

**ASSIGNMENT**

**A case study on:**

**Security Checklist**

**For**

**Network Security**

**(CP2414)**

**Bachelor of Information Technology**

by

UDAYA BHASKAR REDDY MALKANNAGARI

Student ID: 13368171

Under the Guidance of

Mrs. SARITA SINGH

**Contents:**

**Introduction…………………………………………………………………………………………………………………………………3**

**Part 1: Potential Threats……………………………………………………………………………………………………...........3**

**Threat 1……………………………………………………………………………………………………………………………….3**

**Threat 2……………………………………………………………………………………………………………………………….4**

**Threat 3……………………………………………………………………………………………………………………………….5**

**Threat 4…………………………………………………………………………………………………………………………......6**

**Threat 5…………………………………………………………………………………………………………………………......7**

**Threat 6……………………………………………………………………………………………………………………………….8**

**Part II: Applications and Network based attacks…………………………………………………………………………..10**

**Securing the Web Server……………………………………………………………………………………………………..11**

**Securing the Database Server……………………………………………………………………………………………..13**

**Securing the Mail Server……………………………………………………………………………………………………..16**

**Securing the DNS Server………………………………………………………………………………………………………18**

**Part III: Administering Secure Networks……………………………………………………………………………………...19**

**I.VLAN and NAT technologies…………………………………………………………………………………………..….19**

**VLAN………………………………………………………………………………………………………………………....20**

**NAT Technology………………………………………………………………………………………………………….21**

**II. Log Management………………………………………………………………………………………………………………23**

**Part IV: Firewall Planning and Design……………………………………………………………………………………………25**

**Proposed Firewall Diagram………………………………………………………………………………………………26**

**Configuration of the various devices in the Network diagram……………………………...26**

**Conclusion………………………………………………………………………………………………………………………29**

**References……………………………………………………………………………………………………………………..30**

**Introduction:**

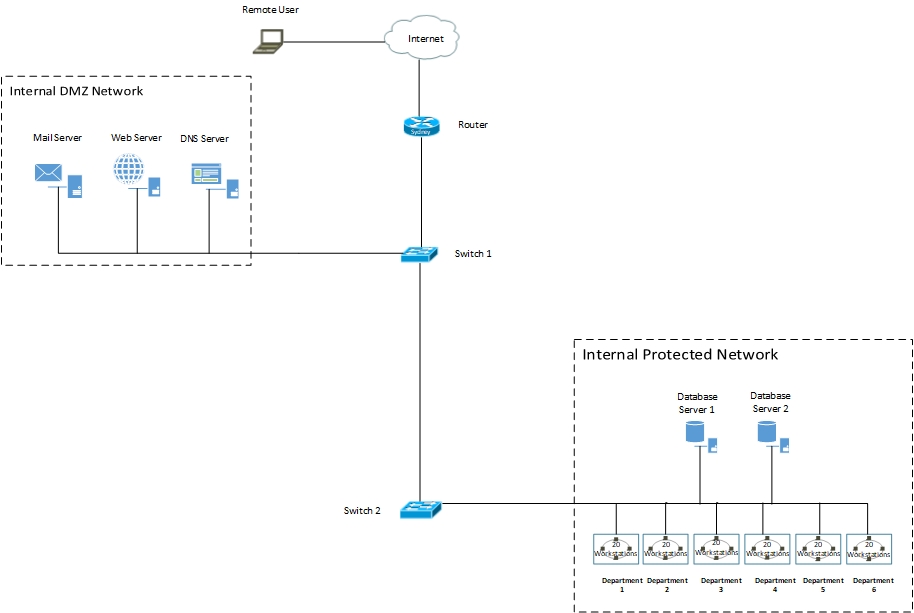
We are given a scenario wherein an Australian export company has asked to provide a comprehensive network security mechanism to its existing infrastructure. Based on the requirements of the company, we analyze the various possible solutions based on the scenario given below.

**Scenario:**

An Australian export company has asked you to identify and analyze application and networking-based threats to the organization due to the rise of cybercrime affecting businesses worldwide. They also ask you to recommend administration strategies and networking technologies to mitigate against intruders and attacks on the network. The company has asked you to work on the Sydney branch only.

***Basic Network Diagram:***

Given the current scenario, we come up with a basic network diagram displaying all the devices that are mentioned in it. The servers are shown as put in a DMZ zone and the workstations within a protected internal network. This will be justified in the explanations as we analyze the various threats and counter measures in the coming sections.



**Part I: Potential Threats**

The company has mentioned that the employees have been complaining about several issues concerning their workstations. This section identifies the threats that might have occurred and the counter measures that can be used to address each threat. It also gives a detailed understanding of the common attacker methodology and some of the alternative attacks that might have happened and their counter-measures which will help in maintaining a more secure network.

***What is a Threat?***

In formal security terminology, an “Asset” can be defined as a resource of value. It can be the data in a database or on the file system or a system resource. A “Threat” is a potential occurrence, malicious or otherwise, that may harm an asset. Countermeasures can be used as safeguards to address the threats and mitigate the risks.

**Threats and Counter-measures:**

**Threat 1:**

***Incident:*** The computer is really slow, it takes ages for my desktop to start and takes a million years to shut down.

***Threat:***  Malware / Background processes

The computer is taking a long time to start and shutdown. It can be inferred that a lot of back ground processes are causing this issue. It can also be a malware related issue that is making the processes use up more memory.

***Causes:***

There are several reasons that could slow down the computer which include the following.

*Too many Background Processes:*  The computer must be checked if there are too many background processes running on the system. If this is the case, unnecessary programs must be disabled to free up more memory.

*Hard drive Corrupted or Fragmented:* A corrupted or a fragmented hard drive can slow the system greatly. The hard drive must be defragmented regularly for optimal use.

*Infected with a malware:*  Malware is a malicious software that infects the system and performs a variety of hostile operations. It includes Trojans, worms, viruses, spyware and other harmful programs. Such infected programs can slow the computer and prevent it from performing its normal operations.

*Computer or Processor overheating:* Making sure that the computer or the processor is not over heating is an essential step in resolving this issue. This can be a result of a hardware failure as well.

***Mitigation Strategy:***

The first step in resolving this issue involves in identifying any hardware failure. In such a case, the damaged part must be replaced with a new one immediately. Background processes must be checked for any discrepancies. If there is any process that is using up a lot of system resources, the problem must be identified if it’s a system process or a malware infection.

Updated antimalware solutions must be used to identify and clear the malware threats. Patching all the softwares including the operating system will close any vulnerabilities and weaknesses in the system. This can greatly enhance the security against any kind of malware intrusion. Having an Intrusion Prevention System (IPS) in place can help in identifying any such malware intrusions.

**Threat 2:**

***Incident:*** I want a bigger hard drive as my hard drive seems to be nearly full now. I think it is strange as I don’t have big files in my drive and I don’t have that many applications installed on my computer.

***Threat:*** Hard disk failure, File System Corruption, Virus attacks

The hard drive filling up fast without having any big files can point to several things. Primarily, it can be a case of a damaged hard disk. Another reason could be a file System corruption or some form of virus attacks

***Causes:***

There can be several causes to the hard drive filling up fast which include,

*Hard disk failure:* This may be because of a damaged hard disk. The hard disk will fail to perform its function normally and show errors as wrong space sizes.

*File system Corruption:* When the file system is corrupted, it will report the free space incorrectly.

Temporary files and Caches: Most programs use temporary files and caches that are stored on the hard drive. If these directories are not deleted permanently, they can eat up a lot of space.

*System Restore Points:* System restores are backups of the OS. Normally, every time we install a new driver or perform a windows update, it creates a restore point by default. This can consume a lot of space.

*Virus attacks:* Some kinds of viruses can display these errors if the computer is infected with them.

***Mitigation Strategy:***

We must first check if the hard disk is not physically damaged. If so, it must be replaced with a newer one. We must also check if the system restore points are eating up a lot of space. If that is the case, clearing all the restore points except for the ones we need can resolve the issue.

File system errors can be checked by scanning the system during the startup. If any errors are found, it will be reported and appropriate measures need to be taken like reinstalling the operating system. Temporary directories must be cleaned with the help of cleanup utilities. This can free up a lot of space.

System must be scanned thoroughly to check for any viruses and infections. Antivirus programs must be updated with the latest virus signatures and service packs. (Dean,2012)

**Threat 3:**

***Incident:*** It takes forever to download a file (even though it is not a big file) or even to access a website.

***Threat:*** Web Server Overload

Despite the fact that the Sydney branch has a high-speed network, the downloading of files or accessing a website is taking very long. This can be inferred as a problem with the web server. The web server is overloading causing it perform ineffectively.

***Causes:***

There are several reasons that can be attributed to this problem. Some of the causes include web server hardware, network congestion, packet loss and web server overload. Most of this point out to one central theme that identifies a problem to the web server. The web server may also be facing a DOS attack or buffer overflows.

As it is mentioned that the Sydney branch must deal with a heavy network traffic during the weekdays, it might be a case of network congestion wherein the server had to process multiple requests at the same time. As a first step, the web server must be checked if its running an older hardware. This can affect the way it is dealing with the process requests. In some cases, network ports which are not large enough to handle the number of connections can also cause the server to slowdown. Large databases, VPN connections, antivirus eat up the resources of the CPU and may cause the server to overload. Each detail must be analyzed before identifying the final problem.

Web server logs must be checked if it is being overwhelmed by any false requests. If that is the case, it clearly points out to a denial of service attack like the SYN flood attack. In this form of attack, the attacker keeps sending the SYN segments in IP packets to sender by modifying the source address to non-existent ones. The server continues to wait for responses which do not come and ultimately runs out of resources.

Another cause could be for the incident could be packet loss. Whenever we send a request to a website, it is split and sent as network packets. These packets are reassembled at their destination to complete the request. However, sometimes packets can be lost because of network congestion and the hardware that is used to deal with it (routers and switches). Because of this, the packet request has to be sent again which would delay the whole process.

***Mitigation Strategy:***

The first step involves checking if the web hardware is in a good condition to handle all the excess data that passes through it. If the hardware is old, replacing it with a new one will benefit greatly to improve the process speed. The CPU and RAM must also be updated to handle all the operations on the server. Any specific processes which are slowing the system must be checked and analyzed. Network ports which are large enough to handle the number of connections must be used. Logs must be monitored regularly to check for any errors and discrepancies.

In case of any denial of service attacks, care needs to be taken to identify the problem and applying the optimal solutions. Firewalls must be configured to handle incoming and outgoing traffic. Any flooding requests must be immediately blocked. All the latest service packs must be installed and server should have a strong TCP/IP configuration. Intrusion Prevention System must be used to check and control suspicious intrusions. Permissions must be restricted and user authentication must be employed in giving access rights to the server.

**Threat 4:**

***Incident:*** I keep getting “Undeliverable message” about emails I didn’t send

***Threat:*** Social Engineering attack - Phishing

The employees are getting “Undeliverable message” about the emails which they did not send. It can be inferred as a form of social engineering techniques known as Phishing

***Causes:***

Phishing is one of the most common form of tactics used by the attackers to extract sensitive information from the users, often in the disguise of a trustworthy entity. In this case, the employees have been receiving emails from unknown sources faking as legitimate messages. The employees may even be asked to disclose personal information, which might include their usernames and password, credit card information, masquerading as a means to validate their credentials. Sometimes, these email messages may even contain malicious links if clicked can install several kinds of malwares on the targeted system. The users may also be tricked into believing that the links to these spoofed websites are legitimate by use of misspelled URLs. Images can be used in place of text to bypass the filters. Once the employees click and visit the phishing website, it could form as a basis for even more attacks like Cross Site Scripting and malicious downloads.

***Mitigation Strategy:***

*Updating Employee Policies:* Strict policies must be set in place that will guide the employees in dealing with such emails.

*Anti-Phishing filters:* Anti phishing filters must be set in place to scan for any phishing emails and notifying the users.

*User Authentication:* As the Sydney branch has a mail server, a two-layer authentication mechanism can be used to access emails. The employees must have a separate login mechanism while accessing mails through the server.

*Email Authentication:* Email authentication allows ISPs to identify the sender of the email. The mail server can be configured and setup to sign all the outbound emails.

**Threat 5:**

***Incident:*** My desktop is getting frozen ever so often

***Threat:*** Computer Virus

One of the possible threats for the desktop freezing can be attributed to some kind of computer virus infecting the system. It can any malicious software program that has entered the network by exploiting the security vulnerabilities in the system.

***Causes:***

There can be several causes of a desktop freezing. It can be an environmental issue like the overheating of the system. It may also be some kind of driver corruption which can lead to hardware failure. In most of the cases, a third-party software can be the most common cause of a system freeze. However, if we look at it from the aspect of a potential threat, it always points out to some kind of computer virus injected into the system without the user’s knowledge.

A computer virus is a malicious software program if when executed infects the system by replicating itself and modifies other computer programs to insert its own code. The damage a virus causes can be varied. It can range from normal freezing of the desktop to devastating outcomes like shutting down the entire network.

There are several possibilities to how the virus has infected the employee workstations. This incident can be looked in relation with another incident wherein the employees are getting unknown emails claiming “undeliverable messages”. The emails may have been used to send malicious attachments spreading the infection to other computers on the network. Proper care needs to be taken in analyzing the whole scenario and suggesting the optimally solutions.

However, the effects a virus can cause can be very damaging. As all the workstations exist in the intranet, the virus can spread quickly to other systems within this network and compromise the database server as well. The attacker can access the database server and use it to gain sensitive data about the company’s assets and its clients. If this goes unchecked, it could lead to catastrophic results that can be hard to rectify.

We can look at the example of one of the devastating viruses in history, CodeRed. This virus targeted computers with Microsoft IIS web servers. It slowed the system by eat8ing up into its resources and replicating itself. And later on, launches a DOS attack on several IP addresses further allowing backdoor access to the server. It caused a damage of $2 billion in productivity. Affecting more than 2 million servers. (Dean,2012)

***Mitigation Strategy:***

The primary mitigation strategy against any computer viruses is to have a strong antivirus software installed on the system. All the employee workstations including the servers must be provided with latest updates of the antivirus solutions. All security patches must be applied and scans must be performed and monitored regularly.

System logs must be checked regularly for any errors and discrepancies. Policies must be set in place to not open any email attachments from unknown senders. Systems must be updated with latest service packs. System hardware must be checked regularly for any damaged parts which are over heating the system, and they must be replaced quickly. Data should be backed up at all times in case of emergencies such as data loss. Furthermore, the system that is facing these constant freezes must be isolated from the network and checked for any infections or damaged parts.

**Threat 6:**

***Incident***: For some reasons, our company website is often unavailable.

***Threat:*** *DDoS attack on the DNS server*

The website must have crashed because of a distributed denial of service attack on the DNS server. The attackers might have overwhelmed the server with false requests making it to crash eventually.

***Causes:***

The Sydney branch has a DNS server that contains a database of public IP addresses and their hostnames. The DNS server (Domain name system) is used as a translating methodology to resolve the common names to IP addresses as requested. If the DNS server cannot find the right IP address for the host name we entered, the website will not load.

The above incident can be inferred as a form of DDoS attack that might have happened on the DNS server. DDoS is short for Distributed denial of Service. In this kind of attack, thousands of zombie computers in a botnet are used to overwhelm the server with false requests. These computers are remotely controlled by the attacker. The attacker uses these computers to send thousands of fake lookup requests to the DNS server. These requests may even have a spoofed source address and configured to receive more data from the server. The goal is to overload the DNS server which will slow down its functioning and crashes it. The DNS server at the Sydney branch might have been at the receiving end of such an attack.

There have been several cases of similar DDoS attacks that have happened over the years. In one such case, Britain’s HSBC, one of the largest banks in the world, faced a similar situation. The bank’s website was down for a long time disrupting its normal online operations. In another similar incident, the myDoom worm attack (considered one of the most devastating DDoS attacks) shutdown the website of the SCO group (UNIX Software maker) crippling their entire network. (Jamaluddin, A. (n.d.), 2017)

***Mitigation Strategy:***

The most basic measure to counter such a threat is to have a strong antivirus program running on the server. This can protect against any malware that attempts to change the DNS server settings. However, this can only act as a first line of defense.

Configuring the firewall will be the second layer of defense against the DDoS attacks. Monitoring the traffic can be done with the use of this firewall. Placing the firewall after the router will be essential in filtering out any malicious packets. Flooding of packets can be stopped by blocking them at the firewall itself. Two types of filtering happen at the firewall, Ingress filtering and Egress filtering. Ingress filtering is used to validate the authenticity of the inbound frames. If the frames are from a trusted public IP address, they are allowed to pass through. Egress filtering also works the same way in validating the outbound frames. By using such filtering techniques, we can reduce the risk of false requests that overwhelm the server making it dysfunctional.

However, care needs to be taken to monitor the security logs regularly to check for any discrepancies. Firewalls cannot distinguish between malicious and legitimate users. Furthermore, certain DDoS attack vectors like HTTP floods are composed of millions of legitimate sessions. Firewalls may only examine individual sessions rather than thousands of concurrent sessions. This will make identifying the malicious packets even more difficult.

Load balancers can be used to detect the DDoS attacks.

Another layer of protective mechanism that we can add to mitigate the flood attacks is the Intrusion Prevention System. A Network based IPS (NIDPS) can be used after the firewall to enhance security. It can also be used to protect against any unauthorized usage. The NIDPS analyzes the protocol activity to monitor for any malicious traffic. Physical security zones are created which, in turn, allows the network to demarcate between good and bad traffic. Several kinds of hostile traffic like viruses, worms, Trojans can be stopped with the help of the NIDPS.

NIDPS works on a set of pre-defined rules. When an event occurs, appropriate action is taken based on these set of rules. Commonly, three types of detection methods are used with the NIDPS,

* Signature Based Detection, based on predetermined and preconfigured attack patterns
* Anomaly Based Detection, wherein a baseline is created on average network conditions
* Protocol State Analysis, by comparing and checking for any deviations in the protocol states

These three layers of protection can greatly enhance the security of the DNS server and make it function optimally. (Alonso,2004)

**Part II – Application and Network Based Attacks**

The Sydney branch has a mail, web, DNS and 2 database servers. Securing these servers is of paramount importance to the organization as they form the critical part of its network infrastructure. In the event of any of these servers being compromised, it will cripple the whole functioning of the organization. These servers are vulnerable to several types of application and networking based attacks. Some of the vulnerabilities can be reflected by the complaints of the employees in the previous section.

Securing these servers starts with ensuring the physical security of these devices. It can be done by keeping the servers in a separate room called the Server room, and provide constant vigilance with the help of CCTV operations and biometric scanners to restrict and moderate user access. This can help against social engineering attacks like tail-gating and shoulder-surfing.

Some of the possible attacks on these servers and their counter measures is discussed below.

**Securing the Web Server:**

A Web server is used for hosting the web applications, and its configuration plays a crucial role in the web application’s security. For an export company, web security forms the most critical part to conduct its business online. Furthermore, the company needs its employees to access its internal network via remote access and this makes it more important to have a heightened security for its web server.

Web servers commonly come within the most targeted zone of the attackers for the kind of sensitive information they host. For example, if the virtual directories are not configured correctly, it can lead to unauthorized user access. A port that is overlooked can become an attacker’s front door entry through the network.

**Threats and Analysis:**

Some of the threats that can occur to the web server includes both application as well as networking based attacks.

***Cross Site Scripting (XSS)***

Happens when the attacker takes advantage of web applications that accept the input from the users without any validation and later presents it back to the user. It injects malicious scripts into web application server to direct attacks at unsuspecting clients. In this way, the company’s web server can become a platform to launch attacks on other computers that access it.

HTTP header manipulation can be used as a launching vehicle for attacks like Cross Site Scripting (XSS).

***Directory Traversal/ Command Injection***

Normally the web server users are restricted to the root directory. Users may not be able to access higher level directories apart from the sub directories. Directory Traversal is a way of gaining access to the restricted directories by giving malformed inputs and exploring the vulnerabilities in the system. Command injection can be used by the attackers to view confidential information by entering commands to execute on the server. In this way, the company’s sensitive data can be accessed and used by the attackers.

***Drive by Download***

In this type of an attack, the client computers may get compromised simply by accessing a web page. Attackers inject malicious content into the web server which will allow them access to the server’s operating system. They can then avoid visual detection by crafting a zero-pixel IFrame (inline frame). When the client’s browser accesses the web server, it downloads malicious script which instructs the computer to download malware. This kind of attack can be extremely detrimental in maintaining a good client relationship. It will further affect the reputation of the company at large.

***Denial of Service (DOS)***

Denial of Service is one of the most common form of attacks that is used to target the web servers. It can cripple the entire networks and stop them from performing its normal operations. In this type of an attack, the server will be overwhelmed by multiple service requests and will become overloaded and unresponsive. As result of this, even legitimate requests from the clients will go unanswered.

A DOS attack can occur in multiple ways.

* In a Distributed denial of service attack, thousands of zombie computers in the botnet will be used by the attacker to overwhelm the server.
* In a ping flood attack, the ping utility is used to overwhelm the server by sending large number of echo request messages.
* In a Smurf attack, the originating address of the ping request is changed to appear as if the target computer is asking for a response from all the systems in the network.
* In a SYN flood attack, the attacker modifies the source address of each IP packet to addresses that do not exist. The server receives false requests and keeps more lines open for responses. In this way, the server runs out of its resources and stops responding to the legitimate requests from the clients.

In a related history, the myDoom worm attack on the website of the SCO group (UNIX software maker), was intended to be a Distributed DOS attack. The attack shutdown the website of the company which forced them to redirect their traffic to a new website. The myDoom worm is considered to be one of the fastest spreading email virus ever released.

*Vulnerabilities*

Some of the vulnerabilities that can be lead to DOS attacks are,

* Server is unpatched
* Server has a weak TCP/IP configuration

*Countermeasures - Firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS)*

The counter measure for a DOS attack starts with installing the latest software patches and system updates. Hardening the TCP/IP stack will close the vulnerability of a weaker configuration.

Using firewalls can be one of the most effective method to reduce the chances of a DOS attack. After the packets pass through the Sydney router, we can use an external firewall as a first layer of defense between the router and the web server. The network traffic can be monitored with the help of this firewall. This can be done by configuring the Ingress and Egress filters to allow a secure communication channel. In addition to this, personal firewalls should be installed on all the workstations on the company intranet.

Installing a firewall is only a starting step in ensuring a secure server. Security administrators must work overtime to maintain a proper working mechanism. Monitoring of the firewalls need to be done on a monthly basis. Log monitoring plays a crucial role in checking for any discrepancies in the network traffic.

Load balancers can be used to detect and prevent these attacks.

We can add another layer of protection to this environment with the help of the IDS and the IPS. Using an NIDPS (Network-Based Intrusion Detection and Prevention System) will add another layer of depth in monitoring network traffic. Any false requests which have gone unnoticed during the filtering at the firewall can be monitored and rejected with the help of this system. Furthermore, we can detect and prevent the intrusion of any malicious programs into the network if such a system is in place. (Threats and Counter measures, 2017)

***Attacks on Access Rights – Elevation of privileges***

Access rights are privileges to access hardware and software resources that are granted to users. These attacks can be of two types, Privilege Escalation and Transitive Access. Privilege Escalation occurs by exploiting a software vulnerability to gain access to secure data.

*Vulnerabilities*

Some of the vulnerabilities that make a web server susceptible to such kind of attacks are to over privileged process and service accounts.

*Counter measures*

Running the processes with least privileged accounts is a way to counter the elevation of privileges.

**Some other recommended measures to ensure Web Server security:**

*Patches:* Install all the security patches and system updates.

*Remote Access*: As the company allows its employees to have access to the intranet while on travel, and to allow work from home and during conferences overseas, there is a strong necessity to maintain a secure remote connection. This can be done by using tunneling and encryption protocols. Security tokens can be used to enhance server security. Along with that, limiting the remote access to only specific accounts and IP’s can further add up to the security infrastructure.

*Server side scripting:* It is a good practice to have the website files and scripts put on a separate partition on the hard drive rather than the operating system. All unnecessary services should be disabled to boost server performance.

*Permissions*: As mentioned above, permissions and privileges must be restricted, and only authorized users must be given access.

*Server log Monitoring:* Web server logs must be stored in a separate area and monitored frequently for any discrepancies. Any strange log entries must be taken into consideration and checked thoroughly.

**Securing the Database Server:**

A database server is a data warehouse to store and maintain data. It performs multiple tasks which include data storage, analysis, archiving and several other non-user specific tasks. As the company has a database server for the Sydney main branch, it can be used effectively to deal with a lot of data and information. Ensuring its security is critical in maintaining a strong client-server relationship.

In a database network, the client executes SQL requests to the server. Many configuration weaknesses can be exposed by the attackers. For example, the database server can be exposed by using an insecure web application. An invalidated application which exceeds its privilege rights can put the database server at a persistent risk.

As mentioned in the network diagram, the database server is placed along with the department workstations within the internal protected network of the company.

**Threats and Analysis**

The Database server can be targeted by exploiting its configuration and application level vulnerabilities. Some of the threats that can happen are listed below.

* SQL injection
* Eavesdropping
* Unauthorized Server Access
* Password cracking

***SQL injection:***

SQL means a Structured Query Language. It is used to manipulate the data that is stored in a relational database. SQL injection is a form of attack wherein the SQL servers are targeted by introducing malicious commands. The attacker takes advantage of the vulnerability in the web application input validation mechanism and uses it to insert malicious commands in the database.

*Vulnerabilities*

Some of the vulnerabilities that can be used for SQL injection include:

* SQL commands which are unsafe to use and dynamically constructed
* No proper input validation while accessing the web application
* Privilege escalation while logging into the database
* No proper permissions to limit the application’s login to the database

*Counter measures*

Some of the countermeasures against SQL injection attacks on the database server include,

* Controlling and sanitizing the user input before it is utilized for SQL queries
* Permissions to be the database should be restricted. Direct table access should not be provided. A separate SQL server login with authorized user access should be used within the company.

Certain SQL parameters should be used by the company’s network that stops the injected code to be treated as executable statements within the database. (Cherry, 2015)

***Eavesdropping – Man in the middle attack:***

The database server contains sensitive information about the company which includes employee information, assets, transaction among many. This kind of information if fallen in the wrong hands can lead to catastrophic results. Network eavesdropping can be a major threat to steal such sensitive information.

A man in the middle attack makes it appear as if the server is communicating with the client but in reality, a third-party attacker will be able to interfere and manipulate the data between the sender and the receiver. Another form of the man in the middle attack is a replay attack wherein the copy of the transmission is made before sending it to the recipient for later use.

*Vulnerabilities*

Some of the vulnerabilities which can be exploited by the network eavesdroppers include,

* Lack of a secure communication channel
* The way user credentials are passed to the database. For example, authenticating the users without a proper server certificate.

*Counter measures:*

* If the company installs a server certificate on the database server, it can ensure an authenticated user access through SQL credentials
* An IPSec encrypted channel can be used between the web server and the database server

A database server certificate can be used. This can be done to protect sensitive data by using an SSL connection between the web server and the database server. (Threats and Counter measures, 2017)

***Unauthorized Server Access:***

Ensuring a restricted user access to specific client and employee computers in order to prevent unauthorized user access.

*Vulnerabilities*

Some of the vulnerabilities that can lead to unauthorized server access happen,

* When the external firewall fails to block the SQL Server port
* When there are no proper filtering policies for IPSec and TCP/IP

These vulnerabilities can be exploited by the attacker to send carefully crafted packets to listening ports in order to gather Server information. Several different hacking tools can be used to establish a connection to the server.

*Counter measures*

To counter the attackers from exploiting these vulnerabilities, we can

* Make sure that within the intranet of the company network, direct access is restricted to any unauthorized hosts. This can be done with the use of IPSec and TCP/IP filters
* Make sure that SQL Server ports are not visible from outside the perimeter network

***Password Cracking:***

Password cracking is one of the most common form of attacks that can happen with the SQL database servers. This will allow for unauthorized user access into the company databases.

*Vulnerabilities*

Password cracking can happen because of,

* Weak passwords which contain everyday words that can be easily cracked

Attackers can use several different methods like a brute-force attack or a dictionary attack to crack the passwords.

*Counter measures*

* Strong and complex passwords must be created for the database server logging accounts
* Strong antivirus measures must be used to safeguard against any password cracking

**Some other recommended measures to ensure database server security:**

*Disable public network access to the Database Server:* As mentioned in the network diagram, the database server is separated from the remaining servers and placed within the internal protected network of the company. The end-users generally don’t need to access the database directly. We can set up SSH tunnel or VPN for the remote administrators.

*Monitor Database dumps:*  By setting up a monitoring system to detect SQL dump files which are there in public folders.

*Encrypting the Application files:* If an attacker succeeds in gaining access to the database server, encrypting the application files can ensure enhanced security.

*Restricting port access:* Use the firewall to close unused ports. Also, the server must restrict or block the ports depending on their usage.

**Securing the Mail Server:**

A mail server is a critical part of the network infrastructure without which sending and receiving emails can become a cumbersome task. The Sydney branch has a mail server which utilizes its functions to transfer emails. These servers can be broken down into two categories, Outgoing mail servers and Incoming mail servers. Outgoing mail servers are known as SMTP servers (Simple Mail Transport Protocol) whereas Incoming mail servers come in two categories, POP3 or Post Office Protocol version 3 and IMAP or Internet Message Access Protocol.

Normal protection for mail server includes a strong antivirus and antispam solutions. These are the first line of defense against any attacks on the mail servers. The employees working in the organization have also complained about receiving “Undeliverable message” about emails that they didn’t send. This is a server related issue which needs to be sorted out quickly. Some of the attacks and threats that can exploit the vulnerabilities in the mail server is discussed herein.

**Threats and Analysis**

***Buffer Overflow attack:***

A Buffer Overflow attack happens when a process attempts to store data in RAM beyond boundaries of fixed-length storage buffer. Data overflows into adjacent memory locations. Attackers can send very large files in emails that do not fit in the memory buffer of the email client. Attackers can also change return address of the memory location of code and redirect it to memory address containing malicious code. (What is buffer overflow?, 2017)

*Vulnerabilities*

A vulnerability exists when the server processes DNS lookup requests. The server cannot allocate memory correctly in the SMTP and Exchange Routing Engine components. This vulnerability can be used by the attacker to crash the SMTP service causing a denial of service like condition.

*Counter measures*

Security patches must be updated regularly to counter such attacks. TCP traffic must be regulated at the external firewall on certain ports that might affect the systems.

***SMTP Relay attacks:***

SMTP relay allows users to send emails through the mail server. Open relays can be a problem as attackers can use the mail servers to send emails which contain malware or other suspicious code under the guise of an unsuspecting open relay owner. The client machines can get infected with the malware which could lead to catastrophic results.

*Counter measures*

Mitigating an SMTP relay attack can be done in two ways.

* By disabling/controlling the SMTP relay on the email server. If we need SMTP relay then it can be enabled for only specific hosts on the server, or configured within the firewall settings.
* Enforcing authentication on the email server. We can also enable password authentication on a mail address that matches the mail server’s domain.

***Attachments – Phishing, Trojan Horse Attacks***

Attachments are files that are coupled to email messages. Malicious attachments are commonly used to spread viruses and Trojans when they are opened. Employees may unknowingly open these email attachments which would infect the whole system. The attackers can try to obtain sensitive information by masquerading as a separate entity in a form of attack known as Phishing. Some of the Trojan horse attacks come as email attachments with file extensions that look like an image file or a spreadsheet. Such attachments can be scanned by the mail server for malware and block any dangerous filetypes, but it cannot be a reliable solution as they are vulnerable to zero-day exploits.

*Counter measures*

Having a viable antivirus, antispam software installed on the server will be the first step in ensuring a secure mail transfer. Patching them with regular updates is essential to maintaining stronger security. Employee policies must be put in place to guide them in dealing with these attachments. As a rule of thumb, one should never click or open these attachments which seem suspicious.

***E-mail header disclosures:***

If both the client and the mail server are configured with defaults, an attacker exploit this by finding important information about the internal IP address of the client system, and the software versions of the client as well as the mail server along with its vulnerabilities. They can also find out Hostnames which can be used to gain information regarding the network naming conventions.

*Counter measures*

To prevent such information disclosures in email headers, we need to rewrite the headers by configuring the mail server or the firewall by altering the information shown or completely removing it. (Threats and Counter measures, 2017)

***Malicious add-ons – Active Content attacks***

In this kind of attacks, the hackers use active HTML and scripting. ActiveX is a set of rules of how applications under the Microsoft windows operating system should share information. Active X controls can be invoked from webpages through the use of a scripting language or directly by HTML command.

**Some other recommended measures to ensure Mail server security:**

* Setting up SMTP authentication to control user access. SMTP Authentication will make the people using the user authenticate their credentials with the aid of a username and password to send email. This method can prevent open relay, and misuse of the server. As the mail server has a routed IP address, this configuration can be extremely beneficial.
* Limiting the connections to protect against DOS attacks. This would provide a mitigative mechanism to counter spam floods and DOS attacks.
* Blocking bogus senders by activating Reverse DNS. Several messaging services use DNS as a tool to verify the sender’s email domain. A reverse DNS lookup allows the mail server to verify whether the sender’s IP address matches the domain and the host names which were submitted.
* Blocking Spammers by maintaining a local IP blacklist. This can be an effective way to prevent unwanted internet connections from intervening with the server.
* Encrypting POP3 authentication. As passwords are transmitted in clear text through the mail server, encrypting them can provide an added layer of security.

**Securing the DNS Server**

The DNS Server (Domain Name System) contains a database of public IP addresses and their associated domain names. They are used to translate the host names to IP addresses as requested. The company’s Sydney branch has a DNS server, and steps need to be taken to provide to the DNS caches. As mentioned in the network diagram, the DNS server is placed along with the web and the mail server in a separate DMZ network. Extra layers of protection will be added to enhance its security based on the requirements.

Attackers can use many vulnerabilities within the network to compromise the DNS server. As DNS attacks involve malware which can change the server settings, a strong antivirus solution will act as a first line of defense Attackers can use many vulnerabilities within the network to compromise the DNS server. Some of these attacks and their mitigative solutions are explained below.

***DNS poisoning***

DNS poisoning is one of the most common attacks that can affect the DNS server. In this kind of attack, the attacker substitutes DNS addresses to redirect the computer to another device. This can occur in two locations, the local host table or the external DNS server. When this happens, the clients will be routed to a wrong website and they may not even know that they are accessing a fake website. This could eventually lead to further devastating attacks like phishing wherein the user login credentials and other such valuable information can be stolen.

*Vulnerabilities*

The attackers make use of the vulnerabilities in the DNS caching system. Every information that is accessed is stored locally as DNS cache on the server for a faster reference. DNS poisoning happens when these caches are compromised.

*Counter measures*

One of the main challenges in dealing with DNS poisoning is that it is very to detect. We can only know of it after the TTL (Time to Live) expires on the cached data. Or, in another case, if the network administrator checks the problem. Sometimes, it could take days for the server to solve the issue as it entirely depends on the duration of the TTL. The best remedy against such a type of attack is to have a regular program updates along with setting short TTL times. Also, care needs to be taken to clear the DNS caches regularly. (Liska,2016)

***DDoS attacks/DNS Amplification for DDoS***

A Distributed denial of Service can be used against the DNS server to crash it and preventing the users from accessing the web. This is evident from the employees complaining that the company’s website is often unavailable. This could be a DNS server related issue that needs to be resolved.

DNS Amplification is basically not a threat against the DNS server, but instead a means to exploit the openness of the DNS service which would aid the attackers in a more strengthened DDoS attack. The attacker could use thousands of botnet computers to send false requests. By using the amplification method, the attacker will try to open the DNS server by sending in thousands of lookup requests. These requests are configured in such a way that they maximize the return of data from the server. The server will be compromised and ultimately it will crash. (NorthCutt, 2005)

*Counter measures*

Configuring the firewall can act as a first line of defense against such a threat. In this way, artificial packets that are trying to flood the system can be dropped. If the attack is on a smaller scale, the IP addresses can be blocked. Increasing the bandwidth of the DNS server can also help in absorbing the attack.

**Some other recommended measures to secure the DNS server:**

* Setting access controls on DNS registry and system entries. This will allow only the accounts that require access to read and change the registry or system settings.
* Enabling DDNS for only the secure connections.

**Part III. Administering Secure Networks**

**I. VLANs and NAT technologies**

***Scenario:*** The company’s requirements include that its employees have access to their computing devices over the internet. They also mention that some employees may have to on the move between different departments or floors and advised to relocate their desktop/devices outside their department areas.

**Analysis:**

Administering a secure network based on the company’s needs can be done with the aid of VLANs and NAT technologies. Firstly, we look at the current requirements and examine how VLANs can be implemented to achieve a secure network and allow employees access to internet and other workstations.

**VLAN – Virtual Local Area Network:**

A Virtual LAN (VLAN) is grouping of network devices that is not restricted to a physical segment or switch. It is used to segment network by separating multiple devices into logical groups. VLAN allows scattered users to be logically grouped together even though physically attached to different switches. They can be configured on most witches to restructure broadcast domains. This domain allows a group of network devices to receive LAN broadcast traffic from each other. We can create multiple VLANs on a single switch or even create one VLAN across multiple switches. Switches basically use MAC addresses to identify devices.

The company advised to relocate some of its employee devices so that they can move among various departments on multiple duties. However, by administering the VLAN technology we can resolve this issue without physically relocating the employee devices.

VLANs help in greatly reducing the cost of moving employees from one location to another because changes can be made at the switch itself. Physically moving a device does not necessitate the changing of the IP addresses of the devices or their subnets because VLANs can be spanned across multiple switches. Even if a group of computers were moved to another department, the switches can be reconfigured to include these ports in the previous VLAN.

***Using Dynamic VLAN for the employees who move between various departments:***

Depending on the switch and the switch management software, VLANs can be configured into types.

* Static VLAN
* Dynamic VLAN

Static VLANs are configured port-by-port. Every port is associated to a specific VLAN. The administrator can also manually type in the mapping of every port and VLAN. This kind of setup can be extremely useful to control the movement of users within the network. By use of the network management software, the administrator can configure each switch port with a VLAN membership. This depends on the VLAN that the host wanted its membership. In this case, the actual physical location of the device does not matter. This allows for a logical grouping of different devices in the same broadcast domain.

Our current scenario requires the use of a dynamic VLAN. A dynamic VLAN can automatically find out a node’s VLAN. It uses a software database of MAC address-to-VLAN mappings that is created manually. The MAC addresses and their corresponding VLANs must be entered and maintained by the network administrative team. For instance, if we connect a node to a switch port that is not assigned, then the VLAN management database can check for the MAC address configuration to assign the switch port to the appropriate VLAN. When the employee is constantly on the move between different departments, it becomes easy to manage and configure because the switch will automatically assign them to the correct VLAN. For this purpose, a MAC address database must be set in place.

Furthermore, the VLANs can also be used to implement a physical change. If we want to divide a department into two sections of separate Local area networks, we can use the VLANs by allocating different ports on the switch to different sections. It will reduce the cost immensely from physically rewiring the whole setup.

Logically, two VLANs are created in this setup. One that consists of the DMZ which includes the servers, and the other is the internal protected network, which includes the workstations and the database servers. We use two multilayer switches for this purpose. Within the internal protected network, the employees who are on the move between various departments will have access to all the departments within this intranet.

As indicated in the network diagram, the servers and the employee workstations are physically separated and connected to different VLAN switches. By using the flexibility of the VLANs, the network administrator can make the servers behave as if they were distributed throughout the local area network. Separate broadcast domains can be setup to control network traffic. It will also provide with increased security because an attacker who targets the network has to go through a two-step process of tapping the network port and then figure out the LAN configuration. The physical layout of the LAN will be hidden from the attackers.

In addition to this, router can be used in combination with the VLAN to provide increased security. It can also be used to monitor traffic between different VLAN switches. By implementing access lists on the routers, inter-VLAN security can be greatly increased. These access lists can be used to restrict communication between separate VLANs.

Some of the advantages of using VLANs include:

* The ease with which stations are added and moved on the LAN
* Enhanced Security
* Network Traffic control
* Ease of reconfiguring the LAN

To summarize it all, by using multiple VLAN switches to connect servers and workstations we can create a network that is easy to manage and provides enhanced security. (Stallings, 2011)

**NAT technology:**

The company wants its employees to have access to the internet. The Sydney branch is also facilitated with a high-speed internet connection. By using the NAT technology, the company will be able to create a more secure connection methodology in accessing the internet. It also allows the company to connect more number of computers to the internet than it otherwise can.

NAT is short for Network Address Translation. We have a pool of private IP addresses that can be used by the company on its internal network. These private IP addresses are not assigned to any specific user or organization. These addresses function as any regular IP addresses on the company’s local network. However, routers normally drop packets with private addresses. NAT allows the private clients to access the internet by mapping their private IP addresses to public IP addresses.

The private IP addresses which can used are shown in the table below:

|  |  |
| --- | --- |
| *Class* | *Private Address Range* |
| A | 10.x.x.x |
| B | 172.16.x.x – 172.31.x.x |
| C | 192.168.x.x |

***Advantages of using NAT***

There are many advantages of using private IP addressing with NAT over public IP addressing which include,

*Conserving public addresses:* The company’s network can make use of this technology to minimize the pool of public IP addresses they use.

*Enhancing security:* It can be used as a method to hide internal IP addressing scheme from the outside world. When attackers try to capture a packet from the host, they only get to know the public IP address not the private IP address that is actually used. This provides increased security to the computers on the company’s network.

*Easy renumbering of IP addresses:* If the company decides to change its ISPs, only the outside NAT addresses are required to be changed. The private IP addresses used in the internal network need not be changed.

***Disadvantages of using NAT***

However, there are a few disadvantages of using NAT. There can be a slight delay in the company’s network as the router takes some time to create and maintain the NAT table. This table consists of both the private as well as their associated public IP addresses. Another disadvantage is the end to end IP traceability of the source IP address is lost. It will become difficult to trace a packet back to the original host computer.

**Implementation of NAT technology within the company’s network**

NAT is available in three forms,

* Static NAT
* Dynamic NAT
* Port Address Translation (PAT)

***Using Static NAT for servers in the company’s network***

In a static NAT, a single private IP address is mapped to a single public IP address. For example, the router could be configured to translate the internal private address of the web server to a single public IP address. These two addresses are mapped to maintain a channel of communication between the server and the receiving host. This is essential when clients from the outside the network access the servers for its services. All the servers in the company’s network must use static NAT as they are required to be accessed by the clients from the outside world. Static NAT provides a permanent mapping between the internal private address and the public IP address that it is translated into.

***Using Dynamic NAT for employee workstations in the company’s network***

In a Dynamic NAT, the router maps a group of private IP addresses to a pool of public IP addresses. In this case, we are not concerned about which IP the internal hosts are using. The network administrator does not need to spend time to create a one-to-one mapping between these addresses. When the employees access the internet, their private IP address will be automatically translated to any of the available public IP addresses by the router. The network administrators can define a pool of public addresses and can configure which of the internal hosts ca use the pool. As employee devices are mostly not required to be directly accessible from the internet, we can use dynamic NAT for the workstations in the various departments. Also, using a dynamic NAT can make it harder for the hackers to crack into the host systems as they will not be able to find the destination IP of the host computers. This essentially enhances the security of the employee workstations.

***PAT or Port Address Translation:***

PAT is a special form of NAT. It can also be referred to as NAT overload. Sometimes, depending on the number of public IP addresses available we can configure the NAT overload. PAT allows several internal private IP addresses to use a single public IP address. This is done by mapping the internal IP addresses to the single external IP address but with different communication ports. If the ISP provides only a single public IP, PAT acts as a useful mechanism to access the internet.

***Subnetting:***

Subnetting is used by create a logical subdivision of the IP network. The private IP addresses are allocated among the various devices, including the servers and the workstations, through subnetting. This will provide security benefits. Tracing a problem on the subnet will also become much faster. Wastage of IP addresses is generally reduced. Furthermore, it provides with a greater deal of flexibility. The number of subnets and hosts on each subnet can be customized and easily changed based on the company’s requirement.

***Summary of NAT implementation:***

The network world, as it is, is transitioning from IPv4 to IPv6 rapidly. This will allow us to have an unending supply of public IP addresses (2^128 in total). However, NAT is an interesting technology if administered correctly can provide valuable benefits. It also inadvertently acts as a sort of a protection to the systems working behind the router. All the private services running within the network are inaccessible to the outside world. This will essentially add another layer of security to the existing network infrastructure. However, additional care needs to be taken in protecting the multiple services that are accessible to the outside clients, which includes the servers within the company’s network. (Whitman, 2016)

**II. Log Management**

A log is a record of events that occur. Almost all the applications that run on a system or a server generates logs. These logs contain important information which helps to analyze how the system is currently operating, and to look at the past events that have occurred during the whole system processes. This becomes the most crucial part of identifying the problem within the system.

Several types of networking issues that are affecting the company have been discussed in the previous sections. Many new devices and additional software measures were suggested. Almost all these devices including the existing servers and systems generate logs which need to be monitored carefully to assess the key issues plaguing the network. Based on the devices suggested, different kinds of logs are generated which can be analyzed below.

**Analysis:**

***Firewall logs:*** As one of threats suggested a DDoS attack which could be mitigated by adding an external firewall to protect the servers, we can use this log data to determine whether new IP addresses are attempting to probe the network, and if stronger rules are required to block them.

***NIDPS:*** The NIDPS is also suggested as a second layer of protection against the DNS server attacks. This system records a detailed security log information on suspicious behavior as well as any attacks that are detected. These logs also record the actions taken by the NIDPS to counter these attacks.

***Web server logs:*** One of the incidents suggest a web server overload as a possible threat to be resolved. These logs can provide valuable information about the type of attack that can help in configuring the server for enhances security.

***VPN concentrators:*** As VPN concentrators are suggested to provide a secure VPN connection for remote access, these logs can be monitored for any attempts to gain unauthorized access to the company’s network.

***Email server:*** These logs can give us an indication of the malware and phishing attacks that were attempted with the use of malicious attachments. One of the threats that was identified can be analyzed by looking through this information.

Furthermore, some security logs can give us an indication of the type of attacks that might have happened in the network. These can be analyzed by looking through the access logs which provide information regarding the requests for specific files, or the audit logs which record the user’s actions.

However, manually going through these logs can be a cumbersome and time-consuming task considering the large volumes of data that needs to be dealt with. Generating these logs, storing, analyzing and disposing of its data can be achieved by simpler means using a Centralized log analyzer. It will have a easy to use interface that allows us to access all the log data from one central location.

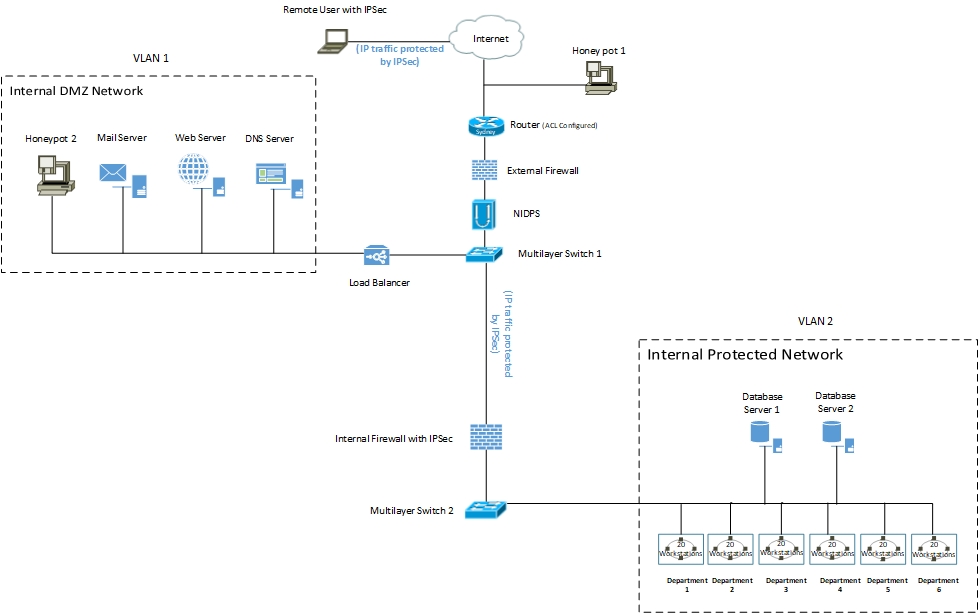
There are many benefits to using a Centralized logging mechanism which include,

* Having a central location to store the log data from several devices
* Specific alerts can be generated depending on the metrics we allow to be defined within the logs
* Important data can be backed up with low cost
* Easy searching
* Retention policies can be enforced on the logs stating the time period they are available
* Sharing the log information will become much more simple and easy
* We can also grant specific users with a login access without granting them any server root access

All in all, if the company takes advantage of implementing a Centralized Log Analyzer, it will help it immensely in making its network into a more dynamic, profitable and secure environment.

**Part IV. Firewall Planning and Design**

1. **Proposed Firewall Diagram**

****

1. **Explanation of the configuration of the various devices in the Network diagram**

The network diagram gives us an understanding of the way the network operates. We can look at the various devices that are used and what their advantages are in providing a secure network environment in the section below.

**Internal DMZ network:**

All the servers, excluding the database servers, are located within this zone. As these servers require outside access, a Demilitarized Zone is used for this purpose. The zone is provided with multiple layers of security starting from the Access control lists, the external firewall, the NIDPs and the load balancers. The placement of these devices can help ensure a secure DMZ.

**Firewalls:**

***What are firewalls?***

As suggested in the previous sections, the use of firewalls can be necessitated to monitor and control incoming and outgoing network traffic. Firewalls can add an extra layer of protection to the existing network architecture. They can be a single computer or a set of two or more computers that cooperate to perform the firewall function. In simple words, firewall acts as a sort of barrier between the internal network of the company and the outside world. They can be categorized into two types, Network firewalls and Host-based firewalls. Security protocols can be set at the firewalls to control the flow of the traffic that comes and goes through it.

**Firewalls used to protect the company’s network:**

We use two firewalls to protect the company’s network which include,

* An external firewall that acts as a first line of defense to protect the servers.
* An internal firewall which adds another layer of protection to the intranet of the company’s network which includes the workstations and the database server.

***External Firewall:***

The external firewall is placed at the edge of the network, just inside the boundary router. This forms a critical part of protecting the servers which are placed within the DMZ (Demilitarized Zone). These servers, which include the Web server, the mail Server and the DNS server, require external connectivity and access to its resources from the outside. The external firewall provides a measure of access control and protection for these servers based on their need for external connectivity. All the traffic passing through this firewall can be filtered and unwanted traffic can be blocked or rejected. The company can place local security policies to allow only authorized traffic through the firewall. This includes the IP address ranges, certain applications types and content types.

User authentication can be used to allow access to the servers. Packet filtering can also be done to control incoming and outgoing packets.

***Internal Firewall and implementation of IPSec:***

The internal firewall is placed after the VLAN switch that is connected to the DMZ (Figure 2). Primarily, it can serve two purposes.

* It adds more stringent filtering capability to protect the workstations and the database server. If a malicious packet escapes the filtering of the external firewall and the NIDPS, the internal firewall may be able to filter it out from reaching the workstations.
* It can provide a two-way protection with respect to the systems in the DMZ. If one or more of the servers in the DMZ is compromised, the internal firewall acts as a barrier in protecting the workstations. Any existent viruses, worms or rootkits that are lodged in the DMZ may not be able to penetrate the internal firewall to reach the workstations of the company. In the same way, the internal firewall also protects the DMZ from any attacks from the internal protected network. For example, in one of the threats mentioned, the employees may have unknowingly opened a malicious attachment and infected their system. The internal firewall can filter out such malware from reaching the servers in the DMZ.

***Virtual Private Network (VPN) and IPSec to secure remote access over the internet***

We have implemented a VPN setup to provide a secure communication channel between the internal protected network and the employees who are accessing it from the outside world. Some of the company’s employees like the sales representatives are usually required to travel. Some employees may have to attend conferences overseas. The company is also considering to allow employees work from home. This is done by allowing remote access through the internet.

However, use of a public network may expose these systems to eavesdropping and allow entry of unauthorized users. To counter this, the use of VPN is suggested as mentioned in the diagram. VPN uses encryption and authentication to provide a secure channel of communication. IPSec is the most common protocol mechanism used for this purpose.

IPSec is short for IP Security. The primary feature of IPSec is that it supports varied applications that can be encrypted and authenticate all the traffic at the IP level. IPSec is extremely beneficial to offsite employees as the data transfer that happens from outside the network will be secure. IPSec is an end-to-end communication. In this case, the remote users also have to have IPSec installed on their systems. Within the network, IPSec is implemented in a separate box behind (internal to) the firewall. The VPN traffic passing through the firewall in both directions will be encrypted. However, as the data is in an encrypted form, the firewall will be unable to perform its filtering function and other security functions such as access control, logging or scanning for viruses.

All in all, IPSec can be a cost-effective mechanism to provide a secure tunnel of communication with the offsite employees and clients. (Stallings, 2011)

***Host-Based Firewall:***

In addition to the above suggested methods, host-based firewalls can be used to add another layer of depth to the overall security. A host-based firewall is a software module used to secure an individual host. The functions remain the same as any normal firewall, but it can work on a single host. If the company is willing to provide additional costs, such a mechanism can be implemented on each of the workstations and servers within the network.

**Load-Balancers:**

As illustrated in the diagram, a load balancer is placed between the router and the servers within the DMZ. It is used to distribute network as well as application traffic across the servers to avoid overloading. This will improve the performance of the servers greatly. Furthermore, load balancer can be used to detect and prevent the DoS attacks on the servers. The DNS server has already faced a threat of DDoS attack as mentioned before. The load balancer can act as added layer of defense in countering such attacks. In addition to this, they can also hide HTTP error messages or remove server identification headers from HTTP responses. This will deny the attackers from gaining information about the internal network.

**Switches:**

Two switches are indicated in the network diagram. These are multilayer VLAN switches. One switch connects to the servers within the DMZ. It is located after the external firewall and NIDPS. The second switch is used for the internal protected network. These switches allow the network into two logical groups, the DMZ and the internal network.

**Access Control Lists (ACL):**

ACLs act as a kind of network filter to all the incoming and outgoing traffic through the router. By configuring the ACLs, we can permit and restrict data that enters or leaves the network. It can also be used to set permissions and priorities while transmitting data between the Sydney and the Brisbane branch. It can provide a basic level of security to the existing system infrastructure.

**Honeypot:**

Honeypots are decoy systems. They are used to lure the attackers away from the critical systems. Honeypots can be designed in such a way that any attack against them is made to seem successful. While this happens, the administrators will have the time to mobilize and log and track the attackers without ever exposing their true critical systems.

Honeypots are deployed in two different locations as illustrated in the diagram.

*Location 1:* This honeypot is located outside the external firewall. It is useful to track any attempts that are made to connect to unused IPs within the company’s network. As the honeypot here will attract many potential attacks, it reduces the alerts issued by the firewall and the NIDPS sensors easing management burden. However, a honeypot at this location cannot detect any attacks from inside the network as the firewall filters traffic in both directions.

*Location 2:* This honeypot is located within the DMZ. However, care needs to be taken by the security administrator to assure that the other servers in the DMZ are secure against any activity generated by the honeypot. If the administrators

We can also use a fully internal honeypot within the internal protected network. The main advantage of this location is it can catch internal attacks. However, if the honeypot is compromised it can attack other internal systems. As we already have a three layer of protection which includes the external firewall, NIDPs and a secure IPSec channel on the internal firewall, having an extra element of protection can be implemented based on the company’s requirements.

**Network based Intrusion Detection and prevention System (NIDPS):**

The NIDPS offers a second layer of protection to the servers as well as the internal network. It is placed between the external firewall and the switch connected to the DMZ. At this location, it can analyze the incoming traffic after being filtered at the firewall. Any bad patterns such as malwares or other deviations in traffic can be detected. Unlike the firewall, the NIDPS will signal an alarm if an intrusion is detected and attempts to prevent it.

**Host based Intrusion Detection and Prevention System (HIDPS):**

Additionally, a HIDPS can be put in place on the individual devices within the internal protected network. This will monitor the inbound and outbound packets from the workstation and alert the administrators if any discrepancies are found. IT will also attempt to prevent the intrusion by dropping the packets.

**Conclusion**

Albert Einstein was quoted as saying, “Problems cannot be solved with the same level of awareness that created them.”

In the end, we can conclude that security is one of the defining factors for the long-term survival and prosperity of any organization, failing which may incur monetary as well as an adverse effect on the image of the company. Therefore, strong security measures must be planned and implemented to maintain the balance in confidentiality, integrity and authority.

**References:**

1. Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security* (Fifth ed.). Boston MA: Cengage Learning.
2. Dean, T. (2012). *Network+ guide to networks (with printed access card)* (6th ed.) Wadsworth.
3. Stallings, W. (2011). *Network security essentials: applications and standards.* Boston, MA: Pearson
4. Northcutt, S. (2005). *Inside network perimeter security.* Indianapolis, IN: Sams Pub.
5. Alonso, M. (2004). Intrusion detection system: (NIDS-HIDS). Fribourg.
6. Cherry, D. (2015). Securing SQL Server: Protecting Your Database from Attackers. Saint Louis: Elsevier Science.
7. Liska, A., Stowe, G., & Gallo, T. (2016). DNS security: defending the domain name system. Cambridge, MA: Syngress.
8. Threats and Countermeasures. (n.d.). Retrieved August 30, 2017, from <https://msdn.microsoft.com/en-us/library/ff648641.aspx>
9. What is buffer overflow? - Definition from WhatIs.com. (n.d.). Retrieved August 30, 2017, from <http://searchsecurity.techtarget.com/definition/buffer-overflow>
10. Jamaluddin, A. (n.d.). 10 Most Destructive Computer Viruses. Retrieved August 30, 2017, from <http://www.hongkiat.com/blog/famous-malicious-computer-viruses/>