8/22/2025

Enterprise Network Planning

FIT3168 – A1: Forensic Readiness

Param Dave
33586047

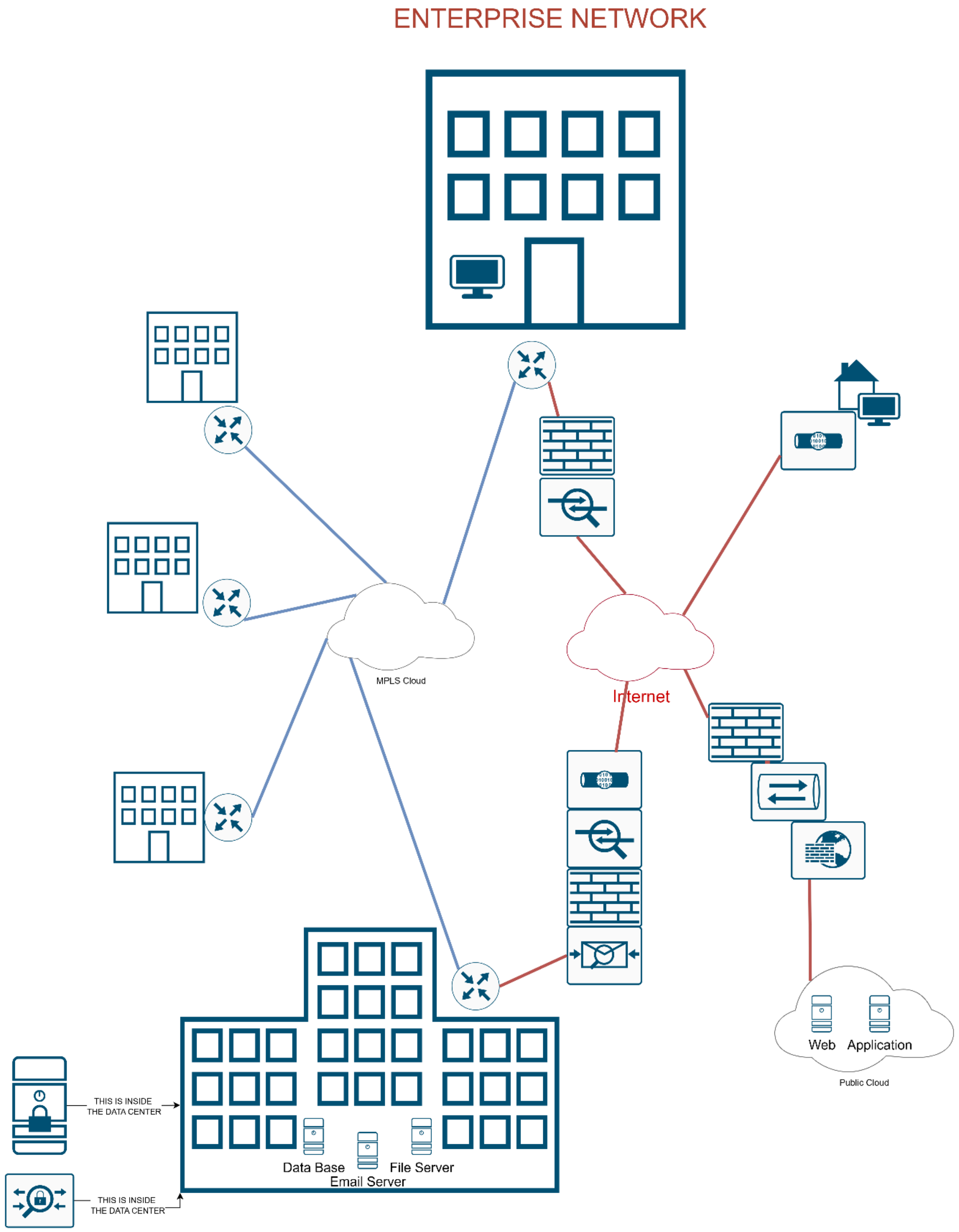
Table of Contents

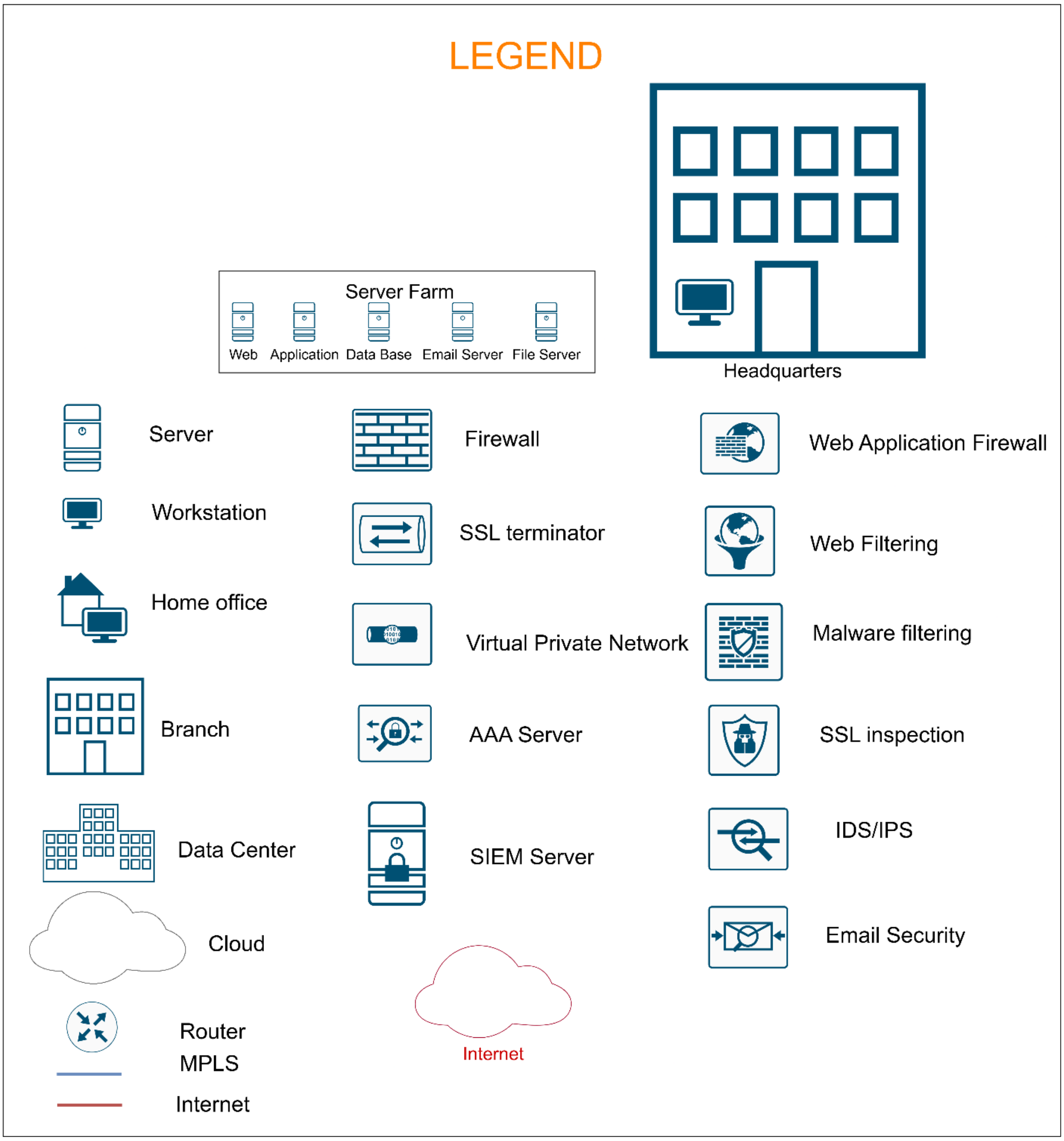
Enterprise Network Diagram:

Student ID: **33586047**

Number of Branches: **1 + 3**

WFH: **Yes**




LEGEND
Server Farm
Web
Application
Data Base
Email Server
File Server
Headquarters
Server
Firewall
Web Application Firewall
Workstation
SSL terminator
Web Filtering
Home office
Virtual Private Network
Malware filtering
Branch
AAA Server
SSL inspection
Data Center
SIEM Server
IDS/IPS
Cloud
Email Security
Internet
Router
MPLS
Internet

Introduction

This report proposes a secure and forensic-ready network design capable of supporting 160 employees across a headquarter, three branch offices (national and international), and work-from-home (WFH) users.

The goal is to ensure the infrastructure remains sustainable for 10 years, while embedding forensic readiness in line with ISO/IEC 27043:2015, which defines guidelines for preparing, collecting, and preserving digital evidence efficiently. According to ISO/IEC 27043, forensic readiness involves building logging, monitoring, and evidence preservation directly into the infrastructure, thereby reducing investigation costs and improving resilience to cyber incidents (ISO, 2015).

The following sections justify the server, WAN, and defence design choices, explain placement of core security devices, evaluate enterprise defence tools, and estimate costs proportionate to an Australian IT company of this size.

NOTE: All costs are calculated in **AUD.**

Server Farm and WAN Choices

Hybrid Server Farm

The design adopts a **hybrid model**:

- **Private Data Centre** (company-owned) hosting: Database server, File server, Email server, AAA server, and SIEM.
- **Public Cloud** hosting: Application/Web server.

This choice balances control and scalability. Sensitive information such as databases and emails remain in a controlled environment, ensuring forensic artefacts like logs, access trails, and system images remain under company custody. ISO/IEC 27043:2015 stresses the importance of controlling evidence sources (Clause 7.2.2), which is best achieved in a private environment (ISO, 2015).

Meanwhile, web applications must scale to client demand and remain publicly accessible. Hosting these in the cloud provides elasticity, geographic redundancy, and distributed denial-of-service (DDoS) resilience that a private data centre cannot match cost-effectively (Telstra, n.d.).

Why not other options?

- **All on-premise (HQ/DC):** Expensive to scale, single point of failure, difficult to guarantee uptime.
- **All public cloud:** Reduces control of forensic artefacts and risks vendor lock-in (Academia.edu, 2016).
- **HQ-only servers:** Creates performance bottlenecks for branches and complicates forensic evidence centralisation.

Thus, the hybrid model ensures sensitive data remains private while still leveraging cloud for scalability and cost savings.

Hybrid WAN (MPLS + Internet)

The WAN uses a combination of MPLS and Internet links:

- **MPLS** interconnects HQ, branches, and Data Centre, offering secure, low-latency traffic with built-in service level agreements (SLAs).
- **Internet** provides external access, WFH connectivity via VPN, and redundancy.

This dual approach ensures continuity: if MPLS suffers disruption, critical operations can fall back on Internet VPNs. From a forensic standpoint, MPLS guarantees consistent traffic paths, making evidence such as NetFlow logs easier to correlate (Telstra, n.d.). Internet access, meanwhile, requires additional logging (VPN, Firewall) but provides flexibility.

Why not MPLS only? Costly over 10 years and poor support for cloud/SaaS access. **Why not Internet only?** Insufficient reliability and QoS for an enterprise with international branches.

The hybrid WAN therefore delivers both operational resilience and forensic visibility across diverse traffic sources.

Core Security Components

AAA Server (Data Centre)

The **AAA** server is located in the private Data Centre to centralise identity management.

- **Justification:** Logs every login, authentication attempt, and privilege change across HQ and branches. Forensic readiness is enhanced by correlating AAA logs with SIEM events to identify insider threats (Academia.edu, n.d.).
- **Why not branch-level AAA?** Having security servers in different locations complicates evidence collection and increases attack surface.

SIEM Server (Data Centre)

A SIEM server aggregates logs from Firewalls, VPN, AAA, and all the servers including the ones in cloud services and is also located in the private Data Centre.

- **Justification:** Correlation of events across systems aligns with ISO/IEC 27043 principles of efficient evidence collection (Clause 7.2.4). The Data Centre location ensures integrity and central storage (ISO, 2015).
- **Why not cloud SIEM?** Higher ongoing licensing costs and potential data residency issues.

Firewalls

Dedicated firewalls are placed at the perimeter of HQ, Data Centre, and Cloud segments.

- **Justification:** Each firewall generates audit logs of denied and permitted traffic, which are vital forensic artefacts in intrusion cases. Placement ensures all ingress/egress traffic is controlled and logged (Academia.edu, 2016).
- **Why not consolidate to HQ firewall only?** Would leave Cloud and DC vulnerable and fragment evidence trails.

VPN Gateway

VPN endpoints are deployed at the Data Centre perimeter.

- **Justification:** Provides secure remote access for WFH staff. VPN logs (user, time, IP) are critical evidence sources (Uptrace.dev, n.d.).
- **Why not HQ VPN only?** Would centralise remote access at one point, reducing redundancy and forensic coverage.

SSL Terminator (Cloud DMZ)

The SSL Terminator is placed in front of the Web/App server in the public cloud.

- **Justification:** Decrypts encrypted HTTPS traffic so WAF and IDS/IPS can inspect payloads. Without this, encrypted malicious traffic would bypass monitoring.
- **Why not server-side SSL only?** Would leave blind spots in forensic inspection and limit log consistency.

Enterprise Defence Tools

Tools used

1. **Web Application Firewall (WAF)**
   - Location: Public Cloud, in front of Web/App server.
   - Protects against OWASP Top 10 threats (e.g., SQL injection, XSS).
   - Forensic role: Detailed logs of attack attempts against public services.
2. **IDS/IPS**
   - Location: Integrated into HQ and Data Centre perimeters.
   - Provides intrusion alerts and blocks suspicious patterns.
   - Forensic role: Preserves packet captures and alerts for incident timelines.
3. **Email Security Gateway**
   - Location: Data Centre, between Email server and Firewall.
   - Protects against phishing, spam, and malicious attachments.
   - Forensic role: Preserves headers, sender metadata, and blocked message logs (ArXiv, 2017).

Tools Not Used

1. **Web Filtering**
   - Omitted to avoid over-engineering; Internet use is limited, and forensic evidence can be gathered at endpoints.
   - Justification: Not cost-effective for 160 workstations (Telstra, n.d.).
2. **Malware Filtering**
   - Better implemented at endpoint level using workstation AV/EDR tools.
   - Network-level malware filtering would duplicate endpoint protections without additional forensic gain.
3. **SSL Inspection**
   - Omitted due to privacy/legal concerns, particularly with international offices.
   - High resource consumption for limited forensic benefit (ISO/IEC 27043 stresses proportionality in readiness).

This selective use of tools reflects **forensic efficiency**: using only what adds value, while avoiding unnecessary complexity and cost.

Cost Estimation (10 Years)

Security Tool/Component	**Cost (for 10 years)**	**Justifications with comments and sources**
AAA Server (RADIUS/TACACS)	~3,000	Use a well-supported RADIUS/TACACS+ server (e.g. Radiator). Radiator's license is only $1k (dbjournal.ro); add a midrange rack server (~$2k) for hosting. Centralized AAA logs user auth/events for forensics.
SIEM Solution (Log Analytics)	~25,000	Elastic/Splunk-class SIEM. Elastic Cloud SIEM "Standard" starts at $1,140 USD /yr (underdefense.com). Assuming a moderate plan ($2k USD/yr) to cover 1–2 GB/day logs, this is ≈$30k AUD over 10 yrs (≈$25k with some reserved instances). Splunk Enterprise has similar pricing ($1.8k USD/GB/yr (uptrace.dev)). Hardware (2 servers) ~$10k included.
Firewalls (NGFW, 2× HQ/DC)	~44,000	FortiGate 100F (or equivalent) at HQ and DC. Each unit is ~$3.64k AUD (thetechgeeks.com). Ten-year Unified Threat Protection (UTP) maintenance (two 5-yr contracts) is roughly $9,300 AUD per 5 yr (avfirewalls.com.au) (premium services+24×7 support) ×2 = ~$18.6k each. Total ~22k/device; 2 devices = ~$44k. (UTP includes IDS/IPS, AV, etc.)
SSL/TLS Load Balancer (Cloud)	~3,500	AWS Application Load Balancer for SSL termination. Cost $0.0225 USD/hr + $0.008/LCU-hr (aws.amazon.com) . Roughly $300/yr ($3k/10yr) for a light load. Provides certificate management and clear-text to WAF/IDS.
Web Application Firewall (WAF)	~2,000	AWS WAF protecting cloud web apps. Pricing: $5 per WebACL + $1 per rule per month (aws.amazon.com). Example: one ACL + 10 rules ≈ $15/mo (~$180/yr), so ~$1.8k over 10 yrs. Captures OWASP attacks and generates forensic logs of blocks.
Email Security Gateway	~58,000	Hosted filtering (e.g. Proofpoint Essentials). Sherweb lists Proofpoint Essentials Business at $3.03/user/mo (sherweb.com) (~$36/yr). For 160 users: ~$5,800/yr ⇒ ~$58k over 10 yrs. Provides spam/phishing defense and preserves headers/logs.
Servers & Network Hardware	~10,000	Rack servers for AAA, SIEM and core switches. E.g. two midrange servers (~$5k each) for HA, plus $0. Note: OS/software (Linux, etc.) assumed free. These ensure central log storage and processing capabilities.
TOTAL	$145,500 AUD	

Disclaimer:
This 10-year cost estimate (~$145,500 AUD) covers only the specified forensic-readiness components (AAA, SIEM, Firewalls, VPN, WAF, IDS/IPS via firewall, SSL terminator, and Email Security Gateway). It does **not** include:

- Endpoint protection (EDR/AV) licensing for 160 workstations
- General IT infrastructure (switches, routers, cabling, UPS, etc.) beyond the minimum servers noted
- Staff salaries, training, or incident response costs
- Cloud bandwidth, storage, or scaling charges beyond baseline AWS ALB/WAF estimates
- Software upgrade/replacement cycles if vendors sunset products before 10 years
- Backup/disaster recovery systems, redundancy sites, or legal/compliance audits

Actual spend could be higher depending on vendor contracts, support tiers, and growth in log volume or user base.

Conclusion

This design creates a forensic-ready, scalable, and cost-justified enterprise network for the next decade. By adopting a hybrid server and WAN architecture, sensitive data remains protected while public-facing systems leverage cloud elasticity (Telstra, n.d.).

Core security components (AAA, SIEM, Firewalls, VPN, SSL Terminator) were carefully placed to maximise evidence collection and forensic integrity. Defence tools such as WAF, IDS/IPS, and Email Security enhance protection and generate critical forensic artefacts, while unnecessary tools were omitted to reduce complexity (ISO, 2015).

The total cost of **~$145,500 AUD over 10 years** is reasonable for a 160-user consulting firm with international operations. More importantly, the design directly supports the forensic readiness principles in ISO/IEC 27043:2015 by ensuring evidence is continuously generated, preserved, and centralised, allowing the company to minimise investigation costs and respond effectively to future cyber incidents.

References

Academia.edu. (2016). *ISO/IEC 27043:2015 – Role and application* [PDF]. Academia.edu. https://www.academia.edu/105743779/ISO_IEC_27043_2015_Role_and_application (“ISO/IEC 27043:2015 standard harmonises incident response forensic process models…”)

Academia.edu. (n.d.). *Digital forensic readiness in cloud using ISO/IEC 27043 guidelines on security monitoring* [PDF]. Academia.edu. https://www.academia.edu/66089112/Digital_forensic_readiness_in_operational_cloud_leveraging_ISO_IEC_27043_guidelines_on_security_monitoring (“ISO/IEC 27043:2015 … maximize the potential use of digital evidence while minimising the cost…”)

ISO. (2015). *ISO/IEC 27043:2015 Information technology—Security techniques—Incident investigation principles and processes*. https://www.iso.org/standard/44407.html

Telstra. (n.d.). *IPVPN from Telstra Enterprise*. Telstra Business (Australia). https://www.telstra.com.au/business-enterprise/products/networks/adaptive-networks/private-networks/ipvpn (“Delivered using MPLS technology … highly secure and reliable…”)

Telstra. (n.d.). *Telstra Business IP secure MPLS IPVPN solution* [PDF]. Telstra. https://www.telstra.com.au/content/dam/shared-component-assets/tecom/networks/private-networks/pdf/business-ip-data-sheet.pdf (“Telstra Business IP is your flexible solution for a fast and scalable MPLS-based IP VPN network… global reach of over 2,000 points…”)

Uptrace.dev. (n.d.). *Guide to Splunk pricing and costs in 2025*. Uptrace.dev. https://uptrace.dev/blog/splunk-pricing (“An in-depth analysis of Splunk pricing models, licensing costs…”)

UnderDefense. (n.d.). *Splunk SIEM pricing ranges*. UnderDefense.com. https://underdefense.com/industry-pricings/splunk-siem-pricing/ (“Splunk’s ingestion-based pricing can range from $1,800 to $18,000 per year for a data volume of 1–10 GB/day…”)

ITQlick. (2025). *Splunk pricing: How much does it cost in 2025?* ITQlick.com. https://www.itqlick.com/splunk/pricing (“Splunk Enterprise license costs around $1,500 per year for 1 GB/day… for 100 GB/day, roughly $60,000 per year.”)

ArXiv. (2017). *Are you ready? Towards the engineering of forensic-ready systems*. https://arxiv.org/abs/1705.03250 (“…maximise the potential use of evidence whilst minimising the costs of an investigation.”)