
cisco
You make possible

Fixing Email!

Cisco Email Security Advanced Troubleshooting

Hrvoje (Harry) Dogan, SEM SecOps APJC

BRKSEC-3265

Barcelona | January 27-31, 2020

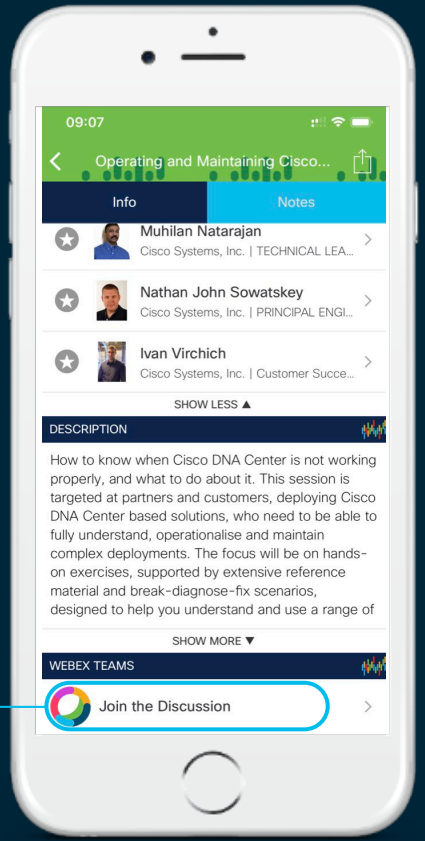
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Agenda

- Introduction
- Email Pipeline And General Precautions
- Reading the `mail_logs`
- Injection Troubleshooting And Mitigation
- Work Queue Troubleshooting And Mitigation
- Delivery Troubleshooting And Mitigation
- Network Stack Troubleshooting And Mitigation
- Email Authentication Troubleshooting And Mitigation
- Q & A

Session Abstract

Even though SMTP claims to be Simple, over its multi-decade history it consistently grew more and more complex.

This Advanced session will go deep in the nooks and crannies of the protocol itself, and Cisco's Email Security products – Appliance and CES – and focus on fixing common (and less common) issues showing up in real life scenarios.

It is an advanced-level technical session, and attendees should be familiar with email architectures, SMTP, DNS and basic networking and routing on the Internet.

Your Speaker

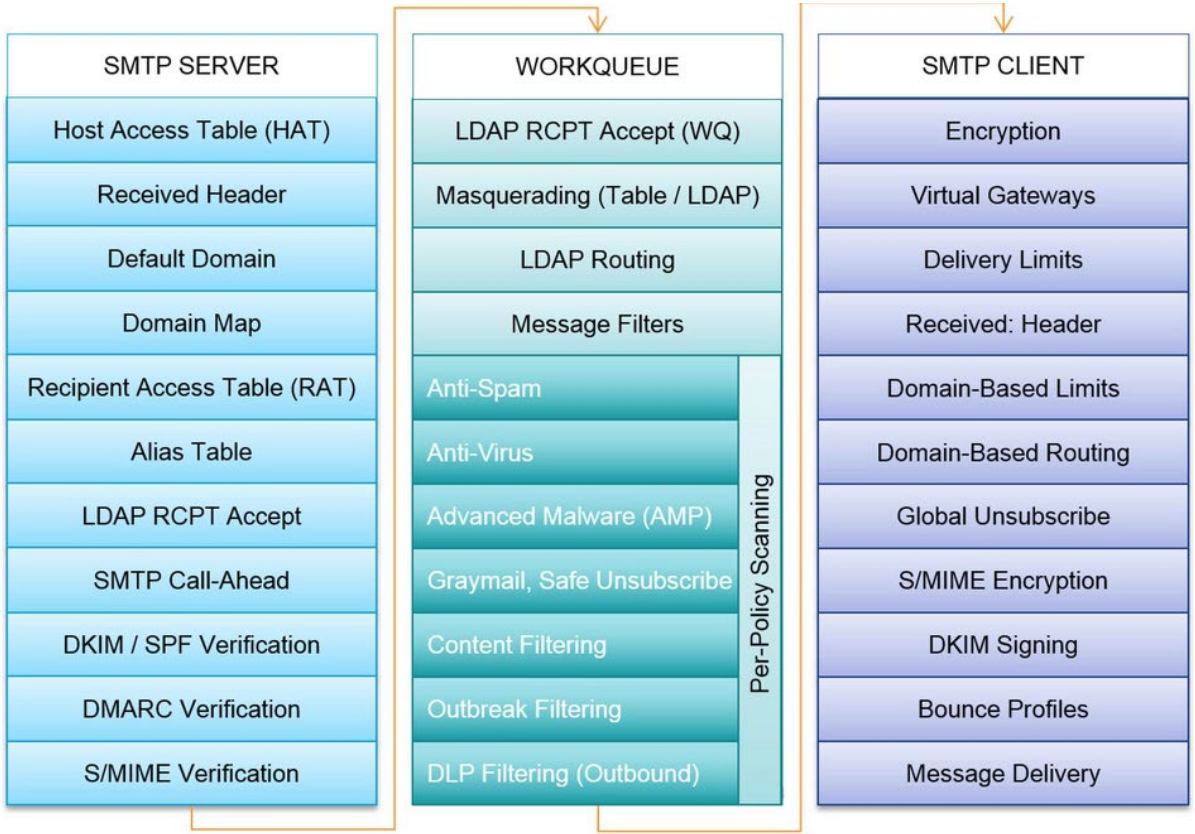
HRVOJE (HARRY) DOGAN

- Ex-IronPorter, Cisconian since 2007
- Cisco Live Distinguished Speaker
- Ex CSE, Ex SSA, Ex TME
- Originally Croatian, now in Singapore
- (Wild?) animal-crazy
- Sailor, Diver, Climber…
- Pawrent of 3 cats & 2 rabbits

Why Do We Need This?

- SMTP is old
- SMTP is broken
- ESA is old too
  - but not broken
- People think email is easy
  - It isn't
- In general, there's very little email hygiene on the Internet
- Fortunately, AsyncOS equips you with some great tools when things go south!

Email Processing Pipeline



Taking Care of Your Email Gateway Infrastructure

- Keep your time in sync
- Make sure your DNS is done right:
  - Use reliable, always-on DNS servers
  - All hostnames should resolve
  - All IPs should reverse-resolve
  - Hostname and IP resolution should match
- If you publish SPF, DMARC, DANE… make sure it's correct and complete!
- Be careful about IP Interface hostnames

Network Interfaces and IP Addresses

Add IP Interface...

Name	IP Address	Hostname
Data 1	68.232.150.244/24	esa1.hc252-80.c3s2.iphmx.com

Into The Nitty-Gritty

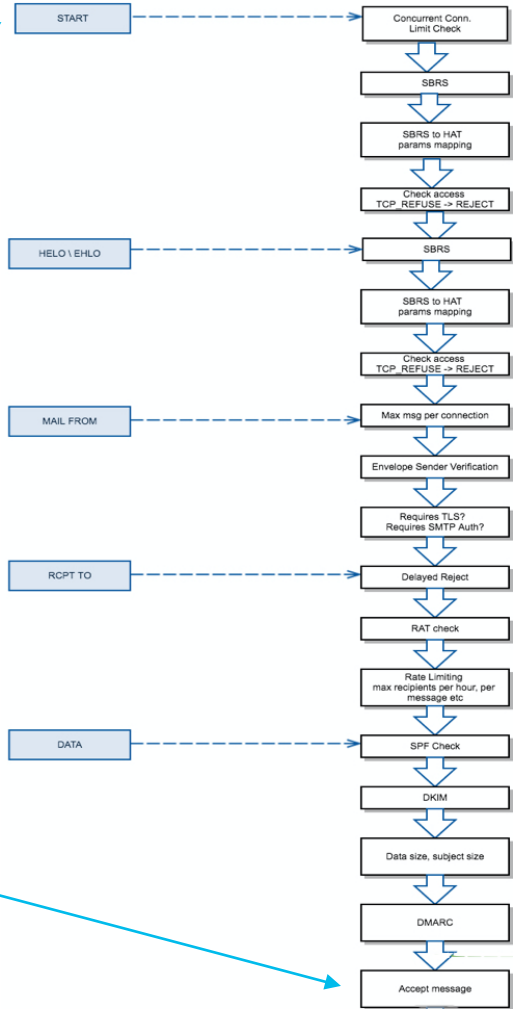
Reading the `mail_logs`

```
$ telnet mx2.hc252-80.c3s2.iphmx.com 25
Trying 68.232.150.244...
Connected to mx2.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
220 esa1.hc252-80.c3s2.iphmx.com ESMTP
EHLO tecsec-2310.cat
250-esa1.hc252-80.c3s2.iphmx.com
250-8BITMIME
250-SIZE 104857600
250 STARTTLS
MAIL FROM:<hdogan@tecsec-2310.cat>
250 sender <hdogan@tecsec-2310.cat> ok
RCPT TO:<hrdogan@cisco.com>
250 recipient <hrdogan@cisco.com> ok
DATA
354 go ahead
From: Hrvoje Dogan <hdogan@tecsec-2310.cat>
Subject: Test Email
Hello, world!
.
250 ok:  Message 409544 accepted
quit
221 esa1.hc252-80.c3s2.iphmx.com
Connection closed by foreign host.
```

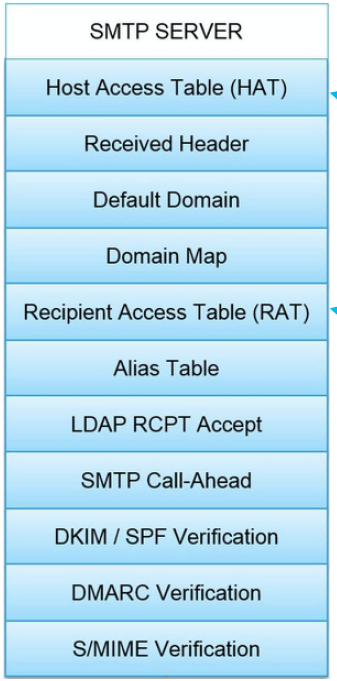
```
Fri Jan  3 13:17:16 2020 Info: New SMTP ICID 2309644 interface Data 1
(68.232.150.244) address 178.162.218.204 reverse dns host unknown verified no
Fri Jan  3 13:17:16 2020 Info: ICID 2309644 RELAY SG RELAYLIST match 178.162.218.204
SBRS +2.8 country Germany

Fri Jan  3 13:17:35 2020 Info: Start MID 409544 ICID 2309644
Fri Jan  3 13:17:35 2020 Info: MID 409544 ICID 2309644 From: hdogan@tecsec-2310.cat

Fri Jan  3 13:17:40 2020 Info: MID 409544 ICID 2309644 RID 0 To: hrdogan@cisco.com

Fri Jan  3 13:17:49 2020 Info: MID 409544 Message-ID '<5f1891$cfu8@esa1.hc252-
80.c3s2.iphmx.com>'
Fri Jan  3 13:17:49 2020 Info: MID 409544 Subject 'Test Email'
Fri Jan  3 13:17:49 2020 Info: MID 409544 SDR: Tracker Header :
4LyFTtbCbrs6GgtxRCpX9tvTj5AA0UC9PT7fZ099I
Fri Jan  3 13:17:49 2020 Info: MID 409544 ready 224 bytes from hdogan@tecsec-
2310.cat
Fri Jan  3 13:17:50 2020 Info: ICID 2309644 close
```

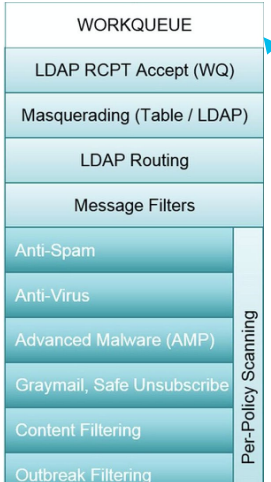
Reading the mail_logs

```
$ telnet mx2.hc252-80.c3s2.iphmx.com 25
Trying 68.232.150.244...
Connected to mx2.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
220 esa1.hc252-80.c3s2.iphmx.com ESMTP
EHLO tecsec-2310.cat
250-esa1.hc252-80.c3s2.iphmx.com
250-8BITMIME
250-SIZE 104857600
250 STARTTLS
MAIL FROM:<hdogan@tecsec-2310.cat>
250 sender <hdogan@tecsec-2310.cat> ok
RCPT TO:<hrdogan@cisco.com>
250 recipient <hrdogan@cisco.com> ok
DATA
354 go ahead
From: Hrvoje Dogan <hdogan@tecsec-2310.cat>
Subject: Test Email
Hello, world!
.
250 ok:  Message 409544 accepted
quit
221 esa1.hc252-80.c3s2.iphmx.com
Connection closed by foreign host.
```



Reading the `mail_logs`

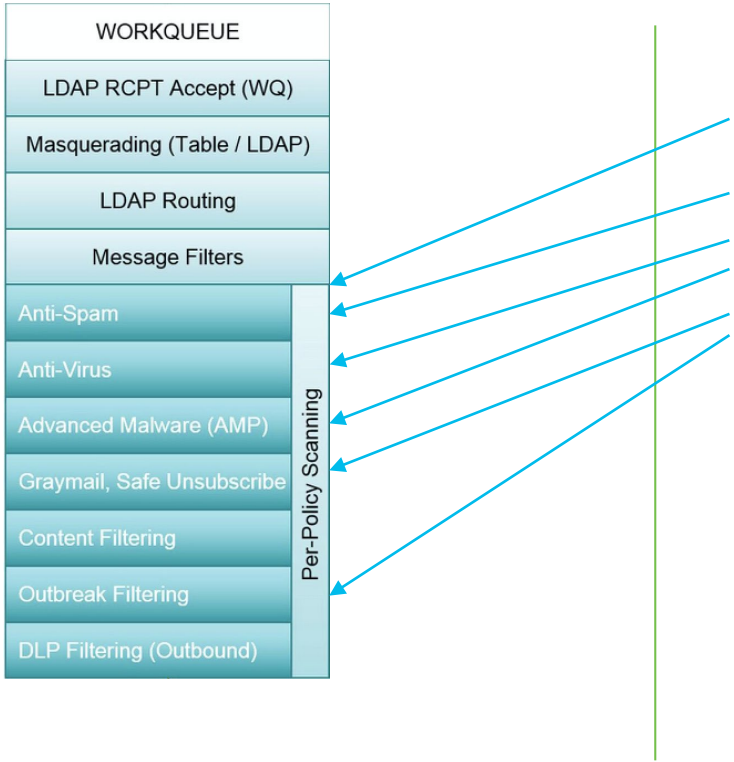





```
Fri Jan  3 13:17:16 2020 Info: New SMTP ICID 2309644 interface Data 1 (68.232.150.244)
address 178.162.218.204 reverse dns host unknown verified no
Fri Jan  3 13:17:16 2020 Info: ICID 2309644 RELAY SG RELAYLIST match 178.162.218.204 SBRS
+2.8 country Germany
```

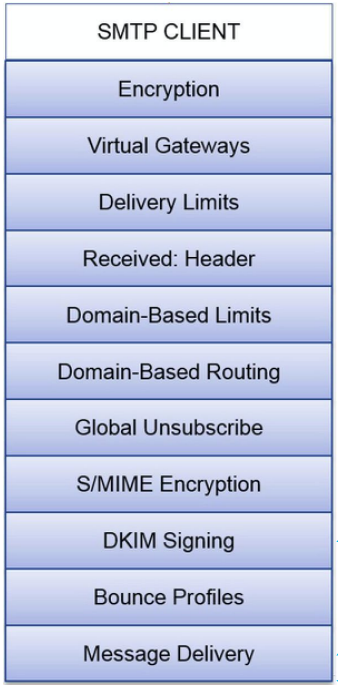
```
Fri Jan  3 13:17:35 2020 Info: Start MID 409544 ICID 2309644
Fri Jan  3 13:17:35 2020 Info: MID 409544 ICID 2309644 From: hdogan@tecsec-2310.cat

Fri Jan  3 13:17:40 2020 Info: MID 409544 ICID 2309644 RID 0 To: hrdogan@cisco.com

Fri Jan  3 13:17:49 2020 Info: MID 409544 Message-ID '<5f1891$cfu8@esa1.hc252-
80.c3s2.iphmx.com>'
Fri Jan  3 13:17:49 2020 Info: MID 409544 Subject 'Test Email'
Fri Jan  3 13:17:49 2020 Info: MID 409544 SDR: Tracker Header :
4LyFTtbCbrs6GgtxRCpX9tvTj5AA0UC9PT7fZ099I
Fri Jan  3 13:17:49 2020 Info: MID 409544 ready 224 bytes from hdogan@tecsec-2310.cat

Fri Jan  3 13:17:50 2020 Info: ICID 2309644 close
```

Reading the `mail_logs`



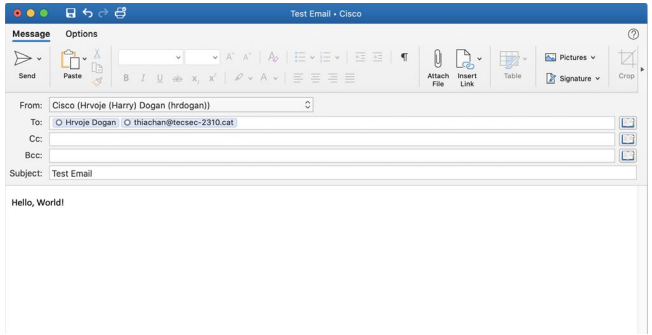

```
Sat Jan  4 14:53:29 2020 Info: MID 409783 ready 224 bytes from <hdogan@tecsec-2310.cat>
Sat Jan  4 14:53:29 2020 Info: MID 409783 matched all recipients for per-recipient policy
tecsec-2310 in the outbound table
Sat Jan  4 14:53:29 2020 Info: MID 409783 interim verdict using engine: CASE spam negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 using engine: CASE spam negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 interim AV verdict using Sophos CLEAN
Sat Jan  4 14:53:29 2020 Info: MID 409783 antivirus negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 AMP file reputation verdict : SKIPPED (no
attachment in message)
Sat Jan  4 14:53:29 2020 Info: MID 409783 using engine: GRAYMAIL negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 Outbreak Filters: verdict negative
```

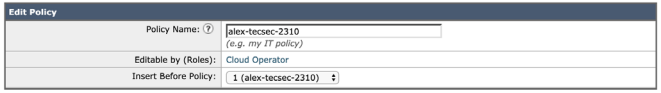
Reading the `mail_logs`

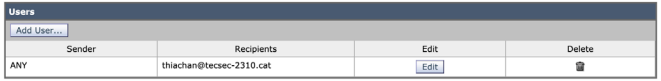



```
Sat Jan  4 14:53:29 2020 Info: MID 409783 ready 224 bytes from <hdogan@tecsec-2310.cat>
Sat Jan  4 14:53:29 2020 Info: MID 409783 matched all recipients for per-recipient policy
tecsec-2310 in the outbound table
Sat Jan  4 14:53:29 2020 Info: MID 409783 interim verdict using engine: CASE spam negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 using engine: CASE spam negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 interim AV verdict using Sophos CLEAN
Sat Jan  4 14:53:29 2020 Info: MID 409783 antivirus negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 AMP file reputation verdict : SKIPPED (no
attachment in message)
Sat Jan  4 14:53:29 2020 Info: MID 409783 using engine: GRAYMAIL negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 Outbreak Filters: verdict negative
Sat Jan  4 14:53:29 2020 Info: MID 409783 DomainKeys: cannot sign - no profile matches
hdogan@tecsec-2310.cat
Sat Jan  4 14:53:29 2020 Info: MID 409783 DKIM: cannot sign - no profile matches
hdogan@tecsec-2310.cat
Sat Jan  4 14:53:29 2020 Info: MID 409783 queued for delivery
Sat Jan  4 14:53:30 2020 Info: New SMTP DCID 412552 interface 68.232.150.244 address
173.37.147.230 port 25
Sat Jan  4 14:53:30 2020 Info: DCID 412552 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Sat Jan  4 14:53:30 2020 Info: Delivery start DCID 412552 MID 409783 to RID [0]
Sat Jan  4 14:53:32 2020 Info: ICID 2311957 close
Sat Jan  4 14:53:33 2020 Info: Message done DCID 412552 MID 409783 to RID [0]
Sat Jan  4 14:53:33 2020 Info: MID 409783 RID [0] Response 'ok:  Message 207685440
accepted'
Sat Jan  4 14:53:33 2020 Info: Message finished MID 409783 done
```

Reading the `mail_logs`: Splintering








```
Sat Jan  4 15:21:19 2020 Info: New SMTP ICID 2289881 interface Data 1 (68.232.151.78) address
173.37.86.77 reverse dns host rcdn-iport-6.cisco.com verified yes
Sat Jan  4 15:21:19 2020 Info: ICID 2289881 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0] SBRS
3.5 country United States
Sat Jan  4 15:21:20 2020 Info: ICID 2289881 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Sat Jan  4 15:21:20 2020 Info: Start MID 385012 ICID 2289881
Sat Jan  4 15:21:20 2020 Info: MID 385012 ICID 2289881 From: <hrdogan@cisco.com>
Sat Jan  4 15:21:20 2020 Info: MID 385012 ICID 2289881 RID 0 To: <thiachan@tecsec-2310.cat>
Sat Jan  4 15:21:20 2020 Info: MID 385012 ICID 2289881 RID 1 To: <hdogan@tecsec-2310.cat>
Sat Jan  4 15:21:20 2020 Info: MID 385012 SPF: helo identity postmaster@rcdn-iport-6.cisco.com
Pass (v=spf1)
Sat Jan  4 15:21:20 2020 Info: MID 385012 SPF: mailfrom identity hrdogan@cisco.com Pass
(v=spf1)
Sat Jan  4 15:21:21 2020 Info: MID 385012 SPF: pra identity hrdogan@cisco.com None headers
from
Sat Jan  4 15:21:21 2020 Info: MID 385012 DKIM: pass signature verified (d=cisco.com s=iport
i=@cisco.com)
Sat Jan  4 15:21:21 2020 Info: MID 385012 DMARC: Message from domain cisco.com, DMARC pass
(SPF aligned True, DKIM aligned True)
Sat Jan  4 15:21:21 2020 Info: MID 385012 DMARC: Verification passed
Sat Jan  4 15:21:21 2020 Info: MID 385012 Message-ID '<59B847A1-4946-471E-9E0C-
52808D29DA4E@cisco.com>'
Sat Jan  4 15:21:21 2020 Info: MID 385012 Subject 'Test Email'
Sat Jan  4 15:21:21 2020 Info: MID 385012 ready 7710 bytes from <hrdogan@cisco.com>
Sat Jan  4 15:21:21 2020 Info: MID 385012 was split creating MID 385013 due to a per-recipient
policy tecsec-2310 in the inbound table
Sat Jan  4 15:21:21 2020 Info: MID 385013 ICID 0 From: <hrdogan@cisco.com>
Sat Jan  4 15:21:21 2020 Info: MID 385013 ICID 0 RID 0 To: <thiachan@tecsec-2310.cat>
Sat Jan  4 15:21:21 2020 Info: MID 385012 was split creating MID 385014 due to a per-recipient
policy DEFAULT in the inbound table
Sat Jan  4 15:21:21 2020 Info: MID 385014 ICID 0 From: <hrdogan@cisco.com>
Sat Jan  4 15:21:21 2020 Info: MID 385014 ICID 0 RID 0 To: <hdogan@tecsec-2310.cat>
Sat Jan  4 15:21:21 2020 Info: Message finished MID 385012 done
```

Reading the `mail_logs`: Splintering

```
Sat Jan  4 15:21:21 2020 Info: MID 385013 ICID 0 From:
<hrdogan@cisco.com>
Sat Jan  4 15:21:21 2020 Info: MID 385013 ICID 0 RID 0 To:
<thiachan@tecsec-2310.cat>
Sat Jan  4 15:21:22 2020 Info: MID 385013 interim verdict using engine:
CASE spam negative
Sat Jan  4 15:21:22 2020 Info: MID 385013 using engine: CASE spam
negative
Sat Jan  4 15:21:22 2020 Info: MID 385013 interim AV verdict using
McAfee CLEAN
Sat Jan  4 15:21:22 2020 Info: MID 385013 interim AV verdict using
Sophos CLEAN
Sat Jan  4 15:21:22 2020 Info: MID 385013 antivirus negative
Sat Jan  4 15:21:22 2020 Info: MID 385013 AMP file reputation verdict :
SKIPPED (no attachment in message)
Sat Jan  4 15:21:22 2020 Info: MID 385013 using engine: GRAYMAIL
negative
Sat Jan  4 15:21:22 2020 Info: MID 385013 Outbreak Filters: verdict
negative
Sat Jan  4 15:21:22 2020 Info: MID 385013 queued for delivery
```

```
Sat Jan  4 15:21:21 2020 Info: MID 385014 ICID 0 From:
<hrdogan@cisco.com>
Sat Jan  4 15:21:21 2020 Info: MID 385014 ICID 0 RID 0 To:
<hdogan@tecsec-2310.cat>
Sat Jan  4 15:21:22 2020 Info: MID 385014 using engine: CASE using
cached verdict
Sat Jan  4 15:21:22 2020 Info: MID 385014 interim verdict using engine:
CASE spam negative
Sat Jan  4 15:21:22 2020 Info: MID 385014 using engine: CASE spam
negative
Sat Jan  4 15:21:22 2020 Info: MID 385014 interim AV verdict using
McAfee CLEAN
Sat Jan  4 15:21:22 2020 Info: MID 385014 interim AV verdict using
Sophos CLEAN
Sat Jan  4 15:21:22 2020 Info: MID 385014 antivirus negative
Sat Jan  4 15:21:22 2020 Info: MID 385014 AMP file reputation verdict :
SKIPPED (no attachment in message)
Sat Jan  4 15:21:22 2020 Info: MID 385014 using engine: GRAYMAIL
negative
Sat Jan  4 15:21:22 2020 Info: MID 385014 Outbreak Filters: verdict
negative
Sat Jan  4 15:21:22 2020 Info: MID 385014 queued for delivery
```

Reading the `mail_logs`: Splintering

```
Sat Jan  4 15:21:22 2020 Info: New SMTP DCID 419048 interface 68.232.151.78 address 178.162.218.204 port 25
Sat Jan  4 15:21:22 2020 Info: DCID 419048 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
```

```
Sat Jan  4 15:21:22 2020 Info: Delivery start DCID 419048 MID 385013 to
RID [0]
Sat Jan  4 15:21:22 2020 Info: Message done DCID 419048 MID 385013 to
RID [0]
Sat Jan  4 15:21:22 2020 Info: MID 385013 RID [0] Response '2.0.0 Ok:
queued as BBBCDB2012C3'
Sat Jan  4 15:21:22 2020 Info: Message finished MID 385013 done
```

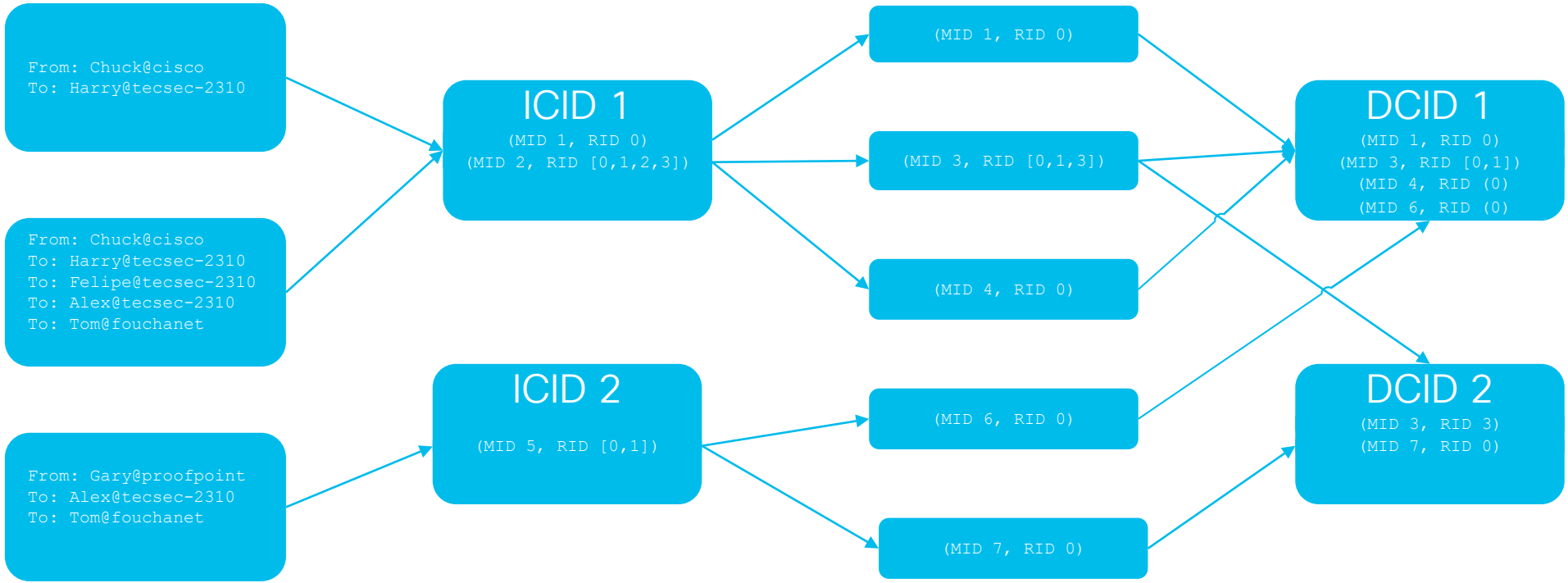
```
Sat Jan  4 15:21:22 2020 Info: Delivery start DCID 419048 MID 385014 to
RID [0]
Sat Jan  4 15:21:22 2020 Info: Message done DCID 419048 MID 385014 to
RID [0]
Sat Jan  4 15:21:22 2020 Info: MID 385014 RID [0] Response '2.0.0 Ok:
queued as DFCBEB2012C6'
Sat Jan  4 15:21:22 2020 Info: Message finished MID 385014 done
```

```
Sat Jan  4 15:21:26 2020 Info: ICID 2289881 close
Sat Jan  4 15:21:27 2020 Info: DCID 419048 close
```

Untangling the Identifiers

- `ICID`: Incoming Connection ID
  - A single connection can inject hundreds of messages to dozens of domains
- `MID`: Message ID (internal to ESA, not to be confused with `Message-ID` header)
  - Each message on injection has a unique `MID`
- `RID`: Recipient ID, unique per message, ordered list starting with `[0]`
  - Each set of (`MID,RID[0..x]`) that matches a Mail Policy will spawn a new `MID`
  - Delivery destination determined separately for each (`MID, RID`) pair
- `DCID`: Delivery Connection ID
  - A connection established to a delivery host. Single DCID can be used to deliver multiple unrelated messages to the same destination
  - A single message of multiple recipients may be delivered over multiple DCIDs

Untangling the Identifiers



Injection Troubleshooting

Let's Start At the Very Beginning

```
Sat Jan  4 15:21:19 2020 Info: New SMTP ICID 2289881 interface Data 1 (68.232.151.78)
address 173.37.86.77 reverse dns host rcdn-iport-6.cisco.com verified yes
Sat Jan  4 15:21:19 2020 Info: ICID 2289881 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0] SBRS 3.5 country
United States
```

- Most Injection issues can be attributed to incorrectly configured Sender Group match

```
Sat Jan  4 15:21:20 2020 Info: ICID 2289881 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-
SHA384
```

- Next: Check that the connection can be fully established.

Closed Connections

```
$ telnet mx2.hc252-80.c3s2.iphmx.com 25
Trying 68.232.151.78...
Connected to mx2.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
220 esa2.hc252-80.c3s2.iphmx.com ESMTP
quit
221 esa2.hc252-80.c3s2.iphmx.com
Connection closed by foreign host.
```

```
Mon Jan  6 12:36:47 2020 Info: New SMTP ICID 2293474
interface Data 1 (68.232.151.78) address 178.162.218.204
reverse dns host unknown verified no
Mon Jan  6 12:36:47 2020 Info: ICID 2293474 RELAY SG
RELAYLIST match 178.162.218.204 SBRS None country Germany
Mon Jan  6 12:36:53 2020 Info: ICID 2293474 close
```

```
$ telnet mx2.hc252-80.c3s2.iphmx.com 25
Trying 68.232.151.78...
Connected to mx2.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
220 esa2.hc252-80.c3s2.iphmx.com ESMTP
^]
telnet> q
Connection closed.
```

```
Mon Jan  6 12:38:02 2020 Info: New SMTP ICID 2293477
interface Data 1 (68.232.151.78) address 178.162.218.204
reverse dns host unknown verified no
Mon Jan  6 12:38:02 2020 Info: ICID 2293477 RELAY SG
RELAYLIST match 178.162.218.204 SBRS None country Germany
Mon Jan  6 12:38:10 2020 Info: ICID 2293477 lost
Mon Jan  6 12:38:10 2020 Info: ICID 2293477 close
```

Timed Out Connections

```
$ telnet mx2.hc252-80.c3s2.iphmx.com 25
Trying 68.232.151.78...
Connected to mx2.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
220 esa2.hc252-80.c3s2.iphmx.com ESMTP
EHLO dir.hr
250-esa2.hc252-80.c3s2.iphmx.com
250-8BITMIME
250-SIZE 104857600
250 STARTTLS
421 Exceeded allowable connection time,
disconnecting.
Connection closed by foreign host.
```

```
Mon Jan  6 12:39:31 2020 Info: New SMTP ICID 2293479
interface Data 1 (68.232.151.78) address 178.162.218.204
reverse dns host unknown verified no
Mon Jan  6 12:39:31 2020 Info: ICID 2293479 RELAY SG
RELAYLIST match 178.162.218.204 SBRS None country Germany
Mon Jan  6 12:44:31 2020 Info: ICID 2293479 disconnected
address 178.162.218.204, no messages injected within
timeout period
Mon Jan  6 12:44:31 2020 Info: ICID 2293479 close
```

Timed Out Connections

```
$ telnet mx2.hc252-80.c3s2.iphmx.com 25
Trying 68.232.151.78...
Connected to mx2.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
220 esa2.hc252-80.c3s2.iphmx.com ESMTP
EHLO dir.hr
250-esa2.hc252-80.c3s2.iphmx.com
250-8BITMIME
250-SIZE 104857600
250 STARTTLS
MAIL FROM:<hdogan@dir.hr>
250 sender <hdogan@dir.hr> ok
RCPT TO:<hrdogan@cisco.com>
250 recipient <hrdogan@cisco.com> ok
DATA
354 go ahead
Subject: Test to time out
Connection closed by foreign host.
```

```
Mon Jan  6 12:48:19 2020 Info: New SMTP ICID 2293490
interface Data 1 (68.232.151.78) address 178.162.218.204
reverse dns host unknown verified no
Mon Jan  6 12:48:19 2020 Info: ICID 2293490 RELAY SG
RELAYLIST match 178.162.218.204 SBRS None country Germany
Mon Jan  6 12:48:30 2020 Info: Start MID 385309 ICID
2293490
Mon Jan  6 12:48:30 2020 Info: MID 385309 ICID 2293490
From: <hdogan@dir.hr>
Mon Jan  6 12:48:40 2020 Info: MID 385309 ICID 2293490 RID
0 To: <hrdogan@cisco.com>
Mon Jan  6 12:53:49 2020 Info: ICID 2293490 lost
Mon Jan  6 12:53:49 2020 Info: ICID 2293490 close
```

… A Very Good Place To Start!

- Next, check your receiving rates

```
alln-inbound-a.cisco.com> rate 1

Type Ctrl-C to return to the main prompt.

Time     Connections Recipients          Recipients              Queue
            In   Out   Received    Delta  Completed    Delta     K-Used
16:48:55    21     3  224741542        0  213292502        0        101
16:48:56    22     3  224741550        8  213292505        3        658
16:48:57    22     3  224741554        4  213292507        2        602
16:48:58    22     3  224741556        2  213292510        3        606
16:48:59    17     2  224741558        2  213292511        1        613
16:49:00    20     1  224741562        4  213292519        8        139
16:49:01    22     4  224741565        3  213292524        5        104
16:49:02    23     4  224741572        7  213292527        3        113
```

- And connected hosts

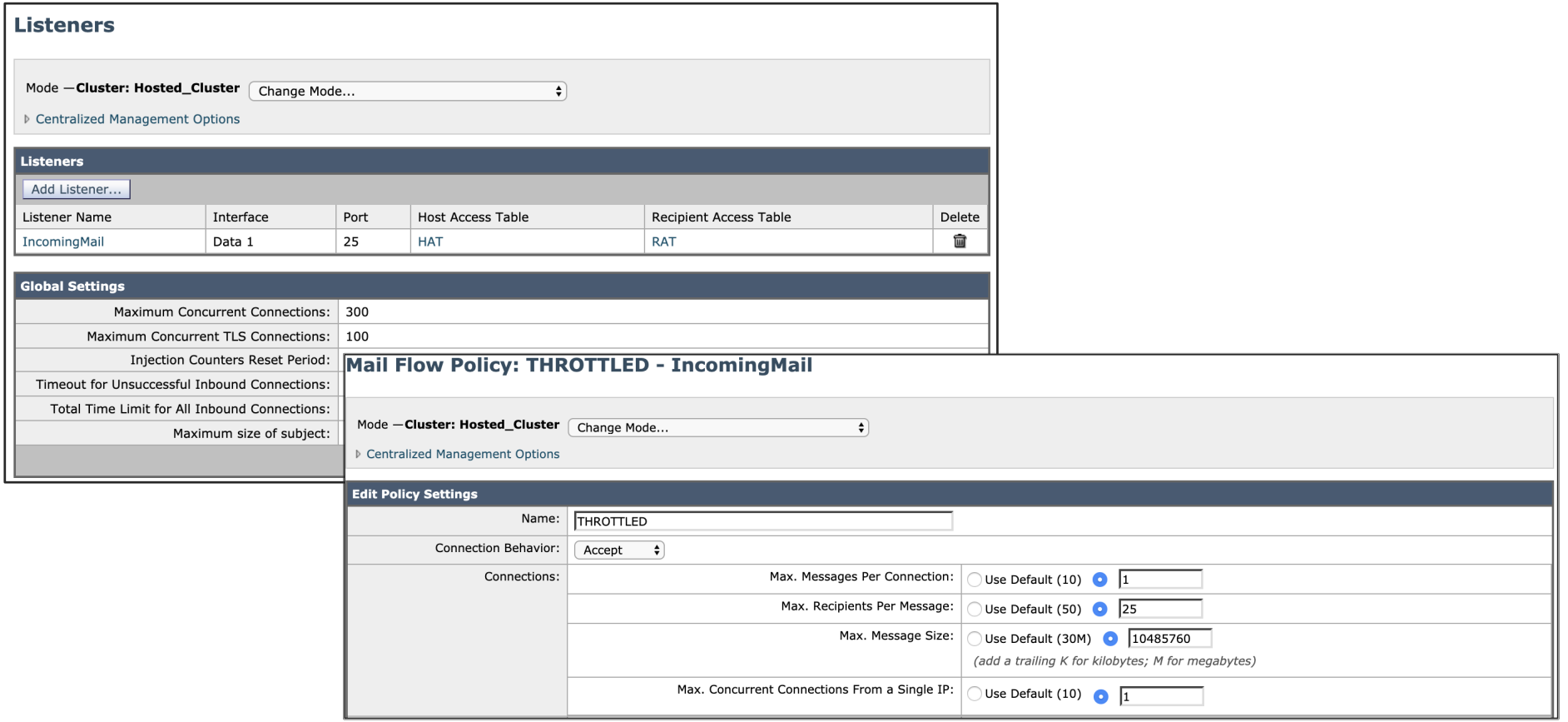
```
alln-inbound-a.cisco.com> topin

Status as of:                  Mon Jan 20 16:53:17 2020 GMT

#  Remote hostname            Remote IP addr.   Listener        Conn. In
1  162.248.201.16             162.248.201.16    listener01             2
2  192.168.115.42             192.168.115.42    listener01             2
3  a4-17.smtp-out.eu-west-1.a 54.240.4.17       listener01             2
4  m229-149.mailgun.net       159.135.229.149   listener01             1
5  168-128-66-48-eu7.mcp-serv 168.128.66.48     listener01             1
6  192.168.115.45             192.168.115.45    listener01             1
7  mail191.atl21.rsgsv.net    205.201.133.191   listener01             1
8  mail-ot1-x329.google.com   2607:f8b0:4864:20::329 listener01        1
9  mail-pf1-x431.google.com   2607:f8b0:4864:20::431 listener01        1
10 mail-vs1-xe2f.google.com   2607:f8b0:4864:20::e2f listener01        1
```

Concurrency limits reached

```
$ telnet mx1.hc252-80.c3s2.iphmx.com 25
Trying 68.232.150.244...
Connected to mx1.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
220 esa1.hc252-80.c3s2.iphmx.com ESMTP


[Ctrl-A-C]


$ telnet mx1.hc252-80.c3s2.iphmx.com 25
Trying 68.232.150.244...
Connected to mx1.hc252-80.c3s2.iphmx.com.
Escape character is '^]'.
421 #4.4.5 Too many connections from your
host.
Connection closed by foreign host.
```

```
Tue Jan  7 16:58:56 2020 Info: New SMTP ICID 2318064 interface
Data 1 (68.232.150.244) address 193.198.212.57 reverse dns host
griffin.linux.hr verified yes
Tue Jan  7 16:58:56 2020 Info: ICID 2318064 ACCEPT SG
SUSPECTLIST match 193.198.212.57 SBRS None country Croatia
Tue Jan  7 16:59:11 2020 Info: New SMTP ICID 2318065 interface
Data 1 (68.232.150.244) address 193.198.212.57 reverse dns host
griffin.linux.hr verified yes
Tue Jan  7 16:59:11 2020 Info: ICID 2318065 ACCEPT SG
SUSPECTLIST match 193.198.212.57 SBRS None country Croatia
Tue Jan  7 16:59:11 2020 Warning: System limit reached:
connection limit for IP 193.198.212.57 on listener IncomingMail
ICID 2318065: max: 1
Tue Jan  7 16:59:11 2020 Info: ICID 2318065 Receiving Failed:
Connection limit exceeded
Tue Jan  7 16:59:11 2020 Info: ICID 2318065 close
```

All the ways to limit concurrency



All the ways to limit concurrency

```
(Cluster Hosted_Cluster)> listenerconfig
Currently configured listeners:
1. IncomingMail (on Data 1) SMTP TCP Port 25 Public

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
- CLUSTERSET - Set how listeners are configured in a cluster.
- CLUSTERSHOW - Display how listeners are configured in a
cluster.
[]> edit

Enter the name or number of the listener you wish to edit.
[]> 1

Name: IncomingMail
Type: Public
Interface: Data 1 TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 300 (TCP Queue: 50)
Domain Map: Disabled
TLS: Preferred
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead Profile: CES_SMTP
LDAP: Off
```

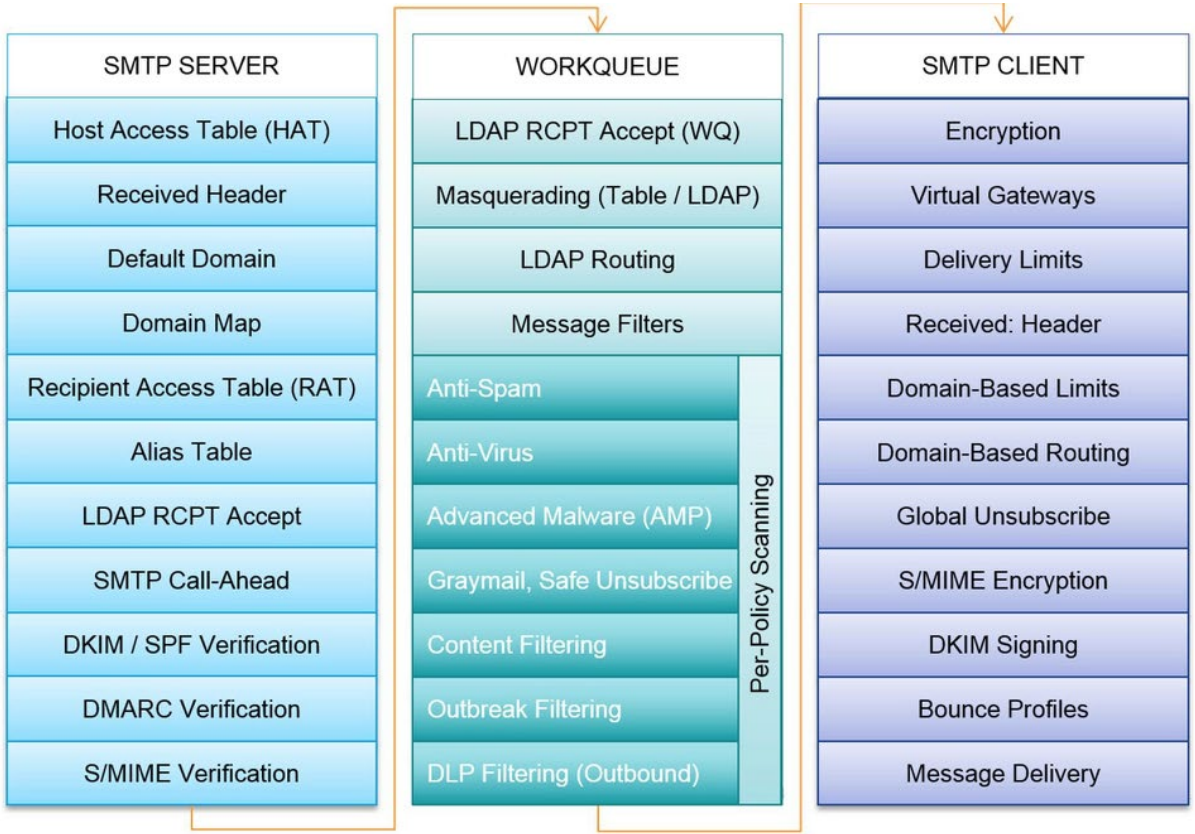
```
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- CALLAHEAD - Configure SMTP Call-Ahead settings for this listener.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected
on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> limits

Enter the maximum concurrent connections allowed for this listener.
[300]>
```

See What They See: Injection Debug Log

```
Fri Jan  3 13:17:16 2020 Info: 2309644 Sent to '178.162.218.204': '220 esa1.hc252-80.c3s2.iphmx.com ESMTP\r\n'
Fri Jan  3 13:17:29 2020 Info: 2309644 Rcvd from '178.162.218.204': 'EHLO tecsec-2310.cat\r\n'
Fri Jan  3 13:17:29 2020 Info: 2309644 Sent to '178.162.218.204': '250-esa1.hc252-80.c3s2.iphmx.com\r\n250-
8BITMIME\r\n250-SIZE 104857600\r\n250 STARTTLS\r\n'
Fri Jan  3 13:17:35 2020 Info: 2309644 Rcvd from '178.162.218.204': 'MAIL FROM:<hdogan@tecsec-2310.cat>\r\n'
Fri Jan  3 13:17:35 2020 Info: 2309644 Sent to '178.162.218.204': '250 sender <hdogan@tecsec-2310.cat> ok\r\n'
Fri Jan  3 13:17:40 2020 Info: 2309644 Rcvd from '178.162.218.204': 'RCPT TO:<hrdogan@cisco.com>\r\n'
Fri Jan  3 13:17:40 2020 Info: 2309644 Sent to '178.162.218.204': '250 recipient <hrdogan@cisco.com> ok\r\n'
Fri Jan  3 13:17:42 2020 Info: 2309644 Rcvd from '178.162.218.204': 'DATA\r\n'
Fri Jan  3 13:17:42 2020 Info: 2309644 Sent to '178.162.218.204': '354 go ahead\r\n'
Fri Jan  3 13:17:48 2020 Info: 2309644 Rcvd from '178.162.218.204': 'From: Hrvoje Dogan <hdogan@tecsec-2310.cat>\r\n'
Fri Jan  3 13:17:48 2020 Info: 2309644 Rcvd from '178.162.218.204': 'Subject: Test Email\r\n\r\nHello, world!\r\n'
Fri Jan  3 13:17:49 2020 Info: 2309644 Rcvd from '178.162.218.204': '.\r\n'
Fri Jan  3 13:17:49 2020 Info: 2309644 Sent to '178.162.218.204': '250 ok:  Message 409544 accepted\r\n'
Fri Jan  3 13:17:50 2020 Info: 2309644 Rcvd from '178.162.218.204': 'quit\r\n'
Fri Jan  3 13:17:50 2020 Info: 2309644 Sent to '178.162.218.204': '221 esa1.hc252-80.c3s2.iphmx.com\r\n'
```

Workqueue Troubleshooting

Email Processing Pipeline



Work Queue Processing

- First In – First Out
- A single broken message can pause the entire queue
- A single broken engine can pause the entire queue
- A single network error can pause the entire queue
- Paused Work Queue -> Resource Starvation -> System Crash

What to look for

- `rate`

```
alln-inbound-a.cisco.com> rate 1
Type Ctrl-C to return to the main prompt.

Time     Connections Recipients          Recipients              Queue
            In   Out   Received    Delta  Completed    Delta     K-Used
16:48:55    21     3  224741542        0  213292502        0        101
16:48:56    22     3  224741550        8  213292505        3        658
16:48:57    22     3  224741554        4  213292507        2        602
16:48:58    22     3  224741556        2  213292510        3        606
16:48:59    17     2  224741558        2  213292511        1        613
16:49:00    20     1  224741562        4  213292519        8        139
16:49:01    22     4  224741565        3  213292524        5        104
```

vs.

- `workqueue rate`

```
alln-iport-1.cisco.com> workqueue rate 1
Type Ctrl-C to return to the main prompt.

Time      Pending    In   Out
16:55:02        2     0     0
16:55:03        0    10    12
16:55:04        1     9     8
16:55:05        1    12    12
16:55:06        2     9     8
16:55:07        2    10    10
16:55:08        1     5     6
16:55:09        0     9    10
16:55:11        0    10    10
16:55:12        0    12    12
```

What to look for

- `status`

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> status
Enter "status detail" for more information.

Status as of:                  Wed Jan 08 11:22:34 2020 +06
Up since:                      Tue Jul 02 15:41:45 2019 +06 (189d 19h 40m 49s)
Last counter reset:            Never
System status:                 Work Queue Paused
Oldest Message:                22 weeks 4 days 16 hours 56 mins 2 secs
```

vs

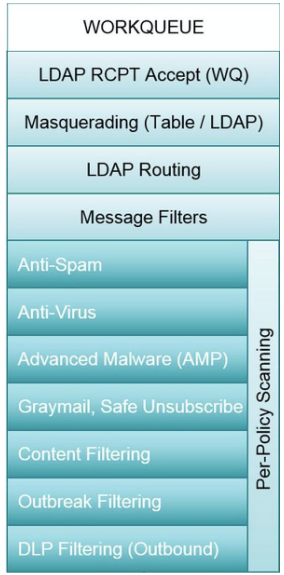
- `workqueue status`

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> workqueue status
Status as of:  Wed Jan 08 11:22:46 2020 +06
Status:        Paused by Antivirus
Messages:       37
```

What to look for

- Before looking at log files, use "`suspend`" or at least "`suspendlistener`"
  - This will stop overloading the machine with receiving (and delivering) messages
- Look for long delays in individual message processing sequence in mail_logs
- No indicators in logs for Message Filters or Content Filters
  - `log-entry()` action is your friend!
- Use individual engine logs for more detail

- OPEN A TAC CASE!!!



Let's Find the Needle In the Haystack!

```
Wed Jan  8 11:42:38 2020 Info: New SMTP ICID 2297344 interface Data
1 (68.232.151.78) address 173.37.86.77 reverse dns host rcdn-iport-
6.cisco.com verified yes
Wed Jan  8 11:42:38 2020 Info: ICID 2297344 ACCEPT SG UNKNOWNLIST
match sbrs[-1.0:10.0] SBRS 3.5 country United States
Wed Jan  8 11:42:39 2020 Info: ICID 2297344 TLS success protocol
TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Wed Jan  8 11:42:39 2020 Info: Start MID 385701 ICID 2297344
Wed Jan  8 11:42:39 2020 Info: MID 385701 ICID 2297344 From:
<hrdogan@cisco.com>
Wed Jan  8 11:42:39 2020 Info: MID 385701 ICID 2297344 RID 0 To:
<hdogan@tecsec-2310.cat>
Wed Jan  8 11:42:40 2020 Info: MID 385701 SPF: helo identity
postmaster@rcdn-iport-6.cisco.com Pass (v=spf1)
Wed Jan  8 11:42:40 2020 Info: MID 385701 SPF: mailfrom identity
hrdogan@cisco.com Pass (v=spf1)
Wed Jan  8 11:42:40 2020 Info: MID 385701 SPF: pra identity
hrdogan@cisco.com None headers from
Wed Jan  8 11:42:40 2020 Info: MID 385701 DKIM: pass signature
verified (d=cisco.com s=iport i=@cisco.com)
Wed Jan  8 11:42:40 2020 Info: MID 385701 DMARC: Message from domain
cisco.com, DMARC pass (SPF aligned True, DKIM aligned True)
Wed Jan  8 11:42:40 2020 Info: MID 385701 DMARC: Verification passed
Wed Jan  8 11:42:40 2020 Info: MID 385701 Message-ID '<C158ECAB-
0630-44CC-A4B5-037B1C914D4F@cisco.com>'
Wed Jan  8 11:42:40 2020 Info: MID 385701 Subject 'Test Email'
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Domains for which SDR
is requested: reverse DNS host: rcdn-iport-6.cisco.com, helo: rcdn-
iport-6.cisco.com, env-from: cisco.com, header-from: cisco.com,
reply-to: Not Present
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Consolidated Sender
Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 33
years 1 month 17 days for domain: rcdn-iport-6.cisco.com
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Tracker Header :
8+Hbn/f9F8RIo1kJf5jQ5AX91YtVY/
```

```
Wed Jan  8 11:42:40 2020 Info: MID 385701 ready 7425 bytes from
<hrdogan@cisco.com>
Wed Jan  8 11:42:46 2020 Info: ICID 2297344 close
Wed Jan  8 11:44:40 2020 Info: MID 385701 matched all recipients for
per-recipient policy DEFAULT in the inbound table
Wed Jan  8 11:44:42 2020 Info: MID 385701 interim verdict using
engine: CASE spam negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 using engine: CASE spam
negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 interim AV verdict using
McAfee CLEAN
Wed Jan  8 11:44:42 2020 Info: MID 385701 interim AV verdict using
Sophos CLEAN
Wed Jan  8 11:44:42 2020 Info: MID 385701 antivirus negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 AMP file reputation
verdict : SKIPPED (no attachment in message)
Wed Jan  8 11:44:42 2020 Info: MID 385701 using engine: GRAYMAIL
negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 Outbreak Filters: verdict
negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 queued for delivery
Wed Jan  8 11:44:42 2020 Info: New SMTP DCID 419670 interface
68.232.151.78 address 178.162.218.204 port 25
Wed Jan  8 11:44:42 2020 Info: DCID 419670 TLS success protocol
TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Wed Jan  8 11:44:42 2020 Info: Delivery start DCID 419670 MID 385701
to RID [0]
Wed Jan  8 11:44:42 2020 Info: Message done DCID 419670 MID 385701
to RID [0]
Wed Jan  8 11:44:42 2020 Info: MID 385701 RID [0] Response '2.0.0
Ok: queued as BD478B200576'
Wed Jan  8 11:44:42 2020 Info: Message finished MID 385701 done
Wed Jan  8 11:44:47 2020 Info: DCID 419670 close
```

Let's Find the Needle In the Haystack!

```
Wed Jan  8 11:42:38 2020 Info: New SMTP ICID 2297344 interface Data
1 (68.232.151.78) address 173.37.86.77 reverse dns host rcdn-iport-
6.cisco.com verified yes
Wed Jan  8 11:42:38 2020 Info: ICID 2297344 ACCEPT SG UNKNOWNLIST
match sbrs[-1.0:10.0] SBRS 3.5 country United States
Wed Jan  8 11:42:39 2020 Info: ICID 2297344 TLS success protocol
TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Wed Jan  8 11:42:39 2020 Info: Start MID 385701 ICID 2297344
Wed Jan  8 11:42:39 2020 Info: MID 385701 ICID 2297344 From:
<hrdogan@cisco.com>
Wed Jan  8 11:42:39 2020 Info: MID 385701 ICID 2297344 RID 0 To:
<hdogan@tecsec-2310.cat>
Wed Jan  8 11:42:40 2020 Info: MID 385701 SPF: helo identity
postmaster@rcdn-iport-6.cisco.com Pass (v=spf1)
Wed Jan  8 11:42:40 2020 Info: MID 385701 SPF: mailfrom identity
hrdogan@cisco.com Pass (v=spf1)
Wed Jan  8 11:42:40 2020 Info: MID 385701 SPF: pra identity
hrdogan@cisco.com None headers from
Wed Jan  8 11:42:40 2020 Info: MID 385701 DKIM: pass signature
verified (d=cisco.com s=iport i=@cisco.com)
Wed Jan  8 11:42:40 2020 Info: MID 385701 DMARC: Message from domain
cisco.com, DMARC pass (SPF aligned True, DKIM aligned True)
Wed Jan  8 11:42:40 2020 Info: MID 385701 DMARC: Verification passed
Wed Jan  8 11:42:40 2020 Info: MID 385701 Message-ID '<C158ECAB-
0630-44CC-A4B5-037B1C914D4F@cisco.com>'
Wed Jan  8 11:42:40 2020 Info: MID 385701 Subject 'Test Email'
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Domains for which SDR
is requested: reverse DNS host: rcdn-iport-6.cisco.com, helo: rcdn-
iport-6.cisco.com, env-from: cisco.com, header-from: cisco.com,
reply-to: Not Present
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Consolidated Sender
Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 33
years 1 month 17 days for domain: rcdn-iport-6.cisco.com
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Tracker Header :
8+Hbn/f9F8RIo1kJf5jQ5AX91YtVY/
```

```
Wed Jan  8 11:42:40 2020 Info: MID 385701 ready 7425 bytes from
<hrdogan@cisco.com>
Wed Jan  8 11:42:46 2020 Info: ICID 2297344 close
Wed Jan  8 11:44:40 2020 Info: MID 385701 matched all recipients for
per-recipient policy DEFAULT in the inbound table
Wed Jan  8 11:44:42 2020 Info: MID 385701 interim verdict using
engine: CASE spam negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 using engine: CASE spam
negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 interim AV verdict using
McAfee CLEAN
Wed Jan  8 11:44:42 2020 Info: MID 385701 interim AV verdict using
Sophos CLEAN
Wed Jan  8 11:44:42 2020 Info: MID 385701 antivirus negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 AMP file reputation
verdict : SKIPPED (no attachment in message)
Wed Jan  8 11:44:42 2020 Info: MID 385701 using engine: GRAYMAIL
negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 Outbreak Filters: verdict
negative
Wed Jan  8 11:44:42 2020 Info: MID 385701 queued for delivery
Wed Jan  8 11:44:42 2020 Info: New SMTP DCID 419670 interface
68.232.151.78 address 178.162.218.204 port 25
Wed Jan  8 11:44:42 2020 Info: DCID 419670 TLS success protocol
TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Wed Jan  8 11:44:42 2020 Info: Delivery start DCID 419670 MID 385701
to RID [0]
Wed Jan  8 11:44:42 2020 Info: Message done DCID 419670 MID 385701
to RID [0]
Wed Jan  8 11:44:42 2020 Info: MID 385701 RID [0] Response '2.0.0
Ok: queued as BD478B200576'
Wed Jan  8 11:44:42 2020 Info: Message finished MID 385701 done
Wed Jan  8 11:44:47 2020 Info: DCID 419670 close
```

Let's Find the Needle In the Haystack!

```
Wed Jan  8 11:42:38 2020 Info: New SMTP ICID 2297344 interface Data
1 (68.232.151.78) address 173.37.86.77 reverse dns host rcdn-iport-
6.cisco.com verified yes
Wed Jan  8 11:42:38 2020 Info: ICID 2297344 ACCEPT SG UNKNOWNLIST
match sbrs[-1.0:10.0] SBRS 3.5 country United States
Wed Jan  8 11:42:39 2020 Info: ICID 2297344 TLS success protocol
TLSv1.2 cipher ECDHE-RSA-
Wed Jan  8 11:42:39 2020
Wed Jan  8 11:42:39 2020
<hrdogan@cisco.com>
Wed Jan  8 11:42:39 2020
<hdogan@tecsec-2310.cat>
Wed Jan  8 11:42:40 2020
postmaster@rcdn-iport-6.c
Wed Jan  8 11:42:40 2020
hrdogan@cisco.com Pass (v
Wed Jan  8 11:42:40 2020
hrdogan@cisco.com None he
Wed Jan  8 11:42:40 2020
verified (d=cisco.com s=i
Wed Jan  8 11:42:40 2020
cisco.com, DMARC pass (SP
Wed Jan  8 11:42:40 2020
Wed Jan  8 11:42:40 2020
0630-44CC-A4B5-037B1C914D
Wed Jan  8 11:42:40 2020
Wed Jan  8 11:42:40 2020
is requested: reverse DNS host: rcdn-iport-6.cisco.com, helo: rcdn-
iport-6.cisco.com, env-from: cisco.com, header-from: cisco.com,
reply-to: Not Present
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Consolidated Sender
Reputation: Neutral, Threat Category: N/A. Youngest Domain Age: 33
years 1 month 17 days for domain: rcdn-iport-6.cisco.com
Wed Jan  8 11:42:40 2020 Info: MID 385701 SDR: Tracker Header :
8+Hbn/f9F8RIo1kJf5jQ5AX91YtVY/
```

Edit Incoming Mail Policy

Mode —**Cluster: Hosted_Cluster** Change Mode...

Centralized Management Options

Edit Policy

Policy Name:	tecsec-2310 *(e.g. my IT policy)*
Editable by (Roles):	Cloud Operator
Insert Before Policy:	1 (tecsec-2310)

Users

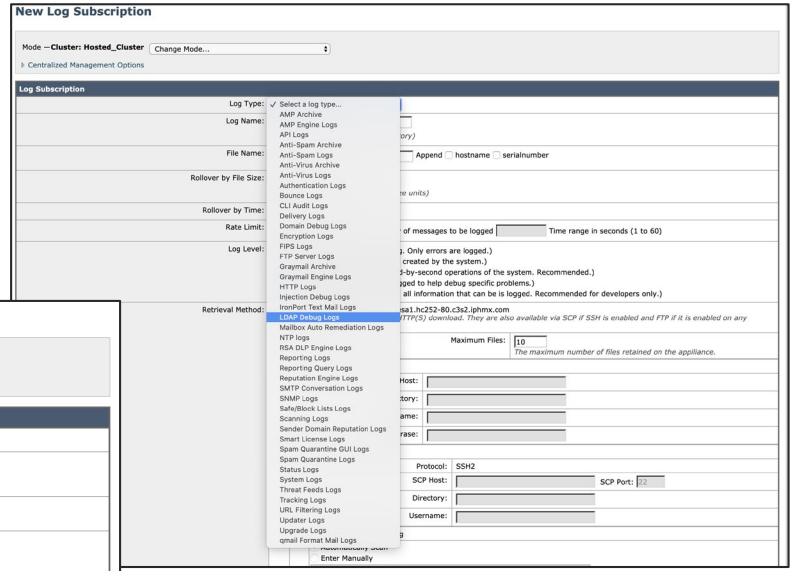
Add User...

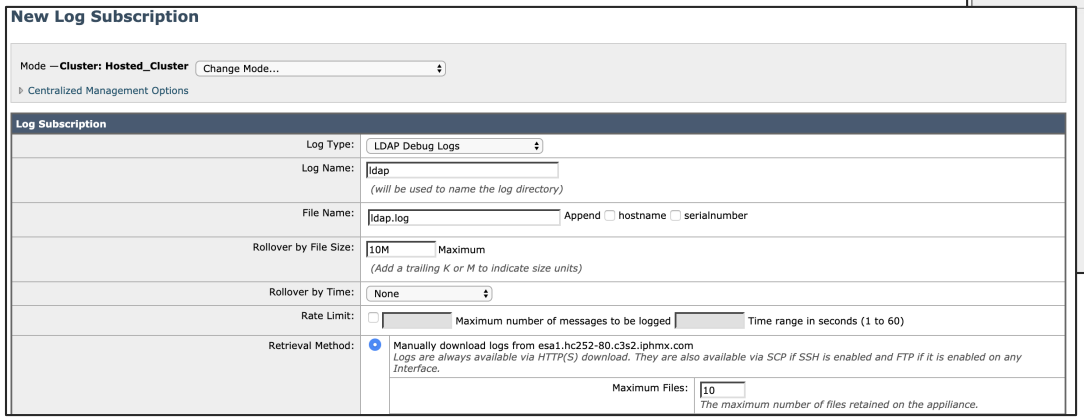
Sender	Recipients	Edit	Delete
ANY	thiachan@tecsec-2310.cat	Edit	
ANY	ldap(foo,bogus-ldap.group)	Edit	

```
Wed Jan  8 11:42:40 2020 Info: MID 385701 ready 7425 bytes from
<hrdogan@cisco.com>
Wed Jan  8 11:42:46 2020 Info: ICID 2297344 close
Wed Jan  8 11:44:40 2020 Info: MID 385701 matched all recipients for
per-recipient policy DEFAULT in the inbound table
Wed Jan  8 11:44:42 2020 Info: MID 385701 interim verdict using
                                                01 using engine: CASE spam
                                                01 interim AV verdict using
                                                01 interim AV verdict using
                                                01 antivirus negative
                                                01 AMP file reputation
                                                sage)
                                                01 using engine: GRAYMAIL
                                                01 Outbreak Filters: verdict
                                                01 queued for delivery
                                                 DCID 419670 interface
                                                ort 25
                                                570 TLS success protocol
                                                384
                                                 start DCID 419670 MID 385701
Wed Jan  8 11:44:42 2020 Info: Message done DCID 419670 MID 385701
to RID [0]
Wed Jan  8 11:44:42 2020 Info: MID 385701 RID [0] Response '2.0.0
Ok: queued as BD478B200576'
Wed Jan  8 11:44:42 2020 Info: Message finished MID 385701 done
Wed Jan  8 11:44:47 2020 Info: DCID 419670 close
```

Other Logs: LDAP Debug

- Not enabled by default!






```
Wed Jan  8 11:56:51 2020 Info: Begin Logfile
Wed Jan  8 11:56:51 2020 Info: Version: 12.1.0-087 SN: 42399DC57E8E7EC75822-AFBCB5A53346
Wed Jan  8 11:56:51 2020 Info: Time offset from UTC: 21600 seconds
Wed Jan  8 11:57:09 2020 Debug: LDAP: bogus-ldap:10.0.12.123(10.0.12.123:3268) (14) Timeout attempting to connect:
Wed Jan  8 11:57:24 2020 Debug: LDAP: bogus-ldap:10.0.12.123(10.0.12.123:3268) (15) connecting to server
Wed Jan  8 11:57:30 2020 Debug: LDAP: (group) Query (mail=hdogan@tecsec-2310.cat) to server bogus-ldap (10.0.12.123:3268)
Wed Jan  8 11:57:30 2020 Debug: LDAP: (group) Query (mail=hdogan@tecsec-2310.cat) lookup failed: LDAP server misconfigured or unreachable
Wed Jan  8 11:57:30 2020 Critical: LDAP: query bogus-ldap.group result LDAP server misconfigured or unreachable
```

Other Logs to Monitor

- Engine-specific logs
  - Individual engine malfunctions are not logged in `mail_logs`
  - Use `mail_logs` to identify the culprit, then consult engine-specific log
- `system_logs`
  - Logging OS and underlying components errors

```
Thu Jan  9 00:00:40 2020 Warning: Received an invalid DNS Response: rcode=ServFail
data="'\\x14\\x84\\x81\\x82\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\rsg2apc01ft033\\teop-
apc01\\x04prod\\nprotection\\x07outlook\\x03com\\x00\\x00\\x01\\x00\\x01'" to IP 68.232.132.138 looking up sg2apc01ft033.eop-
apc01.prod.protection.outlook.com
```

- `status` log
  - readouts captured every minute
  - not human readable!!

```
Thu Jan  9 07:06:03 2020 Info: Status: CPULd 39 DskIO 0 RAMUtil 2 QKUsd 10958 QKFre 8377650 CrtMID 410761 CrtICID 2321505 CrtDCID
413467 InjMsg 258845 InjRcp 279947 GenBncRcp 7501 RejRcp 244018 DrpMsg 21357 SftBncEvnt 165395 CmpRcp 258266 HrdBncRcp 7922
DnsHrdBnc 923 5XXHrdBnc 5807 FltrHrdBnc 0 ExpHrdBnc 1192 OtrHrdBnc 0 DlvRcp 245012 DelRcp 5332 GlbUnsbHt 0 ActvRcp 231 UnatmptRcp
231 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 7471828 NetReq 2632067 CchHit 7656024 CchMis 2383887 CchEct 2028306 CchExp 1693856
CPUTTm 70801 CPUETm 16454438 MaxIO 1501 RAMUsd 168335100 MMLen 230 DstInMem 13 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 15
SophLd 0 BMLd 0 CASELd 0 TotalLd 51 LogAvail 139G EuQ 224 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 1702613 SwOut 1722010 SwPgIn 8865855
SwPgOut 16787340 SwapUsage 1% RptLd 0 QtnLd 0 EncrQ 0 InjBytes 17734563109
```

Kick The Engines with `diagnostic`

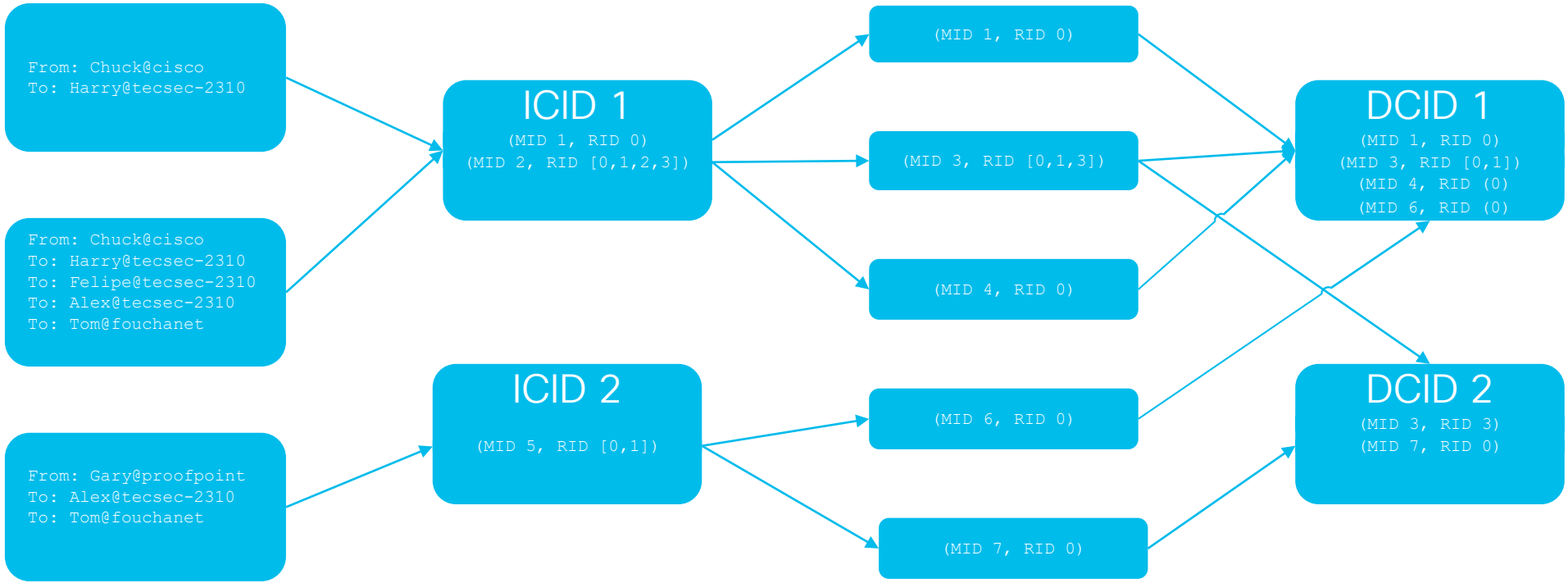
`diagnostic` command lets you restart any AsyncOS services

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> diagnostic


Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial
          manufacturer values.
- SERVICES - Service Utilities.
[]> services
```

```
Choose one of the following services:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- SBRS - Reputation Engine services
- TRACKING - Tracking associated services
- URLFILTERING - URL Filtering
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
- SMART_LICENSE - Smart Licensing Agent
- ETF - External Threat Feeds
- SDR - Sender Domain Reputation
[]> urlfiltering


Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart

Restart command processed. The service URL Filtering should be
up in a moment.
```

Delivery Troubleshooting

Untangling the Identifiers



Reporting on Delivery Is Done Per Destination

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]>

Status as of:                   Tue Jan 21 20:37:15 2020 +06
Hosts marked with '*' were down as of the last delivery attempt.

                                Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host              Recip.    Out     Recip.    Bounced    Bounced

1   [68.232.150.233]               450      0          1          0          0
2*  ayumu58.dev256.xyz               1      0          0          0          0
3*  bollywoodinfoo.com               1      0          0          0          0
4   gmail.com                        1      0         37         46          4
5   dir.hr                           0      0         71          0          0


6   facebookmail.com                 0      0          1          0          0
7   ml1.net                          0      0          4          0          0
8   peekpoke.hr                      0      0          7          0          0
9   ri.t-com.hr                      0      0          1          0          0
10  ritualgym.com                    0      0          1          0          0


11  rivierduinen.nl                  0      0          1          0          0
12  the.cpq.host                     0      0     11,065          0          0
```

Monitor destination delivery rates: `hostrate`

```
alln-inbound-a.cisco.com> hostrate cisco.com

Type Ctrl-C to return to the main prompt.
```

Time	Host Status	CrtCncOut	ActvRcp	ActvRcp Delta	DlvRcp Delta	HrdBncRcp Delta	SftBncEvt Delta
16:54:01	up	1	13	0	40	8	0
16:54:11	up	1	1	-12	62	18	0
16:54:22	up	1	0	-1	47	11	0
16:54:32	up	1	0	0	39	10	0
16:54:42	up	1	0	0	24	7	0
16:54:52	up	1	0	0	31	7	0
16:55:02	up	2	1	1	50	6	0
16:55:12	up	1	0	-1	40	5	0
16:55:22	up	0	0	0	34	1	0
16:55:32	up	1	0	0	24	4	0
16:55:42	up	1	1	1	45	3	0
16:55:52	up	1	0	-1	39	7	0
16:56:02	up	1	0	0	43	6	0
16:56:12	up	1	1	1	42	9	0
16:56:22	up	1	2	1	47	5	0
16:56:32	up	1	0	-2	52	6	0
16:56:42	up	1	1	1	61	6	0
16:56:52	up	1	1	0	39	8	0
16:57:02	up	1	0	-1	10	2	0
16:57:13	up	0	0	0	0	0	0
16:57:23	up	3	12	12	49	11	0

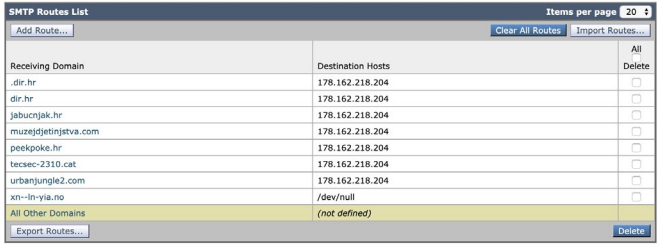
Actual Hosts Are Only Seen In Details

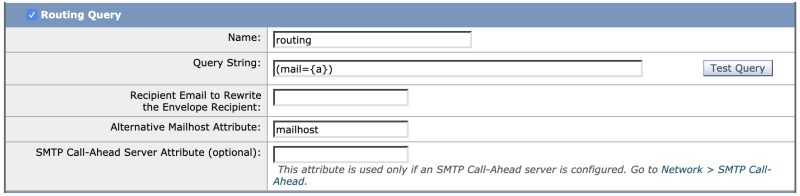
```
(Machine esa1.hc252-80.c3s2.iphmx.com)> hoststatus gmail.com

Host mail status for: 'gmail.com'
Status as of:         Tue Jan 21 20:43:53 2020 +06
Host up/down:         up

Counters:
  Queue
    Soft Bounced Events                     46
  Completion
    Completed Recipients                    41
      Hard Bounced Recipients                4
        DNS Hard Bounces                     0
        5XX Hard Bounces                     4
        Filter Hard Bounces                  0
        Expired Hard Bounces                 0
        Other Hard Bounces                   0
      Delivered Recipients                  37
      Deleted Recipients                     0

Gauges:
  Queue
    Active Recipients                        1
      Unattempted Recipients                 0
      Attempted Recipients                   1
    Connections
      Current Outbound Connections           0
      Pending Outbound Connections           0

Oldest Message        1 day 16 hours 49 mins 43 secs
Last Activity         Tue Jan 21 20:00:48 2020 +06
```

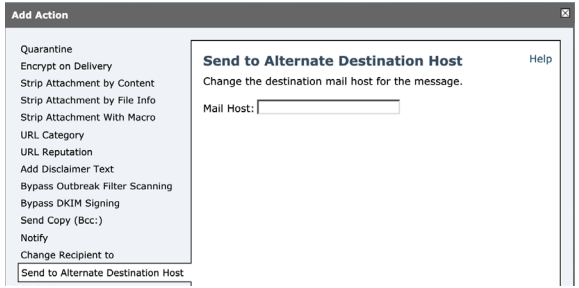
```
Ordered IP addresses: (expiring at Tue Jan 21 21:10:18 2020 +06)
    Preference   IPs
    5            74.125.143.26

    10           142.250.4.27

    20           108.177.97.27

    30           173.194.202.27

    40           108.177.10.26

MX Records:
    Preference   TTL        Hostname
    5            45m10s     gmail-smtp-in.l.google.com
    10           45m10s     alt1.gmail-smtp-in.l.google.com
    20           45m10s     alt2.gmail-smtp-in.l.google.com
    30           45m10s     alt3.gmail-smtp-in.l.google.com
    40           45m10s     alt4.gmail-smtp-in.l.google.com

    Last 5XX Error:
    ----------
    550 5.7.26 Unauthenticated email from facebookmail.com is not
accepted due
to
5.7.26 domain's DMARC policy. Please contact the administrator of
5.7.26 facebookmail.com domain if this was a legitimate mail. Please
visit
5.7.26  https://support.google.com/mail/answer/2451690 to learn about
the
5.7.26 DMARC initiative. g11si22968665edm.366 - gsmtp
    (at Tue Jan 21 19:15:10 2020 +06) IP: 108.177.127.27
    ----------
```

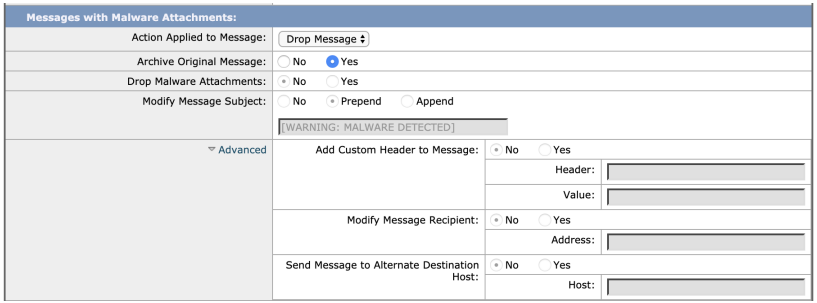
Ways to Determine a Delivery Destination

- First, determine delivery host










```
sinkhole-senders:
if (mail-from-dictionary-match("badSenders") {
alt-mailhost("/dev/null");
}
```

- (Optionally) DNS-resolve delivery host
- Follow IP routing table to deliver

Quarantine Is Just Another Destination

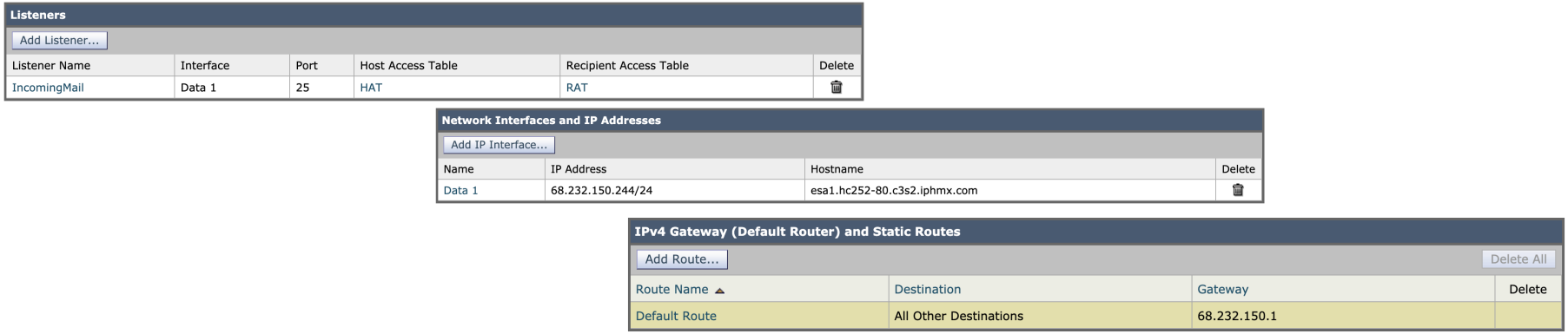
```
Thu Jan  9 05:43:50 2020 Info: MID 410746 enqueued for transfer to centralized quarantine
"Policy" (content filter SpamQ)
Thu Jan  9 05:43:50 2020 Info: MID 410746 queued for delivery
Thu Jan  9 05:43:50 2020 Info: New SMTP DCID 413453 interface 68.232.150.244 address
68.232.150.233 port 25
Thu Jan  9 05:43:50 2020 Info: DCID 413453 TLS success protocol TLSv1.2 cipher DHE-RSA-
AES256-SHA256 the.cpq.host
Thu Jan  9 05:43:50 2020 Info: Delivery start DCID 413453 MID 410746 to RID [0] to
Centralized Policy Quarantine
Thu Jan  9 05:43:50 2020 Info: Message done DCID 413453 MID 410746 to RID [0]
(centralized policy quarantine)
Thu Jan  9 05:43:50 2020 Info: MID 410746 RID [0] Response 'ok:  Message 58480 accepted'
Thu Jan  9 05:43:50 2020 Info: Message finished MID 410746 done
Thu Jan  9 05:43:55 2020 Info: DCID 413453 close
```

#1 Source of Confusion With Delivery

LISTENERS DO NOT DELIVER

Listeners Do Not Deliver

- Delivery follows IP routing rules
- IP interfaces (IP addresses) on the ESA usually have listeners attached



Listeners

Add Listener...

Listener Name	Interface	Port	Host Access Table	Recipient Access Table	Delete
IncomingMail	Data 1	25	HAT	RAT	

Network Interfaces and IP Addresses

Add IP Interface...

Name	IP Address	Hostname	Delete
Data 1	68.232.150.244/24	esa1.hc252-80.c3s2.iphmx.com	

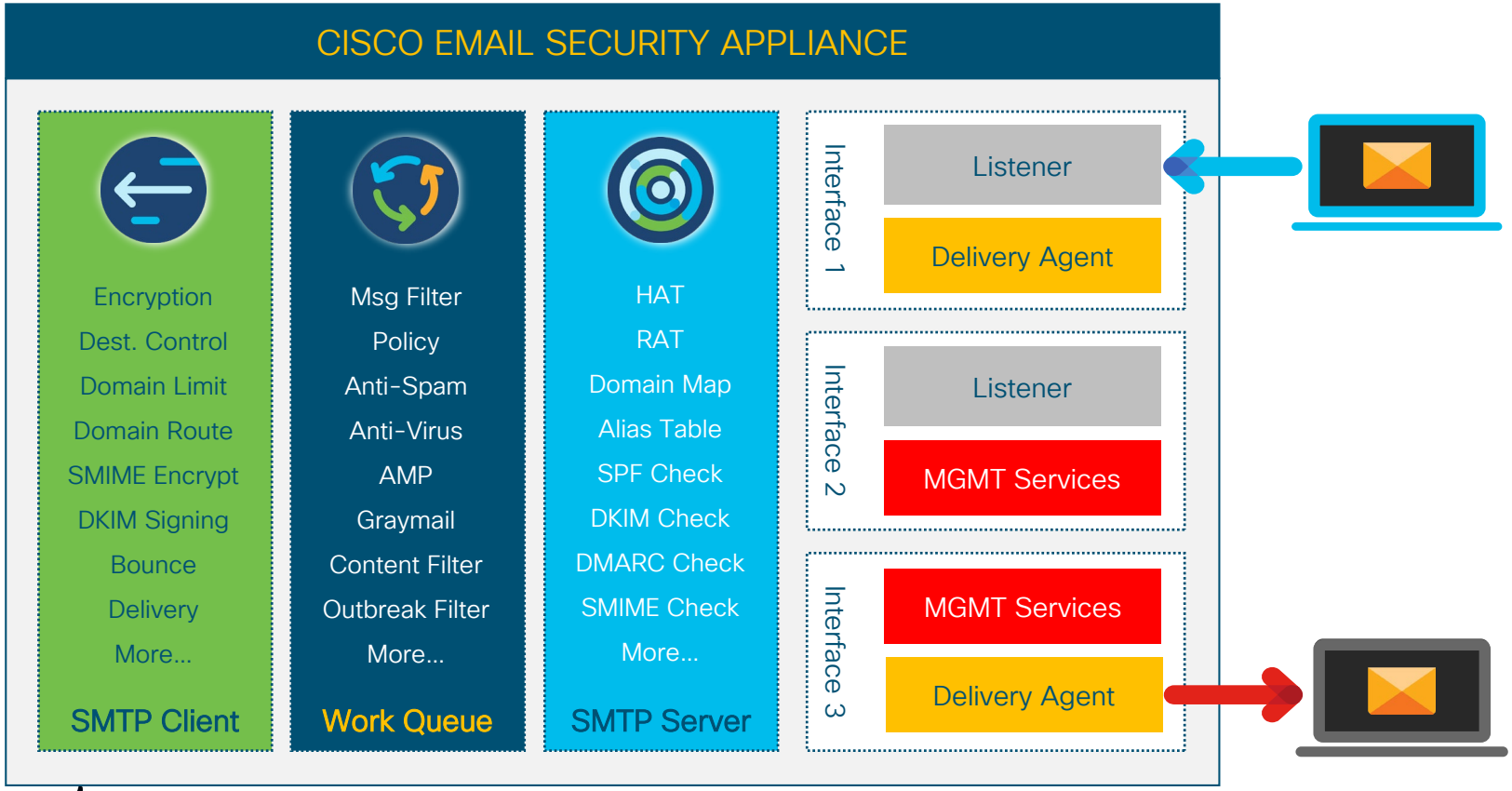
IPv4 Gateway (Default Router) and Static Routes

Add Route... Delete All

Route Name ▲	Destination	Gateway	Delete
Default Route	All Other Destinations	68.232.150.1	

- Correlation does not imply causation
- Listeners and Delivery Client are on complete opposite ends of the pipeline

Listeners vs. Interfaces vs. Delivery Client

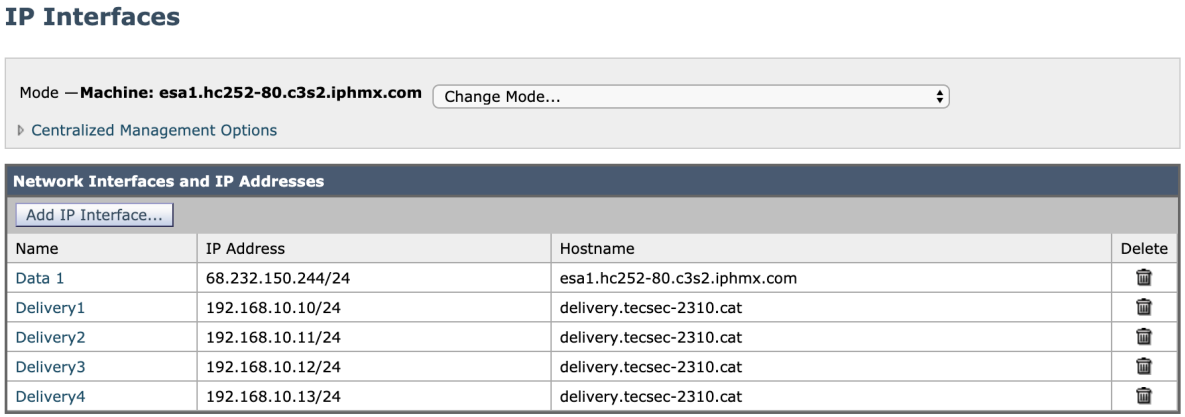


Common Delivery Problems And Solutions

- DNS, DNS, DNS!!!
  - Your Interface Hostnames **must** be in the DNS, **must** correctly reverse-resolve
  - Make sure your SPF, DKIM and DMARC records are all correct
- Remote end requires TLS
  - Destination Controls
- Remote end requires authentication
  - Network -> SMTP Authentication; then SMTP Routes
- You have a bad reputation
  - Fix your problems, then try again

Throttled Due To High Traffic Volume? Worry Not!

```
Thu Jan  9 07:06:24 2020 Info: Connection Error: DCID 413468
domain: pop3.namnerbca.com IP: 5.45.76.120 port: 25 details: 421-
'Too many concurrent SMTP connections; please try again later.'
interface: 68.232.150.244 reason: unexpected SMTP response
```



Throttled Due To High Traffic Volume? Worry Not!

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> interfaceconfig
Currently configured interfaces:
1. Data 1 (68.232.150.244/24 on Data 1: esa1.hc252-80.c3s2.iphmx.com)
2. Delivery1 (192.168.10.10/24 on Data 2: delivery.tecsec-2310.cat)
3. Delivery2 (192.168.10.11/24 on Data 2: delivery.tecsec-2310.cat)
4. Delivery3 (192.168.10.12/24 on Data 2: delivery.tecsec-2310.cat)
5. Delivery4 (192.168.10.13/24 on Data 2: delivery.tecsec-2310.cat)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> groups
Currently configured IP groups:
No groups defined.

Choose the operation you want to perform:
- NEW - Create a new group.
[]> new

Enter the name for this group.
[]> tecsec2310-delivery

Enter the name or number of the interfaces to be included
Separate your choices with commas or specify a range with a dash.
1. Data 1 (68.232.150.244/24: esa1.hc252-80.c3s2.iphmx.com)
2. Delivery1 (192.168.10.10/24: delivery.tecsec-2310.cat)
3. Delivery2 (192.168.10.11/24: delivery.tecsec-2310.cat)
4. Delivery3 (192.168.10.12/24: delivery.tecsec-2310.cat)
5. Delivery4 (192.168.10.13/24: delivery.tecsec-2310.cat)
[1]> 2-5

Group tecsec2310-delivery created.
```

```
(Cluster Hosted_Cluster)> altsrchost

Choose the operation you want to perform:
- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.
- CLUSTERSET - Set how Virtual Gateways(tm) are configured in a cluster.
- CLUSTERSHOW - Display how Virtual Gateways(tm) are configured in a
cluster.
[]> new

Enter the Envelope From address or client IP address for which you want
to set
up a Virtual Gateway(tm) mapping.  Partial addresses such as
"@example.com",
"@.com", "user@", or "user@.com" are allowed.
[]> @tecsec-2310.cat

Which interface do you want to send messages for @tecsec-2310.cat from?
1. Data 1
2. Delivery1
3. Delivery2
4. Delivery3
5. Delivery4
IP Groups:
6. tecsec2310-delivery
[1]> 6

Mapping for @tecsec-2310.cat on interface tecsec2310-delivery created.
```

Destination Is Confirmed Dead; Now What?

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> showrecipients

Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1

Please enter the hostname for the messages you wish to show.
> pop3.namnerbca.com

Showing messages, please wait.

MID/     Bytes/    Sender/                 Subject
[RID]    [Atmps]   Recipient
410508   1658      riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Potvrda_prijave_na_Jabu=C4=8Dnjak?=
[0]      [0]       ehusakga@pop3.namnerbca.com
410512   1658      riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Potvrda_prijave_na_Jabu=C4=8Dnjak?=
[0]      [0]       uzuxar@pop3.namnerbca.com
410513   1658      riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Potvrda_prijave_na_Jabu=C4=8Dnjak?=
[0]      [0]       uzuxar@pop3.namnerbca.com
410532   981       riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Rejection_Subject?=
[0]      [0]       ehusakga@pop3.namnerbca.com
```

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1

Please enter the hostname for the messages you wish to delete.
[]> pop3.namnerbca.com

Are you sure you want to delete all messages being delivered to
"pop3.namnerbca.com"? [N]> y

Deleting messages, please wait..
4 recipients deleted.
```

Destination Is Confirmed Dead; Now What?

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> showrecipients

Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1

Please enter the hostname for the messages you wish to show.
> pop3.namnerbca.com

Showing messages, please wait.

MID/     Bytes/    Sender/                 Subject
[RID]    [Atmps]   Recipient
410508   1658      riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Potvrda_prijave_na_Jabu=C4=8Dnjak?=
[0]      [0]       ehusakga@pop3.namnerbca.com
410512   1658      riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Potvrda_prijave_na_Jabu=C4=8Dnjak?=
[0]      [0]       uzuxar@pop3.namnerbca.com
410513   1658      riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Potvrda_prijave_na_Jabu=C4=8Dnjak?=
[0]      [0]       uzuxar@pop3.namnerbca.com
410532   981       riba@jabucnjak.hr       =?UTF-8?Q?Jabu=C4=8Dnjak_-
_Rejection_Subject?=
[0]      [0]       ehusakga@pop3.namnerbca.com
```

```
(Cluster Hosted_Cluster)> smtproutes

There are currently 8 routes configured.

Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Edit destinations of an existing route.
- DELETE - Remove a route.
- PRINT - Display all routes.
- IMPORT - Import new routes from a file.
- EXPORT - Export all routes to a file.
- CLEAR - Remove all routes.
- CLUSTERSET - Set how SMTP routes are configured in a cluster.
- CLUSTERSHOW - Display how SMTP routes are configured in a cluster.
[]> new

Enter the domain for which you want to set up a permanent route.
Partial hostnames such as ".example.com" are allowed.
Use "ALL" for the default route.
[]> pop3.namnerbca.com

Enter the destination hosts, separated by commas, which you want mail for
pop3.namnerbca.com to be delivered.
Enter USEDNS by itself to use normal DNS resolution for this route.
Enter /dev/null by itself if you wish to discard the mail.
Enclose in square brackets to force resolution via address (A)
records, ignoring any MX records.
[]> 192.168.10.20

Mapping for pop3.namnerbca.com to 192.168.10.10 created.
(Machine esa1.hc252-80.c3s2.iphmx.com)> delivernow host pop3.namnerbca.com

Scheduling all messages to pop3.namnerbca.com for delivery.
```

See What They See: Domain Debug Log

```
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '220-alln-inbound-1.cisco.com ESMTP'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '220 esa1.hc252-80.c3s2.iphmx.com (68.232.150.244) is being throttled due to an unknown or low email
reputation score. See https://talosintelligence.com/reputation_center/lookup?search=68.232.150.244 for details.'
Fri Jan  3 13:17:49 2020 Info: 412359 Sent: 'EHLO esa1.hc252-80.c3s2.iphmx.com'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '250-alln-inbound-1.cisco.com'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '250-8BITMIME'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '250-SIZE 33554432'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '250 STARTTLS'
Fri Jan  3 13:17:49 2020 Info: 412359 Sent: 'STARTTLS'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '220 Go ahead with TLS'
Fri Jan  3 13:17:49 2020 Info: 412359 Sent: 'EHLO esa1.hc252-80.c3s2.iphmx.com'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '250-alln-inbound-1.cisco.com'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '250-8BITMIME'
Fri Jan  3 13:17:49 2020 Info: 412359 Rcvd: '250 SIZE 33554432'
Fri Jan  3 13:17:49 2020 Info: 412359 Sent: 'MAIL FROM:<hdogan@tecsec-2310.cat> SIZE=224'
Fri Jan  3 13:17:50 2020 Info: 412359 Rcvd: '250 sender <hdogan@tecsec-2310.cat> ok'
Fri Jan  3 13:17:50 2020 Info: 412359 Sent: 'RCPT TO:<hrdogan@cisco.com>'
Fri Jan  3 13:17:50 2020 Info: 412359 Rcvd: '250 recipient <hrdogan@cisco.com> ok'
Fri Jan  3 13:17:50 2020 Info: 412359 Sent: 'DATA'
Fri Jan  3 13:17:50 2020 Info: 412359 Rcvd: '354 go ahead'
Fri Jan  3 13:17:50 2020 Info: 412359 Sent: 'Message-Id: <5f1891$cfu8@esa1.hc252-80.c3s2.iphmx.com>\r\n'
Fri Jan  3 13:17:50 2020 Info: 412359 Sent: 'Date: 03 Jan 2020 13:17:35 +0600\r\n'
Fri Jan  3 13:17:50 2020 Info: 412359 Sent: 'IronPort-SDR: 4LyFTtbCbrs6GgtxRCpX9tvTj5AA0UC9PT7fZ099II2/FK7kiMi0jwH/76vwOWEEOWCufq/4Hs\r\n
jTCdvCpWZCd50C+woA2X0G+yTJybYUec2DYJGhx939APhXC7B1viCHmrwAHQWN7RlVDZPSKUtO\r\n
8N1N0nRj+Cxq1STYfvXQjrLO80o8W1IDfMVF0s+rstd6hs2NMoChWqgyq9yLTFk7HbuG0r2SVE\r\n
eyiHsaSQpQ6gt2hTlXt7zHj5u8kqG5uZhS6NWz7ljf9SO42del5fFUMnG+LNp6dCt+QcWwi8JP\r\n sao=\r\n'
Fri Jan  3 13:17:50 2020 Info: 412359 Sent: 'Received: from unknown (HELO tecsec-2310.cat) ([178.162.218.204])\r\n  by esa1.hc252-80.c3s2.iphmx.com
with ESMTP; 03 Jan 2020 13:17:35 +0600\r\nFrom: Hrvoje Dogan <hdogan@tecsec-2310.cat>\r\nSubject: Test Email\r\n\r\nHello, world!\r\n'
Fri Jan  3 13:17:50 2020 Info: 412359 Sent: '.\r\n'
Fri Jan  3 13:17:50 2020 Info: 412359 Rcvd: '250 ok:  Message 213534267 accepted'
Fri Jan  3 13:17:55 2020 Info: 412359 Sent: 'QUIT'
Fri Jan  3 13:17:55 2020 Info: 412359 Rcvd: '221 alln-inbound-1.cisco.com'
```

Network Stack Troubleshooting

Troubleshooting Network Issues

- Probably the trickiest part to troubleshoot
  - Networking people love blaming the messaging people
  - It's always L7!
- Understand your interfaces
  - Physical interfaces vs. IP interfaces (IP addresses)
  - Understand your routing
- Use AsyncOS built-in tools: `ping`, `ping6`, `traceroute`, `nslookup`, `dig`…
- Make sure there are no devices doing SMTP fixup in the path
  - Once you're sure, check again
- `packetcapture` will help you capture network traffic to a file

Swiss Army Knife #1: `netstat`

AsyncOS `netstat` lets you print routing tables

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> netstat

Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
[1]> 3

1. IPv4 only.
2. IPv6 only.
[1]> 1

Show network addresses as numbers? [N]> y
```

```
Routing tables

Internet:
Destination        Gateway            Flags      Netif
Expire
default            68.232.150.1       UGS         Data 1
68.232.150.0/24    link#2             U           Data 1
68.232.150.244     link#2             UHS         lo0
127.0.0.1          link#4             UH          lo0
192.168.10.0/24    link#3             U           Data 2
192.168.10.10      link#3             UHS         lo0
192.168.10.11      link#3             UHS         lo0
192.168.10.11/32   link#3             U           Data 2
192.168.10.12      link#3             UHS         lo0
192.168.10.12/32   link#3             U           Data 2
192.168.10.13      link#3             UHS         lo0
192.168.10.13/32   link#3             U           Data 2
```

Swiss Army Knife #1: `netstat`

AsyncOS `netstat` lets you monitor interface traffic in real time

```
alln-inbound-a.cisco.com> netstat

Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
[1]> 5

Enter the number of seconds between displays.
[10]> 1

Select the ethernet interface whose state you
wish to display:
1. Data 1
2. Data 2
3. Data 3
4. Data 4
5. Data 5
6. Management
7. ALL
[]> 7

Show the number of dropped packets? [N]> y
```

```
Press Ctrl-C to stop.

          input        (Total)           output
  packets  errs idrops      bytes    packets  errs      bytes colls drops
      827     0      0     426870       1170     0     679632     0     0
      604     0      0     248130        892     0     499221     0     0
     2303     0      0    2360983       2506     0     443282     0     0
     1076     0      0    1119303       1124     0     132115     0     0
      874     0      0     752084        975     0     175989     0     0
     1204     0      0     251126       2625     0    2575912     0     0
      831     0      0     113038       1747     0    1721814     0     0
      464     0      0     133118        572     0     189809     0     0
     1740     0      0    2187050       1811     0     169045     0     0
     1285     0      0     320682       2749     0    2697868     0     0
     1055     0      0     574237       1293     0     419464     0     0
     1072     0      0    1008321       1174     0     272901     0     0
     1240     0      0    1182763       1368     0     274056     0     0
     1277     0      0    1309303       1463     0     335713     0     0
     1370     0      0    1413720       1532     0     376569     0     0
     1354     0      0     277312       3524     0    4184089     0     0
      419     0      0      56022        619     0     517380     0     0
      848     0      0    1114515        880     0      79671     0     0
     1105     0      0    1393939       1152     0     100034     0     0
      556     0      0     463436        634     0     152345     0     0
     1720     0      0     705301       3418     0    3166580     0     0
```

Swiss Army Knife #2: `diagnostic -> network`

`network` section of `diagnostic` command lets you see/clear ARP table

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> diagnostic


Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial
           manufacturer values.
- SERVICES - Service Utilities.
[]> network
```

```
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> arpshow

System ARP cache contents:

(192.168.10.10) at 00:50:56:89:08:b4 on nic2 permanent [ethernet]
(192.168.10.11) at 00:50:56:89:08:b4 on nic2 permanent [ethernet]
(192.168.10.12) at 00:50:56:89:08:b4 on nic2 permanent [ethernet]
(192.168.10.13) at 00:50:56:89:08:b4 on nic2 permanent [ethernet]
(68.232.150.244) at 00:50:56:89:0e:b0 on nic1 permanent [ethernet]
(68.232.150.233) at 00:50:56:89:79:b6 on nic1 expires in 628 seconds
[ethernet]
(68.232.150.1) at 00:00:0c:9f:f0:02 on nic1 expires in 313 seconds
[ethernet]
```

Swiss Army Knife #2: `diagnostic -> network`

`network` section of `diagnostic` command lets you test an SMTP server

```
(Machine esa1.hc252-80.c3s2.iphmx.com)> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial
               manufacturer values.
- SERVICES - Service Utilities.
[]> network
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> smtpping
Enter the hostname or IP address of the SMTP server:
[esa1.hc252-80.c3s2.iphmx.com]> cisco.com

The domain you entered has MX records.
Would you like to select an MX host to test instead? [Y]>
Select an MX host to test.
1. aer-mx-01.cisco.com
2. alln-mx-01.cisco.com
3. rcdn-mx-01.cisco.com
[1]>
```

```
Do you want to type in a test message to send?  If not, the connection will
be
tested but no email will be sent. [N]> y

Enter the From e-mail address:
[from@example.com]> hdogan@tecsec-2310.cat

Enter the To e-mail address:
[to@example.com]> gary@proofpoint.com

Enter the Subject:
[Test Message]>

Enter the Body of the message one line at a time.  End with a "." on a line
by
itself.
Hello, World!
.


Starting SMTP test of host aer-mx-01.cisco.com.
Resolved 'aer-mx-01.cisco.com' to 173.38.212.150.
Connection to 173.38.212.150 succeeded.
Command EHLO succeeded
Command MAIL FROM succeeded.
Command RCPT TO failed.  Remote server said: 550 ['#5.1.0 Address rejected.']
```

Email Authentication Troubleshooting

It’s Not You, It’s Me

- We know you’ll do Email Authentication right; it’s other people that don’t
- In general, few main sources of errors:

1. Incomplete SPF records
2. Incorrect SPF records
3. Failure at DMARC alignment
4. Failure at specifying a DMARC policy altogether

How To Spot a Culprit?

Headers show the truth

```
Authentication-Results: esa2.hc252-80.c3s2.iphmx.com;
spf=None smtp.pra=hrdogan@cisco.com; spf=Pass
smtp.mailfrom=hrdogan@cisco.com; spf=Pass
smtp.helo=postmaster@rcdn-iport-5.cisco.com; dkim=pass
(signature verified) header.i=@cisco.com; dmarc=pass
(p=quarantine dis=none) d=cisco.com
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901;
d=microsoft.com; cv=none;
b=lygJF4GD21zc9ZRub1CFJfpscjByuFyv41L4XCuZB/Tz9lO/WnpqTF9zlDb
GJWlw2parepvJp+dMhGNlBd+AhRSOarHOKzd/DIclfGFB7PiOMMS/VPu3EFxp
lvfWzF1ecwz06xxw+ET+ITk1FLwYGlak9L9owsaAke9Q3cSYvxEzNmE1aRJ/l
ZdfKM7Nqo4EEUOrQR7oD08e+hYw1aRMajnXOXuX/00rM9k/iln+2mAAQHn85r
aYMcD0fWRIlO7sw1UzSjQgF/f69K6qxKbJkdy8YZszzsgYDJDSMQgzdm0ZK7x
V1m+rYpgo3A1H3Ap4SgxSz0Jb1yyuBMVcgW0Vyw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed;
d=microsoft.com;
s=arcselector9901;h=From:Date:Subject:Message-ID:Content-
Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=5p6QioVXEc5BL4HDv5N/rutYlomsnkMZiJLZnIQgfGs=;
b=QEfI4/qXotVe4HnMZx+XXCh7EkzqWYMyl4s0IYbSgcDtEXqZi0TuUUEBn11
+qoRbtNGGu9iumOJTnhhQeyyfHJXhYx0vNF+AC9ulK8JWRH825bE8iDIXb2NQ
h1ZCgzXgN6k2tpoOD1501FxBi+MjhBQO2wyG/Qwyr77a7Mq07iQtBTItrywzj
XLjgIN60PR9OOahaMKS3k8tz39lFIy5Q2dnfgrni2YWlsyBO1y8jsFLx26hDR
wy7dt0EpuAwjdMYca6Sz/o2QeY5FXB1JVAdb0WKeJzX48TYWWMFKOlNp/ytnb
BL15eDpJnZ/7vBa8pqzjh/fRdpTtZBZLAbR85uw==
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass
 smtp.mailfrom=cisco.com; dmarc=pass action=none
header.from=cisco.com;
 dkim=pass header.d=cisco.com; arc=none
```

```
Received-SPF: None (esa2.hc252-80.c3s2.iphmx.com: no sender
  authenticity information available from domain of
  hrdogan@cisco.com) identity=pra; client-ip=173.37.86.76;
  receiver=esa2.hc252-80.c3s2.iphmx.com;
  envelope-from="hrdogan@cisco.com";
  x-sender="hrdogan@cisco.com";
  x-conformance=sidf_compatible.downgrade_pra
Received-SPF: Pass (esa2.hc252-80.c3s2.iphmx.com: domain of
  hrdogan@cisco.com designates 173.37.86.76 as permitted
  sender) identity=mailfrom; client-ip=173.37.86.76;
  receiver=esa2.hc252-80.c3s2.iphmx.com;
  envelope-from="hrdogan@cisco.com";
  x-sender="hrdogan@cisco.com";
  x-conformance=sidf_compatible.downgrade_pra;
  x-record-type="v=spf1"; x-record-text="v=spf1
  ip4:173.37.147.224/27 ip4:173.37.142.64/26
  ip4:173.38.212.128/27 ip4:173.38.203.0/24 ip4:72.163.7.160/27
  ip4:72.163.197.0/24 ip4:66.187.208.0/20 ip4:173.37.86.0/24
  include:spf.protection.outlook.com
  include:spfb._spf.cisco.com ~all"
Received-SPF: Pass (esa2.hc252-80.c3s2.iphmx.com: domain of
  postmaster@rcdn-iport-5.cisco.com designates 173.37.86.76 as
  permitted sender) identity=helo; client-ip=173.37.86.76;
  receiver=esa2.hc252-80.c3s2.iphmx.com;
  envelope-from="hrdogan@cisco.com";
  x-sender="postmaster@rcdn-iport-5.cisco.com";
  x-conformance=sidf_compatible.downgrade_pra;
  x-record-type="v=spf1"; x-record-text="v=spf1 a -all"
```

... Sometimes It's Just The Ordinary SPF Stuff...

```
Authentication-Results: esa1.hc252-80.c3s2.iphmx.com; spf=None smtp.pra=enquiry@
unionpower.com.sg; spf=PermError smtp.mailfrom=bounce+adc652.8c5d5-hdogan=dir.hr
@unionpower.com.sg; spf=None smtp.helo=postmaster@so254-36.mailgun.net; dkim=pass
(signature verified) header.i=@unionpower.com.sg

unionpower.com.sg      text = "v=spf1 +a +mx +ip4:124.6.61.19
+include:spf.protection.outlook.com -all"
unionpower.com.sg      text = "v=spf1 include:mailgun.org ~all"

Authentication-Results: esa2.hc252-80.c3s2.iphmx.com; dkim=none (message not signed)
header.i=none; spf=None smtp.pra=noreply@commontown.com; spf=PermError
smtp.mailfrom=ctown@passiton.org.sg; spf=PermError smtp.helo=postmaster@passiton.org.sg;
dmarc=fail (p=none dis=none) d=commontown.com

passiton.org.sg        text = "v=spf1 mx a ptr ip4:202.172.254.54 include:202.157.161.165
-all"
```

... Yet Sometimes it looks benign...

```
vimboxmovers.sg          text = "v=spf1 a mx include:websitewelcome.com ~all”

  websitewelcome.com  text = "v=spf1 include:spf.websitewelcome.com include:spf1.websitewelcome.com include:spfgwp.websitewelcome.com
  include:_spf.google.com -all”

  spf.websitewelcome.com          text = "v=spf1 ip4:192.185.0.0/16 ip4:50.116.64.0/18 ip4:50.87.152.0/21 ip4:108.167.128.0/18
  ip4:216.172.160.0/19 ip4:108.179.192.0/18 ip4:162.144.0.0/16 include:relay.mailchannels.net”

     relay.mailchannels.net       text = "v=spf1 include:spf1.mailchannels.net include:spf2.mailchannels.net ~all”

      spf1.mailchannels.net       text = "v=spf1 ip4:46.232.183.0/24 ip4:23.83.208.1/20 ip4:177.153.0.128/25 ip4:191.252.57.0/25
      ~all”

      spf2.mailchannels.net       text = "v=spf1 ip4:199.10.31.235/32 ip4:199.10.31.236/32 ip4:172.255.62.10/32  ip4:172.255.62.11/32
      ip4:103.18.109.138/32 ip4:177.153.0.130/32 ip4:54.214.232.113/32 ip4:54.245.125.39/32 ~all”

  spf1.websitewelcome.com         text = "v=spf1 ip4:100.42.48.0/20 ip4:104.152.64.0/21 ip4:104.171.0.0/20 ip4:108.175.144.0/20
  ip4:23.91.112.0/20 ip4:198.58.80.0/20 ip4:198.252.64.0/20 ip4:192.169.48.0/20 ip4:162.253.144.0/21 ip4:162.254.160.0/21”

  spfgwp.websitewelcome.com       text = "v=spf1 ip4:66.147.240.0/20 ip4:67.20.64.0/19 ip4:67.20.96.0/21 ip4:67.222.32.0/19
  ip4:69.89.16.0/20 ip4:70.40.192.0/19 ip4:74.220.192.0/19”

  _spf.google.com     text = "v=spf1 include:_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com
  ~all”

  _netblocks.google.com           text = "v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19 ip4:66.102.0.0/20 ip4:66.249.80.0/20
  ip4:72.14.192.0/18 ip4:74.125.0.0/16 ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:209.85.128.0/17 ip4:216.58.192.0/19
  ip4:216.239.32.0/19 ~all”

  _netblocks2.google.com          text = "v=spf1 ip6:2001:4860:4000::/36 ip6:2404:6800:4000::/36 ip6:2607:f8b0:4000::/36
  ip6:2800:3f0:4000::/36 ip6:2a00:1450:4000::/36 ip6:2c0f:fb50:4000::/36 ~all”

  _netblocks3.google.com          text = "v=spf1 ip4:172.217.0.0/19 ip4:172.217.32.0/20 ip4:172.217.128.0/19 ip4:172.217.160.0/20
  ip4:172.217.192.0/19 ip4:172.253.56.0/21 ip4:172.253.112.0/20 ip4:108.177.96.0/19 ip4:35.191.0.0/16 ip4:130.211.0.0/22 ~all"
```

... Yet Sometimes it looks benign...

vimboxmovers.sg text = "v=spf1 **a mx include:websitewelcome.com** ~all”

websitewelcome.com text = "v=spf1 **include:spf.websitewelcome.com include:spf1.websitewelcome.com include:spfgwp.websitewelcome.com include:_spf.google.com** -all”

spf.websitewelcome.com text = "v=spf1 ip4:192.185.0.0/16 ip4:50.116.64.0/18 ip4:50.87.152.0/21 ip4:108.167.128.0/18 ip4:216.172.160.0/19 ip4:108.179.192.0/18 ip4:162.144.0.0/16 **include:relay.mailchannels.net**”

relay.mailchannels.net text = "v=spf1 **include:spf1.mailchannels.net include:spf2.mailchannels.net** ~all”

spf1.mailchannels.net text = "v=spf1 ip4:46.232.183.0/24 ip4:23.83.208.1/20 ip4:177.153.0.128/25 ip4:191.252.57.0/25 ~all”

spf2.mailchannels.net text = "v=spf1 ip4:199.10.31.235/32 ip4:199.10.31.236/32 ip4:172.255.62.10/32 ip4:172.255.62.11/32 ip4:103.18.109.138/32 ip4:177.153.0.130/32 ip4:54.214.232.113/32 ip4:54.245.125.39/32 ~all”

spf1.websitewelcome.com text = "v=spf1 ip4:100.42.48.0/20 ip4:104.152.64.0/21 ip4:104.171.0.0/20 ip4:108.175.144.0/20 ip4:23.91.112.0/20 ip4:198.58.80.0/20 ip4:198.252.64.0/20 ip4:192.169.48.0/20 ip4:162.253.144.0/21 ip4:162.254.160.0/21”

spfgwp.websitewelcome.com text = "v=spf1 ip4:66.147.240.0/20 ip4:67.20.64.0/19 ip4:67.20.96.0/21 ip4:67.222.32.0/19 ip4:69.89.16.0/20 ip4:70.40.192.0/19 ip4:74.220.192.0/19”

_spf.google.com text = "v=spf1 include:**_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com** ~all”

_netblocks.google.com text = "v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19 ip4:66.102.0.0/20 ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:74.125.0.0/16 ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:209.85.128.0/17 ip4:216.58.192.0/19 ip4:216.239.32.0/19 ~all”

_netblocks2.google.com text = "v=spf1 ip6:2001:4860:4000::/36 ip6:2404:6800:4000::/36 ip6:2607:f8b0:4000::/36 ip6:2800:3f0:4000::/36 ip6:2a00:1450:4000::/36 ip6:2c0f:fb50:4000::/36 ~all”

_netblocks3.google.com text = "v=spf1 ip4:172.217.0.0/19 ip4:172.217.32.0/20 ip4:172.217.128.0/19 ip4:172.217.160.0/20 ip4:172.217.192.0/19 ip4:172.253.56.0/21 ip4:172.253.112.0/20 ip4:108.177.96.0/19 ip4:35.191.0.0/16 ip4:130.211.0.0/22 ~all"

... Sometimes It's Just The Ordinary DKIM Stuff...

```
Authentication-Results: esa2.hc252-80.c3s2.iphmx.com; dkim=permerror (domain mismatch) header.i=none;
spf=None smtp.pra=e-news@resorts.RWSentosa.com; spf=Pass smtp.mailfrom=v-
bioaeeb_elcebijinb_dcenmfgd_dcenmfgd_a@bounce.rwsentosa.mkt7151.com; spf=Pass
smtp.helo=postmaster@mail6552.rwsentosa.mkt7151.com

Authentication-Results: esa2.hc252-80.c3s2.iphmx.com; dkim=permerror (signing time is in the future)
header.i=none; spf=None smtp.pra=no-reply@payoo.com.vn; spf=Pass smtp.mailfrom=no-reply@payoo.com.vn;
spf=None smtp.helo=postmaster@mx1.payoo.com.vn

Authentication-Results: esa2.hc252-80.c3s2.iphmx.com; spf=None smtp.pra=no-reply@mail.xmind.net;
spf=SoftFail smtp.mailfrom=bounce+b196d5.f9f2-hdogan=dir.hr@xmind.net; spf=None
smtp.helo=postmaster@p225.mailgun.us; dkim=permerror (no key for signature) header.i=@xmind.net

Authentication-Results: esa1.hc252-80.c3s2.iphmx.com; spf=None smtp.pra=ebillsummary@spgroup.com.sg;
spf=Pass smtp.mailfrom=ebillsummary@spgroup.com.sg; spf=None
smtp.helo=postmaster@pesa1.singaporepower.com.sg; dkim=permerror (no key for signature)
header.i=@spgroup.com.sg; dkim=permerror (no key for signature) header.i=@spgroup.com.sg; dmarc=pass
(p=none dis=none) d=spgroup.com.sg
```

… But Most of the Time It's Alignment…

```
Authentication-Results: spf=fail (sender IP is 64.101.210.228) smtp.mailfrom=wirefire.ca;
cisco.mail.onmicrosoft.com; dkim=pass (signature was verified)
header.d=Wirefire.onmicrosoft.com;cisco.mail.onmicrosoft.com;
dmarc=fail action=none header.from=wirefire.ca;
```

Standard	Authenticates…
SPF	MAIL FROM, HELO
DKIM	SDID ("d=")
DMARC	From Header

- Identifier Alignment is a concept of alignment between From Header and identifiers checked by DKIM and SPF
- Message passes DMARC check if one or more of the authentication mechanisms (DKIM and/or SPF) pass with proper alignment

DMARC Alignment Types

RELAXED (Default) VS. STRICT

SPF RELAXED

```
MAIL FROM: <sender@tecsec-2310.cat>
250 sender <sender@tecsec-2310.cat> ok
RCPT TO: <user1@cisco.com>
250 recipient <user1@cisco.com> ok
From: Sender <sender@sub.tecsec-2310.cat>
To: User One (user1) <user1@cisco.com>
```

SPF STRICT

```
MAIL FROM: <sender@tecsec-2310.cat>
250 sender <sender@tecsec-2310.cat> ok
RCPT TO: <user1@cisco.com>
250 recipient <user1@cisco.com> ok
From: Sender <sender@sub.tecsec-2310.cat>
To: User One (user1) <user1@cisco.com>
```

DKIM RELAXED

```
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed; d=tecsec-2310.cat;
From: Sender <sender@sub.tecsec-2310.cat>
To: User One (user1) <user1@cisco.com>
```

DKIM STRICT

```
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed; d=tecsec-2310.cat;
From: Sender <sender@mail.tecsec-2310.cat>
To: User One (user1) <user1@cisco.com>
```

... And Then You Have These People...

```
$ host -t txt _dmarc.domain.com

_dmarc.domain.com descriptive text "v=spf1 ip4:194.127.3.0/26
ip4:194.127.24.225 ip4:194.127.26.225 ip4:87.106.1.21
ip4:208.86.168.7 ip4:135.84.68.123 ip4:193.240.14.113
ip4:204.93.80.116 ip4:204.93.80.117 " "ip4:168.114.112.22
ip4:168.114.112.23 include:_spf.domain.com
include:_spf2.domain.com ~all"
```

... But, Maybe It Is You?

- ...an email from one of our VPs:

```
Authentication-Results-Original: alln-inbound-k.cisco.com; spf=Pass
smtp.mailfrom=bounce-p2-p5jyrwxj8vh748-65zkpw4d-a01-zn2z-
00100000004PiFmAAK@cvent-planner.com;
spf=Pass smtp.helo=postmaster@m239a.cvtsv.com; dkim=pass (signature
verified)
header.i=@cvent-planner.com; dmarc=fail (p=quarantine dis=none)
d=cisco.com
```

- Bottom line: Be careful if you outsource email!

Q & A

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

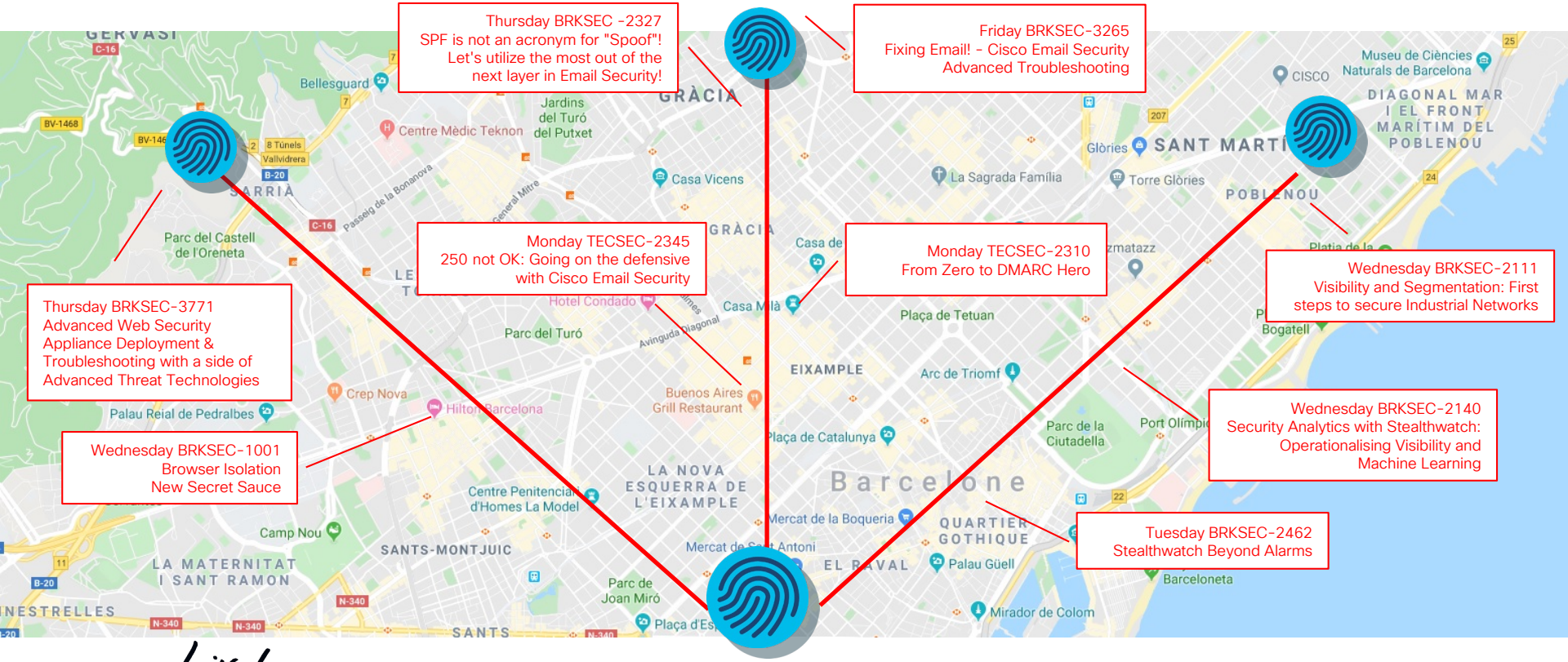
Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

EMAIL, Web Security and Visibility Learning maps



Thank you

You make **possible**