World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Sap S/4hana applications on data security and protections for sap cloud services

Vedaprada Raghunath *

IT Director, IMR soft LLC, USA.

World Journal of Advanced Research and Reviews, 2024, 23(03), 2530–2538

Publication history: Received on 14 August 2024; revised on 24 September 2024; accepted on 26 September 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.3.2911

Abstract

This study focuses on how to secure enterprise resource planning (ERP) systems that are hosted in the cloud. We utilized SAP S/4HANA cloud (Public edition) for this research. Here we take a look at the difficulties and concerns around cloud data security. The essay will provide a comprehensive analysis of the research findings. We implement global protection strategies and policies to mitigate risks and threats, guaranteeing the highest level of data safety in Cloud ERP. While many apps would benefit from access to ERP data in the cloud, doing so would also make that data available to apps that may already have security flaws.We chose to investigate cloud-based ERP since many organizations are moving away from on-premises ERP systems in favor of them. Concerns regarding the safety of data while it is in transit or at rest are also covered in the article. The study makes use of platforms as a service (PaaS) and software as a service (SaaS) at all levels. As part of our investigation, we look at potential fixes for several Cloud ERP security vulnerabilities.

Keywords: Data Security; Cloud Computing; SAP S/4HANA; Cloud ERP

1. Introduction

Enterprise resource planning software is accessible through the internet, often known as cloud ERP. When it comes to an organization's information technology, cloud ERP software is like the "brains" or "backbone"it provides state-of-the-art capabilities for all the important business processes. Many cloud-based enterprise resource planning (ERP) software solutions are provided "as a service," or housed on the provider's cloud computing infrastructure.

Customers pay to rent the software on an annual or monthly basis rather than buy it outright [1-3]. The provider takes care of application upkeep, upgrades, storage systems, and security; you won't have to worry about initial hardware costs. Software as a service enterprise resource planning, also called cloud ERP, is managed by your provider's IT department and housed on their cloud platform. In contrast, on-premises ERP requires your in-house IT department or a third party to install and manage the software on your servers and other hardware [4-8]. More and more, companies are looking to the cloud as an alternative for ERP deployment. Cloud ERP software is preferred over on-premises ERP by 63% of firms, according to recent research. A key component for success in the present era is cloud ERP, thanks to its unique features and agility.

Companies have reaped tremendous benefits from ERP systems in the past, which have helped them increase productivity and gather expertise. But everything has changed, even the level of competition, due to digitization. There is just no way for locally installed ERP systems to stay up [9-13]. They have a hard time adjusting to changes that last a long time. Companies are looking for ERP systems that can help them run more efficiently and with more insight into their customers' needs, but most of the older systems aren't up to the task because they were designed for a simpler environment.[14-16] Faster product and service delivery, improved reliability, lower costs, and continual product and service improvement are all demands from modern customers. It is not uncommon for businesses to have to look

* Corresponding author: Vedaprada Raghunath

outside their four walls to find the finest solutions for their consumers. [17-19] Even the most fundamental parts of their operation are handled by them and their numerous digital partners, including production, product distribution, sales management, service, and support.

Consequently, they need software that can assist with the management of both their global business networks and their ever-increasingly complex internal processes. That can't happen until you use cloud ERP [20-21]. With all the news about viruses and data breaches recently, it's understandable to question the security of cloud ERP. While it's true that no system is completely secure, the implementation and oversight of your system determine its level of protection.

By enforcing compliance with the company's established security standards, SAP HANA Security safeguards critical data against unauthorized access. One of SAP HANA's features, multitenant databases, allows you to build many databases on a single system.

The official name for it is multitenant database container. Consequently, SAP HANA provides all capabilities pertaining to security for all databases that have multiple tenants [22-23]. The main difference between SAP Security for S/4HANA as seen in figure 1 and the old three-tier architecture is that in the former, the database could only be accessible through the ECC, but in the latter, security had to be implemented at both the application and database layers [24-29].

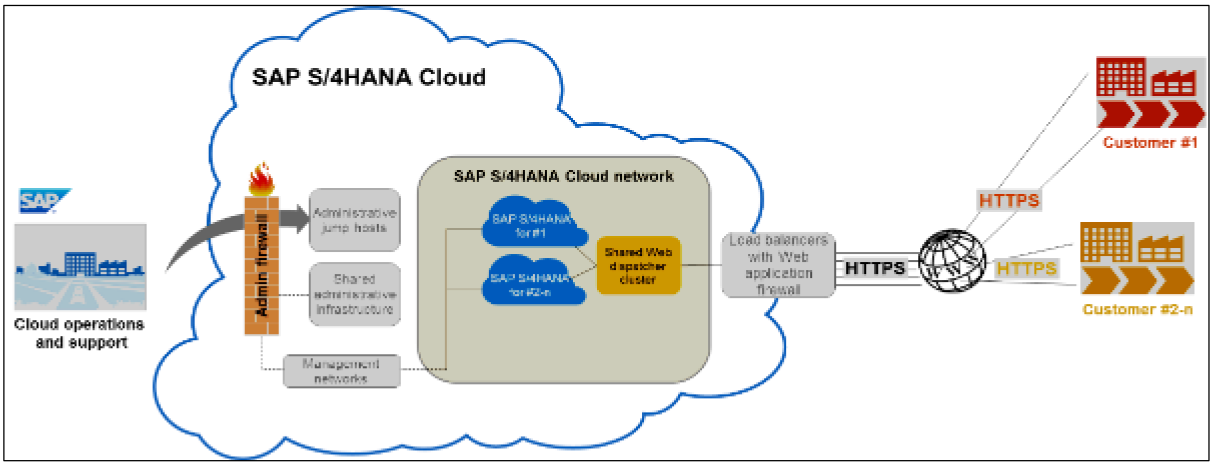
SAP S/4HANA Cloud
SAP
Cloud operations and support
Admin firewall
Administrative jump hosts
Shared administrative infrastructure
Management networks
SAP S/4HANA Cloud network
SAP S/4HANA for #1
SAP S/4HANA for #2-n
Shared Web dispatcher cluster
Load balancers with Web application firewall
HTTPS
HTTPS
HTTPS
Customer #1
Customer #2-n

Figure 1 SAP S/4HANA Cloud

Secure cloud operations: SAP S/4HANA Cloud meets high standards of trust to deliver an SaaS offering and is compliant with ISO 27001 for information security.

- The audit reports that SAP regularly produces are in accordance with ISAE3402/SSAE16-SOC 1 Type I and SOC 2 Type I. The SOC 2 Type II and SOC 1 Type II audit reports are presently being prepared. Trust Services Principles (TSP) 100 form the basis of the ISAE 3000 SOC 2 engagement's security measures. Three data centers in three different countries—Sydney, Australia; St. Leon-Rot, Germany; and Sterling, Virginia, USA—host the software. In terms of physical security and backup infrastructure, they have achieved a minimum SAP data center grade of Level 3.
- By utilizing robust encryption techniques and the industry-standard transport layer security protocol, all system access is accomplished over encrypted communication channels.
- Patching the infrastructure (OS or VM hypervisor), applications, and databases for security issues is common procedure. Reverse proxy farms provide an extra layer of protection by masking the network's architecture. A web application firewall safeguards the portions that are exposed to the internet.
- The network layer isolates customer instances, limiting the technical communication that a system can initiate with other systems within the same customer or with systems outside of the customer.
- The SAP Fiori apps for managing identities and permissions are role-based, which allows for secure access. Data protection and privacy rules can be respected by activating Read Access Logging.

2. Sap on their business customers on sensitive data in cloud services

Cloud services allow SAP clients to store mission-critical and sensitive company data, while SAP takes care of platform-level protection through a shared security approach. Cloud computing from SAP comes with a plethora of security assurances, such as a SLA, a Support Policy, and a Data Processing Agreement that covers both organizational and technical measures.

With enterprises collecting and processing more data than ever before, SAP offers solutions that provide clients more control and transparency over their data security. Our approach to data security is focused on the needs of our customers. Customers who use SAP cloud services on public clouds, such as AWS, Azure, or Google Cloud Platform, often want to know how their data is protected. Following the invalidation of the EU-US Privacy Shield framework by the Court of Justice of the European Union's (CJEU) Schrems II decision, new privacy standards for cross-border data transfers were established, and data transfer mechanisms were subject to increased scrutiny. New rules have resulted from this, making it more difficult for companies to transfer consumer data from the EU to the US without taking additional security measures.

Capabilities that are typically sought after by customers include:

- Competencies for handling their personal encryption keys.
- The ability to see the locations and usage of their data.
- Having access to audit records and reports for their own SAP applications.
- Efficiently manage security incidents and events to keep an eye on the SAP environment.
- Advanced Identity and Authentication Management.
- The ability to mask and log user interface activities.

We will go over the many security solutions and technologies that our customers can utilize to protect their data on SAP cloud services, as well as the specific use cases for each. You might need to purchase an extra license to use certain of these security services with certain cloud services.

2.1. SAP Data Custodian Key Management Service

As an increasing number of SAP clients adopt a cloud-first strategy, public cloud platforms such as AWS, Azure, and GCP are quickly becoming the go-to locations for hosting SAP S/4HANA applications.

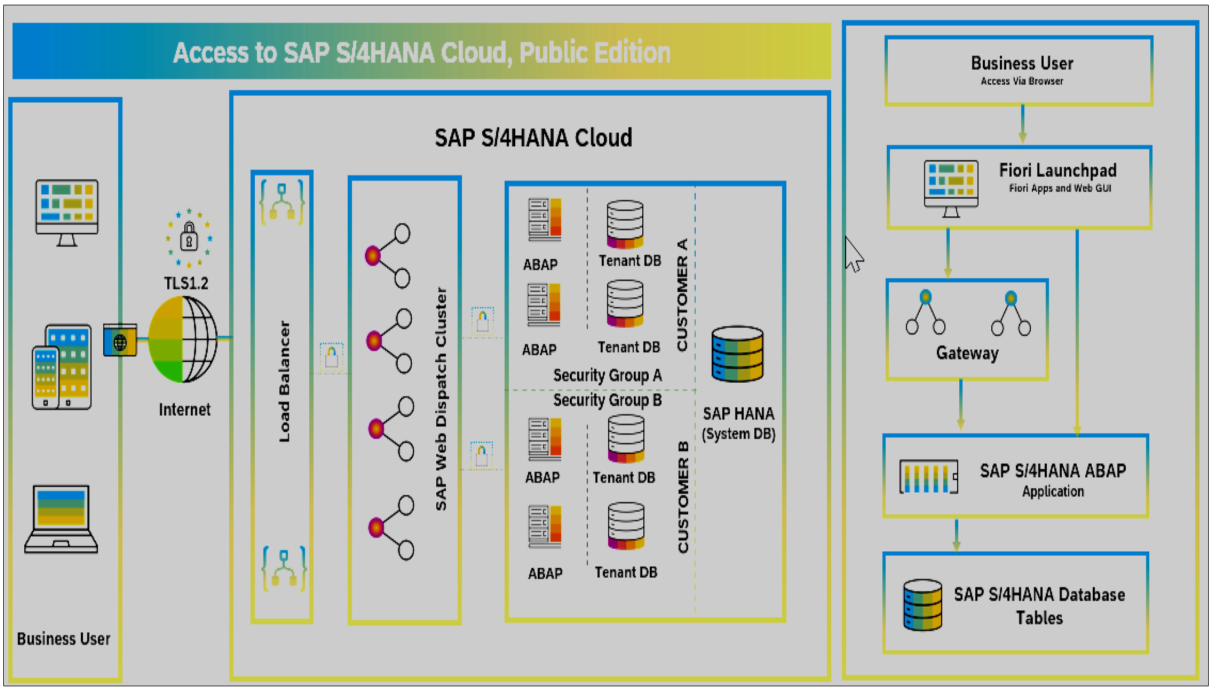

Figure 2 Use of the SAP S/4HANA public cloud edition

Our clients need autonomy over their cryptographic keys so they may proactively safeguard data stored in SAP cloud services, which improves security and data protection. The SAP Data Custodian Key Management Service (KMS) streamlines data protection in many cloud environments, including public, private, hybrid, and multi-cloud. It provides control, monitoring, and cryptographic key provisioning services to ensure the security of your data.

Use the SaaS paradigm, and SAP Data Custodian will provide you with an independent KMS. Based on our research, we can confirm that SAP Data Custodian KMS is compatible with S/4HANA single-tenant deployments. This includes BYOL, SAP Analytics Cloud (Private Edition), SAP S/4HANA Cloud, Private Edition (in roadmap), and S/4HANA hosted in public clouds as shown in figure 2. Among SAP Data Custodian KMS's most crucial features are:

- On certain instances, conformity with FIPS 140-2 certification is required.
- Privacy and security of data.
- Keeping cloud service providers in the dark about client information.
- Discipline according to task.
- External to the HANA environment, Master Key Management.
- Hierarchy of key chains with multiple levels.
- Role-based access, authentication, and authorization.
- Records of KMS access audits.

3. Secure data flow for sap s/4hana cloud, private edition

Each client receives their own Azure subscription, Amazon Web Services "Account," or Google Cloud "Project" as part of the "RISE with SAP S/4HANA Cloud, Private Edition (PCE)" infrastructure. With SAP Enterprise Cloud Services (ECS) in charge of the landscape, customers are kept out of the hyperscale provider's infrastructure layer. All subscriptions, accounts, and projects have their own VPC or VNET, which consists of many subnets. To keep these subnets safe, network security groups or security groups assigned to the Gateway, Application Gateway, Admin, and Production areas are necessary.

Customers have the option to request the creation of additional subnets for non-production use. The Customer Gateway server is managed by the admin subnet. It offers several features, including DNS, Internet Proxy, and Source NAT. To secure incoming internet traffic, a Web Application Firewall is connected to an Azure Application Gateway in the Application Gateway subnet. While this example uses Azure, similar configurations are utilized for AWS and Google Cloud and it was shown in figure 3.

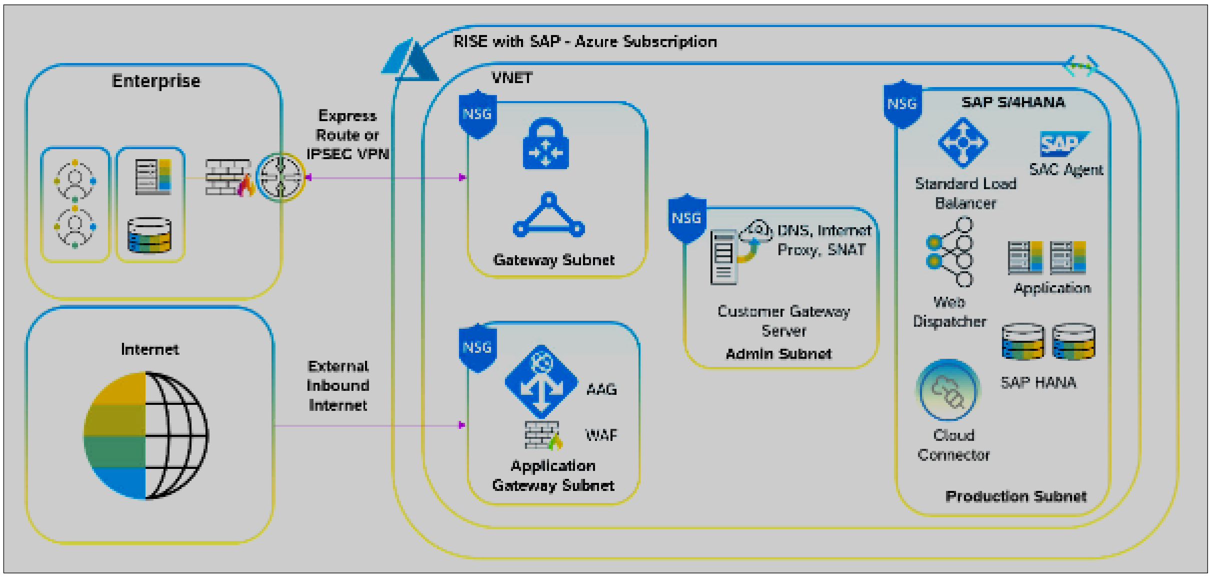

Figure 3 Climb the corporate ladder with SAP S/4HANA on the cloud

3.1. External Inbound Internet Traffic to SAP S/4HANA Cloud, Private Edition

- By connecting to the Web Application Firewall (WAF), the Azure Application Gateway (AAG) in SAP S/4HANA Cloud, private edition can inspect incoming internet traffic and determine if it is allowed. One more thing it can do is balance loads on Layer 7. When it comes to protecting applications from threats like SQL injection and cross-site scripting (XSS), AWS employs the Web Application Firewall (WAF) in tandem with the Application Load Balancer, whereas Google Cloud relies on Cloud Armor.

- Protecting web applications against common vulnerabilities and exploits outlined by OWASP, the Web Application Firewall (WAF) on the Azure Application Gateway provides integrated protection. Installed on a dedicated network subnet, the Application Gateway restricts all incoming HTTPS connections to those with TLS 1.2 or higher.
- Prior to transmission to the backend, the Azure Application Gateway decrypts was deployed in figure 4 and re-encrypts this traffic. The Azure documentation is a good resource for learning about the features and capabilities of Azure's Application Gateway and Web Application Firewall. In order to comply with this criterion, AAG/WAF will not be triggered, as some customers have prohibited incoming traffic to this landscape.

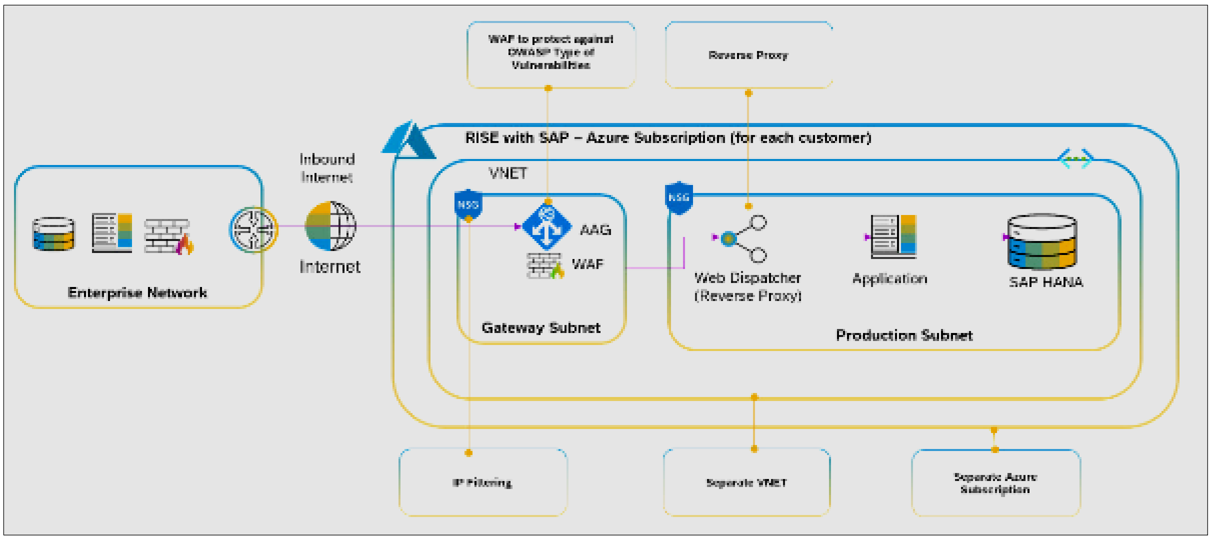
WAF to protect against OWASP Type of Vulnerabilities
Reverse Proxy
RISE with SAP – Azure Subscription (for each customer)
Inbound Internet
VNET
NSG
AAG
WAF
NSG
Web Dispatcher (Reverse Proxy)
Application
SAP HANA
Enterprise Network
Internet
Gateway Subnet
Production Subnet
IP Filtering
Separate VNET
Separate Azure Subscription

Figure 4 Internet Data Transfers from External Sources

3.2. Outbound Traffic to SAP Business Technology Platform

- Using SAP S/4HANA Cloud, private edition, in a variety of integration and extension scenarios requires the SAP Business Technology Platform (SAP BTP) communication. Even though SAP BTP is usually only accessible over the internet, a secure mTLS 1.2 tunnel connection can be established by establishing a mutual TLS 1.2 authentication between the SAP Cloud Connector in the PCE landscape and the connectivity service layer of SAP BTP.
- All outbound traffic from the private edition landscape is redirected to the Internet using the "Internet Proxy" that is set up in the Admin Subnet. Another feature of this Internet Proxy is the ability to configure it to just "allow list" outbound URLs that are directed to SAP BTP is shown in figure 5. Even though the diagram illustrates AWS settings, the same deployment setups work for Azure and Google Cloud.

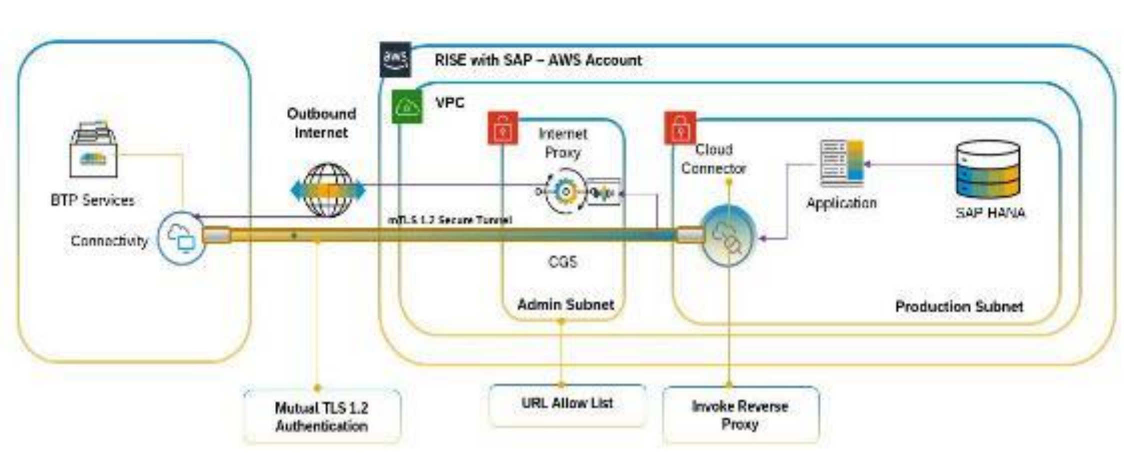

Figure 5 Connecting External Resources to SAP BTP

3.3. Inbound HTTPS Traffic from a Dedicated Network or IPSEC VPN

- Figure 4 shows the data flow from on-premises to RISE using SAP S/4HANA Cloud, private edition, in the landscape that is described below. The RISE platform can be accessed by dedicated network connections such as Azure ExpressRoute, AWS Direct Connect, or Cloud Interconnect. Another option is to set up a highly available IPsec tunnel between the two sites.
- Standard Load Balancer (SLB) receives traffic from on-premises devices using dedicated network or IPSEC. Azure Standard Load Balancers (SLBs) allow customers' on-premises to seamlessly access Azure, as seen in the diagram. Layer 4 (transport layer) protocols are supported by the SLB, which allows it to operate with TCP, HTTP, and HTTPS. Since SLBs are designed to balance loads, they can provide service to both the production and non-production member pools simultaneously. You should depend on the SLB's backend pool members, like the web dispatcher, for SSL termination.
- Furthermore, certificates linked to load balancer hostnames should also be stored on servers. Web Dispatcher and Load Balancer are the pathways that application outgoing traffic takes in response to incoming traffic. The application can bypass the Web Dispatcher and Load Balancer by sending outward traffic directly via dedicated connection was given in figure 6. The catastrophe recovery area ought to likewise use a comparable SLB setup. The configuration for inbound HTTPS traffic on the AWS and Google Cloud platforms is comparable. Private edition of SAP S/4HANA typically blocks non-https traffic, with the exception of SAP GUI and SAP S/4HANA cloud.

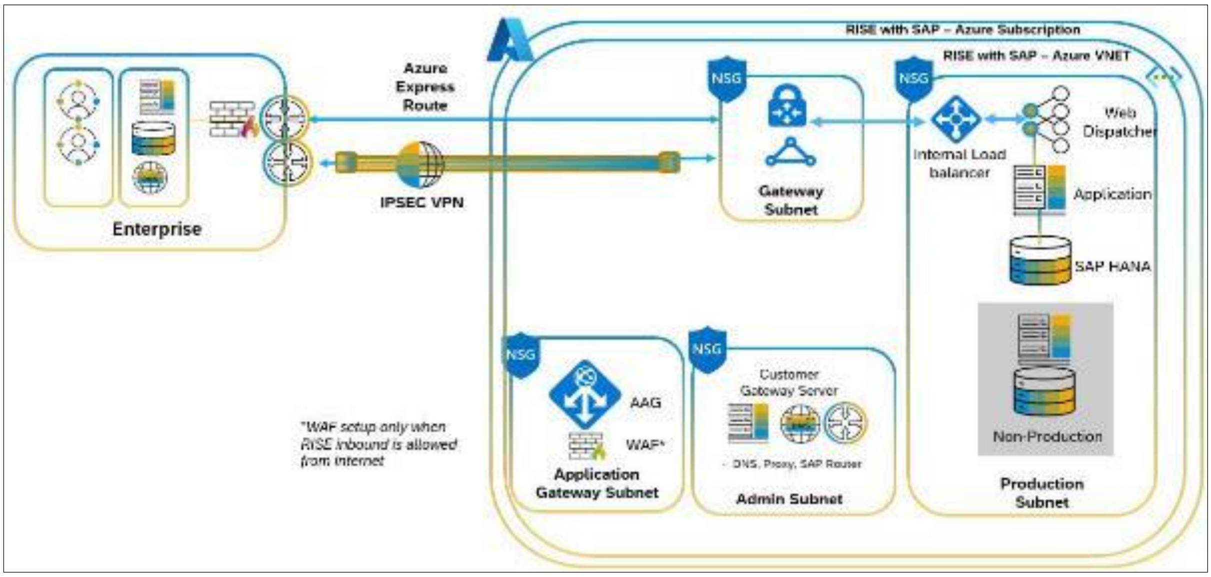

Figure 6 Arrival at Destination from Authorized Network

3.4. External Outbound HTTPS Traffic to Internet

- Several systems within the SAP S/4HANA PCE production subnet, including SAP Cloud Connector and SAC Agent, have the capability to create outbound "https" connections to the internet. The Customer Gateway Server (CGS) has an Internet Proxy already installed, so this is feasible. This proxy only works with the "https" protocol can ge seen in figure 7.
- The purpose of this security measure is to restrict access to the internet to the Internet Proxy and not to client servers directly. Customers can tailor the Internet Proxy to their own needs by providing a "allowed" (allow list) of URLs. When you configure the Internet Proxy, it comes with a "allow list" that you can use to access to various SAP SaaS applications.
- Platforms such as Ariba, Fieldglass, SAP BTP, SuccessFactors, the Service Marketplace, and SAP Support Hub connections fall into this realm. Throughout the course of a project, the "allow list" might be modified to accommodate client requirements.

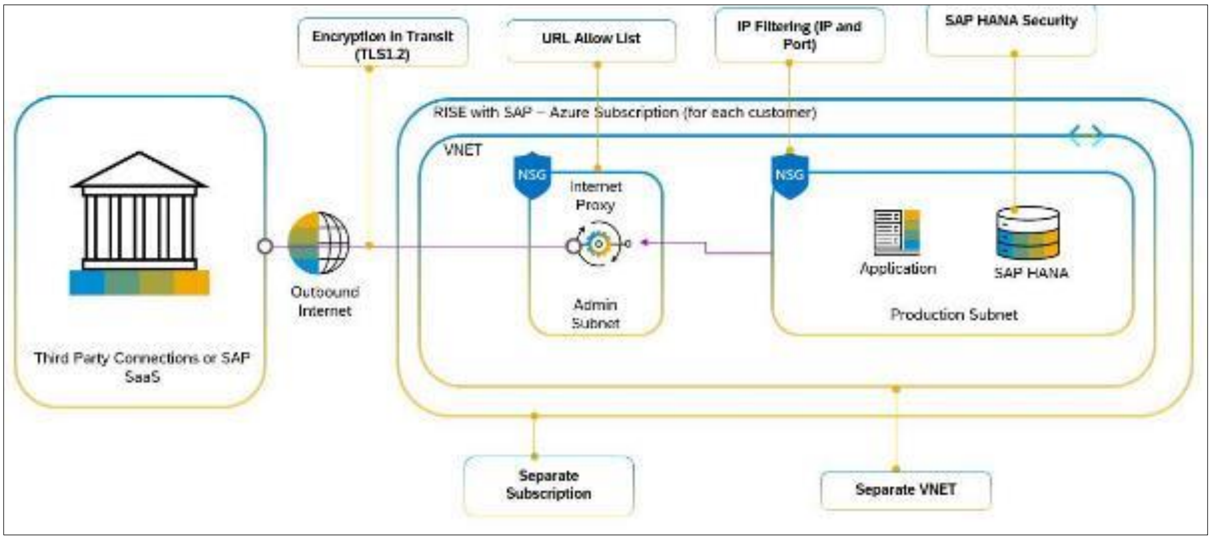

Figure 7 Internet from Outside the Company

3.5. Outbound non-HTTPS traffic

- An Azure-hosted SAP S/4HANA PCE will use the Azure Virtual Network to route all non-https requests, including SFTP, to an outbound-configured Azure Standard Load Balancer (SLB). With the help of Source Network Address Translation (SNAT), this SLB transforms the private IP address of the SAP system into its public IP address. A crucial point to remember is that IP addresses, not hostnames, should be used to create routing or connection rules.
- The request is processed and returned to the SLB's public IP address by the external system. The SLB then uses its NAT table to send the response to the SAP S/4HANA system via the Azure Virtual Network, inverting the SNAT procedure. To keep things organized and controllable, outgoing traffic is handled by a separate Azure SLB instance from any instances that handle incoming traffic. To further guarantee continuity and resilience during Disaster Recovery, an extra outbound SLB must be deployed to the DR region can be shown in figure 8.

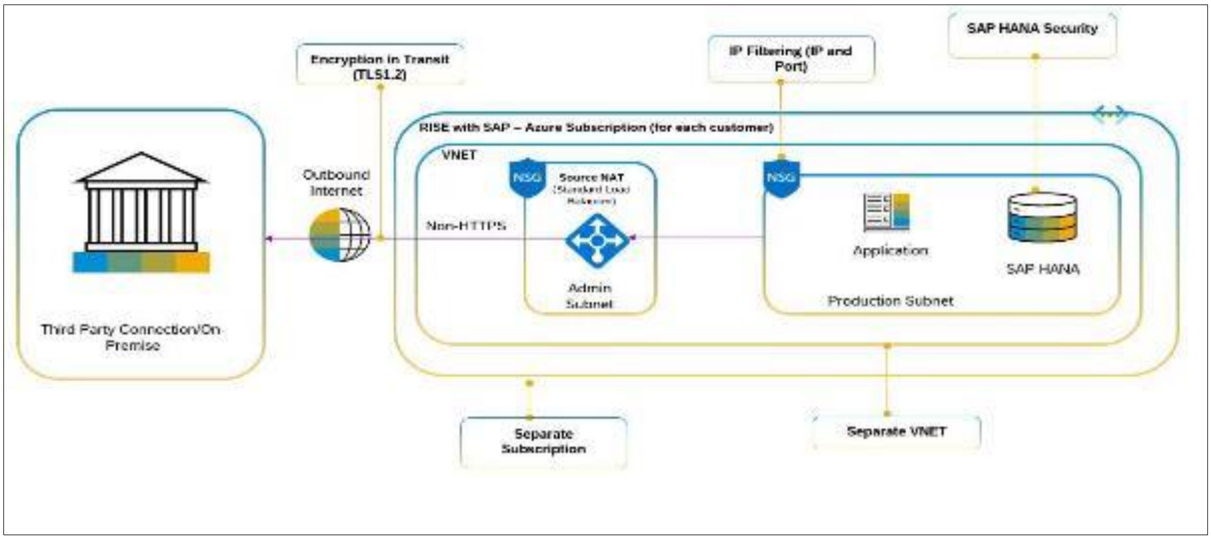
Encryption in Transit (TLS1.2)
IP Filtering (IP and Port)
SAP HANA Security
RISE with SAP – Azure Subscription (for each customer)
VNET
Outbound Internet
NSG
Source NAT (Standard Load Balancer)
NSG
Non-HTTPS
Application
SAP HANA
Admin Subnet
Production Subnet
Third Party Connection/On-Premise
Separate Subscription
Separate VNET

Figure 8 External connection that is not secured by HTTPS

4. Conclusion

Increasing reliance on cloud computing for data storage is likely fueling a trend toward better cloud data storage practices. There is a risk to data kept on the cloud if it is not well secured. The purpose of this essay was to look at three separate security issues and the potential threats to cloud-based data. It is necessary to study virtualization in order to identify hypervisor hazards. Many have voiced similar worries about public clouds and multitenancy. Problems with data security and ways to fix them in the cloud were the primary foci of this article. Several different kinds of data and encryption techniques for securely storing information in the cloud have been discussed. Every organization's security is dependent on how well it adapts to digital transformation. Maintaining a secure data flow is critical when connecting platforms such as SAP S/4HANA Cloud, private edition with SAP SuccessFactors, SAP Ariba, SAP Concur, and other SaaS options. Inbound and outbound interfaces alike are not immune to potential threats. There must be strong security procedures in place for evaluating risks and for carefully defining trust limits. Although operational efficiency is improved through seamless data integration, the security of the data flow must not be compromised. More than just a technical need, data flow security is critical to a company's success in this age of increasing cyber threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] R. Brunel et al., "Supporting hierarchical data in SAP HANA," 2015 IEEE 31st International Conference on Data Engineering, Seoul, Korea (South), 2015, pp. 1280-1291, doi: 10.1109/ICDE.2015.7113376.

[2] Morawiec, P.; Sołtysik-Piorunkiewicz, A. Cloud Computing, Big Data, and Blockchain Technology Adoption in ERP Implementation Methodology. Sustainability 2022, 14, 3714. https://doi.org/10.3390/su14073714

[3] Figueiredo, M. (2022). Administration of SAP HANA Cloud. In: SAP HANA Cloud in a Nutshell. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842- 8569-5_2

[4] Harale, N. D., & Meshram, D. B. B. (2016). Data mining techniques for network intrusion detection and Prevention Systems. International Journal of Innovative Research in Computer Science & Technology.

[5] Haohai Zhang et al 2019 J. Phys.: Conf. Ser. 1314 012143DOI 10.1088/1742- 6596/1314/1/012143

[6] Alizai, F., & Burgess, S. (2009). An ERP adoption model for midsize businesses. Enterprise information systems for business integration in SMEs: Technological, organizational and social dimensions, 153-174.

[7] August, T., Niculescu, M. F., & Shin, H. (2014). Cloud implications on software network structure and security risks. Information Systems Research, 25(3), 489-510.

[8] Beijsterveld, J. A., & Groenendaal, W. J. (2016). Solving misfits in ERP implementations by SMEs. Information Systems Journal, 26(4), 369-393.

[9] Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. MIS quarterly, 369-386.

[10] Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems, 52(1), 232-246.

[11] Chen, P.-y., & Wu, S.-y. (2012). The impact and implications of on-demand services on market structure. Information Systems Research, 24(3), 750-767.

[12] Coyte, R., Ricceri, F., & Guthrie, J. (2012). The management of knowledge resources in SMEs: an Australian case study. Journal of Knowledge Management, 16(5), 789-807.

[13] Duan, J., Faker, P., Fesak, A., & Stuart, T. (2012). Benefits and drawbacks of cloud-based versus traditional ERP systems. Advanced Resource Planning. Engebrethson, R. (2012). Comparative analysis of ERP emerging technologies.

[14] Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)

[15] R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama.

[16] GPB GRADXS, N RAO, Behaviour Based Credit Card Fraud Detection Design And Analysis By Using Deep Stacked Autoencoder Based Harris Grey Wolf (Hgw) Method, Scandinavian Journal of Information Systems 35 (1), 1-8.

[17] R Pulimamidi, GP Buddha, Applications of Artificial Intelligence Based Technologies in The Healthcare Industry, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4513-4519.

[18] R Pulimamidi, GP Buddha, AI-Enabled Health Systems: Transforming Personalized Medicine And Wellness, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4520-4526.

[19] GP Buddha, SP Kumar, CMR Reddy, Electronic system for authorization and use of cross-linked resource instruments, US Patent App. 17/203,879.

[20] Nadella, G. S. (2023). Validating the Overall Impact of IS on Educators in U.S. High Schools Using IS-Impact Model – A Quantitative PLS-SEM Approach, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, ISBN 9798381388480, 189, 2023.

[21] Gonaygunta, Hari, Factors Influencing the Adoption of Machine Learning Algorithms to Detect Cyber Threats in the Banking Industry, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, United States, ISBN 9798381387865, 142, 2023.

[22] Hari Gonaygunta (2023) Machine Learning Algorithms for Detection of Cyber Threats using Logistic Regression, 10.47893/ijssan.2023.1229.

[23] Hari Gonaygunta, Pawankumar Sharma, (2021) Role of AI in product management automation and effectiveness, https://doi.org/10.2139/ssrn.4637857.

[24] Sri Charan Yarlagadda, Role of Artificial Intelligence, Automation, and Machine Learning in Sustainable Plastics Packaging markets: Progress, Trends, and Directions, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 818–828, 2023.

[25] Sri Charan Yarlagadda, The Use of Artificial Intelligence and Machine Learning in Creating a Roadmap Towards a Circular Economy for Plastics, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 829-836, 2023.

[26] B. Nagaraj, A. Kalaivani, S. B. R, S. Akila, H. K. Sachdev, and S. K. N, "The Emerging Role of Artificial intelligence in STEM Higher Education: A Critical review," International Research Journal of Multidisciplinary Technovation, pp. 1–19, Aug. 2023, doi: 10.54392/irjmt2351.

[27] D. Sivabalaselvamani, K. Nanthini, Bharath Kumar Nagaraj, K. H. Gokul Kannan, K. Hariharan, M. Mallingeshwaran, Healthcare Monitoring and Analysis Using ThingSpeak IoT Platform: Capturing and Analyzing Sensor Data for Enhanced Patient Care, IGI Global eEditorial Discovery, Pages: 25, 2024. DOI: 10.4018/979-8-3693-1694-8.ch008.

[28] Amol Kulkarni, Amazon Athena Serverless Architecture and Troubleshooting, International Journal of Computer Trends and Technology, Vol, 71, issue, 5, pages 57-61, 2023.

[29] Amazon Redshift Performance Tuning and Optimization,International Journal of Computer Trends and Technology, vol, 71, issue, 2, pages, 40-44, 2023