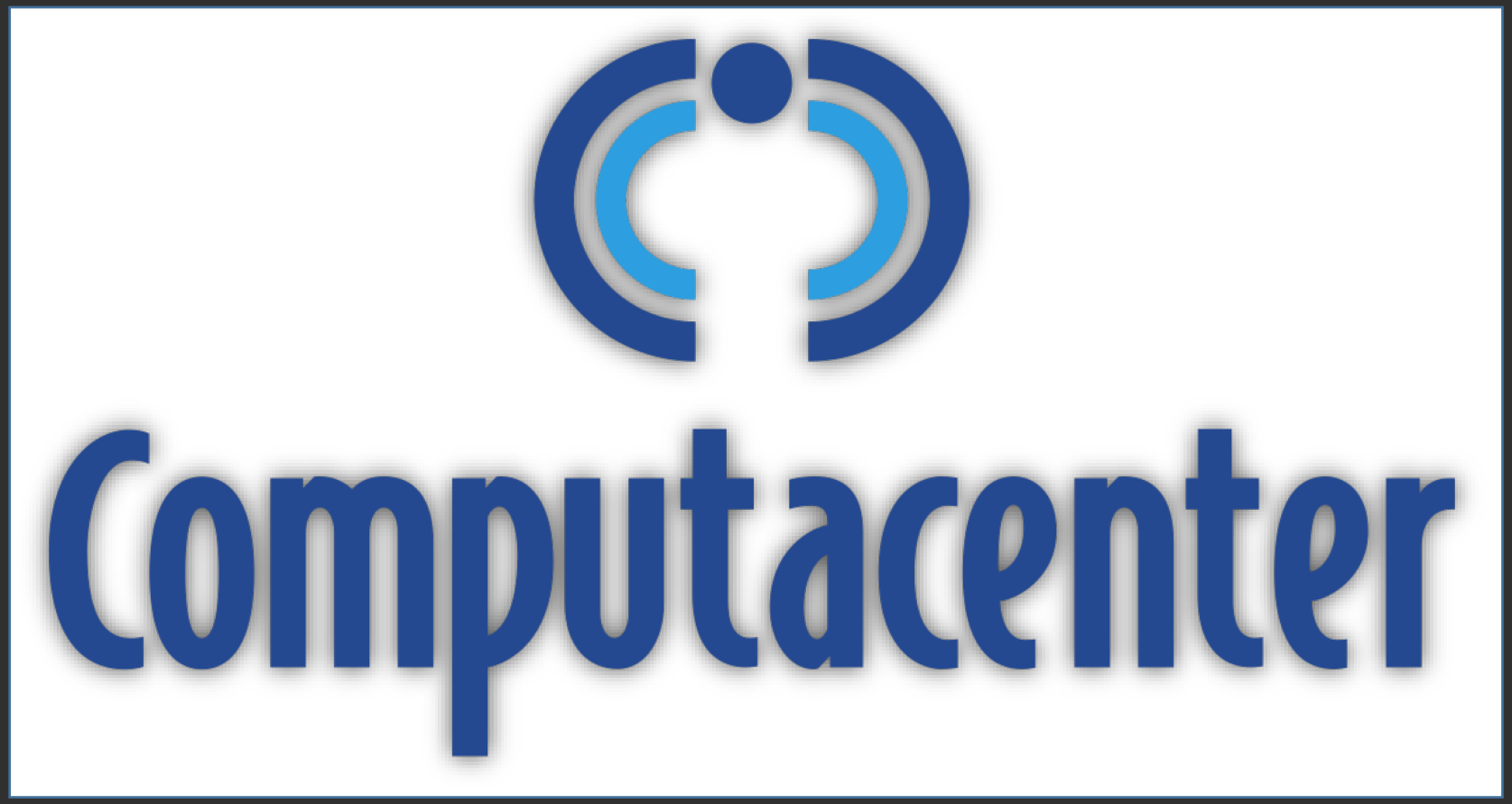
Exchange User Group
Meetup Q3 2023
{Hybrid Edition}

31. August 2023

Location Sponsor



https://www.computacenter.com

Sponsor

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

https://www.enowsoftware.com

Meetup Q2 2022

Edge-Transport-Rolle, das Stiefkind von Exchange
- *Thomas Stensitzki*

Exchange Server Security Update August 2023 und mehr

Exchange Q & A

Die Talks werden aufgezeichnet. The sessions will be recorded.
https://go.granikos.eu/EXUSG-Recs

Edge-Transport-Rolle, das Stiefkind von Exchange

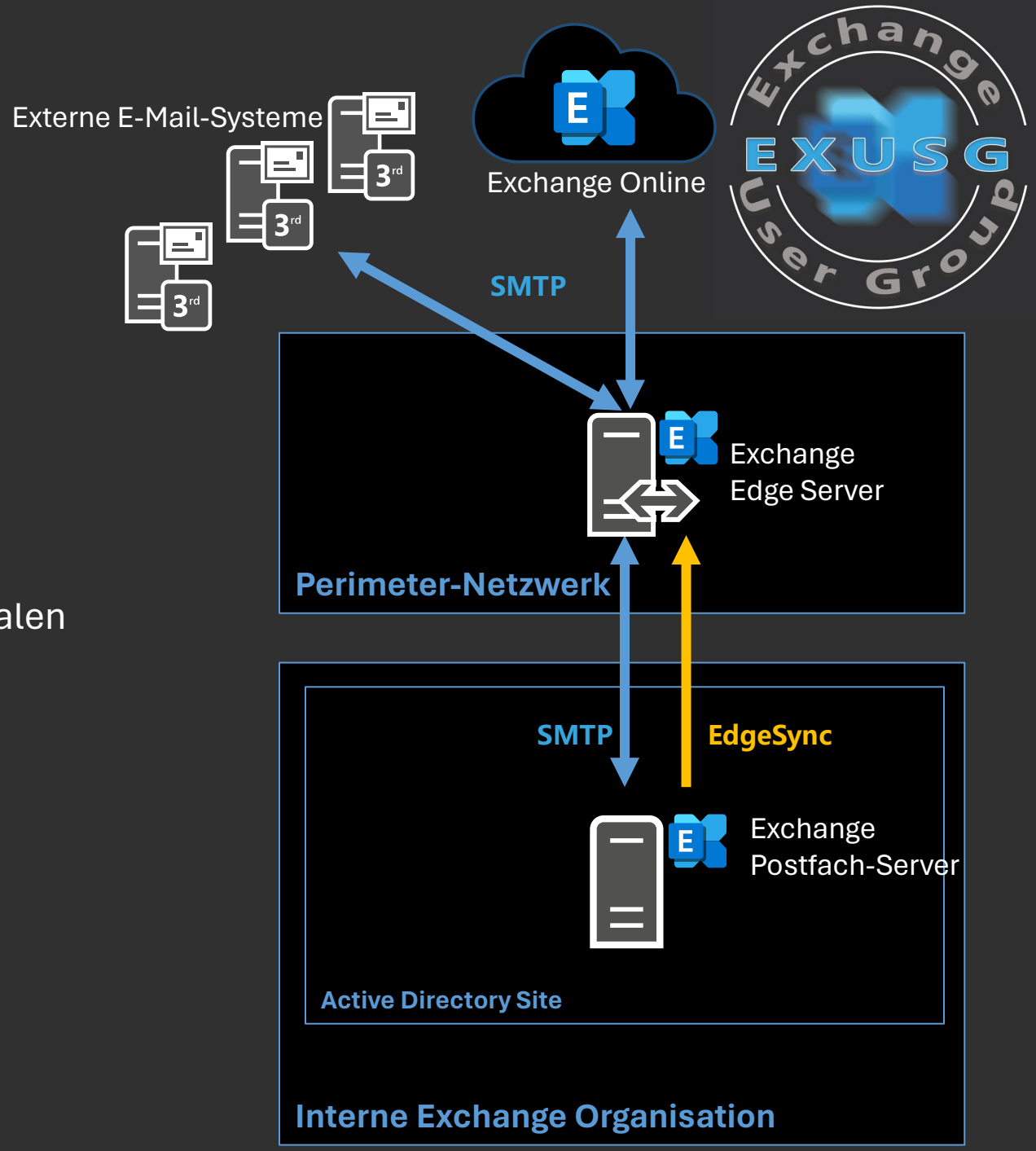
Thomas Stensitzki

EdgeSync

Edge-Transport-Rolle

- Erstmalig verfügbar mit Exchange Server 2007
- SMTP-Gateway im Perimeter-Netzwerk
  - Für Internet-Nachrichten
  - Für hybride Kommunikation mit Exchange Online
- Windows Server OS ist kein Domänenmitglied
- Erhält organisationsweite Konfigurationen von der lokalen Exchange Organisation per EdgeSync
- Server-spezifische Konfigurationen erfolgen lokal

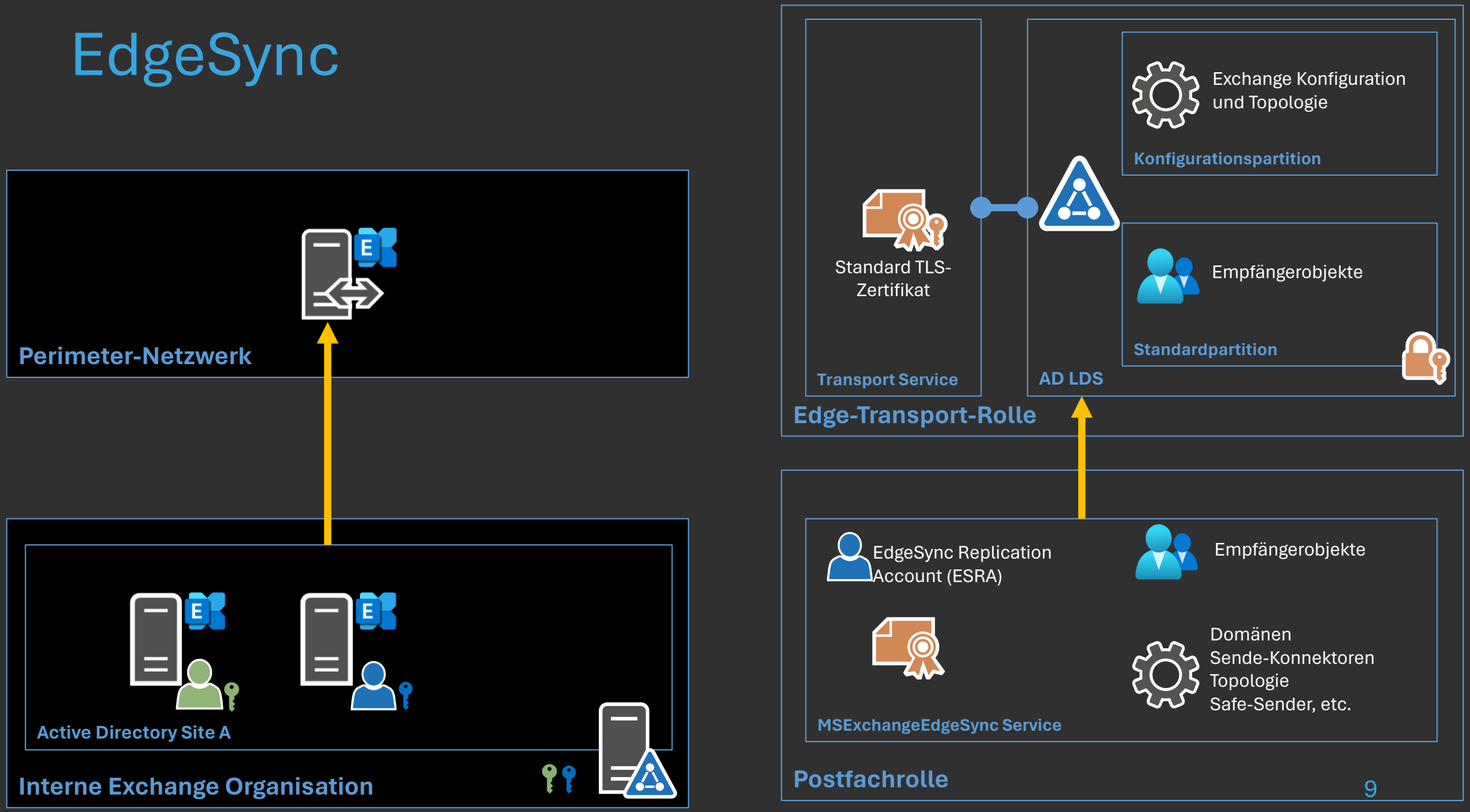
1. Edge-Abonnement zur Einbindung in die Exchange Organisation
2. Edge-Transport-Konfiguration
   - Sende- und Empfangskonnektoren
   - Transportregeln
   - Anti-Spam und Anti-Malware



EdgeSync – Einfach erklärt

- EdgeSync ist der Protokollname für eine Secure LDAP (LDAPS)-Verbindung auf TCP-Port 50636
- Die Verbindung erfolgt von jedem Exchange Server, der zum Zeitpunkt der Edge-Abonnement-Einrichtung in der Active Directory Site aktiv ist
- Die Absicherung der Verbindung erfolgt mit automatisch erstellen Authentifizierungskonten, deren jeweiliges Kennwort durch einen TLS-Zertifikatsschlüssel verschlüsselt ist
- Die jeweils zum Zeitpunkt der Abonnement-Einrichtung aktiven Standardzertifikate der Transportdienste auf dem Edge-Transport-Server und den Exchange Postfach-Servern werden verwendet
- Ein zufällig ausgewählter Exchange Server der Active Directory Site führt die initiale Replikation mit Hilfe eines Bootstrap-Kontos durch
- Alle weitere Exchange Server der Active Directory Site nutzen neue erstellte und per EdgeSync synchronisierte Authentifizierungskonten

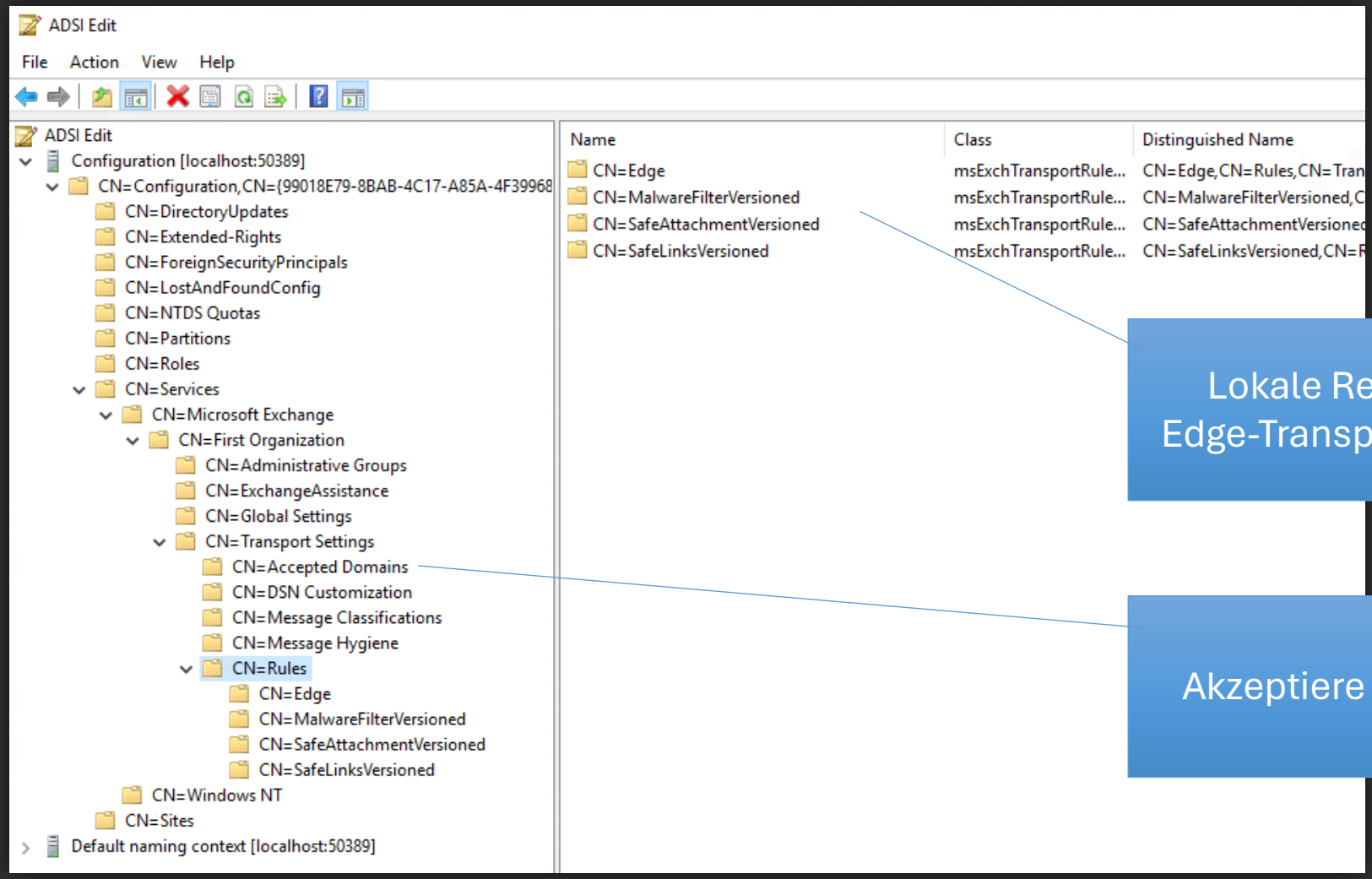
EdgeSync


Perimeter-Netzwerk
Active Directory Site A
Interne Exchange Organisation
Standard TLS-Zertifikat
Transport Service
Exchange Konfiguration und Topologie
Konfigurationspartition
Empfängerobjekte
Standardpartition
AD LDS
Edge-Transport-Rolle
EdgeSync Replication Account (ESRA)
MSExchangeEdgeSync Service
Empfängerobjekte
Domänen
Sende-Konnektoren
Topologie
Safe-Sender, etc.
Postfachrolle

Was überträgt EdgeSync?

- Exchange Konfiguration
  - Vollqualifizierten Domänennamen (FQDN) jedes Exchange Servers der Active Directory Site
  - Akzeptierte Domänen (Authoritative, Internal/External Relay)
  - Remote Domänen
  - Nachrichtenklassifizierungen
  - Sendekonnektoren
  - Interne SMTP-Server
  - Sichere Domänen (Domain Secure Liste für Mutual TLS)
  - Topologie-Informationen der internen Exchange Organisation

Edge AD LDS – Konfigurationspartition



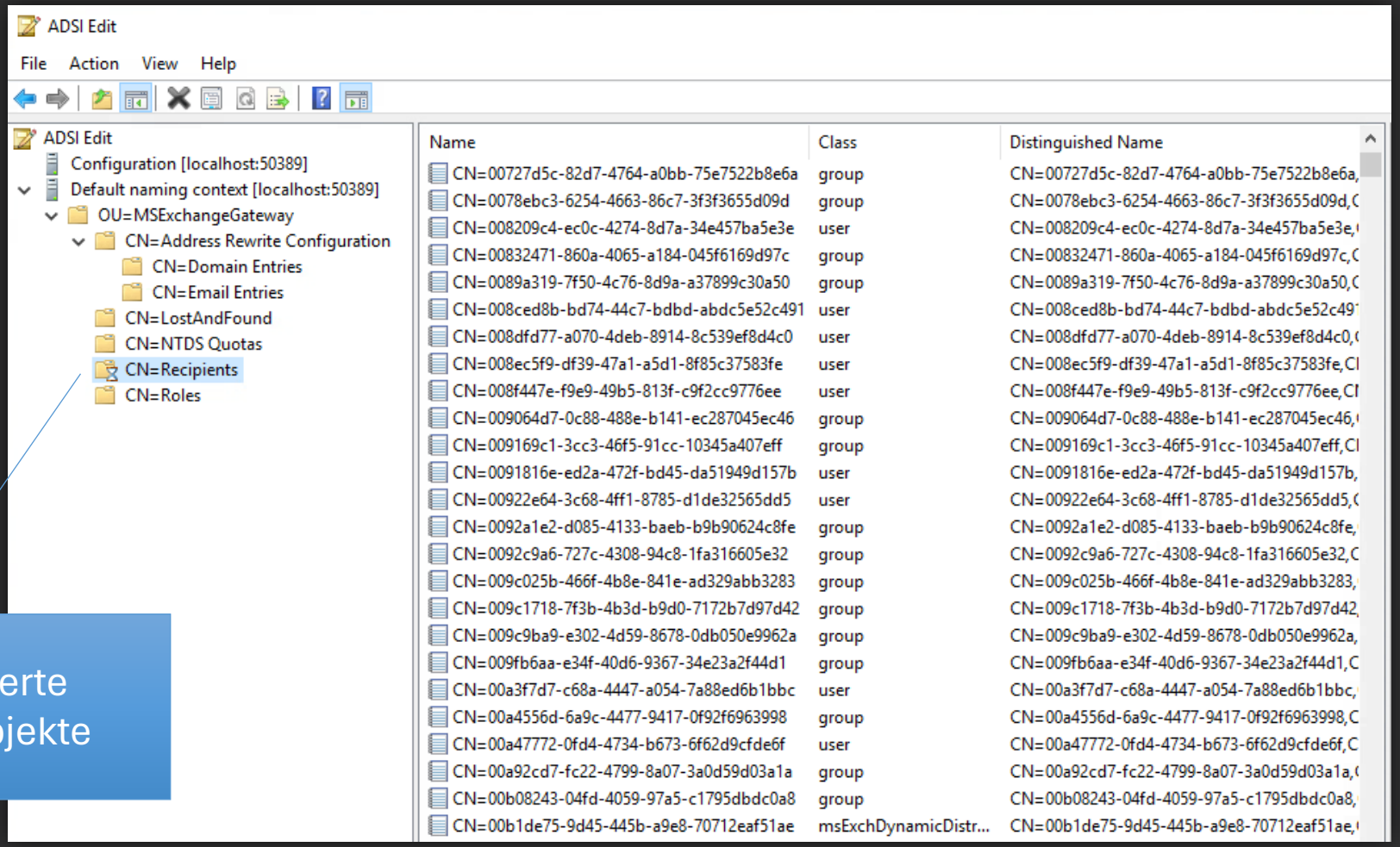
Lokale Regeln des Edge-Transport-Servers

Akzeptiere Domänen

Was überträgt EdgeSync?

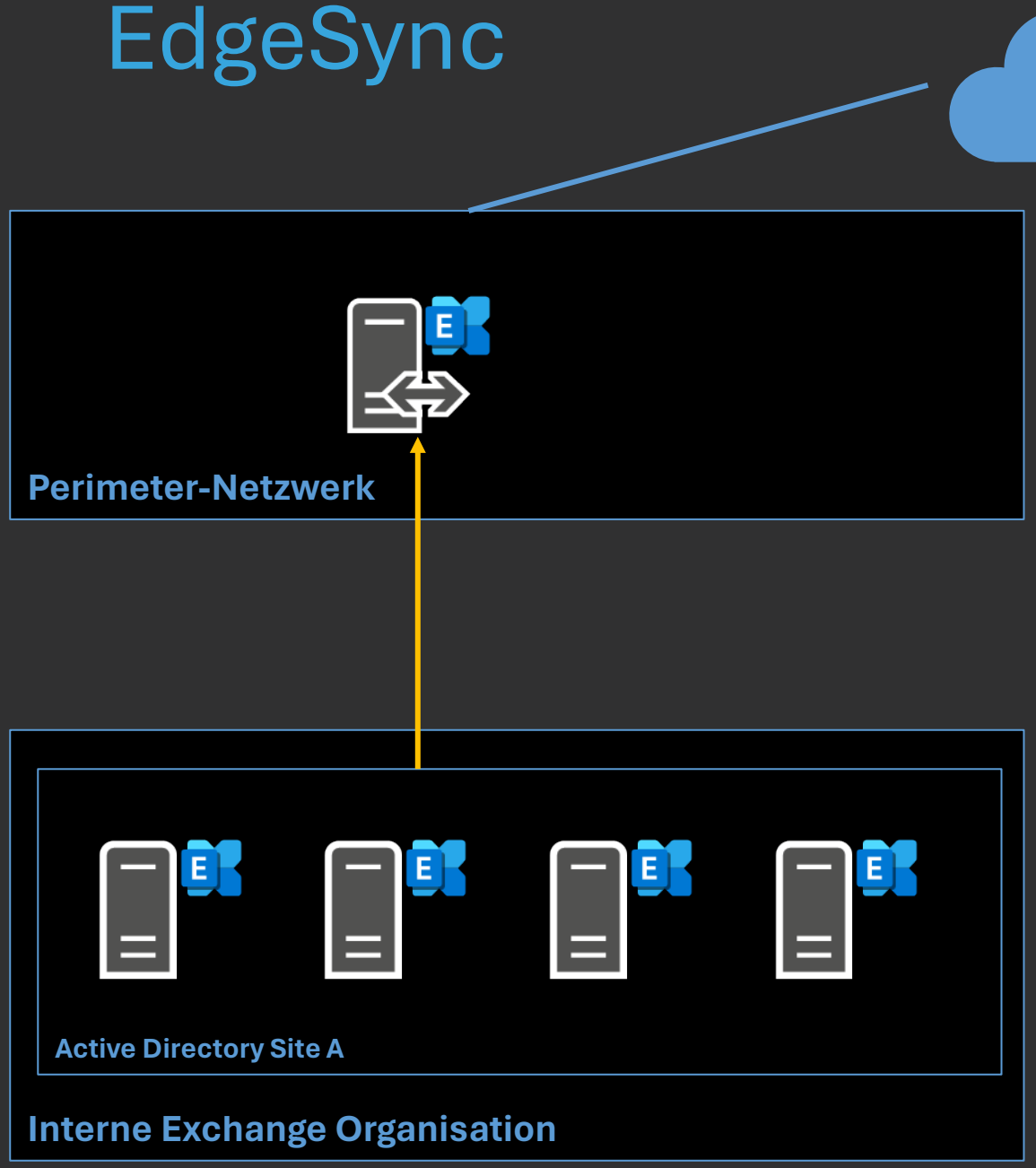
- Empfängerinformationen
  - Alle Active Directory Empfängerobjekte, für die der Empfang von Nachrichten außerhalb der Organisation erlaubt ist
    → Informationen deaktivierter oder gelöschter Postfächer werden nicht repliziert
  - Proxy-Adressen werden SHA-256 Hash verschlüsselt übertragen und in AD LDS gespeichert
  - Liste der sicheren und blockierten Absender und der sicheren Empfänger
  - Anti-Spam-Einstellungen, die auf Postfachebene definiert sind

Edge AD LDS – Default Partition



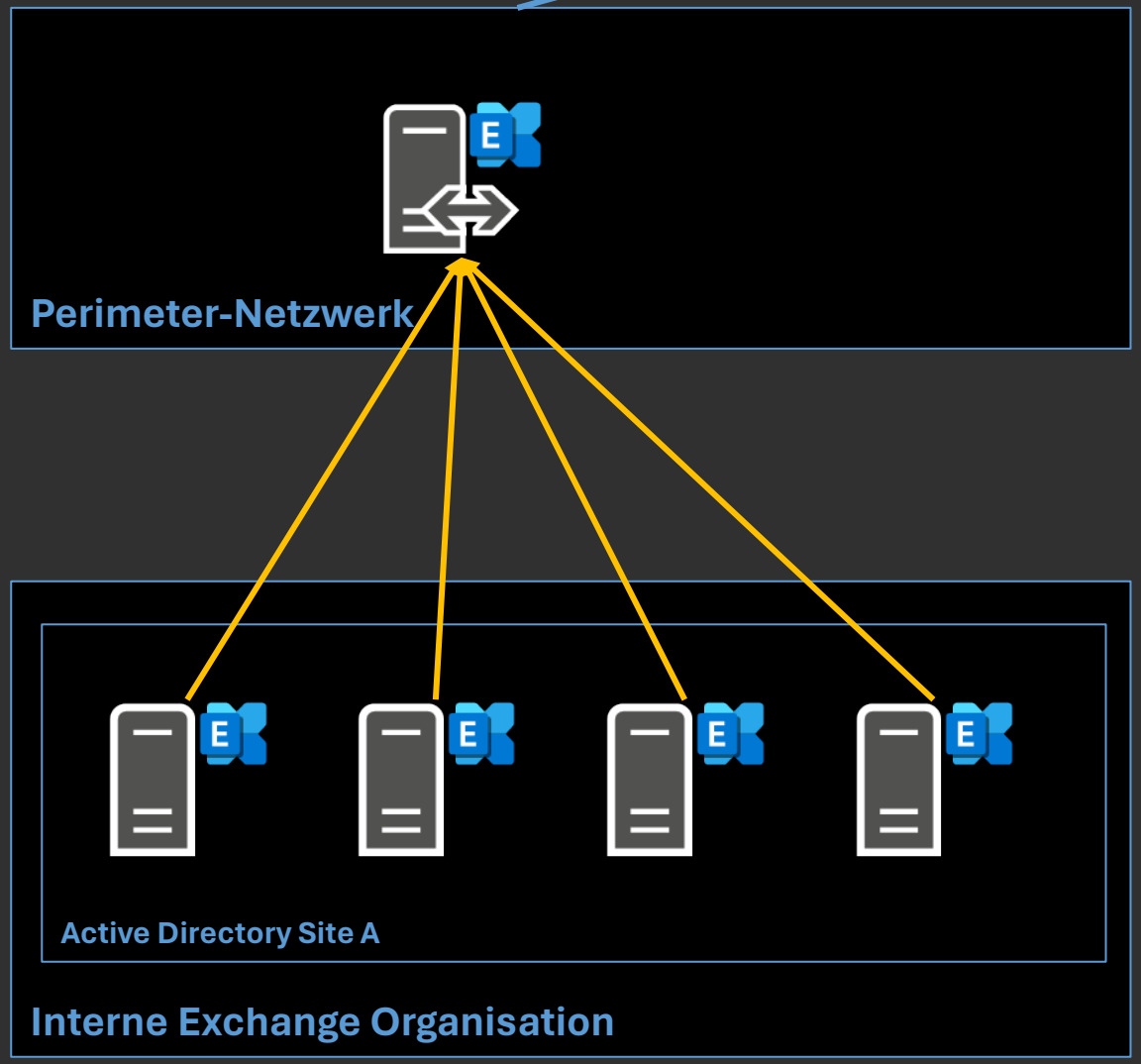
Synchronisierte Empfängerobjekte

EdgeSync



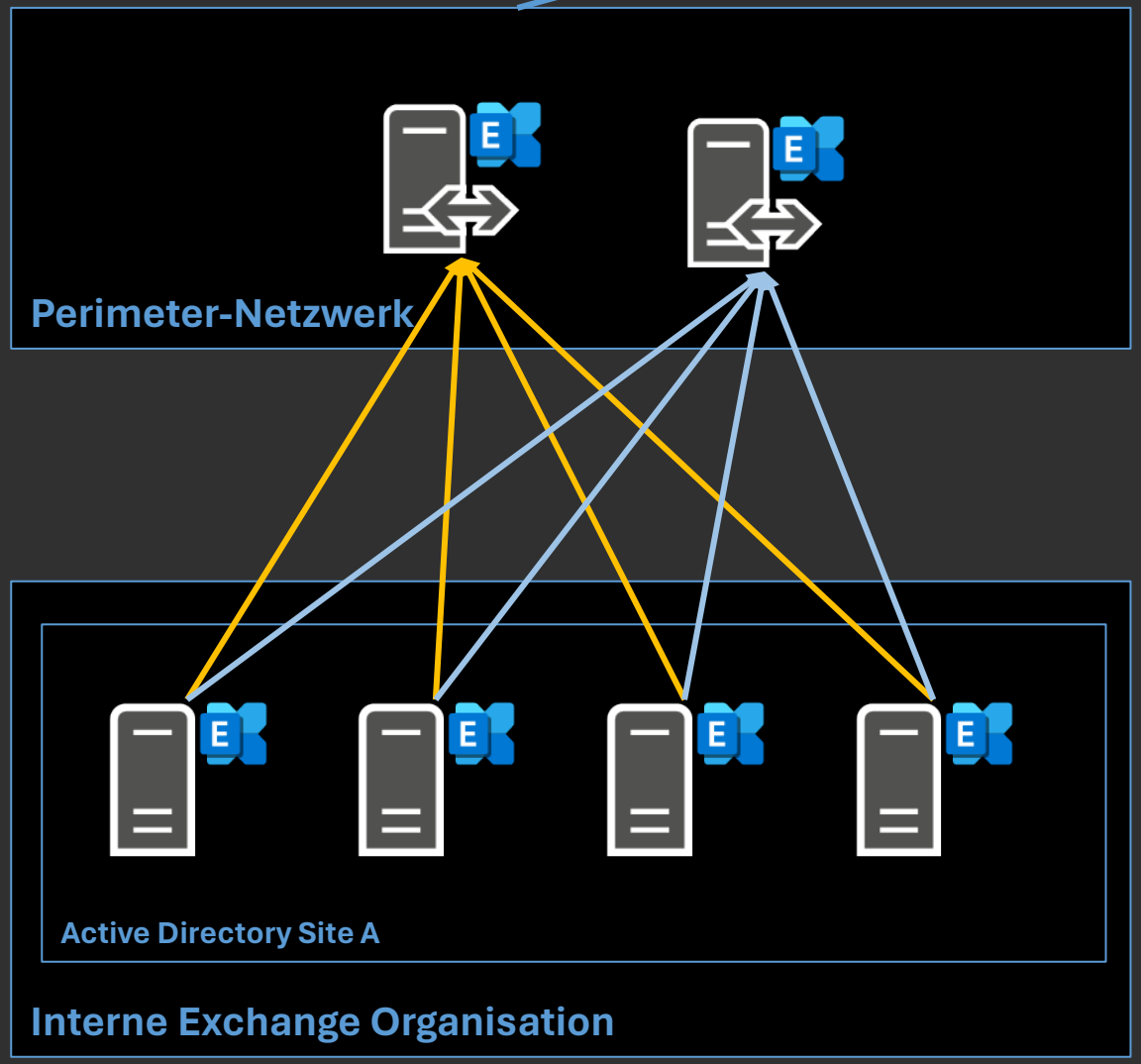
- Vereinfachte Darstellung einer EdgeSync-Synchronisierung aus einer Active Directory Site zu einem Edge-Transport-Server

1 Server + 1 AD-Site



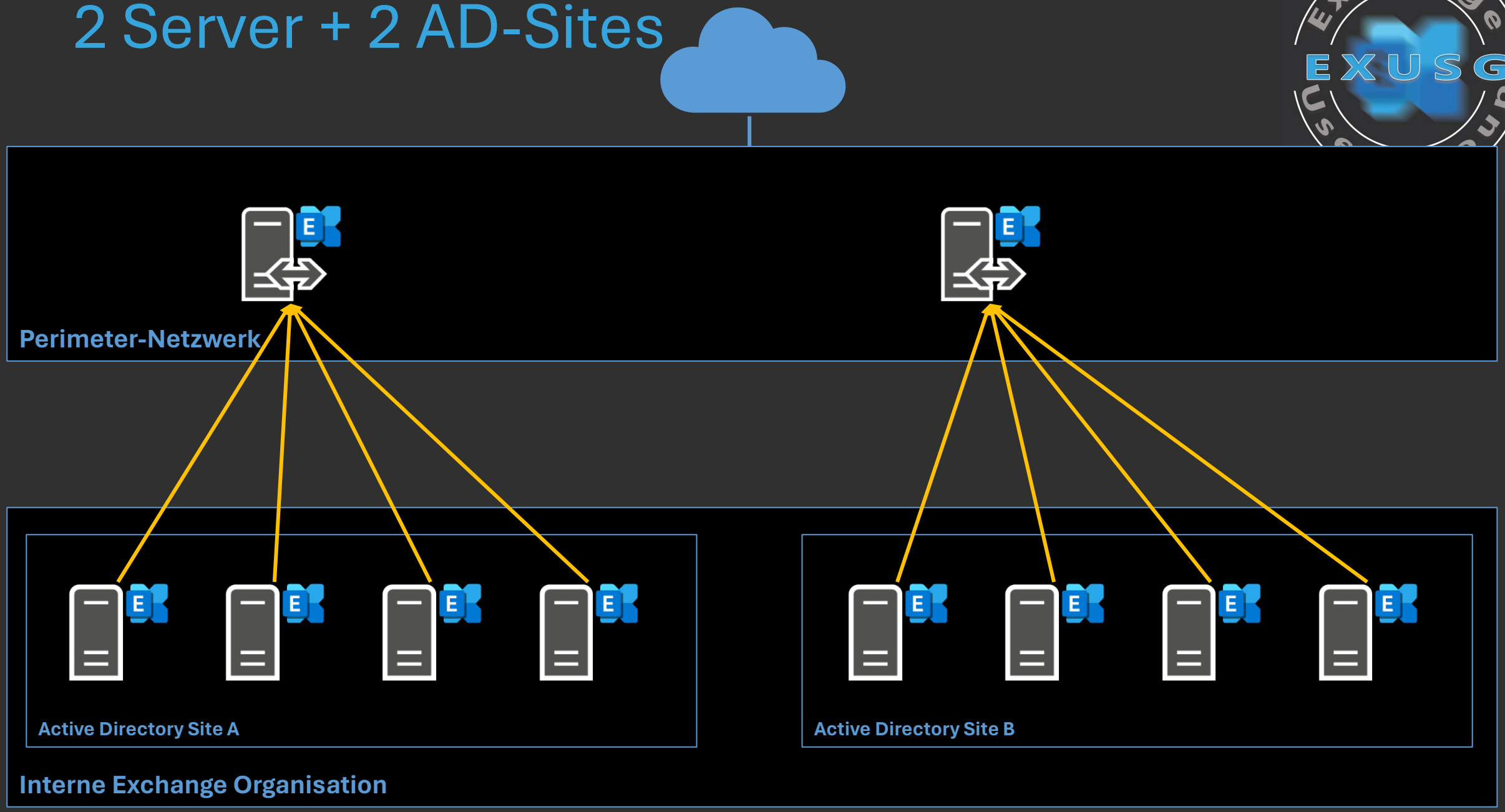
- Jeder Exchange Server verbindet sich eigenständig per EdgeSync zum abonnierten Edge-Transport-Server

2 Server + 1 AD-Site

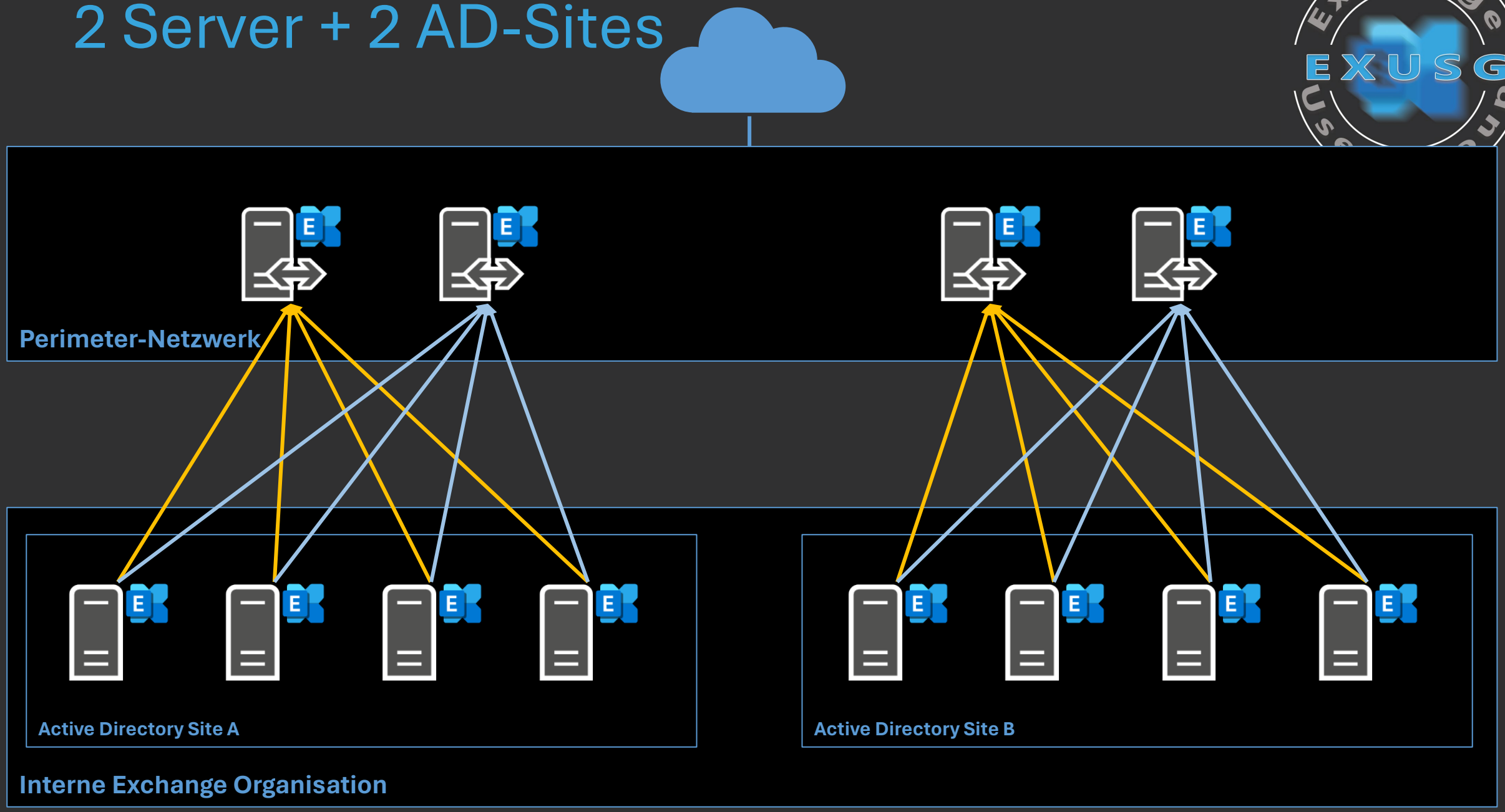


- Jeder Exchange Server verbindet sich eigenständig per EdgeSync zum abonnierten Edge-Transport-Server
- Dies gilt für jeden Edge-Transport-Server, der zu dieser Active Directory Site abonniert ist

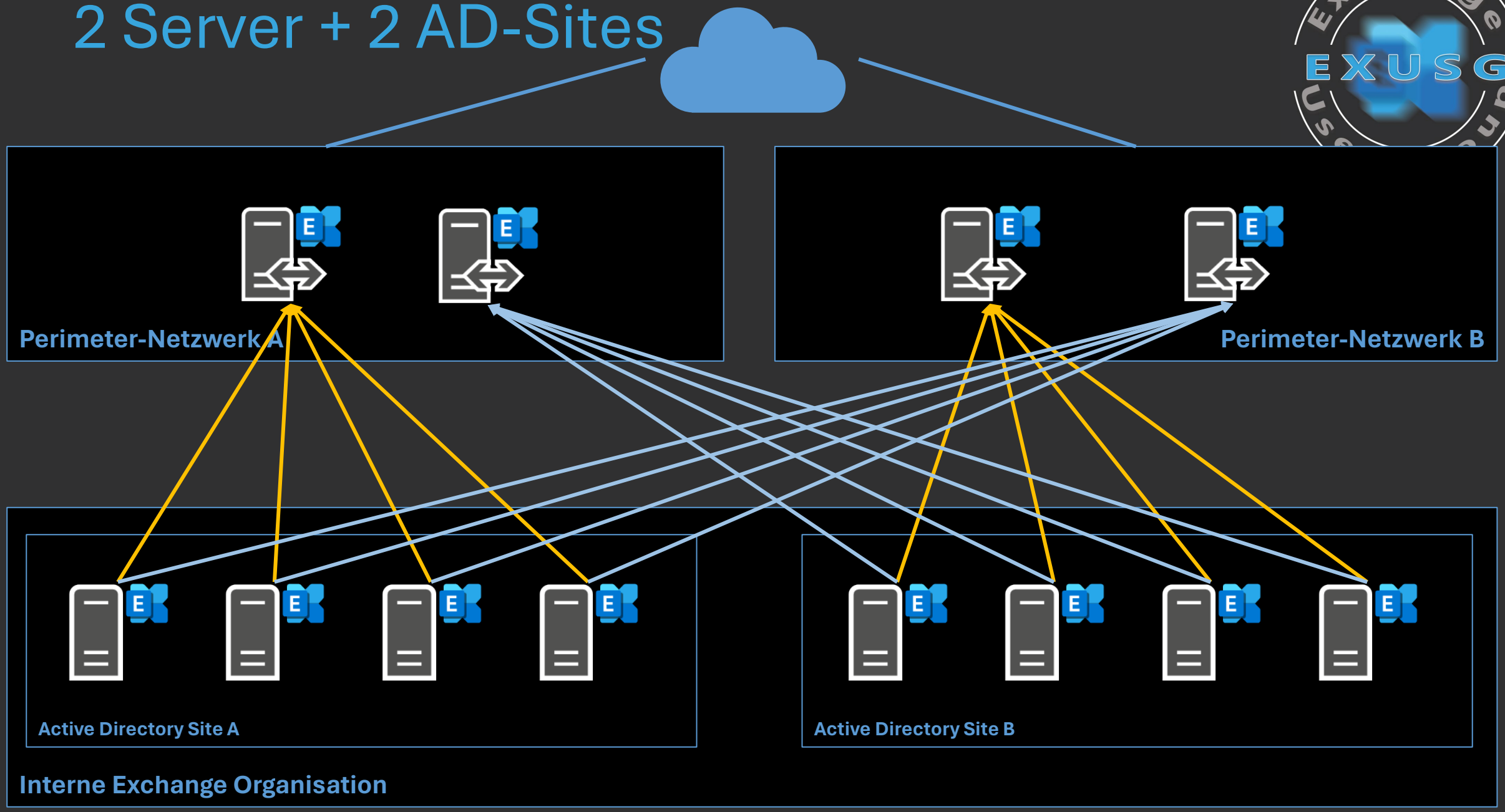
2 Server + 2 AD-Sites



2 Server + 2 AD-Sites



2 Server + 2 AD-Sites



EdgeSync Replication Accounts

- **ESRA.edge** → ESRA-Edge-Konto
  - EdgeSync-Replikationskonto des Edge-Transport-Server-Objektes
  - Verschlüsselt mit dem öffentlichen Schlüssel des Standardzertifikates des Edge-Transport-Servers
  - Gespeichert im Edge-Server-Konfigurationsobjekt
  - Jeder Postfach-Server verschlüsselt das Konto mit dem eigenen Standardzertifikat und speichert es im eigenen Konfigurationsobjekt

EdgeSync Replication Accounts

- **ESRA.edge.Mailboxname.#** →ESRA-Postfach-Server-Konten
  - EdgeSync-Replikationskonto eines Exchange Postfach-Servers
  - Verschlüsselt mit dem öffentlichen Schlüssel des Standardzertifikates des lokalen Transportdienstes
  - Die maximale Kennwortlänge des Windows-Betriebssystems definiert die Kennwortlänge des ESRA-Kontos --> 344 Zeichen (Ziffern) bei Windows Server 2019
  - Gespeichert im Exchange-Server-Konfigurationsobjekt
  - ESRA-Anmeldeinformationen werden automatisch erneuert
    - Neues ESRA-Konto 7 Tage vor Ablauf, 3 Tage vor Ablauf effektiv in Nutzung

Exchange Server und EdgeSync

- Ein neues Edge-Abonnement erstellt ein neues Konfigurationsobjekt im Active Directory
  - Edge-Zertifikat wird im Objekt gespeichert
    - *msExchServerInternalTLSCert*
- Jeder Exchange Server der Active Directory Site erhält eine Benachrichtigung über ein neues Edge-Abonnement
  - Ein **serverspezifisches ESRA-Edge-Konto** für den neuen Edge-Transport-Server wird erstellt und mit dem öffentlichen Schlüssel des eigenen Transportdienstes verschlüsselt
  - Ein **serverspezifisches ESRA-Postfach-Server-Konto** für die **Authentifizierung am Edge-Transport-Server** wird erstellt und mit dem lokalen Transportzertifikat verschlüsselt
    - *msExchServerInternalTLSCert*
  - Verschlüsselte Kontoinformationen werden im Postfach-Server-Objekt gespeichert
    - *msExchEdgeSyncCredential*

Lokale Exchange Organisation

EdgeSync-Konten eines Postfach-Servers
3 Einträge je Edge

Abonnierte Edge-Transport-Server

Exchange Postfach-Server

ADSI Edit

File Action View Help

CN=Device Registration Configuration
CN=Group Key Distribution Service
CN=Microsoft Exchange
CN=Active Directory Connections
CN=
CN=Address Lists Container
CN=AddressBook Mailbox Policies
CN=Addressing
CN=Administrative Groups
CN=
CN=Exchange Administrative Grou
CN=Advanced Security
CN=Arrays
CN=Database Availability Grou
CN=Databases
CN=Folder Hierarchies
CN=Routing Groups
CN=Servers
CN=
CN=
CN=Microsoft MTA
CN=Protocols
CN=
CN=
CN=
CN=
CN=
CN=
CN=
CN=Approval Applications
CN=Auth Configuration
CN=Auth Policies
CN=Availability Configuration
CN=Client Access
CN=Connections

Name	Class	Distinguished N
CN=	container	CN=Connector
CN=InformationStore	msExchInfor...	CN=Informatio
CN=Microsoft MTA	mTA	CN=Microsoft
CN=Microsoft System Atte...	exchangeAd...	CN=Microsoft S
CN=Protocols	protocolCfg...	CN=Protocols,C
CN=Transport Configuration	msExchExch...	CN=Transport C

Actions
CN=inmxms11
More Actions

CN= Properties

Attribute Editor | Security

Attributes:

Attribute	Value
msExchContentAggregationMaxNumberOfAttempts	3
msExchContentAggregationRemoteConnectionTimeout	100
msExchCurrentServerRoles	16423
msExchCustomerFeedbackEnabled	FALSE
msExchDataLossForAutoDatabaseMount	6
msExchDataPath	D:\Prograr
msExchEdgeSyncAdamSSLPort	50636
msExchEdgeSyncCredential	<?xml vers
msExchELCAuditLogFileAgeLimit	0
msExchELCAuditLogFileSizeLimit	10485760
msExchELCAuditLogPath	D:\Prograr
msExchHomeRoutingGroup	CN=Excha
msExchHttpProtocolLogAgeQuotaInHours	604800
msExchHTTPProtocolLogDirectorySizeQuota	26214400

Edit | Filter

OK | Cancel | Apply | Help

Multi-valued Octet String Editor

Attribute: msExchEdgeSyncCredential

Values:

<?xml version="1.0"?><EdgeSyncCredential xmlns:x
<?xml version="1.0"?><EdgeSyncCredential xmlns:x
<?xml version="1.0"?><EdgeSyncCredential xmlns:x
<?xml version="1.0"?><EdgeSyncCredential xmlns:x
<?xml version="1.0"?><EdgeSyncCredential xmlns:x
<?xml version="1.0"?><EdgeSyncCredential xmlns:x

Add | Remove | Edit

OK | Cancel

ESBRA-Edge-Konto


```
<?xml version="1.0"?>

<EdgeSyncCredential xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <EdgeServerFQDN>edge02.varunagroup.de</EdgeServerFQDN>

  <ESRAUsername>CN=ESRA.edge02,CN=Services,CN=Configuration,CN={3FF3B938-06C7-4655-9B4D-
DB88AD786F26}</ESRAUsername>

  <EncryptedESRAPassword>KMYN9g69oeHM7aJCsM09JLyTk71fUgkhsXyJI7...</EncryptedESRAPassword>

  <EffectiveDate>638089294466151552</EffectiveDate>

  <Duration>864000000000</Duration>

  <IsBootStrapAccount>true</IsBootStrapAccount>

</EdgeSyncCredential>
```

ESRA-Postfach-Server-Konto – 1


```
<?xml version="1.0"?>
<EdgeSyncCredential xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <EdgeServerFQDN>edge02.varunagroup.de</EdgeServerFQDN>
  <ESRAUsername>cn=ESRA.edge02.dehvnmx03.0,CN=Services,CN=Configuration,CN={99018E79-8BAB-4C17-A85A-
4F3996855D12}</ESRAUsername>
  <EncryptedESRAPassword>JT5tOLaA62RlJrWWCIyrOi5JS5ZVoDXlRNn1I...</EncryptedESRAPassword>
  <EdgeEncryptedESRAPassword>VDmanMpqBiia3S7Cdmvu1NsBPD/YWSI/S...</EdgeEncryptedESRAPassword>
  <EffectiveDate>638202702915378844</EffectiveDate>
  <Duration>12960000000000</Duration>
  <IsBootStrapAccount>false</IsBootStrapAccount>
</EdgeSyncCredential>
```


Sonntag, **21. Mai 2023**
12:51:31

ESRA-Postfach-Server-Konto – 2


```
<?xml version="1.0"?>
<EdgeSyncCredential xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <EdgeServerFQDN>edge02.varunagroup.de</EdgeServerFQDN>
  <ESRAUsername>cn=ESRA.edge02.dehvnmx03.1,CN=Services,CN=Configuration,CN={99018E79-8BAB-4C17-A85A-
4F3996855D12}</ESRAUsername>
  <EncryptedESRAPassword>i/lmWIruFFP2E4kv/p3UbAierdciq738o...</EncryptedESRAPassword>
  <EdgeEncryptedESRAPassword>LD4OCt3JFw0fOY3QZoMgqgop6lKLt...</EdgeEncryptedESRAPassword>
  <EffectiveDate>638215662915378844</EffectiveDate>
  <Duration>12960000000000</Duration>
  <IsBootStrapAccount>false</IsBootStrapAccount>
</EdgeSyncCredential>
```


Montag, **5. Juni 2023**
12:51:31

Exchange Server und Edge Sync

Zusammenfassung

- Initiale EdgeSync-Replikation zu AD LDS
  - Der ausführende Postfach-Server für die initiale Replikation wird zufällig ausgewählt
  - Replikation neu erstellter ESRA-Postfach-Server-Konten für die Authentifizierung aller weiteren Replikationen
    → zeitliche Verzögerung, bis alle Exchange Server korrekt replizieren

- Weitere EdgeSync-Replikationen
  - Exchange Postfach-Server (MSExchangeEdgeSync) baut eine LDAPS-Verbindung auf TCP-Port 50636 auf
  - MSExchangeEdgeSync auf dem Postfach-Server überprüft das vom Edge-Transport-Server präsentierte TLS-Zertifikat
  - MSExchangeEdgeSync präsentiert dem Edge-Transport-Server die ESRA-Postfach-Server-Anmeldung
  - Edge-Transport-Server validiert die Anmeldeinformationen gegen die Information in AD LDS
  - MSExchangeEdgeSync überträgt die Anmeldeinformationen weiterer Postfach-Server, die erst **nach** dieser Übertragung EdgeSync erfolgreich ausführen können

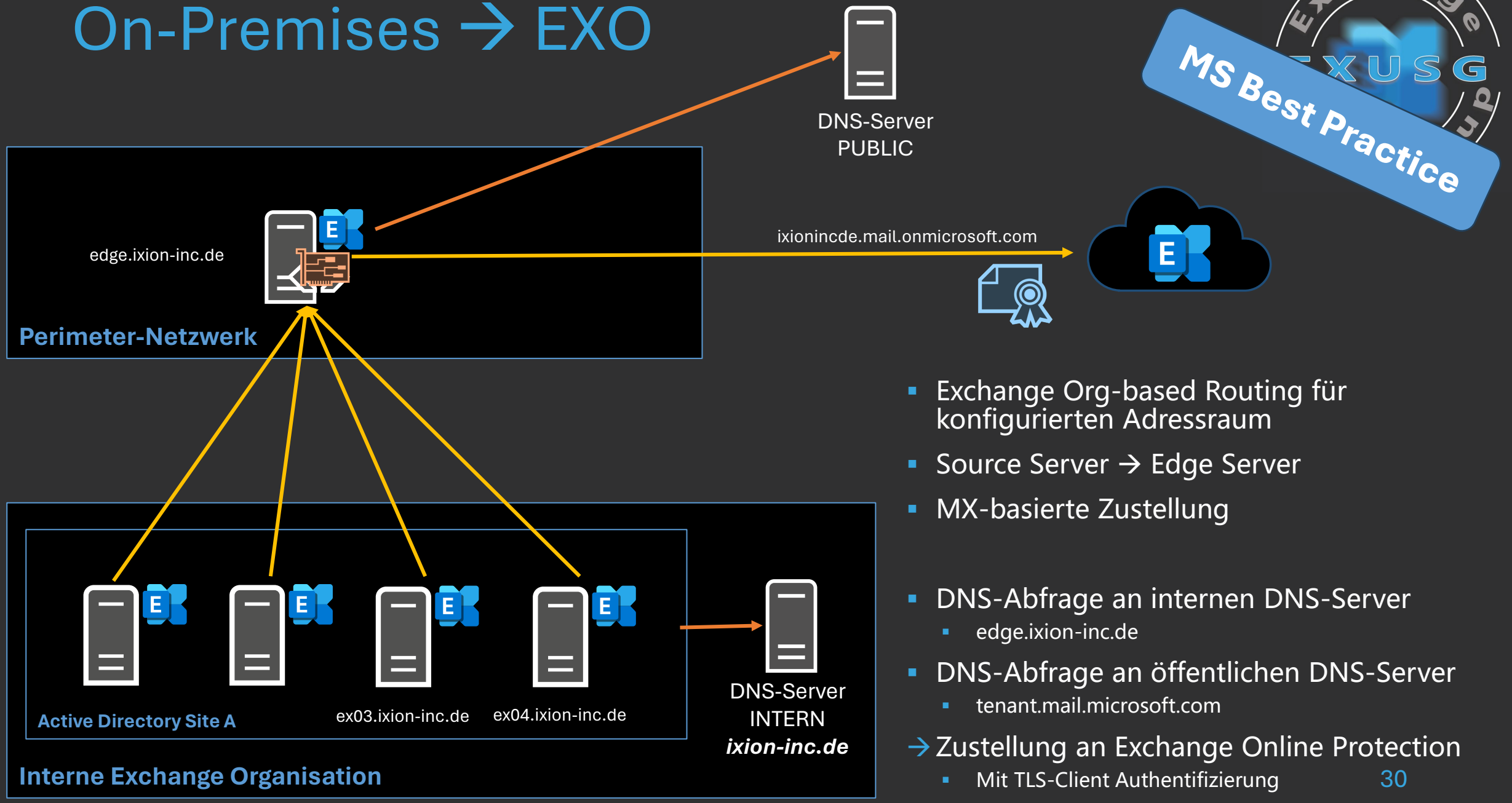
Exchange Server und EdgeSync

Zusammenfassung

- Wechsel der Standard-TLS-Zertifikate für den Exchange Edge-Transportdienst erfordern eine Erneuerung des Edge-Abonnements
- Die Zertifikatsschlüssel der TLS-Zertifikate müssen **CAPI1**-verschlüsselt sein, **CNG**-Zertifikate werden nicht unterstützt

SMTP-Transport

On-Premises → EXO

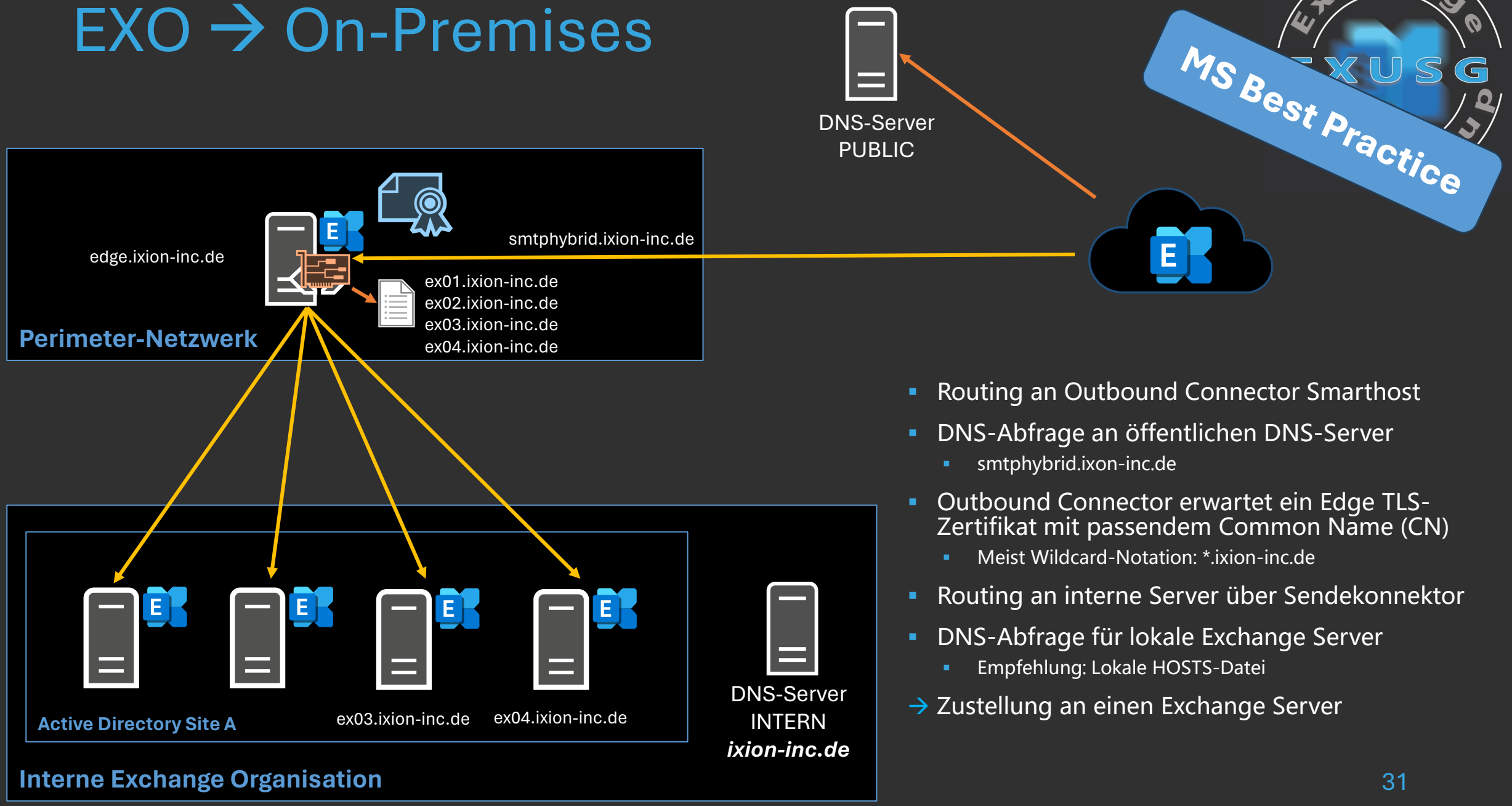


- Exchange Org-based Routing für konfigurierten Adressraum
- Source Server → Edge Server
- MX-basierte Zustellung

- DNS-Abfrage an internen DNS-Server
  - edge.ixion-inc.de
- DNS-Abfrage an öffentlichen DNS-Server
  - tenant.mail.microsoft.com

→ Zustellung an Exchange Online Protection
  - Mit TLS-Client Authentifizierung

EXO → On-Premises



- Routing an Outbound Connector Smarthost
- DNS-Abfrage an öffentlichen DNS-Server
  - smtphybrid.ixon-inc.de
- Outbound Connector erwartet ein Edge TLS-Zertifikat mit passendem Common Name (CN)
  - Meist Wildcard-Notation: *.ixion-inc.de
- Routing an interne Server über Sendekonnektor
- DNS-Abfrage für lokale Exchange Server
  - Empfehlung: Lokale HOSTS-Datei

→ Zustellung an einen Exchange Server

Edge Sendekonnektor

- Name : Outbound to Office 365 - 12c1a4b4-d1d6-471d-b2cf-6b99122a127b
- AddressSpaces : {SMTP:**ixionincde.onmicrosoft.com**;1, smtp:**ixionincde.mail.onmicrosoft.com**;1}
- Fqdn : **smtphybrid.ixion-inc.de**
- SourceTransportServers : {**Edge**}
- TlsDomain : **mail.protection.outlook.com**
- TlsAuthLevel : **DomainValidation**
- TlsCertificateName : <I>CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB<S>**CN=smtphybrid.ixion-inc.de**
- MaxMessageSize : **35 MB** (36,700,160 bytes)

Edge Sendekonnektor

- Name : EdgeSync - Inbound to Default-First-Site-Name
- AddressSpaces : {smtp:--;100}
- Fqdn :
- SourceTransportServers : {**Edge**}
- TlsDomain :
- TlsAuthLevel :
- TlsCertificateName :
- MaxMessageSize : **Unlimited**

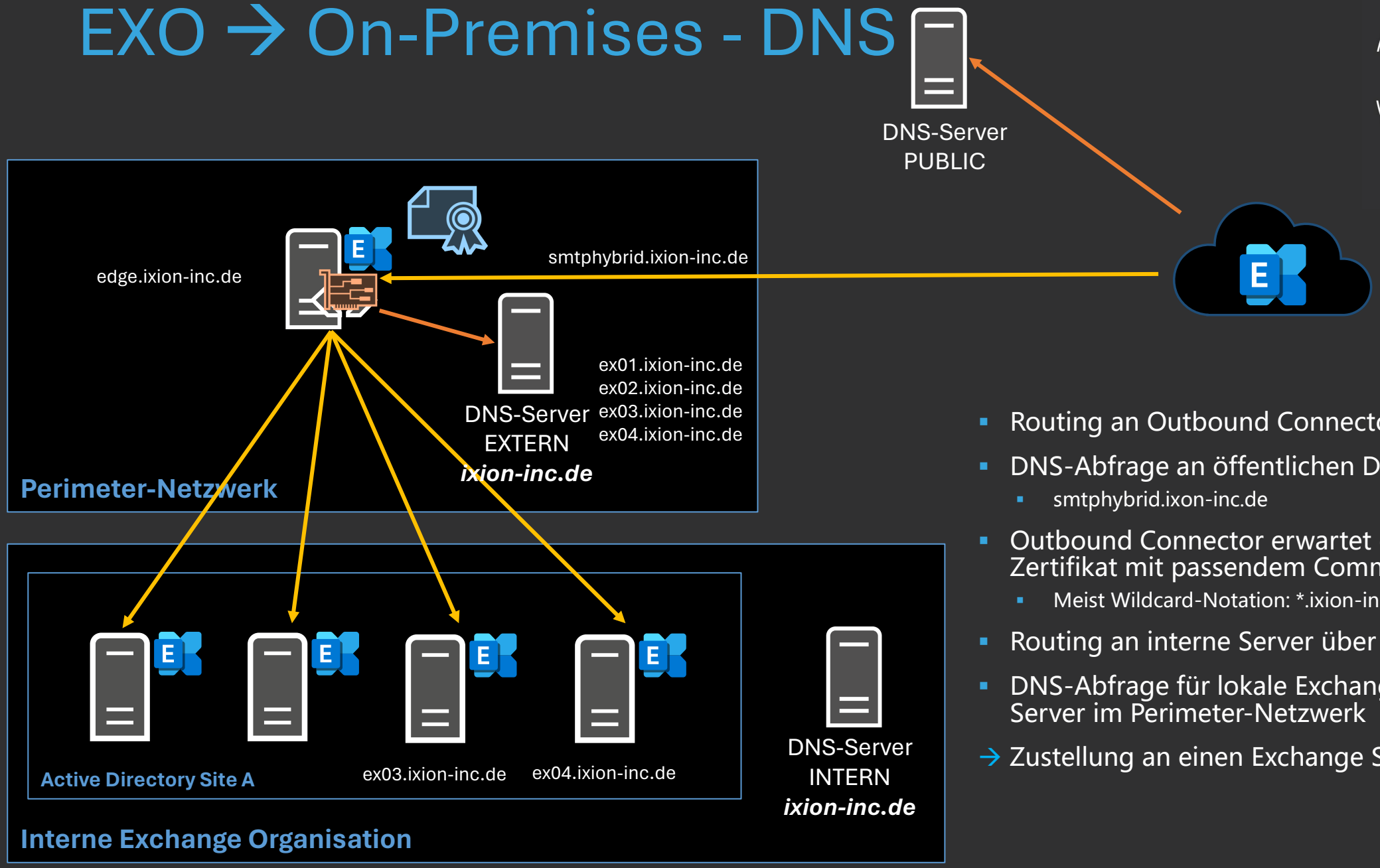
Edge Empfangskonnektor

- Name : Default internal receive connector EDGE
- Banner :
- Fqdn : **smtphybrid.ixion-inc.de**
- AuthMechanism : **Tls, ExchangeServer**
- Bindings : {**0.0.0.0:25**}
- RemoteIPRanges : {**0.0.0.0-255.255.255.255**}
- TlsDomainCapabilities : {**mail.protection.outlook.com:AcceptOorgProtocol**}

Edge-Transport-Server

Variationen und Probleme

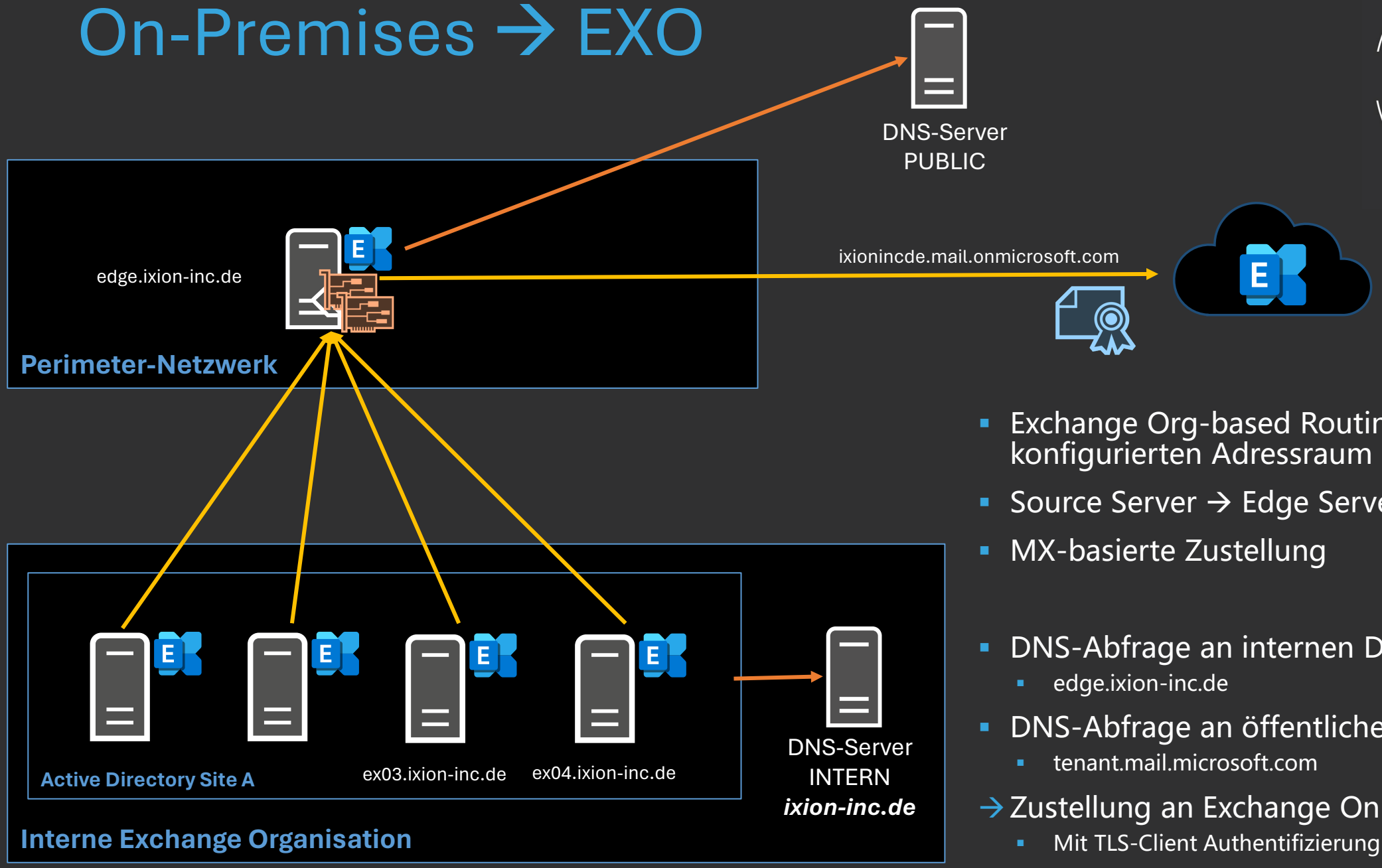
EXO → On-Premises - DNS



- Routing an Outbound Connector Smarthost
- DNS-Abfrage an öffentlichen DNS-Server
  - smtphybrid.ixon-inc.de
- Outbound Connector erwartet ein Edge TLS-Zertifikat mit passendem Common Name (CN)
  - Meist Wildcard-Notation: *.ixion-inc.de
- Routing an interne Server über Sendekonnektor
- DNS-Abfrage für lokale Exchange Server an DNS-Server im Perimeter-Netzwerk

→ Zustellung an einen Exchange Server

On-Premises → EXO



- Exchange Org-based Routing für konfigurierten Adressraum
- Source Server → Edge Server
- MX-basierte Zustellung

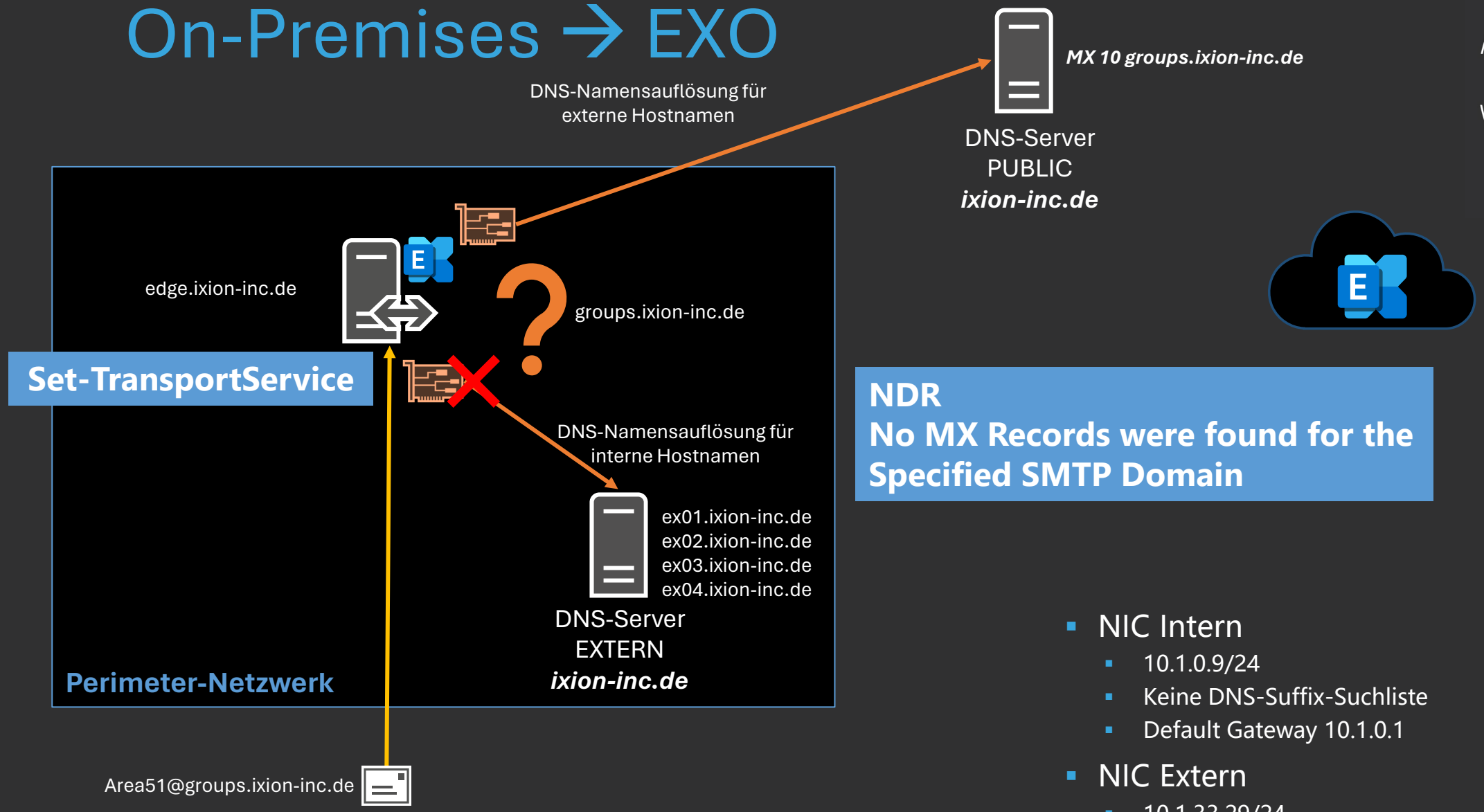
- DNS-Abfrage an internen DNS-Server
  - edge.ixion-inc.de
- DNS-Abfrage an öffentlichen DNS-Server
  - tenant.mail.microsoft.com

→ Zustellung an Exchange Online Protection
  - Mit TLS-Client Authentifizierung

Ist Edge-Transport-Server ein Router?

Am Beispiel für Microsoft 365 Gruppen und einer Hybriddomäne

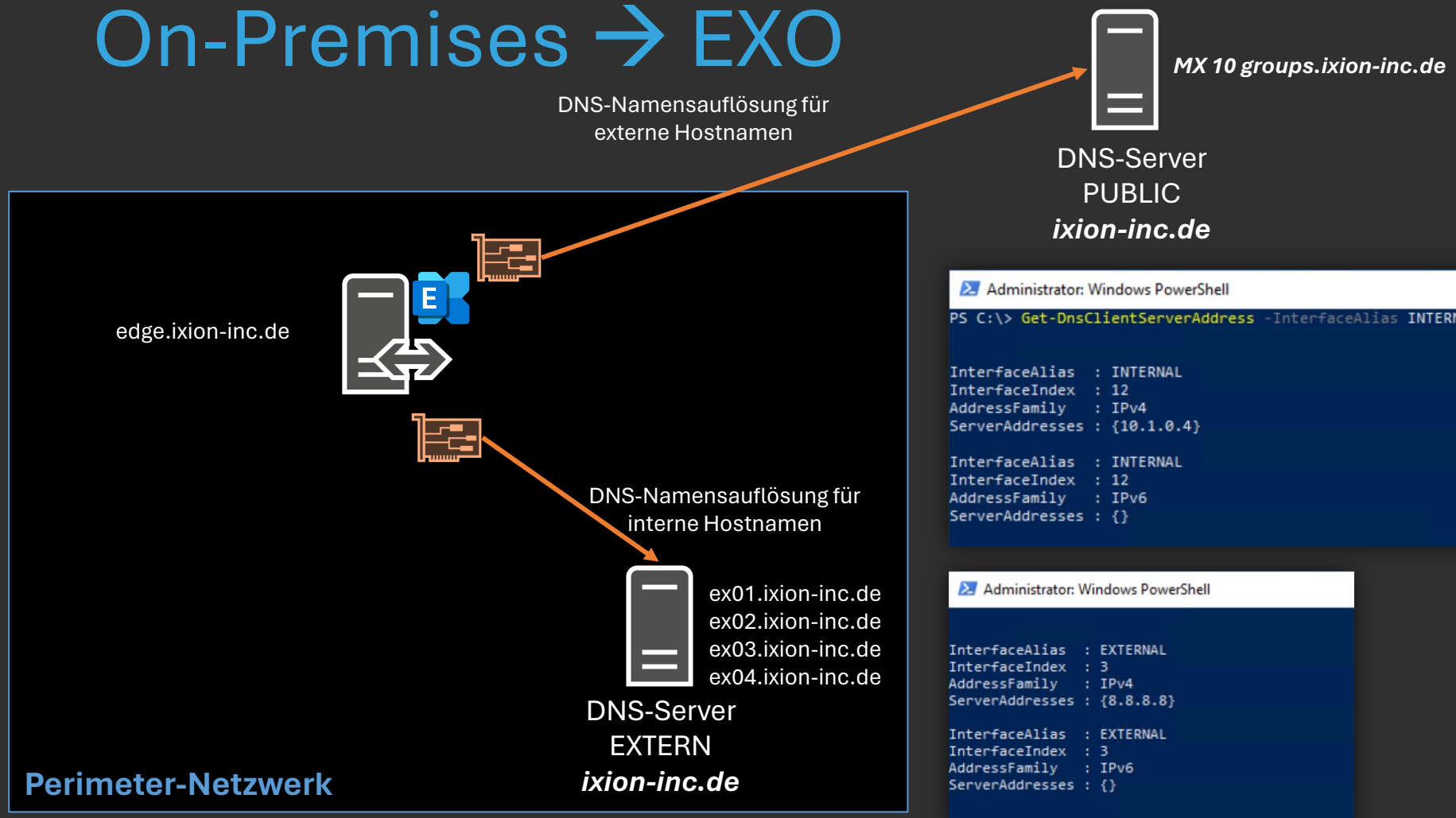
On-Premises → EXO



NDR
No MX Records were found for the Specified SMTP Domain

- NIC Intern
  - 10.1.0.9/24
  - Keine DNS-Suffix-Suchliste
  - Default Gateway 10.1.0.1
- NIC Extern
  - 10.1.33.29/24
  - Keine DNS-Suffix-Suchliste
  - Default Gateway 10.1.31.1

On-Premises → EXO



Administrator: Windows PowerShell

```
PS C:\> Get-DnsClientServerAddress -InterfaceAlias INTERNAL | fl


InterfaceAlias  : INTERNAL
InterfaceIndex  : 12
AddressFamily   : IPv4
ServerAddresses : {10.1.0.4}

InterfaceAlias  : INTERNAL
InterfaceIndex  : 12
AddressFamily   : IPv6
ServerAddresses : {}
```

Administrator: Windows PowerShell

```
InterfaceAlias  : EXTERNAL
InterfaceIndex  : 3
AddressFamily   : IPv4
ServerAddresses : {8.8.8.8}

InterfaceAlias  : EXTERNAL
InterfaceIndex  : 3
AddressFamily   : IPv6
ServerAddresses : {}
```

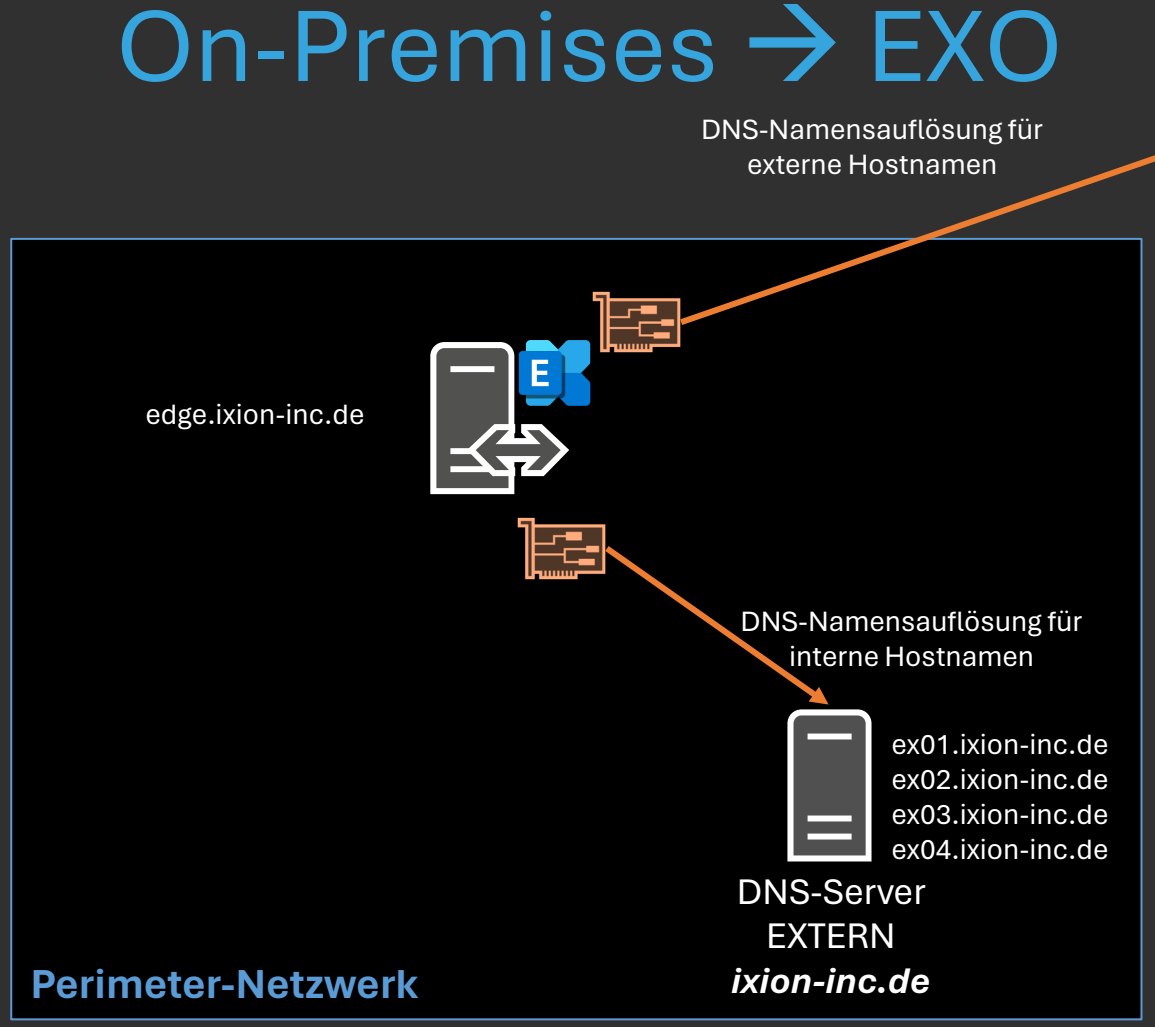
Exchange Transport Service

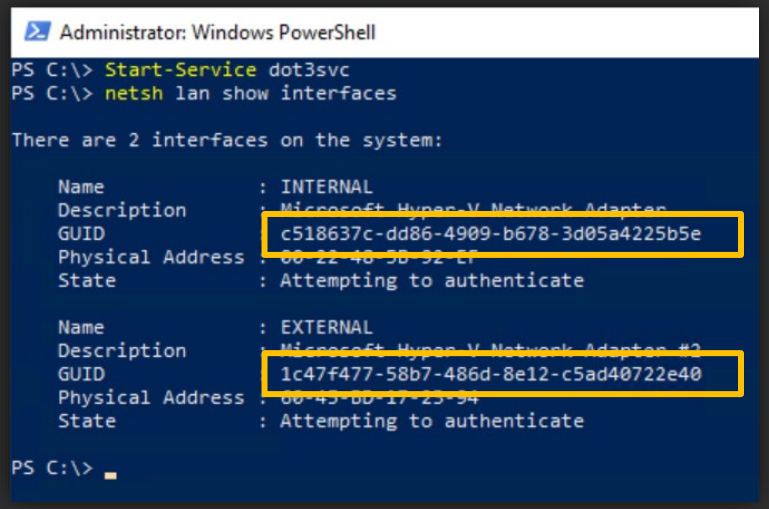
DNS-Adapter Standardeinstellungen

- `InternalDNSAdapterEnabled : True`
- `InternalDNSAdapterGuid : 00000000-0000-0000-0000-000000000000`
- `InternalDNSProtocolOption : Any`
- `InternalDNSServers : {}`

- `ExternalDNSAdapterEnabled : True`
- `ExternalDNSAdapterGuid : 00000000-0000-0000-0000-000000000000`
- `ExternalDNSProtocolOption : Any`
- `ExternalDNSServers : {}`

On-Premises → EXO





- Interface Guids abfragen
  - Start-Service dot3svc
  - netsh lan show interfaces

Exchange Transport Service

Setzen der NIC Adapter Guids

- `InternalDNSAdapterEnabled : True`
- `InternalDNSAdapterGuid : c518637c-dd86-4909-b678-3d05a4225b5e`
- `InternalDNSProtocolOption : Any`
- `InternalDNSServers : {10.1.0.4}`

?

- `ExternalDNSAdapterEnabled : True`
- `ExternalDNSAdapterGuid : 1c47f477-58b7-486d-8e12-c5ad40722e40`
- `ExternalDNSProtocolOption : Any`
- `ExternalDNSServers : {8.8.8.8, 8.8.4.4}`

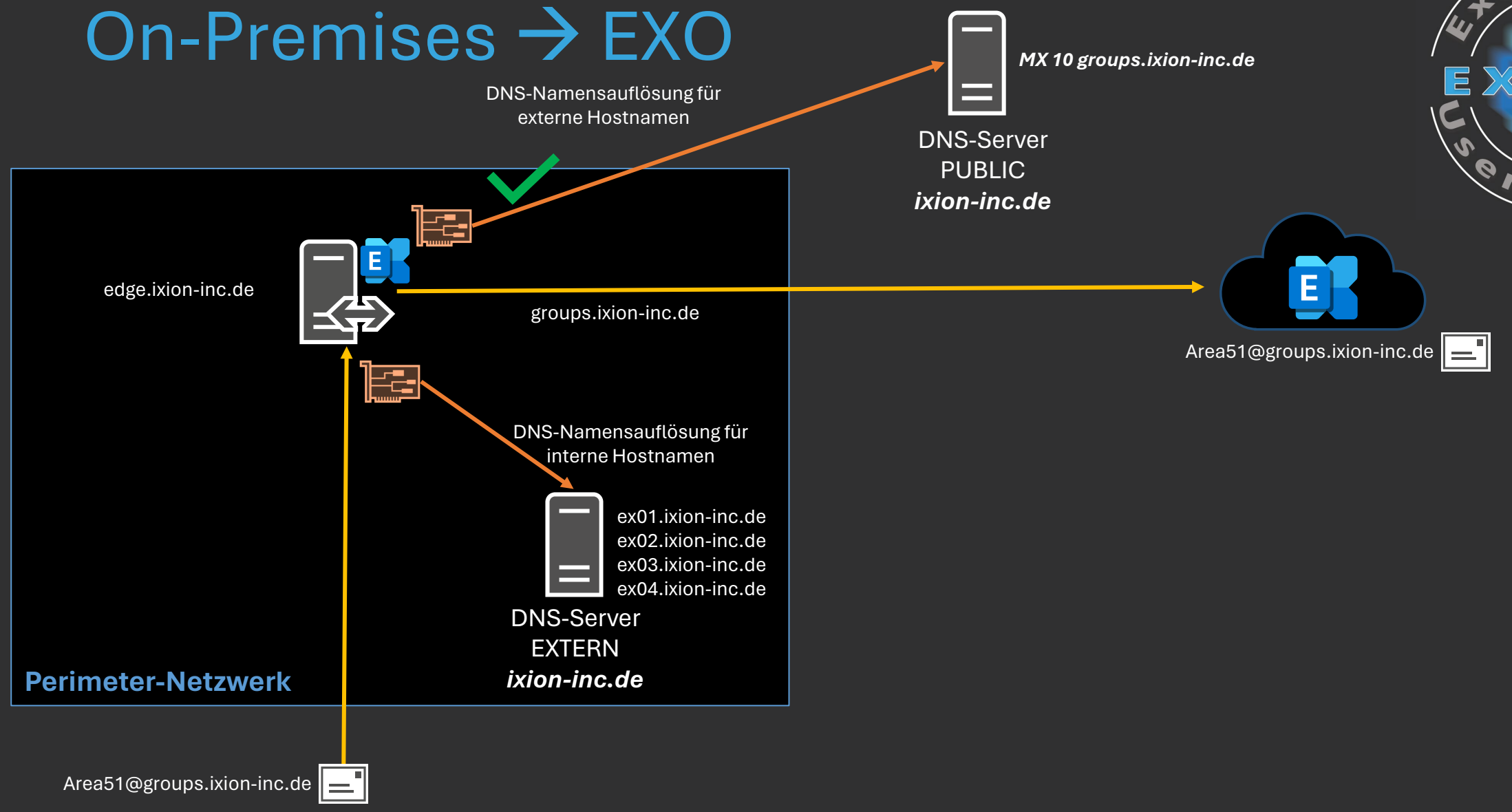
Exchange Transport Service

Externes Netzwerk-Interface

- `InternalDNSAdapterEnabled : True`
- `InternalDNSAdapterGuid : c518637c-dd86-4909-b678-3d05a4225b5e`
- `InternalDNSProtocolOption : Any`
- `InternalDNSServers : {10.1.0.4}`

- `ExternalDNSAdapterEnabled : False`
- `ExternalDNSAdapterGuid : 1c47f477-58b7-486d-8e12-c5ad40722e40`
- `ExternalDNSProtocolOption : Any`
- `ExternalDNSServers : {8.8.8.8, 8.8.4.4}`

On-Premises → EXO



Ressourcen

- Set-TransportService
- Advanced Office 365 Routing: Locking Down Exchange On-Premises when MX points to Office 365
- Edge-Abonnementanmeldeinformationen
- How to Manage AD LDS on an Edge Transport Server with ADSIEdit | Practical365
- Edge Transport Server, EdgeSync und TLS-Zertifikate

Exchange Server Security Update August 2023 und mehr

Thomas Stensitzki

Security Update August 2023

- Version 1 – 8. August 2023 nur lauffähig auf englischsprachigen Systemen
  - Verteilung per Download und WSUS
- Version 2 – 15. August 2023

HSTS-Unterstützung für Exchange 2016/2019

- Nicht zu verwechseln mit MTA-STS
- Zusätzliche Absicherung von HTTPS
  - Konfiguration der Internet Information Services (IIS)

Exchange Server 2019

```
Import-Module IISAdministration
Reset-IISServerManager -Confirm:$false
Start-IISCommitDelay

$sitesCollection = Get-IISConfigSection -SectionPath "system.applicationHost/sites" | Get-IISConfigCollection
$siteElement = Get-IISConfigCollectionElement -ConfigCollection $sitesCollection -ConfigAttribute @{"name"="Default
Web Site"}
$hstsElement = Get-IISConfigElement -ConfigElement $siteElement -ChildElementName "hsts"
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "enabled" -AttributeValue $true
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "max-age" -AttributeValue 300
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "includeSubDomains" -AttributeValue $true
Stop-IISCommitDelay
```

Ankündigung

HSTS-Unterstützung für Exchange 2016/2019

- Client
  - Forcierter Wechsel zu HTTPS nach Empfang des Strict-Transport-Security Headers
- TLS-Zertifikat
  - Aktiver Gültigkeitszeitraum und sichere Vertrauensstellung des Clients
  - CN/SAN muss die Domäne oder Subdomäne enthalten, die der Client aufgerufen hat
- Funktion
  - Client nutzt immer HTTPS, auch bei HTTP-Links oder direkter Eingabe der Adresse ohne Protokoll
  - Keine Möglichkeit, um Zertifikatswarnungen zu umgehen

- HSTS-Preload
  - https://hstspreload.org

Extended Protection ab CU14

- Automatische Aktivierung ab Exchange Server 2019 CU14
- Reduzierung von "Man in the Middle"-Angriffen
- Windows Feature für IIS seit 7.5 (2008 R2)
  - Dokumentation
- Implementierung per PowerShell-Skript
  - https://aka.ms/ExchangeEPScript

"We send you thoughts and prayers, and very strong but gentle guidance to update your servers to the latest SU immediately."

Ankündigung

Exchange Q & A

Exchange Q & A

- Exchange Server 2019 CU 2023 H1 (CU13)

Organisatorisches

Exchange Coffee Talk

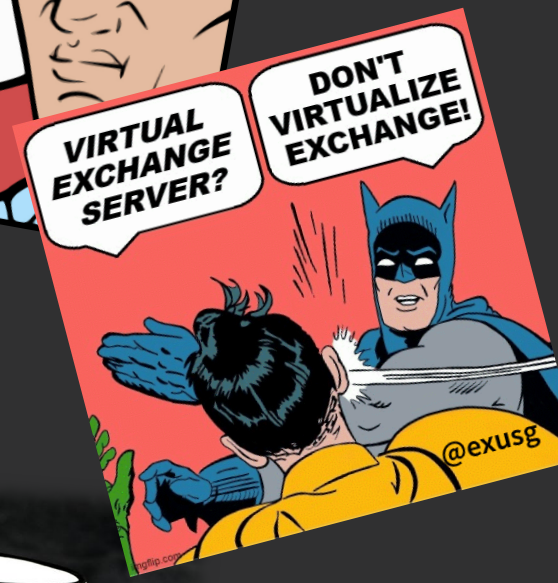
- Lockere Kaffeerunde
- Bringt eure Themen mit

- Einmal im Monat
  - Letzter Mittwoch im Monat
  - 17 Uhr
  - 1 Stunde

Exchange User Group

Organisatorisches

- **Exchange User Group Team**
  - Registrierung → Link auf Homepage
- **Themenvorschläge**
  - https://go.granikos.eu/EXUSG-Themen
- **Community Sticker**
  - https://go.granikos.eu/CommunitySticker
- **EXUSG Mugs**
  - https://go.granikos.eu/EXUSGMug



Exchange User Group

Organisatorisches

Exchange User Group

Nächster Termin **9. November 2023**

- MTA-STS, DANE und mehr, Andres Bohren
- TLS-Magie mit Exchange Server, Thomas Stensitzki

https://exusg.de

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