COIT20246 NETWORKING AND CYBER SECURITY – MEL GROUP 40

**Table of Contents**

[Introduction 3](#_Toc209032111)

[Network Design 3](#_Toc209032112)

[Assumptions 3](#_Toc209032113)

[Design Philosophy 4](#_Toc209032114)

[IP Addressing Scheme 5](#_Toc209032115)

[WiFi Design 6](#_Toc209032116)

[Hardware Recommendations 6](#_Toc209032117)

[Cloud Services 7](#_Toc209032118)

[Options Considered 7](#_Toc209032119)

[Evaluation 8](#_Toc209032120)

[Recommendation 8](#_Toc209032121)

[Cybersecurity Risk Assessment 8](#_Toc209032122)

[Approach 8](#_Toc209032123)

[Key Risks 8](#_Toc209032124)

[Controls & Mitigation 8](#_Toc209032125)

[Ethical and Social Issues 9](#_Toc209032126)

[Reflection 10](#_Toc209032127)

[Conclusion 10](#_Toc209032128)

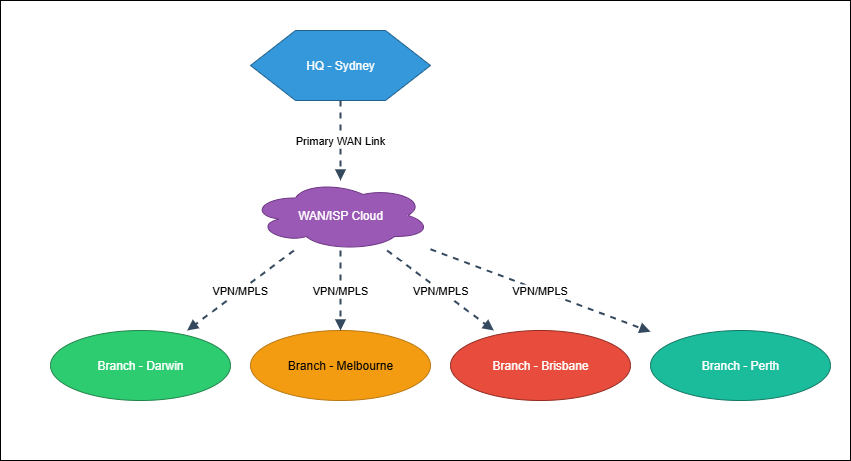
[References 12](#_Toc209032129)

# Introduction

Truelec is a prominent electrical contracting company, which is introduced as a fast growing organization that needs upgraded and secure IT infrastructure to operate. The company has its headquarters in Melbourne and a branch in Darwin and this has placed great importance on effective communication, network functioning performance, and secure access to corporate resources. The report will build a scalable network service, evaluate the options of cloud computing, and quantify the risks of cybersecurity which are relevant to the business context. It also considers other ethics and social responsibilities that address privacy of data and organizational responsibility. To address these demands, the research confirms that through the use of a systematic approach to the network planning, security and governance, the efficiency of operations and long-term sustainability of Truelec will be guaranteed, not to mention addressing the academic and professional learning outcomes of MEL Group 40.

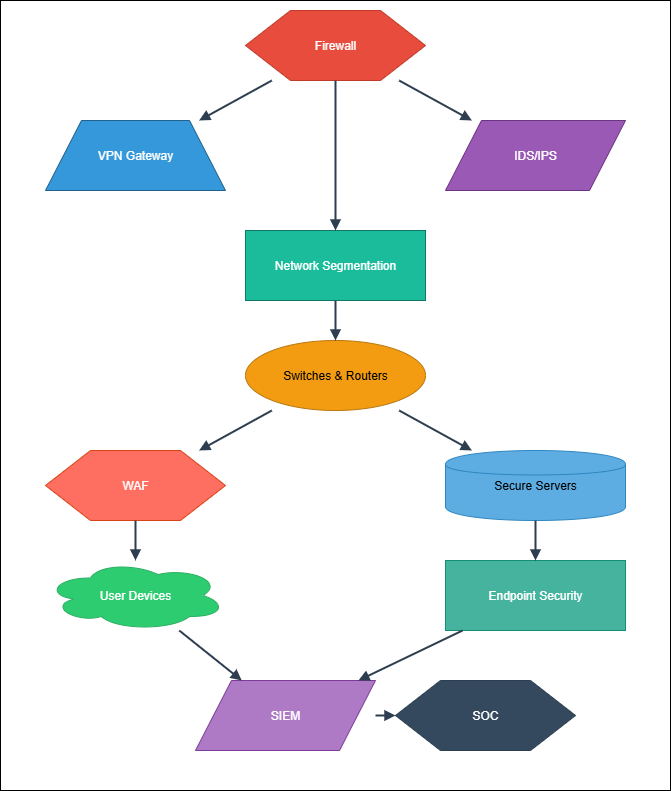
# Network Design

## Assumptions



**Figure 1: WAN connection for all sites**

The diagram is a hub-and-spoke type of network with HQ as a central hub and the branches being linked via the VPN/MPLS to the ISP cloud (Mazhar et al. 2023). This architecture provides single point administration, scaling and secure connectivity. A single instance of HQ WAN connection is thus susceptible such that it must be redundant and ideally traffic-path routing is required to remain solid.

****

**Figure 2: Security Architecture**

The architecture is a layered security which includes firewalls, VPNs, IDS/IPS, segmentation and endpoint protection. Integrated SIEM and SOC have centralized monitoring and response (Pawlicki et al. 2022). This defense-in-depth approach promotes resilience by guaranteeing protection of traffic, applications and devices. It is however very efficient and should be updated regularly, staffed with experts and the complexity of configuration minimized.

## Design Philosophy

The network design adheres to the hierarchical architecture, which includes Core, Distribution, and Access layers to provide good structuring of connectivity and easy management. The Core layer is used to provide high-speed backbone services, the Distribution layer carries out policies and routing, and the Access layer provides end-user access(Pawlicki *et al*. 2022). Such a layered approach is more scaling and less complicated to trouble shoot. Redundant links, backup devices and failover mechanisms ensure high availability and reduce the downtime in order to achieve business continuity. Scalability helps in the expansion in the future as the company expands. VLANs and firewalls provide security segmentation to isolate sensitive systems to minimize the attack surfaces and prevent the access of corporate data by unauthorized parties.

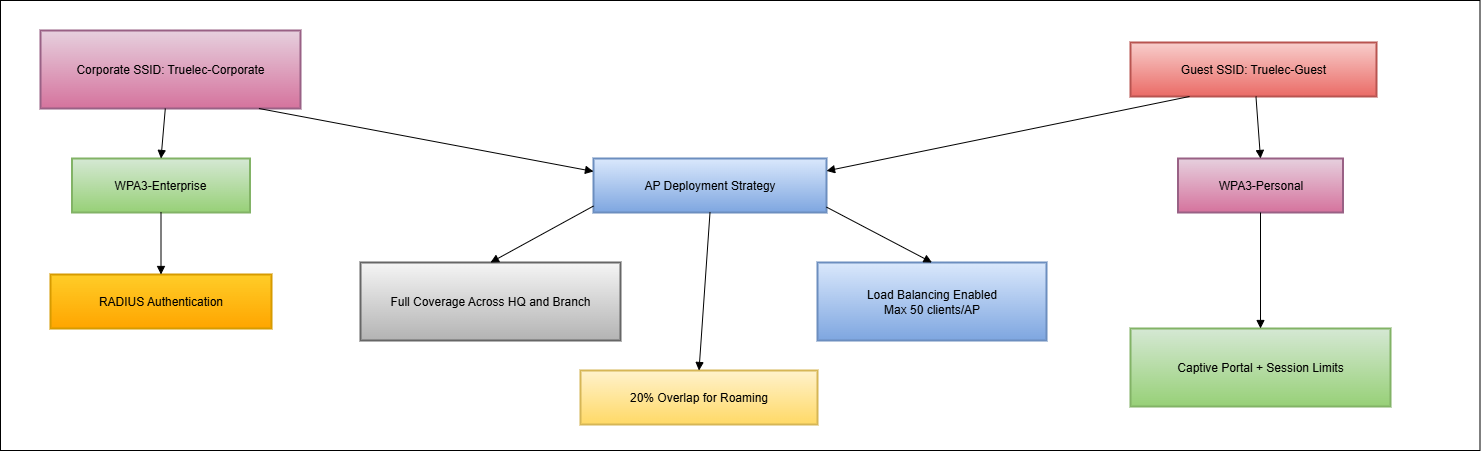
## IP Addressing Scheme

|  |  |  |  |
| --- | --- | --- | --- |
| Location & Segment | IP Range | Subnet Mask | Purpose |
| Melbourne HQ – Core | 54.10.0.0/16 | 255.255.0.0 | Core backbone and inter-VLAN routing |
| Melbourne HQ – Servers | 54.20.10.0/24 | 255.255.255.0 | Application, database, file servers |
| Melbourne HQ – Staff LAN | 54.20.20.0/24 | 255.255.255.0 | Office desktops, laptops, printers |
| Melbourne HQ – WiFi Corp | 54.20.30.0/24 | 255.255.255.0 | Secure corporate wireless network |
| Melbourne HQ – WiFi Guest | 31.10.40.0/24 | 255.255.255.0 | Guest wireless with internet-only |
| Darwin Branch – Staff LAN | 31.20.50.0/24 | 255.255.255.0 | Branch office desktops and devices |
| Darwin Branch – Servers | 31.20.60.0/24 | 255.255.255.0 | Local file/print and backup servers |
| WAN Links (HQ–Branch) | 54.30.0.0/30 | 255.255.255.252 | Point-to-point WAN connections |
| Management VLAN (All) | 54.40.70.0/24 | 255.255.255.0 | Switches, routers, APs management |
| CCTV & IoT Devices | 31.50.80.0/24 | 255.255.255.0 | Surveillance cameras and IoT sensors |

**Table 1: IP Addressing Scheme**

## WiFi Design

The wireless network should be built in such a way that it offers secure, reliable and high performance to the staff and guests. There are two SSIDs deployed: a Corporate WiFi based on WPA3 Enterprise with RADIUS authentication of staff equipment, and a Guest WiFi with no access to internal resources and to the internet(Mazhar *et al*. 2023). The access points are well distributed to provide uninterrupted coverage, load balancing and roaming within office locations. VLAN will isolate the traffic of guests and corporate and reduce security threats. Band steering makes devices steer to 5GHz with greater throughput and still be compatible with 2.4GHz. The controller-based management allows for monitoring, updating, and detecting intrusions, which guarantee stability in security and performance.



**Figure 3: Wifi Design**

## Hardware Recommendations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Recommended Device | Quantity | Purpose | Approx. Cost |
| Core Switch | Cisco Catalyst 9500-24Q | 1 | High-performance backbone switching | $18,000 |
| Distribution Switches | Cisco Catalyst 9300-24T | 2 | Policy enforcement and VLAN routing | $9,000 each |
| Access Switches | Cisco Catalyst 9200-24P | 6 | End-user connectivity with PoE support | $4,500 each |
| Routers (HQ & Branch) | Cisco ISR 4331 | 2 | WAN connectivity and routing | $3,800 each |
| Firewalls | Fortinet FortiGate 100F | 2 | Next-gen firewall for HQ and branch | $6,000 each |
| HQ Servers | Dell PowerEdge R740 (2×Xeon, 64GB RAM) | 2 | Application, database, virtualization | $12,500 each |
| Branch Server | Dell PowerEdge R540 (1×Xeon, 32GB RAM) | 1 | File/print services and local backup | $7,500 |

**Table 2: Hardware Recommendations**

**Estimated Total (Approx.):** $90,000 AUD

# Cloud Services

## Options Considered

The physical servers in the Truelec can be substituted with the virtual machines on the public cloud architectures in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Both provide compute instances which are similar to the proposed Dell PowerEdge servers in terms of multi-core CPUs, large memory, and expandable storage(Dini *et al*. 2023). Pricing models differ, and AWS is generally more flexible on the pay-as-you-go basis, Azure is more integrative with Microsoft services and GCP is more cost-optimized. Backup, monitoring, and high availability is also an option in all the providers and thus can be used instead of physical servers.

## Evaluation

A comparison of total cost of ownership (TCO) over five years shows major differences. Physical servers would cost in the range of about 32, 500 AUD to purchase, maintain and energy. Similar cloud VMs will cost approximately 1000-1200 AUD per month each, which amounts to 60000-720000 AUD in five years. The cloud has apparent benefits, such as scalability, built-in updates, disaster recovery, and decreased IT maintenance overheads(Wazan and Cuppens, 2023). Nevertheless, the drawbacks are increased long-term operating expenses, the need to have a constant internet connection, the remote branches may require latency, and the vendor may end up being locked-in.

## Recommendation

The most appropriate provider that can fit Truelec on its cost, flexibility, and integration is Microsoft Azure because it fits well with the current infrastructure based on Microsoft and has hybrid cloud support(Duary *et al*. 2024). It is proposed to do a partial migration, keeping the critical applications on-premises to ensure performance and migrating backup, email, and collaboration workloads to the cloud. This hybrid architecture is a compromise between scalability, resilience and cost-efficiency.

# Cybersecurity Risk Assessment

## Approach

A mini risk assessment scheme is implemented to define the key assets of Truelec and the threats. The most important resources are on-premises servers, data related to clients and projects, CCTV systems, IoT devices, WiFi infrastructure, and cloud-based resources(Wazan and Cuppens, 2023). They are all tested on weaknesses, probability of attack, and the possible effect on operations.

## Key Risks

The key threats have been found as follows: malware infections, phishing, insider threats, denial of service (DoS) attacks, physical devices theft, misconfigurations, social engineering, and ineffective authentication practices(Aldhyani and Alkhatani, 2022). Of all these, the most vulnerable asset is client data stored in servers and cloud platforms as it is sensitive and regulatory in nature.

## Controls & Mitigation

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Description | Mitigation Effect | Risk Level After Control |
| Next-Generation Firewall (NGFW) | Inspects traffic, blocks malicious packets, and enforces policies. | Reduces exposure to DoS, malware, and intrusion attempts. | Medium |
| Multi-Factor Authentication (MFA) | Requires multiple credentials (password + token/biometric) for system access. | Mitigates weak authentication, phishing, and insider misuse. | Low |
| Data Encryption (AES-256) | Encrypts sensitive client data at rest and in transit. | Protects confidentiality even if data is stolen or intercepted. | Low |

**Table 3: Controls & Mitigation Table**

All these controls are aimed at confidentiality, integrity and availability. Nevertheless, they can be also problematic: NGFWs and encryption cause latency and increase expenses, and MFA can cause inconvenience(Dini *et al*. 2023). Nevertheless, despite these restrictions, their implementation reduces the risk of significant violations and increases the adherence to the conditions of data protection.

# Ethical and Social Issues

The management of the information systems of an electrical contracting business such as Truelec incorporates ethical and social issues in its management. Sensitive information such as HR records, client information and confidential information of projects are stored by the organization and thus need a high level of protection in order to maintain privacy and trust(Duary *et al*. 2024). Legal requirements, including the Privacy Act 1988 (Australia) and the General Data Protection Regulation (GDPR) to operate globally should be met to make sure that personal data are handled in ways that are legal. In addition to compliance, the company holds a moral role of ensuring that stakeholders are not victimized by their breach of data(Badhon and Aggarwal, 2021). A breach would hurt relationships with clients, project derailment and destroy the confidence of employees. Ethical practice requires informed consent, clarity in the use of the data, and clear accountability measures in case the incident takes place. Focusing on its privacy, fairness, and accountability, Truelec becomes responsible and enhances its image as a safe and reliable company partner in the construction and electrical market.

# Reflection

Being two team members, Arpit and Rushi, we equally shared responsibilities and succeeded in completing the project. I, Arpit, worked mainly on creating the network topology and working on the IP addressing scheme making sure that the requirement of the student ID is fulfilled. Rushi focused on cloud service analysis, cybersecurity risk analysis, and ethics. It was a joint effort, where we had to draft, edit and clean up the final report so that there is consistency and precision.

We listed our work with the help of commits and version control that allowed us to monitor individual work in a transparent manner. The online meetings and frequent chats ensured communication, which made it possible to solve the problems quickly and make informed decisions. This team work enhanced productivity and satisfaction of both the technical and non- technical factors.

We were also strong in the way we divided tasks and communicated regularly, thus keeping overlaps and confusion to a minimum. There were however difficulties in reading and understanding complicated requirements especially on IP addressing policies and the finer details of the report. These challenges were met through the reviews of each other in their sections and the subsequent improvement of their sections.

We intend to raise the bar in the future by ensuring that we use predefined templates, project management software and short meetings with each other. It was an experience that improved our technical knowledge as well as our teamwork skills.

# Conclusion

This report will offer a detailed solution to the problem of Truelec; the company requires a secure, scalable and future-proof IT infrastructure. The hierarchical network design was offered with clear IP addressing, WiFi segmentation, and the proper hardware recommendations. An assessment of cloud service value was conducted with consideration of cost and efficiency of operations and a risk assessment was made to list significant threats related to cybersecurity and mitigation strategies that can be used. Ethical and social aspects were also pointed out with the underlining of data privacy and accountability. The report also concludes that through the combination of effective technical design and governance and ethical work, Truelec will be able to tighten its resilience, aid in its growth, and increase the trust of its stakeholders towards its operations.

# References

Aldhyani, T.H. and Alkahtani, H., 2022. Attacks to automatous vehicles: A deep learning algorithm for cybersecurity. *Sensors*, *22*(1), p.360. <https://www.mdpi.com/1424-8220/22/1/360>

Badhon, A.J. and Aggarwal, D.S., 2021. Cybersecurity in Networking Devices. *Journal of Cybersecurity and Information Management*, *8*, pp.35-41. <https://www.researchgate.net/profile/Vijay_Sinha2/publication/355875716_Cybersecurity_in_Networking_Devices/links/618278850be8ec17a964de47/Cybersecurity-in-Networking-Devices.pdf>

Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q. and Gasmi, K., 2023. Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity. *Applied Sciences*, *13*(13), p.7507. <https://www.mdpi.com/2076-3417/13/13/7507/pdf>

Duary, S., Choudhury, P., Mishra, S., Sharma, V., Rao, D.D. and Aderemi, A.P., 2024, February. Cybersecurity threats detection in intelligent networks using predictive analytics approaches. In *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1-5). IEEE. <https://www.researchgate.net/profile/Deepak-Dasaratha-Rao/publication/381675573_Cybersecurity_Threats_Detection_in_Intelligent_Networks_using_Predictive_Analytics_Approaches/links/66f58645906bca2ac3cf7cd4/Cybersecurity-Threats-Detection-in-Intelligent-Networks-using-Predictive-Analytics-Approaches.pdf>

Mazhar, T., Irfan, H.M., Khan, S., Haq, I., Ullah, I., Iqbal, M. and Hamam, H., 2023. Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. *Future Internet*, *15*(2), p.83. <https://www.mdpi.com/1999-5903/15/2/83>

Pawlicki, M., Kozik, R. and Choraś, M., 2022. A survey on neural networks for (cyber-) security and (cyber-) security of neural networks. *Neurocomputing*, *500*, pp.1075-1087. <https://www.sciencedirect.com/science/article/pii/S0925231222007184>

Wazan, A.S. and Cuppens, F., 2023. Cybersecurity in networking: adaptations, investigation, attacks, and countermeasures. *Annals of Telecommunications*, *78*(3), pp.133-134. <https://link.springer.com/content/pdf/10.1007/s12243-023-00956-9.pdf>