Microsoft Security

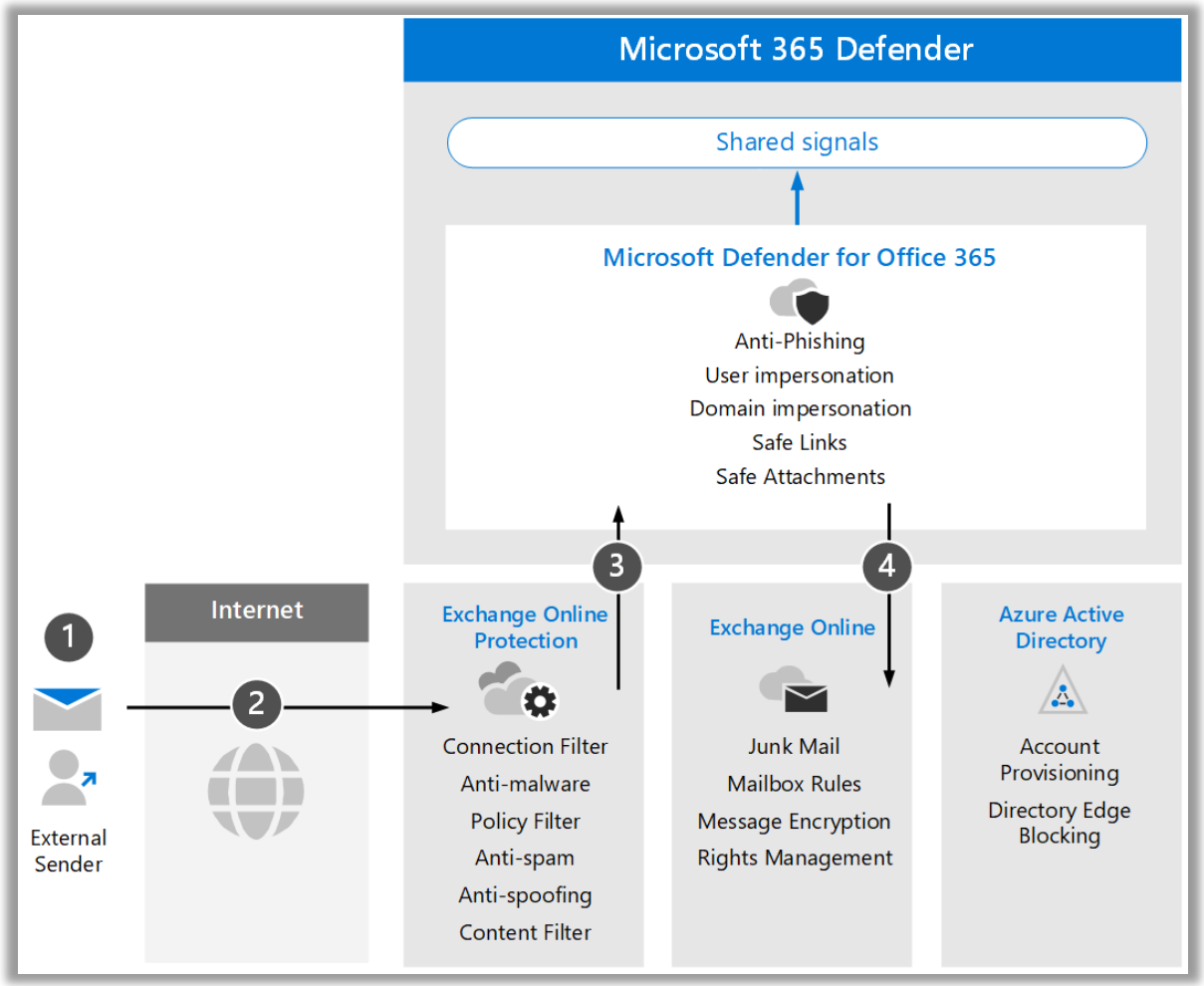
Mail flows & connectors in EXO, EOP and MDO

Complex scenarios and troubleshoot

Sébastien AIMÉ
Security Technical Specialist
Fall 2024

EOP versus MDO

Reminder



Exchange Online Protection

Built-in and basic protection for collaboration stack.
Technical mail flow and attachments analysis.
Effective on "technical-only" threats.

Microsoft Defender for Office 365

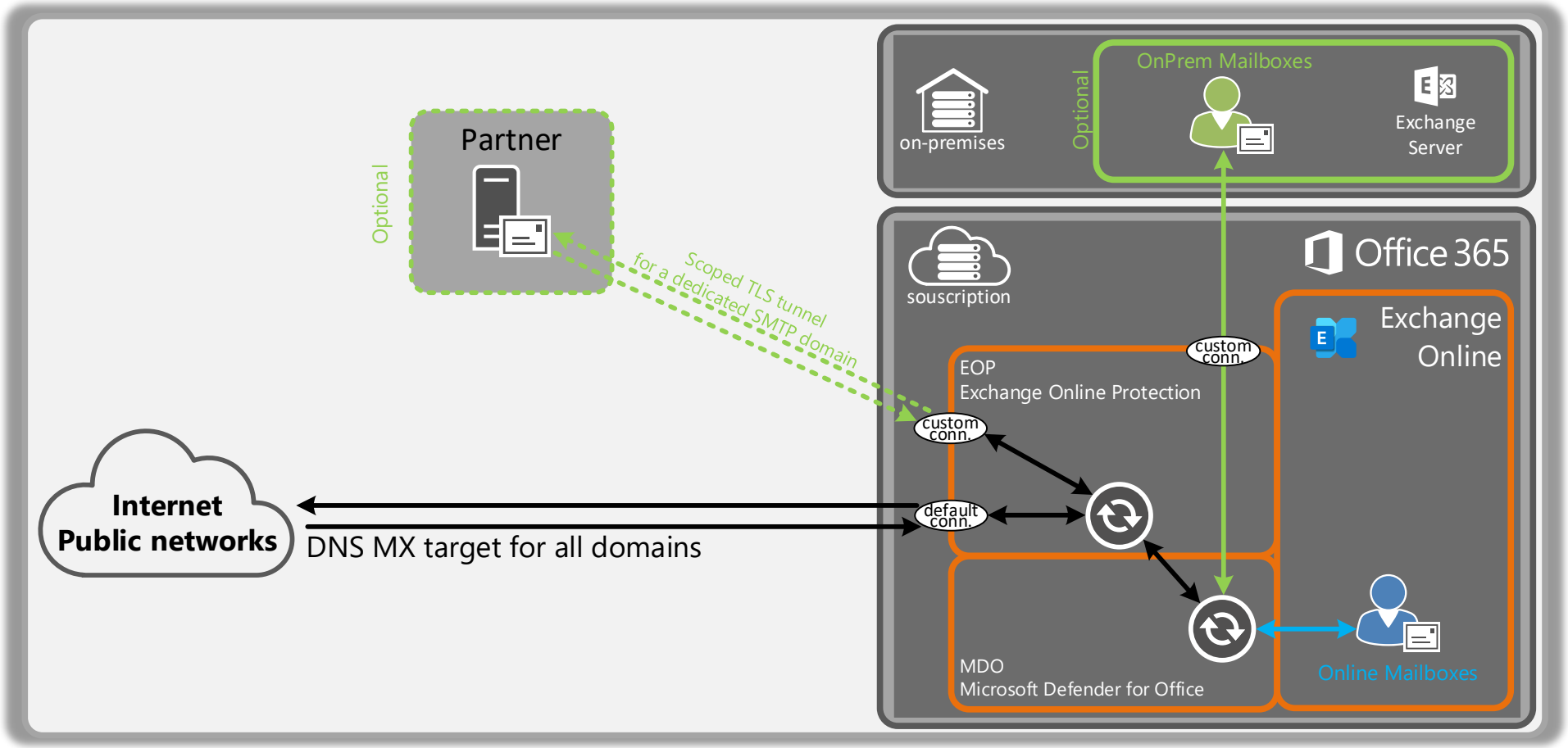
Advanced protection for collaboration stack.
Technical and tricky mail flow, attachments, uploaded files and URLs analysis.
Effective on campaign and spear threats.

Microsoft learn reference

Typical deployment
with typical options

Typical deployment

Exchange Hybrid and Partner tunnels deployments are optional but commonly used



Exchange Online is ready to send and receive email from the internet right away. **Default connectors are implicit and invisible.**

EOP and MDO work together:
Depending on the security feature, messaging hygiene may be handled by EOP (basic checks) or MDO (modern features and deep checks).

Configure mail flow using connectors in Exchange Online

Key takeaways

Behaviors

Routing	-Default in and out connectors are implicit, invisible and not customizable.	Microsoft Learn
	-Routing intelligence only handled at the EOP level by the objects directory (EntraID) also called the GAL – Global Address List.	Microsoft Learn
	-Optionally, dedicated connectors can be used to enhance the mail flow's security with a partner or an Exchange On-Premises platform.	Microsoft Learn
Hygiene	-Hygiene handled by both EOP and MDO depending on the filtering technology used	Microsoft Learn
	-Anti-malware signatures checks are mandatory and can not be disabled.	
Direct internet facing	-Microsoft highly recommends EOP (and therefore MDO) in front of the internet (MX target) to be fully able to resolve the previous smarthost, analyze the SMTP headers integrity etc.	Microsoft Learn
	-Who is sending the message, the IP address of the server that originally sent the message, and the behavior of the connecting mail server, all help determine whether a message is legitimate or spam.	Microsoft Learn

Specific case of MX targetting OnPrem is out-of-scope of this deck

Multi-Layered protection stack

** Components unique to MDO*

*** Enhanced/Additional items unique to MDO*

Increasing cost

Edge protection

- Network throttling
- IP reputation/throttling
- Domain reputation
- Directory-based edge filtering
- Backscatter detection
- Enhanced filtering for on-prem routing

Sender intelligence

- Account compromise detection
- DMARC DKIM, SPF, ARC
- Intra-org spoof intelligence
- Cross-domain spoof intelligence
- Bulk filtering
- Brand Impersonation
- Mailbox intelligence
- Mailbox intelligence impersonation *
- User impersonation *
- Domain impersonation * (micr0soft.com)

Content filtering

- Transport custom rules
- AV engines
- Type blocking
- Attachment reputation blocking
- Clustering and fingerprints
- ML models **
- Tenant allow/block lists
- URL reputation blocking
- Content heuristics
- Image processing **
- Safe attachments *
- Linked content detonation *
- URL detonation *

Post-delivery protection

- Safe links *
- Phish zero-hour auto-purge **
- Malware zero-hour auto-purge **
- Spam zero-hour auto-purge **
- Campaigns **
- End-user reporting **
- Office clients *
- OneDrive/SharePoint *
- URL detonation *
- Investigations and Hunting *

[Step-by-step threat protection stack in Microsoft Defender for Office 365]

Need some tech ?

❤️ PowerShell ❤️

Connectors overview

Identify the connectors available within your subscription.

Brand new tenant connectors overview (defaults are not visible):

```
PS C:\> Get-InboundConnector
PS C:\> Get-OutboundConnector
PS C:\>
```

Connectors overview with optional components (hybrid+partner):

```
PS C:\> Get-InboundConnector
Name                                          SenderDomains SenderIPAddresses Enabled
----                                          ------------- ----------------- -------
PARTNER - custom.domain                       {}            {}                True
Inbound from 4b2d737d-1c31-4506-923f-ec361b0425c1 {smtp:*;1}    {}                True

PS C:\> Get-OutboundConnector
Name                                         RecipientDomains SmartHosts        Enabled
----                                         ---------------- ----------        -------
Outbound to 4b2d737d-1c31-4506-923f-ec361b0425c1 {[redacted]}     {[redacted]]} True
```

Connectors selection

```
PS C:\> Get-InboundConnector | select Name,ConnectorType,SenderIPAddresses,SenderDoma
ins,AssociatedAcceptedDomains,RequireTls,RestrictDomainsToIPAddresses,RestrictDomains
ToCertificate,TlsSenderCertificateName


Name                          : PARTNER - custom.domain
ConnectorType                 : Partner
SenderIPAddresses             : {}
SenderDomains                 : {}
AssociatedAcceptedDomains     : {[redacted]}
RequireTls                    : True
RestrictDomainsToIPAddresses  : False
RestrictDomainsToCertificate  : True
TlsSenderCertificateName      : [redacted]

Name                          : Inbound from 4b2d737d-1c31-4506-923f-ec361b0425c1
ConnectorType                 : OnPremises
SenderIPAddresses             : {}
SenderDomains                 : {smtp:*;1}
AssociatedAcceptedDomains     : {}
RequireTls                    : True
RestrictDomainsToIPAddresses  : False
RestrictDomainsToCertificate  : True
TlsSenderCertificateName      : [redacted]
```

#1

#2

Connectors are evaluated using the most restrictive criteria that better fit.

Few criteria are evaluated to do this:

-ConnectorType (mostly for specific Exchange Hybrid scenarios)
-RestrictDomainsToIPAddresses so therefore *SenderIPAddresses* value
-RestrictDomainsToCertificate so therefore *TlsSenderCertificateName* value
-AssociatedAcceptedDomains so directly linked to the *AcceptedDomains* set within the tenant.
-RequireTLS about the connection security state.

Need some tech ?

❤️ PowerShell ❤️

Connector selection validation #1

Connectors are evaluated using the most restrictive criteria that better fit. To ensure that the appropriate connector is selected, you can use the following PowerShell method:

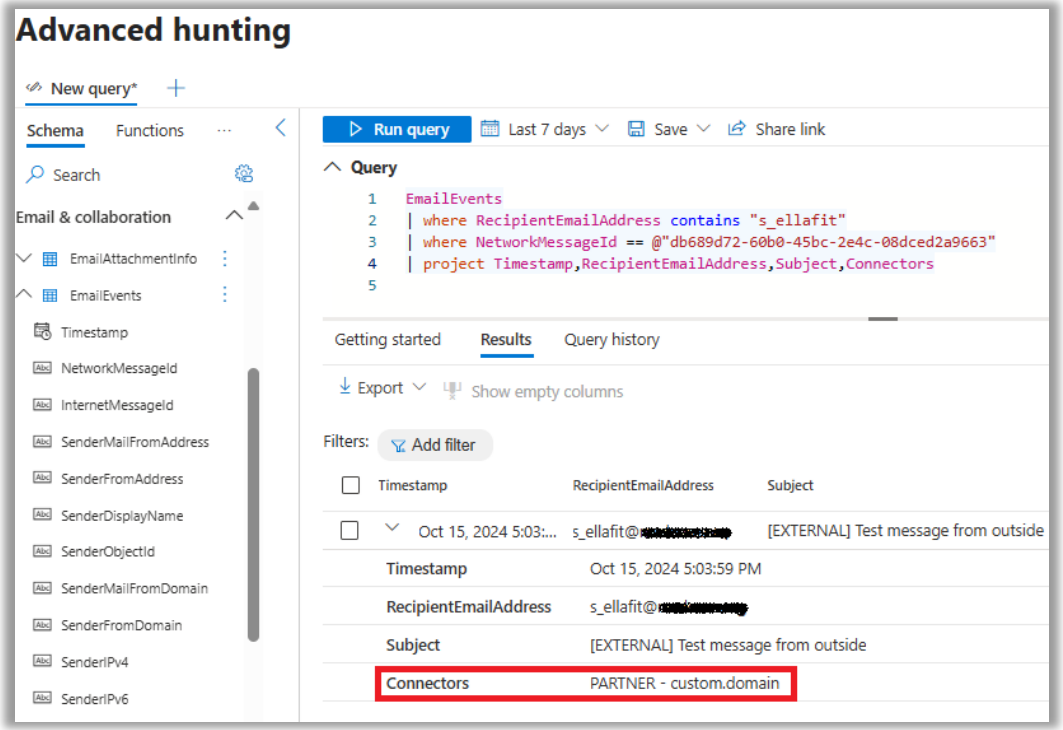
```
PS C:\> Get-MessageTrace -StartDate (Get-Date).AddDays(-1) -EndDate (Get-Date) -SenderAddress sender.external@[redacted] -S
tatus Delivered | ft MessageTraceId,RecipientAddress,Subject,Status

MessageTraceId                       RecipientAddress     Subject                          Status
--------------                       ----------------     -------                          ------
db689d72-60b0-45bc-2e4c-08dced2a9663 s_ellafit@[redacted] [EXTERNAL] Test message from outside Delivered


PS C:\> (Get-MessageTraceDetail -MessageTraceId db689d72-60b0-45bc-2e4c-08dced2a9663 -RecipientAddress s_ellafit@[redacted]
 -Event "RECEIVE").Data
<root><MEP Name="ConnectorId" String="IA1PR10MB7538\Default IA1PR10MB7538"/><MEP Name="ClientIP" String="2603:10b6:5:1f4::3
9"/><MEP Name="ServerHostName" String="IA1PR10MB7538.namprd10.prod.outlook.com"/><MEP Name="FirstForestHop" String="IA1PR10
MB7538.namprd10.prod.outlook.com"/><MEP Name="DeliveryPriority" String="Normal"/><MEP Name="ReturnPath" String="sender.exte
rnal@[redacted]"/><MEP Name="CustomData" Blob="S:ProxyHop1=DS3PEPF000099DC.mail.protection.outlook.com(10.167.17.198);S:Pro
xyHop2=DM6PR02CA0098.outlook.office365.com(2603:10b6:5:1f4::39);'S InboundConnectorData=Name=PARTNER - custom.domain Connec
torType=Partner;TenantId=4741b2d7-7af7-4dae-b649-934962f52f13';S:tlsversion=SP_PROT_TLS1_2_SERVER;S:tlscipher=CALG_AES_256;
S:ProxiedClientIPAddress=98.66.160.162;S:ProxiedClientHostname=[redacted]"/><MEP Name="SequenceNumber" Long="0"/><MEP
 Name="RecipientReference" String=""/></root>
PS C:\>
```

If you can't see any *InboundConnectorData* tag:
Default Connectors has been used to route the current message.

```
PS C:\> (Get-MessageTraceDetail -MessageTraceId 13ef3559-b9aa-44bf-4470-08dceec3a1f4 -RecipientAddress s_ellafit@[redacted]
)[2].Data
<root><MEP Name="SourceContext" String="08DCEDAADB13F6BC;2024-10-17T15:52:05.672Z;ClientSubmitTime:"/><MEP Name="MailboxSer
ver" String="PH7PR10MB7782.namprd10.prod.outlook.com"/><MEP Name="DeliveryPriority" String="Normal"/><MEP Name="TotalLatenc
y" Integer="9"/><MEP Name="ReturnPath" String="sender.external@[redacted]"/><MEP Name="ClientName" String="DS7PR10MB5069.na
mprd10.prod.outlook.com"/><MEP Name="CustomData" Blob="S:PrioritizationReason=EnvelopePriority"/><MEP Name="SequenceNumber"
 Long="0"/><MEP Name="RecipientReference" String=""/></root>
PS C:\>
```

Connector selection validation #2

KQL queries within the *Advanced Hunting* feature of *Defender XDR* portal is also possible: https://security.microsoft.com



MessageTrace, MessageTraceDetail CmdLets and KQL queries may take few minutes to retrieve the latest datas ...

Advanced deployments
with customizations

Protocols basics

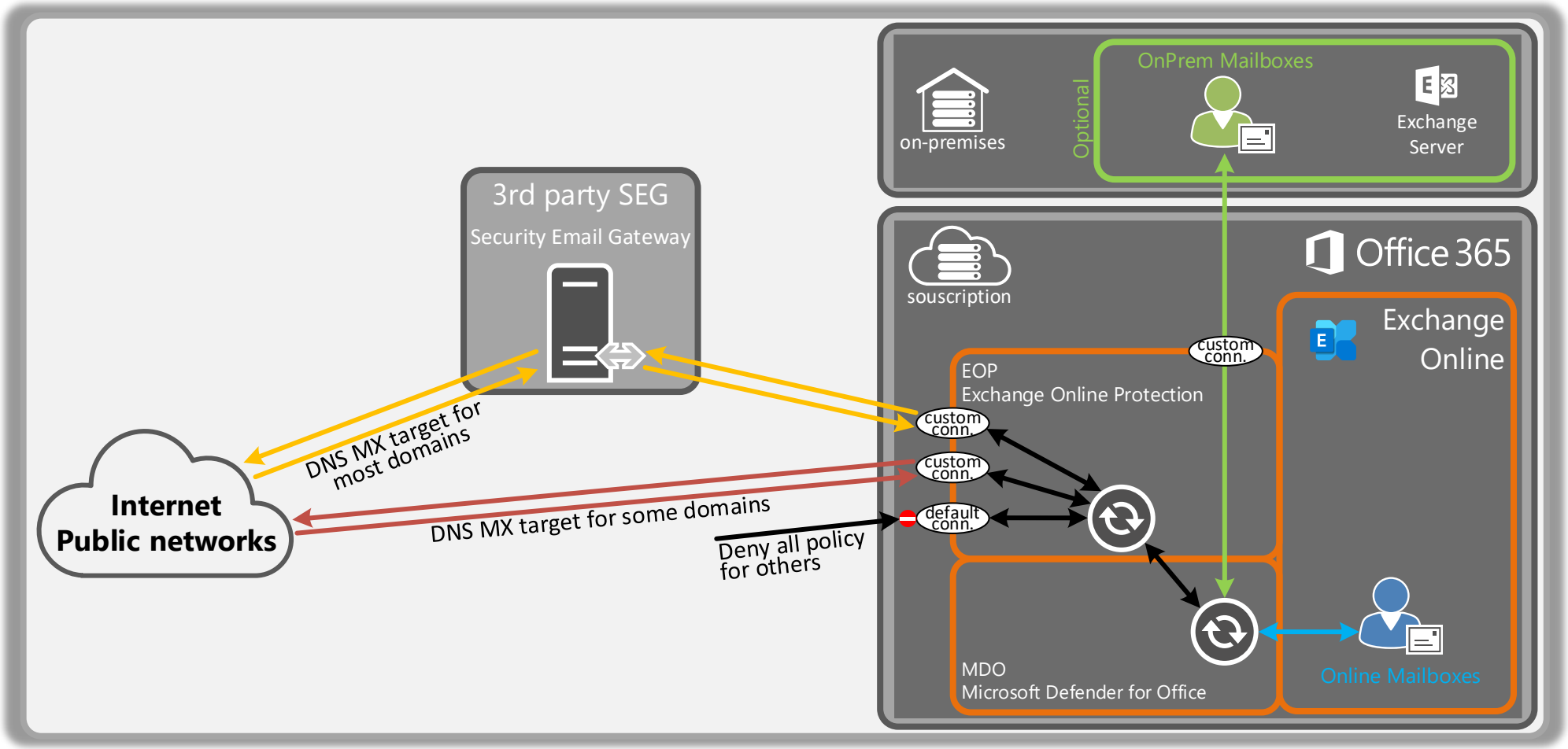
Reminders

Protocol	#RFC	Description
SMTP	8314	The Simple Mail Transfer Protocol (SMTP) is an Internet standard communication protocol for electronic mail transmission.
DKIM	6376	DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in email.
DMARC	7489	Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication protocol designed to give email domain owners the ability to protect their domain from unauthorized use.
ARC	8617	Authenticated Received Chain (ARC) is an email authentication system designed to allow an intermediate mail server like a mailing list or forwarding service to sign an email's original authentication results.

Technical context	SMTP Command	#RFC	Item
SMTP envelope	MAIL FROM	RFC5321	Return address also known as P1 FROM
SMTP envelope	RCPT TO	RFC5321	Delivery address
Email header	FROM	RFC5322	Sender address also known as P2 FROM
Email header	TO	RFC5322	Recipient address
Email header	REPLY-TO	RFC5322	Reply address
Email body	BODY	RFC5322	Message body

Advanced deployment with 3rd party SEG

Complex deployments commonly used with EOP and MDO



-Alternative MX targets for some domains is commonly used for POC or testing scenarios.

-The "DenyAll" policy is often deployed to block direct tenant delivery that could bypass the official SEG (Microsoft Learn)

3rd party SEG highlights

and known bad behaviors

3rd party SEG known side effects

Known side effects to be careful with:
-The *connecting IP* viewed by EOP/MDO may be the SEG's outgoing IP instead of the true sender. → *SPF* will *FAIL* and may induce a *DMARC FAILURE* → This generates a FP (False Positive).
-*DKIM* signature may creates a mismatch with the *FROM* field.
-If messages are updated or modified, the *DKIM* signature can *FAIL.*

Architecture attention points

-A mismatch between the *MAILFROM* and the *FROM* fields may happens in the *authentication-results* header → A clean *SPF* would have saved this message (See side effects).
-SEG dedicated connector (YELLOW) is not always in place (Default connector used).
-Deny all settings (BLACK⛔) to deny all other mail flows not always in place (especially targeting "**.onmicrosoft.com*").
-Sometime dedicated connectors for specific technical domains or sub-domains (RED) in place but *badly scoped.*
-Sometime few additional connectors dedicated to specific app flows that blur the view.

To go further

-Careful with outgoing mail flows that do not take the same outgoing route that the incoming one! Some providers downgrade the trust level if the outgoing IP does not match the DNS MX value.

-Need example ?! → Next slide

Need some tech ? SMTP headers through 3rd party SEG in depth

Received headers

Hop	Submitting host	Receiving host	Time	Delay	
1	localhost (localhost [127.0.0.1])	mail4.sea31.mcsv.net (Mailchimp)	1/18/2024 7:00:07 PM		ESMTP
2	mail4.sea31.mcsv.net (mail4.sea31.mcsv.net [148.105.11.4])	mx0b-00108d02.pphosted.com	18/18/2024 7:01:32 PM	1 minute 25 seconds	ESMTP
3	pps.filterd (m0078984.ppops.net [127.0.0.1])	mx0b-00108d02.pphosted.com (8.16.0.43/8.16.0.43)	1/18/2024 7:01:32 PM	0 seconds	SMTP
4	mx0b-00108d02.pphosted.com (148.163.158.140)	BN1NAM02FT025.mail.protection.outlook.com (10.13.2.139)	1/18/2024 7:01:32 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
5	BN1NAM02FT025.eop-nam02.prod.protection.outlook.com (2603:10b6:404:151ﾈ)	BN6PR20CA0070.outlook.office365.com (2603:10b6:404:151::32)	1/18/2024 7:01:33 PM	1 second	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
6	BN6PR20CA0070.namprd20.prod.outlook.com (2603:10b6:404:151::32)	MWHPR05MB3246.namprd05.prod.outlook.com (2603:10b6:300:b2::15)	1/18/2024 7:01:33 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
7	NAM10-DM6-obe.outbound.protection.outlook.com (104.47.58.103)	SN1NAM02FT0046.mail.protection.outlook.com (10.97.5.4)	1/18/2024 7:01:35 PM	2 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
8	SN1NAM02FT0046.eop-nam02.prod.protection.outlook.com (2a01:111:e400:fc4a::)	SN1NAM02HT0021.eop-nam02.prod.protection.outlook.com (2a01:111:.::201)	1/18/2024 7:01:35 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)

SuperTool Beta9

mail4.sea31.mcsv.net:148.105.11.4 — SPF Record Lookup

spf:mail4.sea31.mcsv.net:148.105.11.4 — Find Problems — Solve Email Delivery Problems

```
v=spf1 ip4:148.105.11.4 include:spf.mandrillapp.com -all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	148.105.11.4	Pass	Match if IP is in the given range.
+	include	spf.mandrillapp.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

Other headers

#	Header	Value
1	Authentication-Results	spf=fail (sender IP is 148.163.158.140) smtp.mailfrom=mail4.sea31.mcsv.net; dkim=fail (body hash did not verify) header.d=contoso.com; dmarc=fail action=oreject header.from=contoso.com; compauth=fail reason=000
2	Received-SPF	Fail (protection.outlook.com: domain of mail4.sea31.mcsv.net does not designate 148.163.158.140 as permitted sender) receiver=protection.outlook.com; client-ip=148.163.158.140; helo=mx0b-00108d02.pphosted.com;
3	Authentication-Results-Original	northwindtraders.com; spf=pass smtp.mailfrom=bounce-mc.us19_104887398.6217408-29f16e68f8@mail4.sea31.mcsv.net; dkim=pass header.d=contoso.com header.s=k2; dmarc=pass
4	DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=contoso.com; s=k2; t=1629307707; i=info=3Dcontoso.com@mcsv.net; bh=QvNMBhCTadpyUxqmAt13Ar0vkNZN0hKPnDZJ7zSnfMA=; h=Subject:From:Reply-To:To:Date:Message-ID: w02Ii9UPwuZCZI9kSL7KAQzdQaQIb733cNVGycHQVKz/UZD4dotS PFJQDNXeBez0/2ZI5jwI7C0rOIce8mRE0PgJw56566yHaVcI+ueHhvBBSDL+I jF89h4huOYGLxspXxbopQYhA4I9HgyGZMaVRI97BCk+RVdGWJIcmeZhoS8an+Me WEV9ws7cgq8LT/IS8YsYM9nbap9/LXWZbqIAWpV4eR+Ss8GETx61znRIIjG1BAzoS4 Iyz2fqS/5pCRg==

Known side effects

- Incoming connecting IP used by EOP/MDO to run security checks → Wrong IP → SPF **FAIL**
- True connecting IP is the one before the SEG → Should be used to run security checks → Using this SPF, result would be **PASS**
- DKIM and the FROM do align → DKIM could save this message from a **DMARC failure**
- DKIM failed (body hash didn't verify) → Message likely modified in transit ?

Attention points

- MAILFROM and FROM don't align → SPF alone can't save this message from a DMARC failure
- This message looks to also have left the tenant and come back in → More filtering somewhere (TR?) ?

Enhanced Filtering and/or ARC seal

How could this help ?

Why

- **Authenticated Received Chain (ARC)** should typically be used along the delivery chain to maintain message integrity using DKIM and arbitrary enhance the chain trust level → However, DKIM frequently fails because many services that modify the message don't support ARC.

-**Enhance Filtering (EF)** primarily supports the ability for EOP/MDO to understand the **true** connecting IP address and provides accurate SPF checks. **EF** also shows appropriate source IP information in hunting experiences, detection technologies etc.

When

- **ARC** helps reduce inbound email authentication failures from message modification by legitimate email services along the way. **ARC** preserves the original email authentication information at the email service and allows downstream smarthosts to re-use it → **ARC capable** smarthosts needed.

- **EF** should be used on the connector accepting messages from a 3rd party SEG in front of the Internet, along with **ARC** if supported → An **EOP dedicated connector** is needed.

How

- **ARC** can be GUI enabled using the security portal: https://security.microsoft.com/authentication
or through PowerShell using **Get-ArcConfig** / **Set-ArcConfig** CmdLets.

- **EF** can be GUI enabled using the security portal: https://security.microsoft.com/skiplisting
or through PowerShell using **Set-InboundConnector -EFSkipLastIP $true -EFSkipIP x.x.x.x** CmdLet.

-**Composite Authentication (CompAuth)** value is used by Microsoft 365 to combine multiple types of authentication (SPF, DKIM, and DMARC), or any other part of the message to determine whether or not the message is authenticated.

Composite authentication

Configure trusted ARC sealers

Enhanced filtering for connectors in Exchange Online

Need some tech ? SMTP headers through 3rd party SEG in depth and EF enabled

Received headers

Hop	Submitting host	Receiving host	Time	Delay	Type
1	localhost (localhost [127.0.0.1])	mail4.sea31.mcsv.net (Mailchimp)	1/18/2024 7:00:07 PM		ESMTP
2	mail4.sea31.mcsv.net (mail4.sea31.mcsv.net [148.105.11.4])	mx0b-00108d02.pphosted.com	18/18/2024 7:01:32 PM	1 minute 25 seconds	ESMTP
3	pps.filterd (m0078984.ppops.net [127.0.0.1])	mx0b-00108d02.pphosted.com (8.16.0.43/8.16.0.43)	1/18/2024 7:01:32 PM	0 seconds	SMTP
4	mx0b-00108d02.pphosted.com (148.[illegible].140)	BN1NAM02FT025.mail.protection.outlook.com (10.13.2.139)	1/18/2024 7:01:32 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
5	BN1NAM02FT025.eop-nam02.prod.protection.outlook.com (2603:10b6:404:151[illegible])	BN6PR20CA0070.outlook.office365.com (2603:10b6:404:151::32)	1/18/2024 7:01:33 PM	1 second	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
6	BN6PR20CA0070.namprd20.prod.outlook.com (2603:10b6:404:151::32)	MWHPR05MB3246.namprd05.prod.outlook.com (2603:10b6:300:b2::15)	1/18/2024 7:01:33 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
7	NAM10-DM6-obe.outbound.protection.outlook.com (104.47.58.103)	SN1NAM02FT0046.mail.protection.outlook.com (10.97.5.4)	1/18/2024 7:01:35 PM	2 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
8	SN1NAM02FT0046.eop-nam02.prod.protection.outlook.com (2a01:111:e400:fc4a::)	SN1NAM02HT0021.eop-nam02.prod.protection.outlook.com (2a01:111:.::201)	1/18/2024 7:01:35 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)

Other headers

#↕	Header	Value
1	Authentication-Results	spf=pass (sender IP is 148.105.11.4) smtp.mailfrom=mail4.sea31.mcsv.net; dkim=fail (body hash did not verify) header.d=contoso.com; dmarc=fail action=oreject header.from=contoso.com; compauth=none reason=920
2	Received-SPF	Pass (protection.outlook.com: domain of mail4.sea31.mcsv.net designates 148.105.11.4 as permitted sender) receiver=protection.outlook.com; client-ip=148.105.11.4; helo=mail4.sea31.mcsv.net;
3	Authentication-Results-Original	northwindtraders.com; spf=pass smtp.mailfrom=bounce-mc.us19_104887398.6217408-29f16e68f8@mail4.sea31.mcsv.net; dkim=pass header.d=contoso.com header.s=k2; dmarc=pass
4	DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=contoso.com; s=k2; t=1629307707; i=info=3Dcontoso.com@mcsv.net; bh=QvNMBhCTadpyUxqmAt13Ar0vkNZN0hKPnDZJ7zSnfMA=; h=Subject:From:Reply-To:To:Date:Message-ID:List-ID: w02Ii9UPwuZCZI9kSL7KAQzdQaQIb733cNVGycHQVKz/UZD4dotS PFJQDNXeBez0/2ZI5jwI7C0rOlce8mRE0PgJw56566yHaVcI+ueHhvBBSDL+I jF89h4huOYGLxspXxbopQYhA4I9HgyGZMaVRI97BCk+RVdGWJIcmeZhoS8an+MeMMA N WEV9ws7cgq8LT/IS8YsYM9nbap9/LXWZbqIAWpV4eR+Ss8GETx61znRIIjG1BAzoS4 Iyz2fqS/5pCRg==
5	X-MS-Exchange-ExternalOriginalInternetSender	ip=[148.105.11.4];domain=mail4.sea31.mcsv.net
6	X-MS-Exchange-SkipListedInternetSender	ip=[148.105.11.4];domain=mail4.sea31.mcsv.net

Key takeaway

- DNS MX targets the 3rd party SEG and ***EF*** is enabled for this incoming mailflow in EOP/MDO.
- ***DMARC/DKIM*** fails but ***ALIGNED***.
- In this situation ***COMPAUTH*** result is ***NONE*** and reason code is ***460*** or ***920***.