Network and Infrastructure Architecture DD-TEC-070

Introduction

Purpose

The purpose of this document is to outline the infrastructure and network architecture for SyWay project.

Scope

This document describes the high-level infrastructure and network design for SAP RISE and non-RISE deployments. It also covers the network design for specialized integration scenarios and deployment in China region.

Out of scope:

- Infrastructure and network design for SaaS applications.
- SD-WAN and cloud infrastructure detailed design or configurations.
- Existing Syensqo systems that SyWay project integrates with.
- SAP RISE and Azure operating model.

Assumptions

- Azure will be chosen as SyWay cloud service provider for all regions.
- Syensqo network will connect to Azure tenants via ExpressRoute for all regions
- Standard SAP RISE integration patterns will be leveraged when integrating S/4HANA, SAP connectors and SAP SaaS applications.
- As of writing this document, there are pending architectural decisions regarding North America & China, and RISE infrastructure. These designs will be added to this document as they are finalized.

Overview

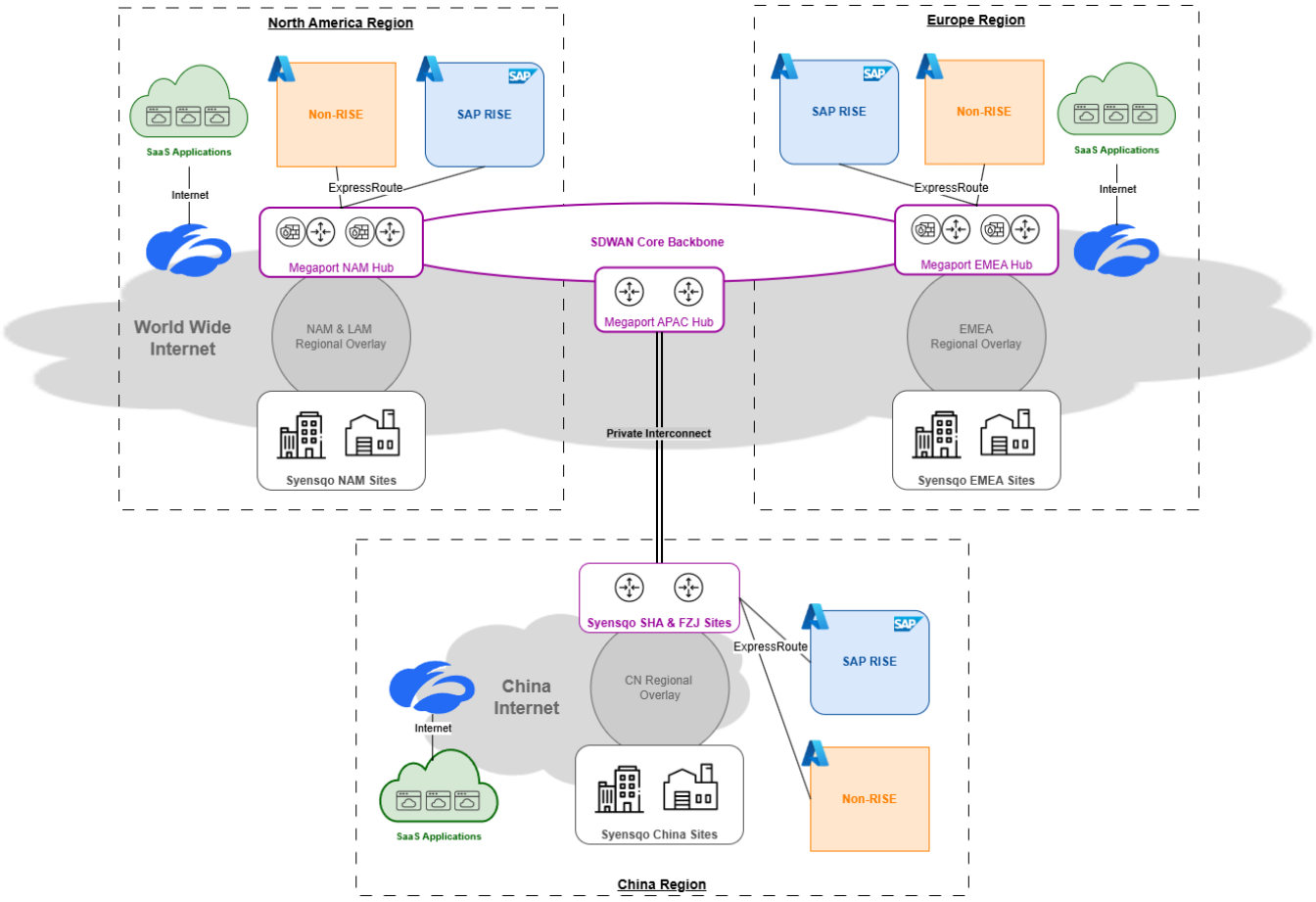
SyWay systems can be classified into 3 hosting models:

SAP RISE[1]	S/4HANA and SAP applications that are hosted in SAP RISE cloud tenants and managed by SAP.
Non-RISE	On-premise applications that cannot be hosted in SAP RISE and are hosted in Azure tenants managed by Syensqo IT.
SaaS	Applications that follow the SaaS model and are access from the internet

[1]See KDD026 - SAP S/4HANA Deployment Model for the comparison between various deployment options for S/4HANA and the decision.

In addition to the different hosting models, SyWay systems can be deployed to 1 or more regions (North America, Europe and China). The figure below describes how SyWay systems are deployed across Syensqo's network.

> The design for China SDWAN Hub is in progress and the diagram below will be updated after Syensqo network team completes the design.



Infrastructure Architecture

SAP RISE

Overview

S/4HANA is hosted in SAP RISE along with supporting connectors and web dispatchers. SyWay project would leverage a common Sandbox, Development landscape that are deployed in Europe region and individual Integration Testing, Training, UAT, Parallel Testing and Production systems that are deployed to all three regions.

The table below lists the landscape, systems and the corresponding system ID (SID) for the three different regions.

		S/4HANA (HANA DB)	Web Dispatcher	SAP Cloud connector	SAP Data Provisioning Agent	SAC Agent	OpenText Connector
Europe	Sandbox	ERS (HRS)	WRS	N/A	N/A	N/A	N/A
	Development	ERD (HRD)	WRD	CRD[1]	DRD[1]	SRD[1]	ORD[1]
	Integration Testing	ERT (HRT)	WRT	N/A	N/A	N/A	N/A
	Training	ER2 (HR2)	WR2	N/A	N/A	N/A	N/A
	UAT	ERQ (HRQ)	WRQ	N/A	N/A	N/A	N/A
	Parallel Testing	ER1 (HR1)	WR1	N/A	N/A	N/A	N/A
	Production	ERP (HRP)	WRP & WRH	CRP	DRP	SRP	ORP
North America	Integration Testing	*EXT (HXT)*	*WXT*	*CXD*[1]	*DXD*[1]	*SXD*[1]	*TBC*[1]
	Training	*EX2 (HX2)*	*WX2*	N/A	N/A	N/A	N/A
	UAT	*EXQ (HXQ)*	*WXQ*	N/A	N/A	N/A	N/A
	Parallel Testing	*EX1 (HX1)*	*WX1*	N/A	N/A	N/A	N/A
	Production	*EXP (HXP)*	*WXP*	*CXP*	*DXP*	*SXP*	*TBC*
China	Integration Testing	*ECT (HCT)*	*WCT*	*CCD*[1]	*DCD*[1]	*SCD*[1]	*OCD*[1]
	Training	*EC2 (HC2)*	*WC2*	N/A	N/A	N/A	N/A
	UAT	*ECQ (HCQ)*	*WCQ*	N/A	N/A	N/A	N/A
	Parallel Testing	*EC1 (HC1)*	*WC1*	N/A	N/A	N/A	N/A
	Production	*ECP (HCP)*	*WCP*	*CCP*	*DCP*	*SCP*	*OCP*

[1]System shared across all non-PRD systems

Landscape Provisioning

The following diagrams illustrates the different RISE landscapes that are provision for the different phases. Post Go-Live, INT and PAR landscapes will be decommissioned and a 5 tier landscape will be maintained.

Europe

High Availability and Disaster Recovery

The table below summaries the SLA for HA and DR for production and non-production systems

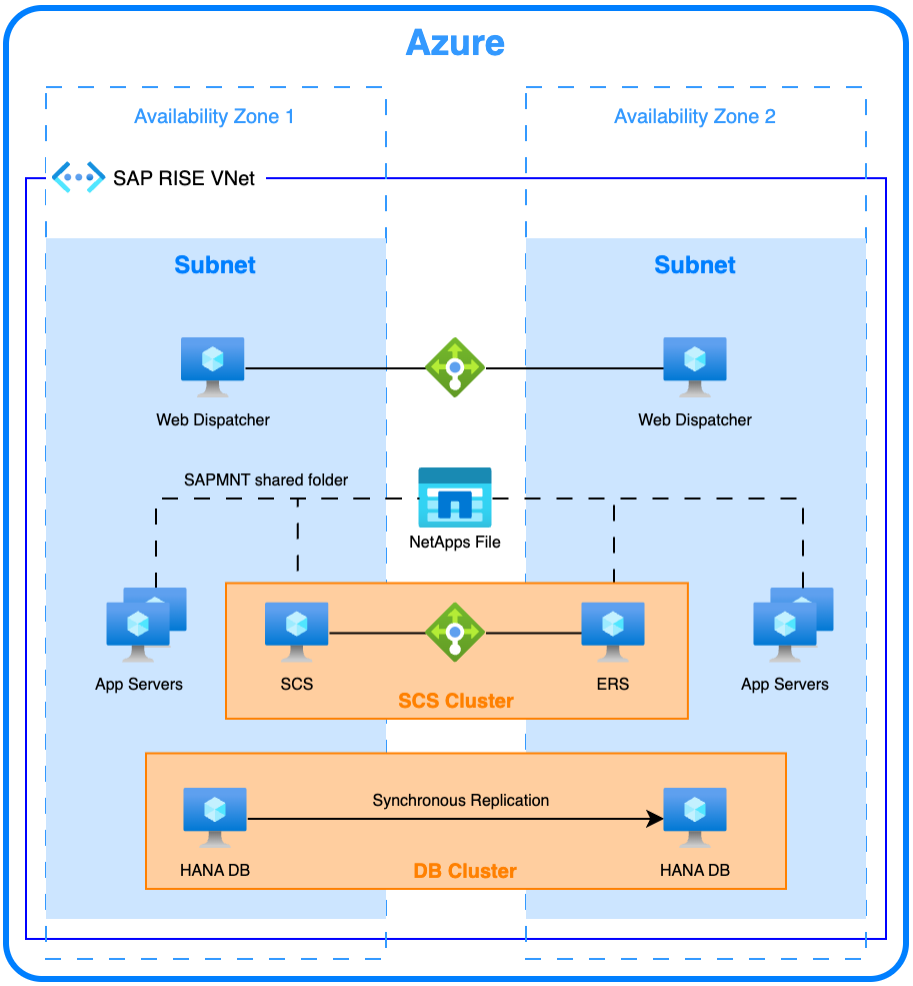
Landscape	Availability SLA	RPO	RTO
Production	99.9%	0	Contractually-guaranteed: 12 hours Achievable: ~10 minutes
Non-Production	98%	N/A	N/A

S/4HANA

In SAP RISE, High Availability (HA) and Disaster Recovery (DR) is applicable to Production instances. For SyWay project, S/4HANA Production is provisioned with the following RISE add-ons.

- Short distance disaster recovery
- 99.9% SLA

With these add-ons, S/4HANA production is deployed across 2 availability zones with synchronous database replication and automated fail-over via pacemaker clusters as shown below.



The table below describes how HA is achieved for the different components.

Component	HA Design
Web Dispatcher	Deployed to both AZs in active-active configuration and Azure load balancer is used to distribute incoming HTTP traffic to both instances.
S/4HANA Application servers	Two application servers are deployed to each AZs in an active-active configuration.
S/4HANA Message server (SCS & ERS)	Pacemaker cluster is configured between SCS and ERS servers to ensure SCS & ERS services fails over accordingly in the event of a failure.
SAPMNT Shared folder	NetApp files is used to host the SAPMNT shared folder and is mounted across all S/4HANA application, SCS and ERS servers.
HANA DB	Two HANA nodes are deployed across 2 AZs in an active-standby configuration. HANA synchronous replication is configured to replicate data from the active to standby node. Pacemaker cluster is configured to ensure that the standby node is promoted to active node in the event of a failure.

SAP Connectors

Two instances of SAP Cloud connectors are deployed across 2 AZs and configured as active-standby nodes. In the event of a failure, the standby node will take over as active node

The following connectors do not have out of the box high-availability and will require SAP RISE team to manually failover the system in the event of a failure.

- SAP Data Provisioning Agent - Currently not supported (SAP Note 3275211)
- SAC Agent - Currently not supported (SAP Note 3595999)
- OpenText Connector

SAP RISE VM Details

Azure Region	Environment	SID	Purpose	Physical Hostname	Virtual Hostname	CPU	Memory /GB	OS
North Europe (Dublin)	Sandbox	ERS	App Server	hec42v331805.irl.sap.eu.cloud.syensqo.com (172.16.33.10)	vhysqersci.sap.eu.cloud.syensqo.com (172.16.33.12) vhysqerscs.sap.eu.cloud.syensqo.com (172.16.33.11)	16	64	SUSE SLES15
		HRS	HANA DB	hec42v331250.irl.sap.eu.cloud.syensqo.com (172.16.33.5)	vhysqersdb.sap.eu.cloud.syensqo.com (172.16.33.13) vhysqhrsdb01.sap.eu.cloud.syensqo.com (172.16.33.8) vhysqhrsdb.sap.eu.cloud.syensqo.com (172.16.33.7)	32	256	SUSE SLES15
		WRS	Web Dispatcher	hec42v331253.irl.sap.eu.cloud.syensqo.com (172.16.33.6)	vhysqwrswd01.sap.eu.cloud.syensqo.com (172.16.33.9)	2	8	SUSE SLES15
	Development	ERD	App Server	hec42v303048.irl.sap.eu.cloud.syensqo.com (172.16.33.48)	vhysqerdci.sap.eu.cloud.syensqo.com (172.16.33.49) vhysqerdcs.sap.eu.cloud.syensqo.com (172.16.33.50)	8	64	SUSE SLES15
		HRD	HANA DB	hec42v302672.irl.sap.eu.cloud.syensqo.com (172.16.33.37)	vhysqerddb.sap.eu.cloud.syensqo.com (172.16.33.51) vhysqhrddb01.sap.eu.cloud.syensqo.com (172.16.33.42) vhysqhrddb.sap.eu.cloud.syensqo.com (172.16.33.43)	32	256	SUSE SLES15
		WRD	Web Dispatcher	hec42v302675.irl.sap.eu.cloud.syensqo.com (172.16.33.40)	vhysqwrdwd01.sap.eu.cloud.syensqo.com (172.16.33.44)	2	8	SUSE SLES15
		CRD	Cloud Connector	hec42v302678.irl.sap.eu.cloud.syensqo.com (172.16.33.45)	vhysqcrdcc01.sap.eu.cloud.syensqo.com (172.16.33.46)	2	8	SUSE SLES15
		DRD	Data Provisioning Agent	hec42v302676.irl.sap.eu.cloud.syensqo.com (172.16.33.41)	vhysqdrddpa01.sap.eu.cloud.syensqo.com (172.16.33.47)	4	16	SUSE SLES15
		SRD	SAC Agent	hec42v302674.irl.sap.eu.cloud.syensqo.com (172.16.33.39)	vhysqsrdweb01.sap.eu.cloud.syensqo.com (172.16.33.38)	4	16	SUSE SLES15
		ORD	OpenText Connector	hec42v318041.irl.sap.eu.cloud.syensqo.com (172.16.33.54)	vhysqordotc01.sap.eu.cloud.syensqo.com (172.16.33.55)	4	16	SUSE SLES15

Non-RISE

Overview

Systems that follow an IaaS or on-premises deployment model and are not hosted in SAP RISE, are hosted in Syensqo's Azure subscription. The following systems are classified as Non-RISE. Depending on complexity, separate documents may be used to describe the architecture for these applications.

Application	Region	Dev	INT	UAT	TRG	PAR	PRD
SAP WWI Server	EU	Non-PRD					PRD
	US	-	Non-PRD				PRD
	China	-	Non-PRD				PRD
Syniti Replicate	EU	PRD					
	China	PRD					
Syniti Connector	EU	PRD					
	US	PRD					
	China	PRD					
NextLabs	EU	DEV	QAS		-	PAR	PRD
	US	-	QAS		PAR	PRD	
	EU	DEV	QAS				PRD
	US	-	QAS				PRD

OpenText xECM	China	-	QAS	PRD

Hosting Region

Following considerations were taken into account in deciding the Azure hosting regions

- NextLabs provides attribute-based access control (ABAC) and evaluates access to sensitive data during runtime execution. To prevent performance issues, NextLabs will require low latency network connection to S/4HANA.
- NextLabs have its own Azure subscription and will be hosted in the same region & physical zone as S/4HANA. vNET peering will be established between SAP RISE and NextLabs vNET to achieve low latency connectivity.
- Other applications can be hosted in region that is in line with Syensqo's Azure deployment strategy.
- US OpenText xECM instance may contain sensitive data. To consolidate SyWay applications, all non-RISE US instances will be hosted together,
- Different subscriptions will be created for different environment: non-PRD, Pre-PRD and PRD

Region	Category	Subscriptions	Azure Region
EU	NextLabs	3 (non-PRD, Pre-PRD, PRD)	North Europe (Dublin)
	Non-RISE (excluding NextLabs)	2 (non-PRD, PRD)	France Central (Paris)
US	NextLabs	3 (non-PRD, Pre-PRD, PRD)	Department of Defense (DoD) in Azure Government Virginia
	Non-RISE (excluding NextLabs)	2 (non-PRD, PRD)	Department of Defense (DoD) in Azure Government Virginia
China	Non-RISE	2 (non-PRD, PRD)	Shanghai

Azure Subscriptions

VM Details

Shared File Systems

Network Architecture

Europe

The figure below describes the overall network connectivity for SAP RISE and non-RISE Azure vNETs in Europe.

SAP RISE

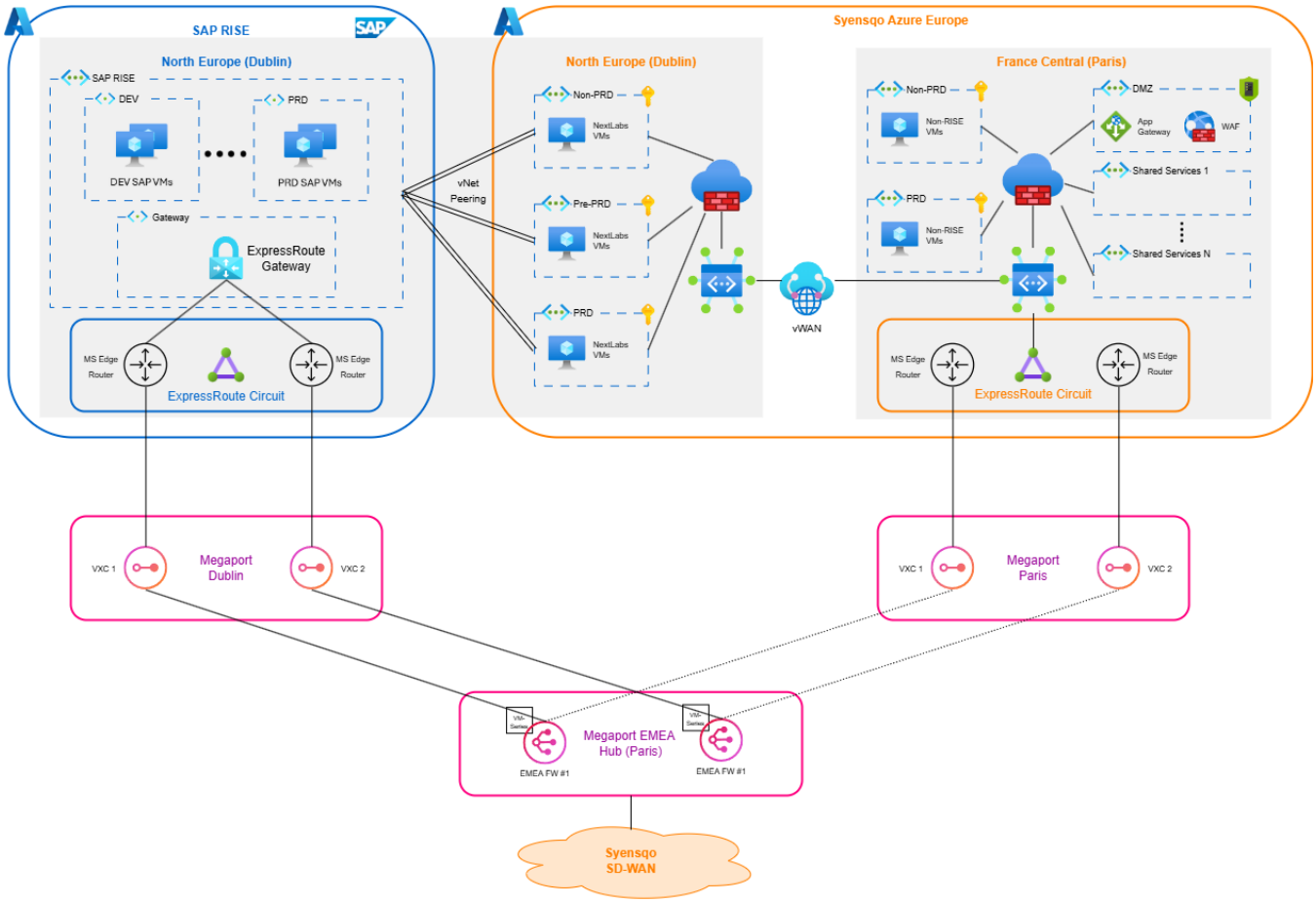
- SAP RISE tenant is deployed in Azure North Europe.
- Connection SAP RISE is established via ExpressRoute which is connecting through Megaport Paris and Dublin.

Non-RISE

- Non-RISE systems will be deployed in Azure France Central.
- Workloads are deployed to Non-PRD and PRD subscriptions.
- Syensqo Azure network architecture (ExpressRoute, vWAN and firewall) will be leveraged for SyWay non-RISE systems.
- Connection between SAP RISE and non-RISE will traverse Megaport EMEA hub.

NextLabs

- NextLabs systems will be deployed in Azure North Europe (same region as SAP RISE).
- Workloads are deployed to 3 subscriptions: Non-PRD, PRE-PRD and PRD.
- Connection to Syensqo WAN will be established via Azure vWAN and ExpressRoute.
- vNET Peering is configured between the 3 NextLabs vNETs and and SAP RISE.



North America

China

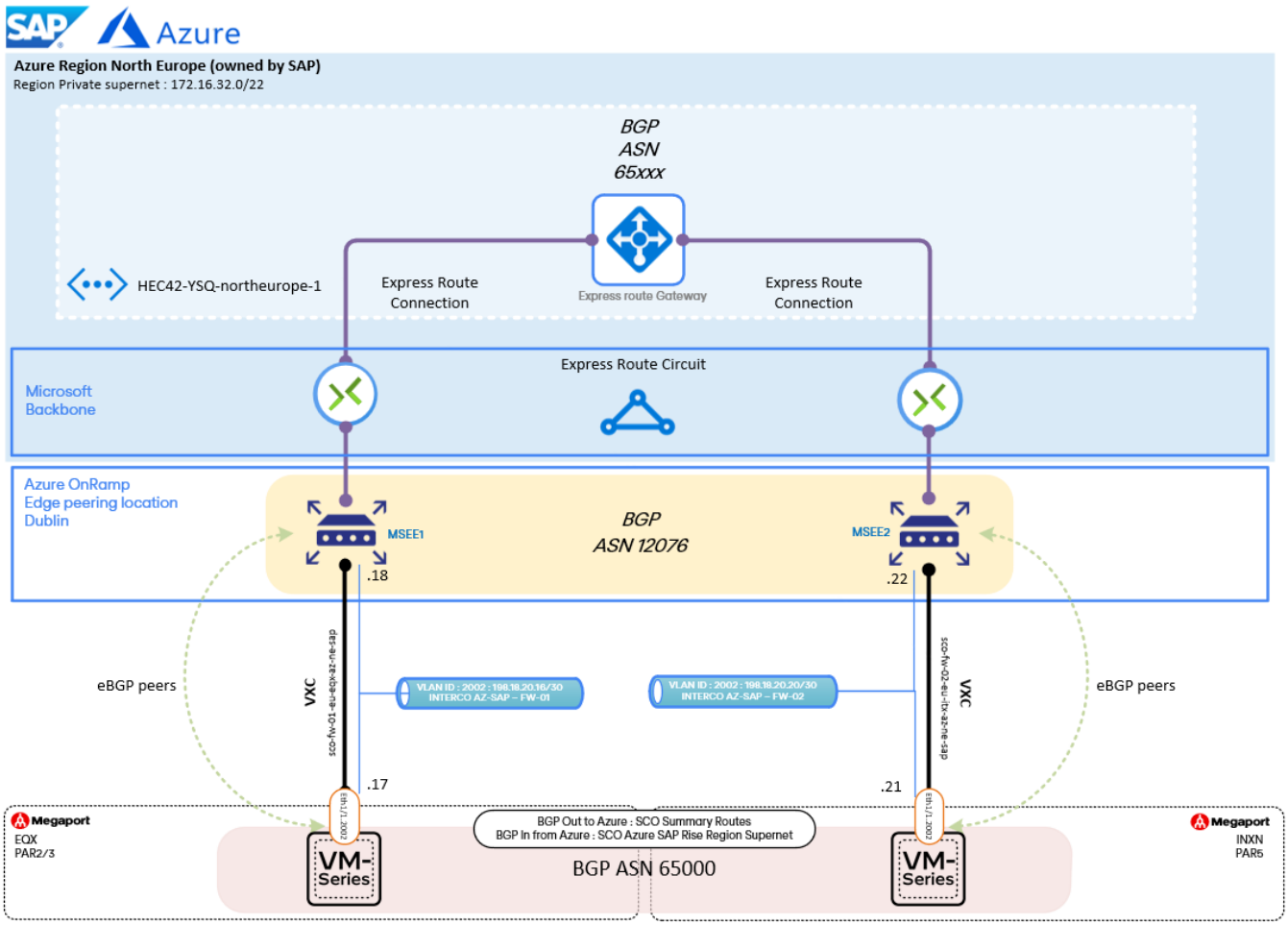
SAP RISE ExpressRoute Design

The table below lists down the regional hub and Azure edge location for NAM, EMEA and China regions.

Region	Megaport Location	Azure Edge location	SAP RISE Region	Non-RISE Region
Europe	Paris Equinix PA2/3 & Paris Interxion PAR5	Dublin	Azure North Europe (Dublin)	Azure France Central (Paris)
North America	Ashburn Equinix DC4 & Reston Core Site VA1	*TBC*	*TBC*	*TBC*
China	*TBC*	*TBC*	*TBC*	*TBC*

Europe

The following diagram describes the ExpressRoute design between Megaport and SAP RISE in EU region.



North America

TBC

China

TBC

IP Allocation

SAP RISE

The 172.16.32.0/19 IP range has been allocated for SAP RISE globally. The following table lists down the IP allocation for the different regions and subnets.

RISE Region	Region IP Allocation	RISE Subnet	Subnet IP Allocation	Range	Usable Hosts
Europe	172.16.32.0/22	Production	172.16.34.0/25	172.16.34.0 - 172.16.34.127	126
		Production (HA components)	172.16.34.128/25	172.16.34.128 - 172.16.34.255	126
		ECS Services	172.16.32.0/24	172.16.32.1 - 172.16.32.254	254
		Sandbox	172.16.33.0/27	172.16.33.1 - 172.16.33.30	30
		Development	172.16.33.32/27	172.16.33.33 - 172.16.33.62	30
		Integration Test	172.16.33.64/27	172.16.33.65 - 172.16.33.94	30
		QA / UAT	172.16.33.96/27	172.16.33.97 - 172.16.33.126	30
		Pre-Production	172.16.33.128/27	172.16.33.129 - 172.16.33.158	30
		Training	172.16.33.160/27	172.16.33.161 - 172.16.33.190	30

		Non-Prod Reserve	172.16.33.192/27	172.16.33.193 - 172.16.33.222	30
		Tools / Other Needs	172.16.33.224/27	172.16.33.225 - 172.16.33.254	30
		Unassigned	172.16.35.0/24	172.16.35.1 - 172.16.35.254	254
China	172.16.36.0/22	*TBC*	*TBC*	172.16.36.0 - 172.16.39.255	1022
North America	172.16.40.0/21	*TBC*	*TBC*	172.16.40.0 - 172.16.47.255	2046
Unassigned	172.16.48.0/20	-	-	172.16.48.0 - 172.16.63.255	4094

Non-RISE

Region	Region IP Allocation	Subnet	Subnet IP Allocation	Range	Usable Hosts
Europe	*TBC*	*TBC*	*TBC*	*TBC*	*TBC*
North America	*TBC*	*TBC*	*TBC*	*TBC*	*TBC*
China	*TBC*	*TBC*	*TBC*	*TBC*	*TBC*

DNS Architecture

Domain Name

The following domains names are used for the respective RISE regions.

RISE Region	SAP RISE Domain	Non-RISE Domain
Europe	*.sap.eu.cloud.syensqo.com	*TBC*
North America	*.sap.us.cloud.syensqo.com	*TBC*
China	*.sap.cn.cloud.syensqo.com	*TBC*

DNS Integration

2-way DNS integration is configured between Syensqo and SAP RISE DNS.

- Syensqo DDI team has select **DNS Domain Delegation** as the integration method. Syensqo DNS are configured to redirect SAP RISE DNS queries to the respective SAP RISE DNS deployed in the different regions.
- SAP RISE DNS have a **DNS forwarder** configured to redirect all Syensqo DNS queries to the respective Syensqo regional DNS servers.

The table below lists the Syensqo and SAP RISE DNS servers.

Region	Syensqo DNS	SAP RISE DNS
Europe	172.23.128.104 10.53.73.3 10.129.131.52 10.129.131.53 172.18.180.142 172.18.181.116 172.19.1.42 172.19.1.57 10.237.6.11 10.233.6.5 172.23.193.70 172.23.193.86 172.18.164.7 172.18.164.22 172.19.113.69 172.19.113.86	DNS –CSN-A-HA IP - 172.16.32.14 (vhysqirlcsna-ha.irl.sap.eu.cloud.syensqo.com) DNS –CSN-B-HA IP - 172.16.32.30 (vhysqirlcsnb-ha.irl.sap.eu.cloud.syensqo.com) DNS –CSN-C-HA IP - 172.16.32.46 (vhysqirlcsnc-ha.irl.sap.eu.cloud.syensqo.com)
North America		*TBC*
China		*TBC*

Network Firewall

For SyWay project, the following firewalls will be leveraged to manage the corresponding traffic.

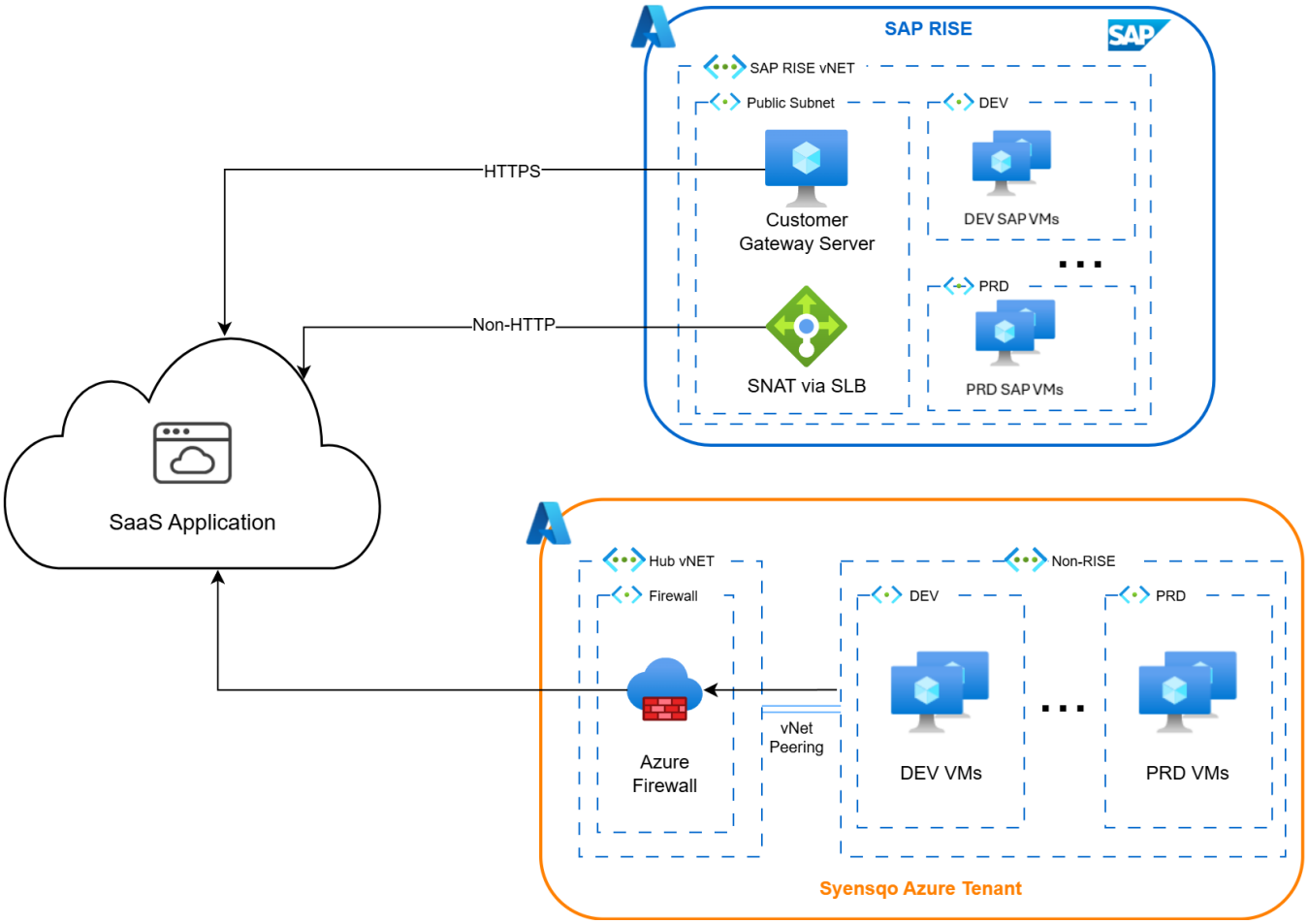
Firewall	Network Traffic

Regional Hub Firewall	• Incoming network traffic to SAP RISE.. • Outgoing network traffic from SAP RISE.
Syensqo Azure Firewall	• Incoming network traffic to Non-RISE and NextLabs vNETs. • Outgoing network traffic from Non-RISE and NextLabs vNETs.

Internet Traffic

To connect SyWay systems deployed in Azure (SAP RISE or non-RISE) and SaaS applications, a middleware (i.e., using Cloud connector and SAP Integration Suite) based integration approach will be preferred. If the integration scenario requires direct connection between S/4HANA and SaaS applications, the following sections covers how inbound and outbound network connections can be established.

Outbound Internet Traffic



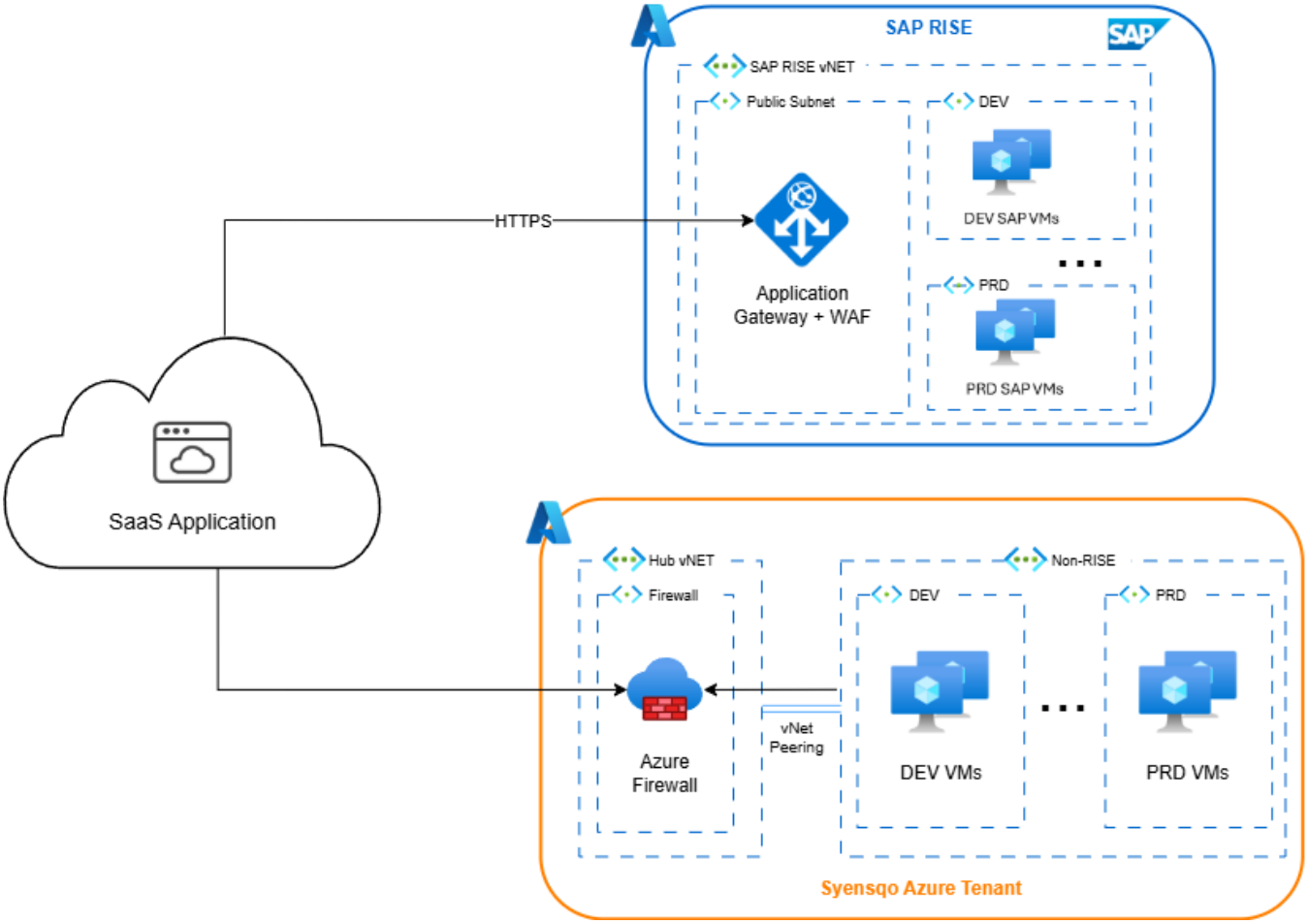
- Outbound HTTPS traffic from SAP RISE is routed through the Customer Gateway server which has an internet proxy (Squid Proxy) installed in the VM.
- Outbound non-HTTP traffic (e.g., SDTP) from SAP RISE is NAT-ed via Azure Standard Load Balancer.
- Outbound internet traffic from Non-RISE application is routed to Azure firewall in Syensqo Hub which filters the traffic before allowing it to the external application.

The following outbound traffic is configured in SAP RISE.

Source	Destination	Port/Protocol	Method
All S/4HANA Application server	Mailjet (34.22.188.249)	587/SMTP TLS	Azure Load balancer

Inbound Internet traffic

Currently there is no requirements for inbound internet traffic to SAP RISE and non-RISE systems. This method of connectivity will be considered if there are no other alternatives and will require cybersecurity approval.



- SAP RISE uses Azure Application Gateway with Web Application Firewall to manage inbound HTTPS traffic. Non-HTTP inbound traffic are not permitted and will required further approvals from SAP.
- Inbound internet traffic to non-RISE vNET are filtered through Azure firewall in Syensqo Hub vNET before it is routed to the non-RISE vNET.

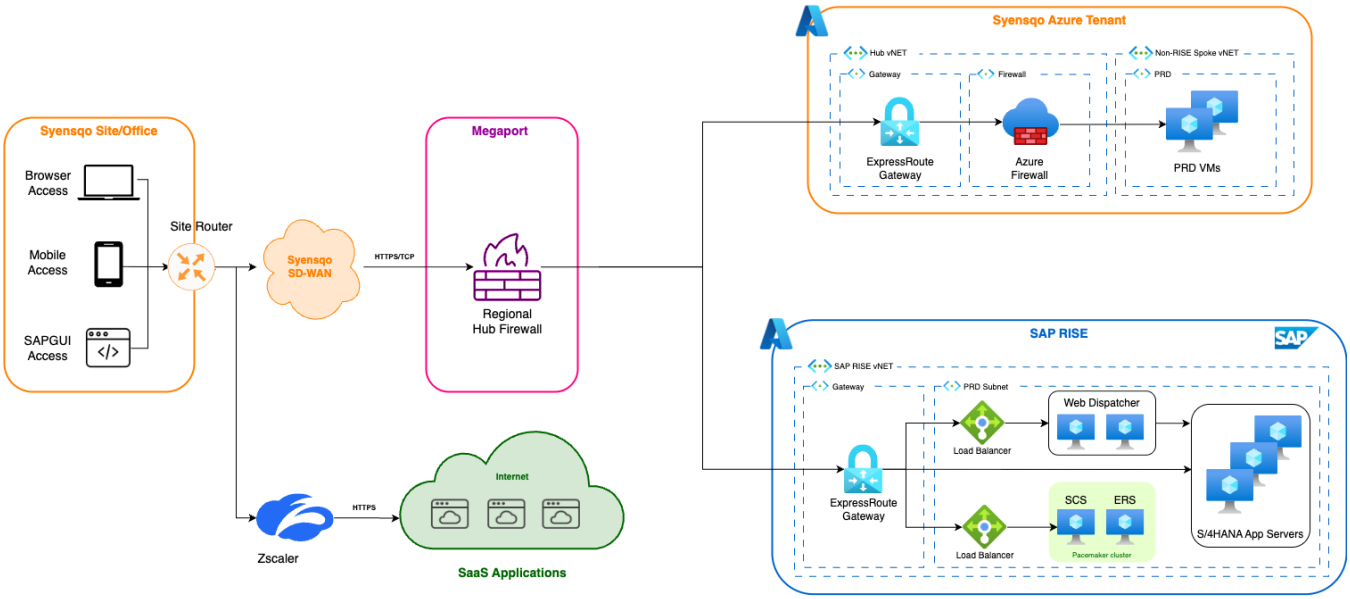
User Access

The following sections describes how SAP RISE and non-RISE systems are access by users within (internal) and outside (external) Syensqo network. For SaaS application access, users can access them through their existing internet access.

These section cover the network perspective and does not include the authentication processes where single sign-on will be configured with Syensqo Identity provider.

Internal Access

End users will access SyWay systems via browser, mobile app or SAPGUI (for S/4HANA) (refer KDD036). The figure below describes the network traffic from user's terminal to SyWay systems.



SAP RISE Web Access:

- Primary mode of access for SAP RISE system is through HTTPS.
- User's HTTPS traffic is routed from Syensqo local site network to SAP RISE through SDWAN and ExpressRoute connection.
- In SAP RISE, Azure load balancer is provisioned to load balance the incoming HTTPS traffic to SAP web dispatchers.
- SAP web dispatchers act as proxies and forward the request to S/4HANA application server.

SAP RISE SAPGUI Access

- SAP administrators and support staff may access S/4HANA using SAPGUI which uses TCP protocol.
- User's SAPGUI connections are routed from Syensqo local site network to SAP RISE through SDWAN and ExpressRoute connection.
- In SAP RISE, a pacemaker cluster is configured between SCS and ERS servers for HA and Azure load balancer is used to direct network traffic to the active SCS node.
- SCS redirects users to one of the available S/4HANA application server and there after, the communication is directly between user's SAPGUI and the application server.

Non-RISE Access:

- User traffic is routed from Syensqo local site network to Syensqo's Hub vNET through SDWAN, Megaport and ExpressRoute connection.
- In the hub vNET, traffic is filtered through Azure firewall before being routed to Non-RISE vNET and non-RISE application.

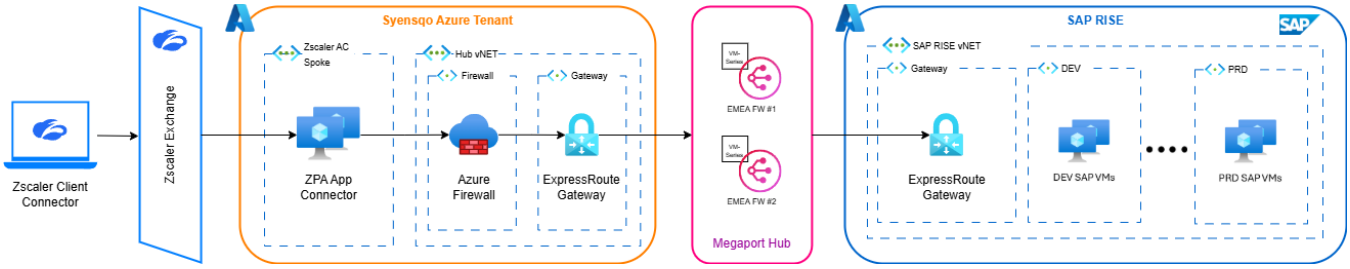
SaaS:

- Primary mode of access for SaaS applications is via HTTPS.
- User's HTTPS traffic is routed from Syensqo local site network to Zscaler which acts as a proxy and connects to the SaaS applications.

External Access

No direct external access from the internet is enabled for SyWay systems hosted in RISE. Users with a Syensqo-issued device can access systems hosted in RISE from outside the Syensqo network via ZScaler Private Access (ZPA).

ZPA App Connectors will be deployed in non-RISE Azure vNET and will be registered with Syensqo's Zscaler Exchange. Users will connect from their terminal using Zscaler client connector and the network traffic will traverse as shown below.



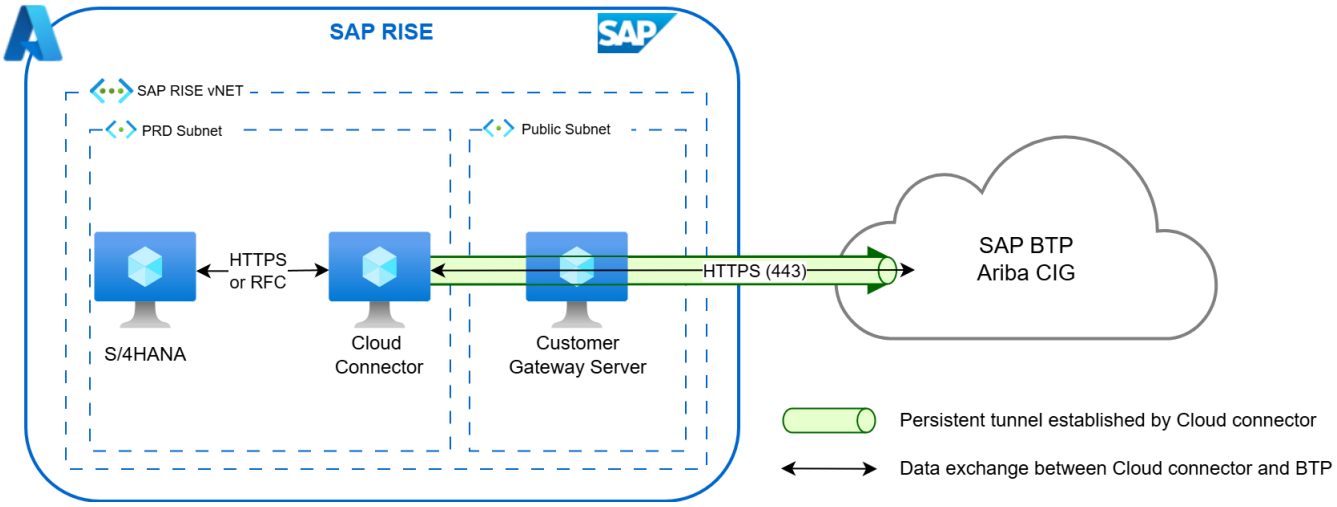
Integration

The following sections describes the network design and flow for the following integration scenarios.

SAP Cloud Connector

The SAP Cloud connector are deployed in SAP RISE and acts as a reverse invocation proxy to establish network connection between SAP RISE systems and SAP BTP services (Integration suite, API management, SAP Analytics Cloud etc.) and Ariba Cloud Integration Gateway (CIG). Due to its reverse invoke capabilities, the network traffic originates from SAP Cloud connector to SAP BTP and once the link as been established, data can be exchanged between SAP RISE systems and BTP. HTTPS or RFC protocols are used between SAP Cloud Connector and S/4HANA, and HTTPS protocol is used between Cloud Connector and S/4HANA.

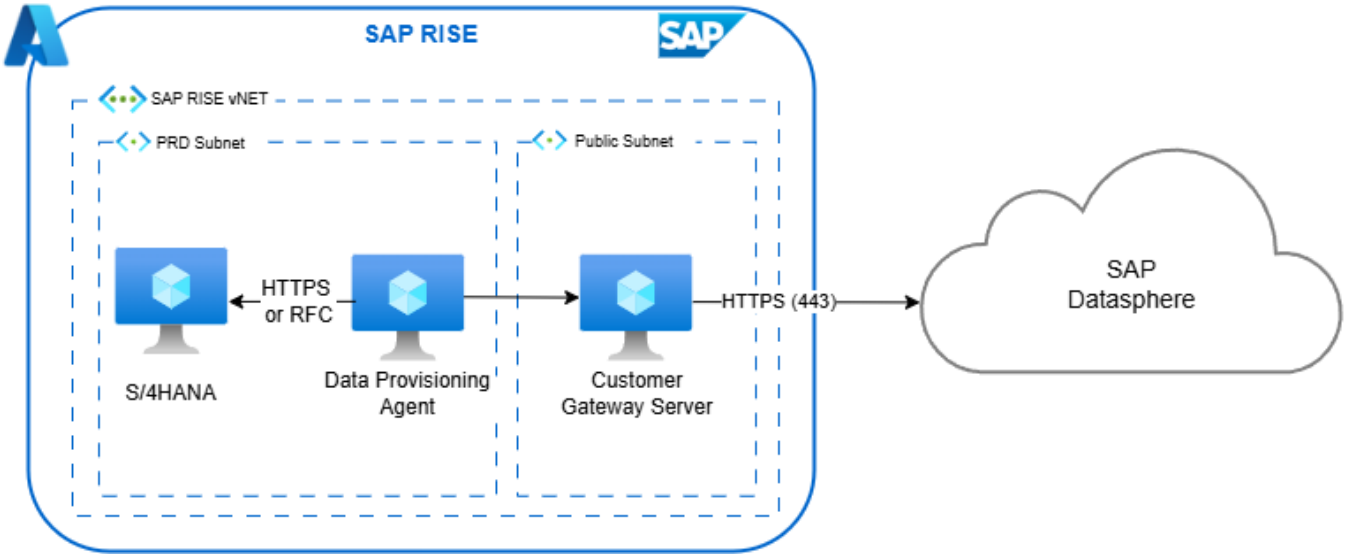
To enable outbound internet traffic from SAP RISE, SAP has provisioned a customer gateway server (CGS) with a forward internet proxy installed on it.



EIM Data Provisioning Agent

EIM Data Provisioning Agent (DPA) is used to integrate S/4HANA and SAP Datasphere. The network connection to SAP Datasphere is initiated by DPA and CGS is used to facilitate the internet connection to SAP Datasphere.

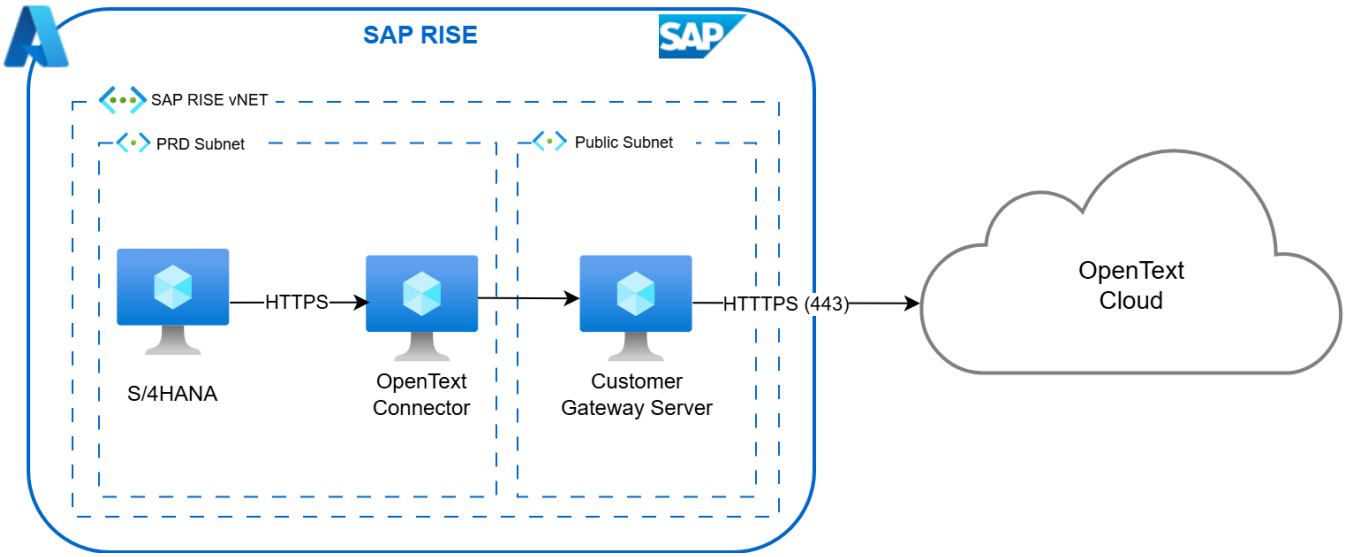
DPA uses the HTTPS or RFC protocols to communicate with S/4HANA and uses the HTTPS protocol to communicate with SAP Datasphere.



OpenText Connector

OpenText connector facilitates the connection between S/4HANA and the OpenText cloud. The connection is initiated from S/4HANA to the OpenText connector and to OpenText cloud via CGS.

The HTTPS protocol is used for communication between all components.



SAP Router

SAP has configured a VPN connection between the Syensqo SAP RISE tenant and SAP's Management network (used by SAP support). SAP Router is deployed in SAP RISE to manage SAP support's connection to SAP systems.