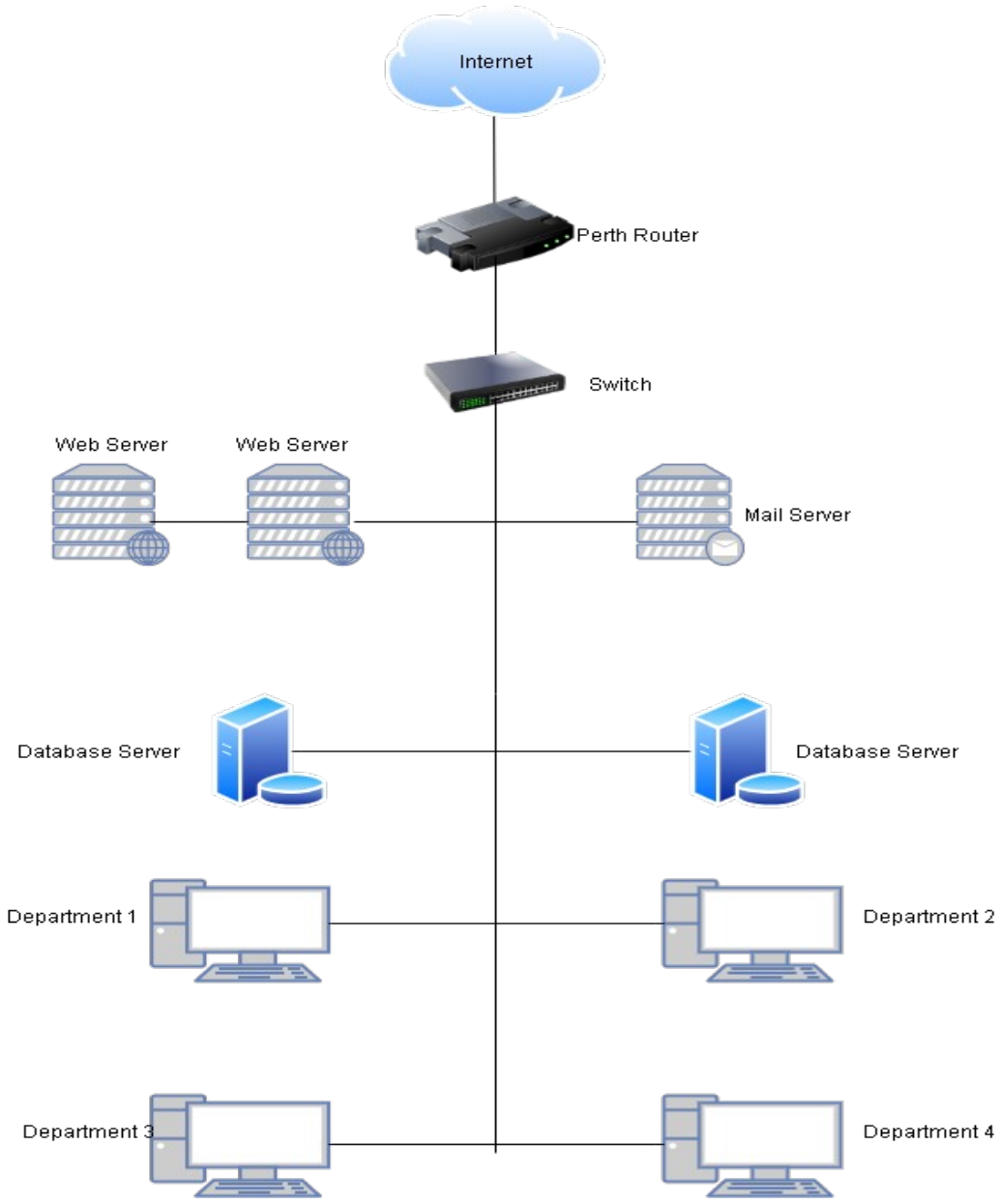
Original Network Diagram



Part 1: Potential Threats

Complaint 1 (Teddy): My computer takes a long long time to start up and shut down. It seems like there are other programs which I don't use running when I start my computer as well.

Possible Threats:

Computer might be crash or overheat and stop working.
If this is caused by virus, the virus may be spread across the network to other devices.

Causes:

- RAM is not powerful enough to run a lot of applications.
- Hard Disk is used for a long time and is at maximum capacity.
- There are too many start up programs and applications.

Solution:

Firstly, call boot system and start the computer with safe mode. If computer is working well in safe mode, the main problem is that there are too many applications and programs that run normally when the computer runs. Solution to fix this problem is that uninstalling some applications and disallow applications from starting up. This all steps can be done by killing applications at task manager.

Another way is that downloading Anti-Virus application and run a deep scan. Kill all threats and see if it has fixed the problem.

If the problem it not fixed, hard disk would be the problem. Install larger capacity of hard disk or install larger capacity of solid-state drive so that this problem would be solve easily. To avoid this problem in future is to limit the downloads and always delete unnecessary applications and files from the hard disk. To make this process, CCleaner or AVG anti-virus is recommended.

Complaint 2 (Christina): I often get the blue screen of death; my workstation keeps crashing. I found it to be so frustrating.

Possible Threats:

Windows and Drivers might be out of date.

Hard disk that installed windows is crashed.

Causes:

- Hard disk is damaged by electricity volt.
- Drivers are out of date and got some problems with PC's hardware or issue with its hardware driver software.

Solution:

Blue screen of death in Windows is technically known as a stop error or factual system error. To fix this problem, windows and every driver in computer might be up to date. Drivers and Windows can be update in system setting > update and security > Windows update.

If blue screen of death is still happening, deep scan for malware is needed because malware can damage user's Windows system files and result in a blue screen. To run deep scan, Malwarebytes is recommended.

If the problem is still happening, the final step is to reset the hard disk and reinstalling windows. To make this step, user will have to download the windows ISO files via www.microsoft.com and remove that windows file to a new USB stick. That USB stick might have at least 8GB. After downloading windows, run the computer into boot and format the hard disk and reinstall windows. This might fix the blue screen death problem.

Complaint 3 (Meredith): It takes forever to download a file from the company servers. It doesn't even matter what the size or type of the file are.

Possible Threats:

The network system would be under attack.

Causes

- Bandwidth of the network is not enough to accommodate to all devices.
- Proxy virus use all the bandwidth of the network.
- Attacker launches a denial of service attack on the network.
- Poor server performance and lots of traffic.

Solution:

The first step would be figuring the main problem out. When other devices on the same network aren't having the same problem, then the system is the problem. So, try to be restarting the network router, if they do. This may also be attacker who is attempting to penetrate the system or just overloading it. Also, proxy virus can happen this problem. If proxy virus made this, there are some solutions to fix this problem will be shown in second part.

If the problem is the computer, check if this applies only to the browser or to any application that requires the use of the network. If it is only happening to the browser, clear the cache and try again. If it is happening to browser and all other applications, go to setting > network and internet > proxy > manual proxy setup > turn off use a proxy server.

If does not solve the problem, the network card is the problem. Search "Device Manager" on the start menu and go to the network adapters and update all the drivers. This will solve the problem. If still not working, there is only 1 possible problem is that malware. As I said in complaint 2, "Malwarebytes" is the best application to check for malware. If there is malware that is corrupting the software setting of the card so, try to remove the malware by using that application and restart the computer.

Complaint4 (Alex): I've got customers and colleagues informing me that I've been sending them emails, this is very weird because my job doesn't really concern sending out emails to my colleagues, let alone customers.

Possible Threats:

Email is hacked by some reasons.

Causes:

- Email password is weak and easily to hack.
- By clicking a malicious email, IM conversation, or on a social networking site, or webpage.

Solution:

First, user must always check and update user's computer security because most of the hackers collect passwords by using malware that has been installed on user's computer or user's mobile phone. User should anti-virus programs and anti-malware programs to avoid this problem.

Second step is to use stronger email password that would be difficult for hackers to guess. Most of the people give their personal account passwords as their birthdates, their phone numbers and their names. So, try to give difficult passwords including over 12 characters, numbers, symbols, capital letters, low-case letters by mixing them all.

Third step is to use secure wi-fi network. If user use unsecure wi-fi network, hackers were able to eavesdrop on user's data and user's password. To avoid this, users should only ever connect to reputable networks that user trust and passwords are protected.

Final step is to enable step-2 verification system on every account. Enabling step-2 verification is a huge advantage for user to believe that his accounts are safe. Because step-2 verification is always connected with user's phone number so even hacker got passwords, he can't log in because step2 verification code is required to log in.

Complaint 5 (Richard): I get a lot of pop-ups on my screen; I have never visited any bad(inappropriate) websites.

Possible Threats:

Attacked by malware and ransomware.

Causes:

- Pop-ups can be caused by some adware (or advertising-supported software) that hides on user's computer and automatically displays advertising material when user is online.
- Also, tech support scammers will try to swindle money from unsuspecting users. Most of the tech scammers will try to scare user into thinking he have a problem with his computer, such as a virus.

Solution:

To avoid pop-ups, firstly user must use pop-up blocker as much as possible. In these days, most of the people install pop-up blocker and avoid pop-ups. User can add pop-up blocker by searching "Chrome Store" in google and add to his browser.

Secondly, user must scan for malware by using "Malwarebytes" or "BitDefender" that is free to use and remove malware from user's computer and tell user which programs are causing problems for him. If these steps cannot fix the problem, there is a final way to fix which will be shown in paragraph 3.

Final step is to restart the computer in safe mode. If pop-ups are making it difficult for user to use his computer, user should restart in safe mode. This will only start the necessary application that user's computer needs to run. From there, user can search for and. Odd applications to delete or quarantine programs by running malware scanners.

Complaint 6 (Joe); The fan in my computer is just so loud. It seems to be spinning really fast and all the time. Even when I am not using it.

Possible Threats:

Computer air vents might be blocked or overheating.

Background applications are using CPU 100%.

Causes:

- Computer is overheating.
- Dust, dirt and other debris block the air vents of user's computer and it can't create enough air flow to cool down efficiently.

Solution:

The obvious way to check overheating is to feel it. When the fans work noisy and the machine is always very hot, so user need to clean it up. Open the CPU, clean the CPU fan and adding more thermal paste to CPU so that CPU overload will not be happen and CPU over heating will happen less. Try to clean CPU fans every 2 months.

Second way to fix this problem is that installing monitoring applications that can adjust Fan's RPM and easily know which fan is running too loud and why it is working for no reasons. Third way is to keep the computer in the cool room. Computer overheating can cause when the temperature of the room is too high. Using computer in cool room can avoid fan overheating problems.

Final way is to always check task manager when CPU fans run for no reason. By checking via task manager, user can see the usage of CPU and other unnecessary applications and users can end the apps as he like from task manager.

Complain 7 (All employees): Difficulty accessing the website, mail and database servers.

Possible Threats:

The website might be under attack.

Causes:

- DDoS attack might be happening that is causing this unavailability.
- Sever of the website is defective.
- The ISP falls into trouble.
- Proxy virus also harms website, mail and database.

Solution

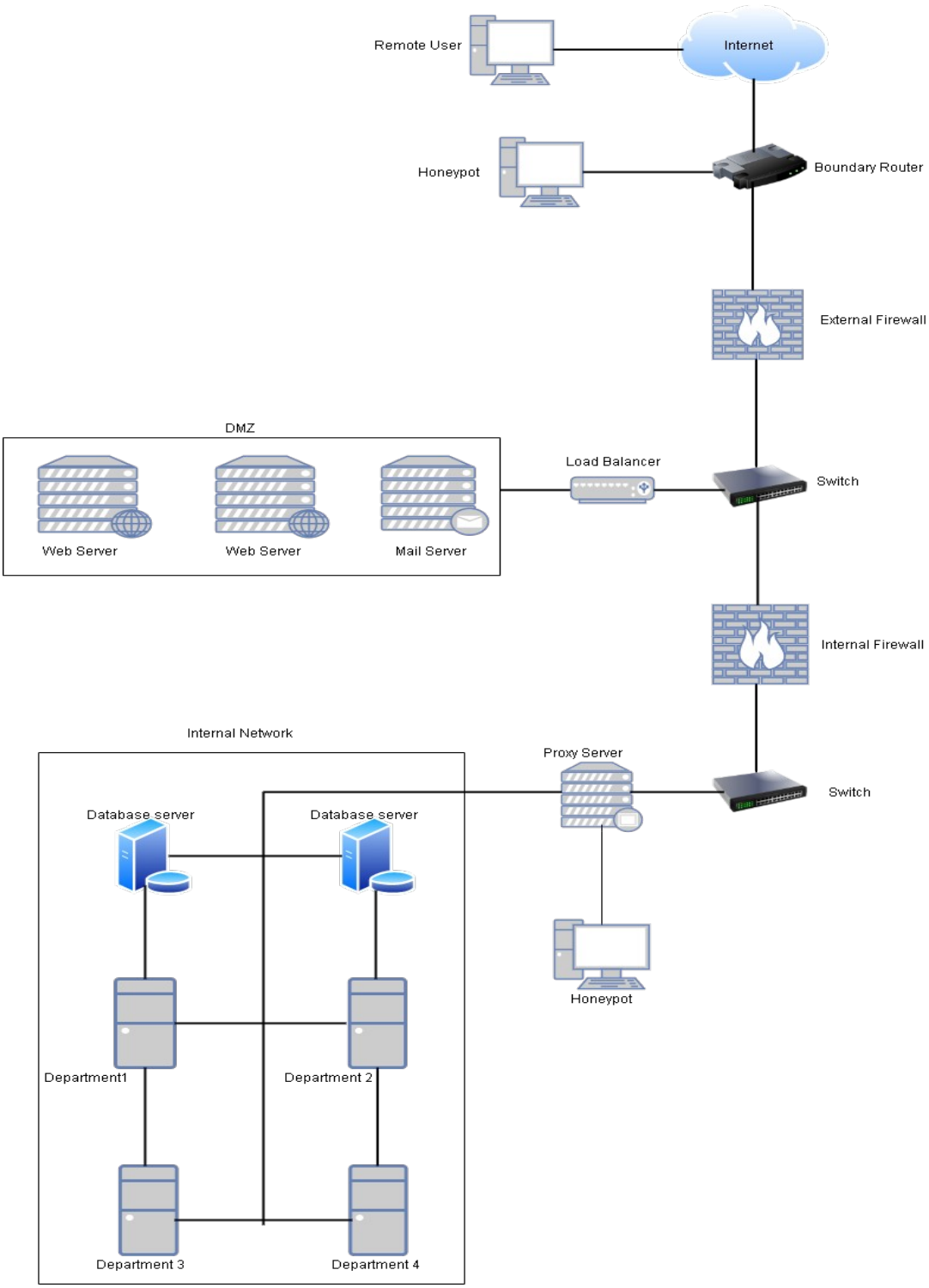
If the ISP got the problem, so there is nothing that can be done by the company. More probable explanation is that there are issues with the network server. Check the registry for any malware and delete it and if that does not solve the problem, an update is required to handle the requests better. Check the packets that are sent back and forth to help understand the issue, because it will include useful details such as what data is being sent. If ISP is not problem, there are two possibilities. One is proxy server error and another one is ISP issue.

If proxy virus is in user's computer, it will not respond to websites that user request. To fix this issue, user can use third party software to remove that virus or resetting internet option or deleting proxy file in registry edit or turning off proxy usage in Setting of the windows.

Final possibility is that hacker attack the company's website with denial of service method. Attacker use DoS method to deny the requests for the company website so that website will automatically run out of resources and can no longer respond to legitimate requests. To prevent this problem, user can use anti-DDoS hardware and DoS protection appliance. Also, user can use flood guard to monitor unanswered request resistance, or a load balancer to identify the attack until it hits the server.

Part2: Firewall, Honeypots and Other Network Security Technologies Planning and Designing for Brisbane Branch

1. Diagram



2a.

External Firewall – External firewall is used because it provides the basic level of protection for the whole network and it can limit the IP address of the devices at the other end of the connection. Also, it provides the DMZ networks with access control and security while also providing for fast external communication.

Internal Firewall – The internal firewall prevents attackers from running rampant in the whole network system and helps to prevent attacks. Also, internal firewall is a filter to protect the internal network. Both external and internal firewalls are transparent to users and are very fast.

b.

Honeypot – In this network design diagram, two honeypots are used. First one is to connect with the boundary router and external firewall to track the attacker without exposing productive systems. The second one is designed to capture internal attacks under internal network. Both honeypots are used as decoy when we want to lure the attacker.

Router – In this diagram, binary router is used because it is meant to use as a main gateway of the whole network system and the internet. The main reason for binary router is to filter out specific types of network traffic to the honeypot with disallow incoming packets that have invalid addresses.

Web and Mail Server – These three servers are under the DMZ, the area between external firewall and internal firewall so that traffic from internet will not reach to servers. Web server is responsible for managing and running company's website and database queries. Mail server is a type of server which deals with sending and receiving emails using standard email protocols.

Load Balancer – Load balancer are act as traffic cop and sit in front of routers and servers but in this case between the switch and servers in DMZ because they can detect and counter against attacks for company's network or server. Also, load balancer can be used to detect and prevent denial-of-service (DoS) and can hide HTTP error pages or denying attackers additional information about the internal network. Load balancer also ensures high availability and reliability by sending requests only to servers that are online.

Proxy Server- Proxy server is used in this network design to prevent DoS attack and gives stronger security for internal network. Also, it can hide client system's IP address from the open internet.

Switches- Switches are key building blocks or any networks and they use MAC address to identify devices. Two switches in the design are meant to split between the DMZ and the internal network and

they provide better security than hubs. Its job is to redirect traffic flow properly and ensure less congestion.

Database Servers- Database servers are in the internal network system and they do not need to be access by the third parties and are can retain classified information that is provided with the maximum capacity.

Departments- 4 departments of the Perth branch are all located within the inner network's deepest level. It provides optimal efficiency as well as strong network interconnectivity, as they are both linked by the same connection. Using VLANS instead of using Ethernet LANS will provides better and stronger security.

Remote User – This is isolated from the system as users cross over to access the network from the internet and thus rely only on the host firewall as protection.

Part 3. IEEE Referencing List

[1] M. Huculak, "How to troubleshoot blue screen errors windows 10?", *Windows Central*, 2019. [Online]. Available: https://www.windowscentral.com/how-troubleshoot-blue-screen-errors-windows-10. [Accessed: 23- Apr- 2020].