



# Exchange User Group Meetup Q4 2024 {Hybrid Edition}

12. Dezember 2024

# Location Sponsor



<https://www.computacenter.com>

# Sponsor



Monitoring Lösungen für  
Microsoft 365 – Exchange Online – Teams  
Exchange Server – Active Directory

Entra Enterprise App-Bewertung  
mit AppGov Score

<https://www.enowsoftware.com>

# Meetup Q3 2024



---

**Viele Wege führen zum... M365 Audit Log**  
→ Andres Bohren

---

**Exchange Server Hybrid & Konnektorsicherheit**  
→ Thomas Stensitzki

---

**Exchange Q & A**

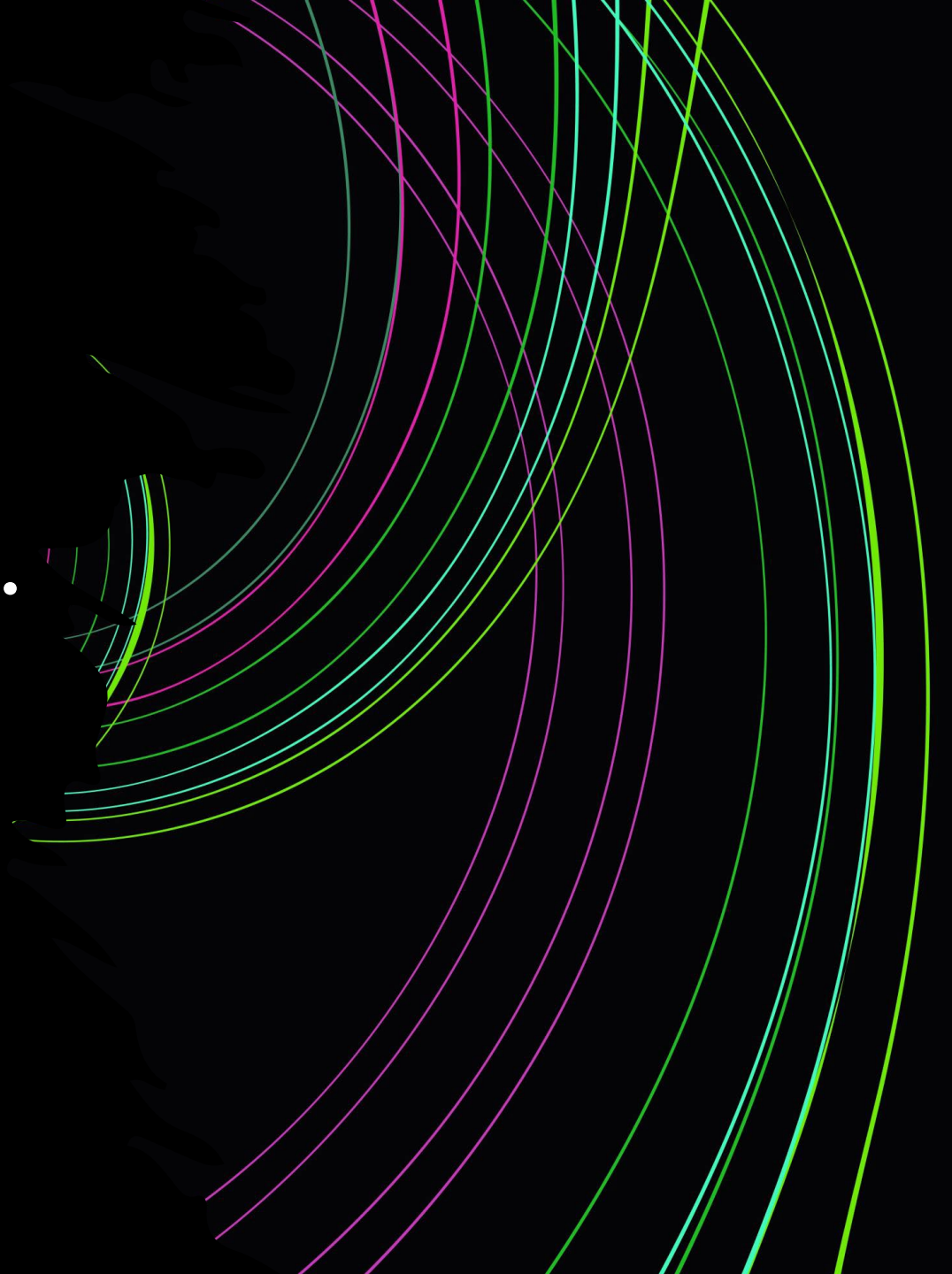


# Viele Wege führen zum...

## M365 Audit Log

Andres Bohren

Meetup Q4 2024



# Exchange Server Hybrid & Konnektorsicherheit

Schwerpunkt EXO → On-Premises

Thomas Stensitzki

Meetup Q4 2024



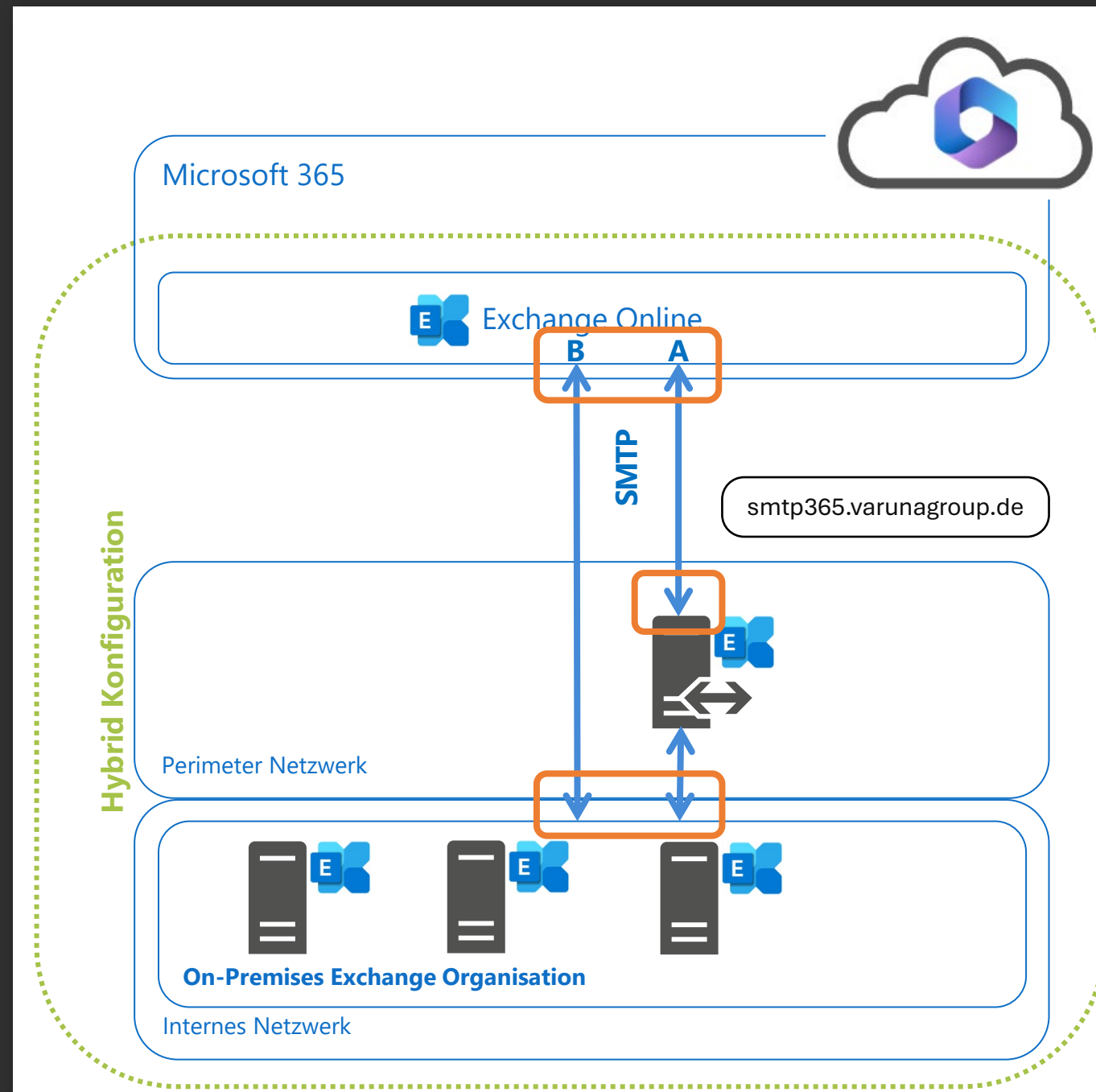
# Exchange Hybrid

## Die SMTP-Seite von Exchange Hybrid

SMTP-Verbindung zwischen On-Premises und Exchange Online

- Separater Hostname (z.B. smtp365.varunagroup.de)
- Zusätzliche öffentliche IP-Adresse
- TLS-Zertifikat für Hostnamen
- (A) **Edge Transport-Rolle** im Perimeter Netzwerk
- (B) Alternativ **direkte** eingehende Verbindung

Fehlt etwas?



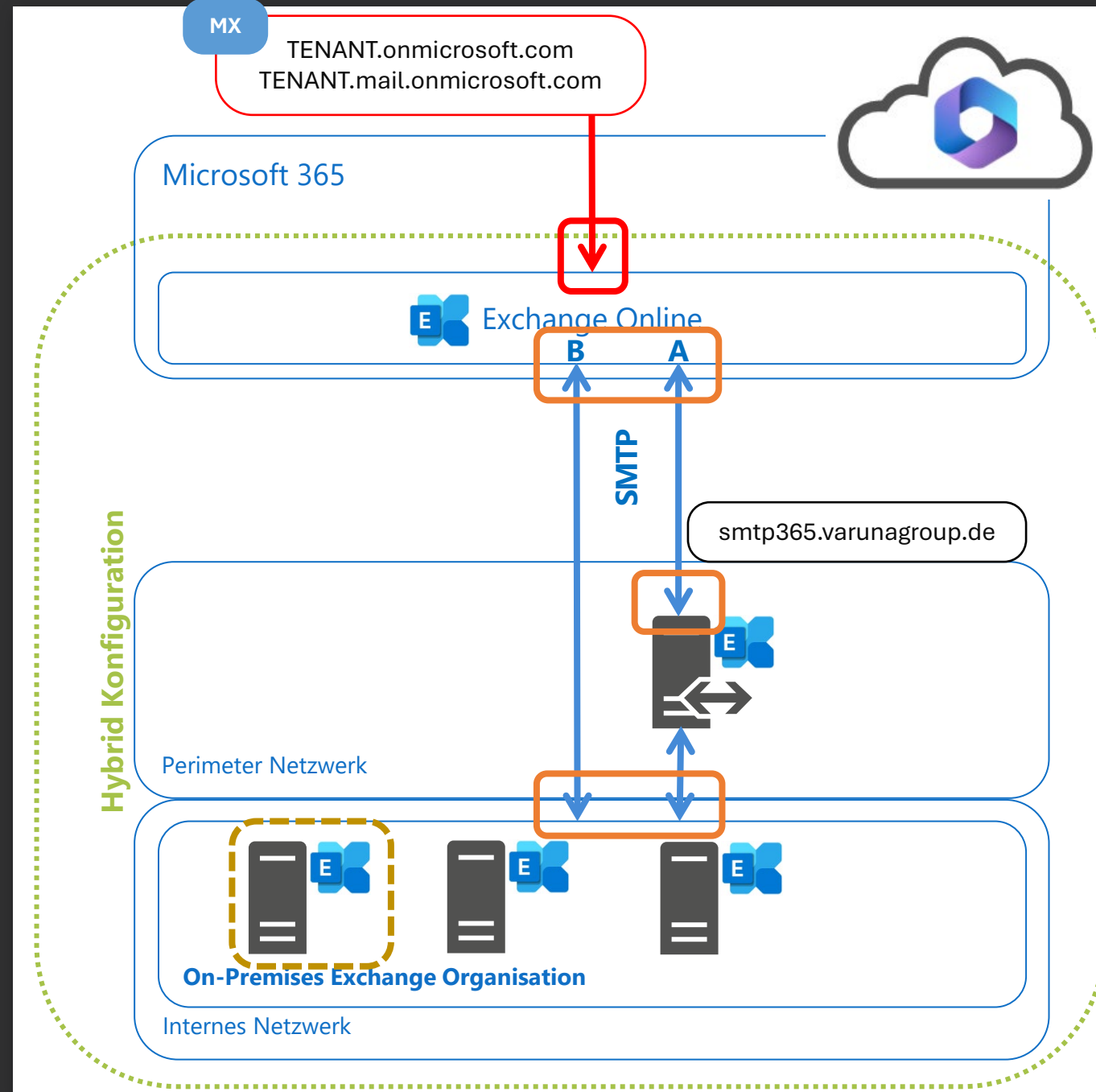
# Exchange Hybrid

## Die SMTP-Seite von Exchange Hybrid

Exchange Online-Konnektoren für die Mandanten-Domänen  
(Standardkonnektor = unsichtbar)

- TENANT.onmicrosoft.com
- TENANT.mail.onmicrosoft.com

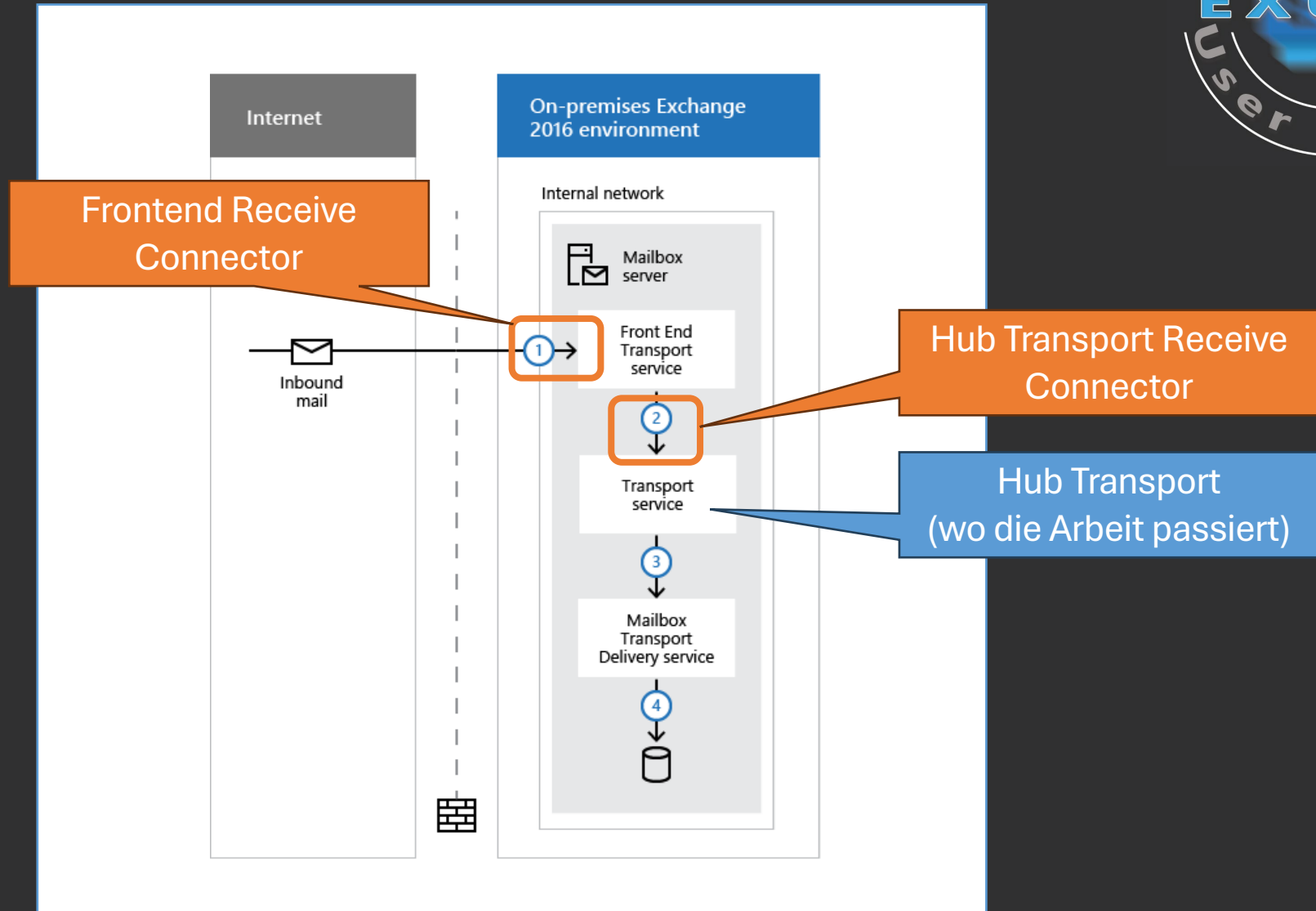
→ Exchange Online Seiteneingang über Standard MX-Records kontrolliert von Microsoft





# Nachrichtenfluss



## Postfach Server



# Nachrichtenfluss

## Postfach Server Empfangskonnektoren



Identity	Bindings	Enabled	
-----	-----	-----	
testms05\ <b>Client Frontend</b> TESTMS05	{[::]:587, 0.0.0.0:587}	True	 <b>Frontend</b>
testms05\ <b>Client Proxy</b> TESTMS05	{[::]:465, 0.0.0.0:465}	True	
testms05\ <b>Default Frontend</b> TESTMS05	{[::]:25, 0.0.0.0:25}	True	 <b>Hub Transport</b>
testms05\ <b>Default</b> TESTMS05	{0.0.0.0:2525, [::]:2525}	True	
testms05\ <b>Outbound Proxy Frontend</b> TESTMS05	{[::]:717, 0.0.0.0:717}	True	

# Nachrichtenfluss

## Postfach Server

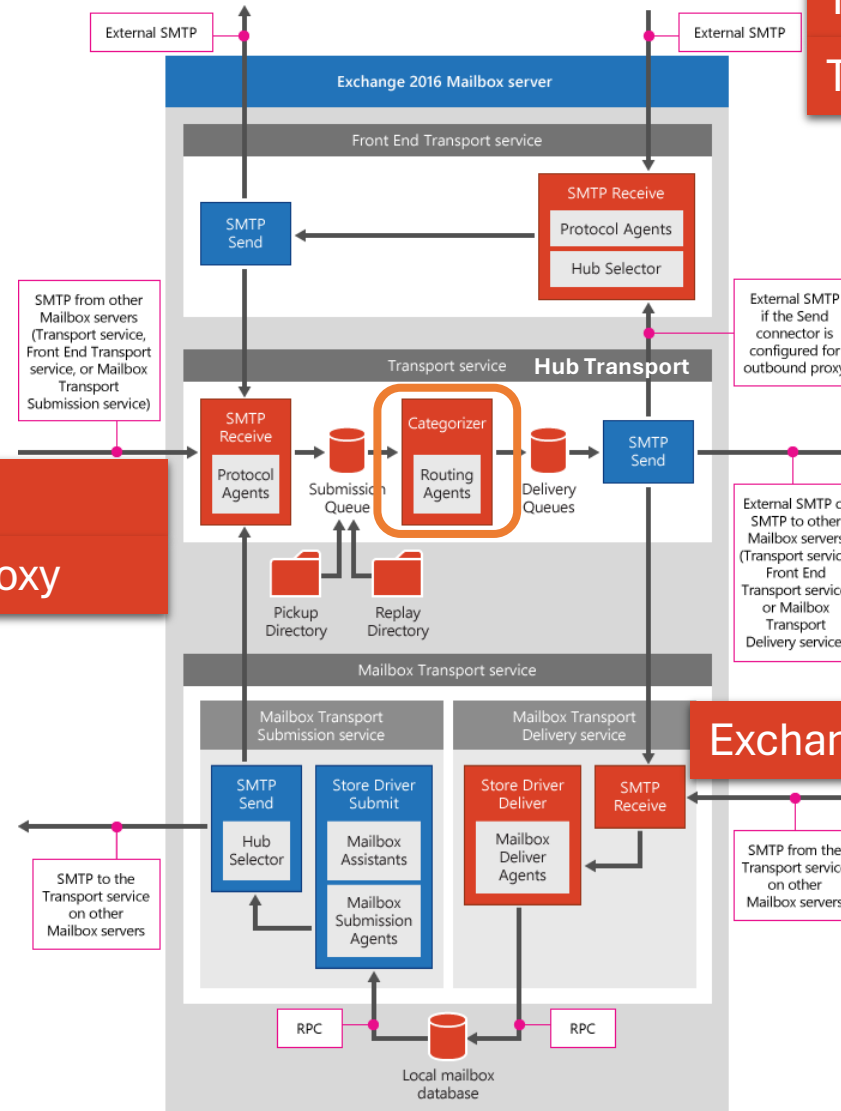


TCP 25 – Default Frontend  
TCP 587 – Client Frontend

TCP 717 – Outbound Proxy Frontend

TCP 2525 – Default  
TCP 465 – Client Proxy

Exchange Internal Receive Connector



Machine: testms05.varunagroup.de

```
[PS] E:\SCRIPTS>Get-ReceiveConnector -Server testms05 | Sort-Object Name
```

Identity	Bindings	Enabled
testms05\Client Frontend TESTMS05	{[::]:587, 0.0.0.0:587}	True
testms05\Client Proxy TESTMS05	{[::]:465, 0.0.0.0:465}	True
testms05\Default Frontend TESTMS05	{[::]:25, 0.0.0.0:25}	True
testms05\Default TESTMS05	{0.0.0.0:2525, [::]:2525}	True
testms05\Outbound Proxy Frontend TESTMS05	{[::]:717, 0.0.0.0:717}	True

# Empfangskonnektor – Details

## Default Frontend

### Remote IP-Adressräume

- Alle IPv4-Adressen
- Alle IPv6-Adressen

### Bindungen

- Alle Netzwerkadapter
- Alle lokalen IP-Adressen

### FQDN

- Vollqualifizierter Servername
- Identisch zum Exchange-Zertifikat



Exchange-Empfangskonnektor - Profile 1 - Microsoft Edge

https://mail.varunagroup.de/ecp/ConnectorMgmt/EditReceiveConnector.aspx?pwmcid=3&ReturnObjectT...

### Default Frontend TESTMS05

Allgemein  
Sicherheit  
► Bereichsdefinition

\*Remotenetzeinstellungen:  
E-Mail von Servern mit diesen Remote-IP-Adressen empfangen.

+ ✎ -

IP-ADRESSEN
0.0.0.0-255.255.255.255

\*Netzwerkadapterbindungen:  
Geben Sie die IP-Adressen und den Port des Netzwerkadapters für die Bindung an den Empfangskonnektor an.

+ ✎ -

IP-ADRESSEN	PORT
(Alle verfügbaren IPv6)	25
(Alle verfügbaren IPv4)	25

FQDN:  
Geben Sie den FQDN an, den dieser Connector als Antwort auf HELO oder EHLO bereitstellen soll.

testms05.varunagroup.de

Speichern Abbrechen

# Empfangskonnektor – Details

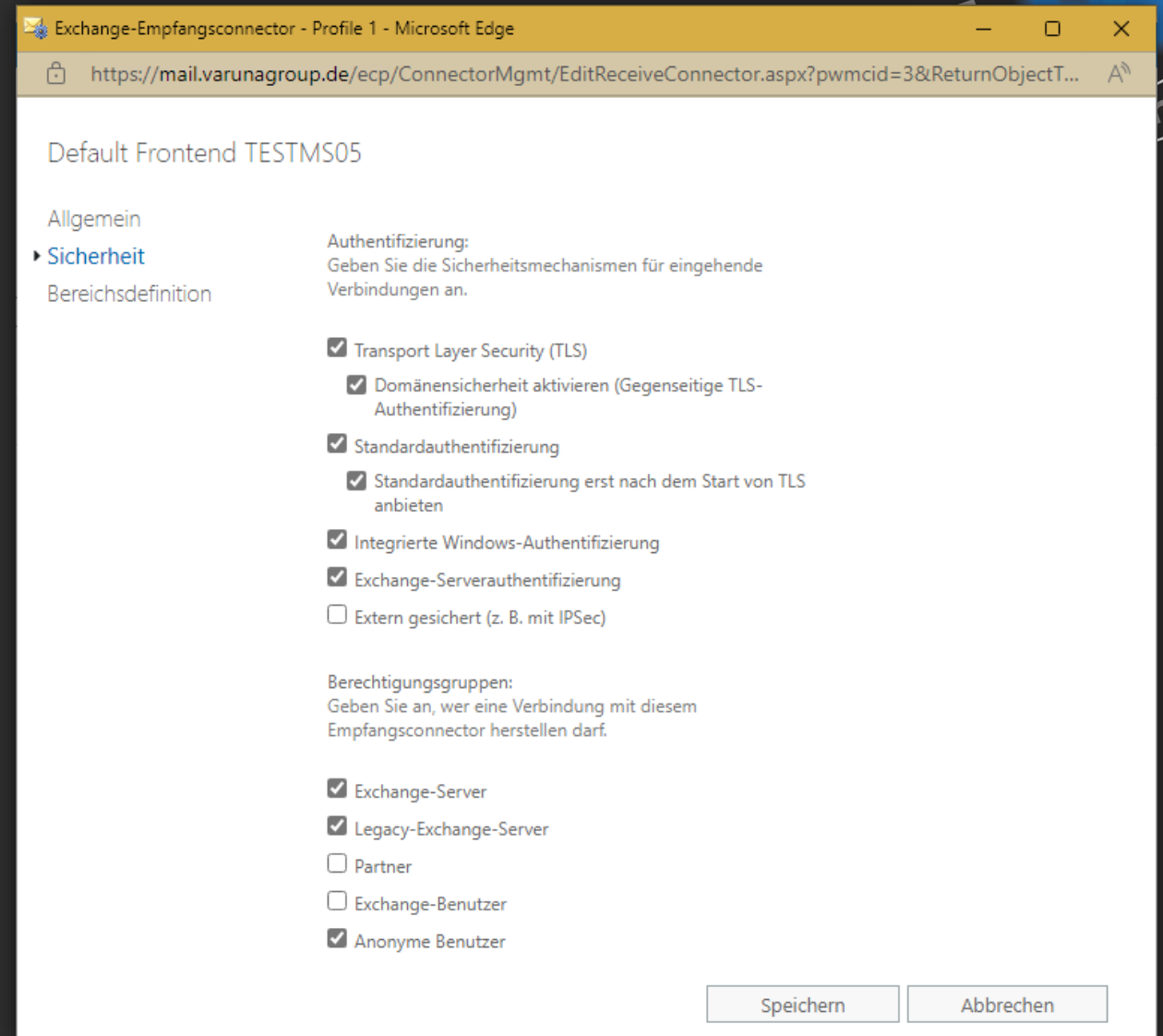
## Default Frontend

### Authentifizierung

- Wie darf sich ein anderes System gegenüber dem Exchange Server authentifizieren

### Berechtigungsgruppen

- Vordefinierte Zustellung von SMTP-Berechtigungen für die Zustellungen von E-Mail-Nachrichten



Exchange-Empfangskonnektor - Profile 1 - Microsoft Edge

https://mail.varunagroup.de/ecp/ConnectorMgmt/EditReceiveConnector.aspx?pwmcid=3&ReturnObjectT...

### Default Frontend TESTMS05

Allgemein

► **Sicherheit**

Bereichsdefinition

Authentifizierung:  
Geben Sie die Sicherheitsmechanismen für eingehende Verbindungen an.

- ☒ Transport Layer Security (TLS)
  - ☒ Domänensicherheit aktivieren (Gegenseitige TLS-Authentifizierung)
- ☒ Standardauthentifizierung
  - ☒ Standardauthentifizierung erst nach dem Start von TLS anbieten
- ☒ Integrierte Windows-Authentifizierung
- ☒ Exchange-Serverauthentifizierung
- ☐ Extern gesichert (z. B. mit IPSec)

Berechtigungsgruppen:  
Geben Sie an, wer eine Verbindung mit diesem Empfangskonnektor herstellen darf.

- ☒ Exchange-Server
- ☒ Legacy-Exchange-Server
- ☐ Partner
- ☐ Exchange-Benutzer
- ☒ Anonyme Benutzer

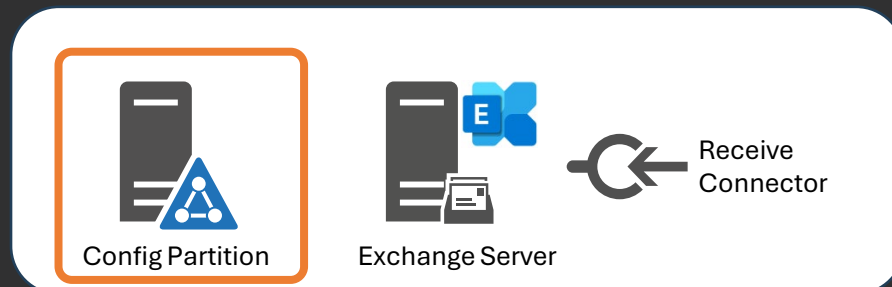
Speichern Abbrechen

# Empfangskonnektor – Details

## Default Frontend

Vereinfachte Darstellung in EAC und PowerShell

- Speicherort der Einstellungen ist die Active Directory Config Partition
- Voraussetzung für /Mode:RecoverServer



```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-ReceiveConnector 'testms05\Default Frontend TESTMS05' | fl AuthMechanism,DomainSecureEnabled,PermissionGroups,RemoteIPRanges,Bindings,Fqdn

AuthMechanism      : Tls, Integrated, BasicAuth, BasicAuthRequireTLS, ExchangeServer
DomainSecureEnabled : True
PermissionGroups    : AnonymousUsers, ExchangeServers, ExchangeLegacyServers
RemoteIPRanges      : {::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, 0.0.0.0-255.255.255.255}
Bindings            : {[::]:25, 0.0.0.0:25}
Fqdn                 : testms05.varunagroup.de
```

The screenshot shows the 'Allgemein' (General) tab of the 'Sicherheitsbereichsdefinition' (Security Area Definition) for a Receive Connector. The 'Authentifizierung' (Authentication) section is highlighted with an orange box, showing the following settings:

- ☒ Transport Layer Security (TLS)
- ☒ Domänensicherheit aktivieren (Gegenseitige TLS-Authentifizierung)
- ☒ Standardauthentifizierung
- ☒ Standardauthentifizierung erst nach dem Start von TLS anbieten
- ☒ Integrierte Windows-Authentifizierung
- ☒ Exchange-Serverauthentifizierung
- ☐ Extern gesichert (z. B. mit IPSec)

The 'Berechtigungsgruppen' (Permissions) section is also highlighted with an orange box, showing the following settings:

- ☒ Exchange-Server
- ☒ Legacy-Exchange-Server
- ☐ Partner
- ☐ Exchange-Benutzer
- ☒ Anonyme Benutzer

Buttons at the bottom include 'Speichern' (Save) and 'Abbrechen' (Cancel).

# Empfangskonnektor – Details

## Default Frontend in Active Directory

Sicherheitseinstellungen  
kontrollieren die SMTP-  
Berechtigungen auf jedem Konnektor

The screenshot shows the ADSI Edit window with the following structure:

- ADSI Edit
- File Action View Help
- Tree view: CN=Servers > CN=testms05 > CN=Protocols > CN=SMTP > CN=SMTP Receive Connectors
- Right pane table:

Name	Class	Distinguished Name
CN=Client Frontend TESTMS05	msExchSmtprReceiveConnector	CN=Client Frontend TESTMS05
CN=Client Proxy TESTMS05	msExchSmtprReceiveConnector	CN=Client Proxy TESTMS05
<b>CN=Default Frontend TESTMS05</b>	<b>msExchSmtprReceiveConnector</b>	<b>CN=Default Frontend TESTMS05</b>
CN=Default TESTMS05	msExchSmtprReceiveConnector	CN=Default TESTMS05
CN=Outbound Proxy Frontend TESTMS05	msExchSmtprReceiveConnector	CN=Outbound Proxy Frontend TESTMS05

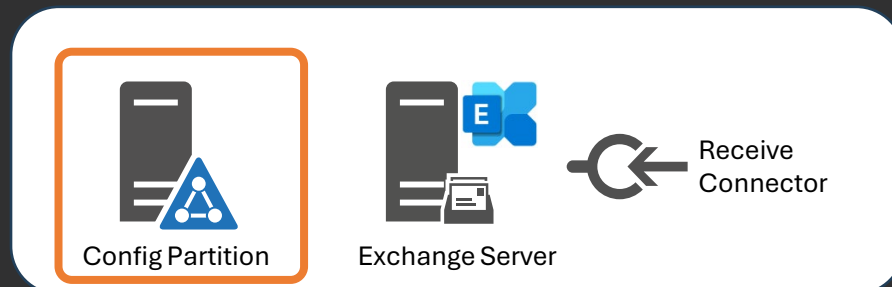
The 'CN=Default Frontend TESTMS05 Properties' dialog box is open, showing the 'Security' tab. The 'Group or user names' list includes:

- Everyone
- SYSTEM
- NETWORK SERVICE
- TST Admin (VARTST@varunagroup.de)
- Organization Management (VARUNAGROUP\Organization Man...)
- Public Folder Management (VARUNAGROUP\Public Folder Ma...)

The 'Permissions for Everyone' table is shown:

Permissions for Everyone	Allow	Deny
Bypass Message Size Limit	<input type="checkbox"/>	<input type="checkbox"/>
Submit Messages for MLS	<input type="checkbox"/>	<input type="checkbox"/>
Submit Messages to any Recipient	<input type="checkbox"/>	<input type="checkbox"/>
Submit Messages to Server	<input type="checkbox"/>	<input type="checkbox"/>
<b>Special permissions</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The 'Special permissions' checkbox is checked. The 'Advanced' button is visible at the bottom right of the dialog.



# Empfangskonnektor – Details

## Default Frontend – Anonymous Logon



Permission Entry for Default Frontend TESTMS05

Principal: ANONYMOUS LOGON [Select a principal](#)

Type: Allow

Permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Accept Routing Headers
<input type="checkbox"/> List contents	<input type="checkbox"/> Accept Xattr
<input type="checkbox"/> Read all properties	<input type="checkbox"/> Accept XMessageContext AD Recipient Cache
<input type="checkbox"/> Write all properties	<input type="checkbox"/> Accept XMessageContext Extended Properties
<input type="checkbox"/> Delete	<input type="checkbox"/> Accept XMessageContext Fast Index
<input type="checkbox"/> Read permissions	<input type="checkbox"/> Accept Xproxy
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Accept XProxyFrom
<input type="checkbox"/> Modify owner	<input type="checkbox"/> Accept XProxyTo
<input type="checkbox"/> All validated writes	<input type="checkbox"/> Accept XSessionParams
<input type="checkbox"/> All extended rights	<input type="checkbox"/> Accept XShadow
<input type="checkbox"/> Accept any Sender	<input type="checkbox"/> Accept XSysProbe
<input type="checkbox"/> Accept Authentication Flag	<input type="checkbox"/> Bypass Anti-Spam
<input type="checkbox"/> Accept Authoritative Domain Sender	<input type="checkbox"/> Bypass Message Size Limit
<input type="checkbox"/> Accept Exch50	<input type="checkbox"/> Submit Messages for MLS
<input type="checkbox"/> Accept Forest Headers	<input type="checkbox"/> Submit Messages to any Recipient
<input type="checkbox"/> Accept Organization Headers	<input checked="" type="checkbox"/> Submit Messages to Server

Properties:

OK Cancel



# Empfangskonnektor – Details

## Default Frontend – Anonymous Logon



```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-ADPermission -Identity 'Default Frontend TESTMS05' | where {($_.Deny -eq $false) -and ($_.IsInherited -eq $false) -and $_.User -like '*\ANONYMOUS LOGON'} | Sort-Object ExtendedRights | Format-Table User,ExtendedRights
```

User	ExtendedRights
NT AUTHORITY\ANONYMOUS LOGON	{ms-Exch-Accept-Headers-Routing}
NT AUTHORITY\ANONYMOUS LOGON	{ms-Exch-SMTP-Accept-Any-Sender}
NT AUTHORITY\ANONYMOUS LOGON	{ms-Exch-SMTP-Accept-Authoritative-Domain-Sender}
NT AUTHORITY\ANONYMOUS LOGON	{ms-Exch-SMTP-Submit}

# Empfangskonnektor – Details

## Default Frontend – Exchange Servers



```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-ADPermission -Identity 'Default Frontend TESTMS05' | where {($_.Deny -eq $false) -and ($_.IsInherited -eq $false) -and $_.User -like '*\Exchange Servers'} | Sort-Object ExtendedRights | Select-Object User,ExtendedRights
```

User	ExtendedRights
VARUNAGROUP\Exchange Servers	{ms-Exch-Accept-Headers-Forest}
VARUNAGROUP\Exchange Servers	{ms-Exch-Accept-Headers-Organization}
VARUNAGROUP\Exchange Servers	{ms-Exch-Accept-Headers-Routing}
VARUNAGROUP\Exchange Servers	{ms-Exch-Bypass-Anti-Spam}
VARUNAGROUP\Exchange Servers	{ms-Exch-Bypass-Message-Size-Limit}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-Any-Recipient}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-Any-Sender}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-Authentication-Flag}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-Authoritative-Domain-Sender}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-Exch50}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-Xattr}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-XProxyFrom}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-XSessionParams}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-XShadow}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Accept-XSysProbe}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Send-XMessageContext-ADRecipientCache}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Send-XMessageContext-ExtendedProperties}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Send-XMessageContext-FastIndex}
VARUNAGROUP\Exchange Servers	{ms-Exch-SMTP-Submit}

# Empfangskonnektor – Details

## Default Frontend – Hub Transport Servers



```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-ADPermission -Identity 'Default Frontend TESTMS05' | where {(($_.Deny -eq $false) -and (($_.IsInherited -eq $false) -and $_.User -like '*\Hub Transport Servers')} | Sort-Object ExtendedRights | Select-Object User,ExtendedRights
```

User	ExtendedRights
MS Exchange\Hub Transport Servers	{ms-Exch-Accept-Headers-Forest}
MS Exchange\Hub Transport Servers	{ms-Exch-Accept-Headers-Organization}
MS Exchange\Hub Transport Servers	{ms-Exch-Accept-Headers-Routing}
MS Exchange\Hub Transport Servers	{ms-Exch-Bypass-Anti-Spam}
MS Exchange\Hub Transport Servers	{ms-Exch-Bypass-Message-Size-Limit}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-Any-Recipient}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-Any-Sender}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-Authentication-Flag}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-Authoritative-Domain-Sender}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-Exch50}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-Xattr}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-XProxyFrom}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-XSessionParams}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-XShadow}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Accept-XSysProbe}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Send-XMessageContext-ADRecipientCache}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Send-XMessageContext-ExtendedProperties}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Send-XMessageContext-FastIndex}
MS Exchange\Hub Transport Servers	{ms-Exch-SMTP-Submit}

# Empfangskonnektor – Details

## Default Frontend – Edge Transport Servers



```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-ADPermission -Identity 'Default Frontend TESTMS05' | where {($_.Deny -eq $false) -and ($_.IsInherited -eq $false) -and $_.User -like '*\Edge Transport Servers'} | Sort-Object ExtendedRights | Select-Object User,ExtendedRights
```

User	ExtendedRights
MS Exchange\Edge Transport Servers	{ms-Exch-Accept-Headers-Forest}
MS Exchange\Edge Transport Servers	{ms-Exch-Accept-Headers-Organization}
MS Exchange\Edge Transport Servers	{ms-Exch-Accept-Headers-Routing}
MS Exchange\Edge Transport Servers	{ms-Exch-Bypass-Anti-Spam}
MS Exchange\Edge Transport Servers	{ms-Exch-Bypass-Message-Size-Limit}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-Any-Recipient}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-Any-Sender}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-Authentication-Flag}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-Authoritative-Domain-Sender}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-Exch50}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-Xattr}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-XProxyFrom}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-XSessionParams}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-XShadow}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Accept-XSysProbe}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Send-XMessageContext-ADRecipientCache}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Send-XMessageContext-ExtendedProperties}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Send-XMessageContext-FastIndex}
MS Exchange\Edge Transport Servers	{ms-Exch-SMTP-Submit}

# Empfangskonnektor – Details

## Default Frontend und TLS bei Hybridstellung



### Konfiguration

- Konfiguriertes TLS-Zertifikat
- TlsDomainCapabilities
  - Cloud-E-Mail mit Zertifikat *mail.protection.outlook.com*
- XOORG wird angeboten
  - Exchange Online sendet die Default Domäne des Mandanten als XOORG, z.B. XOORG=varunagroup.de
- CloudServicesMailEnabled = TRUE
- DomainSecure-Absicherung der TLS-Verbindung spielt **keine** Rolle für Exchange Hybrid

```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-ReceiveConnector 'testms05\Default Frontend TESTMS05' | fl *tls*,DomainSecureEn

SuppressXAnonymousTls : False
TlsCertificateName     : <I>CN=GeoTrust TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc,
                        C=US<S>CN=mail.varunagroup.de
RequireTLS             : False
TlsDomainCapabilities  : {mail.protection.outlook.com:AcceptCloudServicesMail}
DomainSecureEnabled    : True
Fqdn                   : testms05.varunagroup.de
```

# Hybride Remote Domänen

*TrustedMailInboundEnabled*



## Konfiguration durch HCW

- Hybride Domains werden als Remote Domänen für eine vertrauensvolle Zustellung konfiguriert
- Interne Routing-Domäne ist nicht als vertrauensvoll konfiguriert  
→ soll nur Outbound funktionieren

```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-RemoteDomain | ft Name,DomainName,TrustedMailInboundEnabled -AutoSize
```

Name	DomainName	TrustedMailInboundEnabled
Default	*	False
Hybrid Domain - varunagroup.de	varunagroup.de	True
Hybrid Domain - egxde.mail.onmicrosoft.com	egxde.mail.onmicrosoft.com	False
Hybrid Domain - egxde.onmicrosoft.com	egxde.onmicrosoft.com	True



# Hybrider Empfangskonnektor

## *Chancen und Risiken*

- Der konfigurierte hybride Empfangskonnektor behandelt Verbindungen und Nachrichten von Exchange Online besonders
- Cross-Premises-Header werden nicht gefiltert und entfernt, sondern in der Transport-Pipeline zu Org-Header promotet
  - X-MS-Exchange-CrossPremises-\* → X-MS-Exchange-Organization-\*
- X-MS-Exchange-Organization-AuthAs
  - Internal – Interne E-Mailnachrichten
  - Anonymous – Nachrichten von externen Absendern, unabhängig vom Routing
- CloudServicesMailEnabled steuert den Umgang mit als Cloud-E-Mail erkannten Nachrichten



# Schauen wir mal hin

Pipeline Tracing





# Hybrider Empfangskonnektor

## *Der Schelm HCW und die Konnektorwahl*

Wie der Hybrid Configuration Wizard einen Empfangskonnektor auswählt

- Alle IPv6 (::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff) und alle IPv4 (0.0.0.0-255.255.255.255)

Dies ist normalerweise der **Default Frontend Receive Connector**, solange die **RemoteIPRanges** nicht angepasst werden

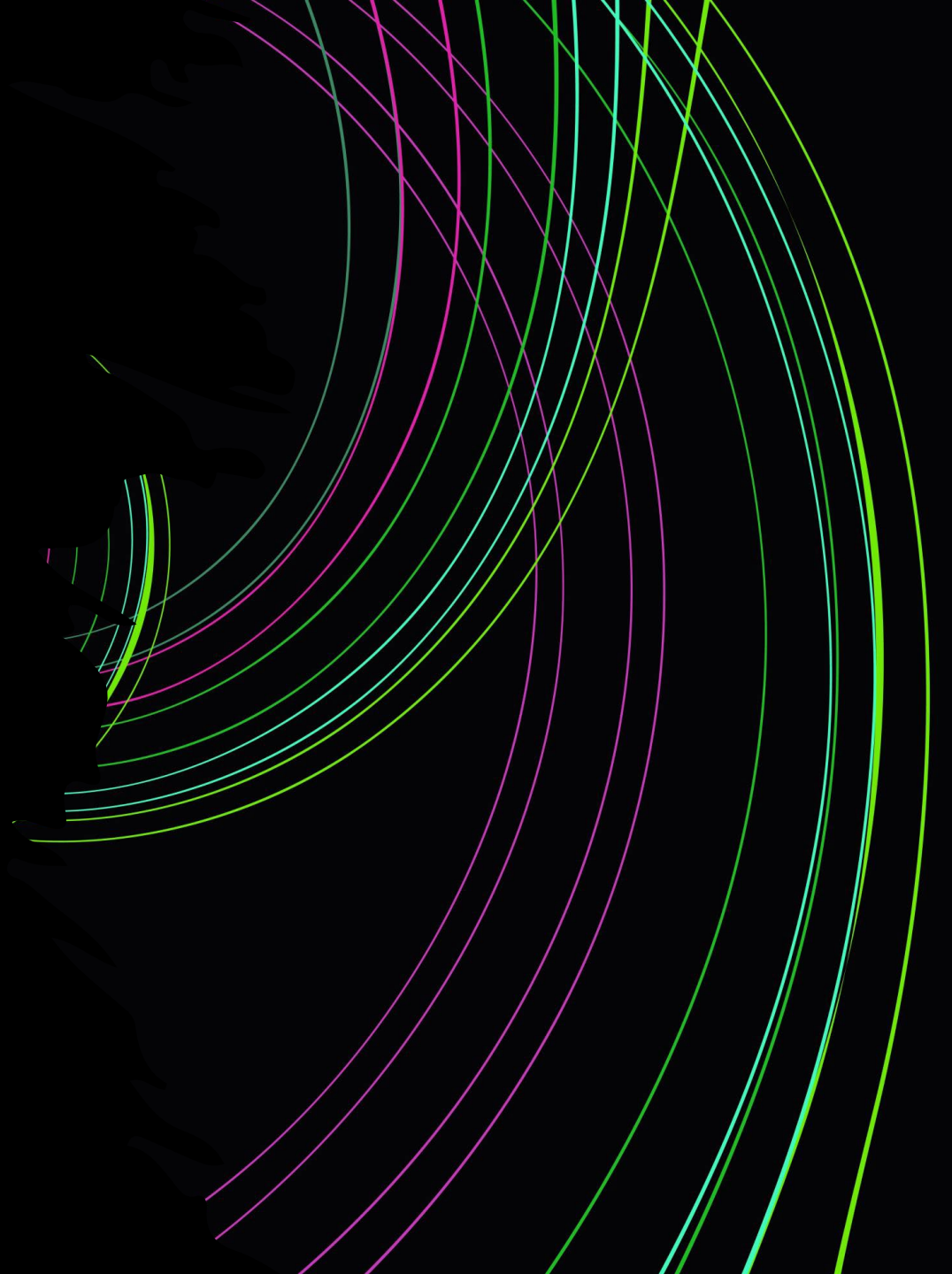
- Nur alle IPv4-Adressen (0.0.0.0-255.255.255.255)
- Nur alle IPv6-Adressen (::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)
- Irgendeine IPv6- und IPv4-Adresse
- Irgendeine IPv4-Adresse



# Fehlt immer noch etwas?

# Exchange Online Seiteneingang

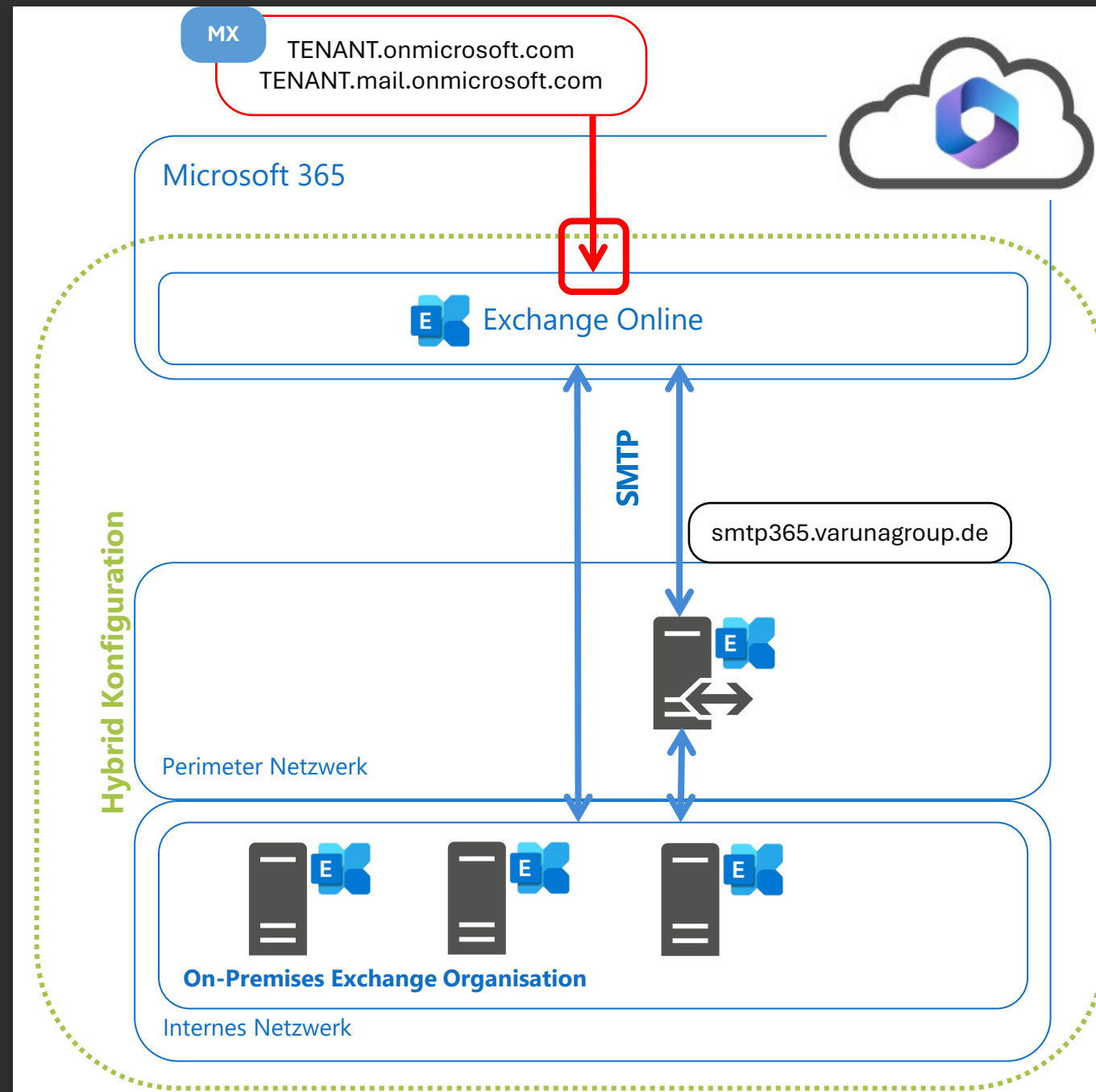
Was tun?



# Exchange Hybrid

## Die SMTP-Seite von Exchange Hybrid

- Exchange Online-Konnektoren für die Mandanten-Domänen
    - TENANT.onmicrosoft.com
    - TENANT.mail.onmicrosoft.com
- Exchange Online Seiteneingang
- Exchange Online-Mandant verfügt standardmäßig über keine ausgehenden oder eingehenden Konnektoren
  - HCW fügt nur Konnektoren für die On-Premises Anbindung hinzu

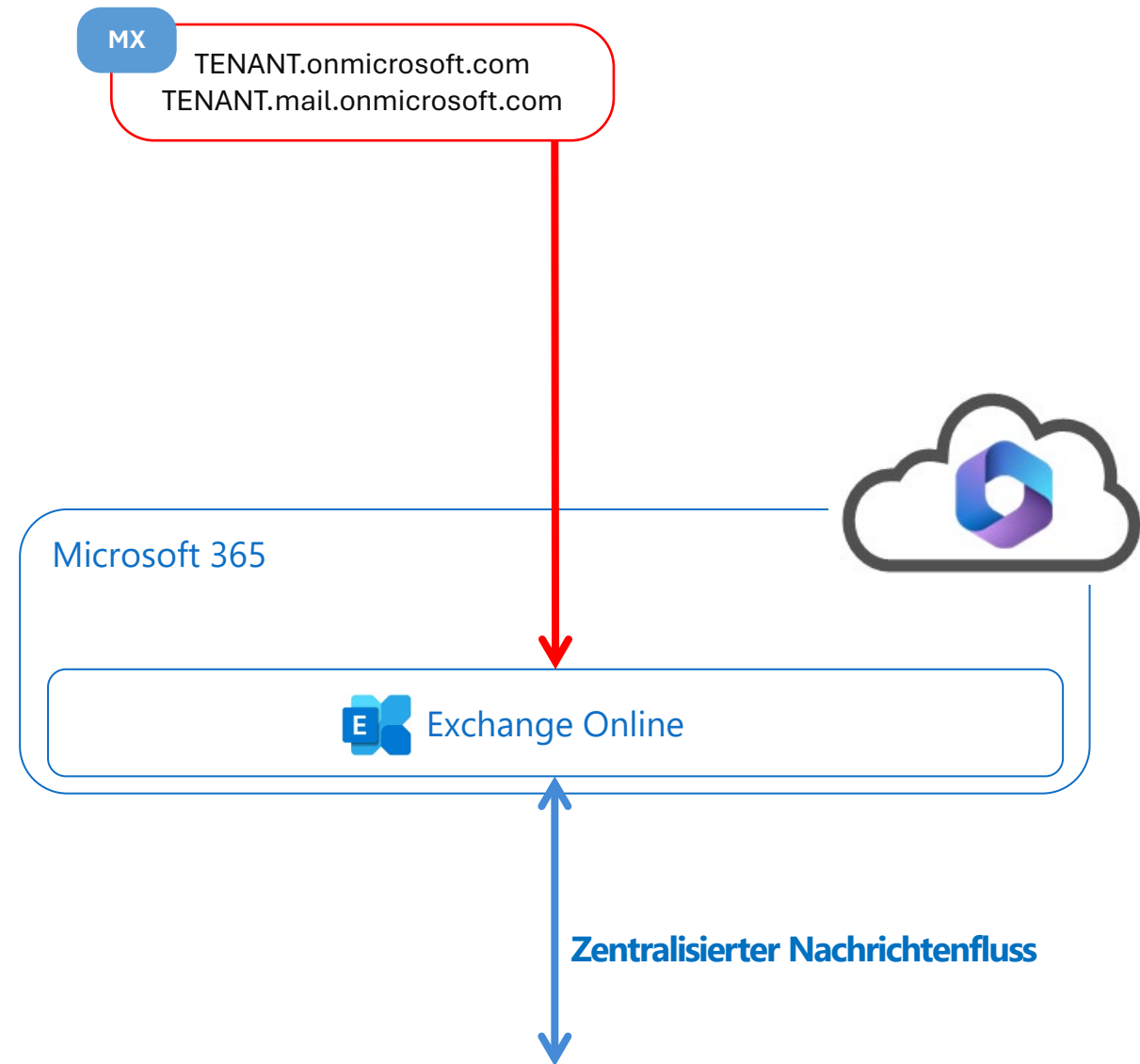


# Exchange Hybrid

## *Blockierung des Seiteneingangs*

Dringend erforderlich bei Nutzung des zentralisierten Nachrichtenflusses

- Alle Nachrichten werden über die lokale Exchange Organisation geroutet



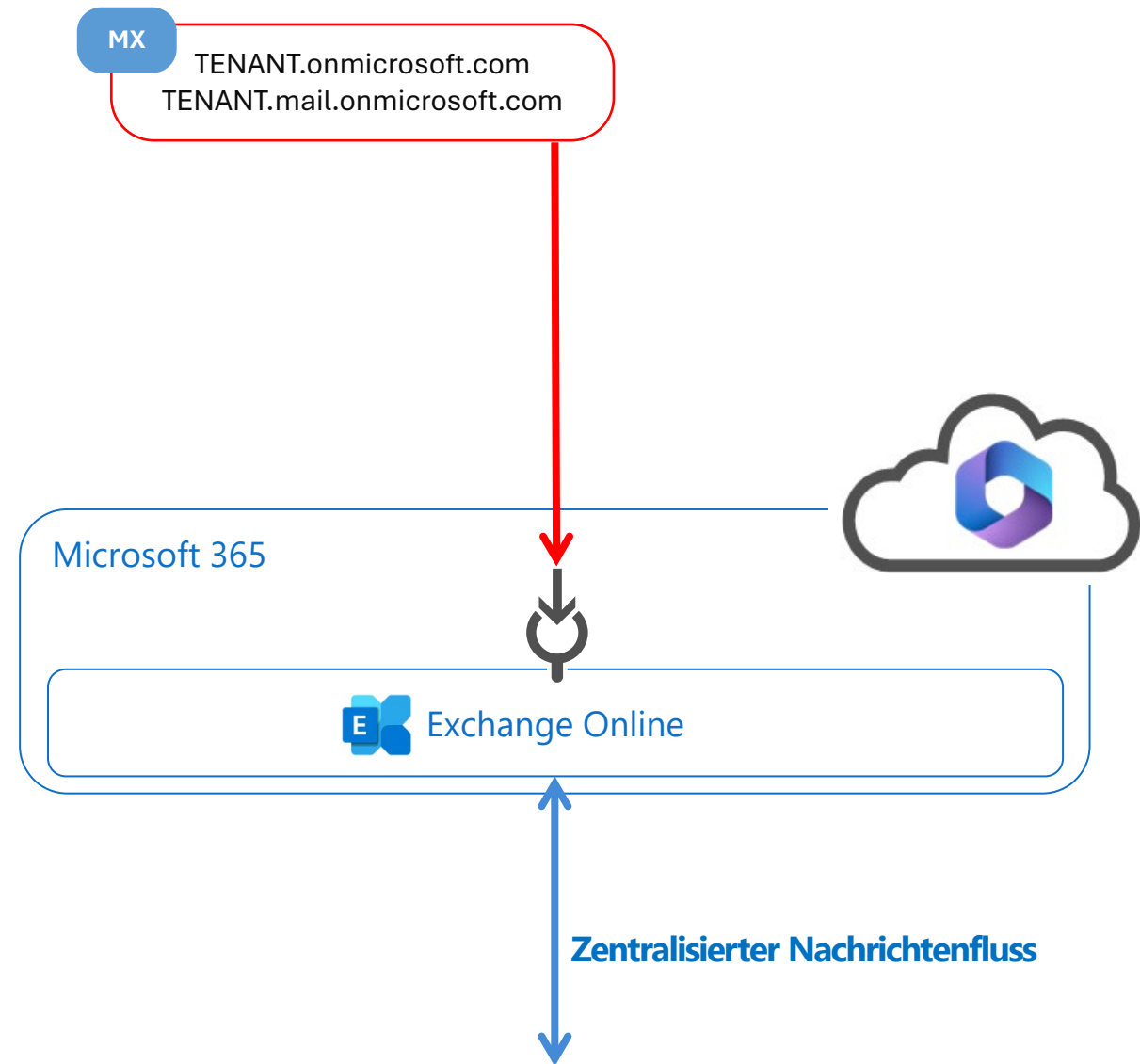
# Exchange Hybrid

## Blockierung des Seiteneingangs

Dringend erforderlich bei Nutzung des zentralisierten Nachrichtenflusses

- Alle Nachrichten werden über die lokale Exchange Organisation geroutet

Erstellung eines dedizierten eingehenden Konnektors zur Blockierung von unerwünschten Verbindungen



# Exchange Hybrid

## Blockierung des EXO-Seiteneingangs

Dedizierter eingehender Partner-Konnektor

- Quell-Adressraum: \*
- Verpflichtende Nutzung von
  - TLS
  - TLS-Zertifikat
- TLS-Zertifikatname kann ein beliebiger Name sein, z.B. *noentry.varunagroup.de*



```
# EXO InboundConnector abfragen
```

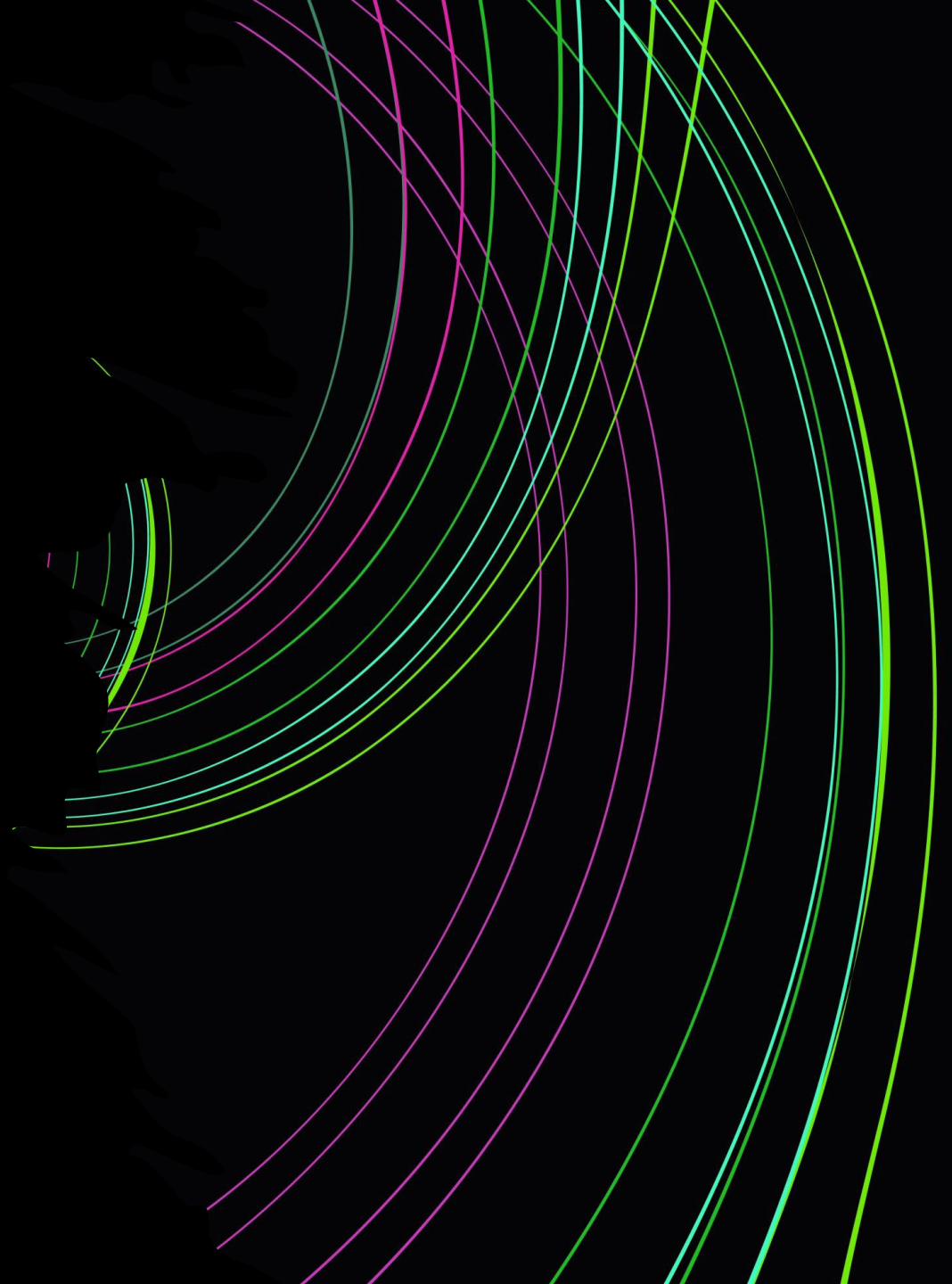
```
$OnPremisesOrg = Get-OnPremisesOrganization |  
Select-Object OrganizationGuid,InboundConnector  
| Where {$_.InboundConnector -ne $null}
```

```
# Neuer InboundConnector
```

```
New-InboundConnector '  
-Name 'Restrict Direct Delivery to Built-In  
Domains' '  
-ConnectorType Partner '  
-SenderDomains * '  
-TlsSenderCertificateName (Get-InboundConnector  
$OnPremisesOrg[0].InboundConnector).TlsSenderCe  
rtificateName '  
-RestrictDomainsToCertificate $true '  
-RequireTls $true
```

# Exchange Online Hintereingang

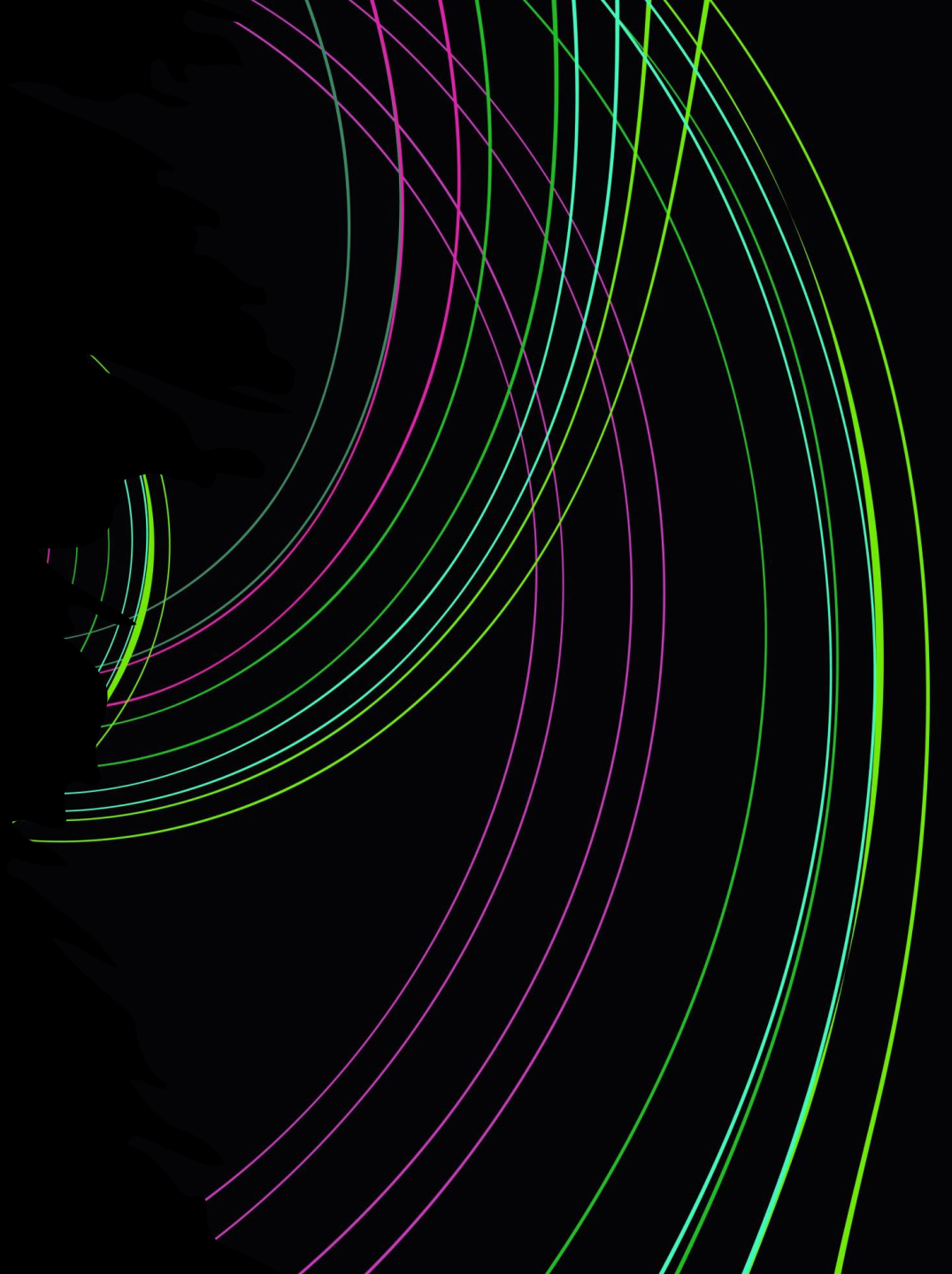
Da war doch was...





# Exchange Online Hintereingang

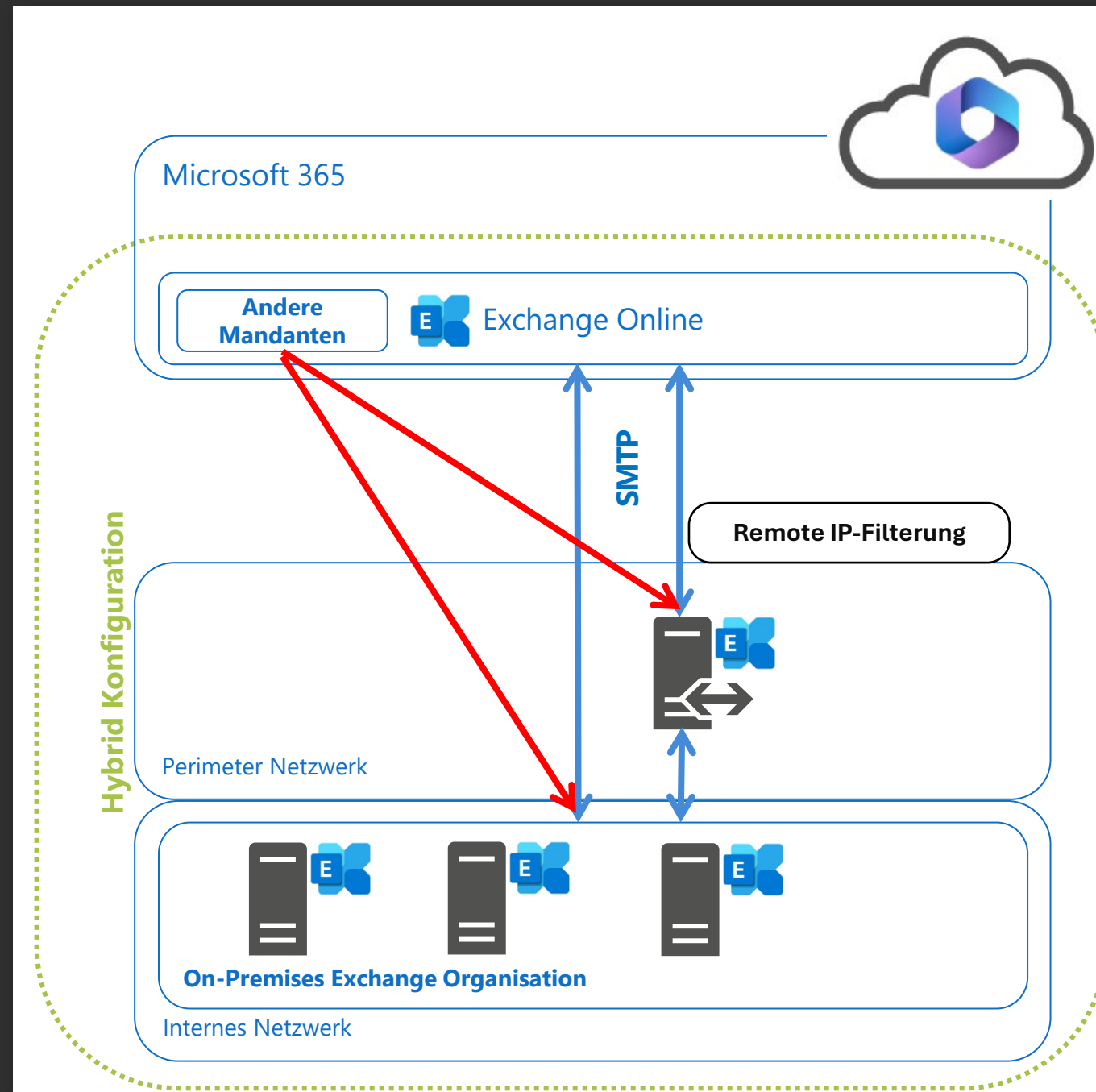
Da war doch was... → andere Mandanten



# Exchange Hybrid

## Der On-Premises Hintereingang

- Absicherung des Empfangskonnektors auf Remote IP-Adressen der Microsoft Exchange Online Rechenzentren
- Andere Mandanten senden aus dem identischen IP-Adressraum
- Risiko einer direkten Zustellung von E-Mail-Nachrichten aus fremden Mandanten in die lokale Exchange Organisation



# Exchange Hybrid

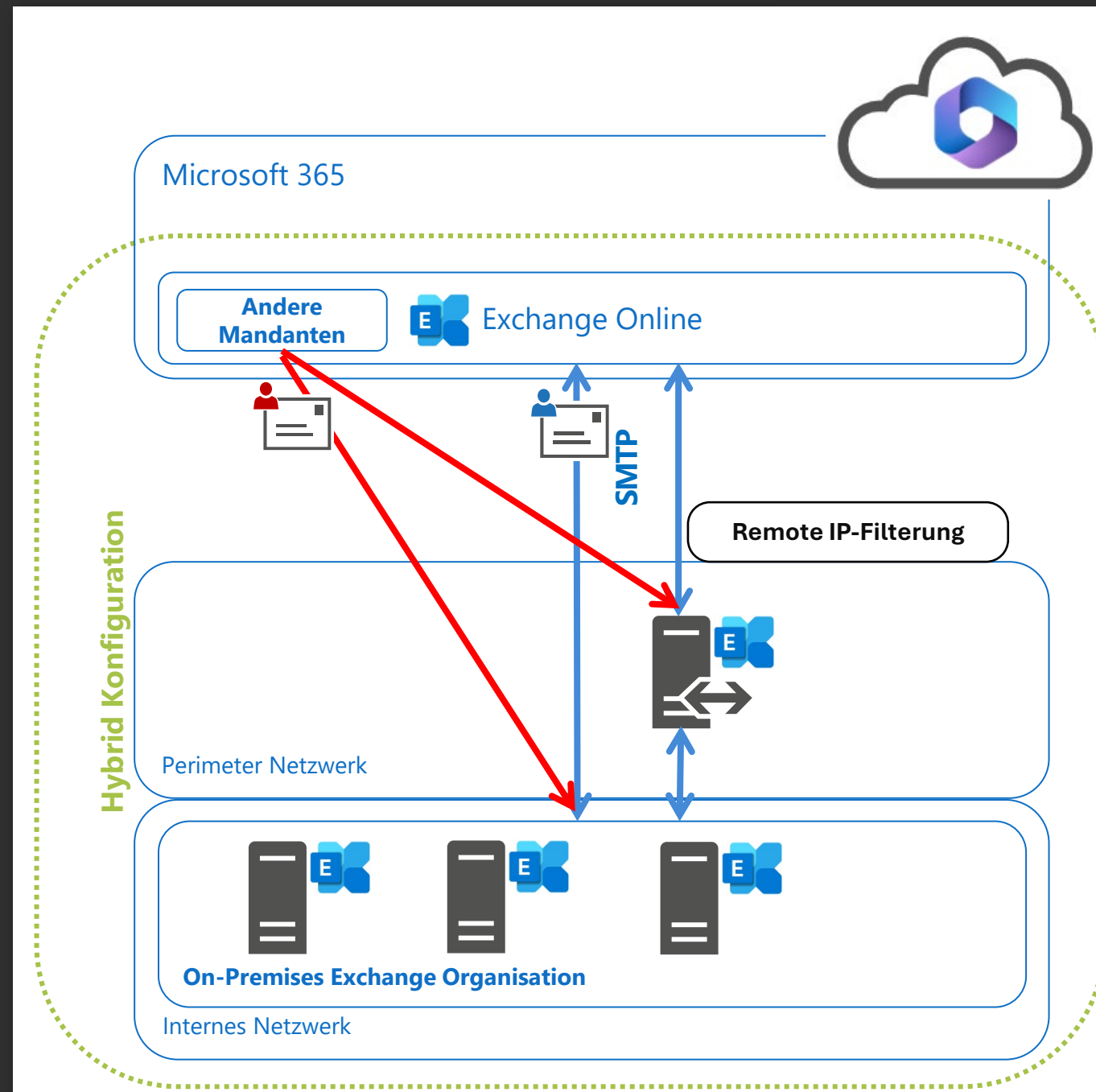
## E-Mail-Unterschiede

E-Mail aus **eigenem** Mandanten

- Authentifizierte Zustellung
- X-MS-Exchange-Organization-AuthAs  
→ **Internal**

E-Mail aus **anderen** Mandanten

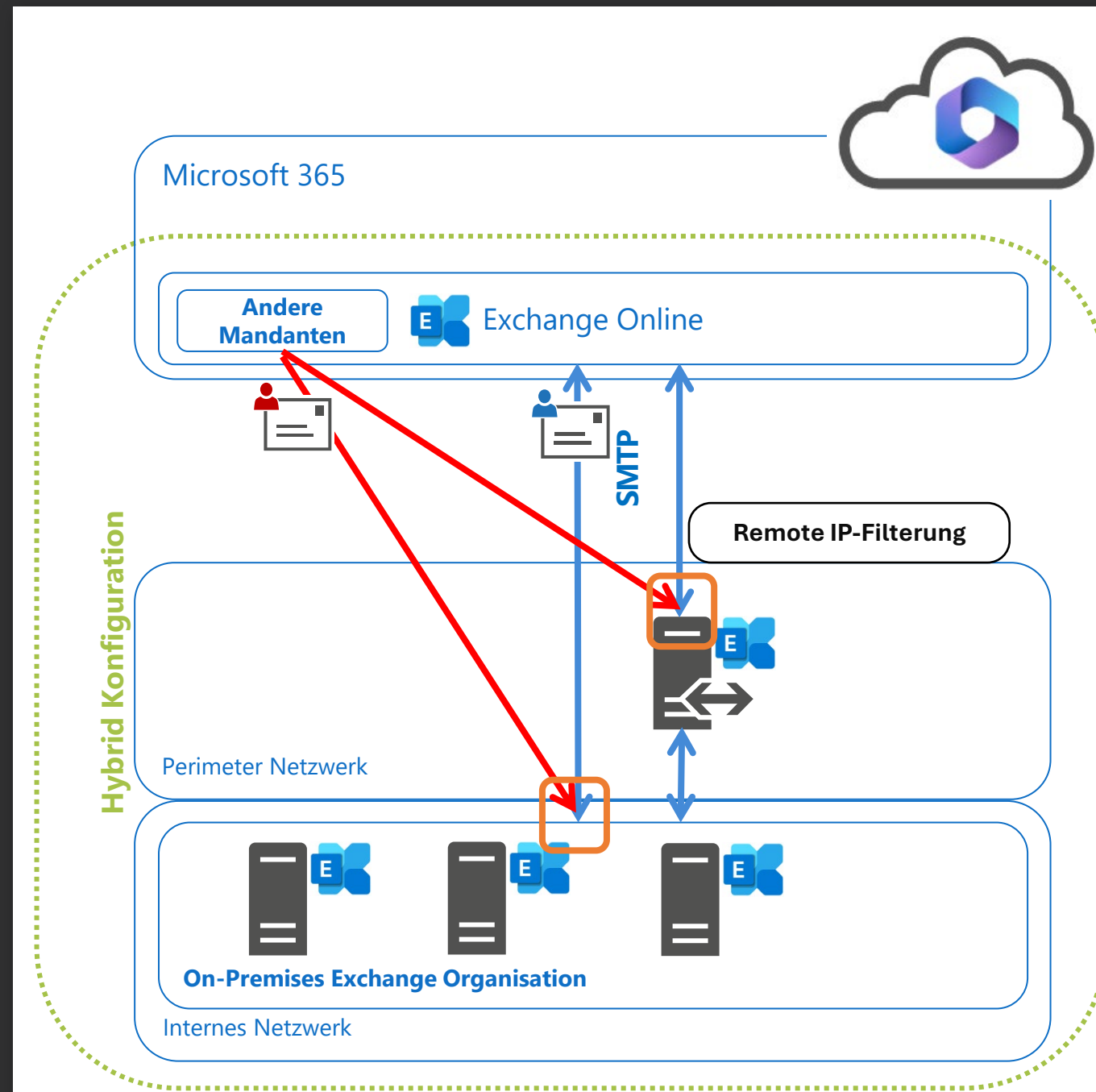
- Nicht authentifizierte Zustellung
- X-MS-Exchange-Organization-AuthAs  
→ **Anonymous**



# Exchange Hybrid

## Der Empfangskonnektor

- TlsDomainCapabilities
    - AcceptedCloudServicesMail
  - XOORG Domäne im MAIL FROM
    - Passt zu einer **akzeptierten Domäne** oder
    - Passt zu einer **Remote-Domäne** mit TrustedMailInboundEnabled = \$true
- Exchange Server stuft die Verbindung als **Authenticated** ein
- **Cross-Premises Header** werden zu **Org-Headers**
- **X-OriginatorOrg** wird auf verifizierte Domäne gesetzt



# Exchange Hybrid

## *CrossPremises Header*



- E-Mail-Nachrichten aus anderen Mandanten enthalten keine CrossPremises-Header
- Empfängerdomäne ist keine akzeptierte Domäne im sendenden Tenant
  - keine CrossPremises-Header

# Exchange Hybrid

## Absicherung des Hintereinganges



- XOORG SMTP-Kommando wird nur von Exchange verstanden
- XOORG kann nicht gespoofed werden (Microsoft)
  - Kombination aus
    - EOP TLS-Zertifikat
    - Einstellungen des lokalen Hybrid-Empfangskonnektors
    - Akzeptierte Domäne

```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>Get-ReceiveConnector 'testms05\Default Frontend TESTMS05' | fl *tls*,DomainSecureEnabled,Fqdn

SuppressXAnonymousTls : False
TlsCertificateName     : <I>CN=GeoTrust TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc,
                        C=US<S>CN=mail.varunagroup.de
RequiresTls            : False
TlsDomainCapabilities  : {mail.protection.outlook.com:AcceptCloudServicesMail}
DomainSecureEnabled    : True
Fqdn                   : testms05.varunagroup.de
```

```
Machine: testms05.varunagroup.de
[PS] E:\>Get-AcceptedDomain

Name                        DomainName                DomainType                Default
-----
varunagroup.de             varunagroup.de            Authoritative             True
varunagroup.com            varunagroup.com           Authoritative             False
groups.varunagroup.de      groups.varunagroup.de     InternalRelay             False
egxde.mail.onmicrosoft.com egxde.mail.onmicrosoft.com Authoritative             False
```

# Exchange Hybrid

## Absicherung des Hintereinganges - Transportregel



## Transportregel in lokaler Exchange Organisation

- *Wenn*
  - Absender der Nachricht ist **außerhalb der Organisation**
- *Dann*
  - **Leite die Nachricht** an ein Postfach **um**  
*oder*
  - **Weise die Nachricht** mit einer Fehlermeldung **ab**
- *Außer*
  - **X-OriginatorOrg-Header** enthält **varungaroup.de**



# Exchange Hybrid

## Absicherung des Hintereinganges - Transportregel



The screenshot shows the 'Regel - Profile 1 - Microsoft Edge' window in a browser. The left sidebar has a table with columns 'EIN' and 'REGEL'. An orange arrow points to the 'Blockierung externer Nachrichten' rule, which is checked. The main area shows the configuration for this rule:

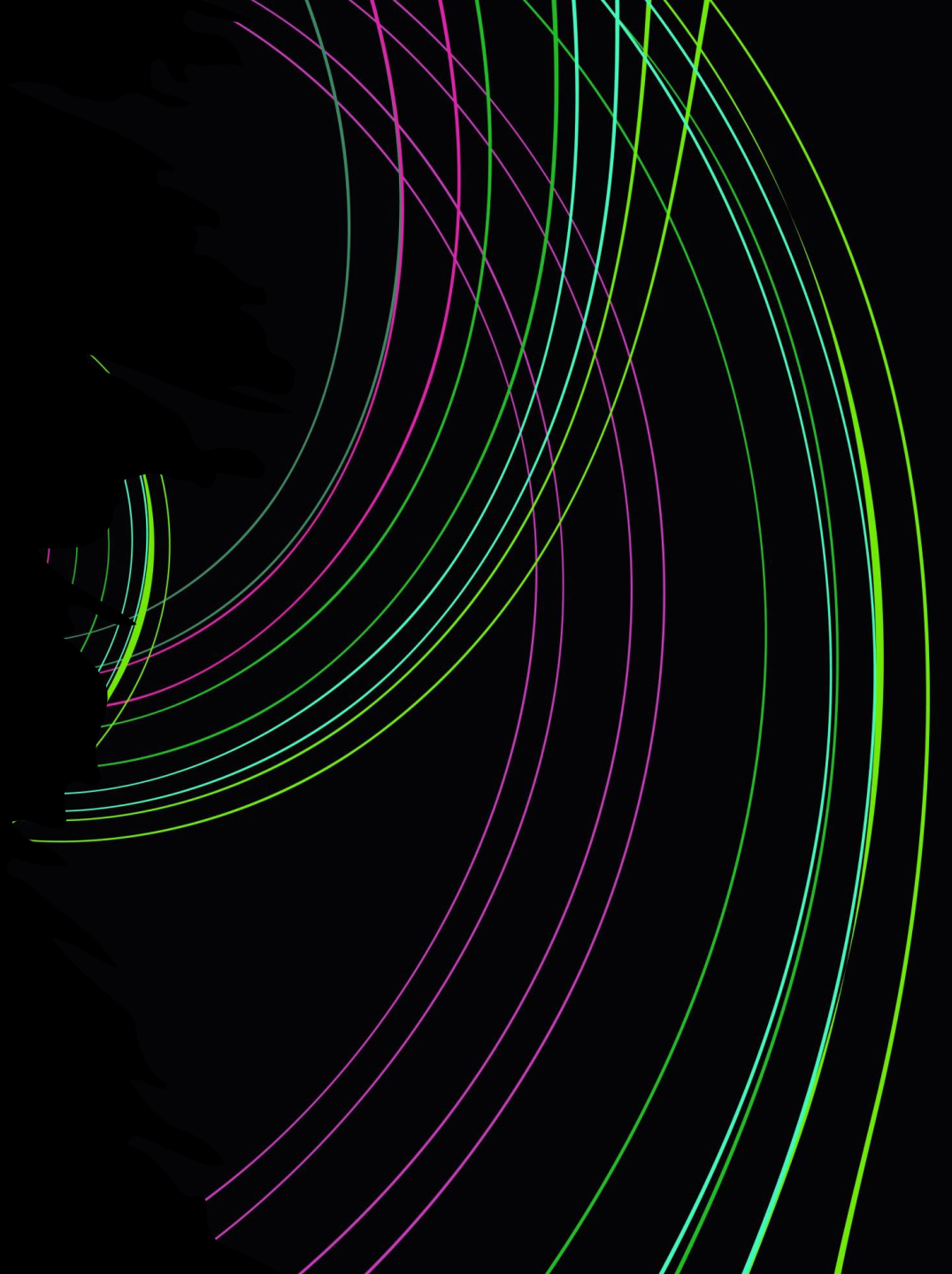
- Name:** Blockierung externer Nachrichten
- \*Diese Regel anwenden, wenn...:** Der Absender befindet sich in... [Außerhalb der Organisation](#)
- \*Folgendermaßen vorgehen...:** Die Nachricht ohne Benachrichtigung anderer Benutzer löschen
- Außer wenn...:** Ein Nachrichtenkopf enthält...  
Kopfzeile 'X-OriginatorOrg' enthält 'egx.mail.onmicrosoft.com' oder 'egxde.onmicrosoft.com' oder 'varunagroup.de'
- Eigenschaften dieser Regel:** Priorität: 0

Buttons at the bottom: Speichern, Abbrechen.



# Exchange Hybrid

Zusammenfassung



# Exchange Hybrid-Konnektoren

## Manuelle Aufgaben



- **Hybrid Configuration Wizard** konfiguriert die **grundsätzliche Funktion** der Hybrid-Stellung, inklusive des Nachrichtenflusses
- **Absicherung** der HTTPS- und SMTP-Strecke ist eine **zusätzliche manuelle Aufgabe** vor Inbetriebnahme der Hybrid-Stellung
- **Konfiguration der lokalen Empfangskonnektoren** hat eine direkte Auswirkung auf die **automatische Konnektor-Auswahl** des HCW
- **CloudServicesMailEnabled** muss mit Vorsicht konfiguriert werden

# Exchange Hybrid





- [https://www.msxfaq.de/exchange/admin/exchange\\_zertifikate\\_rechte.htm](https://www.msxfaq.de/exchange/admin/exchange_zertifikate_rechte.htm)

# Ressourcen



- [Nachrichtenfluss und die Transportpipeline](#)
- [Empfangskonnektoren](#)
- [Transportoptionen in Exchange-Hybridbereitstellungen](#)
- [Advanced Office 365 Routing: Locking Down Exchange On-Premises when MX points to Office 365](#)
- [How to block direct delivery to email address with the suffix as domain.onmicrosoft.com or domain.mail.onmicrosoft.com](#)
- [Set-RemoteDomain](#)
- [Manage mail flow using a third-party cloud service with Exchange Online](#)
- [Deep Dive Hybrid Mail Flow \(Video\)](#)

# Exchange Server / Hybrid / Online Q & A



# Organisatorisches



## Meetup Termine 2025 (Planung)

- Q1 – 27. Februar
- Q2 – 22. Mai
- Q3 – 18. September
- Q4 – 20. November



# Exchange Summit 2025

*Die Exchange Konferenz für die DACH-Region*



- **Zwei Tage** rund um Exchange

→ **Würzburg**

→ **18. und 19. Februar 2025**

- <https://Exchange-Summit.de>



# Exchange Coffee Talk



- Lockere Kaffeerunde zu Exchange-Themen
- Bringt eure Themen mit
- Einmal im Monat
  - Letzter Mittwoch im Monat
  - 27. Februar 2025
  - 17 Uhr
  - 1 Stunde
  - [ExchangeCoffeeTalk.de](https://ExchangeCoffeeTalk.de)
- Dezember & Januar finden nicht statt



# Exchange User Group

## Organisatorisches

- **Exchange User Group Team**
  - Registrierung → Link auf Homepage ([exusg.de](http://exusg.de))
- **Themenvorschläge**
  - <https://sessionize.com/exchange-user-group>
- **Community Sticker**
  - <https://go.granikos.eu/CommunitySticker>
- **EXUSG Mugs**
  - <https://go.granikos.eu/EXUSGMug>



# Danke für die Teilnahme



## Exchange User Group

Nächster Termin in **Q1 2025**

- Talk 1: Exchange Online Message Rate Limit, Thomas Stensitzki
- Talk 2: TBD
- Meetup-Themenwünsche und eure Talks sind immer willkommen ☺

<https://exusg.de>

<https://go.granikos.eu/EXUSG-Recs>

Exchange User Group | @exusg



# Danke für eure Teilnahme