Reference:

XANTEC Solutions Malaysia (50 employees) – SME Award 2017 – annual revenue > 1m

Configura Malaysia (166 employees)

Assume the company has annual revenue over 1m

System engineer to maintain website:

Annual salary = 68000aud

1. Enterprise Defense System

For database server / File server:

Having branch offices in different cities, it means that wide area network (WAN) is being used to allow the network to be extended over a large geographical distance. Due to this, network administrator might find it difficult when it comes to decide whether should they sacrifice security and data privacy for higher performance across the branches.

Having branch offices in different cities, means that WAN is used to allow network to extend over a large geographical distance. It might be difficult to ensure security and data privacy with high performance communication across branches.

This can be solved by applying VPN for in-company communication. By using Cisco Meraki product, auto VPN is provided for the branches to securely connect with each other by using mesh or hub-and-spoke topologies. High security can be expected because each device on the network is isolated from the others through the single connection to the wireless router in hub-and-spoke, whereas in mesh, infrastructure nodes are connected directly and dynamically but not hierarchically. Each

Mesh: Infrastructure nodes are connected directly and dynamically but not hierarchically. Each connection can carry its own data load, providing security and privacy.

Hub-and-spoke: Each device on network is isolated from others through a single connection to wireless router, where secured tunnel extends between individual spoke and the central router (hub).

Cisco Meraki series product has built-in software defined WAN capabilities which it can improve the efficiency on using resources for multi-sites deployments. Besides, it allows the admins to utilize the available bandwidth without sacrificing its security purpose, by looking at the bandwidth consumption for each department, and application usage across the company. Centralized management can be achieved easily by applying this cloud managed security box.

In addition, the Cisco Meraki box itself can act as an Identity-Based Firewall as well. It will assign firewall and traffic shaping rules, ensuring the right policies for each class of users. For example, in a company, there will be staff with different kind of authorities, where the documents they are allowed to access is limited by their job scope. The Cisco Meraki which acts as stateful firewall and integrated Sourcefire intrusion prevention (IPS) engine also protects network resources from vulnerabilities by updating threat definitions and filter lists seamlessly.

Amazon cloud – database server – back up cost – review

Dropbox – key – encrypted

Gaming company

Application/ Web Server (Hardware):

Web servers are computers that are usually set up in facilities called data centers and operated by hosting companies. The purpose of these computers is to store websites so that people can visit them on the Internet. Browsers like Google, Firefox, etc communicate with web servers to bring you information from the Internet.

They have software servers (Daemon Software) running in the background based on the context, such as:

HTTP Server – send website files

FTP Server – upload files

Email server – gathers and directs email

Database server – store essential info to operation of the website itself

Web servers often come as part of a larger package of Internet- and intranet-related programs for serving email, downloading requests for File Transfer Protocol ([FTP](https://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol)) files, and building and publishing Web pages. Considerations in choosing a Web server include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and the particular publishing, search engine and site building tools that come with it.

Apply HTTPS on web server

* encrypted link between a web server and a web client.
* by identifying and authenticating the server as well as ensuring the privacy and integrity of all transmitted data
* When you use HTTPS, you connect to your web pages and resources using the HTTPS protocol instead of HTTP.
* Protect from man-in-the-middle attack

HTTPS = HTTP + SSL

Handshaking process – server hello, exchange cipher suites and certificates

CA-signed certificates

In order to use HTTPS, you need to obtain a server certificate and bind it to the website that hosts ArcGIS Web Adaptor. Each web server has its own procedure for loading a certificate and binding it to a website.

One of the most trusted company to issue certificates is Verisign.

<https://www.websecurity.symantec.com/ssl-certificate>

For a public application/ web server, ECC: Strongest security and vulnerability assessment should be equipped to protect the customer’s information at the base case. From required features stated, the company should get at least the Secure Site Pro option, or the Secure Site Pro with green address bar to provide security sense to the users when they access the website.

Email Server (internal)

* Transparency report – customer owns their own data
* 128bit Encryption – HTTPS and Transport Layer Security 1.1

- authenticated by the SHA1 cryptographic hash function and eventually decoded by the ECDHE\_RSA key exchange mechanism.

- only user has the key

* Custom designed distributed data centres – can be shifted to stable and secure locations
* Continuously monitoring – threat detection
* 2 factor authentication – physical tokens (e.g. code sent to phone)
* Safe browsing feature – warns user when accessing harmful website from gmail
* Access list of devices that accessed gmail
* SMTP STS prevent man in the middle attack
* End to end encryption – pgp – private key locally in browser – public in gmail server
* Detect email sent from services doesn’t support TLS encryption
* Admin of mail server can generate user activity report

- ip addr, geographic location, time and device used

* Admin can use content detector

2. Cost Estimation

The typical budget for one of the appliances costs around $2,800 per year including license fees. This is much less than the cost of hiring a full-time employee while providing intuitive and efficient interfaces for the overworked technical professional.

IDS systems must be tuned by IT administrators to analyze the proper context and reduce false-positives. For example, there is little benefit to analyzing and providing alerts on internet activity for a server that is protected against known attacks.

- Calculate the estimate salary for network administrator for one year including all the bonus

Secure Site Pro - $995/yr

Secure Site Pro with EV - $1499/yr

Gmail

10USD/user/month

1 year with 50 employees = 6000usd = 8500aud

25usd/user/month = 15000usd – 21000aud

With security center and data loss prevention, log analysis, security key enforcement

3. Forensic Readiness Plan

Definition:

FRP is a policy document setting out the procedure to produce useful electronic evidence when they are required in either legal action, digital investigation and so on.

Purpose:

To maximise the ability to gather and use digital evidence and minimize disruption and cost.

Planning processes

Implementation processes

Assessment processes

1. Ownership

Company should assign some senior workers who can make management decisions and trustworthy to own and manage the FRP.

2.