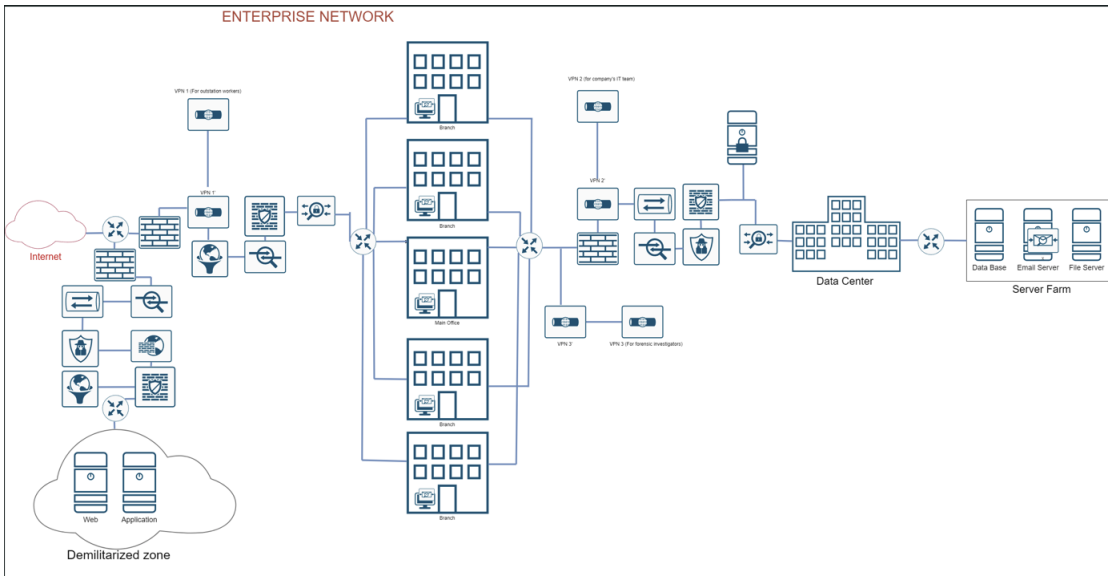
Name: Teh Jia Xuan	Student ID: 32844700
Assignment 1 – IT Forensics 2023	

Network Diagram



1) Server Farm Location, WAN connections, and Internet connection

Hybrid mode is used for server farm location. Web and Application servers are put on cloud, whereas DataBase, Email and File Servers are placed in data centre. Using cloud as Demilitarized Zone(DMZ) provides benefits to digital forensics(DF). Cloud quickly offers resources like storage space and computation power for processing high-volume data(Delvadiya, 2023). DF could solve cases swiftly with such resources. When DF needs resources to investigate as cloud minimises hardware costs(CADO,2023). Furthermore, DF investigations via cloud could minimize business interruptions.

DataBase, Email and file servers contain sensitive data. Hence, it is placed in Data Center instead of cloud due to security concerns as cloud is a third-party company. Additional, Data Center is company's property, it has surveillance cameras and biometric authentication(CISCO, n.d.). This prevents unauthorised access and information loss. Securing data ensures forensic readiness, as it preserves data integrity for analysis. Failure to preserve digital evidence, it cannot be presented in a court of law.

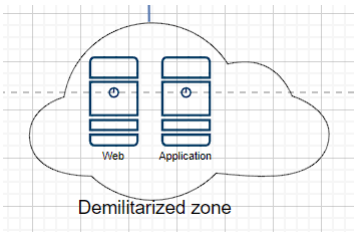


Figure 1.1

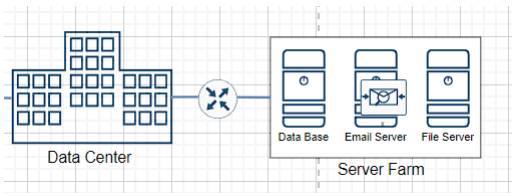


Figure 1.2

Wide Area Network (WAN) connection will use MPLS. MPLS offers a faster and secure network environment (Paloalto, n.d.). Large organisations should prioritise networks to ensure task completion for workers and forensic investigators(FI). Besides that, FI handles massive data, faster data transmission leads to faster analysis.

Multiple protocol label switching(MPLS) connected the internet to router to route to internal network and public servers in cloud. Furthermore, branches and main office are connected to router using MPLS to route to data center which contains all the private servers.

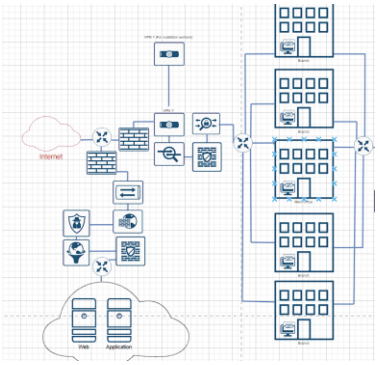


Figure 1.3

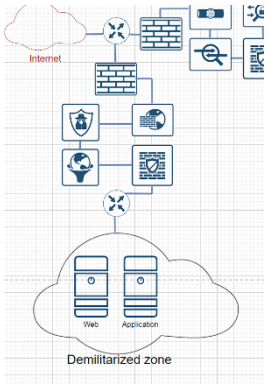


Figure 1.4

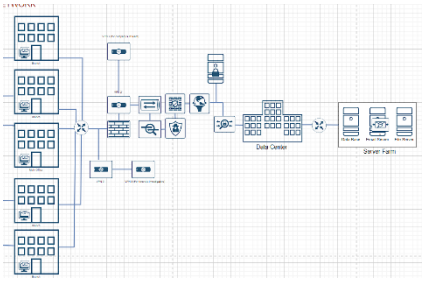


Figure 1.5

2) Authentication, Authorizing, Accounting (AAA) server location, Security information and event management (SIEM) server location, Virtual Private Network(VPN), Secure Socket Layer (SSL) Terminator, and Firewall

AAA server is placed before internal network and data center for controlled access and security. An AAA server ensures data access based on roles. It prevents unauthorised access and limits information exposure. For forensic readiness, AAA server collects valuable data like login attempts. This data is crucial for FI to trace unauthorized access timelines. Moreover, AAA server logs serve as digital evidence, as it records suspicious activity comprehensively

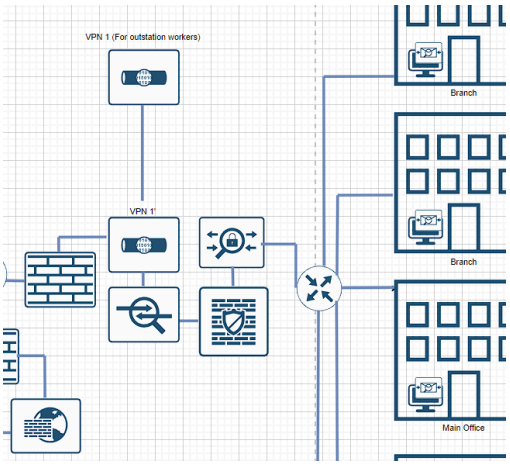


Figure 2.1

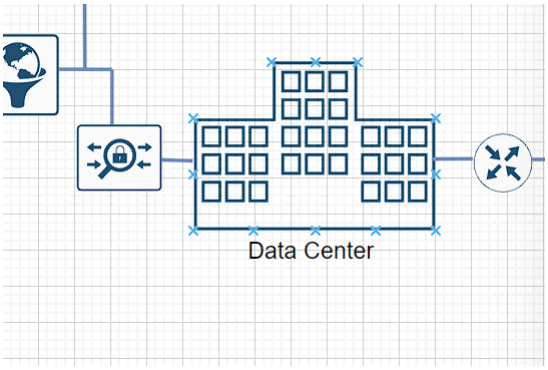


Figure 2.2

SIEM server is placed before entering data center, SIEM enables real-time traffic monitoring and records traffics for future purposes. Moreover, SIEM analyze traffic for signs of malicious activity (Scarfone, 2018). This able to protect data center from any early potential threats. SIEM server benefits FI, during investigations SIEM provides complete history of traffic. This enables FI to reconstruct attack timeline and understand attacker's motive.

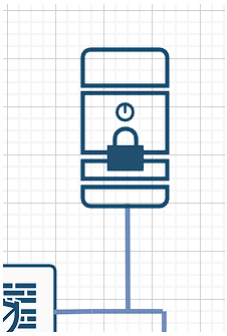


Figure 2.3

VPN provides encrypted tunnels for secure connection with all data transmitted encrypted(cloudflare,n.d.). This enables workers to connect internal networks in public safely. VPN are placed at 3 locations. First is before internal network, facilitating secure connections for outstation workers to access their branch resources. Second before data center is for company's IT team. It provides extra layer of security while connecting to data center. The third VPN is for the FI, FI can access server data through VPN and AAA server. This ensures FI's activities don't interrupt business operations. Additionally, VPN can limit investigators' data access(Meraki, 2022). This reduces investigators encountering unrelated or secret data like upcoming products and company strategies.

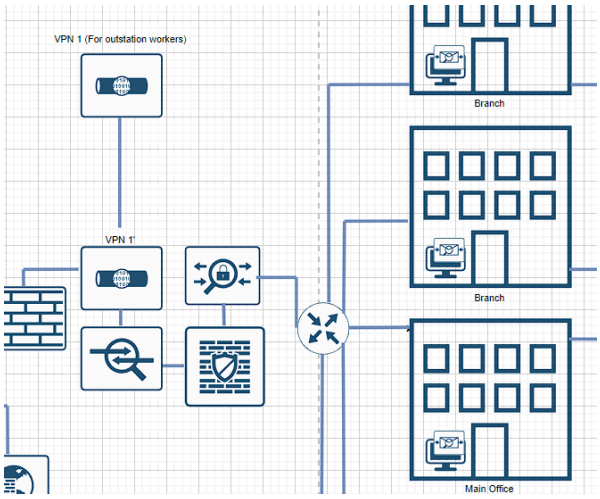


Figure 2.4

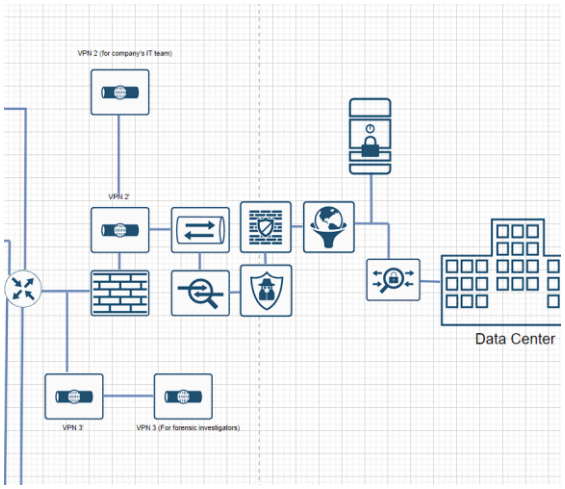


Figure 2.5

SSL terminator is placed before entering cloud and data center (Figure 2.5). SSL terminator is used to decrypt incoming packets before sends to servers(f5, n.d.). Moreover, it reduces load of server and speeds up communication process which enhances response time for user (Docs, 2023). In forensic readiness, SSL terminator provides traffic visibility and saves time for FI as they don't need to decrypt data. Additionally, decrypted traffic enables investigators to understand the communication details.

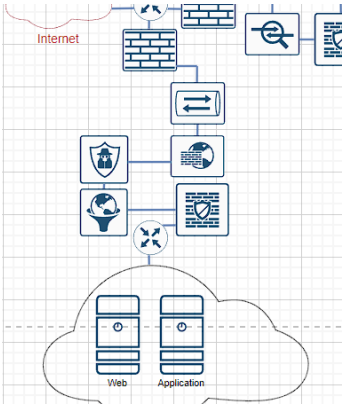


Figure 2.6

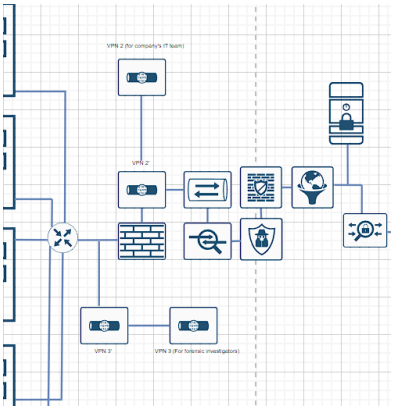


Figure 2.7

Firewall is placed before entering the company, cloud and data center. Firewall acts as first-line defence where it filters incoming packets using security policies(Al-Shaer & Hamed,2004). Firewalls enable FI to gather information from logs like IP addresses, to find the root of crime(ManageEngine,n.d.). Firewalls provide comprehensive traffic activities that occurred before and after incident so it is convenient for investigators to investigate and speed up case progress. Hence, firewalls are prepared for any malicious activities.

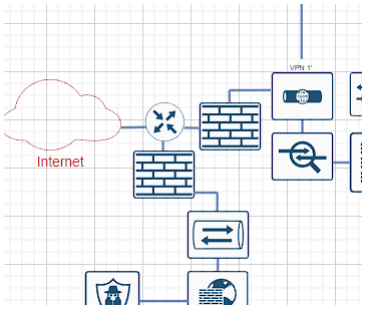


Figure 2.8

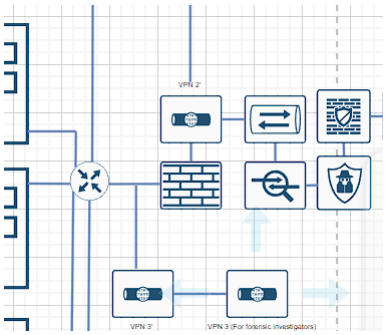


Figure 2.9

3) Enterprise Defence System

Web Application Firewall(WAF) is placed before entering the cloud, it is used to protect web applications from online attacks. Its main function is filter malicious traffic according to security policies. Organisations can modify policy to prevent attacks like DDoS(cloudflare,n.d.). WAF provides logs for detected attacks with information like source IP(aws, n.d.). This is useful for forensic analyses, as it can serve as digital evidence in a court of law.

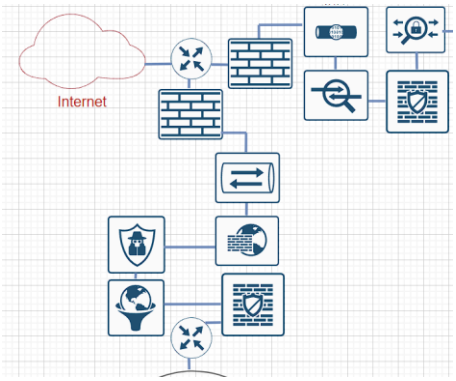


Figure 3.1

Web filtering restricts user content access. This system aims to protect users from harmful internet content(Chen&Wang,2010). Therefore, it is placed before cloud and internal network. Preventing users accessing malicious websites can prevent internal network getting harm. Data stored in servers are important for investigation, as web filtering protects data being contaminated. Furthermore, during investigations, massive data is stored in servers and clouds, so web filtering can prevent destruction of analysed data.

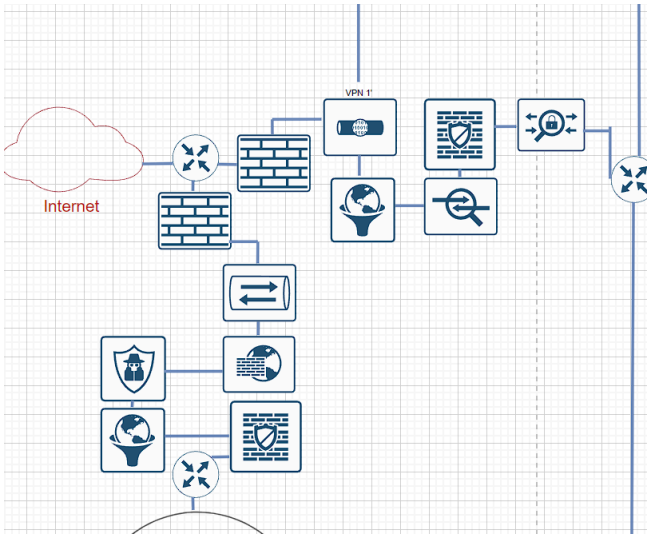


Figure 3.2

Malware filtering is to block malicious software and potential cyber-attacks(EC,2020). Hence it is placed before entering cloud, company and data center. This protects our internal network and cloud from malware. Furthermore, it preserves data integrity so it ensures evidence remains valid and able to present in court.

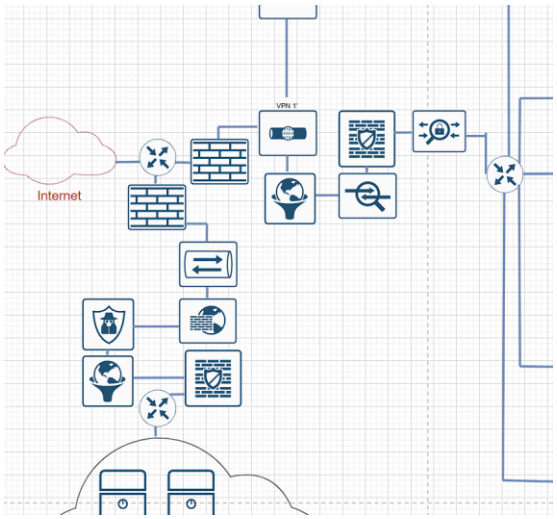


Figure 3.3

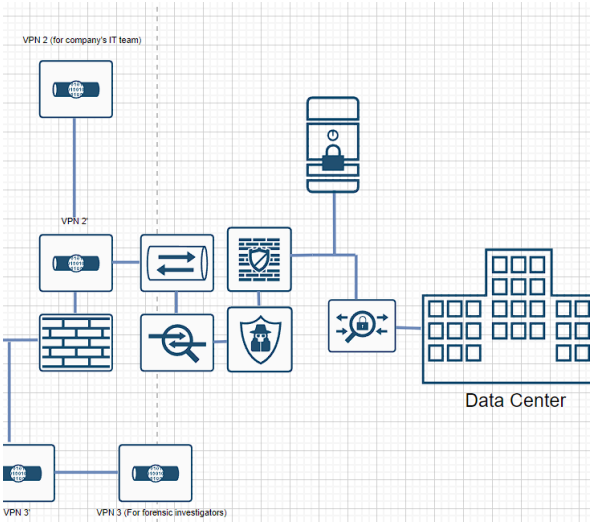


Figure 3.4

SSL inspection is used to decrypt and analyse packets, it scans for malware. Thus, it is placed before cloud and data center to ensure every packet sent to server is filtered. It prevents any malicious packet interact with servers and modify data, as protecting data integrity is important for forensic readiness and reputation. When data is modified or timeline does not match, it cannot be presented in court of law.

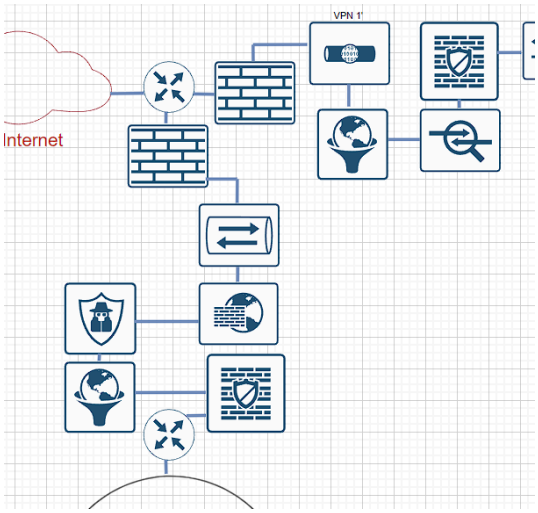


Figure 3.5

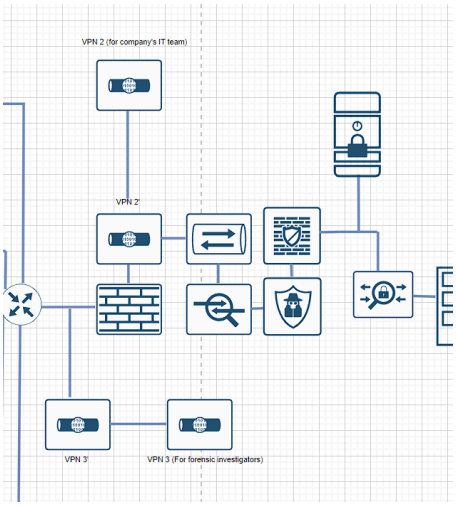


Figure 3.6

IDS/IPS identifies and reacts to malicious activity. IDS monitors network for suspicious activity whereas IPS acts on it(VMware, n.d.). IPS detects, filters and reports malicious traffic to IT team. IPS enables customized security policies to block packets (VMware, n.d.). For forensic readiness, it helps investigators by identifying cybercriminals' techniques as IPS will report. This insight can assist FI to solve cases more efficiently. Therefore, it places before internal network, data center and cloud as malicious packets cause security crises and business interruptions

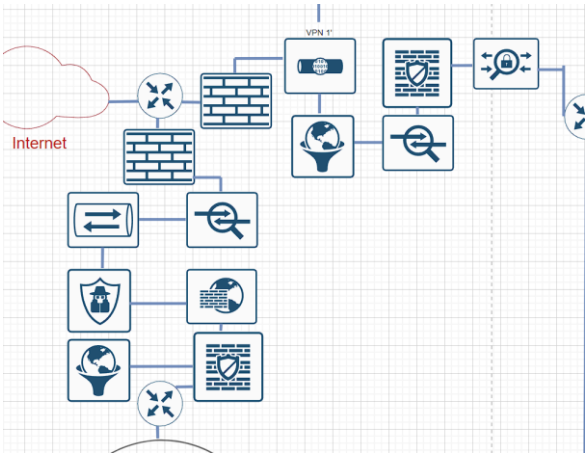


Figure 3.7

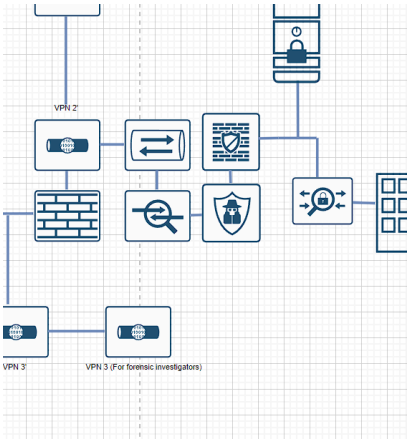


Figure 3.8

Email security is placed on email servers and workstations to ensure confidentiality, authenticity and integrity of email communications by encrypting and signing emails(Mimecast, 2023). Moreover, it blocks phishing and ransomware emails which is crucial for employees. According to Microsoft(n.d.), employee receives 120 emails daily. Cybercriminals has opportunity to attack using phishing emails. One click causes security crisis to organization. Additionally, it enhances forensic readiness by ensuring integrity and authenticity of email. As Email forensics is analysing the content of emails to crack crimes (SalvationData, 2022).

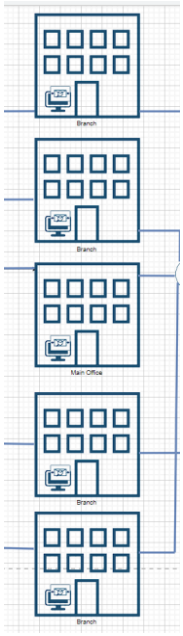


Figure 3.9

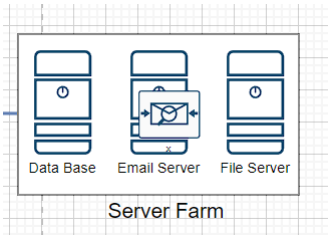


Figure 4.0

4) Cost Estimation and Justification

All with "~" symbol is taking lower bound plus upper bound divide by 2

Equipment	Cost (one-time payment)	Maintenance/cost per year	Maintenance/cost per 10 years	Total (10 years estimation)
SIEM server	Software: $20,000-$1,000,000 = ~$300,000 Implementation: $50,000 Hardware: $25,000-75,000 = ~$40,000 Infrastructure: $10,000 Total = $400,000 (Buchanan, 2022)	Maintenance: $5,000-$10,000 per month = $5000-$10000*12 = $60,000-$120,000 (Foster, 2022)	Maintenance 10 years: $600,000-$1,200,000 = ~$900,000 Replacement (every 5 years): $400,000*2 = $800,000	$900,000 + $800,000 = $1,700,000
Firewall	Equipment purchase $5,000, installation $1,600 (self-estimation)	Maintenance: $1000-$2000 (vc3,2022)	Replacement (every 5 years) (RMON, n.d.): $6600 * 2 = $13,200 Maintenance 10 years: $10,000-$20,000 = ~$15,000	$13,200 + $15,000 = $28,200 Total 3 Firewalls = $28,200 * 3 = $84,600
Web Server (Cloud)		Azure Subscription: $313 per month *12 = $3,756 (Sirius, n.d.)	Azure Subscription 10 years: $3,756 * 10 = $37,560	$37560
Application (Cloud)		Azure Subscription: $313 per month *12 = $3,756 (Sirius, n.d.)	Azure Subscription 10 years: $3756 * 10 = $37,560	$37560

Workstation	Equipment Purchase: $1,800-$5,000 (Self-Estimation)	Maintenance: $90 per year (Checkatrade, 2023)	Replacement (every 5 years): $1,800-$5,000 * 2 = $3,600-$10,000 = ~$6800 Maintenance 10 years: $90*10 = $900	$6,800+$900 = $7,700 Total 200 workstation = $7,700 * 200 = $1,540,000
Data center	Building overall Estimation (including, installation etc) $2,300,000 (SecureIT, n.d.)	Maintenance: 10,000,000 (siteltd, n.d.)	Maintenance 10 years: $100,000,000	$2,300,000+$100,000,000 = $102,300,000
Data Base	Equipment Purchase: $40,000 Installation: $2,000 OS License: $1000 (Insider, 2011)	Maintenance: $5,435 (Microsoft, 2019)	Replacement (every 5 years): ($40,000 + $2000 + $1000)*2 = $86,000 Add 2000TB storage(every 5 years): $20,000 *2 = $40,000 (Self-estimation) Maintenance 10 years: $5,435*10 = $54,350	$86,000 + $54,350 + $40,000 = $180,350
Email server	Equipment purchase: $70,000 Installation: $2,000 (Self-Estimation)	Maintenance: $500-$1,000 (Self-Estimation)	Replacement (every 5 years): ($70,000 + $2000) * 2= $144,000 Add 200TB storage(every 5 years): $15,000 *2 = $30,000 (Self-estimation) Maintenance 10 years: $5,000-$10,000 = ~$7,500	$144,000 + $30,000 + $7,500 = $181,500
File server	Equipment purchase: $5,000-$20,000	Maintenance: $150-$1500 per month *12 = $1,800-$18,000	Replacement (every 5 years): ($5,000 -$20,000 + $2,000) * 2	$29,000 + $99,000 + $40,000 = $168,000

	Installation: $2,000 (Mindanao, 2023)	(Self-Estimation)	$14,000-$44,000= ~$29,000 Add 2,000TB storage(every 5 years): $20,000 *2 = $40,000 (Self-estimation) Maintenance 10 years: $18,000-$180,000 = ~$99,000	
Router	Equipment purchase: $1,217 (officework, 2023)		Replacement (every 5 years): $1,217*2 = $2,434	$2,434 Total 5 routers = $2,434 * 5 = $12,170
AAA server	Equipment purchase: $30,000 Installation: $2,000 (Self-Estimation)	Maintenance: $1500 per month *12 = $18,000 (Self-Estimation)	Replacement (every 5 years): ($30,000 + $2000)*2 = $60,000 Maintenance 10 years: $180,000	$60,000 + $180,000 = $240,000 Total 2 AAA server = $240,000 * 2 = $480,000
SSL terminator	Equipment purchase: $1,500-$5,000 Installation: $1,200 (Self-Estimation)	Maintenance: $200-$1000 (Self-Estimation)	Replacement (every 5 years): ($1,500-$5,000 + $1,200)*2 = $5,400-12,400 = $8,900 Maintenance 10 years: $2,000-$10,000 = $6,000	$8,900 + $6,000 = $14,900 Total 2 SSL terminator: $14,900 * 2 = $29,800
MPLS		Subscription: $750-$1,000 per month * 12 = $9,000-$12,000 (mushroom, n.d.)	Subscription 10 years: $9,000-$12,000 * 10 =$90,000-$120,000 = $105,000	$105,000
VPN		Subscription: $13 per month * 12 = $156	Subscription 10 years: $156*10 = $1,560	$312,000 Total 3 VPN = $312,000 * 3 = $936,000

		Total 200 workstations: $156 * 200 = $31,200 (Hann & Livingston , 2023	Total 200 workstations: $31,200*10 = $312,000	
Web Application Firewall		Subscription: $327.04 per month * 12 = $3,888.48 (Microsoft, 2023)	Subscription 10 years: $3,888.48*10 $38,884.8	$38,884.8
Web filtering		Subscription: $2.20 per month *12 = $26.4 Total 200 workstations = $26.4*200 = $5,280 (g2, n.d.)	Subscription 10 years: $26.4 * 10 = $264 Total 200 workstations = $264 * 200 = $52,800	$52,800 Total 2 web filtering: $52800 * 2 =$105,600
Malware filtering		Subscription: $45 Total 200 workstations = $45 * 200 = $90,000 (Croft & McNally, 2023)	Subscription 10 years: $90,000*10 = $900,000	$900,000 Total 3 Malware Filtering: $900,000 * 3 = $2,700,000
SSL inspection	Equipment purchase: $995 (SonicGuard, 2023)	Maintenance: $500 (Self-Estimation)	Replacement (every 5 years): $995*2 = $1,990 Maintenance 10 years: $5,000	$1,990 + $5,000 = $6,990 Total 2 SSL inspection: $6,990 * 2 = $13980
IDS/IPS	Equipment purchase: $9,800 - $90,000 Installation: $1,500 (Ingalls, 2023)	Maintenance: $1250-$9,250 (self-estimation)	Replacement (every 5 years): ($9,800-$90,000 +$1,500)* 2 = $22,600 - $183,000 = $102,800 Maintenance 10 years: $12,500-$92,500 = $52,500	$102,800 + $52,500 = $155,300 Total 3 IDS/IPS: $155,300 * 3 = $465,900
Email security		Subscription:$1.08 per user per month	Subscription 10 years: $2604.96 * 10 = $26049.60	$26049.60

		Total 200 workstation and 1 server = $1.08*201 = $217.08 $217.08*12 = $2604.96 (TitanHQ, 2021)		
Internet Connection		Subscription: $550 per month * 12 = $6,600 (Hurricane, 2023)	Subscription 10 years: $66,000	$66,000
Branch/Main office	Land cost: $930,000 Construction cost: $1,500,000 Facilities cost: $500,000 Professional Installation: $30,000 (Reider, 2016)			$930,000 + $1,500,000 + $500,000 + $30,000 = $2,960,000 Total 5 Branches including Main Office $2,960,000 * 5 = $14,800,000
				Total = $126,008,954.40

References

ABABankingJournal (2016, October 25). Branch Costs and Size Are Changing. Retrieved from, https://bankingjournal.aba.com/2016/10/branch-costs-and-size-are-changing/

AceCloud(2022, August 18). Managed SIEM Pricing That You Should Know. Retrieved from, https://www.acecloudhosting.com/blog/managed-siem-pricing/

AWS (n.d.) Logging AWS WAF web ACL traffic. Retrieved from, https://docs.aws.amazon.com/waf/latest/developerguide/logging.html

Azure (n.d.). Web Application Firewall pricing. Retrieved from, https://azure.microsoft.com/en-au/pricing/details/web-application-firewall/

CADO (2023, June 6) Forensic Readiness in the cloud. Retrieved from, https://www.cadosecurity.com/forensic-readiness-in-the-cloud/

Cisco (n.d.). AAA server. Retrieved from, https://itprice.com/cisco-gpl/aaa%20server

Cloudflare (n.d.) VPN security: How VPNs help secure data and control access. Retrieved from, https://www.cloudflare.com/learning/access-management/vpn-security/

Cloudflare. (n.d.). What is a WAF? | web application firewall explained |. Retrieved from, https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Croft &McNally (2023, May 23). Malwarebytes Antivirus Review 2023: Is It Worth the Hype? Retrieved from https://allaboutcookies.org/malwarebytes-review#:~:text=Malwarebytes%20cost,-You%20can%20get&text=Premium's%20starting%20cost%20for%20one,%2459.99%20that%20covers%20three%20devices.

Delvadiya (2023, March 14) Impact of Cloud Computing on Digital Forensic. Retrieved from, https://www.tutorialspoint.com/impact-of-cloud-computing-on-digital-forensic#:~:text=There%20are%20many%20advantages%20of,solve%20the%20cases%20more%20quickly.

Docs (2023, July 7) SSL Termination. Retrieved from, https://docs.digitalocean.com/glossary/ssl-termination/

E. S. Al-Shaer and H. H. Hamed, "Modeling and Management of Firewall Policies," in IEEE Transactions on Network and Service Management, vol. 1, no. 1, pp. 2-10, April 2004, doi: 10.1109/TNSM.2004.4623689.

EC (2020, March 12). How Malware Filtering Works. Retrieved from, https://ecmanagedit.com/how-malware-filtering-works/

EC Managed IT. (2023, July 26) *How malware filtering works*. Retrieved from, https://ecmanagedit.com/how-malware-filtering-works/

F5 (n.d.) What is SSL Termination. Retrieved from, https://www.f5.com/glossary/ssl-termination

G2 (2023). SafeDNS web content filtering service. Retrieved from, https://www.g2.com/products/safedns-web-content-filtering-service/pricing

Haan & Livingstron (2023, July 30). Best Business VPN of 2023. Retrieved from, https://www.forbes.com/advisor/business/software/best-business-vpn/

Hurricane (2023). IP Transit. Retrieved from, https://he.net/ip_transit.html?p=&t=&m=p&k=internet%20network&gclid=Cj0KCQjwrfymBhCTARIsADXTabkO0VBa6FZ4nIGc7P4gdyrTR7AzwWRY58j2TCA2-fobjtz_ehr_nm0aAvxrEALw_wcB

Ingalls (2023, January 23). 13 Best Intrusion Detection and Prevention systems (IDPS) for 2023. Retrieved from, https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/

Insider (2011, November 30) 3 Costs Hiding in Your Database. Retrieved from, https://www.businessinsider.com/3-costs-hiding-in-your-database-2011-11#:~:text=Data%20Maintenance,it%20with%20your%20own%20software.

ManageEngine (n.d.) Firewall Analyzer. Retrieved from, https://www.manageengine.com/products/firewall/forensic-log-analysis.html

Microsoft (n.d.). How to license SQL Server. Retrieved from, https://www.microsoft.com/en-us/sql-server/sql-server-2019-pricing

Microsoft (n.d.). What is email security? Retrieved from, https://www.microsoft.com/en-za/security/business/security-101/what-is-email-security#:~:text=Email%20security%20is%20the%20practice,access%2C%20loss%2C%20or%20compromise.

Mindanao (2023, August 2). How Much Does a Server Cost in 2023? Retrieved from, https://www.itsasap.com/blog/server-cost#:~:text=The%20cost%20of%20servers%20can,be%20replaced%20after%20five%20years.

Mushroom(n.d.) What is the Cost of MPLS Network? Retrieved from, https://www.mushroomnetworks.com/blog/what-is-the-cost-of-mpls/#:~:text=MPLS%20Rates%20Compared&text=For%20example%2C%20in%20the%20United,for%20standard%20Broadband%20Internet%20lines.

Paloato (n.d.) SD-WAN vs MPLS vs Internet: What's the Difference? Which is Right for Your Organization? Retrieved from, https://www.paloaltonetworks.com/cyberpedia/sd-wan-vs-mpls-vs-internet

SalvationData(2022, September 13). Email Forensics- Definition and Guideline. Retrieved from, https://www.salvationdata.com/knowledge/email-forensics-definition-and-guideline/#:~:text=Email%20forensics%20refers%20to%20analyzing,and%20incidents%20involves%20various%20approaches.

Sirus (n.d.). How much does a cloud server cost for a small business? Retrieved from, https://siriusofficesolutions.com/cloud-server-price/#:~:text=The%20average%20cloud%20server%20costs,on%20your%20IT%20infrastructure%20costs.

Siteltd (n.d.). What Does it Cost to Build a Data Centre? Retrieved from, https://siteltd.co.uk/blog/what-does-it-cost-to-build-a-data-centre/#:~:text=Data%20Centre%20Cost&text=While%20some%20factors%20influence%20annual,and%20%2425%20million%20per%20year.

SonicGuard (n.d.). SonicWall Deep Packet Inspection of SSL/TLS Encrypted Traffic (DPI-SSL) Licenses, Subscription & Renewals. Retrieved from, https://www.sonicguard.com/Deep-Packet-Inspection.asp

T. M. Chen and V. Wang, "Web Filtering and Censoring," in *Computer*, vol. 43, no. 3, pp. 94-97, March 2010, doi: 10.1109/MC.2010.84.

TitanHQ (n.d.). Email Security Pricing Comparison. Retrieved from, https://www.titanhq.com/email-security-solution-pricing-guide/

Vc3 (2022, October 6). What is a Managed Firewall and How Much Does It Cost? Retrieved from, https://www.vc3.com/blog/managed-firewall-cost

Vmware (n.d). What is an intrusion prevention system? Retrieved from, https://www.vmware.com/in/topics/glossary/content/intrusion-prevention-system.html#:~:text=What%20is%20an%20intrusion%20prevention,it%2C%20when%20it%20does%20occur.

Whitfield (2023, July 19). How Much Does it Cost to Host a Website? Retrieved from, https://www.websitebuilderexpert.com/web-hosting/cost-to-host-a-website/#:~:text=You%20are%20able%20to%20get,is%20going%20to%20cost%20you.