James Alexander Quimpo

Cloud-Based VPN Replacement

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master’s Thesis

31 October 2024

PREFACE

In my role as a network engineer, I am accustomed to engaging in technical tasks and activities, often referring to established documents and configuration guidelines. Although creating a comprehensive thesis document like this one presents a significant challenge for me, it has considerably augmented my writing abilities and professional communication.

Balancing work, studies, personal endeavours, and family obligations can be quite demanding, particularly when one commitment affects another. Time management can be challenging in practice despite being a commonly discussed topic.

Although the journey was not without its difficulties, I am pleased to have fulfilled the necessary criteria for obtaining this degree. This achievement has significantly enhanced my knowledge and skills, propelling me to a higher level of proficiency.

I express immense gratitude to my professors for imparting their knowledge and guidance that enabled me to successfully complete my degree. I am also thankful to my workplace for offering me the opportunity and support for my thesis project. Above all, I bring back the glory and honour to our Almighty Lord and Saviour.

I dedicate this achievement to my dear wife and son. They have been very patient, understanding, and supportive in everything I do.

Espoo, 31 October 2024
James Alexander Quimpo

Abstract

Author:	James Alexander Quimpo
Title:	Cloud-Based VPN Replacement
Number of Pages:	44 pages + 8 appendices
Date:	31 October 2024
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services
Supervisors:	Ville Jääskeläinen, Head of IT Master's Program

Since the outbreak of the Covid-19 pandemic, remote work has become the standard practice. Many companies have faced difficulties in dealing with network connectivity and security issues arising from this abrupt transition. The task of adding extra network resources to accommodate remote work has proven to be a challenging endeavour.

I am employed as an Information and Technology Network Specialist (ITNS) at a Software Company that employs on-premises VPN gateways to facilitate remote access for employees who work remotely. With the growing number of employees working from home, there have been instances where the VPN gateway struggled to manage the high network traffic during peak hours, leading to connectivity and access problems.

As the contract for the on-premises VPN is nearing its end, it presents an opportunity to upgrade or replace it with a more scalable solution that offers enhanced security features, decreased management complexity, and improved network monitoring capabilities. This thesis results in a cloud-based alternative to VPN services.

Keywords: VPN, Gateways, Data Center

Contents

1 Introduction 1

1.1 Case Company 1
1.2 Challenges and Objectives 1

2 Theoretical Background 4

2.1 Virtual Private Network 4
2.2 VPN Gateway 6
2.2.1 How does the VPN gateway work? 6
2.2.2 VPN Gateway Benefits 7
2.2.3 VPN Gateway Disadvantages 8
2.2.4 VPN Gateway Use Cases 9
2.3 Cloud Virtual Private Network 10
2.3.1 How Does a Cloud VPN Work? 10
2.3.2 Differences and Benefits of Cloud VPN 11

3 Present Network Architecture and Support Structure 13

3.1 Network Architecture 13
3.2 Support Teams 14

4 Project Plan 16

4.1 Project Team and Structure 16
4.2 Current and Future State Table 17
4.3 Vendor Pre-Selection 18
4.4 Vendor Engagement 18
4.5 Evaluation Criteria 19
4.5.1 Features and Capabilities 20
4.5.2 Cost Components 27
4.5.3 Technical Training 27
4.6 Proof-Of-Concept 28
4.6.1 Setup and Configuration 29
4.6.2 Technical Demonstration 29
4.6.3 Test and Verification 29
4.7 Scope and Timeline 30

5 Vendor Selection Process and Results 31

5.1 Gartner Comparison 31
5.2 Current State Analysis and Capabilities 31
5.3 Costing Results 32
5.4 Technical training Results 32
5.5 Proof-of-Concept and Testing Results 33

6 Implementation 37

6.1 Deployment Components 37
6.2 Scope of Work 38
6.2.1 Stakeholders 38
6.2.2 RACI Matrix 39
6.2.3 Communications 39
6.2.4 Deployment Monitoring 40
6.3 Operations Support 42

7 Summary and Conclusions 43

References 45

Appendices 46

Appendix 1: Features and Capabilities Table – Results
Appendix 2: Current and Future State Reference
Appendix 3: Gartner Peer Insights Results
Appendix 4: Initial Pricing Results
Appendix 5: Technical Training Results Table
Appendix 6: Evaluation Criteria Table (updated)
Appendix 7: Test and Verification Table Results
Appendix 8: RACI Matrices

List of Abbreviations

AzEU	Azure Europe Region
AzUS	Azure US Region
2FA	Two-Factor Authentication
BYOD	Bring Your Own Device
CAB	Change Advisory Board
DC	Data Center
DNS	Domain Name System
EsDC	Espoo Data Center
HA	High Availability
HeDC	Helsinki Data Center
IKEv2	Internet Key Exchange version 2
InfoSec	Information Security Team
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
IT	Information and Technology Team
ITNS	Information and Technology Network Specialist
NOC	Network Operations Center Team
P2S	Point-to-Site
RACI	Responsible, Accountable, Consulted, Informed
S2S	Site-to-Site
SaaS	Software-as-a-Service
SASE	Secure Access Secure Edge
SD-WAN	Software Defined – Wide Area Network
SSL/TLS	Secure Socket Layer / Transport Layer Service
USDC	US Data Center
VPN	Virtual Private Network
VPNaaS	Virtual Private Network-as-a-Service
WAN	Wide Area Network
ZTNA	Zero Trust Network Access

1 Introduction

The global pandemic forced millions of employees to work at home, pushing information security to the limit. When organizations returned to the office environment and settled into a hybrid work model, these same teams struggled to protect an ill-defined perimeter with their increasingly vulnerable architecture.

Organizations could no longer rely on traditional network architectures to safeguard employees in a highly distributed workplace. When these architectures failed to keep up with Virtual Private Network (VPN) vulnerabilities and the shift from Data Centers (DC) to the cloud and Software-as-a-Service (SaaS) platforms, it was necessary to implement zero trust architecture as an alternative solution. This would help strengthen end-to-end defenses.

1.1 Case Company

Company ABZ is an IT company that was founded in 2015 with headquarters in Finland and more than 2000 workers spread over 21 offices in different regions. They provide integrated retail planning SaaS solutions to their customers worldwide.

Through customized assortments, profitable use of retail space, precise forecasting and restocking, and efficient personnel planning, the company is committed to assist retail enterprises to increase their competitiveness and significantly decrease food waste.

1.2 Challenges and Objectives

With the company expanding the business worldwide, the need for a global presence in terms of infrastructure is necessary, especially for the company staff, administrators and developers that manages and provides support to the customers. A robust infrastructure is necessary to ensure the company can support the needs of their customers. With technology evolving and most

companies adapting a hybrid working model, hackers are finding ways to exploit weaknesses of the current on-premises solutions. Due to this, access and security are still the top priority especially for those working remotely.

Most employees work from home these days, and the business relies on an on-premises VPN solution to give them access to critical internal resources for their jobs. The current VPN solution used by Company ABZ is hosted in a physical location managed directly by the in-house Information Technology (IT) and Network Operations Center (NOC) teams. To scale up this solution, it requires additional resources that will take a lot of time and effort to deploy. In addition, managing the solution, requires specific manpower skills dependent on the VPN vendor and brand being utilized. Since this is hosted in a physical device and though configured in High Availability (HA) pair, device failure is still a possibility and could impact all employees' access to the resources for situations such as power outages and device failure. In addition, the present solution is unable to offer end user traffic visibility for troubleshooting purposes. As VPN relies on networking, lateral network access by any user is possible and decreases the security aspect of the current solution. The capability of the on-premises VPN to provide granular control between user access to work applications poses a challenge to administrators these days.

The goal of this study is to select a suitable vendor in the market that offers a Cloud-based VPN solution that is scalable, flexible and gearing towards a Zero Trust Network Access (ZTNA) approach, that would significantly enhance security, as a viable replacement to the company's current VPN. The vendor' solution should also provide end-user traffic visibility that delivers an efficient way to troubleshoot network access issues. This also aims to implement the selected solution. It is important to highlight that the solution should integrate well with the Company's preferred architecture and design, as well as, with any existing systems in place.

The thesis comprises of seven sections. The first section presents the issue and objectives of the thesis, while the second section covers the theoretical and

technical definitions found in the relevant literature for the thesis project. The third section explores the current architecture and organization of the subject Company, and the fourth section details the project plan and proposed actions to reach the goals and objectives of the thesis. The fifth section will discuss the process and outcomes of selecting the vendor, while section 6 will cover the implementation of the chosen solution. The final section (7th) will outline the key findings and wrap up the thesis study.

2 Theoretical Background

This chapter introduces the concepts and principles of VPN and discusses the advantages and disadvantages of using them. Understanding these fundamentals will lay a solid groundwork for comprehending the technical framework upon which the study is built.

2.1 Virtual Private Network

The following paragraphs below were taken from the book by Stewart, Chappie and Gibson [1. p517-518].

According to them, “a VPN is a communication tunnel that provides point-to-point transmission to both authentication and data traffic over an intermediary untrusted network. Most VPN’s use encryption to protect the encapsulated traffic, but encryption is not necessary for the connection to be considered a VPN.”

They also mentioned that “VPN’s are most commonly associated with establishing secure communication paths through the Internet between two distant networks. However, they can exist anywhere, including within private networks or between end-user systems connected to an Internet Service Provider (ISP). The VPN can link two networks or two individual systems. They can link clients, servers, routers, firewalls, and switches. VPN’s are also helpful in providing security for legacy applications that rely on risky or vulnerable communication protocols or methodologies, especially when communication is across a network.”

The authors believed that “VPN’s can provide confidentiality and integrity over insecure or untrusted intermediary networks. They do not provide or guarantee availability. VPN’s are also in relatively widespread use to get around location requirements for services like Netflix and Hulu and thus provide a (at times questionable) level of anonymity.”

Benefits of using VPN

According to Rao and Nayak [2. p246], “a VPN allows two computers to communicate securely over the public network such as the Internet. This allows for connection of employees, partners, and other small branch offices to the corporate network securely and at low cost.”

Both authors mentioned [2. p247] that “a company’s small branch office can connect to the corporate office using VPN across the Internet and access information on the network as if it is all in the same network.” They summarized the advantages of using a VPN below:

a. Cost savings - Using private networks used to be the only solution for WAN connectivity. However, it was expensive and not always feasible, not easily scalable, and lacked security features. A VPN solution making use of the Internet is an inexpensive alternative, allowing the full advantage of cost savings of the Internet and providing a superior level of security.

b. Smooth and Seamless Integration - VPN allows seamless integration with the existing network infrastructure. There is no need to change your network architecture or any network software component.

c. Secure Remote Access - One of the primary objectives of the VPN is to provide remote users secured access to the organization’s trusted network. VPN technology allows the same connectivity whether it is network to network, host to host, client to server, dial-up connections, or home office or mobile users.

d. Extranet Connections - In today’s global economy, most organizations have one or more partners for mutual growth and success of the business. Companies have to connect to their external partners to share certain information, sometimes even critical, confidential information. Hence, they need to have a secured connection between the two partners. VPN

solutions allow secured connection between the two parties allowing even proprietary information to be shared.

e. Low Maintenance - VPN eliminates much of the day-to-day maintenance such as key management and SNMP.

2.2 VPN Gateway

Based on NordLayer website [3], “a Virtual Private Gateway is a secure way to access the company network and resources through a VPN tunnel with encrypted data in transit. It enables organizations to remotely access devices, hybrid networks, and cloud tools and provide a secured and filtered browsing experience over the internet. Use a Virtual Private Gateway for a secure, reliable VPN connection.”

2.2.1 How does the VPN gateway work?

GoodAccess website [4] mentions that “the main task of a VPN gateway is creating secure tunnels between users, networks, or systems over the internet. The way the tunnel is established and secured depends on the selected VPN protocol, such as OpenVPN, Internet Protocol Security (IPsec), or Internet Key Exchange version 2 (IKEv2). The choice of the protocol determines the speed of the connection and encryption strength, so naturally different protocols excel at different tasks.”

According to Palo Alto Networks [5], “authentication is a fundamental VPN gateway component. Before a user can access the private network, they must prove their identity. Methods of authentication range from trusted certificates on the user's device to inputting credentials in a client application. Enhanced security measures, such as Two-Factor Authentication (2FA), might be used for added protection. In addition to authentication, a VPN gateway assigns an IP address, often static, that uniquely identifies the gateway. The Internet Protocol (IP) address is crucial for tasks such as IP whitelisting and facilitating remote access.

VPN gateways manage Domain Name System (DNS) resolution to direct traffic over the Internet. Some advanced models incorporate DNS filtering to safeguard against threats such as phishing and malware. Another key role is access control, where user access rights are defined and granted, minimizing potential cybersecurity risks."

2.2.2 VPN Gateway Benefits

The VPN gateway provides several advantages. Based on K21Academy website [6], benefits were collated as follows.

a. Secure Connection - VPN gateways offer safe connection by encrypting data sent between devices and networks, shielding critical information from potential threats and illegal access.

b. Remote access - VPN gateways, particularly Point-to-Site (P2S) connections, allow remote users to securely connect to corporate or Azure virtual networks from any location, providing secure access to resources.

c. Site to Site Connectivity - Site-to-Site (S2S) VPN connections allow enterprises to securely connect on-premises networks to Azure virtual networks, enabling seamless communication between sites.

d. Flexibility & Scalability - VPN gateways offer flexibility and scalability by supporting many VPN protocols and configurations. This flexibility enables enterprises to scale their network infrastructure in response to changing business needs.

e. Centralized Management - Azure VPN gateways may be controlled centrally, making it easier for IT administrators to establish, monitor, and troubleshoot VPN connections throughout the enterprise.

2.2.3 VPN Gateway Disadvantages

There are also some disadvantages that VPN gateways have. Palo Alto Networks [5] have listed down these downsides as below:

a. Complexity - Traditional VPN gateways often require intricate setup and manual configuration, which can be cumbersome and time-consuming, especially for large networks with many remote users or branch offices.

b. Scalability Limitations - While virtual private network gateways allow for secure connections, they may struggle to scale smoothly due to their dependence on hardware and static configurations, unlike Software Defined - Wide Area Network (SD-WAN), which is designed for easy expansion across vast networks.

c. Performance Problems - VPN gateways generally lack the advanced traffic optimization and application-aware routing that SD-WAN solutions provide, potentially leading to less efficient data flow.

d. Less Visibility and Control - Compared to Secure Access Secure Edge's (SASE) cloud-native structure, traditional VPN gateways may offer limited visibility and control over network traffic and user activity, restricting detailed oversight.

e. Basic Security Features - SASE integrates various network security functions with Wide Area Network (WAN) capabilities to meet dynamic access needs, while VPN gateways typically focus on secure access without the breadth of integrated security feature.

f. Latency - Traditional VPN gateways can introduce latency by routing traffic through centralized DC's, a drawback for cloud applications, whereas SASE and SD-WAN technologies can leverage cloud gateways to minimize this issue.

g. Cost Ineffectiveness - Operating and expanding traditional VPN gateway infrastructure is generally not cost-effective. It can incur higher expenses compared to the adoption of cloud-native SASE solutions, which often have lower overheads.

h. Isolation - While VPN gateways can act as standalone solutions that may require complex integrations with other security systems, SASE provides a comprehensive and cohesive set of security tools.

i. Less Flexibility and Cloud Readiness - Traditional VPN gateways typically offer less flexibility in adjusting to various connection types and may not be as readily equipped for cloud environments, requiring additional measures for cloud optimization, unlike the inherently cloud-optimized nature of SD-WAN and SASE solutions.

2.2.4 VPN Gateway Use Cases

Palo Alto Networks [5] have summarized the common use cases for using a VPN Gateway as stated below:

a. Site-to-Site Connectivity - VPN gateways facilitate secure encrypted connections between different geographical locations of a business, such as connecting various branch offices to the main corporate network.

b. Remote Access - A point-to-site VPN connects individual devices to corporate networks via secure connections over the internet, often using VPN gateways as the access points. They provide secure access to the corporate network by connecting remote workers, ensuring that

employees can access internal resources from outside the corporate environment with the same level of security as if they were on-site.

c. Network Extension - VPN gateways extend a corporate network through encapsulated and encrypted tunnels over the public internet, allowing the network to span multiple sites over a large geographical area.

2.3 Cloud Virtual Private Network

Based on Fortinet' description [7], "a cloud virtual private network is a form of technology designed to help users access their organization's applications, data, and files through a website or an application. Unlike traditional or static VPNs, a cloud VPN provides a secure connection that can be rapidly deployed globally."

2.3.1 How Does a Cloud VPN Work?

The following paragraphs below which explains how the cloud VPN operates, were taken from Palo Alto Networks website [8].

A cloud VPN is also known as Virtual Private Network-as-a-Service (VPNaaS) or cloud based remote access VPN. A cloud-based VPN works by creating an encrypted VPN connection over the internet between a user and the company's network infrastructure hosted in the cloud. The encrypted connection is often facilitated by a VPN gateway that acts as an intermediary, encrypting and decrypting data sent to and from the cloud resources.

The process begins when a user connects to the cloud VPN service, usually through a client application. The service authenticates the user and their device, often incorporating multifactor authentication for enhanced security. Once authentication is successful, the cloud VPN sets up an encrypted tunnel using established VPN protocols, such as IPsec or Secure Socket Layer / Transport Layer Service (SSL/TLS). This tunnel ensures that data transferred between the

user and the cloud remains secure and unreadable to any unauthorized entities intercepting the traffic.

Within the cloud, a VPN gateway encrypts outgoing data before it travels across the internet and decrypts incoming data for the receiving device. This encryption is crucial for protecting sensitive information as it traverses potentially insecure networks. The cloud VPN maintains the encryption tunnel, adapting as necessary to network changes. This is especially important for remote workers who may switch between different internet connections.

Cloud-based VPNs often include advanced security measures beyond the encrypted tunnel. These can include network segmentation to control application-level access, ensuring users only reach the specific resources they are authorized to use. Security features may also extend to threat prevention, with cloud VPN services providing protections against malware, phishing, and other cyberthreats, reinforcing the security posture of cloud-based networks.

2.3.2 Differences and Benefits of Cloud VPN

This section summarizes the main differences between a traditional on-premises VPN gateway and cloud-based solution which includes its benefits. The following paragraphs below were taken from Palo Alto Networks website [8].

Cloud-based remote access VPNs and traditional VPNs serve the same basic purpose of secure remote access. They differ significantly in deployment and management. Traditional VPNs rely on physical infrastructure, necessitating on premises hardware such as VPN concentrators and dedicated VPN servers for authentication. They often require significant upfront investment in hardware and expertise to manage the network.

Cloud VPNs are service based, eliminating the need for extensive on-premises hardware. They offer a plug-and-play approach, where the VPN service is hosted in the cloud and managed by the VPN service provider. This translates to lower

initial costs and reduces the complexity of scaling as a business grows. The flexibility of cloud VPNs allows for rapid deployment and seamless integration with cloud platform services, making them more adaptable to modern business needs.

Cloud VPNs can provide better reliability through distributed architecture, which is designed to handle the dynamic nature of internet-based networking. They also typically offer a more user-friendly interface for both administrators and end users, simplifying the management and user experience of VPN services.

3 Present Network Architecture and Support Structure

This section will analyse and assess the current network architecture and operational support structure of the business, which will serve as the foundation for the thesis.

3.1 Network Architecture

Company ABZ has implemented Palo Alto devices as physical firewalls at each of its office and DC locations. The company has three separate VPN clusters that are used by employees and contractors. These VPN clusters are isolated from each other and provide access to internal resources as well as external whitelisted systems and applications when connected to the company's VPN. The VPN gateways are in three distinct DC locations: Helsinki (HeDC) and Espoo (EsDC) in Finland, and United States (USDC), specifically deployed in Atlanta, Georgia. The company primarily uses two VPN gateways in Finland due to most of its resources being situated in that region.

The DC sites are linked together in a mesh configuration through a secure and encrypted connection, with each site linked to their respective infrastructure in Microsoft Azure, where extra resources are stored. Within Azure, there are two regions accessible: Azure Europe (AzEU) and Azure US (AzUS) regions. HeDC and EsDC are linked to AzEU, while USDC is linked to AzUS. All connections from the DC's to Azure utilizes the Azure express route service that provides private and dedicated connections. The two Azure regions are not connected to each other and contain distinct resources that are exclusive to each respective region.

Employees from various locations need to connect to a VPN Gateway to access internal resources located in HeDC, EsDC, USDC, and Azure. However, when accessing public or internet-bound resources, the traffic is split-tunnelled to the local network. This setup ensures that security measures only apply to the networks accessed through the VPN, and not to internet-bound traffic.

The network architecture and connections between its components are illustrated in Figure 1 below.

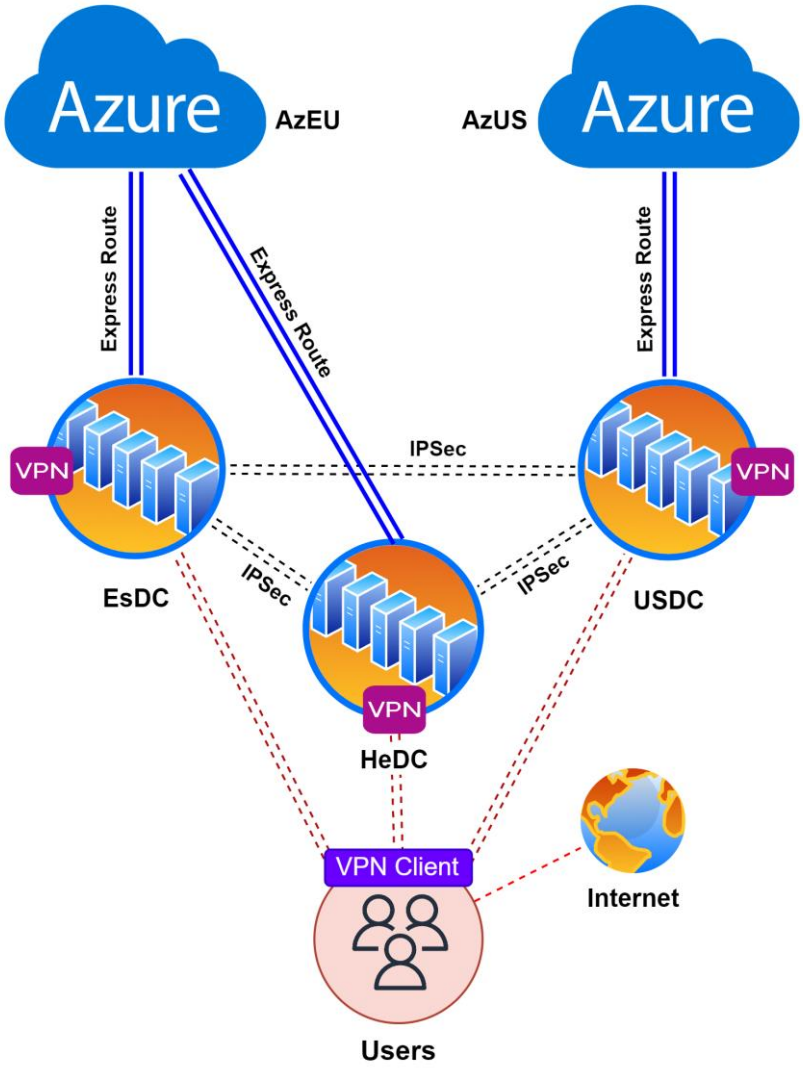

Figure 1: High Level Network Backbone Architecture

3.2 Support Teams

Within Company ABZ, there are two support teams dedicated to VPN services: the IT team and the NOC team.

The IT team focuses on providing internal network services to employees, whereas the NOC team handles customer network services. The IT team consists

of service desk personnels and desktop engineers who troubleshoot device related issues (ranging from Level 0 to Level 1). On the other hand, the NOC team comprises Junior to Senior Network Engineers (ranging from Level 2 to Level 3) who possess advanced networking skills.

The primary use of the VPN service is to provide employees and contractors with access to internal resources, necessitating specialized skills for its management and support. As a result, the NOC team is primarily responsible for handling complex issues related to the VPN.

4 Project Plan

This chapter discusses the steps prepared to select the qualified vendor and solution that addresses the use cases set by the Project team.

4.1 Project Team and Structure

The Project Team is comprised of the nominated subject matter experts of each relevant team in Company ABZ. The team members include:

a. Two Senior Network Engineers from the Network Operations Center (NOC) team – responsible for evaluating and reviewing networking related solutions
b. Two Senior Security Experts from the Information Security (InfoSec) team – responsible for evaluating and reviewing security related solutions and identifying risks.
c. One Project Manager and Engineer from the Information Technology (IT) – The Project Manager is responsible for managing the internal project communications, plan, progress and timelines while the Project Engineer is responsible in the overall project evaluation, testing and documentation up to implementation.
d. Head and Vice President of Information Technology (IT) – management team responsible to oversee the overall IT project progress and tasked to provide overall project support resources, feedback and evaluation based on the management perspective.

A Project Steering Team will also be established, consisting of the Vice Presidents of each Project Team member and key management team members from critical teams affected by the project. A monthly meeting will be organized to review the project's advancement and collect feedback. The Project Steering Team will be responsible for making rapid management decisions to facilitate a seamless project transition and effective communication among various teams in the organization.

4.2 Current and Future State Table

The primary motivation for the project is to comprehend and acknowledge the obstacles and adverse effects on business caused by the existing VPN solution. This effort is closely linked to defining the anticipated results, essential capabilities required, and the positive business outcomes that are expected from the new solution. To illustrate this concept, the Project team has developed Table 1, which will be completed by the Project team and subsequently distributed to all vendors under evaluation as a benchmark. In addition to the table provided, the Current Architecture depicted in Figure 1 and the Desired Architecture illustrated in Figure 2, which outlines the optimal future deployment, will also be shared.

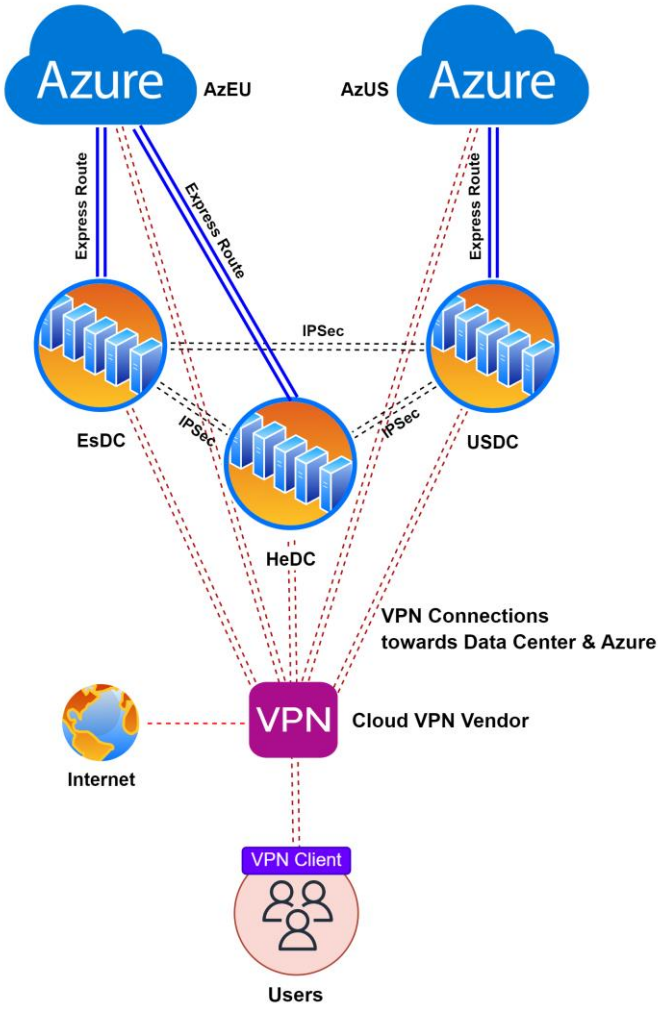

Figure 2: Desired Architecture for the new VPN

Table 1: Current and Future State Table

Current State		
Current State	*Current Challenges*	*Negative Business Impact*
Future State		
Desired Outcome and Expected Benefits	*Critical Capabilities*	*Positive Business Impact*

4.3 Vendor Pre-Selection

As a member of the project team, my role was designated as the Project Engineer. I was responsible for the preliminary selection of vendors using my expertise, research, and credible sources for feedback. This feedback included input from peers and colleagues regarding their experiences working with the vendors. Although there were numerous solutions available, we aimed to narrow down the list to the top 4 candidates who could potentially be suitable for advancing to the subsequent evaluation phases.

4.4 Vendor Engagement

Each vendor will first be contacted via email to schedule a discussion aimed at gaining a deeper insight into their capabilities beyond what is publicly available. In addition to sharing the Current and Future State table (Table 1) and Architectures depicted in Figures 1 and 2, vendors will also receive a list of

expected features for the new solution. Communication will primarily be conducted through email and video meetings using platforms like Zoom or Teams.

4.5 Evaluation Criteria

This section outlines the evaluation criteria that will be used to assess and choose the vendor solution that best meets the company's needs. Each criterion is given a weight percentage to distinguish between vendors based on their proposed solutions. Table 2 illustrates how the criteria are aggregated.

Table 2: Evaluation Criteria

Evaluation Criteria	Weight (%)	Vendor 1	Vendor 2	Vendor 3	Vendor 4
1. Cost	30%				
2. Proof-of Concept	25%				
3. Technical Workshops	15%				
4. Troubleshooting Tools	15%				
5. Credibility	15%				

a. Cost – this will be based on the advertised values available publicly and applicable offline discounts from initial discussions during the engagements with the requirements as similar as possible across all vendors.
b. Proof-of-Concept – an agreed, partial solution deployment in the company’s test or production environment to show its feasibility with the company’s critical systems and requirements.
c. Technical Workshops – initial technical sessions organized to understand the solution concepts and address relevant questions raised by the Project team.
d. End User Monitoring Service – must-have service to monitor end user device health status.

e. Credibility – measure of how the vendors manage the project discussion and how they have addressed all the questions and request coming from the Project Team. Feedback and reviews from any employees who have worked and have experienced the vendor, or solution will also be taken into consideration, as well as the comparison result of the overall features and capabilities.

4.5.1 Features and Capabilities

A list of all Cloud VPN related features and capabilities, shown from Table 3 below, have been collected based on research, from data available in each of the vendors public website, with columns for current state, target state and improvement level. The tables are explained as below:

a. Current – feature capability of the existing VPN solution
b. Target – desired level to achieve in the new solution
c. Improvement Level – difference between the current and target state that indicates how much improvement is required. This also shows the criticality of the feature being available in the solution.

Table 3: Features and Capabilities Table – Project Team

FEATURES AND CAPABILITIES	Project Team (Confidential)		
	Current	Target	Improvement Level
Advanced Threat Protection			
Anti malware / Spyware			
App-ID			
Bandwidth Control			
Command and Control Infrastructure (C2) Protection			
Cloud Access Security Broker (CASB)			

Device Quarantine			
Domain Name System (DNS) filtering			
DNS Security			
End User Experience Monitoring			
Host Information Profile (HIP)			
Intrusion Prevention System (IPS)			
Internet of Things (IoT) Security			
Logging			
Malware analysis and Protection			
Next Generation Firewall (NGFW)			
Packet Loss Mitigation			
Policy Optimizer			
Quality of Service (QoS)			
Site-to-Site IPsec VPN			
SSL Decryption/Inspection			
Secure Web Gateway (SWG)			
Threat Detection			
Uniform Resource Locator (URL) Filtering			
User Authentication			
User-ID			
Vulnerability Protection			
Wildfire and antivirus			
WAN Optimization			
With Client			
Clientless / Web Based			
Always Connect			
On Demand			
Central Management			
Internal Single Sign-On (SSO)			
Attribute-based access control (ABAC)			
Role-based access control (RBAC)			

INTEGRATIONS with VENDORS - PARTNERS	Project Team (Confidential)		
	Current	Target	Improvement Level
Office 365			
Now			
Salesforce			
Slack			
Gitlab			
Zoom			
Azure			
AWS			
Google			
Microsoft ADFS			
OKTA			
PING			
Azure AD			
SailPoint			
Google Workspace			
Citrix			
Centrify			
Onelogin			
SAML			
OpenID Connect (OIDC)			
Saviynt			
Jumpcloud			
Microsoft Endpoint Manager			
Azure Sentinel			
Apple iOS			
Apple macOS			
Google Android			
Android App for Chromebook			

CentOS Linux			
Red Hat Enterprise Linux			
Ubuntu			
Windows 10 and Universal Windows Platform (UWP)			
CERTIFICATIONS	Project Team (Confidential)		
	Current	Target	Improvement Level
International Organization for Standardization (ISO) 27001			
Service Organizational Control Type 2 (SOC 2)			
General Data Protection Regulation (GDPR)			

This will be scored by the Project team based on the Capability Rating Table shown in Table 4 below. The final scoring will be used as internal reference for the Project Team and will not be shared to the vendor.

Table 4: Capability Rating Table

Capability Rating Table		
Rating	Description	Remarks
1	No capability	No related capability within the enterprise
2	Limited capability	Enterprise has some aspects of the capability
3	Moderate capability	Enterprise has good level of capability, must lacks some aspects of it
4	Full capability	Enterprise has all the required aspects of the capability is use

The same list of capabilities will be provided to all the vendors, as shown in Table 5 below, to fill in with key columns for:

a. Availability – determines whether the feature is available or not. (e.g. Yes / No or Filled up / Blank)
b. Rating – this will be based on the Capability Rating Table in Table 4.
c. Packaging – this refers whether the specific feature is part of the base offering which is inclusive or add-on which will incur additional cost
d. Remarks – additional comments or link references provided by the vendor to support the answers.

Table 5: Features and Capabilities Table – Vendors

FEATURES AND CAPABILITIES	VendorX			
	Availability	Rating	Packaging	Remarks
Advanced Threat Protection				
Anti malware / Spyware				
App-ID				
Bandwidth Control				
C2 Protection				
CASB				
Device Quarantine				
DNS filtering				
DNS Security				
End User Experience Monitoring				
HIP				
IPS				
IoT Security				
Logging				
Malware analysis and Protection				
NGFW				
Packet Loss Mitigation				
Policy Optimizer				
QoS				

Site-to-Site IPsec VPN				
SSL Decryption/Inspection				
SWG				
Threat Detection				
URL Filtering				
User Authentication				
User-ID				
Vulnerability Protection				
Wildfire and antivirus				
WAN Optimization				
With Client				
Clientless / Web Based				
Always Connect				
On Demand				
Central Management				
Internal SSO				
ABAC				
RBAC				
INTEGRATIONS with VENDORS - PARTNERS	VendorX			
	Availability	Rating	Packaging	Remarks
Office 365				
Now				
Salesforce				
Slack				
Gitlab				
Zoom				
Azure				
AWS				
Google				

Microsoft ADFS				
OKTA				
PING				
Azure AD				
SailPoint				
Google Workspace				
Citrix				
Centrify				
Onelogin				
SAML				
OIDC				
Saviynt				
Jumpcloud				
Microsoft Endpoint Manager				
Azure Sentinel				
Apple iOS				
Apple macOS				
Google Android				
Android App for Chromebook				
CentOS Linux				
Red Hat Enterprise Linux				
Ubuntu				
Windows 10 and UWP				
CERTIFICATIONS	VendorX			
	Availability	Rating	Packaging	Remarks
ISO 27001				
SOC 2				
GDPR				

This overall result derived in this section will be included in the Evaluation Criteria for Credibility identified in Table 2.

4.5.2 Cost Components

The project team will be evaluating the initial cost provided by each vendor in relation to the solution that they will offer based on the identified future state and desired architecture for the new VPN. The project team acknowledges that components of the solution offered might differ between vendors and will consider the relevance and complexity based on how it will address the current challenges.

4.5.3 Technical Training

The training session will consist of an in-depth technical conversation to comprehend the functionality of the solution and its ability to tackle various challenges and scenarios. The project team will participate in the session along with technical subject matter experts. Each vendor will have a 3-hour slot to present their technical solution and respond to any queries or concerns from the project team. Each vendor will receive a comprehensive list of use cases outlined in Table 6, excluding any ratings, two weeks before the session to allow for adequate preparation.

Following the session, the project team will collect feedback from the team members and work together to generate an overall score and evaluation displayed in Table 6.

Table 6: Technical Training Use Case Table

Use Case		VendorX Rating (1 - 5)	Weightage	Remarks
A	Internal (Private DC)	5	20.00 %	
	Internal (Public Cloud)	5	20.00 %	
	Internal (SaaS)	5	10.00 %	
B	External (internet)	5	10.00 %	
C	Whitelisting	5	15.00 %	
D	End user Support	5	10.00 %	
E	Device Management	5	5.00 %	
G	IGA/IAM Integration	5	5.00 %	
H	Support for Linux Users	5	5.00 %	
	TOTAL	45	100.00 %	

Vendor rating will be based on the overall satisfaction level and acceptance of the Project team' assessment of the solution.

- Rating between 4 to 5: Fulfilling our requirements
- Rating 3: Satisfied but can be improved
- Rating between 1 to 2: Not satisfied but okay
- Rating 0: Not satisfied at all

4.6 Proof-Of-Concept

Following the initial evaluations conducted in the earlier stages, the two best vendors will be chosen to proceed with the proof-of-concept discussion. During this phase, they will offer trial licenses and assistance with the initial setup to facilitate the implementation of the solution in our test environment for further evaluation of its feasibility. This entire process will be confined to a one-month timeframe, with regular monitoring and efficient allocation of resources. The tests will continue to be aligned with the specific use cases identified during the technical training.

The primary goal of the activity is to recognize possible obstacles that may arise during deployment. Additionally, it seeks to guarantee the practicality and effectiveness of the solution when tested against key systems that will be part of the deployment for evaluation and comparison.

4.6.1 Setup and Configuration

During this phase, the project team will be responsible for identifying and setting up the required test environment infrastructure. The vendor will be tasked with obtaining the necessary licenses and supplying the resources needed for the testing activity.

Additionally, the project team will ensure that there are sufficient internal resources available throughout the entire testing period. This involves individuals with expertise in technical subjects, owners of the system under consideration, and verifying that all required requests have been properly reviewed and authorized.

4.6.2 Technical Demonstration

Every vendor will have the chance to demonstrate and explain the functionality of their solution, highlighting its advantages and features. This exercise will also serve to tackle any issues and explore possible solutions or workarounds.

4.6.3 Test and Verification

In addition to the technical training scenarios outlined for evaluation in Table 6, supplementary assessments will be incorporated, as illustrated in Table 7.

Table 7: Test and Verification Table

Test Criteria	Task	Test User and Device	Date and Time	Location	Result		Pass / Fail	Remarks
					Existing VPN	Vendor X		
					Latency (ms)	Latency (ms)		
Latency Test								
User experience with client								

4.7 Scope and Timeline

The project will commence with the vendor pre-selection process and continue through to the implementation phase. The timeline for the project is set to start in November 2022 with the goal of completing the implementation by November 2023. The focus of the thesis will be on the deployment of VPN services for employees of Company ABZ, with the exclusion of contractors. The execution will encompass just three DC locations (HeDC, EsDC, and USDC) and two Azure regions (AzEU and AzUS). It will also involve the successful installation on a minimum of 20 user devices utilizing various operating systems, including Mac, Windows, and Linux Operating Systems, which are supplied and maintained by Company ABZ.

5 Vendor Selection Process and Results

This section focuses on the outcomes of the vendor selection strategy outlined in section 4. The goal is to choose a single vendor for the implementation stage.

5.1 Gartner Comparison

Following the evaluation of feedback and information obtained during the preliminary vendor pre-selection process outlined in section 4.3, we have identified the top four vendors to proceed with for further assessment and selection.

To compare the vendors based on the similar or equally related service offering, we have utilized Gartner Peer Insights Comparison website [9] and selected the Security Service Edge Service as baseline for comparison due to its similar nature with the VPN. We have the following summarized results shown in Appendix 3.

From the results, Vendor1 and Vendor2 has the highest rating (4.6) while being followed by Vendor4 (4.5) and Vendor3 (4.4).

5.2 Current State Analysis and Capabilities

The project team has completed the Current and Future state table, as displayed in Appendix 2. This table will be used as a guide for the pre-selected vendors to understand Company ABZ's needs and provide appropriate services and solutions. Identifying the issues Company ABZ aims to address is crucial in determining the services that can be offered to achieve the desired future state.

Table 3 has been filled up by the project team and results were compiled and included in Appendix 1.

A video session has been arranged to the vendors individually to clarify information from Table 4 and required data in Table 5. This is also to clear up any questions that they may have. The vendors were provided a week to revert with the completed data in Table 5. The compiled list is shown in Appendix 1, and it includes the overall scoring and weightage used to compare each vendor. The results shows that Vendor3 has the highest capability rating at 97.65, followed by Vendor1 at 90.97, Vendor4 at 90.71 and Vendor2 at 83.98.

5.3 Costing Results

After understanding the capabilities of each vendor, they have been requested to provide the licenses required and rough pricing needed based on the below additional criteria in reference to Appendix 4:

- 1,000 users
- Connection to 3 x Private DC's and 2 x Azure Cloud Regions

Initial basic components and pricing has been provided by the vendors shown and the summarized results as shown in Appendix 4:

From the results, Vendor1 and Vendor4 are relatively cheaper than Vendor2 and Vendor3.

5.4 Technical training Results

In the evaluation phase, it was determined that Vendor4 insists on deploying their own proprietary physical device at each of the DC locations to handle the traffic for the new VPN. However, Company ABZ finds this requirement unsuitable as it would result in increased support overhead for maintenance and operations. Moreover, deploying physical devices onsite carries risks such as device failures and power outages that could impact the overall service quality. Therefore, Vendor4 has been eliminated from the selection process.

As a result, the remaining three vendors will undergo technical training with the project team to enhance their understanding of the advanced technical aspects and address any immediate queries. Before the training session, a Table outlining the specific use cases that need to be emphasized has been shared with the vendors for reference.

Throughout the training session, the project team gained a clear understanding of the technical distinctions and crucial elements distinguishing various vendors. Subsequently, a scoring system was implemented, and the outcomes are detailed in Appendix 5.

Following an analysis of these results and in preparation for the proof-of-concept phase and the assessment of troubleshooting tools, the Evaluation Criteria Table was revised to include the latest findings, as presented in Appendix 6.

5.5 Proof-of-Concept and Testing Results

During the Proof-of-Concept phase, Company ABZ will need substantial resources to evaluate three vendors. While it is possible to manage, this process may disrupt regular business activities because of the tight project schedule. According to the findings in Appendix 5 and the exclusion of Vendor4 from the technical workshop, the revised partial results in Appendix 6 indicate a significant preference for Vendor1. Due to practical considerations, the Project team opted to proceed with Vendor1 and discontinue engagement with the other vendors. This decision carries a potential risk in the event that Vendor1's performance does not meet expectations in the future stages of the project.

The Steering team has been informed about this issue. The outcomes have been communicated and the input of each member of the Project team has been taken into account. As Vendor1 has shown promising results, the Steering Team recommended proceeding with the Proof-of-Concept exclusively with Vendor1 to ensure successful delivery of results. Vendor1's main drawback is the expense associated with future expansion, specifically in terms of additional network

connections for future deployments. However, considering Company ABZ's projected growth over the next five years, the existing connections included in Vendor1's base package should be sufficient to accommodate any potential expansions. Negotiations regarding pricing will be postponed for a later stage. In order to mitigate the risk of Vendor1's failure during this phase, Vendor2 and Vendor3 will only be notified of the final decision after the Proof-of-Concept stage with Vendor1 is concluded. This approach will also guarantee the availability of a contingency plan in the event of Vendor1's failure in the evaluation process.

Hence, the Project team organized a Proof-of-Concept demonstration for Vendor1. They set up and implemented network connections in the testing environment, activated trial licenses for a 2-month period to allow sufficient testing before the licenses expire. Figure 3 illustrates the network architecture intended for the testing phase.

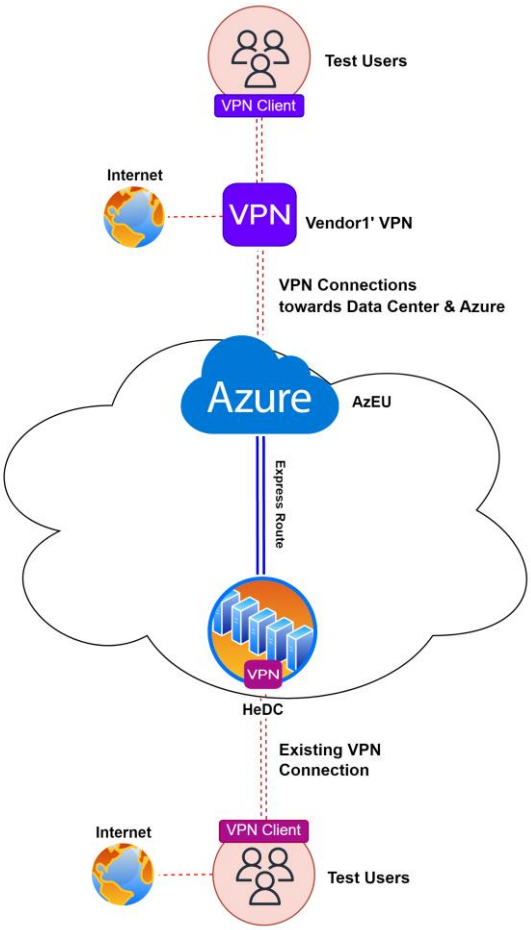

Figure 3: Test Architecture for the new VPN

The components have been implemented as anticipated, and testing has been scheduled according to the Test and Verification Table presented in Table 7. As there is only one vendor assessed at this point, the comparison will be made between the outcomes of Vendor1 and the existing on-premises VPN solution.

Due to the nature of the test environment and available trial licenses, the deployment was focused on connection towards HeDC in Finland. The following test and setup conditions were outlined as:

a. user must be in good quality local network and with internet that is sufficient (1Gbps if possible, with no other users)
b. each test has minimum 2 runs at a time, and are conducted multiple times at different times of day and week (to accommodate Vendors platform scalability and outliers in network quality)
c. time of each test run with the result must be documented with timestamp. Individual results are saved, average of total is provided.

The findings presented in Appendix 7 indicate that Vendor1 primarily experienced failed latency results. Upon reviewing the results with Vendor1, it was determined that the issue lies in the limited connections between the test Data Center (HeDC) and Vendor1's VPN solution. Potential improvements in the connections were discussed to address this high latency issue. Moreover, the outcome of an extra hop caused by the modifications in Company ABZ's egress connection (routing through Azure instead of Company ABZ's DC's) led to an additional layer that contributes to the latency compared to the current VPN arrangement. Following the evaluation, the latencies could be minimized by setting up additional connections in the live deployment, with dedicated links to each DC's and multiple VPN gateways accessible for usage. While certain latencies may remain elevated compared to the current VPN setup, the variances are deemed satisfactory in terms of user experience and can be enhanced during the live deployment.

The tools and services in Vendor1's dashboard have undergone testing, particularly for end user traffic visibility to assist in troubleshooting situations. The

findings reveal numerous telemetry data points that offer visual and statistical insights into user traffic flow, device specifics, and other pertinent information for the operations team's analysis and reference. These tools enable the operations team to pinpoint network issues accurately and swiftly implement the necessary solutions. The dashboard functioned as a central hub for accessing the necessary tools to implement, maintain, operate, and oversee the solution.

After conducting a final evaluation and analysing the outcomes, the Project team opted to proceed with the solution proposed by Vendor1. The Steering team has been notified and they have endorsed the decision. As a result of this, Vendor2 and Vendor3 received official notification via email that they were not chosen based on the overall outcomes.

6 Implementation

This section addresses the overall execution of the chosen solution, including the procedures and components utilized to accomplish the tasks. It does not cover the procurement process, which includes the Vendor's contract, negotiations, and purchases. Instead, it concentrates on the technical implementation of the selected solution, which incorporates the responsibility assignment matrix for the stakeholders participating in the project.

6.1 Deployment Components

Based on the overall outcome of the Vendor evaluation, it was identified to deploy additional and optimal connections from Vendor1' network towards Company ABZ DC's. The decision was based on technical feasibility and cost considerations for the new setup.

As a result, two connections will be created from Vendor1' infrastructure and linked directly to the Azure regions instead of connecting them to all the DC's to reduce costs. The addition of this feature will enhance overall latency performance. Additionally, multiple VPN gateways will be accessible for deployment in various regions to facilitate quicker user connections to internet-based applications and internal systems. The following revised architecture will be implemented for the deployment process.

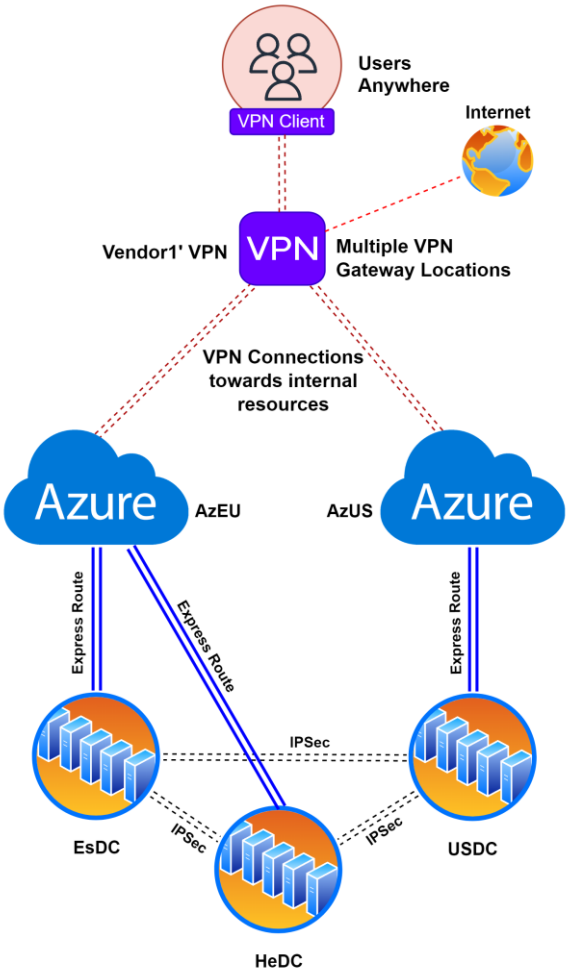

Figure 4: Final Architecture for the new VPN

6.2 Scope of Work

The Project team has identified and planned the overall scope of work and will be limited to the general components on how the solution will be implemented and supported within Company ABZ's resources.

6.2.1 Stakeholders

The focus of the Project team will continue to be on executing the solution. This will involve creating plans for deployment, such as setting up new network connection, adjusting routing updating security policies, and communicating with users during the pilot and launch phases.

However, identifying the stakeholders in this section will only comprise of teams that will be responsible to use, support and manage the solution in day-to-day operations. Stakeholders involves:

a. User – responsible to report any incidents or in raising any requests in relation to the VPN.
b. IT Operations teams – responsible for Level 0 to Level 1 support
c. IT Network Team – responsible for Level 2 support
d. NOC Team – responsible for supporting cases where DC and cloud network is involved.
e. Vendor – responsible in Level 3 support for complex cases that can't be resolved by the IT network team within the VPN.

6.2.2 RACI Matrix

The stakeholders have been recognized, and the project team has established a responsibility assignment matrix which identifies the tasks of each stakeholder involved in the day-to-day operations of the new VPN. This matrix is called RACI Matrix and according to Good L [10], "RACI is a project management acronym for the different responsibility types within a project: Responsible, Accountable, Consulted, and Informed. The RACI matrix clarifies the roles named individuals or groups will play in the successful delivery of the project. Accurate RACI matrices can help ensure a project's success before it even begins."

The RACI Matrices has been prepared in relation to processes involving service requests, management of incidents and changes and platform upgrades and maintenance as seen in Appendix 8.

6.2.3 Communications

A dedicated internal information page has been created to offer users details about the recently implemented VPN solution. The page includes a brief overview of the project, comparisons with the current system, and advantages of the new

solution. Sub-pages feature FAQs, user guides, support resources, and operational guidelines for the new solution.

The method of communication chosen to notify all users will be email. The scheduled launch date is set for 27th November 2023, allowing a minimum of 3 months for system and application owners to make necessary adjustments to their environment. Detailed technical information, including new VPN IP Addresses and security policies, has been incorporated into internal information pages. The corresponding links will be provided in the email notifications sent to all users. According to the project's execution and communication plan, the activities align with the scheduled project timeline and can be finished as planned.

In addition to our regular help-desk support channel, we have introduced an internal chat group specifically for addressing any new VPN-related issues or reports swiftly and providing high-priority support during and after the project's launch. This initiative aims to ensure immediate assistance is accessible and to gather feedback for enhancing service quality.

Several email reminders were sent according to a predetermined schedule to ensure users were kept updated and could familiarize themselves with the new solution. Moreover, the old VPN will remain accessible for a period of 3 months following the implementation date, providing a fallback option in case of any significant issues post-implementation. However, the availability of this fallback option will be determined on a case-by-case basis, contingent upon the severity of the issue, and will ultimately be assessed and determined by the project team.

6.2.4 Deployment Monitoring

This section will discuss the post-deployment scenario, highlighting the feedback received from users.

Following the implementation, several systems faced challenges in transitioning their policies to the new VPN. Consequently, certain internal users were unable

to access their applications or systems through the new VPN. These users were permitted to continue using the old VPN temporarily, with a requirement to make the necessary adjustments within three months or before the old VPN is deactivated.

Despite some systems missing the deadline for changes, the migration from the old to the new VPN proceeded smoothly. Most users expressed contentment with the enhancements and new features that were implemented. Additionally, there was a noticeable improvement in latency. Nevertheless, two significant incidents were identified during the monitoring phase.

Initially, several websites that were previously accessible were found to be blocked. The Project team conducted a thorough review and identified that the default security policies of the new VPN have more stringent rules for blocking URLs/Domains categorized as:

- New Domains: Websites that was registered within 30 days.
- Anonymous Proxies: Websites identifies as using proxy servers to bypass filtering.
- Insufficient: Test websites or those with insufficient contents

The matter was deliberated with our Information Security team, and a resolution to potentially lift the restrictions on certain blocked categories was considered. Nevertheless, monitoring and logging activities will persist as part of the security assessment in the future. Subsequent adjustments were made, leading to a decrease in incidents related to blocked websites.

Additionally, several users encountered difficulties with the new VPN application during their initial connection attempts. It has been determined that the presence of cached data from the previous VPN configuration is causing conflicts with the new VPN settings, leading to issues with the correct functioning and freezing of the new application. To resolve this issue, it is necessary to restart the device.

The Project team carefully reviewed reports from multiple users and implemented the necessary fixes. A solution was added to the user instruction page to provide better self-help guidance for similar issues in the future.

Monitoring was conducted for three months after the project's launch date. Subsequently, the old VPN was deactivated and reserved for specific rollback situations as required.

6.3 Operations Support

This section focuses primarily on the RACI matrix introduced in Section 6.2.2 and detailed in Appendix 8. The RACI matrix is utilized for identifying the key stakeholders responsible for assisting the implementation of the new VPN operations.

In addition to the RACI matrix, specialized training sessions have been organized to educate and aid in the support of the new VPN service. A dedicated internal information page has been created for the operations team, which includes details such as:

- Support Contact Information and Escalation Matrix
- Important Project links and Documentations
- Network Architectures
- Area of Responsibility and Scope of Work
- Support Processes

The content presented on this internal page is designed to assist members of the operations team in effectively resolving any issues or requests related to the new VPN service. It serves as a comprehensive resource for gaining a better understanding of the new VPN service.

7 Summary and Conclusions

As a result of the rapid expansion of companies and the rise in the number of employees working from home or remotely, having a strong global presence and reliable VPN infrastructure is essential. This is crucial to ensure that employees can access internal resources without any disruption, thereby supporting the needs of their customers effectively. However, the lack of visibility into end-user traffic can present challenges for operations support teams when addressing issues related to user VPN connections. The objective of this project was to identify an appropriate solution that can accommodate the company's rapid growth, be adaptable to changes, and align with a Zero Trust Network Access (ZTNA) approach to enhance cloud security. Additionally, the solution should incorporate enhanced features for end-user traffic monitoring.

To assess potential solutions, a preliminary selection process was conducted, and an evaluation criteria table was developed by the project team. This table facilitated the comparison of solutions in terms of cost, proof-of-concept, technical workshops, troubleshooting tools, and credibility. After evaluating the initial results based on specific criteria, Company ABZ chose to proceed with Vendor1, as it had already demonstrated positive outcomes before the completion of the proof-of-concept and troubleshooting tools assessment. The evaluation of the remaining criteria for Vendor1 also yielded positive results. Upon consolidating and validating all the results, Vendor1 advanced to the implementation stage.

The implementation process faced certain challenges; however, they were successfully resolved, and the project was finished within the designated timeframe.

Following the successful implementation and current utilization of the solution by Company ABZ, it has been determined that the offering from Vendor1 has been well-received. The outcome has enhanced the overall user experience because of its user-friendly interface and increased accessibility, particularly with the inclusion of multiple VPN gateways accessible in various regions worldwide. The

enhanced user experience was particularly beneficial for individuals working remotely and abroad. It also led to a decrease in operational costs for the team responsible for the service, as the technical aspects of the service were simplified. Furthermore, the vendor now oversees the main infrastructure, resulting in a reduced workload for company ABZ's operations team.

As this VPN solution operates in the cloud, there is potential for additional security enhancements to be developed and integrated in the future. This will bolster security measures and safeguard the company's assets and users from cyber threats. Vendor1 provides various services aligned with ZTNA, a direction that Company ABZ plans to pursue. While these service enhancements are currently available, but inactive, they can be addressed later as part of service improvement discussions.

The project team also conducted a project retrospective to collect input on the completed work and ways to enhance team engagement. The project was deemed successful, and the management acknowledged and rewarded the contributions of all team members.

References

1 Stewart JM, Chapple M, & Gibson D. *ISC2 Certified Information Systems Security Professional: Official Study Guide*. 7th ed. Canada: Sybex Inc; 2014.

2 Rao, UH & Nayak U. *The InfoSec Handbook: An Introduction to Information Security*. Apress Berkeley, CA; 2014. doi:10.1007/978-1-4302-6383-8

3 Nord Security. *Virtual Private Gateway*. NordLayer Website. 2024. Accessed September 29, 2024. https://nordlayer.com/features/private-gateway/

4 GoodAccess. *VPN Gateway: Everything You Need To Know*. GoodAccess Website. 2024. Accessed on September 29. 2024. https://www.goodaccess.com/blog/vpn-gateway-everything-you-need-to-know

5 Palo Alto Networks. *What is a VPN Gateway?.* Palo Alto Networks Website. 2024. Accessed September 29, 2024. https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn-gateway

6 Raj A. *Overview of Azure VPN Gateway.* K21Academy Website. Updated March 18, 2024. Accessed September 29, 2024. https://k21academy.com/microsoft-azure/architect/overview-of-azure-vpn-gateway/#3

7 Fortinet. *What Is Cloud VPN? Categories and Classifications.* Fortinet Website. 2024. Accessed September 29, 2024. https://www.fortinet.com/resources/cyberglossary/cloud-vpn

8 Palo Alto Networks. *What Is a Cloud VPN? | Cloud-Based Remote Access VPNs Explained.* Palo Alto Networks Website. 2024. Accessed September 29, 2024. https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-vpn

9 Gartner Peer Insights. *Choose Enterprise Technology Software and Services with Confidence.* Gartner Website. 2022. Accessed on December 19, 2022. https://www.gartner.com/peer-insights/home

10 Good L. *What Is a RACI Matrix?.* Project-Management Website. Updated April 19, 2024. Accessed September 29, 2024. https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/

Appendices

Appendix 1: Features and Capabilities Table – Results

FEATURES AND CAPABILITIES													POINT CREDIT			
	FEATURES AND CAPABILITIES	Current	Target	Improvement Level	Vendor 1		Vendor2		Vendor3		Vendor4		Vendor1	Vendor2	Vendor3	Vendor4
FEATURES	Advanced Threat Protection	3	4	1	4	Standard	4	Add-on	4	Standard	4	Add-on	4	4	4	4
	Anti malware / Spyware	2	2	0	4	Standard	4	Add-on	4	Standard	4	Standard	2	2	2	2
	App-ID	2	2	0	4	Standard	4	Standard	4	Standard	3	Standard	2	2	2	2
	Bandwidth Control	1	1	0	4	Standard	4	Standard	4	Standard	3	Add-on	1	1	1	1
	C2 Protection	2	2	0	4	Standard	4	Add-on	4	Standard	3	Standard	2	2	2	2
	CASB	1	3	2	4	Add-on	4	Add-on	4	Standard	3	Add-on	3	3	3	3
	Device Quarantine	1	1	0	4	Standard	3	Standard	4	Add-on	3	Standard	1	1	1	1
	DNS filtering	2	2	0	4	Standard	4	Standard	4	Standard	4	Standard	2	2	2	2
	DNS Security	2	2	0	4	Standard	3	Add-on	4	Standard	4	Standard	2	2	2	2
	End User Experience Monitoring	1	4	3	4	Standard	3	Standard	4	Standard	4	Add-on	4	3	4	4
	Host Information Profile (HIP)	2	2	0	4	Standard	3	Standard	4	Standard	3	Standard	2	2	2	2
	Intrusion Prevention System (IPS)	4	4	0	4	Standard	4	Add-on	4	Standard	2	Add-on	4	4	4	2
	IoT Security	1	1	0	4	Add-on	1		4	Add-on	2	Standard	1	1	1	1
	Logging	3	4	1	4	Standard	4	Standard	3	Standard	3	Standard	4	4	3	3
	Malware analysis and Protection	3	3	0	4	Standard	4	Add-on	4	Standard	3	Add-on	3	3	3	3
	NGFW	1	3	2	4	Standard	4	Standard	4	Standard	4	Standard	3	3	3	3
	Packet Loss Mitigation	1	1	0	1	Add-on	4	Standard	1		4	Add-on	1	1	1	1
	Policy Optimizer	1	2	1	4	Add-on	1		4	Add-on	1		2	1	2	1
	Quality of Service (QoS)	1	1	0	4	Standard	4	Standard	4	Standard	3	Standard	1	1	1	1
	Site-to-Site IPsec VPN	3	4	1	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
	SSL Decryption/Inspection	1	1	0	4	Standard	4	Standard	4	Standard	4	Standard	1	1	1	1
	SWG	1	2	1	4	Standard	4	Standard	4	Standard	3	Standard	2	2	2	2
	Threat Detection	3	3	0	4	Standard	4	Add-on	4	Standard	4	Standard	3	3	3	3
	URL Filtering	2	2	0	4	Standard	4	Standard	4	Standard	4	Standard	2	2	2	2
	User Authentication	3	3	0	4	Standard	4	Standard	4	Standard	4	Standard	3	3	3	3
	User-ID	2	2	0	4	Standard	4	Standard	4	Standard	4	Standard	2	2	2	2
	Vulnerability Protection	3	3	0	4	Standard	4	Add-on	4	Standard	1		3	3	3	1
	Wildfire and antivirus	2	2	0	4	Standard	4	Add-on	4	Standard	3	Add-on	2	2	2	2
	WAN Optimization	1	1	0	1		2	Standard	1		3	Add-on	1	1	1	1
USER ACCESS to VPN	With Client	4	4	0	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
	Clientless / Web Based	1	4	3	4	Standard	3	Standard	4	Standard	2	Standard	4	3	4	2
USER ACCESS TYPE	Always Connect	1	3	2	4	Standard	4	Standard	4	Standard	4	Standard	3	3	3	3
	On Demand	4	4	0	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
MGMT INTERFACE	Central Management	1	3	2	4	Standard	4	Standard	4	Standard	4	Standard	3	3	3	3
ACCESS MANAGEMENT	Internal SSO	3	4	1	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
ACCESS CONTROL	Attribute-based access control (ABAC)	1	4	3	4	Standard	1		4	Standard	3	Standard	4	1	4	3
	Role-based access control (RBAC)	4	4	0	4	Standard	4	Standard	4	Standard	3	Standard	4	4	4	3
	Sub-Total (Features)	74	97										97	91	96	87
	Sub-Total (Weightage)	30.52	40.00										40.00	37.53	39.59	35.88

INTEGRATIONS with VENDORS - PARTNERS													POINT CREDIT			
	INTEGRATIONS	Current	Target	Improvement Level	Vendor 1		Vendor2		Vendor3		Vendor4		Vendor1	Vendor2	Vendor3	Vendor4
SAAS INTEGRATION	Office 365	3	4	1	4	Standard	3	Add-on	4	Standard	4	Standard	4	3	4	4
	Now	1	1	0	4	Standard	1		4	Standard	4	Standard	1	1	1	1
	Salesforce	3	4	1	4	Standard	3	Add-on	4	Standard	4	Standard	4	3	4	4
	Slack	4	4	0	4	Standard	3	Add-on	4	Standard	4	Standard	4	3	4	4
	Gitlab	4	4	0	1		3	Add-on	4		4	Standard	1	3	4	4
	Zoom	1	3	2	4	Standard	1		4	Standard	4	Standard	3	1	3	3
CLOUD PROVIDERS	Azure	3	4	1	3	Standard	4	Standard	4	Standard	3	Standard	3	4	4	3
	AWS	3	3	0	1		4	Standard	4	Standard	3	Standard	1	3	3	3
	Google	1	1	0	1		3	Standard	4	Add-on	3	Standard	1	1	1	1
IDENTITY MANAGEMENT	Microsoft ADFS	1	2	1	4	Standard	1		4	Standard	4	Standard	2	1	2	2
	OKTA	3	3	0	4	Standard	4	Standard	4	Standard	4	Standard	3	3	3	3
	PING	1	1	0	4	Standard	1		4	Standard	4	Standard	1	1	1	1
	Azure AD	4	4	0	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
	SailPoint	1	4	3	1		1		4	Standard	1		1	1	4	1
	Google Workspace	1	1	0	4	Standard	3	Add-on	4	Standard	4	Standard	1	1	1	1
	Citrix	2	2	0	2		3	Add-on	1		4	Standard	2	2	1	2
	Centrify	1	1	0	4	Standard	1		4	Standard	4	Standard	1	1	1	1
	Onelogin	1	1	0	2	Standard	4	Standard	4	Standard	4	Standard	1	1	1	1
	SAML	4	4	0	2	Standard	1		4	Standard	4	Standard	2	1	4	4
	OIDC	2	2	0	1	Standard	3	Standard	4	Standard	4	Standard	1	2	2	2
	Saviynt	1	4	3	2	Standard	1		4	Standard	1		2	1	4	1
	Jumpcloud	1	1	0	4	Standard	3	Standard	3	Standard	4	Standard	1	1	1	1
ENDPOINT SECURITY / MANAGEMENT	Microsoft Endpoint Manager	4	4	0	4	Standard	1		4	Standard	4	Standard	4	1	4	4
OPERATIONS	Azure Sentinel	1	3	2	4	Standard	4	Standard	4	Standard	3	Standard	3	3	3	3
END USER PLATFORM SUPPORT	Apple iOS	4	4	0	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
	Apple macOS	4	4	0	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
	Google Android	4	4	0	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
	Android App for Chromebook	3	3	0	4	Standard	4	Standard	4	Standard	2	Standard	3	3	3	2
	CentOS Linux	2	3	1	4	Standard	4	Standard	4	Standard	4	Standard	3	3	3	3
	Red Hat Enterprise Linux	2	3	1	4	Standard	1		1		4	Standard	3	1	1	3
	Ubuntu	2	3	1	4	Standard	4	Standard	4	Standard	4	Standard	3	3	3	3
	Windows 10 and UWP	4	4	0	4	Standard	4	Standard	4	Standard	4	Standard	4	4	4	4
	Sub-Total (Features)	76	93										79	72	90	85
	Sub-Total (Weightage)	49.03	60.00										50.97	46.45	58.06	54.84
	TOTAL (%)	79.55	100.00										90.97	83.98	97.65	90.71

Appendix 2: Current and Future State Reference

Current State

Current State	Current Challenges	Negative Business impact
- 3 Palo Alto clusters (virtually separated as internal and external user VPN GW) - Microsoft Entra ID as Identity Provider - Microsoft Intune as Device Management tool - OKTA for Access Management - 2 x Remote Offices (Hub and Spoke S2S VPN) - 3 x Data Centers with Express Routes to Azure - hosting customer' web and apps - Hybrid user model with majority on remote work) - Access to multiple SaaS Applications without VPN - Users: Internal (permanent employees, contract-based and acquisitions), External (contractors and vendors) - NOC team managing both customer, L3 and VPN	- Not enough capacity in VPN setup (no redundancy) - Access to resources are getting slower - Centralized VPN chokepoint - VPN Gateway not covering all regions worldwide - Unable to scale quickly if need to increase capacity - Unable to see insights about user end-to-end experience - Official Linux Client requires Global Protect License - Not optimal routing paths for traffic for 2 x Remote Offices - Identity based access is partially implemented (Role Based Access Control) - External users and contractors have no proper user control and access management in place - Poor to no support for external and offsite users - Large number of S2S VPN tunnels within the Data Centers and Remote Sites - No license for advanced security protection like URL/Wildfire/DNS security - Limits on throughput and performance	- Decreased productivity - Longer data travel time for remote users reliant to VPN. - Delays in project deployment and resource intensive activity that affects allocation of resources. - Troubleshooting requires longer time that affects Ops and users' productivity. - Increased user based for Linux unable to connect thru VPN

Future State

Desired outcome and expected benefits	Critical capabilities	Positive Business Impact
Cloud Based VPN Solution - Replacement of the existing physical VPN - Scalable solution with worldwide presence for improved latencies - Consolidation of access routes to improve management - Central management dashboard for operations - Visibility of end-to-end user traffic and telementry data - Improved and proactive security controls and features - SASE future integration	*- Features: Advanced Threat Protection, Intrusion and Prevention System, Site-to-Site VPN, and other security features* *- Operational Management: Central Management User Interface* *- User Access to VPN: with client or clientless* *- User Access Type: on demand or always connect* *- Access to Apps: Single Sign on* *- Access Control: Role Based Access Control or Attribute Based Access Control* *- SAAS Integration: O365* *- Cloud Integration: Azure* *- IAM Integration: Saviynt* *- Endpoint Security and Management: Microsoft* *- End User Platform Support: Windows, Apple iOS, macOS, Google Android, Chromebook, Linux, Ubuntu* *- Certifications: ISO 27001 and SOC2* *- Logs: 6-12 mos retention (can be exported)* *- GDPR compliant*	- Less VPN tunnels, common routing points (lesser management overhead) - Simplify and segregate, users away from on-premise firewall hardware - Any location works the same: office, home, hot-spot, café. Any location is managed the same. No trust based on assumptions. - Multiple gateways available globally, not tied to limited locations (Cloud gateways) - Support for both internal and external users. - Cut VPN dependencies to physical locations - Segregation of traffic between customers and Company ABZ' employees - Lower latencies from "any" location globally - Better global user experience and availability - Improved security and logging, access mgmt - Internal and external users with productized approach - Enterprise Level Quality for experience, security and

Appendix 3: Gartner Peer Insights Results

Comparison	Vendor1	Vendor2	Vendor3	Vendor4
Overall Rating	**4.6**	**4.6**	4.4	4.5
Overall Capability Score	4.7	4.7	4.5	4.6
Scalability				
Integration				
Customization				
Ease of Deployment, admin and maintenance				
Evaluation and Contracting	4.6	4.6	4.3	4.6
Pricing Flexibility				
Ability to understand needs				
Integration and Deployment	4.6	4.6	4.5	4.5
Ease of Deployment				
Quality of End User Training				
Ease of Integration using Standard APIs and tools				
Availability of 3rd party resources				
Service and Support	4.5	4.6	4.6	4.5
Timeliness of Vendor Response				

Quality of technical support				
Quality of Peer User Community				
Evaluation Criteria (15%)	**13.80%**	**13.80%**	**13.20%**	**13.5%**

The calculation of the 30% Evaluation Criteria for cost are as follows:
[(Overall Rating / 5) * 15]%

Appendix 4: Initial Pricing Results

	Vendor1	**Vendor2**	**Vendor3**	**Vendor4**
Estimated Monthly Price	14 000 €	32 000 €	19 000 €	14 000 €
Evaluation Criteria (30%)	24.68 %	17.85 %	22.78 %	24.68 %

The calculation of the 30% Evaluation Criteria for cost are as follows:
Evaluation Criteria (30%) = [1 – (Monthly Price / Total Monthly price for all vendors) * 30]%

Appendix 5: Technical Training Results Table

Use Case		**Vendor1**		**Vendor2**		**Vendor3**	
		Weightage		**Weightage**		**Weightage**	
A	Internal (Private DC)	4	16.00 %	3	12.00 %	3	12.00 %
	Internal (Public Cloud)	4	16.00 %	3	12.00 %	3	12.00 %
	Internal (SaaS)	4	8.00 %	4	8.00 %	3	6.00 %
B	External (Internet)	4	8.00 %	3	6.00 %	3	6.00 %
C	Whitelisting	4	12.00 %	2	6.00 %	4	12.00 %
D	End user Support / Monitor	4	8.00 %	4	8.00 %	2	4.00 %
E	Device Management	3	3.00 %	3	3.00 %	3	3.00 %
G	IGA/IAM Integration	3	3.00 %	3	3.00 %	2	2.00 %
H	Support for Linux	2	2.00 %	3	3.00 %	3	3.00 %
	TOTAL	**32**	**76.00 %**	**28**	**61.00 %**	**26**	**60.00 %**
	Evaluation Criteria (15%)		**11.40%**		**9.15%**		**9.00%**

The calculation of the 15% Evaluation Criteria for technical training are as follows:

Evaluation Criteria (15%) = [(Total) * 15]%

Appendix 6: Evaluation Criteria Table (updated)

Evaluation Criteria	Weightage (%)	Vendor1	Vendor2	Vendor3
1. Cost	30.00 %	24.68 %	17.85 %	22.78 %
2. Proof-of Concept	25.00 %	-	-	-
3. Technical Workshops	15.00 %	11.40 %	9.15 %	9.00 %
4. Troubleshooting Tools	15.00 %	-	-	-
5. Credibility	15.00 %	13.80 %	13.80 %	13.20 %
TOTAL	100.00 %	49.88 %	40.80 %	44.98 %

Appendix 7: Test and Verification Table Results

Tests	Criteria	Task	Test User and Device	Date and Time	User Location	Result		Pass / Fail	Remarks
						Existing VPN Latency (ms)	Vendor1 VPN Latency (ms)		
Test 1	Latency Test	compare VPN between HeDC and Vendor1 for Finland Gateway	Test User1 - Windows	28/06/2023 09.10	Espoo	7	16	Fail	faster average speed for exisitng VPN using ping to sharepoint site
		Finland DC private access (direct for VPN vs. via Azure VWAN path difference + platform difference)	Test User2 - MAC	27/06/2023 14.47	Vantaa	35	84	Fail	User connected to HeDC VPN and Finland VPN
		Access to Azure EU over private path	Test User2 - MAC	27/06/2023 14.47	Vantaa	42	60	Fail	VPN Gateway locations is the reason for high latency in Vendor1
		Access to Azure EU over internet path	Test User2 - MAC	27/06/2023 14.47	Vantaa	47	55	Fail	Vendor1 has higher latency when connected to Finland gateway
		Access to AWS EU over private path	Test User2 - MAC	27/06/2023 14.47	Vantaa	44	115	Fail	Throughput test from user to HeDC jumpx with SFTP upload from user. (Vendor1: 20MB/s -- ExistingVPN:31MB/s)
		Access to AWS EU over internet path	Test User2 - MAC	27/06/2023 14.47	Vantaa	-	-	-	no result. No public IP in AWS to test with. But expect it to be same as public IP in Azure or DC
		Global DNS servers (8.8.8.8)	Test User1 - Windows	28/06/2023 08.10	Espoo	4.33	7	Fail	used global DNS 8.8.8.8 for both; unable to ping Vendor1 DNS
		Performance differences for same than previous if possible	Test User1 - Windows	28/06/2023 09.15	Espoo	-	-	Fail	speed in accessing resources is faster in exisitng VPN (app/systems loading time is faster) -- tested opening a recorded video in Teams
		Video Application experience over browser (a site that gets tunneled via the vpn path (not youtube, netflix))	-	-	-	-	-	Fail	same as above
	user experience with client	Connection establishment time	Test User1 - Windows	28/06/2023 09.30	Espoo	-	-	Pass	Similar results; connects to nearest gateway after successful authentication of user credentials
		Recovery of connectivity from loss of network	Test User1 - Windows	28/06/2023 09.30	Espoo	-	-	Pass	Similar results; tested by disconnecting and reconnecting to wifi
		Recovery of connectivity from loss change of LAN network	Test User1 - Windows	28/06/2023	Espoo	-	-	Pass	Similar results; tested by reconnecting to a mobile hotspot
		Always on feature testing - windows login provided vpn turn on	Test User1 - Windows and MAC	28/06/2023	FI and US	-	-	Pass	Tested "Always-on" with test user devices and works
Test 2	Latency Difference Test	compare VPN between HeDC and Vendor1 for Finland Gateway	Test User1 - Windows	30/06/2023 00.51	Espoo	7.33	6	Pass	faster average speed for Vendor1 using ping to sharepoint site
		Finland DC private access (direct for VPN vs. via Azure VWAN path difference + platform difference)	Test User2 - MAC	28/06/2023 15.45	Vantaa	20	76	Fail	User connected to HeDC VPN and Finland VPN
		Access to Azure EU over private path	Test User2 - MAC	28/06/2023 15.45	Vantaa	45	54	Fail	User connected to HeDC VPN and Finland VPN
		Access to Azure EU over internet path	Test User2 - MAC	28/06/2023 15.45	Vantaa	43	54	Fail	Vendor1 has higher latency when connected to Finland gateway
		Access to AWS EU over private path	Test User2 - MAC	28/06/2023 15.45	Vantaa	44	111	Fail	Throughput test from user to HeDC jumpx with SFTP upload from user. (Vendor1: 23MB/s , ExistingVPN:36MB/s)
		Access to AWS EU over internet path	Test User2 - MAC					-	no result. No public IP in AWS to test with. But expect it to be same as public IP in Azure or DC
		Global DNS servers (8.8.8.8)	Test User1 - Windows	30/06/2023 00.45	Espoo	14.67	9.33	Pass	used global DNS 8.8.8.8 for both; unable to ping Vendor1 DNS
		Performance differences for same than previous if possible	Test User1 - Windows	30/06/2023 01.00	Espoo	-	-	Pass	speed in accessing resources is faster in Vendor1 (app/systems loading time is faster) -- tested opening a recorded video in Teams
		Video Application experience over browser [a site that gets tunneled via the vpn path (not youtube, netflix)]	-	-	-	-	-	Pass	same as above
	user experience with client	Connection establishment time	Test User1 - Windows	30/06/2023 01.03	Espoo	18	5	Pass	Similar results; connects to nearest gateway after successful authentication of user credentials
		Recovery of connectivity from loss of network	Test User1 - Windows	30/06/2023 01.05	Espoo	18	5	Pass	Vendor1 recovered back faster than existing VPN after wifi was turned off and on
		Recovery of connectivity from loss change of LAN network	Test User1 - Windows	30/06/2023 01.10	Espoo	7	6	Pass	Vendor1 reconnected back faster than existing VPN after reconnected to new wifi SSID.
		Always on feature testing - windows login provided vpn turn on	Test User1 - Windows and MAC	28/06/2023	FI and US	-	-	Pass	Tested "Always-on" with test user devices and works

Appendix 8: RACI Matrices

Service Request						
Steps	**Activities**	**End User**	**IT Ops**	**ITNS**	**NOC**	**Vendor**
1	Raise a request ticket to ITOps	A/R	I/C			
2	Receive Service Request	I	A/R			
3	Request Validation	I	A/R	C	C	
4	Request Fulfillment	I	A/R	C	C	
5	Perform Verification with User	R	A			
6	Close request ticket once resolved	I	A/R			

Incident Management (Proactive)					
Steps	**Activities**	**IT Ops**	**ITNS**	**NOC**	**Vendor**
1	Check Email Alerts	A/R	C/I	C/I	
2	Raise an incident ticket	A/R	C/I	C/I	
3	Validate and Troubleshoot (Tshoot)	A/R	C/I	C/I	
If VPN Gateway Related:					
4	Validate and Tshoot	A/R	C/I	I	
5	Engage Vendor for Tshoot/Support	A/R	C/I	I	I
6	Vendor Support	R	R	I	A/R
7	Perform verification	A/R	R	I	R
8	Close incident ticket once resolved	A/R	R	I	I
If Connection to Data Center Related:					
9	Escalate to ITNS	A/R	R/C	I	
10	ITNS Validate and Tshoot	I	A/R	C/I	
11	Engage Vendor for Tshoot/Support	I	A/R	C/I	C/I
12	Vendor Support	R	R	I	A/R
13	Perform verification	A/R	R	I	R
14	Close incident ticket once resolved	A/R	R	I	I
If Cloud Networks Related:					
15	Escalate to NOC	A/R	C/I	R	
16	NOC Validate and Tshoot	I	C/I	A/R	
17	Engage Vendor for Tshoot / Support	I	C/I	A/R	C/I
18	Vendor Support	I	I	R	A/R
19	Perform verification	R	R	A/R	R
20	Close incident ticket once resolved	A/R	I	I	I

Incident Management (Reactive)						
Steps	**Activities**	**End User**	**IT Ops**	**ITNS**	**NOC**	**Vendor**
1	Report incident thru #help-it	A/R	I			
2	Validate and Tshoot	I	A/R	C	I	
If VPN Gateway Related:						
3	Validate and Tshoot	I	A/R	C/I	I	
4	Engage Vendor for Tshoot/Support	I	A/R	C/I	I	I
5	Vendor Support	I	R	R	I	A/R
6	Perform verification	A/R	R	R	I	R
7	Close incident ticket once resolved	I	A/R	R	I	I
If Connection to Data Center Related:						
8	Escalate to ITNS	I	A/R	R/C	I	
9	ITNS Validate and Troubleshoot	I	I	A/R	C/I	
10	Engage Vendor for Tshoot /Support	I	I	A/R	C/I	C/I
11	Vendor Support	I	R	R	I	A/R
12	Perform verification	I	R	A/R	R	R
13	Close incident ticket once resolved	I	A/R	R	I	I
If Cloud Networks Related:						
14	Escalate to NOC	I	A/R	R/C	I	
15	NOC Validate and Tshoot	I	I	R	A/R	
16	Engage Vendor for Tshoot / Support	I	I	R	A/R	I
17	Vendor Support	I	I	R	R	A/R
18	Perform verification	I	R	R	A/R	R
19	Close incident ticket once resolved	I	A/R	I	I	I

Change Management						
Steps	**Activities**	**End User**	**IT Ops**	**ITNS**	**NOC**	**CAB**
1	Raise a request ticket in IT Operations	A/R	I/C			
2	Receive Change Request	I	A/R			
3	Review Change Request		A/R	C		
For Standard Change						
4	Validate Change Request	I	R	A/R	C	
5	Implement Change	I	A/R	C/I	C/I	
6	Perform Verification with User	R	A/R	C/I	C/I	
7	Close request ticket once resolved	I	A/R	I	I	
For Normal Change						
8	Validate Change Request	I	R	A/R	C	
9	Prepare Change Plan (VPN)	I	I	A/R	C/I	
10	Prepare Change Plan (Private / Public DC Networks)	I	I	R/C/I	A/R	
11	Review, Validate and Approve	I	I	R	R	R/A/C
12	Implement Change (VPN)	I	R/I	A/R	C/I	I
13	Implement Change (Private / Public DC Networks)	I	I	C/I	A/R	I
14	Perform Verification with User	R	A/R	C/I	C/I	
15	Close request ticket once resolved	I	A/R	I	I	
For Emergency Change						
16	Validate Change Request	I	A/R	R/C/I	R/C/I	
17	Raise Incident Ticket	I	A/R	I	I	
18	Implement Change (VPN - Simple)	I	A/R	C/I	I	
19	Implement Change (VPN - Complex)	I	R/I	A/R	C/I	
20	Implement Change (Private / Public DC Networks)	I	I	C/I	A/R	
21	Perform Verification with User	R	A/R	C/I	C/I	
22	Close request and incident ticket once resolved	I	A/R	I	I	

Platform Upgrade (VPN Infrastructure)				
Steps	**Activities**	**End User**	**Company ABZ**	**Vendor**
For Proactive Upgrades				
1	Upgrade Notification in email		I	A/R
2	Inform Users (not necessary)	I	R/A	C
For Reactive Upgrades				
1	Incident Creation to Vendor (refer to Incident Management)		R/A	C/I
2	Review, tshoot and decide that platform upgrade is required		C/I	R/A
3	Prepare upgrade plan and share		I	R/A/C
4	Perform the upgrade as per agreed schedule		I	R/A/C
5	Update status and results		I	R/A/C
6	Test and verify	I	R/A	C
7	Close ticket once resolved	I	A/C	R