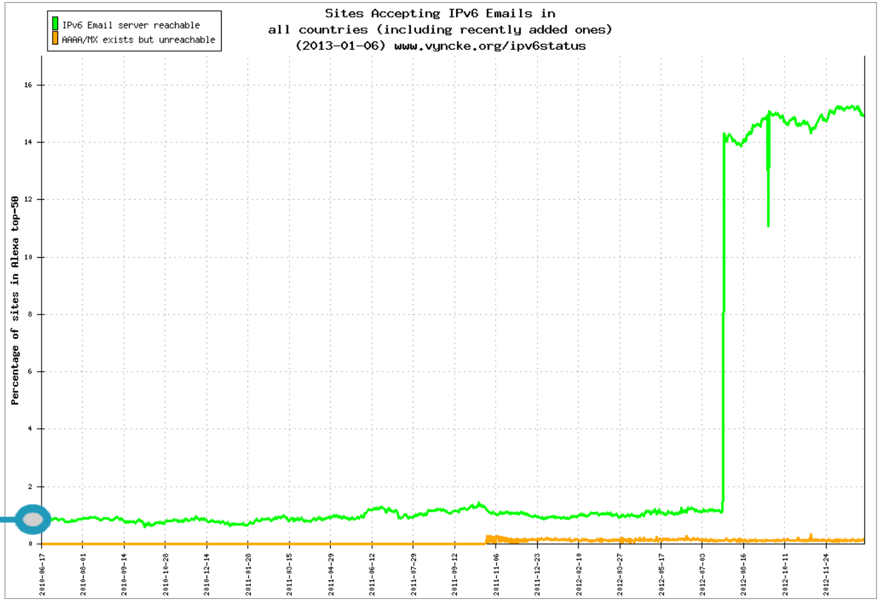
IPv6

E-mail Security Appliance and IPv6

- IPv6 code existed in AsyncOS as a separate code train for years
- With AsyncOS 7.6, IPv6 merged into production releases
- Phased approach for IPv6 support – more exposed functions first
  - **Phase 1: basics**
    - Networking (dual-stacked interfaces, routing, NIC pairing)
    - SMTP (HAT/RAT, SMTP routes, destination controls, SMTP Call-Ahead, filters)
    - Reporting (reporting, tracking, trace)
    - GUI/CLI
  - **Phase 2: everything else**
    - Inter-device communication (clustering, SMA communication)
    - Infrastructure services (alerts, SNMP, DNS, LDAP, FTP, updates/upgrades, support tunnels)

How Much of the World Accepts IPv6 E-mail?

Time scale: June 2010 – December 2012

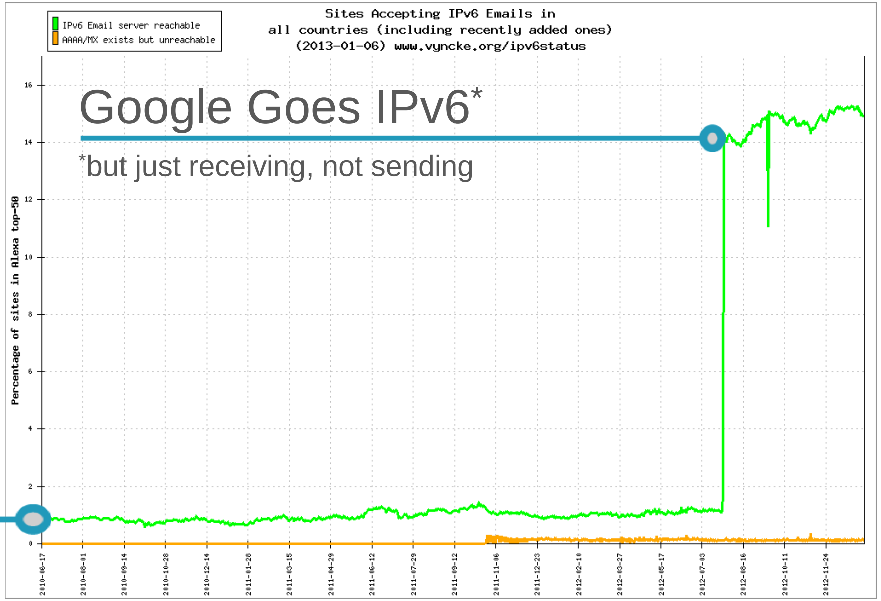


Until recently, only about 1% of sites globally even accepted IPv6 connections

Eric Vyncke talks more about IPv6 security at BRKSEC-2003!

How Much of the World Accepts IPv6 E-mail?

Time scale: June 2010 – December 2012



Google Goes IPv6*

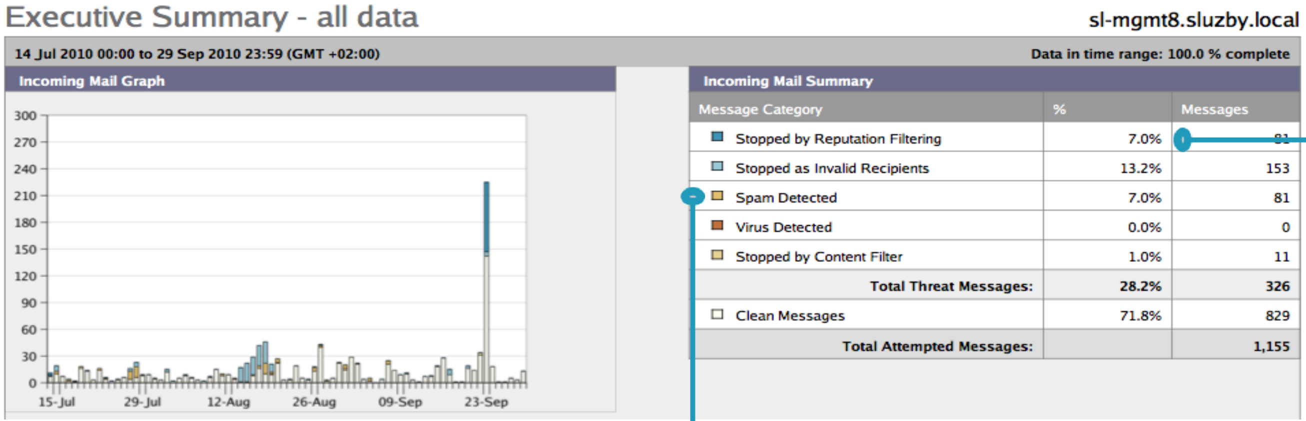
*but just receiving, not sending

Until recently, only about 1% of sites globally even accepted IPv6 connections

Eric Vyncke talks more about IPv6 security at BRKSEC-2003!

SBRS and IPv6

Back in 2010…



Executive Summary - all data

sl-mgmt8.sluzby.local

14 Jul 2010 00:00 to 29 Sep 2010 23:59 (GMT +02:00)

Data in time range: 100.0 % complete

Incoming Mail Graph

Incoming Mail Summary

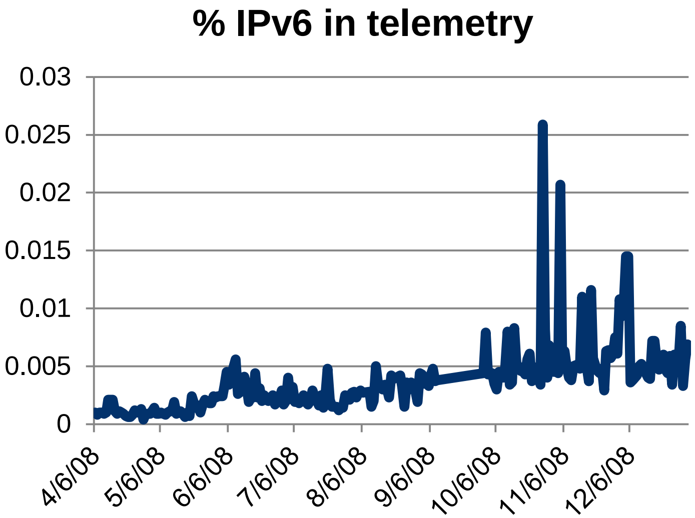
Message Category	%	Messages
🟦 Stopped by Reputation Filtering	7.0%	81
🟦 Stopped as Invalid Recipients	13.2%	153
🟨 Spam Detected	7.0%	81
🟧 Virus Detected	0.0%	0
🟨 Stopped by Content Filter	1.0%	11
Total Threat Messages:	**28.2%**	**326**
□ Clean Messages	71.8%	829
Total Attempted Messages:		**1,155**

Negligible reputation data

Traces of IPv4 spamming tools

…Not Much Different Today!

- Reality:
  - 1-2% of SMTP traffic is IPv6
  - IPv6-enabled spamtraps, although in place, not providing relevant amount of traffic
  - Lack of data feed providers for IPv6 SBRS



- Still, it’s a thing to come, and we’re ready – and:
- We Need Your Help: Have IPv6? Give us your feed!

Demonstration

- Configuring an IPv6 interface
- Sending an e-mail through IPv6 interface to IPv4 destination
- Sending an e-mail through IPv4 interface to IPv6 destination
- Viewing IPv6 information in tracking/reporting

Cloud/Hybrid Migration

Cisco Cloud E-mail

Choice of delivery options

Dedicated cloud infrastructure

Cloud capacity assurance

Cloud availability guarantee

CLOUD

- DLP and Encryption
- Targeted attack / APT defence with Cisco SIO
- Anti-Malware / Antivirus
- Outbreak Filter

Mobile smartphone email encryption

Anti-Spam

Defence against emerging IPv6 threats

EMAIL SECURITY FAMILY OF PRODUCTS

Appropriately sized to plug into your environment

High performance

Easy to install and manage

APPLIANCES

Cisco Cloud E-mail

Why migrate?

- **Lower operational cost vs. on-prem**
- **Guaranteed scalability / capacity assurance**
- **Service Level Agreements** 👍
  - 99.999% uptime
  - 99% inbound spam catch rate
  - 1/1 million FP rate
  - 100% known virus catch rate
  - 99.999% CRES uptime
- **Hybrid model: Best of both worlds**
  - Cloud for inbound, on-prem for outbound

Demonstration

- Connecting to a cloud system
- Connecting to Cisco ROS, opening a ticket

Migration Considerations

- **Challenge: Recipient validation and group policies**
  - Solution 1: Leverage SMTP Call-Ahead and open up your LDAP to the cloud
  - Solution 2: SMTP Call Ahead in the cloud + local policies on on-prem appliances
- **Challenge: Using Message Filters for incoming mail processing**
  - Solution: Open a ROS ticket for CLI access
- **Challenge: Using complex Incoming Mail Policies**
  - Solution: Alert the Activation Team, or work with your Cisco Security SE
- **Challenge: Split reporting/tracking**
  - Solution: Submit reporting data from hybrid devices to cloud SMAs
- **Caveat: Careful about the amount of generated traffic**

Cloud Deployment Limitations

- **Virtual Gateways are not supported**
  - Use Hybrid Deployment and on-prem ESAs for marketing email etc.
- **Limited administrative access**
  - “Administrator” account locked down; “Cloud Administrator” given to customers; limitations: no network configuration, shutdown/reboot, upgrade, cluster manipulation etc…
- **LDAP required a hole in the firewall**
  - But can be encrypted…
- **Upgrades are scheduled and performed according to Cisco’s upgrade schedule**

Centralised Centralised Management – Yes or No?

Be careful what you wish for…

- **In-the-cloud and on-prem boxes can’t be combined in a single cluster**

- **Do you really want to do that?**
  - Network data definitely not shared between them
  - On-prem boxes and Cloud boxes have completely different policies
  - Only advantage: “single pane of glass” management

- **Drawbacks**
  - Cloud and on-prem must be on the same SW versions
  - Unnecessarily complex configurations exchanged between all units
  - Would require privilege escalation beyond “Cloud Administrator” role, and CLI access

Message Filters

“Message filters allow you to create special rules describing how to handle messages as they are received by the Cisco IronPort appliance. A message filter specifies that a certain kind of email message should be given special treatment. Cisco IronPort message filters also allow you to enforce corporate email policy by scanning the content of messages for words you specify.”

Cisco AsyncOS 7.6 for Email Advanced User Guide

Chapter 6, “Using Message Filters to Enforce Email Policies

Message Filters: What They Are

- High-performance scriptable filtering capability
- Accessible from the CLI only (filters command)
- Working on entire mail flow
- Allowing complex logical operators between conditions
- Executed serially
- If enabled, always executed

A Message Filter

```
myFilter
If (mail-from==“bugs.bunny@warnerbros.com”) {
      drop();
}
```

A Message Filter

Label

```
myFilter
If (mail-from==“bugs.bunny@warnerbros.com”) {
        drop();
}
```

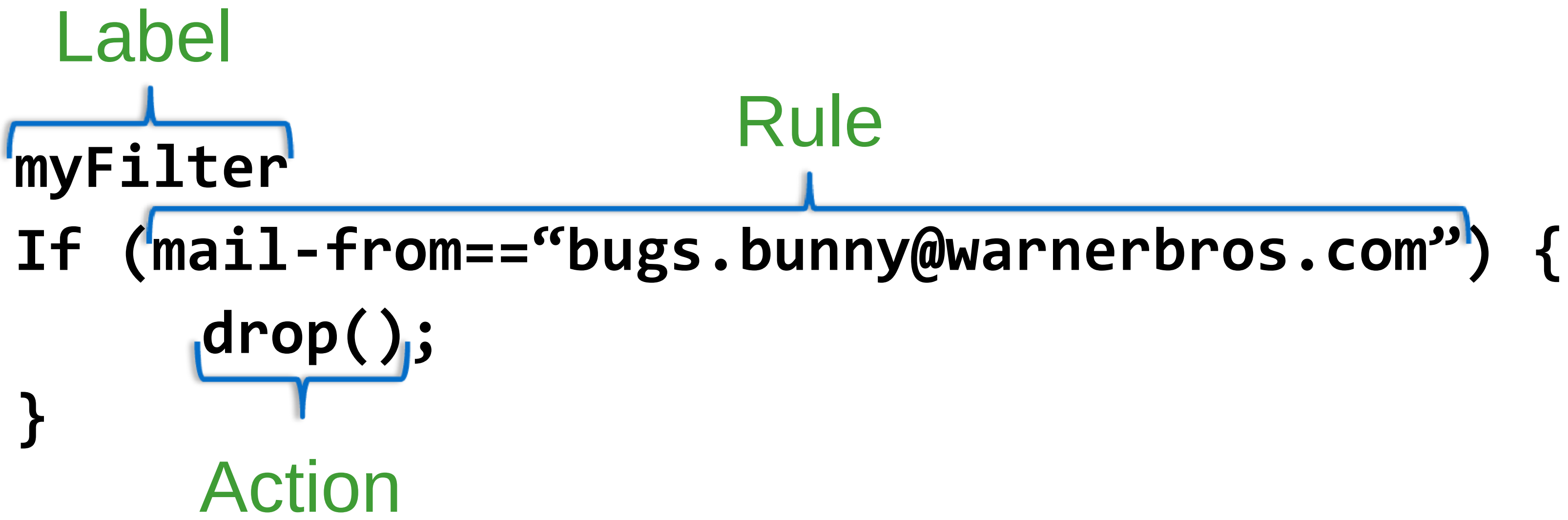
A Message Filter

Label

Rule

```
myFilter
If (mail-from==“bugs.bunny@warnerbros.com”) {
       drop();
}
```

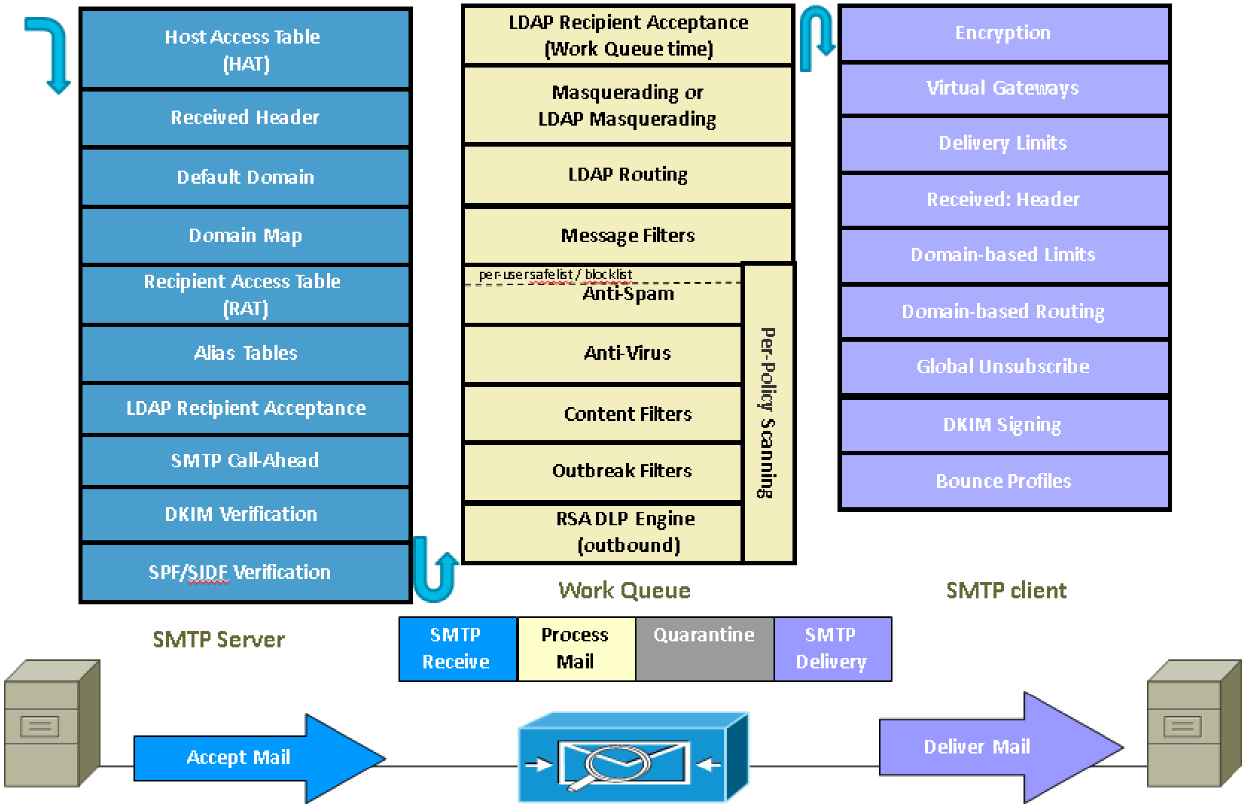
A Message Filter



```
myFilter
If (mail-from==“bugs.bunny@warnerbros.com”) {
        drop();
}
```

Message Filters in the Pipeline

For Your Reference



SMTP Server

- Host Access Table (HAT)
- Received Header
- Default Domain
- Domain Map
- Recipient Access Table (RAT)
- Alias Tables
- LDAP Recipient Acceptance
- SMTP Call-Ahead
- DKIM Verification
- SPF/SIDF Verification

Work Queue

- LDAP Recipient Acceptance (Work Queue time)
- Masquerading or LDAP Masquerading
- LDAP Routing
- Message Filters
- per-user safelist / blocklist
- Anti-Spam
- Anti-Virus
- Content Filters
- Outbreak Filters
- RSA DLP Engine (outbound)

Per-Policy Scanning

SMTP client

- Encryption
- Virtual Gateways
- Delivery Limits
- Received: Header
- Domain-based Limits
- Domain-based Routing
- Global Unsubscribe
- DKIM Signing
- Bounce Profiles

SMTP Receive	Process Mail	Quarantine	SMTP Delivery

Message Filters vs. Content Filters

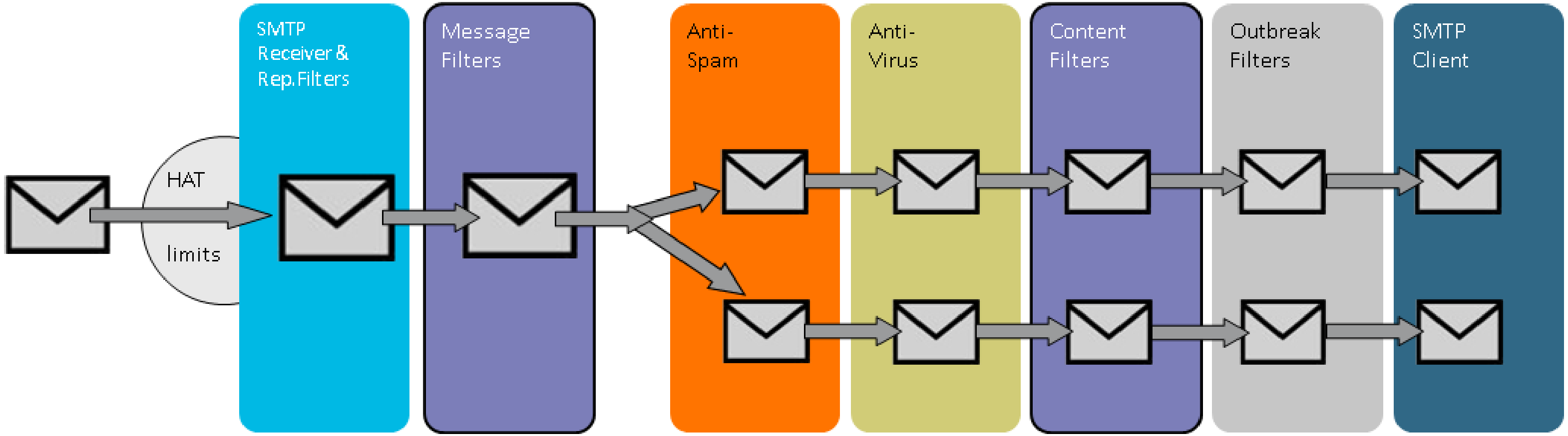
- Content Filters
  - Executed after the Policy Engine
  - Executed after security engines
  - Nice, easy-to-use GUI
  - Limited scope of conditions/actions
  - Either “AND” or “OR” logical operators between all conditions
  - Separate set of filters for Incoming and Outgoing mail

- Message Filters
  - Executed before the Policy Engine
  - Applies to the entire mail flow
  - More flexible in both capabilities and scriptability

The Danger of Message Filters

For Your Reference

Mail Policies cause message splintering



- Different recipients may have different mail policies
- A message is splintered into multiple policies after Message Filters
- Message Filters can only apply one policy

The Message Filter Death Trap

```
devNoExe:
if (rcpt-to-group==“Development”) {
        drop-attachments-by-filetype(“Executable”);
};
salesNoHTML:
if (rcpt-to-group==“Sales”) {
        html-convert();
};
```

- What happens if a message is sent to two: Sales and Development?
- What happens if they are in Development and Management?

Hint: The entire message matches

The Advance Part: Regex and Boolean

```
noBadguysPresos:
if ((mail-from==“@badguys.com”) AND (attachment-type=“ppt|pptx”)) {
        quarantine(“Badguys”);
        notify(infosec@cisco.com);
};
```

The Advance Part: Regex and Boolean

Actually, Regex is always on

```
noBadguysPresos:
if ((mail-from==“@badguys\\.com”) AND (attachment-type=“ppt|pptx”)) {
        quarantine(“Badguys”);
        notify(infosec@cisco.com);
};
```

- Don’t forget to double-escape (\\)!
- The Email Security Appliance uses Python Regex syntax (http://docs.python.org/2/howto/regex.html)

More Coolness: Action Variables

- Action Variables are expressions that are dynamically expanded based on the content/context of the message

```
if (spf-status=“pra”==“Fail”) {$EnvelopeFrom
       notify(secoff@domain.com, “SPF Failed: to
$EnvelopeRecipients”);
}
```

- Can be used in Text Resources (notifications, headers, footers, and Content Filters too!

Supported Action Variables

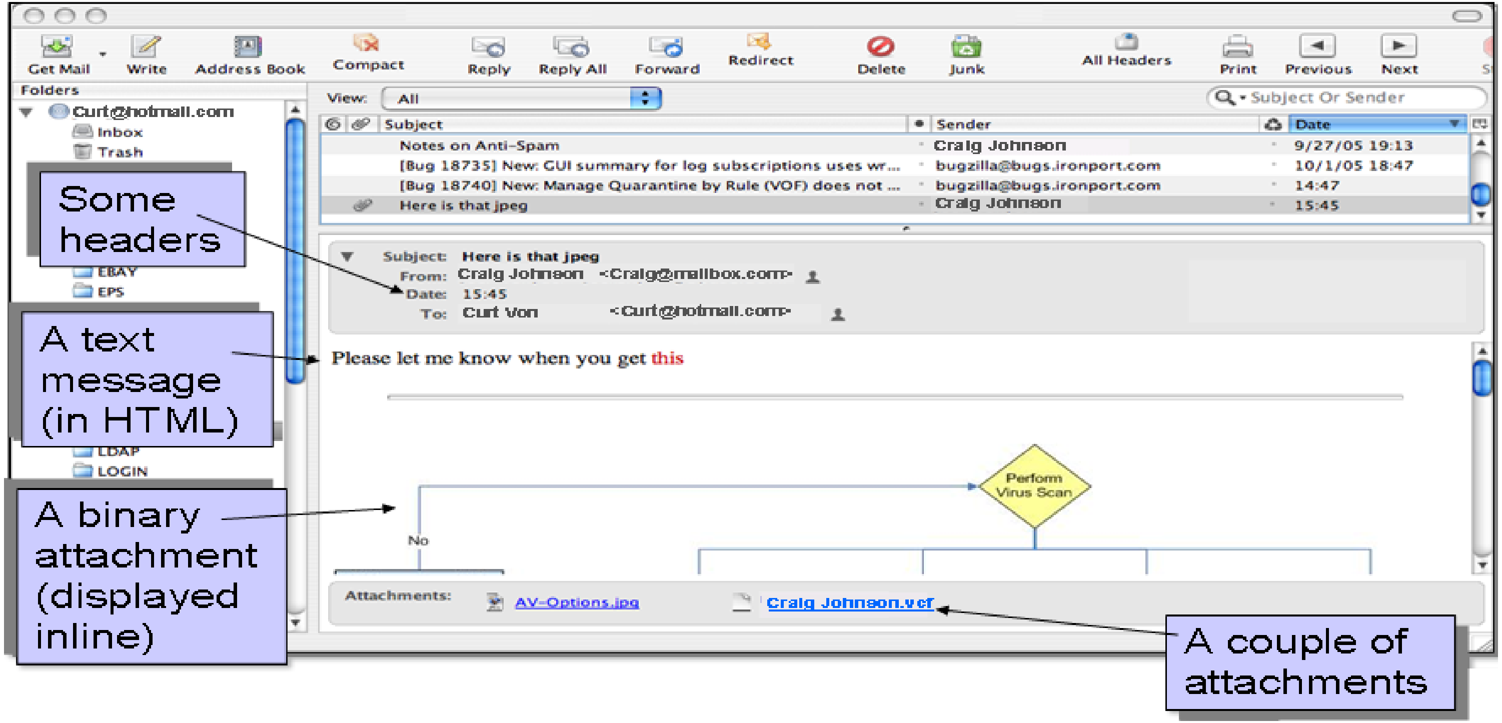
For Your Reference

- $EnvelopeFrom
- EnvelopeRecipients
- $RecvInt
- $RecvListener
- $RemoteIP
- $remotehost
- $Reputation
- $Hostname
- $Group
- $Policy
- $MID

- $BodySize
- $filenames
- $filesizes
- $dropped_filename
- $dropped_filenames
- $dropped_filetypes
- $filetypes
- $MatchedContent
- $CertificateSigners

- $AllHeaders
- $Header[“name”]
- $Subject
- $Date
- $Time
- $Timestamp
- $GMTTimeStamp
- $FilterName

What is a Message Body?



Subject	Sender	Date
Notes on Anti-Spam	Craig Johnson	9/27/05 19:13
[Bug 18735] New: GUI summary for log subscriptions uses wr...	bugzilla@bugs.ironport.com	10/1/05 18:47
[Bug 18740] New: Manage Quarantine by Rule (VOF) does not ...	bugzilla@bugs.ironport.com	14:47
Here is that jpeg	Craig Johnson	15:45

Subject: Here is that jpeg
From: Craig Johnson <Craig@mailbox.com>
Date: 15:45
To: Curt Von <Curt@hotmail.com>

Please let me know when you get this

Attachments: AV-Options.jpg Craig Johnson.vcf

Some headers

A text message (in HTML)

A binary attachment (displayed inline)

A couple of attachments

What is a Message Body? (2)

```
From: Craig Johnson<Craig@mailbox.com>
Subject: Here is that jpeg
To: Curt Von <curt@hotmail.com>
MIME-version: 1.0
Content-type: multipart/mixed; boundary="Boundary_11111"

This is a multi-part message in MIME format.

--Boundary_11111
Content-type: multipart/alternative;
 boundary="Boundary_22222"

  --Boundary_22222
  Content-type: text/plain; format=flowed; charset=us-ascii
  Content-transfer-encoding: 7bit

  Please let me know when you get this!

  --Boundary_22222
  Content-type: text/html; charset=us-ascii
  Content-transfer-encoding: 7bit

  <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
  <html>
  ...
  </html>

  --Boundary_22222--

--Boundary_11111
```

MIME multipart/mixed + Boundary

Preamble

MIME multipart/alternative + Boundary_22222

Alternative text part

Alternative HTML Part

Alternative HTML Part

What is a Message Body? (3)

```
Content-type: image/jpeg; name=AV-Options.jpg
Content-transfer-encoding: base64
Content-disposition: inline;
 filename=Antivirus-Options.jpg

/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRof
KACiiigAooooAKKKKACiiigAooooAKKKKACiiigD/9k=
```

Filetype verified by fingerprinting

```
--Boundary_11111
Content-type: text/plain; CHARSET=us-ascii; name="Craig Johnson.vcf"
Content-transfer-encoding: 7bit
Content-disposition: inline; filename="Craig Johnson.vcf"

BEGIN:VCARD
VERSION:3.0
N:Johnson;Craig;;;
...
END:VCARD
```

Text/plain vcard attachment

```
--Boundary_11111--
```

Closing Boundary_11111

So… What IS a Message Body???

- RFC5322: Anything following the headers, regardless of the content type
- Humans: The textual part following the headers, but not the binaries
- Email Security Appliance:
  - The first text/plain part following the headers
  - The first multipart/alternative part following the headers, if it contains a text/plain part
  - Binaries encoded within the first text/plain part (e.j. uuencoded) are considered attachments

Filters: A Few Advanced Applications

Add policy granularity

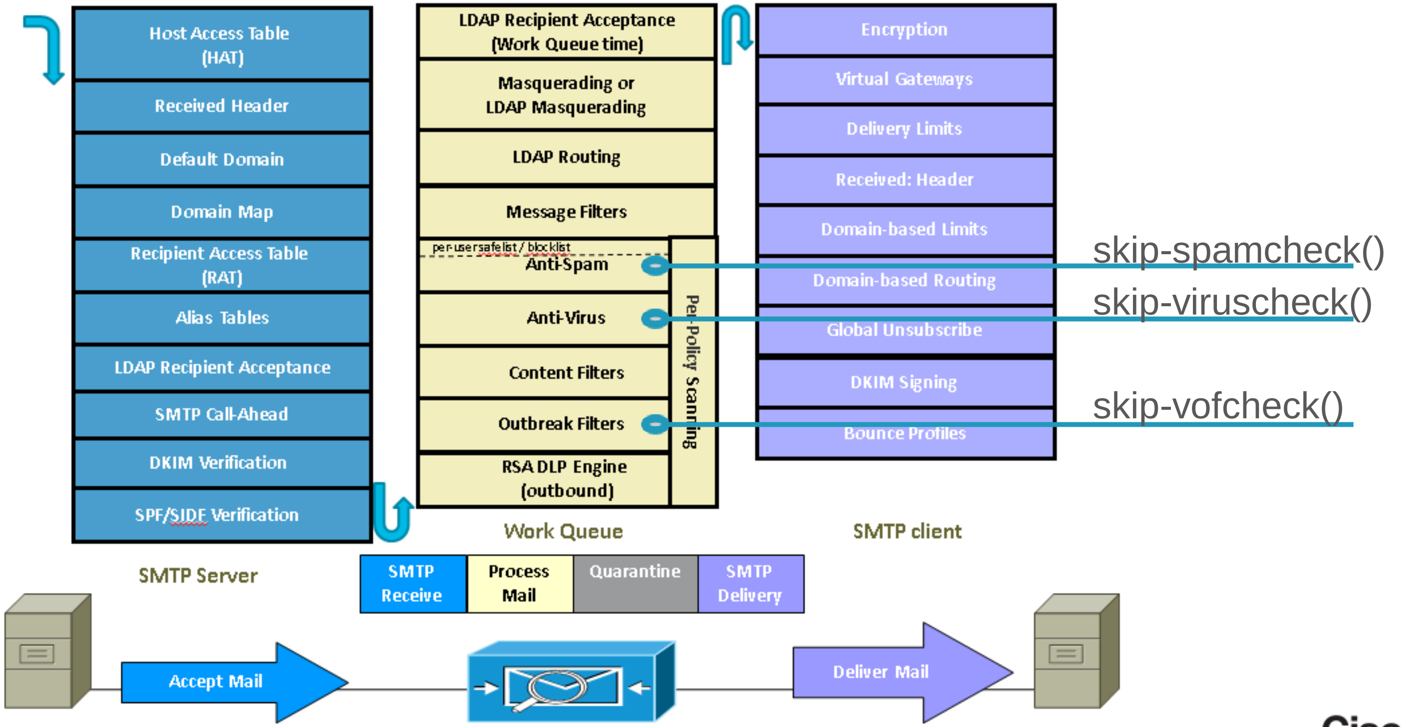
```
noASfromSalesToMgmt:
if ((rcpt-to-group==“Management”) AND (mail-from-
group=“Sales”)) {
       skip-spamcheck();
};
```

The Policy Engine can only OR senders/recipients in policy specification

Message Filters can skip security engines

Message Filters in the Pipeline

You can't control Anti-Spam and Anti-Virus with Content Filters!



Filters: A Few Advanced Applications

Delay Delivery of Large Messages

- Set up a quarantine to retain 8 hours , then release

```
if ((recv-listener==“OutgoingMail”) AND (body-size > 10M) AND
(date > “01/30/2013 08:00”) AND (date < “01/30/2013 1600”)) {
       quarantine(“Delayed”);
       notify(postmaster@domain.com, “$EnvelopeFrom Trying to
send large messages”;
};
```

- Method 2: Use altsrchost() to change delivery IP addressand QoS on the routers

Filters: A Few Advanced Applications

Processing S/MIME signatures

```
notOurkey:
if ((signed-certificate(“signer”) AND (signed-
certificate(“signer”) != “cisco\\.com$”)) {
        notify(infosec@cisco.com, “Outgoing S/MIME message
signed with non-Cisco certificate!);
        quarantine(“Policy”;
};
```

Filters: A Few Advanced Applications

Processing S/MIME signatures

```
notOurkey:
if ((signed-certificate(“signer”) AND (signed-
certificate(“signer”) != “cisco\\.com$”)) {
        notify(infosec@cisco.com, “Outgoing S/MIME message
signed with non-Cisco certificate!);
        quarantine(“Policy”;
};
```

Message is signed

But, not by us!

Filters: A Few Advanced Applications

The most polite Message Filter in the world ☺

```
obfuscateMailBombs:
if (addr-count(“To”, “Cc” > 30) {
        strip-header(“Cc”);
        edit-header-text(“To”, “undisclosed-recipients”);
};
```

- Your friends mass-mailing jokes are also a spammer’s best friend. Don’t let them get away with it!

Optimising and Streamlining

- Regex is less expensive than Boolean , in every aspect
  - Bad:

```
if (attachment-filename==“\\.exe$”) OR (attachment-filename==“\\.com$”) OR
(attachment-filename==“\\.bat$”) OR attachment-filename==“\\.dll”) {
```

  - Good

```
if (attachment-filename==“\\.(exe|com|bat|dll)$”) {
```

- Auto-optimisation: Use nested IFs to avoid auto-optimisation

```
if ((recv-listener==“Incoming”) AND (rcpt-to-group==“Sales”))
```

vs.

```
if (rcpt-to-group==“Sales”) {
if (recv-listener==“Incoming”) {
```

Optimising and Streamlining (2)

- Filters with Final Actions first

  `drop(), bounce(), skip-filters()`

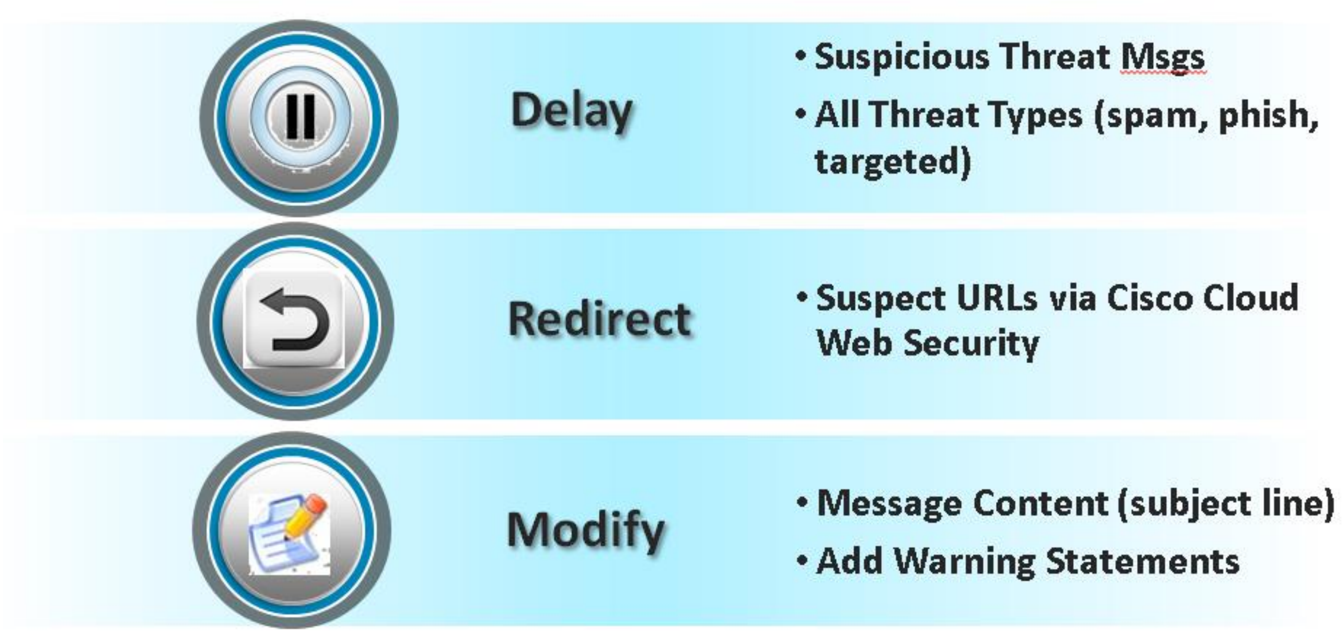
- Most executed filters first
- Clean your filters up!
  - Filters that are inactive are still evaluated – just actions are not executed
  - Check for filters that are never triggered: search through mail_logs for matches
  - If you need to keep unused filters, insert a “catch-all” filter at the end of your used ones”

```
if (true) {
skip-filters();
}
```

Anti-Phishing: OF, DKIM And SPF

Outbreak Filters

Introduced in AsyncOS 7.5.x



Delay

- Suspicious Threat Msgs
- All Threat Types (spam, phish, targeted)

Redirect

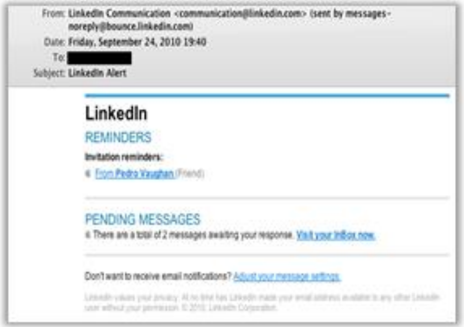
- Suspect URLs via Cisco Cloud Web Security

Modify

- Message Content (subject line)
- Add Warning Statements

Outbreak Filters

Protection from suspect e-mails



From: LinkedIn Communication <communication@linkedin.com> (sent by messages-noreply@bounce.linkedin.com)
Date: Friday, September 24, 2010 19:40
To: [redacted]
Subject: LinkedIn Alert

LinkedIn

REMINDERS

Invitation reminders:

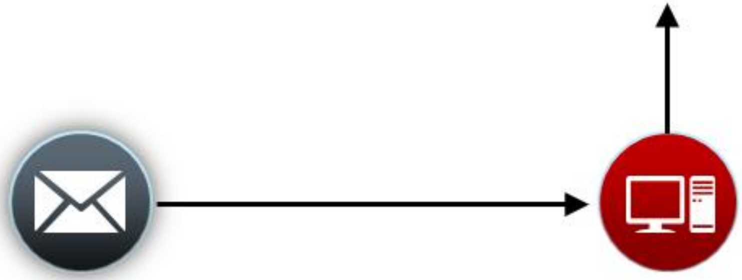
- From Pedro Vaughan (Friend)

PENDING MESSAGES

- There are a total of 2 messages awaiting your response. Visit your InBox now.

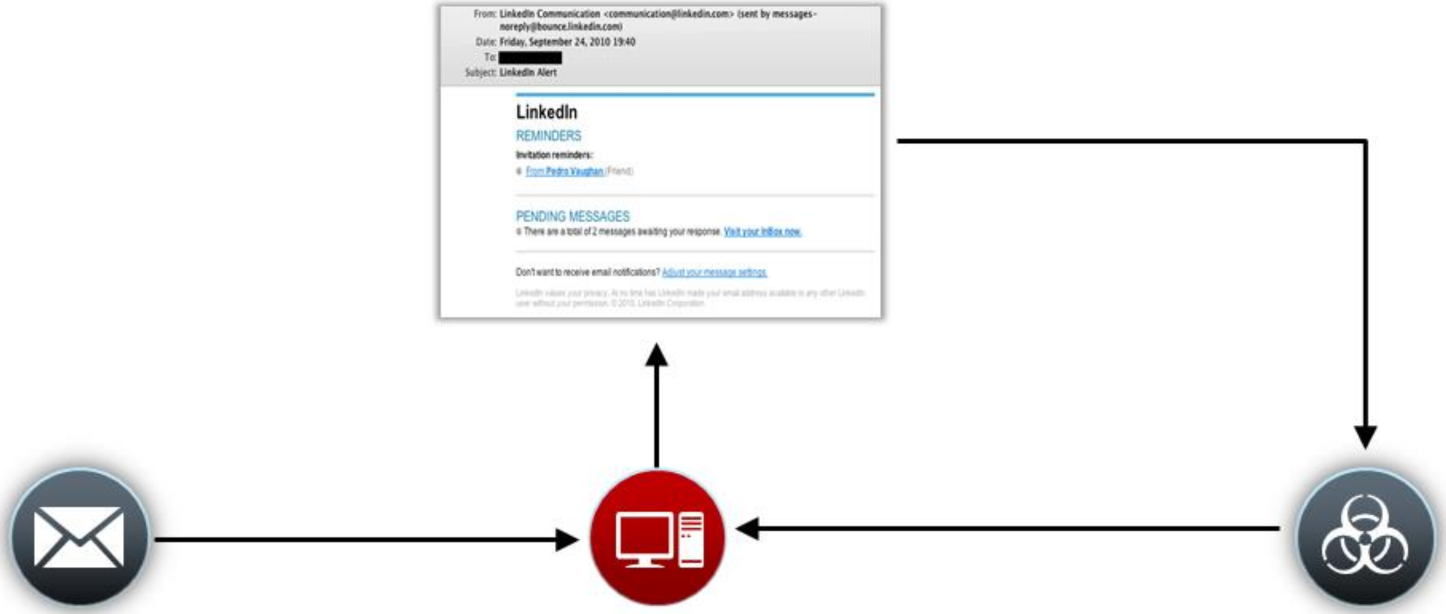
Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010, LinkedIn Corporation.



Outbreak Filters

Protection from suspect e-mails



From: LinkedIn Communication <communication@linkedin.com> (sent by messages-noreply@bounce.linkedin.com)
Date: Friday, September 24, 2010 19:40
To: [redacted]
Subject: LinkedIn Alert

LinkedIn

REMINDERS

Invitation reminders:

- From Pedro Vaughan (Friend)

PENDING MESSAGES

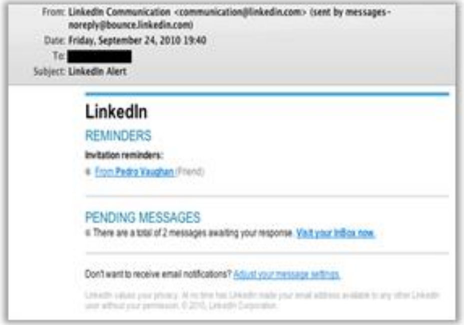
- There are a total of 2 messages awaiting your response. Visit your InBox now.

Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010, LinkedIn Corporation.

Outbreak Filters

Protection from suspect e-mails



From: LinkedIn Communication <communication@linkedin.com> (sent by messages-noreply@bounce.linkedin.com)
Date: Friday, September 24, 2010 19:40
To: [redacted]
Subject: LinkedIn Alert

LinkedIn

REMINDERS

Invitation reminders:

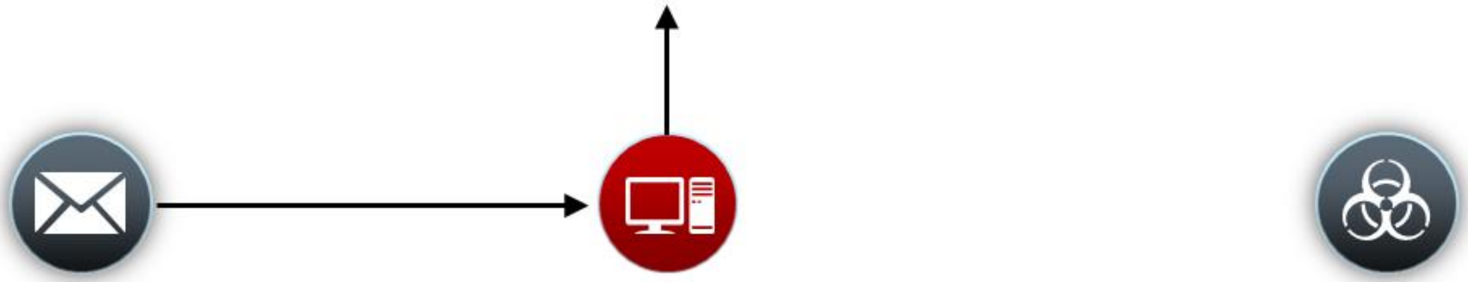
- From Pedro Vaughan (Friend)

PENDING MESSAGES

- There are a total of 2 messages awaiting your response. Visit your InBox now.

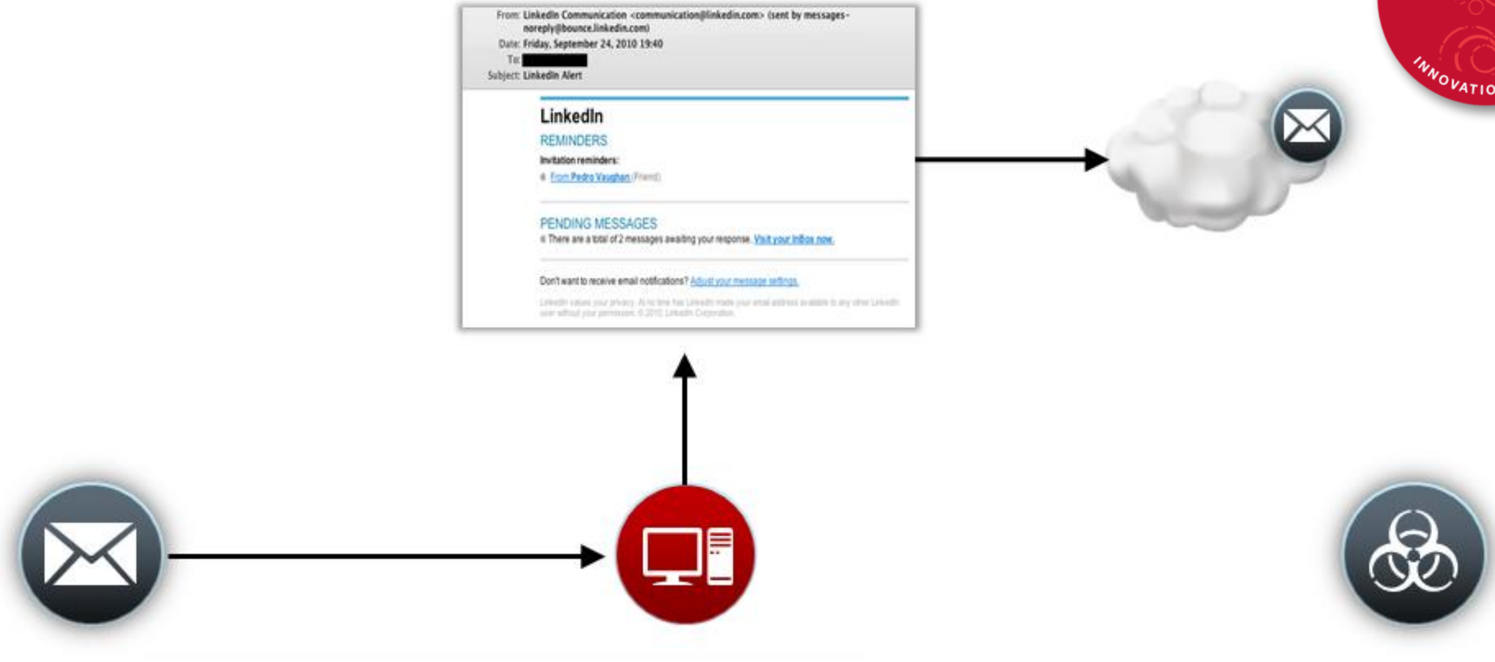
Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010, LinkedIn Corporation.



Outbreak Filters

Protection from suspect e-mails



From: LinkedIn Communication <communication@linkedin.com> (sent by messages-noreply@bounce.linkedin.com)
Date: Friday, September 24, 2010 19:40
To: [redacted]
Subject: LinkedIn Alert

LinkedIn

REMINDERS

Invitation reminders:

- From Pedro Vaughan (Friend)

PENDING MESSAGES

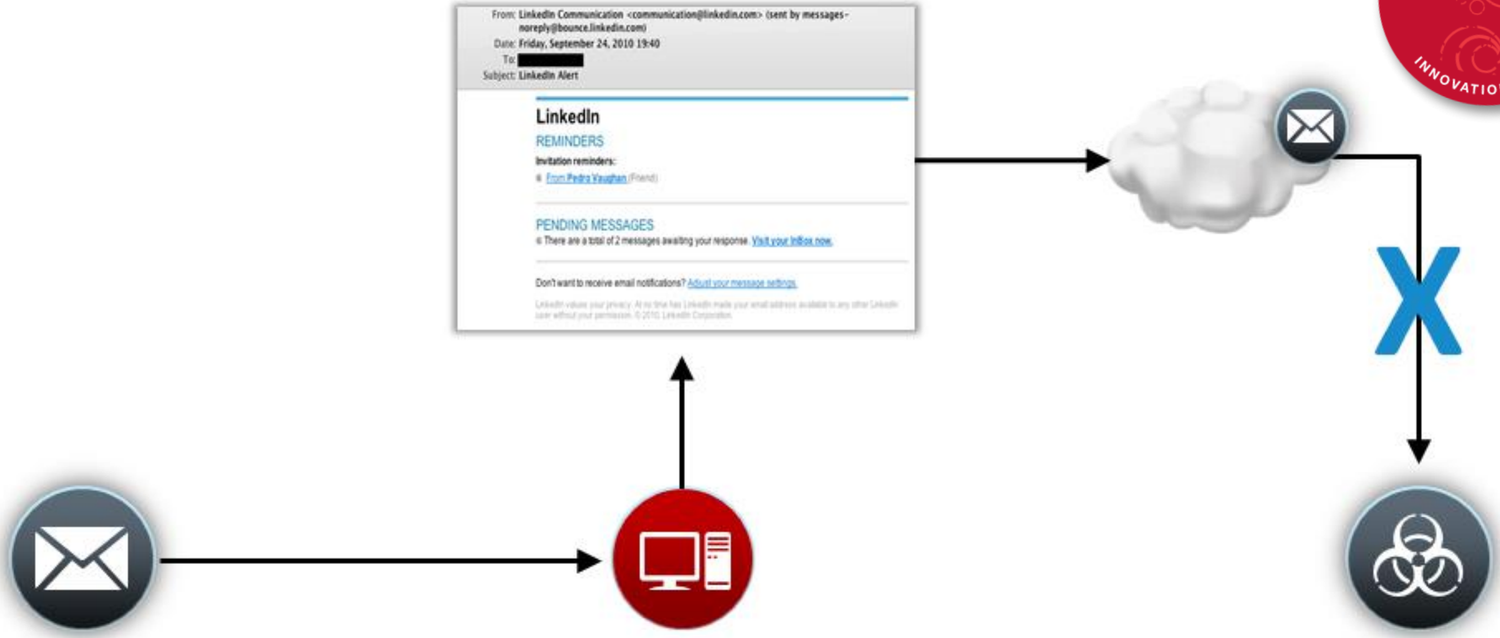
- There are a total of 2 messages awaiting your response. Visit your InBox now.

Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010 LinkedIn Corporation.

Outbreak Filters

Protection from suspect e-mails



From: LinkedIn Communication <communication@linkedin.com> (sent by messages-noreply@bounce.linkedin.com)
Date: Friday, September 24, 2010 19:40
To: [redacted]
Subject: LinkedIn Alert

LinkedIn

REMINDERS

Invitation reminders:

- From Pedro Vaughan (Friend)

PENDING MESSAGES

- There are a total of 2 messages awaiting your response. Visit your InBox now.

Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010, LinkedIn Corporation.

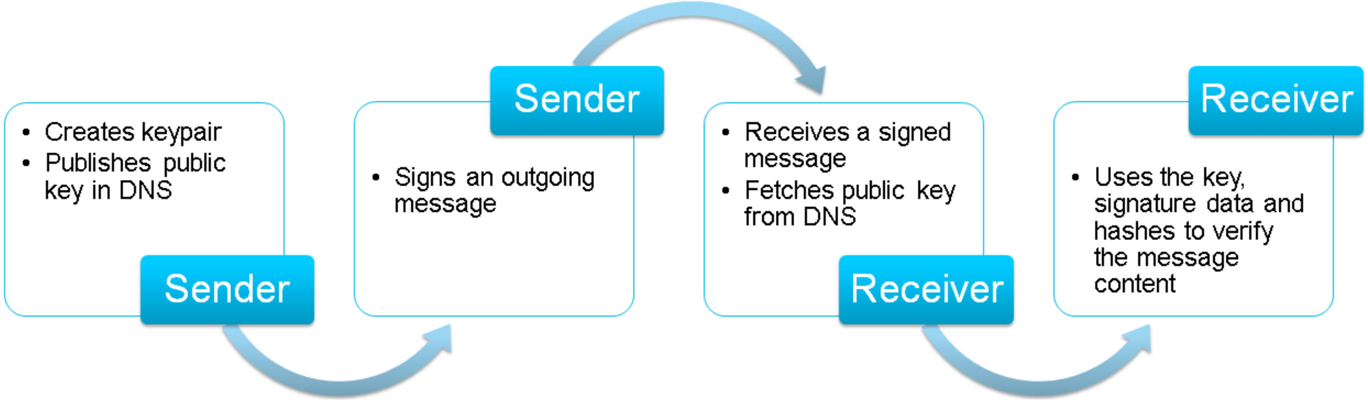
Demonstration

- Configuring Message Modification to On in Outbreak Filters configuration
- Sending a message with “X-Advertisement: outbreak” and a URL
- Verifying the URL got redirected in Webmail

E-mail Authentication Technologies

Domain Keys Identified Mail (DKIM) – RFC5585 et al.

- Asymmetric encryption based message integrity, authentication, and non-repudiation
- Information stored in DKIM Signature header
- Verification key obtained from DNS



Sender
- Creates keypair
- Publishes public key in DNS

Sender
- Signs an outgoing message

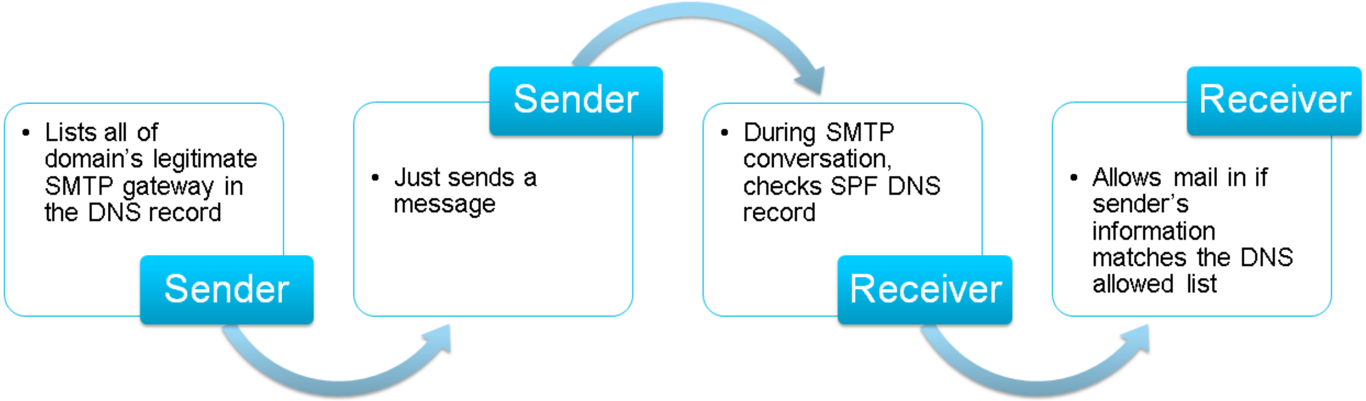
Receiver
- Receives a signed message
- Fetches public key from DNS

Receiver
- Uses the key, signature data and hashes to verify the message content

E-mail Authentication Technologies

Sender Policy Framework (SPF) – RFC4408

- Simple, DNS-based anti-spoofing technology
- Lists all legitimate SMTP gateways for a domain; provides information on what to do with senders not on the list (“-”: hard fail; “~” soft fail)
- Provides no integrity checking (susceptible to MitM) or non-repudiation



- Lists all of domain’s legitimate SMTP gateway in the DNS record

Sender

Sender

- Just sends a message

- During SMTP conversation, checks SPF DNS record

Receiver

Receiver

- Allows mail in if sender’s information matches the DNS allowed list

Why Use E-mail Authentication Technologies

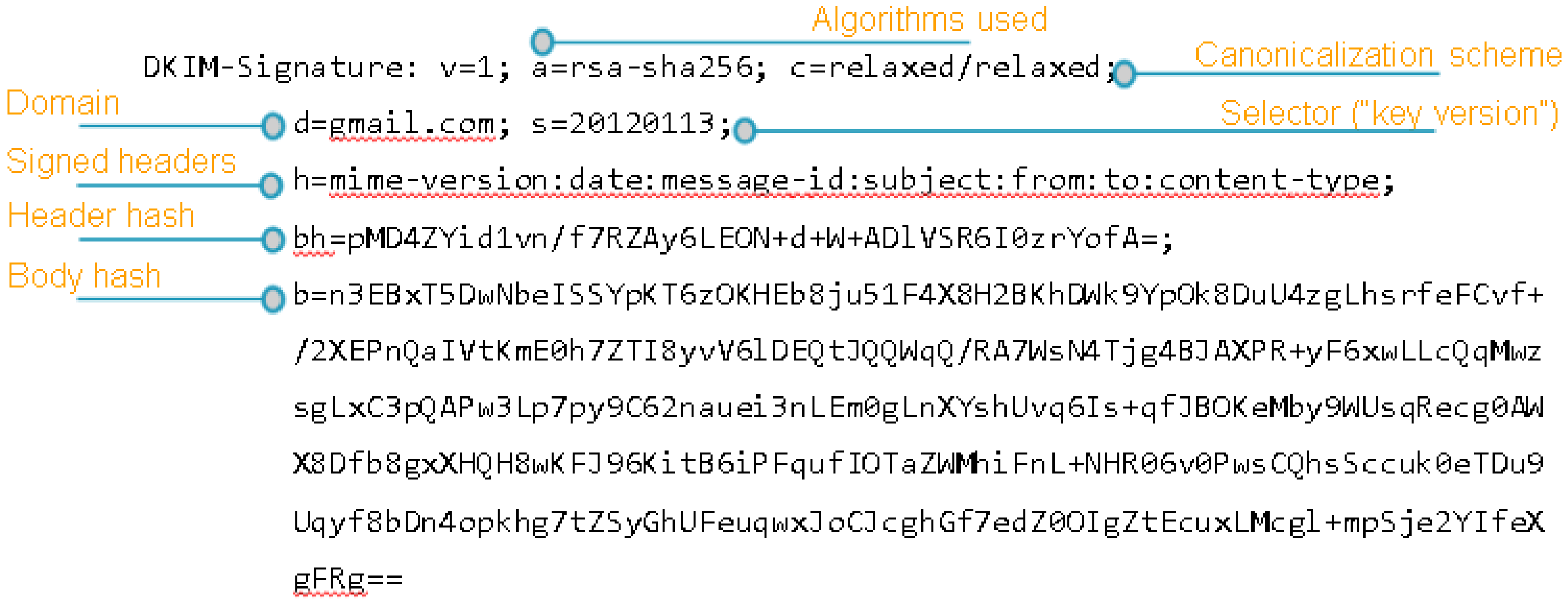
- As a sender:
  - Avoid spoofing of your messages
  - Increase your reputation
  - Avoid getting blacklisted
- As a receiver:
  - Block phishing and spoofing attacks
  - Apply more liberal policies to AUTTHENTICATED external sources
  - And, universally, help keep the Internet a nice and safe place – be a good Internet citizen

Implementing DKIM

The easy path: Use the tools on the Email Security Appliance

- Create a signing keypair
- Configure a DKIM signing profile using the key, and specify parameters:
  - Domain name, canonicalisation method, what to sign, additional tags to use, and which messages to sign
- Generate the DNS record and add it to your DNS zone(s)
- Use the “Test” option of the DKIM profile to verify if keys in the pair match

DKIM Signature



```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:date:message-id:subject:from:to:content-type;
bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+ADlVSR6I0zrYofA=;
b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhDWk9YpOk8DuU4zgLhsrfeFCvf+
/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4BJAXPR+yF6xwLLcQqMwz
sgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYshUvq6Is+qfJBOKeMby9WUsqRecg0AW
X8Dfb8gxXHQH8wKFJ96KitB6iPFqufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9
Uqyf8bDn4opkhg7tZSyGhUFeuqwxJoCJcghGf7edZ0OIgZtEcuxLMcgl+mpSje2YIfeX
gFRg==
```

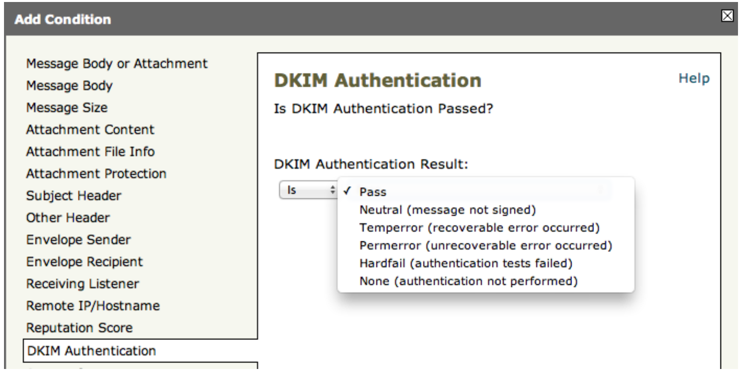
DKIM Public Key

```
$ host -T -t txt 20120113._domainkey.gmail.com
20120113._domainkey.gmail.com descriptive text "k=rsa\;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabgbFwh
+eBCsSTrqmwIYYvywlbhbqoo2DymndFkbjOVIPIldNs/m40KF+yzMn1skyoxcTUGCQ
s8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD07y2+07wlNWwIt8svnxgdxGkVbb
hzY8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjViiAH+ghvvIhkx4xYSIc9oSwVmAl5Oct
MEeWUwg8Istjqz8BZeTWbf41fbNhte7Y+YqZOwq1Sd0DbvYAD9NOZK9vlfuac0598H
Y+vtSBczUiKERHv1yRbcaQtZFh5wtiRrN04BLUTD21MycBX5jYchHjPY/wIDAQAB"
```

Email Security Appliance and DKIM

The easy path: Use the tools on the Email Security Appliance

- Enable DKIM in Mail Flow Policies
  - Signing in Outgoing Mail Flow Policy (“RELAY” by default)
  - Verification in Incoming (or Default) Mail Flow Policies
- Use Message Filters or Content Filters for verification
- Parse Authentication-Results header in Message Filters, or use “DKIM Authentication” Content Filters rule



DKIM Authentication

Is DKIM Authentication Passed?

DKIM Authentication Result:

Is ✓ Pass

Neutral (message not signed)

Temperror (recoverable error occurred)

Permerror (unrecoverable error occurred)

Hardfail (authentication tests failed)

None (authentication not performed)

Implementing SPF

- Figure out your outgoing SMTP sending hosts
- Create your SPF record
- Publish it for the world!

- Biggest challenge: Figuring out your outgoing SMTP sending hosts
  - You think you know them… but
    - There’s always a rouge PC with no SMTP gateway configured
    - Internal applications might send e-mail directly
    - Servers/services from DMZ might send alerts/notifications

“My opinion is that any company which does not know where their SMTP servers are has to commit seppuku in front of the building starting from the CIO. DNS administrators can prove their loyalty by cutting one finger from their right hand.”

Member of Messaging Support Team

Very Large Global Corporation, a Cisco Email Security Customer

“My opinion is that any company which does not know where their SMTP servers are has to commit seppuku in front of the building starting from the CIO. DNS administrators can prove their loyalty by cutting one finger from their right hand.”

Member of Messaging Support Team

Very Large Global Corporation, a Cisco Email Security Customer

A Few SPF Records

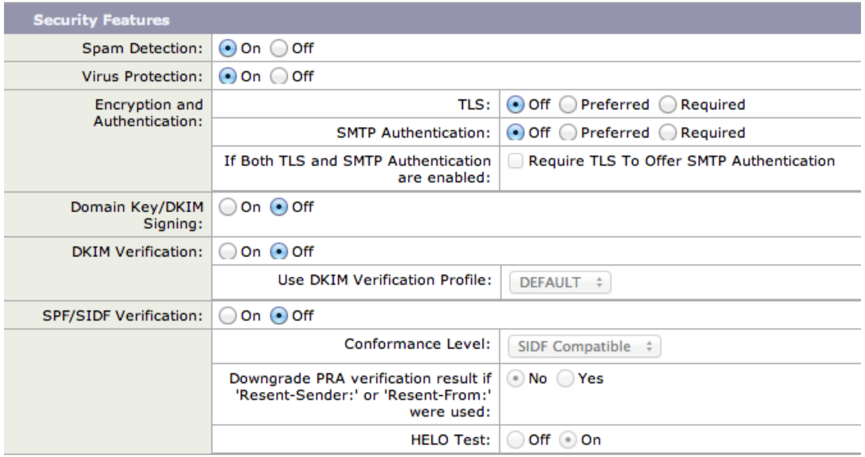
```
$ host -t txt cisco.com

cisco.com descriptive text "v=spf1 ip4:171.68.0.0/14 ip4:64.100.0.0/14
ip4:64.104.0.0/16 ip4:72.163.7.160/27 ip4:72.163.197.0/24 ip4:128.107.0.0/16
ip4:144.254.0.0/16 ip4:66.187.208.0/20 ip4:173.37.86.0/24 ip4:173.36.130.0/24
ip4:204.15.81.0/26 ip4:216.206.186.129/25 ip4:208.90.57.0/26 mx:res.cisco.com ~all”
```

```
$ host -t txt google.com

google.com descriptive text "v=spf1 include:_netblocks.google.com
include:_netblocks6.google.com ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all”
```

```
$ host -t txt amazon.com

amazon.com descriptive text "v=spf1 include:spf1.amazon.com include:spf2.amazon.com
include:amazonses.com -all”
```

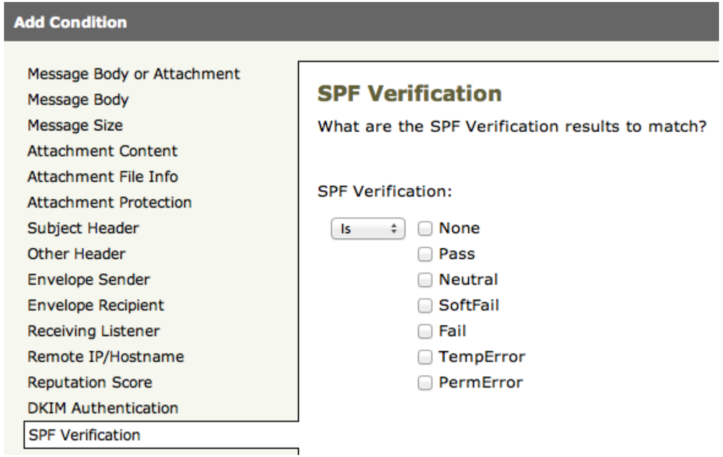
Email Security Appliance and SPF

- Not much to do there – publish your SPF records, configure verification in MPF, and use Message Filters or Content Filters to enforce (spf-status or spf-passed rules)



Security Features

Spam Detection:	● On ○ Off	
Virus Protection:	● On ○ Off	
Encryption and Authentication:	TLS:	● Off ○ Preferred ○ Required
	SMTP Authentication:	● Off ○ Preferred ○ Required
	If Both TLS and SMTP Authentication are enabled:	□ Require TLS To Offer SMTP Authentication
Domain Key/DKIM Signing:	○ On ● Off	
DKIM Verification:	○ On ● Off	
	Use DKIM Verification Profile:	DEFAULT
SPF/SIDF Verification:	○ On ● Off	
	Conformance Level:	SIDF Compatible
	Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:	● No ○ Yes
	HELO Test:	○ Off ● On



Add Condition

- Message Body or Attachment
- Message Body
- Message Size
- Attachment Content
- Attachment File Info
- Attachment Protection
- Subject Header
- Other Header
- Envelope Sender
- Envelope Recipient
- Receiving Listener
- Remote IP/Hostname
- Reputation Score
- DKIM Authentication
- SPF Verification

SPF Verification

What are the SPF Verification results to match?

SPF Verification:

Is
□ None
□ Pass
□ Neutral
□ SoftFail
□ Fail
□ TempError
□ PermError

Demonstration

- Configuring a DKIM signing profile
- Sending outgoing message, view signature
- Receiving a DKIM-Signed message, verifying signature
- Configuring SPF verification
- Receiving an SPF-verified message

The Future

A shining new star on the skyline: DMARC

- Domain-based Message Authentication, Reporting, and Conformance – draft-dmarc-base-00
- Combines DKIM and SPF to eliminate their shortcomings
  - DKIM provides no way to advertise
  - SPF provides no integrity checks
- Additional layer: DKIM and SPF must be *in sync*
- Provides mechanism to send feedback *back to the senders*
- Based on DNS TXT records

A Sample DMARC Record

Agari.com

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=agari.com; i=@agari.com; q=dns/txt;
s=s1024; t=1340901310; x=1372437310; h=mime-version:in-reply-to:references:date:message-
id:subject:from:to:cc; bh=VL1kbrttnEN3rBcJqiuYwwCXKG+X0ivxazuWBsqsy1c=;
b=OhHljRyHHtRSnP1fHPqL7eEsW4E5uKhz3nsiVQ7v2EtcA7orMqtitDL5Al/Inx6/lvkckKs28eFrcFduPluIPpMc9t+4+gw
TKDIXq0AO4lblbFCdfnYoe8XNvR/7UmcYIdV36tP/A06eQQ8bYOgFXCKOOKoZv9b2yuuxsC4f5go=;
```

```
s1024._domainkey.agari.com descriptive text "v=DKIM1\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQwPqBxkIOc1YVnJv3OccfbdS3S68p8E5BafsirMBaSPxqIgnzaxNSyPp8
INEPL61cIRKo3u195Px5XHNwjEfq76BvDu7eUYXxY8zKcAS74heKAeyfpVaMFWHUzCoujPNzzorCIRtP5CuY+ILw+Vj1SKN6x
lBWhouCSHWhOr/vcYQIDAQAB"
```

```
agari.com descriptive text "v=spf1 ip4:82.135.8.34 ip6:2001:a60:901e::22 ip4:72.250.241.196
ip4:74.250.241.195 ip4:74.217.77.9 ip4:74.217.77.10 ip4:74.116.66.11 ip4:74.116.66.12
include:_spf.google.com include:support.zendesk.com -all”
```

```
_dmarc.agari.com descriptive text
"v=DMARC1\;p=none\;pct=100\;ruf=mailto:d@ruf.agari.com\;rua=mailto:d@rua.agari.com"
```

And a Little More…

The Future

Coming soon to a Cisco Email Security environment near you!

- AsyncOS 8.0 and ESAv: Virtual Email Security Appliance
  - OVF file; ESXi 4.1 and 5.0 supported
  - 4 different virtual appliances, roughly equivalent to current hardware models
  - Available to all existing hardware appliance customers at FCS
  - No limitation on number of instances run
- Centralised Policy Quarantines
  - Migration Wizard for existing on-box quarantines
  - Search through multiple quarantines, release messages from multiple quarantines at once
- FIPS support and more, including Customisable Reporting Dashboard, Quick Links, and Landing Page in the web UI

Call to Action

- Visit the Cisco Campus at the World of Solutions

  To experience the following demos/solutions in action: Cisco Email Security, Cisco Security Intelligence Operations

- Get hands-on experience attending one of the walk-in labs
- Meet the Engineer
  - Walk up to our Security Solutions Architects at the Content Security Booths at the World of Solutions – or come over for a chat at the MTE area
- Discuss your project's challenges at the Technical Solutions Clinics

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com cisco TM