Possibilities

#CiscoLive

SPF is not an acronym for "Spoof"!

Let's utilize the most out of the next layer in Email Security!

Robert Sherwin, Cisco Email Security TME

DGTL-BRKSEC-2327

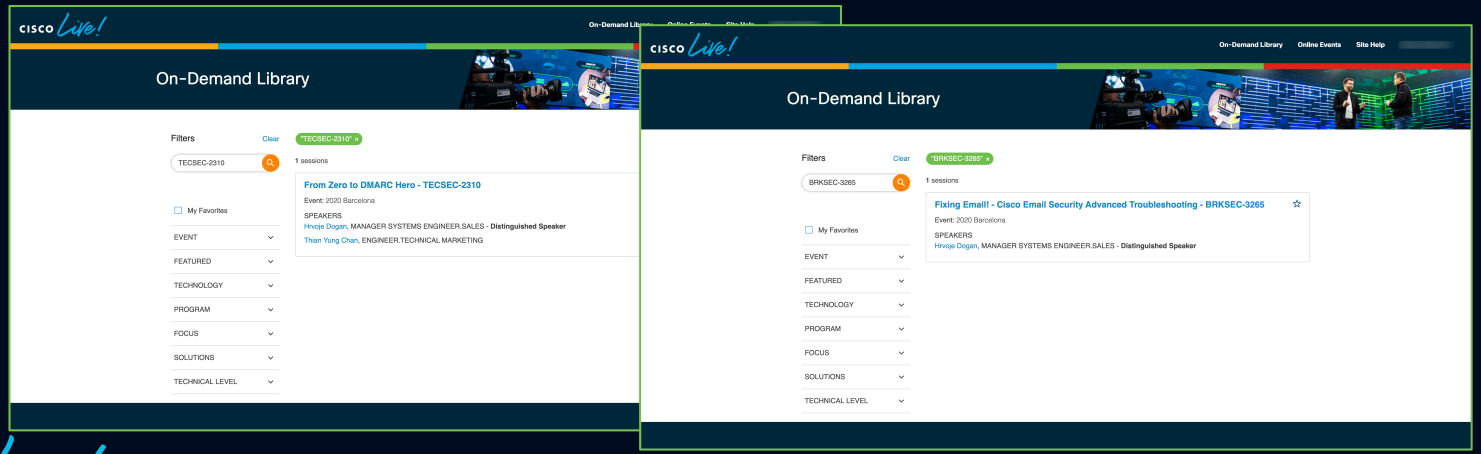
Agenda

- Review (or Intro) to Cisco Email Security
  - Mail flow & email pipeline
  - Common acronyms
  - A typical message
- Utilizing SPF, DKIM, DMARC on Cisco Email Security
- Cisco Advanced Phishing Protection
- Cisco Domain Protection
- Phishing Efficacy
- Cisco Security Awareness

Ready? Let's get started!

Agenda

- What this session will not cover:
  - In-depth SPF, DKIM, DMARC record creation and understanding.
    - Please see TECSEC-2310, From Zero to DMARC Hero
  - SPF, DKIM, DMARC troubleshooting.
    - Please see BRKSEC-3265, Fixing Email! - Cisco Email Security Advanced Troubleshooting



The Speaker

- Technical Marketing Engineer, Email Security
- Joined Cisco December 2011
- Cisco Live Speaker in US, EMEA, APJC
- 18 years of combined Network, Data Center, and Security experience
- 6 years in Cisco TAC, joined TME team in 2018
- Based out of Morrisville, NC (US)

Robert Sherwin
(robsherw@cisco.com)

January 28, 2020

"... sent phishing emails that gave them access to the companies' email systems – giving the fraudsters an even bigger trove of information about the victim companies."

"The two companies wired several payments to the fraudulent accounts, adding up to more than $120 million."

– US FBI News: Leader of Fraud Ring Sentenced

*“**6.4 billion** – the number of fake emails sent worldwide – every day.”*

– EY Global Information Security Survey 2018-19

Let’s take a different look in context at 6.4 billion and compare to something more quantifying, like, time...

6,000 minutes = 4.166667 days
6,000,000 minutes = 4166.667777 days (or 11.41 years)
6,000,000,000 minutes = 4166666.667777 days (or 11407.71 years)

That is a LOT of emails! *Everyday...*

Review of Cisco Email Security

As we discuss layers of email security, our ‘layers’ of security are provided from the mail flow pipeline...

Cisco Email Security Mail Flow Pipeline

INCOMING

Connection level protection	Sender Reputation Filtering (SBRS)
Anti-spoof, throttling & verification	Connection Filtering
Sending domain verdict analysis	Sender Domain Reputation (SDR)
Spam protection, URL analysis	Anti-spam Scanning (AS)
Virus protection	Anti-virus Scanning (AV)
Malware protection	Advanced Malware Protection (AMP)
Marketing/Social/Bulk email detection	Graymail Detection
Content protection	Content Filtering
Malware, Phishing, URL threat protection	Outbreak Filtering (VOF)
Phishing behavioral analytics & protection	Advanced Phishing Protection (APP)

* Message Filtering

Per-policy

Cisco Email Security Mail Flow Pipeline

OUTBOUND

Connection level protection	Sender Reputation Filtering (SBRS)
Encryption & authentication enforcement	Connection Filtering
Spam protection, URL analysis	Content Scanning (CASE)
Virus protection	Anti-virus Scanning (AV)
Malware protection	Advanced Malware Protection (AMP)
Marketing/Social/Bulk email detection	Graymail Detection
Content protection	Content Filtering
Malware, Phishing, URL threat protection	Outbreak Filtering (VOF)
Sensitive data protection & encryption	Data Loss Prevention (DLP)
Brand protection, SPF/DKIM/DMARC administration	Domain Protection (DMP)

* Message Filtering

Per-policy

Cisco Email Security Mail Flow Pipeline

Post Delivery

Unsubscribe validation and management	Graymail Unsubscribe
URL reporting + end-user click tracking	URL rewrite & tracking
Verdict change alerting & mailbox administration	AMP retrospection & remediation
Threat detection, investigation, remediation	Cisco Threat Response (CTR)

Email pipeline (what happens and where)

Per-listener settings

SMTP Server

- Host Access Table (HAT)
  - IP Reputation
  - External Threat Feeds (IoC)
  - Connection Throttling
  - Sender Verification
  - SPF, DKIM, DMARC
  - Sender Domain Reputation
- Received Header
- Default Domain
- Domain Map
- Recipient Access Table
- Alias Table
- LDAP RCPT Accept
- SMTP Call-Ahead

Workqueue

- LDAP RCPT Accept (WQ deferred)
- Masquerading (Table/LDAP)
- LDAP Routing
- Message Filters
- (Per-policy scanning)
  - Anti-Spam
  - Anti-Virus
  - AMP
    - File Reputation
    - File Analysis
  - Graymail Detection
  - Content Filtering
  - DLP filtering (Outbound)
  - Outbreak Filtering

SMTP Client

- Encryption
- Virtual Gateways
- Delivery Limits
- Received Header
- Domain Based Limits
- Domain Based Routing
- Global Unsubscribe
- S/MIME Encryption
- DKIM Signing
- Bounce Profiles
- Message Delivery
- Encryption
- Virtual Gateways

System or virtual gateway

Within these layers of email security, Cisco Email Security features and services that always come with acronyms...

Common acronyms used in email security

Who loves acronyms? (Cisco ❤'s to utilize acronyms...)

ADFS : Active Directory Federation Services
AMP : Advanced Malware Protection
API : Application Programming Interface
APPC : Advanced Phishing Protection Console
AS (A/S) : Anti-spam
AV (A/V) : Anti-virus
BATV : Bounce Address Tag Validation
BEC : Business Email Compromise
BIMI : Brand Indicator Message Identification
CASE : Context Adaptive Scanning Engine
CDP (DMP) : Cisco Domain Protection
CDR: Continuous Detection and Response
CES : Cloud Email Security
CLI : Command Line Interface
CMD: Cisco Mailbox Defense
CRES: (see RES)
CSA: Cisco Security Awareness
CTR : Cisco Threat Response
CUA: Cloud URL Analysis
DC: Data Center
DCID : Delivery Connection ID
DHAP : Directory Harvest Attack Prevention
DKIM : Domain Keys Identified Mail
DLP : Data Loss Prevention
DMARC : Domain-based Message Authentication, Reporting and Conformance
DNS : Domain Name System
ESA : Email Security Appliance
ESMTP : Extended (or Enhanced) Simple Mail Transfer Protocol
ETF : External Threat Feed

EUQ : End-user Quarantine (aka Spam Quarantine)
FA : File Analysis (Threat Grid)
FED : Forged Email Detection
FR : File Reputation (AMP)
GUI : Graphical User Interface
HAT : Host Access Table
ICID : Incoming Connection ID
IETF : Internet Engineering Task Force
IMS : Intelligent Multi-Scan
IoC: Indicator of Compromise
IPAS : IronPort Anti-Spam
ISQ : IronPort Spam Quarantine
LB: Load Balancer
LDAP : Lightweight Directory Access Protocol
MAR : Mailbox Auto Remediation
MFP: Mail Flow Policy
MID : Message ID
MX : Mail Exchange (DNS record)
NGUI: Next Generation User Interface
NTP : Network Time Protocol
PoC : Proof of Concept
PoV : Proof of Value
PXE : PostX Encryption
RAT : Recipient Access Table
REPENG : Reputation Engine
RID : Recipient ID
RES : Registered Envelope Service
S&R: Search and Remediate
SAML : Security Assertion Markup Langua
SBG : Security Business Group
SBRS : Sender Base Reputation Service

SDR : Sender Domain Reputation
SLBL : Safe List Block List
SMA: Security Management Appliance
S/MIME : Secure/Multipurpose Internet Mail Extensions
SMTP : Simple Mail Transfer Protocol
SNMP : Simple Network Management Protocol
SOC : Security Operations Center
SPF : Sender Policy Framework
SSL : Secure Sockets Layer
TA : Threat Analyzer
TLS : Transport Layer Security
TME : Technical Marketing Engineer
TOC : Threat Operations Center
UI : User Interface
URL: Uniform Resource Locator
vESA (ESAv/ESAV) : Virtual Email Security Appliance
vSMA (SMAv/SMAV) : Virtual Security Management Appliance
VOF : Virus Outbreak Filtering
WBRS : Web Base Reputation Service
WSA : Web Security Appliance
XML : Extensible Markup Language
2FA : (2) Two Factor Authentication

Too many, not enough time, right?
https://docs.ces.cisco.com/docs/acronyms

A typical SMTP conversation

```
$ telnet alln-mx-01.cisco.com 25
Trying 173.37.147.230...
Connected to alln-mx-01.cisco.com.
Escape character is '^]'.
220 alln-inbound-e.cisco.com ESMTP
helo pipershark.com
250 alln-inbound-e.cisco.com
MAIL FROM:<admin@pipershark.com>
250 sender <admin@pipershark.com> ok
RCPT TO:<robsherw@cisco.com>
250 recipient <robsherw@cisco.com> ok
DATA
354 go ahead
Subject: SMTP CONVERSATION TEST MESSAGE
From: Email Admin <admin@pipershark.com>
To: Robert Sherwin (robsherw) <robsherw@cisco.com>
Here is the email, hope you receive it.
.
250 ok:  Message 143004492 accepted
quit
221 alln-inbound-e.cisco.com
Connection closed by foreign host.
```

Envelope

Body

Headers

Body

Envelope From, Mail From, Envelope Sender, ...

Envelope To, Envelope Recipient

Header From, RFC5322.From, "Friendly From", ...

Recipient, Header To, RFC5322.To, ...

What gets verified or authenticated?

```
$ telnet alln-mx-01.cisco.com 25
Trying 173.37.147.230...
Connected to alln-mx-01.cisco.com.
Escape character is '^]'.
220 alln-inbound-e.cisco.com ESMTP
helo pipershark.com
250 alln-inbound-e.cisco.com
MAIL FROM:<admin@pipershark.com>
250 sender <admin@pipershark.com> ok
RCPT TO:<robsherw@cisco.com>
250 recipient <robsherw@cisco.com> ok
DATA
354 go ahead
Subject: SMTP CONVERSATION TEST MESSAGE
From: Email Admin <admin@pipershark.com>
To: Robert Sherwin (robsherw) <robsherw@cisco.com>
Here is the email, hope you receive it.
.
250 ok:  Message 143004492 accepted
quit
221 alln-inbound-e.cisco.com
Connection closed by foreign host.
```

Envelope

Body

Headers

Body

Verified by SPF

(Invisible to end-user)

Verified by DMARC

(Visible to end-user)

Verified and authenticated by DKIM

(Invisible to end-user)

Sender Policy Framework (SPF)

- Allows recipients to verify sender IP addresses by looking up DNS records listing authorized Mail Gateways for a domain.
- Verification of SPF records can produce these results:


```
> dig igo232.com TXT +short
"v=spf1 ip4:139.138.32.156 ip4:139.138.56.31 ip4:136.56.60.2 -all"
```

Domain Keys Identified Mail (DKIM)

- Specifies methods for gateway-based cryptographic signing of outbound messages, embedding verification data in an e-mail header, and ways for recipients to verify integrity of the messages.

```
> dig google._domainkey.igo232.com TXT +short
"v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqDsxWVJKWk/MO0fEIhaTqJFECwVysZnASTnl"
"5me66ixhpsTfpvt4bw7sbTeM5a8OHadKkReCx1D2tBoXKPWhDICq5glRBcCh1f5pkpcUtc4ZV49GUI0T"
"pUcMoOZl8QJhiRIoEN5VH+bJBHC4B3UuUaGA778j0r1zgyVluHOgBTipl5YKwvOl7SaLwrvhI054O62p"
"hu5OoZfBhXVmwh1l3hcTaeQbfrZOwpVX3+5RuFPwD+qdANCJVjzm5Xz5vVI1mDtqrg+df5EXra5YrWjE"
"E4qd2CMz7KTd+CMfvS4WdYmLgEjKNExvg0NXC4DCYr0QVykmtvM/c31TjYD2MmKGZQIDAQAB"
```

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

- Leveraging great existing technologies, providing a glue to keep them in sync, and allowing **senders** to mandate rejection policies and have visibility of offending traffic.
- Reports back to the spoofed entity.
- BOTH SPF authentication and DKIM verification.
- Synchronization between *Envelope From*, *Header From*.

```
> dig _dmarc.igo232.com TXT +short
"v=DMARC1; p=none; fo=1; ri=3600;
rua=mailto:pipershark@rua.dmp.cisco.com,mailto:robsherw@igo232.com;
ruf=mailto:pipershark@ruf.dmp.cisco.com,mailto:robsherw@igo232.com"
```

A typical incoming mail example

INCOMING

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

A typical incoming mail example

Sender Reputation Filtering (SBRS)

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

A typical incoming mail example

Connection Filtering

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

A typical incoming mail example


```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

A typical incoming mail example

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTX
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

* Message Filtering

A typical incoming mail example

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

Per-policy filtering

A typical incoming mail example

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF al
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Cate
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@ig
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo2
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamp
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Resu
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com>
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

Anti-spam Scanning (AS)

Anti-virus Scanning (AV)

Advanced Malware Protection (AMP)

When enabled, we would also see...

Graymail Detection

Content Filtering

Outbreak Filtering (VOF)

A typical incoming mail example

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

SMTP Client

A typical incoming mail example

```
Sun Jan 19 07:48:31 2020 Info: New SMTP ICID 553697 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Sun Jan 19 07:48:31 2020 Info: ICID 553697 ACCEPT SG WHITELIST match 136.56.60.2 SBRS None country United States
Sun Jan 19 07:48:31 2020 Info: Start MID 47831 ICID 553697
Sun Jan 19 07:48:31 2020 Info: MID 47831 ICID 553697 From: <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 ICID 553697 RID 0 To: <robsherw@bce-demo.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: SPF Verdict Cache using cached verdict
Sun Jan 19 07:48:32 2020 Info: SPF Verdict Cache cache status: hits = 21, misses = 599, expires = 66, adds = 597, seconds saved = 1.25, total seconds = 9.85
Sun Jan 19 07:48:32 2020 Info: MID 47831 SPF: mailfrom identity robsherw@igo232.com Pass (v=spf1)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Message from domain igo232.com, DMARC pass (SPF aligned True, DKIM aligned False)
Sun Jan 19 07:48:32 2020 Info: MID 47831 DMARC: Verification passed
Sun Jan 19 07:48:32 2020 Info: MID 47831 Message-ID '<20200119104055.152731@igo232.com>'
Sun Jan 19 07:48:32 2020 Info: MID 47831 Subject 'test Sun, 19 Jan 2020 10:40:55 -0500'
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: igo232.com, env-from: igo232.com, header-from: igo232.com, reply-to: Not
Present
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 7 years 7 months 9 days for domain: igo232.com
Sun Jan 19 07:48:32 2020 Info: MID 47831 SDR: Tracker Header :
Z70s+zOlQHLls4HSI8tlwK7ZNzPd7yJ4OjxJcV3FQSJIClldZrc1B+xFSS3EwCBdn9hVe8nxgbuhPqL6DICgRRjgJRvy6fvpOttFh29MMdLzxZDAAetqfXXtCa+AMJ7Mv8vXiMVSGrpphnZ1wqorUeUcAdzi/I/qKqvobDm2i8Pnt5NZU98RalCTrB6/MZ2eeUB
od5EEsBFdYsAO2yAawuP28/z6B4T2YDDridD6CZG5CNWusOvmaEjxy3Md7P8dm+1kdg/YTtMz+k8X6BTwxh3bET76uqu7Lz3EBA0QwRUETZdj/VA7w9312kQsHTXe
Sun Jan 19 07:48:32 2020 Info: MID 47831 ready 795 bytes from <robsherw@igo232.com>
Sun Jan 19 07:48:32 2020 Info: MID 47831 Custom Log Entry: <<<=== MF_SDR_Verdict_matched ===>>>
Sun Jan 19 07:48:32 2020 Info: MID 47831 matched all recipients for per-recipient policy robsherw in the inbound table
Sun Jan 19 07:48:32 2020 Info: ICID 553697 close
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim verdict using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 using engine: CASE spam negative
Sun Jan 19 07:48:32 2020 Info: MID 47831 interim AV verdict using Sophos CLEAN
Sun Jan 19 07:48:32 2020 Info: MID 47831 antivirus negative
Sun Jan 19 07:48:33 2020 Info: MID 47831 AMP file reputation verdict : UNKNOWN
Sun Jan 19 07:48:33 2020 Info: MID 47831 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Sun Jan 19 07:48:33 2020 Info: MID 47831 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Sun Jan 19 07:48:34 2020 Info: MID 47831 rewritten to MID 47832 by add-footer filter 'Footer Stamping'
Sun Jan 19 07:48:34 2020 Info: Message finished MID 47831 done
Sun Jan 19 07:48:34 2020 Info: MID 47832 queued for delivery
Sun Jan 19 07:48:34 2020 Info: New SMTP DCID 27388 interface 139.138.56.31 address 104.47.70.110 port 25
Sun Jan 19 07:48:34 2020 Info: DCID 27388 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Sun Jan 19 07:48:35 2020 Info: Delivery start DCID 27388 MID 47832 to RID [0]
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass
smtp.mailfrom=robsherw@igo232.com; dmarc=pass (p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
Sun Jan 19 07:48:36 2020 Info: MID 47832 RID [0] Response '2.6.0 <20200119104055.152731@igo232.com> [InternalId=4307852199405, Hostname=MN2PR13MB3184.namprd13.prod.outlook.com] 15696 bytes in
0.296, 51.633 KB/sec Queued mail for delivery'
Sun Jan 19 07:48:36 2020 Info: Message finished MID 47832 done
```

Delivery

Utilizing SPF, DKIM, DMARC on Cisco Email Security

Anti-spoof, throttling & authentication

Encryption & authentication enforcement

Where does Cisco Email Security help?

Anti-spoof, throttling & authentication

Connection Filtering INCOMING

Encryption & authentication enforcement

Connection Filtering OUTBOUND

Remember the email security mail flow pipeline?

AsyncOS supports email verification and signing to prevent email forgery.

Incoming mail verification supports & uses:

- Sender Policy Framework (SPF)
- Sender ID Framework (SIDF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Forged Email Detection (FED)

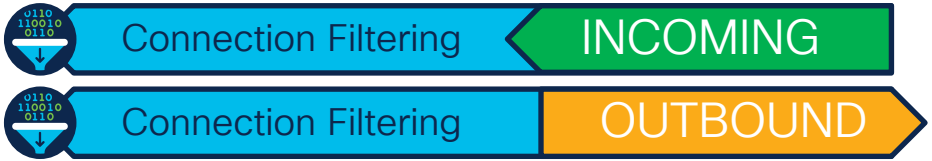
(And, remember list our acronyms?)

To authenticate outbound mail, DomainKeys and DKIM signing are supported.

Where does Cisco Email Security help?

Anti-spoof, throttling & authentication

Encryption & authentication enforcement



SPF, DKIM, DMARC checks using the security features inside of a Mail Flow Policy are included in the Cisco Email Security licensing.

Note: AsyncOS 13.5 for Email Security - the ESA incorporates the **Cisco Advanced Phishing Protection (APP)** product and act as the sensor, forwarding metadata of an email to the APP Cloud.

Note: Cisco Advanced Phishing Protection is a separate subscription (license).
See the Cisco Email Security Ordering Guide for GPL: http://cs.co/email_GPL

We will discuss APP in just a few minutes...

Where does Cisco Email Security help?

Anti-spoof, throttling & authentication

Connection Filtering

INCOMING

To pass DMARC verification, an email must pass at least one of these authentication mechanisms, and the Authentication Identifiers must comply with RFC 5322.

The Email Security appliance allows you to:

- Verify incoming emails using DMARC.
- Define profiles to override (accept, quarantine, or reject) domain owners' policies.
- Send feedback reports to domain owners, which helps to strengthen their authentication deployments.
- Send delivery error reports to the domain owners if the DMARC aggregate report size exceeds 10 MB or the size specified in the RUA tag of the DMARC record.

- The ESA will not perform DMARC verification of messages from domains with malformed DMARC records. However, the appliance can receive and process such messages.

DMARC verification workflow

Anti-spoof, throttling & authentication

Connection Filtering INCOMING

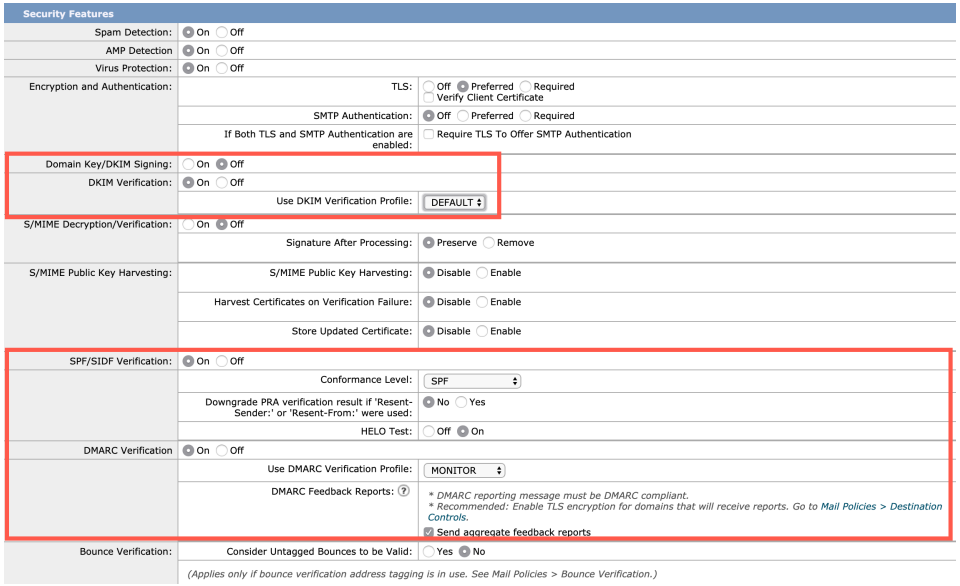
1. A listener configured on an ESA receives an SMTP connection.
2. The ESA performs SPF and DKIM verification on the message.
3. The ESA fetches the DMARC record for the sender's domain from the DNS.
   - If no record is found, the ESA skips the DMARC verification and continues processing.
   - If the DNS lookup fails, the ESA acts based on the specified DMARC verification profile.
4. Depending on DKIM and SPF verification results, ESA performs DMARC verification on the message.
   - Note: If DKIM and SPF verification is enabled, DMARC verification reuses the DKIM and SPF verification results.
5. Depending on the DMARC verification result and the specified DMARC verification profile, the ESA accepts, quarantines, or rejects the message. If the message is not rejected due to DMARC verification failure, the ESA continues processing.
6. The ESA sends an appropriate SMTP response and continues processing.
7. If sending of aggregate reports is enabled, the ESA gathers DMARC verification data and includes it in the daily report sent to the domain owners. For more information about the DMARC aggregate feedback report, see DMARC Aggregate Reports.
   - Note: If the aggregate report size exceeds 10 MB or the size specified in the RUA tag of the DMARC record, the ESA sends delivery error reports to the domain owners.

Policy level (Mail Flow Policies)

Anti-spoof, throttling & authentication

Connection Filtering INCOMING

- Cisco recommendation is to configure at the policy level, SPF, DKIM, DMARC verification during the initial connection for incoming, and signing during outgoing.



Security Features		
Spam Detection:	◉ On ○ Off	
AMP Detection	◉ On ○ Off	
Virus Protection:	◉ On ○ Off	
Encryption and Authentication:	TLS:	○ Off ◉ Preferred ○ Required ○ Verify Client Certificate
	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
S/MIME Decryption/Verification:	○ On ◉ Off	
	Signature After Processing:	◉ Preserve ○ Remove
S/MIME Public Key Harvesting:	S/MIME Public Key Harvesting:	◉ Disable ○ Enable
	Harvest Certificates on Verification Failure:	◉ Disable ○ Enable
	Store Updated Certificate:	◉ Disable ○ Enable
SPF/SIDF Verification:	◉ On ○ Off	
	Conformance Level:	SPF
	Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:	◉ No ○ Yes
	HELO Test:	○ Off ◉ On
DMARC Verification	◉ On ○ Off	
	Use DMARC Verification Profile:	MONITOR
	DMARC Feedback Reports:	* DMARC reporting message must be DMARC compliant. * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies > Destination Controls. ☑ Send aggregate feedback reports
Bounce Verification:	Consider Untagged Bounces to be Valid:	○ Yes ◉ No
	(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)	

Mail logs example

Anti-spoof, throttling & authentication

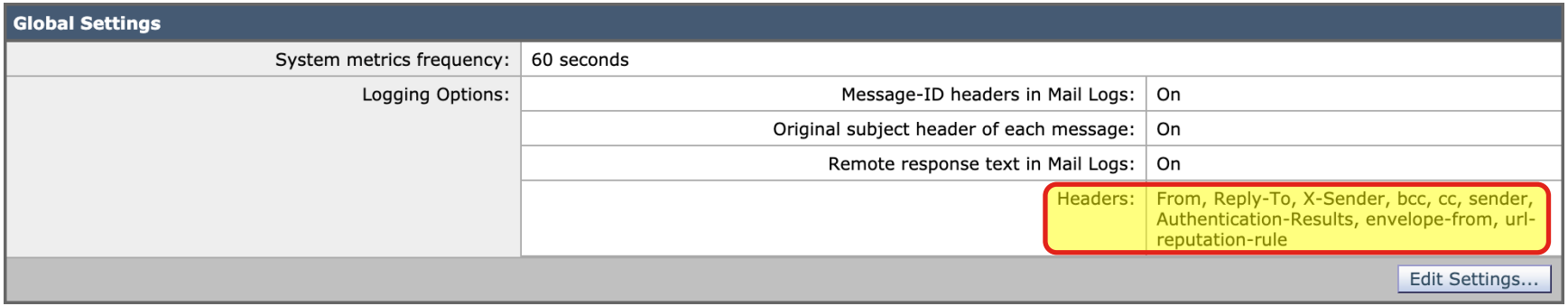
Connection Filtering INCOMING

When enabled, looking at the mail logs, we see the ESA validates SPF, DKIM, DMARC right at the start of communication...

```
Thu Jan 16 08:57:35 2020 Info: New SMTP ICID 550475 interface Data 1 (139.139.139.139) address 136.136.1.1 reverse
dns host unknown verified no
Thu Jan 16 08:57:35 2020 Info: ICID 550475 ACCEPT SG WHITELIST match 136.136.1.1 SBRS None country None
Thu Jan 16 08:57:36 2020 Info: Start MID 47676 ICID 550475
Thu Jan 16 08:57:36 2020 Info: MID 47676 ICID 550475 From: <admin@pipershark.com>
Thu Jan 16 08:57:37 2020 Info: MID 47676 ICID 550475 RID 0 To: <robsherw@bce-demo.com>
Thu Jan 16 08:57:38 2020 Info: MID 47676 SPF: mailfrom identity admin@pipershark.com Pass (v=spf1)
Thu Jan 16 08:57:43 2020 Info: MID 47676 DMARC: Message from domain pipershark.com, DMARC pass (SPF aligned True,
DKIM aligned False)
Thu Jan 16 08:57:43 2020 Info: MID 47676 DMARC: Verification passed
Thu Jan 16 08:57:43 2020 Info: MID 47676 Subject '.:|:.:|:. SMTP - EMAIL Jan 16 11:50:09 AM ‘

...
```

Logging additional headers



- Under Log Subscriptions Settings (GUI) or the **logconfig** command (CLI), configure additional headers to be logged
- These will be displayed in the mail_logs and message tracking output upon creation of a DCID (Delivery Connection ID)

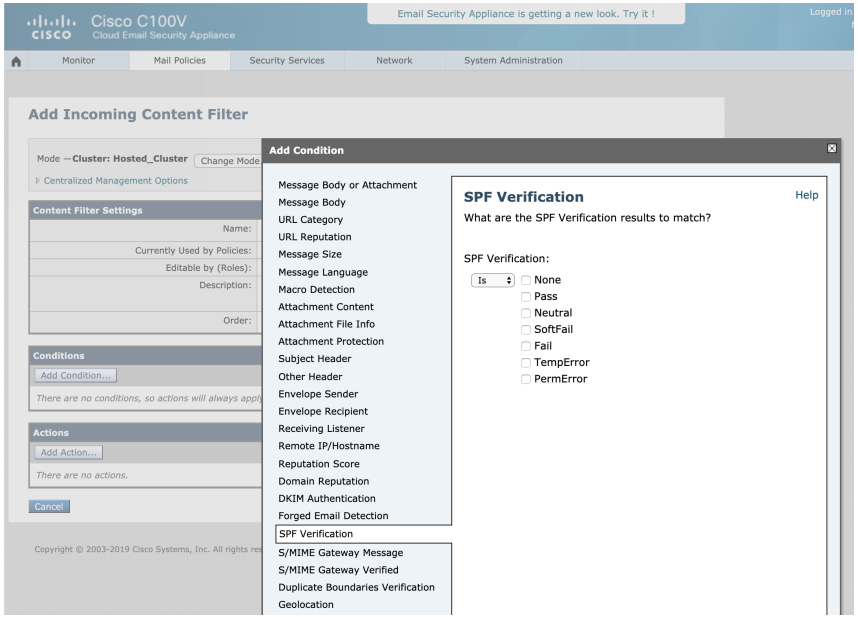
```
Sun Jan 19 07:48:36 2020 Info: Message done DCID 27388 MID 47832 to RID [0] [('Authentication-Results', 'esa1.hc3033-
47.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass smtp.mailfrom=robsherw@igo232.com; dmarc=pass
(p=none dis=none) d=igo232.com'), ('from', 'robsherw@igo232.com')]
```

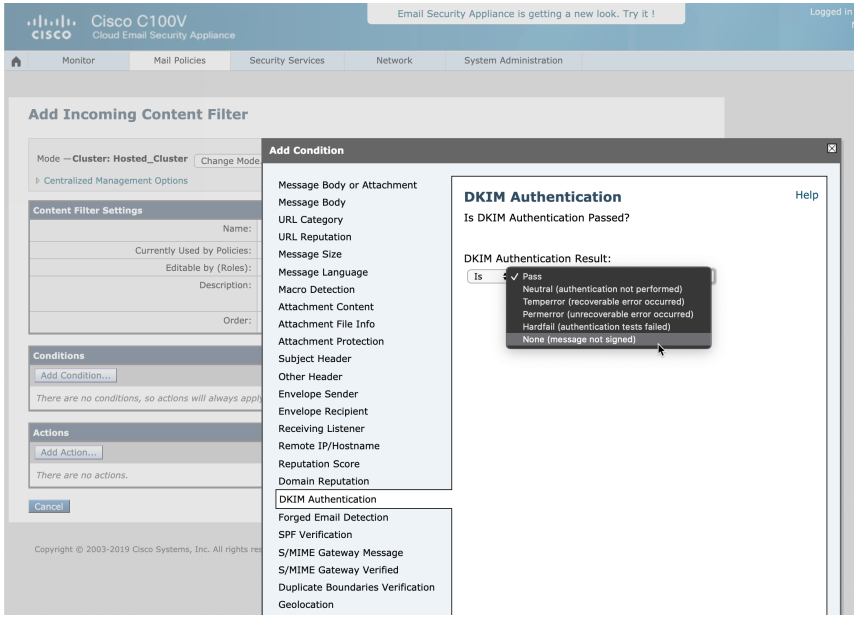
Content filtering conditions (Incoming/Outgoing Mail Policies)

Content protection

Content Filtering INCOMING

As mail moves through the pipeline, with Content Filtering, an administrator could choose to take further actions based on SPF & DKIM conditions...





Content filtering example

Content protection

Content Filtering INCOMING

In this example, we'll choose to quarantine any message that Fails or SoftFails SPF...

```
Thu Jan 16 09:39:49 2
Thu Jan 16 09:39:54 2
Thu Jan 16 09:39:54 2
Thu Jan 16 09:39:54 2
...
Thu Jan 16 09:39:56 2
'SPF_DKIM_FAIL'
...
Thu Jan 16 09:39:56 2
(duplicated by conten
Thu Jan 16 09:39:56 2
Thu Jan 16 09:39:56 2
```

Content Filter Settings

Name:	SPF_DKIM_FAIL
Currently Used by Policies:	robsherw
Editable by (Roles):	Cloud Operator
Description:	Evaluate the result of SPF and take a quarantine action
Order:	18 (of 52)

Conditions

Add Condition... Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	SPF Verification	spf-status == "softfail,fail"	
2	DKIM Authentication	dkim-authentication == "hardfail"	

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("SPF_DKIM_FAILURES")	
2	Add Log Entry	log-entry("<<<=== SPF_DKIM_FAIL ===>>>")	

Forged Email Detection (FED)

Taking what we know from 'authentication' and applying w/ FED

- FED will only create a log entry for a score that is the same or higher than what is configured; Enable logging of From and Reply-To headers.

Content Filter Settings

Name:	CF_FED
Currently Used by Policies:	robsherw, Default Policy
Editable by (Roles):	Cloud Operator
Description:	
Order:	4 (of 52)

Conditions

Add Condition... | Apply rule: Only if all conditions match

Order	Condition	Rule	Delete
1	Forged Email Detection	forged-email-detection("FED_DICTIONARY", 70, "")	
2	Other Header	header("authentication-results") == "fail"	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<=== FED DICTIC	
2	Add/Edit Header	insert-header("X-FED-IDENTI	
3	Quarantine	quarantine("FORGED_EMAIL"	

Best Practices Guide for Anti-Spoofing
http://cs.co/esa_antispoof

Skipped DMARC verification

Content protection

New with AsyncOS 12.5: Configuring content and message filters to handle messages that skipped DMARC verification...

You can configure your appliance to take actions on the messages that skipped the DMARC verification.

Use the following settings in the **Other Header** content filter to categorize the messages that skipped the DMARC verification:

- Add the Header Name as **X-Ironport-DMARC-Check-Result**
- Select Header Value, choose Equals, and add any one of the following values:
  validskip, invalidskip, temperror, and permerror

The following is an example of a message filter rule syntax that is used to categorize a message that skipped the DMARC verification:

```
Quarantine_messages_DMARC_skip: if(header("X-Ironport-DMARC-Check-Result") ==
"^validskip$") { quarantine("Policy"); }
```

* Message Filtering

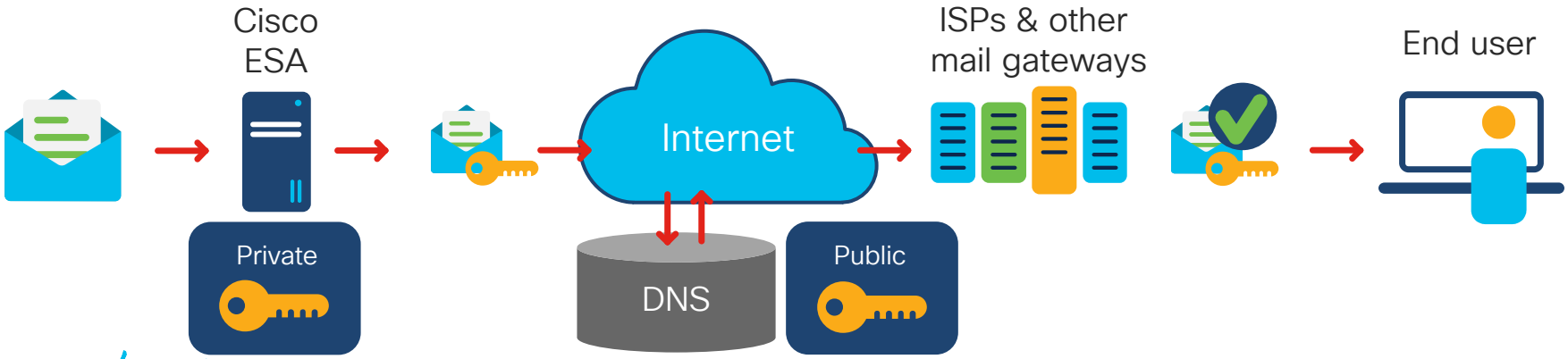
Signing Keys + Signing Profiles

Encryption & authentication enforcement

Connection Filtering | OUTBOUND

- With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography. The verified domain can then be used to detect forgeries by comparing it with the domain in the From: (or Sender:) header of the email.

- DomainKeys and DKIM consist of two main parts: signing and verification. The ESA supports the “signing” half of the process for DomainKeys, and it supports both signing and verification for DKIM.



A typical outbound email

OUTBOUND

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09/GSidNs/zWaCqHdz/LSOTTGOpTihpZdte/xx6X0joa48dB7cxrhG/TQCyhr6cfhLD4Tj4dtbakHQcHfNNDrgVjjBggYNXKSKk
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcysML08k=
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for delivery
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 interface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing: Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none'), ('from',
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com> [InternalId=4728758996564, Hostname=BN7PR13MB2484.namprd13.prod.outlook.com] 12330 bytes in
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```

A typical outbound email

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09/GSidNs/zWaCqHdz/LSOTTGOpTihpZdte/xx6X0joa48dB7cxrhG/TQCyhr6cfhLD4Tj4dtbakHQcHfNNDrgVjjBggYNXKSKk
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcysML08k=
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for delivery
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 interface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing: Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none'), ('from',
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com> [InternalId=4728758996564, Hostname=BN7PR13MB2484.namprd13.prod.outlook.com] 12330 bytes in
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```

Sender Reputation Filtering (SBRS)

A typical outbound email

Connection Filtering

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09/GSidNs/zWaCqHdz/LSOTTGOpTihpZdte/xx6X0joa48dB7cxrhG/TQCyhr6cfhLD4Tj4dtbakHQcHfNNDrgVjjBggYNXKSKk
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcysML08k=
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for delivery
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 interface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing: Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none'), ('from',
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com> [InternalId=4728758996564, Hostname=BN7PR13MB2484.namprd13.prod.outlook.com] 12330 bytes in
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```

A typical outbound email

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09/GSidNs/zWaCqHdz/LSOTTGOpTihpZdte/xx6X0joa48dB7cxrhG/TQCyhr6cfhLD4Tj4dtbakHQcHfNNDrgVjjBggYNXKSKk
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcysML08k=
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for delivery
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 interface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing: Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none'), ('from',
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com> [InternalId=4728758996564, Hostname=BN7PR13MB2484.namprd13.prod.outlook.com] 12330 bytes in
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```

Per-policy filtering

A typical outbound email

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcy
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for delivery
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 interface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing: Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com>
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```

- Anti-virus Scanning (AV)
- Advanced Malware Protection (AMP)
- Data Loss Prevention (DLP)

When enabled, we would also see...

- Anti-spam Scannig (AS)
- Graymail Detection
- Content Filtering
- Outbreak Filtering (VOF)

A typical outbound email

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09/GSidNs/zWaCqHdz/LSOTTGOpTihpZdte/xx6X0joa48dB7cxrhG/TQCyhr6cfhLD4Tj4dtbakHQcHfNNDrgVjjBggYNXKSKk
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcysML08k=
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for deli
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 in erface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS succes protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none'), ('from',
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com> [InternalId=4728758996564, Hostname=BN7PR13MB2484.namprd13.prod.outlook.com] 12330 bytes in
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```

SMTP Client

```
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
```

A typical outbound email

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09/GSidNs/zWaCqHdz/LSOTTGOpTihpZdte/xx6X0joa48dB7cxrhG/TQCyhr6cfhLD4Tj4dtbakHQcHfNNDrgVjjBggYNXKSKk
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcysML08k=
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for delivery
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 interface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing: Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none'), ('from',
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com> [InternalId=4728758996564, Hostname=BN7PR13MB2484.namprd13.prod.outlook.com] 12330 bytes in
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```

Delivery

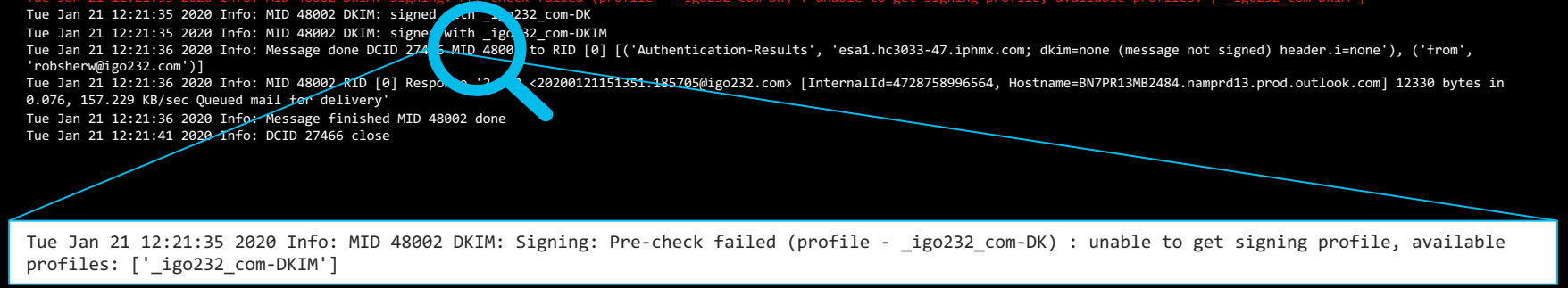
```
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
```

Audience question

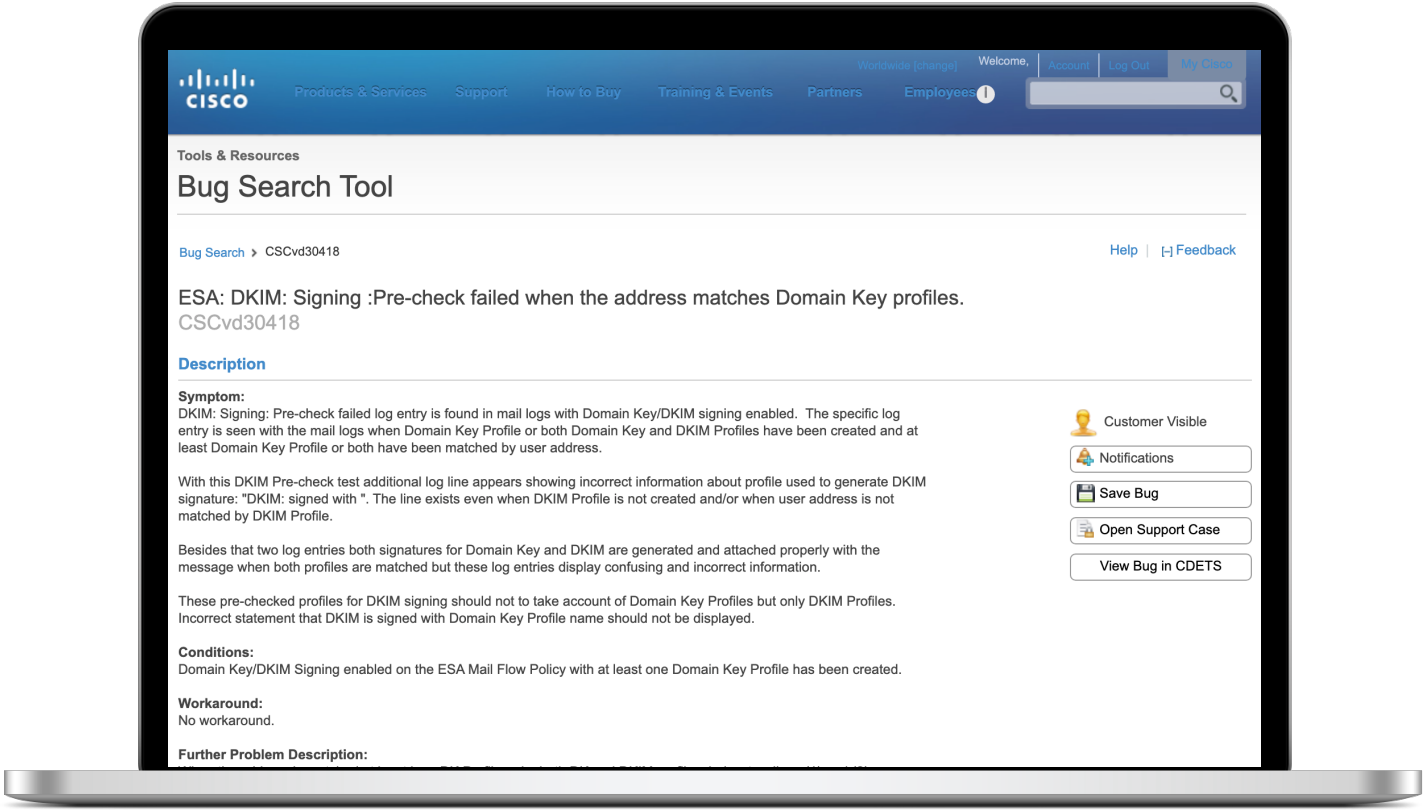
What is the following...

A typical outbound email

```
Tue Jan 21 12:21:33 2020 Info: New SMTP ICID 555358 interface Data 1 (139.138.56.31) address 136.56.60.2 reverse dns host unknown verified no
Tue Jan 21 12:21:33 2020 Info: ICID 555358 RELAY SG RELAYLIST match 136.56.60.2 SBRS 5.1 country United States
Tue Jan 21 12:21:34 2020 Info: Start MID 48002 ICID 555358
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 From: <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 ICID 555358 RID 0 To: <robsherw@bce-demo.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 Message-ID '<20200121151351.185705@igo232.com>'
Tue Jan 21 12:21:34 2020 Info: MID 48002 Subject 'test Tue, 21 Jan 2020 15:13:51 -0500'
Tue Jan 21 12:21:34 2020 Info: MID 48002 SDR: Tracker Header :
/GI+ArS+s96Pw/NDcbjbuOMDRZ7pYV2uRcCkM2E26gK/2Bhhe+9Q84iWmXXHk/EMsCunsx2V/TwPbiQWZW7Jr1UsToU3kCSo09/GSidNs/zWaCqHdz/LSOTTGOpTihpZdte/xx6X0joa48dB7cxrhG/TQCyhr6cfhLD4Tj4dtbakHQcHfNNDrgVjjBggYNXKSKk
VaTXNxp/hEew5ZUI6m2G1ck/VXwTAq3hc3RqlODxnlczByL17Tfd3LEjSLyKCOUNxpsNa1l2PRgR0sK3qdspzCcqu8yxGaoFcysML08k=
Tue Jan 21 12:21:34 2020 Info: MID 48002 ready 795 bytes from <robsherw@igo232.com>
Tue Jan 21 12:21:34 2020 Info: MID 48002 matched all recipients for per-recipient policy DEFAULT in the outbound table
Tue Jan 21 12:21:34 2020 Info: ICID 555358 close
Tue Jan 21 12:21:34 2020 Info: MID 48002 interim AV verdict using Sophos CLEAN
Tue Jan 21 12:21:34 2020 Info: MID 48002 antivirus negative
Tue Jan 21 12:21:34 2020 Info: MID 48002 AMP file reputation verdict : UNKNOWN
Tue Jan 21 12:21:34 2020 Info: MID 48002 DLP no violation
Tue Jan 21 12:21:34 2020 Info: MID 48002 DomainKeys: signing with _igo232_com-DK - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 DKIM: signing with _igo232_com-DKIM - matches robsherw@igo232.com
Tue Jan 21 12:21:34 2020 Info: MID 48002 queued for delivery
Tue Jan 21 12:21:35 2020 Info: New SMTP DCID 27466 interface 139.138.56.31 address 104.47.55.110 port 25
Tue Jan 21 12:21:35 2020 Info: DCID 27466 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jan 21 12:21:35 2020 Info: Delivery start DCID 27466 MID 48002 to RID [0]
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: Signing: Pre-check failed (profile - _igo232_com-DK) : unable to get signing profile, available profiles: ['_igo232_com-DKIM']
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DK
Tue Jan 21 12:21:35 2020 Info: MID 48002 DKIM: signed with _igo232_com-DKIM
Tue Jan 21 12:21:36 2020 Info: Message done DCID 27466 MID 48002 to RID [0] [('Authentication-Results', 'esa1.hc3033-47.iphmx.com; dkim=none (message not signed) header.i=none'), ('from',
'robsherw@igo232.com')]
Tue Jan 21 12:21:36 2020 Info: MID 48002 RID [0] Response '2.6.0 <20200121151351.185705@igo232.com> [InternalId=4728758996564, Hostname=BN7PR13MB2484.namprd13.prod.outlook.com] 12330 bytes in
0.076, 157.229 KB/sec Queued mail for delivery'
Tue Jan 21 12:21:36 2020 Info: Message finished MID 48002 done
Tue Jan 21 12:21:41 2020 Info: DCID 27466 close
```



It’s a bug...



Cisco Advanced Phishing Protection

Phishing behavioral analytics & protection

Advanced Phishing Protection (APP)

Request an evaluation of APP or DP?
https://order.ces.cisco.com/eval/

Cisco Advanced Phishing Protection

More users rely on cloud applications like O365, making them more vulnerable to advanced phishing attacks.

"Phishing attacks cost companies $9.1B in 2017."

- 2017 Global Fraud and Cybercrime Forecast

"**32%** of breaches involved phishing."

- Verizon 2019 Data Breach Investigations Report

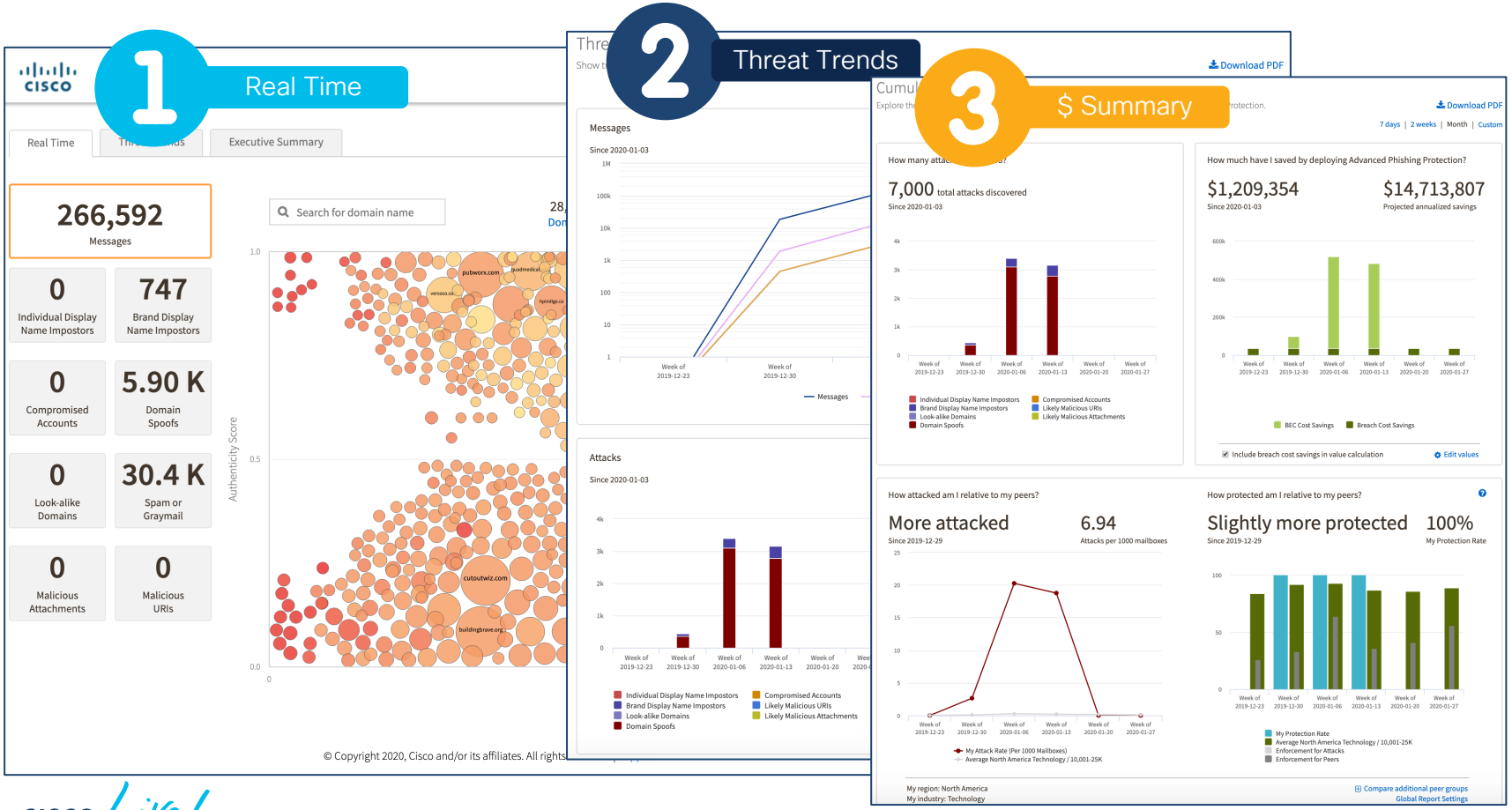
The average solution does not work against advanced phishing attacks because they do not contain malware making them hard to detect. These are sophisticated, low-volume, and targeted email attacks.

Cisco Advanced Phishing Protection

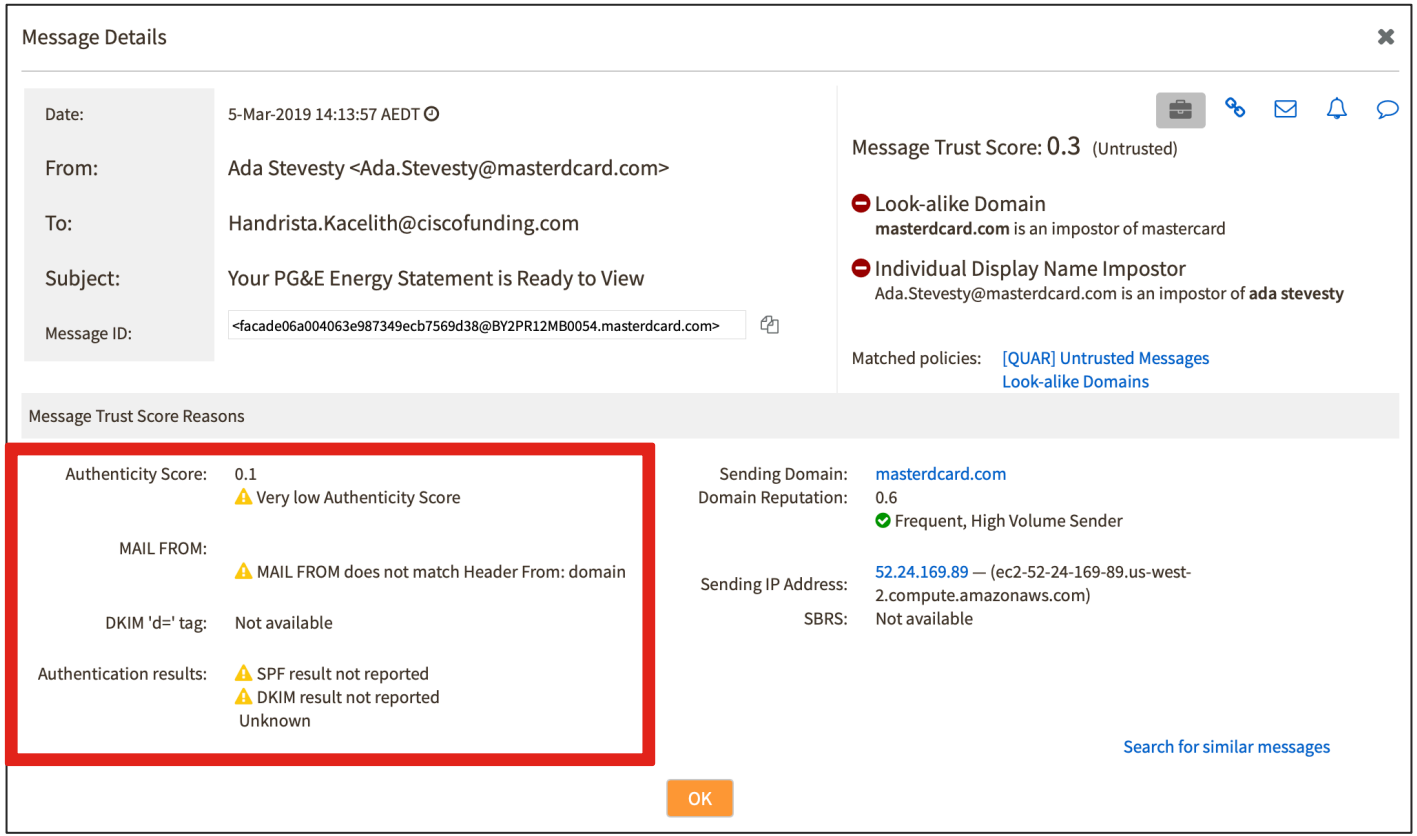
With Cisco Advanced Phishing Protection (APP):

- Gain a real-time understanding of senders, learn, and authenticate email. identities and behavioral relationships to protect against BEC attacks.
- Remove malicious emails from users' inboxes to prevent wire fraud or other advanced attacks.
- Get detailed visibility into email attack activity, including total messages secured and attacks prevented.
- Augment phishing and BEC detection and blocking capabilities offered in Cisco® Email Security.

Cisco Advanced Phishing Protection



Cisco Advanced Phishing Protection



Cisco Advanced Phishing Protection

Cisco Advanced Phishing Protection (APP) provides:

- Advanced intelligence that authenticates senders in real-time.
- A self-learning network that models your organization's unique inbound traffic patterns to detect fraud quickly.
- Efficient removal of malicious emails from users' inboxes - even from Office365 mailboxes.

Cisco Domain Protection

Brand protection, SPF/DKIM/DMARC administration

Domain Protection (DP)

Request an evaluation of APP or DP?
https://order.ces.cisco.com/eval/

Cisco Domain Protection

Your organization allows third party senders use of its domain for brand communications.

Attackers can exploit this and impersonate your domain to send out phishing emails to your customers.

> *"3% of people will click on any given phishing campaign."*
>
> – Verizon 2019 Data Breach Investigations Report

Cisco Domain Protection

(Acronyms!!!!?)

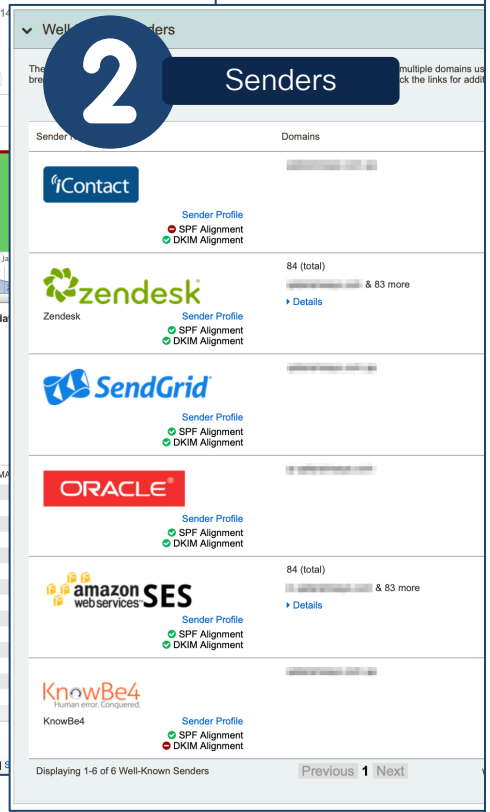
With Cisco Domain Protection (CDP or DP)(sometimes DMP):

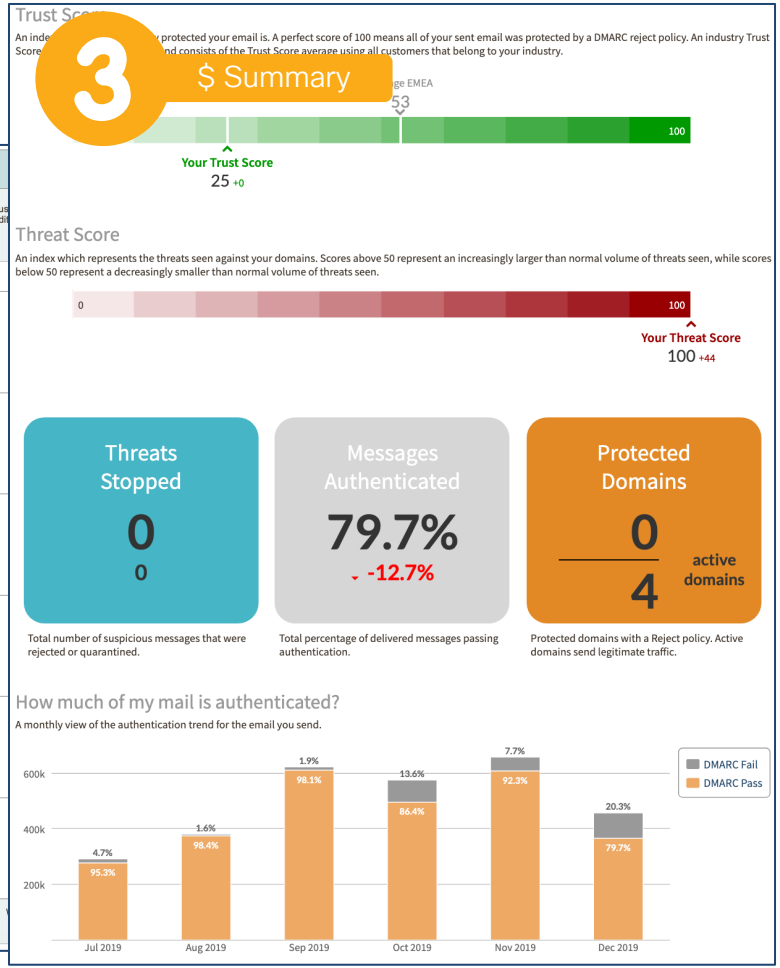
- Automates the DMARC email authentication process to achieve DMARC compliance.
- Gives you visibility into all your email senders via an easy-to-read reporting.
- Helps you block unauthorized senders to reduce or eliminate phishing emails from your domain.

Cisco Domain Protection

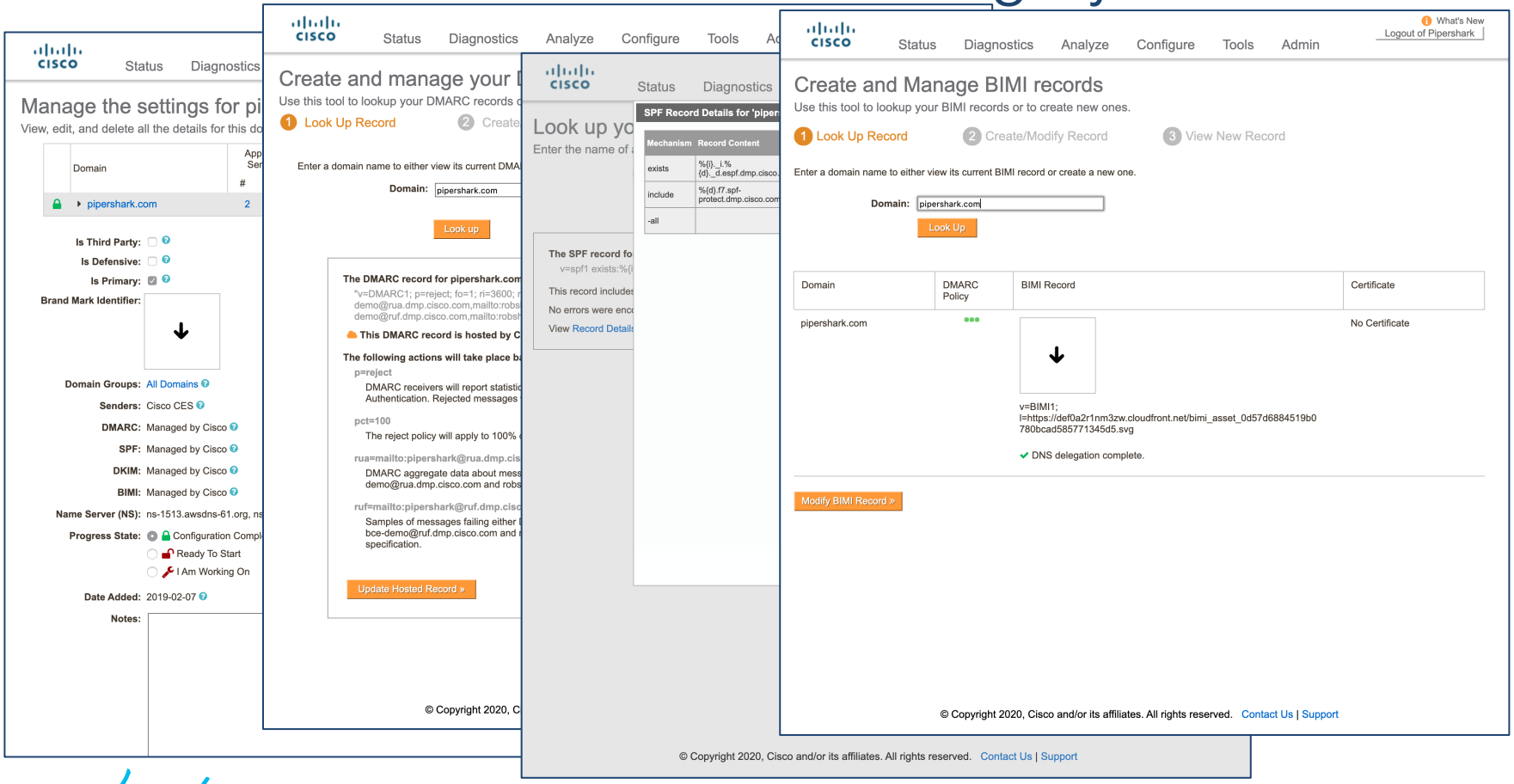
- Typically, a customer sets up their DMARC record and receives reports.
- There are two distinct report types:
  - Aggregate report (rua)
    - Sent on an interval
    - Summary of all incidents from a sender domain
  - Failure report (ruf)
    - Sent on (every) failure
    - Detailed report on individual failures

Cisco Domain Protection





Cisco Domain Protection – manage your DNS



APP & DP are both integrated with ESA

Starting with AsyncOS 13.5 for Email Security [Mar 2020]:

- The ESA may now be configured as the sensor engine for our Cisco Advanced Phishing Protection (APP) cloud service.
- APP relies on a sensor engine to receive a copy of the message metadata sent inbound into your organization.
- BOTH APP and DP reportability from their respective cloud services are integrated into the reportability on ESA & SMA.

Release Notes: http://cs.co/13_5_release_notes
User Guide: http://cs.co/13_5_user_guide

Verifying incoming emails, signing outbound emails are needed steps to reduce fake emails...

What is Cisco doing to improve efficacy when it comes to phishing?

Phishing Efficacy

“32% of breaches covered in the 2019 Verizon Data Breach Investigations Report involved phishing.”

– Gartner 2019 Market Guide for Email Security

- Download: http://cs.co/email_Gartner2019

Phishing efficacy
Improving detection and conviction

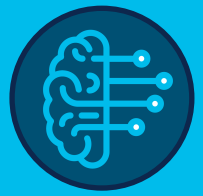
- Cisco Email Security relies on constant and incremental improvements from...

Research and Efficacy Team (RET), Threat Grid (TG)

Natural Language Understanding (NLU)

PoCs

Static analysis for email [CASE]



Machine Learning (ML) classifiers

[CUA, CPA]

Improving threat efficacy via machine learning

Improving Threat Detection Efficacy in AsyncOS 13.5 for Email Security

Cloud URL Analysis (CUA)

- A new engine deployed in Cisco cloud, that intakes URLs from telemetry and collects artifacts and make behavioral determinations based on the URL and the content that it points to.

Cloud Phishing Analysis (CPA)

- A new engine deployed in Cisco cloud, that intakes the consolidated telemetry and features from the platform engines and CUA responses in order to convict phishing attacks.

Cloud URL Analysis (CUA)

- CUA is a URL intelligence generating service that analyses URLs sent to Talos' cloud URL reputation lookup service.

- CUA integrates existing WBRS information with a variety of different analysis techniques, leveraging Cisco's internal information and tooling, 3rd party intelligence, and new research techniques coming from Talos's threat specialists.

- By actively analyzing many facets of a URL, from the structure of the URL itself to information about the domain and even page contents, CUA provides the ability for Talos to detect and deliver intelligence on a variety of URL based attacks.

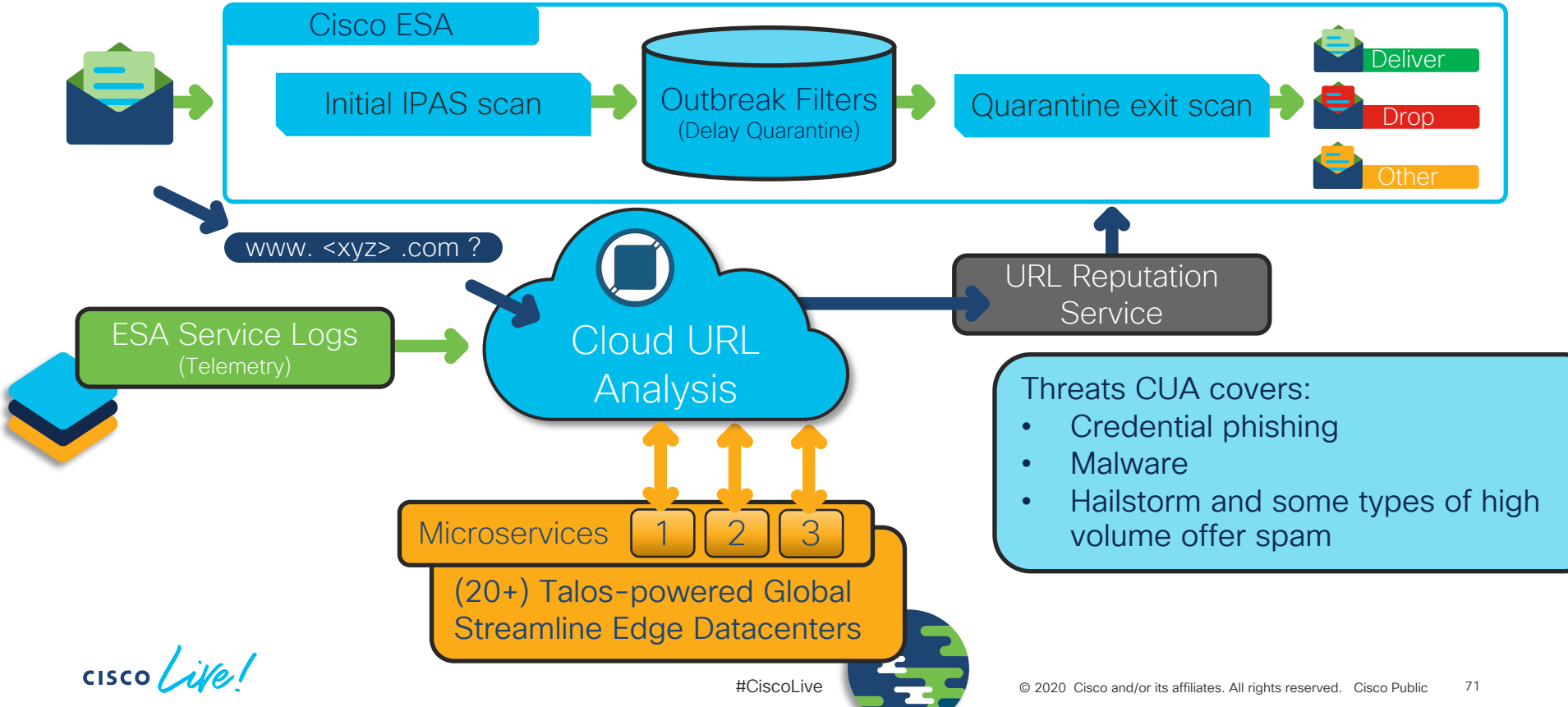
What URLs are analyzed by CUA?

- URLs parsed from messages hitting Outbreak Filters (at any threat level and independent of other verdicts such as IPAS) are analyzed by CUA.

- Emails that trigger Outbreak Filters (at any threat level, regardless of IPAS verdict or quarantine actions) will have their URLs sent for analysis in CUA. This requires the ESA to be using Web Intelligence lookups and have Service Logs(*) enabled.

(*)Note: Service Logs replace senderbase as the telemetry data that is sent to Cisco Talos' Cloud service. Without this data, Cloud URL Analysis (CUA) is unable to gather the information needed in real-time to process and convict.

Cloud URL Analysis (CUA) overview



Threats CUA covers:

- Credential phishing
- Malware
- Hailstorm and some types of high volume offer spam

Cloud URL Analysis (CUA) facts

- CUA performs out-of-band cloud URL analysis.
- CUA is triggered and uses context from new Service Logs.
  - Per-message context around analyzed URLs.
- CUA leverages URL reputation services to deliver verdicts.
- CUA updates/upgrades are transparent.
  - No updates or upgrades on ESA required!

Improving threat efficacy via Threat Grid
and thanks to our Research and Efficacy Team (RET)

- Starting June 2019, RET focused on five major filetypes in TG:

URL	HTML	Office documents	PDF	Email

- Each of these provides a different surface via email to entice the user to do some action.

- RET's end goal: To study phishing attempts to understand what techniques they employ and how they can be detected.

Results
from Research and Efficacy Team (RET)

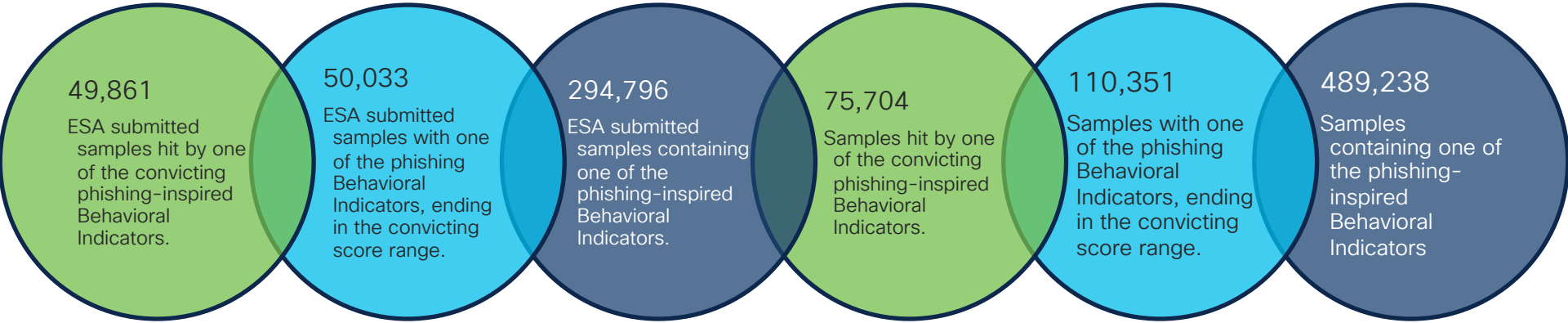
- Since June 2019, by taking these file types and samples seen in Threat Grid, RET was able to:

- Produce sixty (60) YARA rules
- Produce seventeen (17) Behavioral Indicators (BI)
- Produce or improve five (5) utilities to assist with phishing detection efforts

Results

Let's take a closer look into the results

- These BI and YARA rules had a direct and immediate impact on Threat Grid data, reporting and convictions.



What is YARA? What are YARA rules?

- YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples.
  - YARA is a name only, not an acronym!

(Thank goodness, not another acronym!)

- With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

- Each description, a.k.a. rule, consists of a set of strings and a Boolean expression which determine its logic.

More on YARA:

- https://yara.readthedocs.io/en/latest/#
- https://cybersecurity.att.com/blogs/security-essentials/explain-yara-rules-to-me
- https://securityintelligence.com/signature-based-detection-with-yara/

YARA rule example

Realtime example from RET, in use on TG today!

```
rule html_iframe_remote : anomaly
{
  meta:
    description="HTML has 'iframe' containing only remote material."
    author="afasen"
    created_at="2019-09-20"

  strings:
    //<iframe src="http://x0a.in:8080/index.php" width=125 height=112
style="visibility: hidden"></iframe>
    $a1 = /<iframe\s+[^>]*src="https?:\/\/[^"]+"[^>]*><\/iframe>/ nocase

  condition:
    any of them
}
```

How does Email Security benefit from YARA?

- Currently Cisco Email Security relies on tools and engines that operate outside of the ESA to utilize YARA rules.
- Research and analytics behind Threat Grid samples leads to creating YARA rules, which then influences the Behavioral Indicators (BI) with-in Threat Grid.

What are Behavioral Indicators?

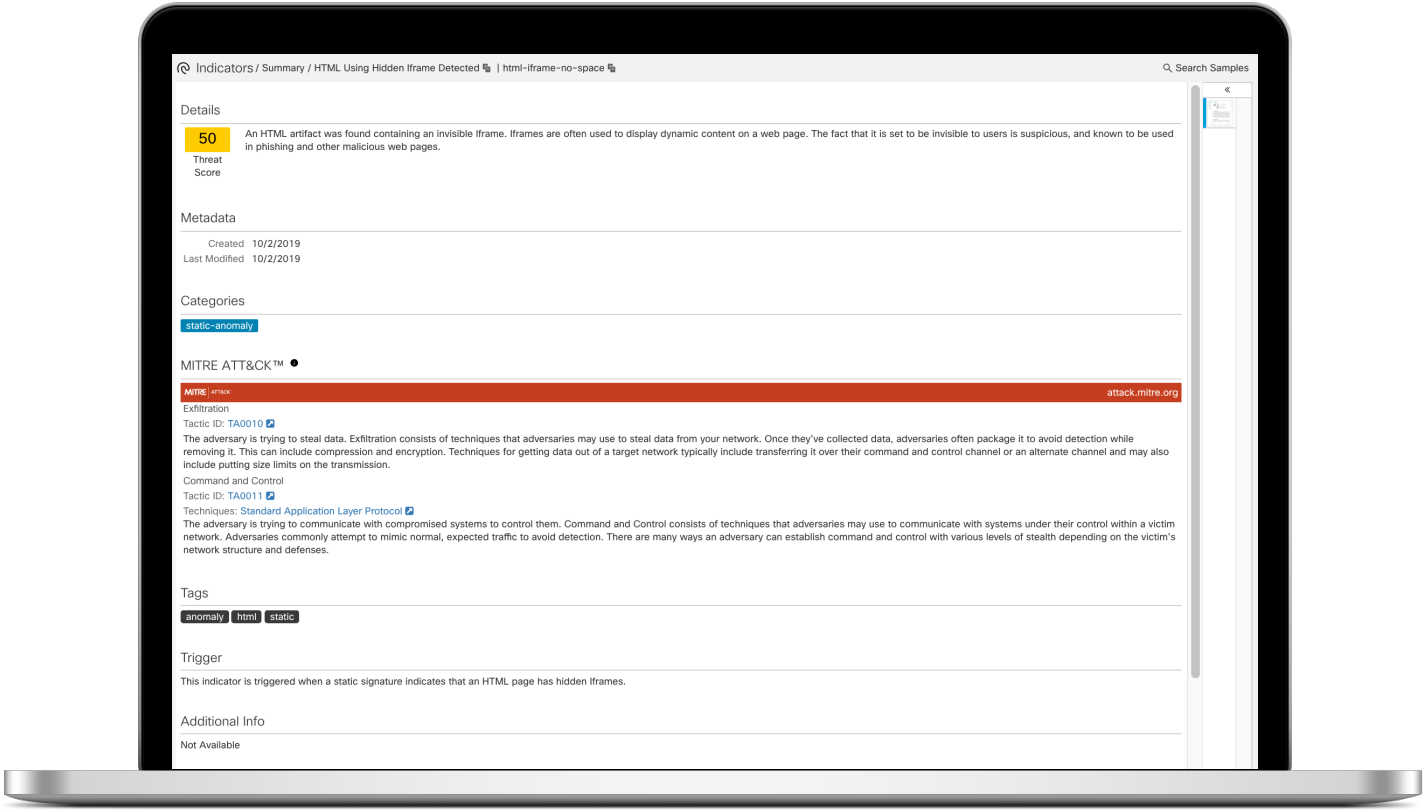
- Behavioral Indicators are the key traits and behaviors that have been identified as indicators of malicious activity.

- Behavioral Indicators include threat severity levels, HTTP Traffic, DNS Traffic, TCP/IP network sessions, Processes, Artifacts, Registry activities, and more.

- How can you see these Behavioral Indicators?
  1. Log-in to https://panacea.threatgrid.com/
  2. Click on Indicators; search Category: Malware > Phishing

- Or, Threat Grid Release Notes: https://panacea.threatgrid.com/mask/doc/mask/release_notes

Behavioral Indicator example



New or updated Threat Grid Behavioral Indicators

Jun 6

An Encrypted Phishing HTML Page Was Found

Phishing Test Detected

Aug 29

HTML Email Based Login Page Detected

Suspected Phishing Login Page Detected

HTML Su[illegible]s Unescaping Detec[illegible]

17 new or updated behavioral indicators

Oct 24

HTML Iframe Static IP Referenced

HTML Object Class ID Referenced

HTML Using Hidden Iframe Detected

Additional

artifact-html-onedrive-phish

Jun 6, 2019 | Aug 15, 2019 | Aug 29, | Sep 12, 2019 | Oct 24, 2019 | Nov 7, 2019 | Additional

Aug 15

Known Phishing Service Document Detected (*)

* Updated BI, originally published May 23

Sep 12

HTML File Starts And Ends With Script Tags

Javascript in HTML References Multiple JQuery Scripts

FakeJquery Javascript Function Within HTML

HTML Contains Only Redirection Code

Javascript in HTML Uses Document.Location.Href Property

Javascript in HTML Uses Self.Location Property

Nov 7

Submitted HTML Minimal Code With Redirect

Stopping fake, unauthenticated emails is great... and we all know that threats **happen**...

How can we focus on educating the end-user?

Cisco Security Awareness

For your review!

Email: Click with Caution
How to protect against phishing, fraud, and other scams

- Download:
  http://cs.co/email_ClickWithCaution

"52% of breaches featured hacking, 28% involved malware and 32-33% included phishing or social engineering, respectively."

- Verizon 2019 Data Breach Investigations Report

"Over 3.4 billion email scams or phishing emails are sent every day. This adds up to one trillion email scams per year"

- Security Magazine (June 11, 2019)

Phishing tips

Protect you and your business

- Security begins with YOU!
- It only takes one wrong click for cyber-criminals to access your company's data.

Phishing tips

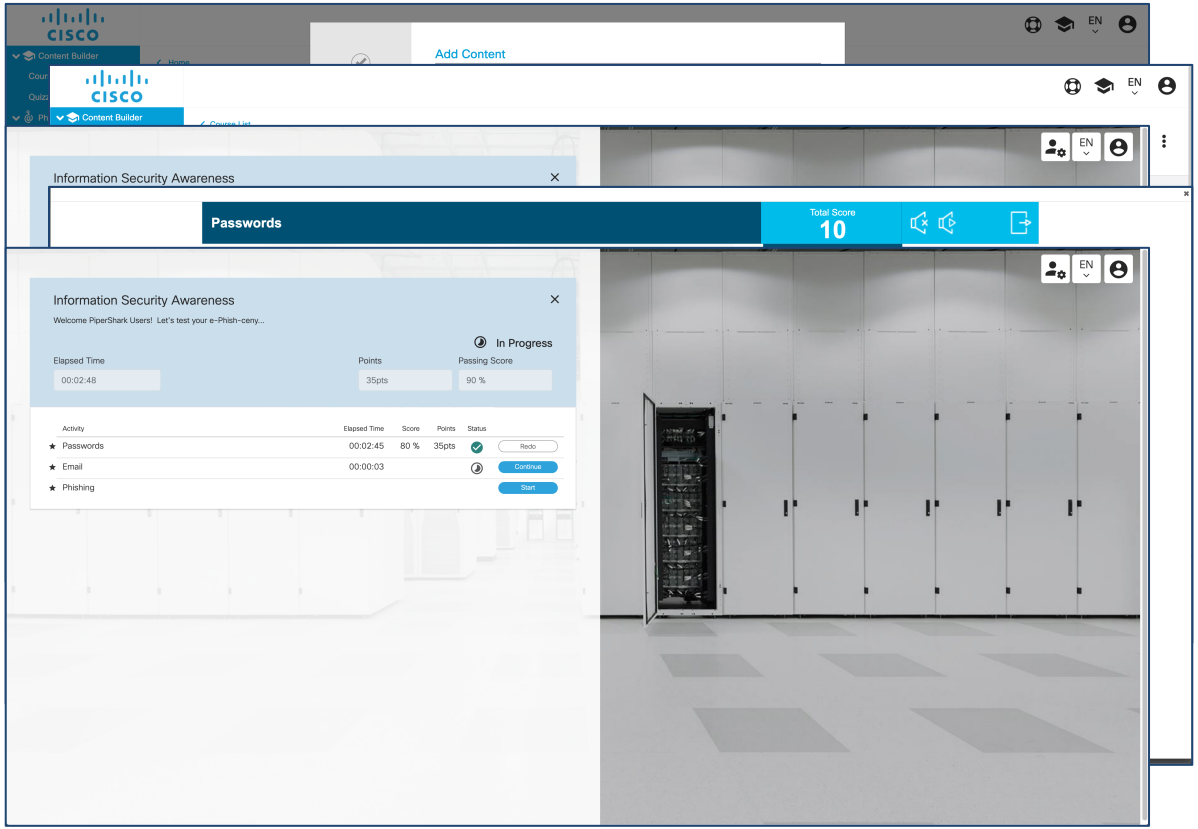
Protect you and your business

- Avoid strangers, check name and email address.
- Don’t rush, be suspicious of emails marked “urgent”.
- Notice mistakes in spelling and grammar.
- Beware of generic greetings, “dear sir/ma’am”.
- Don’t be lured by incredible “deals”.
- Hover over the link before you click to ensure it has a secure URL (https://).
- Never give out personal or financial information based on an email request.
- Don’t trust links or attachments in unsolicited emails.

Cisco Security Awareness

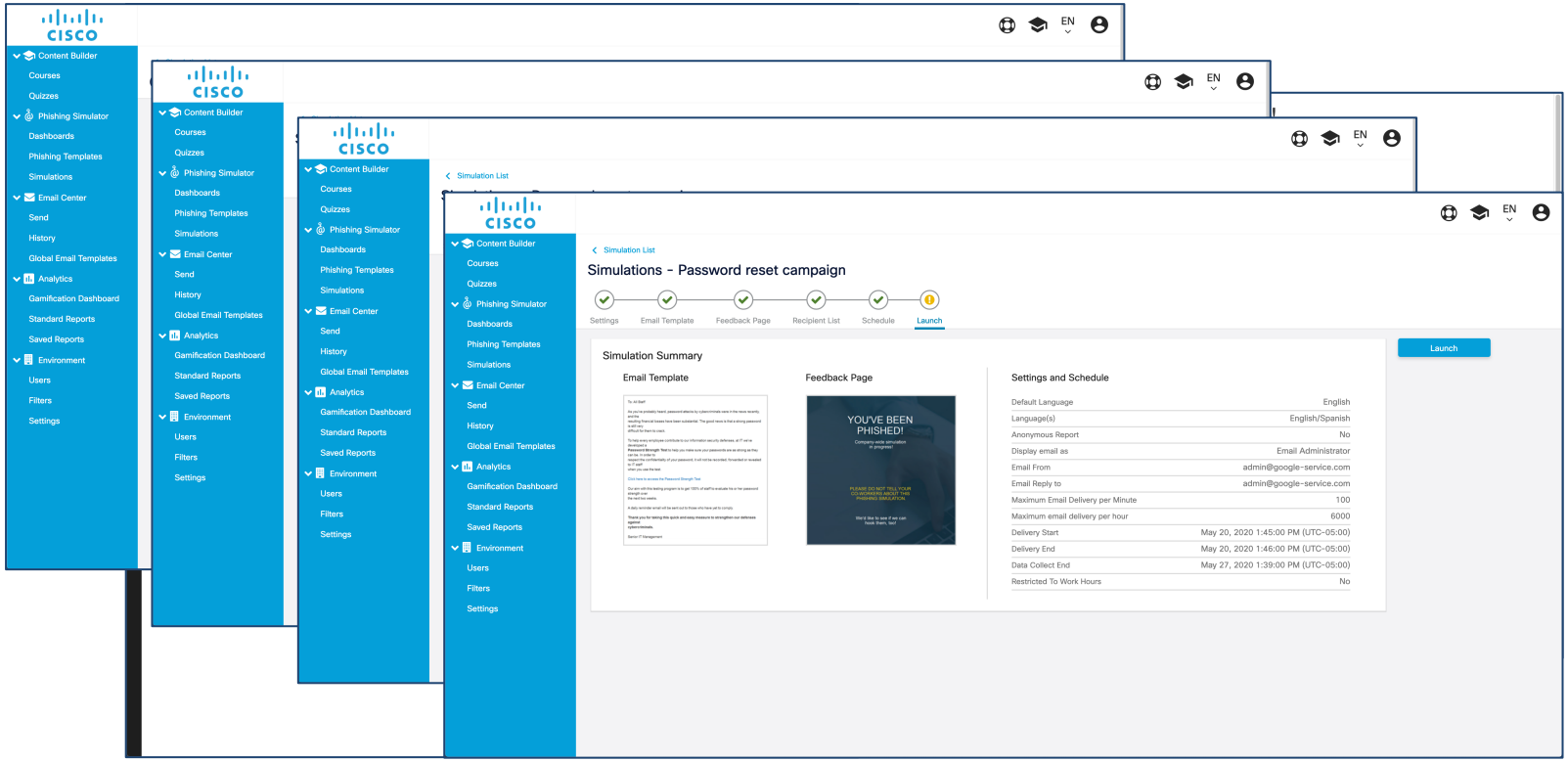
Stand-alone tool to help you educate end-users

- Providing flexibility and support to effectively deploy phishing simulations, awareness training, or both, and measure and report results.
- Empowering security operations teams with the ability to focus on real time threats and not end user mitigation.
- Security training providing the education that helps employees to work smarter and safer.



Cisco Security Awareness

Create your own phishing simulations



Cisco Security Awareness

- High-quality content is central to any security awareness program and a pre-requisite to provide a training experience that is fun, compelling and relevant.
- Our content is developed by a team of experts using a proven approach and methodology for adult learning that ensures the highest degree of engagement.
- Your users will learn about cyber security in a way that expands user knowledge and increases their affinity for your organization to help protect it.

Coming Soon!

CSA will have a **pre-built trial kit**, pre-built with phishing simulation templates for easy launch! Keep eye on Cisco.com for more details!

Cisco Security Awareness

Content

- 150+ learning modules
- Micro and nano learning
- Course builder
- Customization of content available
- Role based
- High degree of interaction
- Gamification

Simulation

- Simulation of real threats
- Integrated with training content
- Just in time feedback

Multilingual

- 40+ languages
- Narration + text
- Further customization available

Communication/ Reinforcement

- Internal campaign promotion
- Videos, posters, newsletters

Consultation

- CISO coaching
- Deploy, measure, and report
- Customer success program

Closing

Reviewing our session...

- High-level overview of Cisco Email Security
  - Mail flow & email pipeline
  - Common acronyms
  - A typical message
- Discussed utilizing SPF, DKIM, DMARC on Cisco Email Security
- Where Cisco Advanced Phishing Protection fits in
- How Cisco Domain Protection helps with SPF, DKIM, DMARC
- Talked about what Cisco is doing today for phishing efficacy
- Finished off our session with a look at Cisco Security Awareness

Cisco Email Security (Suite)

Email Security

- Email Security Appliance (ESA)
- Cloud Email Security (CES)
- Security Management Appliance (SMA)

Cisco Registered Envelope Service (CRES)

- Email Security Plug-in & Add-in

Advanced Phishing Protection (APP)

Domain Protection (DMP)

Cisco Security Awareness (CSA)

Cisco Mailbox Defense (CMD)

For more information:
https://cisco.com/go/emailsecurity

Thank you

Possibilities

#CiscoLive