Seyed Zakaria Mohseni

Network Security for Small Businesses

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communication Technology

Bachelor's Thesis

24 August 2022

Abstract

Author:	Seyed Zakaria Mohseni
Title:	Network Security for Small businesses
Number of Pages:	28 pages + x appendices
Date:	24 August 2022
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	IoT and Cloud Computing
Supervisors:	Janne Salonen, Principal Lecturer

The main purpose for this research originally stemmed from my passion for Network security and its impact on small businesses. Due to the globalization of the Internet and the shift to remote working, there are many security issues that businesses are facing in the online world right now. Threats targeting businesses that use the Internet for email, web applications, or information sharing are major targets for phishing, ransomware, and other malicious cyber activities.

Nowadays, small businesses are even more vulnerable to hackers than large brands. Because small businesses often have a much lower level of security in terms of cyber security. This study in addition to what network security is, and how to build a secure network for a small business, also discusses many Network security solutions, network security layers, and types of threats to small businesses. Also, this thesis provides guidance for selecting the right protocols and policies for network security.

Keywords: network security, cloud, data security, Security Policy, Threat, Vulnerability, small businesses

Contents

List of Abbreviations / Acronyms

CIA:	Confidentiality, Integrity, and Availability
ACLs	Access control lists
DOS:	Denial of Service
2FA:	Two-factor authentication
R2L:	Remote to User Attacks
U2R:	User to Root
ISP	Internet Service Provider
VPN:	Virtual Private Network
L2TP:	Layer 2 Tunneling Protocol
PPTP:	Point to Point Tunneling Protocol
IPSec:	Internet Protocol Security
SSL:	Secure Sockets Layer
TLS:	Transport Layer Security
VLAN:	Virtual local area network
ZT:	Zero Trust
ZTA:	Zero Trust Architecture
PDP:	Policy Decision Point

PE:	Policy Engine
PA:	Policy Administrator
PEP:	Policy Enforcement Point
CDM:	Continuous diagnostics and mitigation
PKI:	Public key infrastructure
SIEM:	Security information and event management
DMZ	Demilitarized Zone
LAN	Local Area Network

1 Introduction

The world is rapidly moving towards digitalization. and also, by increasing number of sensitive organizational information online and the interconnected nature of our daily lives in general are directly related to the exponential growth of cybercrime. But it is not just data breaches that are worrisome. Cybercrime includes phishing, malware attacks, and many other methods that cost billions of dollars to companies, governments, organizations, and individuals and damage their credibility.

Therefore, businesses that use traditional methods are doomed. The use of technology reduces costs and time for services, and this makes businesses and people in the community pay attention to digital commerce. With the increasing use of technology and the collection of personal data, the need for information protection increases. But not all businesses are actively protecting themselves against cybercrime, and on the other hand, cybercriminals are always trying to gain illegal access to electronic data stored on companies' computers or networks. The purpose of this may be to damage the reputation or damage a person or a business, or even to steal valuable data. However, cyber-attacks can target organizations, governments, individuals, or groups.

The popularity of platform-based companies in different sectors including, financial services, banking, and e-commerce has changed the ways that customers were used to interacting with companies’ services. Nowadays connectivity to the internet and maintaining an online presence is the main characteristic of modern professions. Therefore, it is very important for companies to communicate with their customers through well-designed and effective websites and update their social media pages and blogs repeatedly.

Nowadays, because jobs and businesses are going digital not only large businesses, but also small businesses are vulnerable to cyber-attacks, and also small business owners do not have the technical expertise and knowledge necessary to protect their businesses from external and internal cyber threats.

because of this reason, companies must use suitable security protocols to protect their businesses. Cyber security is the solution to protect company data and

confidential information from unauthorized access by implementing multiple security protocols against Cyber Threats. The aim of Cyber security is to reduce cyber threats in general not only for companies but also for their customers.

1.1 Research objective

Although organizations use various technological tools to protect their information assets from security threats, but the evolution of cyber-attacks is endless, this research gives an overview of the best practices in mitigating the known cyber-attacks and recommendations on how to prevent them.
The aims of this research are to reveal and define the concept of network security and threats to small business networks, to highlight different mitigating methods used to circumvent cyber threats and attacks, also to describe the methods and implement the best cybersecurity practices.

1.2 Research methodology

This thesis is written based on literature review, research papers, review of existing network security protocols and policies that can protect data in networks for businesses.
The reviewed material mainly consists of annual network security survey reports published by cyber security research institutions and consulting companies. This research suggests technology solutions to improve security and affordability for small businesses. The proposed solutions are ideally applicable under specific scenarios for small businesses.

1.3 Thesis Structure

This thesis is divided into seven chapters. Chapter 1 is the introduction, it describes the research problem, the objectives of the study, and the research methodology. Chapter 2 describes an overview of Network Security, the network security triangle, and the Network Campus Model. Chapter 3 describes small and

midsize businesses, how network criminals attack small businesses, and introduces some Common threats. Chapter 4 describes different types of cyber-attacks and Types of hackers. Chapter 5 introduces some important ways to prevent cyber-attacks on small businesses. Chapter 6 introduces DMZ (Demilitarized Zone) and DMZ design and Architecture. Chapter 7 is the summary and concludes this research.

2 Network Security

Network security can be defined as a set of rules and configurations that protects the confidentiality, availability, and integrity of data that is stored within computers and network systems. Effective network security can be managed by monitoring the software and hardware technologies that control network access. nowadays, companies are required to provide a solution to protect their customer's private data and information and save their reputation from the possible damage caused by cyber security threats, thus, the main goal of network security is to minimize the risk of cyber-attacks and shield the confidentiality of the data.

2.1 The most important basis of network security

- Protection: The first and most important thing in maintaining a network is its protection. Configure all your computer systems to the highest level of network security.
- Diagnosis: After setting up the network, the network should be checked and analyzed regularly so that in the early stages, there is a problem and network damage is prevented
- Action: After diagnosing the problem in the network, you should take the necessary steps immediately and fix the problem. Solving the network problem is very important and must be done quickly.

2.2 CIA or the network security triangle

The network security triangle, or CIA, is derived from the terms Confidentiality, Integrity, and Availability. This model is introduced and used to create information security in a network. These three components are the main components of network security.

Figure 1. Principles of Network Security.

• Confidentiality

Confidentiality mentions to the accessibility of sensitive data only by authorized persons. Access to sensitive data must be protected from those who are not legally authorized to have valuable information. Security mechanisms such as access control lists (ACLs), usernames, passwords, and encryption are required to ensure that only authorized members have access to information. Information should be considered according to its importance and the potential damage that may cause in the process of retrieving information. Security measures should be implemented accordingly to ensure that unauthorized outsiders cannot disrupt the system and misuse and manipulate data. (geek-university.com)

• Integrity

integrity refers to the accuracy and completeness of data and ensures that the information is kept accordingly and accurately to its original. when a person receives the information that information must be exactly as the sender intended to deliver it. only authorized users can edit the information with the respect to its originality. to implement integrity, security mechanisms such as hashing, and data encryption are required. “It is highly essential to consider that nonhuman caused events such as an electromagnetic pulse (EMP) or server crash quite often can create unwanted changes in the nature of the data, therefore, to ensure data integrity it is suggested to keep the backup procedure and redundant systems in a safe place". (geek-university.com)

• Availability

Availability ensures the availability of information and resources to those users who need them. techniques such as software patching, hardware maintenance, and network optimization are used to the implement availability of data to users. Hardware issues are often inescapable and might occur quite frequently. Different tools and "processes including redundancy, failover, RAID, and high availability clusters are used to mitigate and reduce the occurrence of any hardware hazardous. The use of Dedicated hardware devices can reduce the occurrence of Downtime and unreachable data caused by harmful actions such as distributed denial of service (DDoS) attacks. (geek-university.com)

2.3 Network Campus Model

The network Campus model is suitable for small and medium business networks. Based on their role in the network, it is defined by 3 layers, Core layer, Distribution layer and Access layer.in small and medium-size networks the core and distribution functions can be combined into one layer.

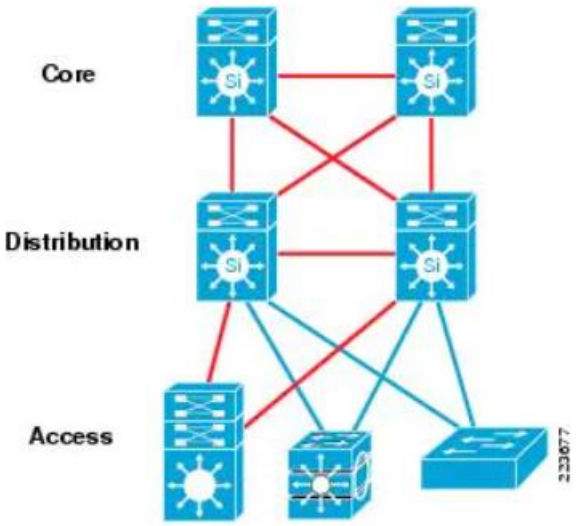

Figure 2 The Layers of the Campus Hierarchy

Access layer: Users and endpoints (computer, printer, camera) can connect to the network through the access layer. The access layer provides flexible security features, can implement authentication, and broadcast control, and also it is where would define QoS and configure voice VLAN.
Distribution layer: This layer has connectivity to core and access layers. Multitude decisions such as quality of service, filtering, and policy-based routing are performed in the distribution layer. It provides separate broadcast and multicast domains and also provides redistribution.
Core or backbone layer: This layer is the central thoroughfare for corporate traffic. All other parts of the network eventually feed into the core layer. The core is the hub for the connections in the network and it connects different campus network areas together. Redundancy is essential in the core layer. The core layer is reliable, high-speed, and provides quality of service. (Enterprise campus 3.0 Architecture: Overview and Framework. 2008)

3 Small And Midsize Business (SMB) definition

Small and medium-sized businesses are special economic units that are not homogeneous in nature and size and directly or indirectly play a significant role in national production, employment, and labor absorption. Each country has a

definition of these businesses according to their specific circumstances. So, most of these definitions are based on the following criteria: 1. Number of Employees 2. Turnover 3. Balance sheet

3.1 Why do hackers attack small businesses?

Hackers prefer to steal information from small and to some extent medium-sized corporate e-mails rather than attack large corporate emails. This is because small and medium-sized corporate usually use free email services and they did not design their own domain for this purpose. Public and free domains used by businesses are more at risk than corporate domains. Because dedicated email domains are more secure. Smaller businesses are more likely to receive cyber-attacks, due to the lack of sufficient and sophisticated investment in cybersecurity. These companies' network systems and computers are more appropriate for hackers to take financial resources or information and as consequence, they can be easily attacked and disrupted. Small business owners must remain aware of these attempts to have a chance of warding off several types of hackers. (HG.org. Small Businesses Are Often a Target for Hackers.)

3.2 How cyber-criminals attack small businesses

Most cyber-attacks on small businesses are done in the form of email scams. Usually, these traps are hidden in an email attachment! small and medium-sized businesses can also be threatened by Viruses, Malware, phishing, and Ransomware, Ransomware is another growing concern for new business owners. Small businesses that do IT-related work using insecure remote desktops endanger their systems and may be hacked by hackers through brute-force attacks. Ransomware refers to the precise type of malware that creates restrictions to access a computer and require victims to pay. Ransomware attacks are usually passed out through software and emails attachment. (www.sba.gov.Stay safe from cybersecurity threats)

3.3 Common threats

Lack of cyber security can cause economic, medical, and government disasters. Cybercriminals are becoming more sophisticated day by day, so they create threats or "traps" that can expose innocent people to cyber threats. Understanding the different types of threats is the first stage to protecting the SMB (small business) from data breaches which can include unauthorized access to customer contact, personal information, banking information, proprietary product, and financial data. The most common cyber security threats are Malware, Phishing, and Ransomware, which are designed to harm or damage a computer network. Whether they are designed to spy on company activities, steal data, or shut down the systems, once malware enters a company's network, it can cause serious business problems. (www.fortinet.com.Why Are SMBs Most Vulnerable to Cyberattacks)

Malware: Malware (“malicious software”) is computer code designed to infect devices for criminal purposes, such as holding the system, stealing confidential data, or installing damaging programs on a company's or individual's device without their knowledge. Types of malwares include.

- Viruses

  One of the most common network security threats that security professionals have to deal with every day is the virus. The virus is a destructive program that is capable of replicating itself and spreading to other computers in a network. Viruses are designed to disrupt a system’s ability to operate, they can corrupt data and files on computers, and steal data and sensitive information.

  Spyware

  Spyware, as the name suggests, is designed to spy on what the user is doing. They hide themselves and collect everything you do online, including passwords, credit card numbers, and other sensitive information.
- Keyloggers

Keyloggers are the type of spyware that can record and steal consecutive keystrokes that the user enters on a device. Software that logs what you type on your keyboard.

- Worms

  A worm is a type of malware that replicates itself and spreads to other computers while operating on infected systems.

  Trojans

  This type of malware disguises itself as legitimate software or is secretly hidden in legitimate software. And they cause viruses and other malware to penetrate the system.

- Phishing

  When attackers send malicious emails designed to trick people into falling for a scam. Typically, the intent is to get users to reveal financial information, system credentials, or other sensitive data

- Ransomware

  They are types of malware that restrict access to the system and their creator makes ransom requests to remove them. Some types encrypt files on the hard disk, and others may simply lock the system and display messages on the screen asking the user to pay some money

- Spam

  It is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media

- Bots

  is a type of software application or script that performs automated tasks on command. Bad bots perform malicious tasks that allow an attacker to remotely take control over an affected computer.

4 Categorization of cyber attacks

Cyber-attacks are divided into four categories, which are Denial of Service (DoS), Remote to User Attacks (R2L), User to Root (U2R) ja Probing. Every cyber-attack on a network can be placed into one of these four groupings (An implementation of intrusion 2012.)

- Denial Of Service (DoS

  DOS or Denial of Service attacks is one of the most dangerous types of cyber-attacks. In a DOS attack, hackers try to consume a large amount of site hardware resources by sending a large volume of requests to enter the site, and this movement causes the server to be out of reach for a while.

- Remote to User Attacks (R2L):

  Remote to User Attacks is an attack in which a user sends packets via the Internet to a machine he does not have access to expose machine vulnerabilities and exploit the privileges of a local user on a computer. xlock and guest are examples of these attacks.

  Attacks (U2R):

  This attack is abuse in which a hacker starts the system with a normal user account and tries to exploit system vulnerabilities to gain a super user. Examples of these attacks are perl, xterm (Denial-of-Service, Probing and Remote to User (R2L) 2012) Attack Detection using Genetic Algorithm.

- Probing:

Probing is an attack in which a hacker scans a network or machine to find vulnerabilities or vulnerabilities that may be exploited later. Examples of this is Nmap. Nmap is an open-source tool that can be used to scan the target network. Nmap can be used to find out which machines are on the network, what services are maintained on the devices, and what is their operating systems. (An implementation of intrusion 2012.)

4.1 What is a hacking tool?

Every hacker has his own tools, no matter what level he is at. For example, many people use the Kali distribution of the Linux operating system. This operating system has many programs that help hackers in the process of infiltration. One of them is called THC Hydra; This program is used to access the password of users of a system in various ways. The program itself becomes a hacker, because they usually do everything themselves, and the person used has little role in the process other than providing the required information.

4.2 Types of hackers

According to a study at the University of Maryland, a hack attack occurs in the world every 39 seconds. (Michel Cukier. Hackers Attack Every 39 Seconds. February 9. 2007)
Hacking" literally means breaking into a computer or a network. A hacker is a person or a group that carries out this infiltration operation. Most hackers do not do these things with good intentions. Hackers are divided into four groups White Hat hackers, Gray Hat hackers, and Black Hat hackers.

White Hat hackers: This hacker is a computer security expert who attacks protected networks and networks to test and measure their security. And they use their skills to improve security by being exposed to vulnerabilities against malicious hackers. By doing this, hackers can find security deficiencies and correct them.

Gray hat hackers mostly look for vulnerabilities in the system without the owner's permission or notice. They are a combination of black hat hackers and white hat hackers' activities. If gray hat hackers find problems, they report them to the business owner and sometimes charge a small fee to fix the problem. These types of hackers are not inherently destructive. they are trying to find something to add to their discoveries. Gray hat hackers generally do not take advantage of existing vulnerabilities. However, the activity of gray hackers is still considered illegal because the hackers did not obtain permission from the owner before attempting to attack the system.

Black Hat hackers: Black hat hackers usually have knowledge of entering the computer network and bypassing security protocols like all types of hackers. Black hat hackers are also responsible for writing malware and the Technique used to access the systems. Their main motive is usually personal, but they can also be involved in espionage and compromising cyber security. (Principles of Network Security, Attackers, and Their Tools)

5 Ways to prevent cyber-attacks on small businesses

A cyber-attack can force a business to shut down temporarily, as it takes a significant amount of time to access data and restore websites and systems. Also, customers may lose their trust in the company and in the long run, the reputation and profit of that business will be damaged. A cyber-attack can cost a small or medium-sized business (SMB) up to $108,000. Meanwhile, for businesses with more than 1000 employees, the cost has risen to $1.41 million, up from $1.23

million the previous year. The financial damage to the business will vary depending on the nature of the breach and the size of the business. However, there are, things the owners can do to protect their small business from a cyberattack and minimize the damage if one does occur. Here are some of them. (prowritersins.com. What is The Expected Cost of a Data Breach for Small Businesses?)

Antivirus software: Antivirus software: Install a suitable antivirus program on all computers, because There are a lot of spyware and viruses on the Internet, and any of them can damage the computer's operating system or personal files. Antivirus software prevents spyware and viruses from infecting a computer.

updates: All cybersecurity software must be kept up to date.

After receiving a notification that software updates are available, it should be installed.

Password Security: The password must be strong, and the password is managed through password management software. Use different passwords for each account otherwise if one account is hacked, another account with the same credential is easily compromised. And also, it is important to educate employees to choose a strong password because their weak passwords could put your business at risk.

Top 10 Worst Passwords - Historic Analysis

	2021	2015	2010	2005	2000
#1	123456	123456	123456	password	password
#2	123456789	password	password	123456	123456
#3	qwerty	12345	12345678	12345678	12345678
#4	password	12345678	qwerty	abc123	qwerty
#5	1234567	qwerty	abc123	qwerty	abc123
#6	12345678	1234567890	123456789	monkey	monkey
#7	12345	1234	111111	letmein	1234567
#8	iloveyou	baseball	1234567	dragon	letmein
#9	111111	dragon	iloveyou	111111	trustno1
#10	123123	football	adobe123	baseball	dragon

Figure 3. Top 10 Worst Password -Historic analysis.

Two-factor authentication: It is also called 2FA which refers to a security system. in this system two different forms of identification are required to access information. The first factor is username and password and the second factor is a unique thing to verify authentication requests such as biometrics, smartphones, and security token. (KENTON WILL. Sep28, 2020. Two-Factor Authentication (2FA))

Updating and training the knowledge of employees: Cyber security training is one of the most important aspects to familiarize employees with different security risks, information leaks, cyber-attacks, and solutions to deal with these threats.

Firewall: Choosing the right firewall for the size and scope of the business is the first important step in creating a secure network. A network firewall helps lock down the ports that hackers use to infiltrate an organization and steal information.

Use a VPN: Setting up a VPN is the second essential step to creating a secure network. During using a VPN, all internet traffic is encrypted and tunneled via an intermediary server in a separate location. Because the IP is masked and replaced with another IP, the Internet Service Provider (ISP) and other third

parties cannot see which websites are visited or what data is sent and received online. VPN is especially useful when employees have to work remotely, as there are a lot of remote risks that VPNs can help address. The confidentiality of information in VPN networks is higher than in public networks. In these networks, information is transmitted in encrypted form, and even if the attacker monitors all network transmissions, the attacker will only see the encrypted information

5.1 Types of VPN protocols

The VPN protocol is a technology that provides various encryption standards for data transmission, the most common protocols used to build tunnels are

- PPTP: Point to Point Tunneling Protocol is one of the oldest VPN protocols, which operates on TCP port 1723, and also PPTP is one of the most common, easiest to install, and computationally fastest, it is very useful for applications where speed is essential, such as video or streaming audio. But its encryption is not strong, and it can be easily broken.
- L2TP/IPSec: The L2TP protocol is based on PPP and does not have encryption capability, in most cases, the L2TP protocol is combined with the IPsec protocol to provide better quality services, which means complete security.
- Open VPN: Open VPN is a very secure protocol that uses Open SSL and SSL / TLS capabilities for encryption. This protocol can be called one of the strongest VPN protocols for encryption and security.
- SSTP: Secure socket tunneling protocol uses SSL to encrypt data, it is a fast protocol that uses a relatively small encryption packet size, and it is an extremely secure VPN protocol used by hospitals, businesses, and other government agencies with strong encryption requirements.
- IKEv2: Internet Key Exchange Version 2 protocol, is based on IPSec version 2, which is the same as Internet Key Exchange Version 2, and one of the important points of this VPN protocol is that if the connection is lost, it will reconnect very quickly. This protocol is very popular among mobile

users. (Mara Calvello. Virtual Private Network (VPN), Category VPN Protocols: Are You Using the Right One? 2020

5.2 Zero Trust

Zero trust refers to the IT security model that assume that users, systems, and services are not trusted by default, and that all users outside or inside the network must be authenticated at any stage to access enterprise resources. The reason for creating the concept of zero trust is to increase the number of security incidents due to users' access to different systems. In the traditional way, users within the organization are trusted by default. The most important problem of the traditional method is when the attacker can somehow penetrate into the organization at any level, and then the attacker can expand the scope of influence and access important organizational resources. (Zero Trust security/What is a Zero Trust network?)

5.2.1 History of Zero Trust security

The concept of Zero Trust occurred after Operation Aurora. Operation Aurora is a series of cyberattacks carried out by the APT, like the Elderwood Group in Beijing, China. Details of the incident in 2010 were explained by Google in a post on its blog about the event. The attacks lasted from mid-2009 to December 2009. A few years later, Google announced that it had implemented the Zero Trust concept on its network. Google’s performance led to the expansion of the use of Zero Trust technology. This concept is credited by John Kindervage in 2010 he coined the term while working at Forrester Research. (Fawad Ali. Everything You Need to Know About Operation Aurora.2022. / Zero Trust security/What is a Zero Trust network)

5.2.2 Components of Zero Trust Architecture

The In zero trust model, the organization's network is divided into smaller sections and different methods are considered to access the resources of each section. Nobody is trusted by default from outside or inside the network. In order to avoid user risk for the organization, the organization provides the minimum access required by the user and removes all resources that are not required by the user. The authentication and validation process are also performed regularly.
To enhance authentication, zero trust provides multiple layers of advanced access control for access to network devices and the servers that support resources.

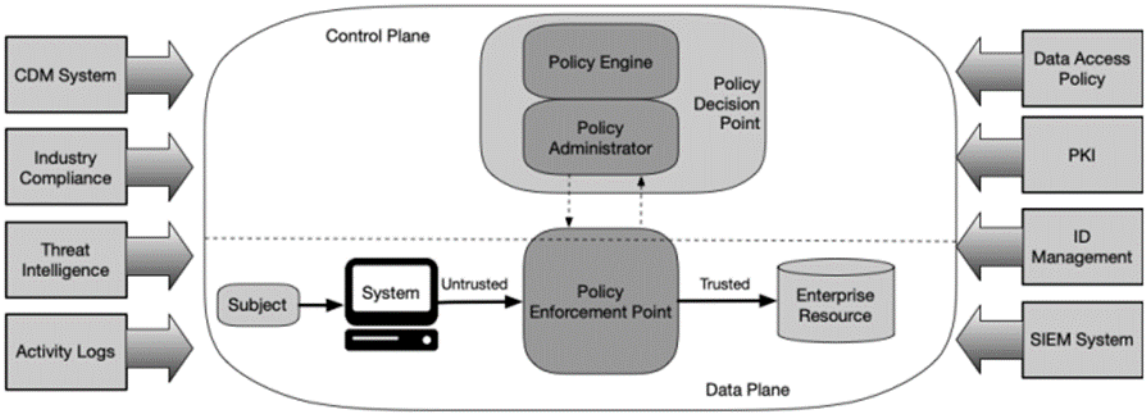

Figure 4. Zero-trust Components.

ZTA or Zero Trust Architecture is the cybersecurity architecture for companies that rely on zero trust concepts. This architecture protects the organization against information leakage and restricts suspicious movements within the network. ZTA does not refer to specific tools or equipment. ZTA is an attitude that has several logical parts. These sections are implemented locally or in the cloud service. Figure 4 shows a logical connection of elements and connections between different parts. In Figure 4, the Policy Decision Point or PDP has two logical parts. These two parts include the policy engine and the policy administrator. The logical parts of ZTA the Control Plane are connected to each

other separately, while the data of the systems are connected to each other in the Data Plane.

- PE (Policy Engine)
  PE is responsible for deciding whether a user can access a requested resource. PE receives input from the organization's policies and other external sources. These inputs are used to confirm or deny trust in PE algorithms to grant access, deny, or revoke access to resources.PE is complementary to Policy Administrator (PA). PE makes decisions and stores them in the log (input including access or denial access) and PA executes decisions.
- PA (Policy Administrator)
  PA is closely related to PE and the implementation of decisions to grant or deny access to PE decisions. If a session is allowed and an authentication request is made, the PA will set the session to start and the PA signals to the PEP to terminate the connection if the session is denied. In some implementations, PE and PA may be considered as a single service.

- PEP (Policy Enforcement Point)
  PEP is responsible for monitoring, enabling, and disconnecting between users and company resources. PEP liaises with PA to submit and update new PA requests and policies. This is a logical part of Zero Trust Architecture. However, it can be divided into two parts: the client side (the tool installed on the laptop) and the organization's resources side (the resource gateway control tool that controls access to them) or a portal access control.

5.2.3 local data sources and external data sources

In addition to the core components in the organization implementing ZTA, a few other input elements create new policies and policies for PE decision making.

- Continuous diagnostics and mitigation (CDM) system

  CDM collects information about the status of the organization's assets and implements software settings updates. The CDM system provides information to the PE about the system requesting access to the resources. Such as whether the system has the latest operating system, organization-approved software and known vulnerabilities. The CDM system is responsible for identifying and enforcing policies on non-organizational equipment in the organization's infrastructure.
- Industry Compliance System

  Industry Compliance System complies with the rules of the industry regulatory sector (such as FISMA requirements). This section covers all the policies that the organization must consider in order to comply with the industry.
- Threat Intelligence Feeds

  Threat Intelligence Feeds generates information from external and internal sources of the organization and this information helps PE in making access decisions. This section can have several services that collect information from internal sources or several external sources about the latest information on attacks and vulnerabilities. It also includes the latest security bugs in the software, detection of the latest malware, and reports of asset attacks. The PE Division decides to deny access to the Company's assets.
- Network and System Activity Logs

  This system collects logs of all the organization's various assets, network traffic, resource access operations, and other events to provide the security status of the organization's systems live or in the near future.
- Data Access Policies

  This section deals with the characteristics, maps, and policies regarding access to organizational resources. Maps can be coded (via the management interface) or dynamically created by PE. These policies are the starting point for credible access to resources. These policies are based on the definition of the organization's plans and needs.
- PKI (Enterprise public key infrastructure)

PKI is responsible for logging and producing certificates issued by the company to the services, resources, topics, and applications.

- ID management system
  The user accounts are created, stored, and managed in this section (for example, LDAP servers). The system includes basic user information (such as name, email address, and credentials) and other organizational attributes such as maps, access characteristics, and registered assets.
- SIEM system (Security information and event management)
  This section collects security information for analysis. This information is used to correct policies and warn of possible attacks on company assets. (Rose, Scott. Borchert, Oliver. Mitchell, Stu. Connelly, Sean. Zero Trust Architecture.2020.)

6. DMZ (Demilitarized Zone)

Businesses that provide services to their customers over the Internet must make their applications or web servers available over the Internet. This exposes the entire internal network and their critical data to cyber-attacks. To protect against cyber threats, public servers are hosted in a separate network called a DMZ network.

A DMZ network sits between unsecured external networks such as the Internet and a company's secure environment. Web servers and other external systems are located in the DMZ without compromising the security of internal resources.

6.1 What is a DMZ (Demilitarized Zone) Network?

The word DMZ is an abbreviation for the term "demilitarized zone", which means that military activities are not allowed in it. ”In computer networking, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks usually the public Internet”. The aim of creating a DMZ in the network is to add an additional layer of security to the LAN in the organization, which limits the ability of hackers to directly access internal servers and data through the Internet. This area is neither as insecure as the public Internet nor as secure as the internal network. Hosts inside the DMZ are restricted to only having limited connectivity to certain hosts on the internal network, as the content of the DMZ is not as secure as the internal network. Likewise, communication between hosts in the DMZ and communication with the external network is also restricted to further secure this area and provide these special services. In this way, hosts inside the DMZ can communicate with both internal and external networks, while an integrated firewall manages traffic between DMZ servers and internal network clients, and another firewall provides control layers to protect the DMZ from the external network. (Erin Risk. DMZ Network: Is It Necessary to Secure Company Resources? Dec 17th, 2021)

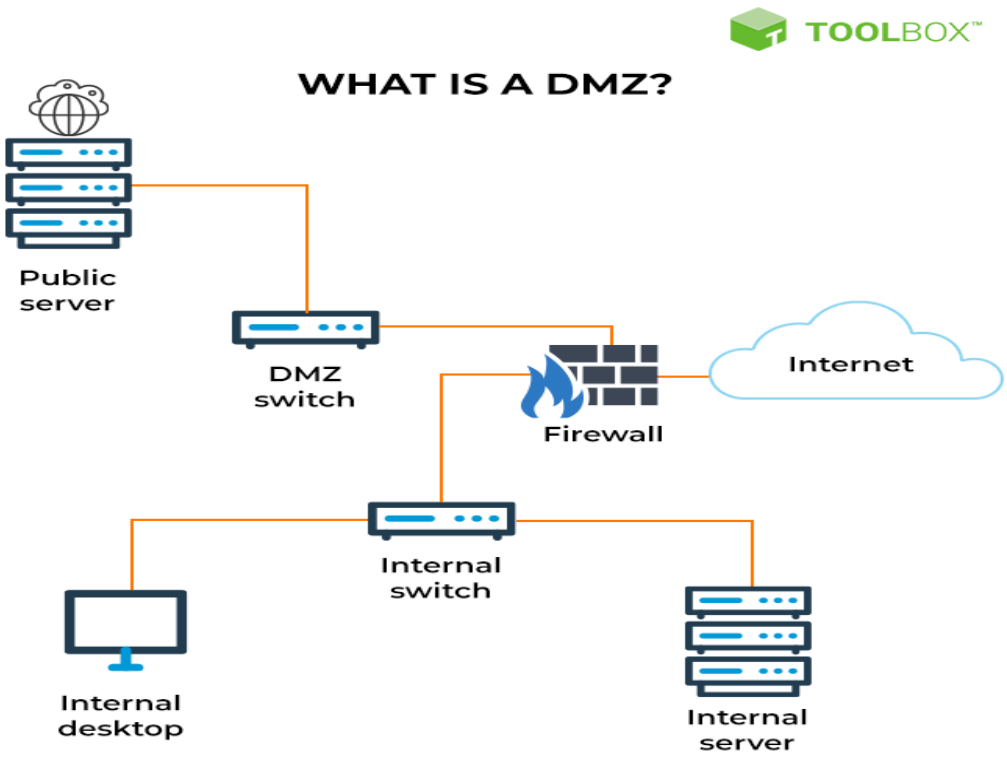

Figure 5. DMZ Network

6.2 How Does a DMZ Network Work?

A DMZ network provides a buffer between the Internet and an organization's private network. The DMZ network is separated by a security gateway such as a firewall that filters traffic between the DMZ and the LAN and the DMZ is protected by another security gateway that also filters incoming traffic from external networks. DMZ is located between two firewalls, and the DMZ firewall configuration ensures that incoming network packets are seen by a firewall or other security tool before entering the host servers in the DMZ network. This means that even if a sophisticated attacker can get past the first firewall, they must also gain access to the DMZ settings before they can harm a network. If an attacker can penetrate an external firewall and compromise a system in the DMZ, then they must also pass through an internal firewall before accessing sensitive

company data. A skilled hacker may be able to compromise a secure DMZ, but the settings in the DMZ will alert to these threats.

6.3 Security Benefits of DMZ

The DMZ provides the internal network with a layer of security by limiting access to servers and sensitive data, which is the main advantage of DMZ. The DMZ network allows website visitors to enable services while providing a shield between them and the organization's private networks. There are several security advantages of this buffer, including Access control, Network reconnaissance prevention, Protection against Internet Protocol (IP) spoofing

- Access control

  Businesses may provide users access to services outside their internal network through the public Internet. The DMZ provides access to these services while implementing network segmentation to make it more difficult for an unauthorized user to access the private network. A DMZ network may also include a proxy server that centralizes internal traffic flow and simplifies monitoring and recording of that traffic.

- Network reconnaissance prevention

  By providing a buffer between the Internet and a private network, a DMZ prevents attackers from conducting reconnaissance activity to hunt for potential targets. The servers inside the DMZ are exposed to the public, but the firewall provides an additional layer of security that prevents an attack from being seen inside the internal network. Even if a DMZ system is hacked, the internal firewall separates the private network from the DMZ to keep it secure and make it difficult for outside detection.

- Protection against Internet Protocol (IP) spoofing

By spoofing the IP address and imitating a signed-in, approved device, attackers may try to gain access to systems. The DMZ can detect and stop such fraud attempts because another service verifies the legitimacy of the IP address. The DMZ also creates network segmentation to create space to organize traffic and access public services away from the internal private network. (Chiradeep BasuMallick. What Is a Demilitarized Zone (DMZ)? June 16, 2022)

6.4 DMZ Design and Architecture

The DMZ is a "completely open network" but there are several architectural designs and methods that protect it. A DMZ can be designed in many ways, from a single firewall approach to having dual and multiple firewalls. Most modern DMZ architectures use dual firewalls that can be extended to develop more complex systems.

- Single firewall: A DMZ with a single firewall design needs three or more network interfaces. It is the first external network that connects the public Internet connection to the firewall. The second network forms the internal network while the third network is connected to the DMZ. Various rules control what traffic is allowed to access the DMZ and restrict connectivity to the internal network.

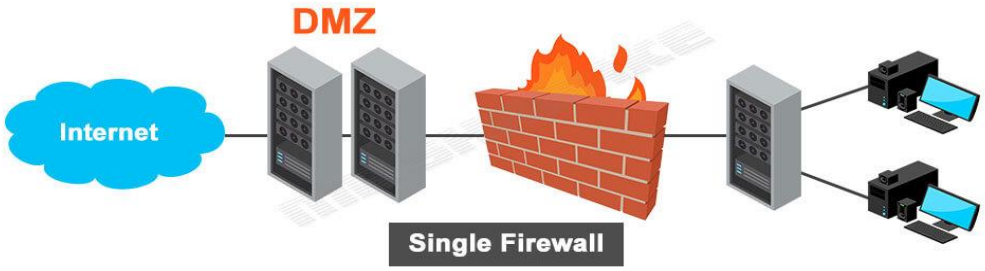

Figure 6. DMZ with a single firewall

- Dual firewall: Deploying two firewalls with a DMZ between them is generally a secure option. The first firewall only allows traffic outside the DMZ, and the second only allows traffic from the DMZ to the internal network. An attacker must pass both firewalls to gain access to the organization's LAN. (Chiradeep BasuMallick. What Is a Demilitarized Zone (DMZ)? June 16, 2022)

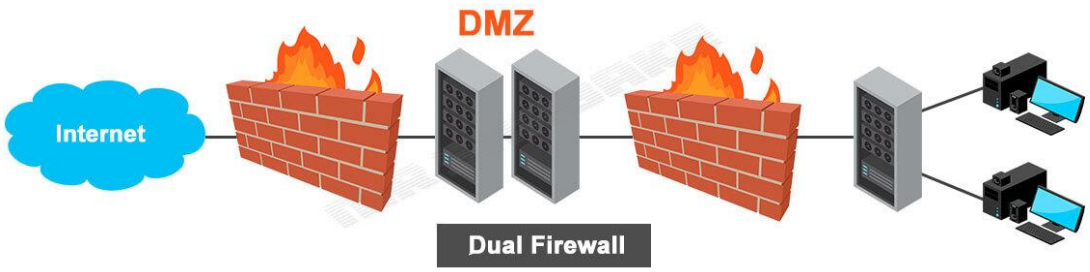

Figure 7. DMZ with a dual firewall

7. Summary

Nowadays the internet became a very dangerous place, especially if the business is dependent on it. As many of us are digitally connected, this threat exists even in our personal lives. The Cyber-attack statistics made it clear that most businesses are targeted, and having a small business becomes more dangerous. Hackers frequently use cyber-attacks on smaller businesses because there is less complexity in the computer system and company's cyber security, and it is easier for hackers to take information or financial resources. The types of attacks that small business may face is phishing, malware, and ransomware. Small business owners should know that education is the best defense against any type of attack, therefore they must be aware of the types of attacks by raising their awareness and do not forget to learn how to protect their data before becoming a victim. And also, they have to make sure their digital and physical assets are

secure. A small business owners are responsible for protecting not only their personal devices, but all the devices used by their employees, best method to create a safer environment is monitoring employee’s internet usage especially if employees are able to access confidential files or obtain sensitive information. by reducing the risk of employees being compromised, small business owners avoid a bigger disaster in the future access confidential files or obtain sensitive information. by reducing the risk of employees being compromised, the small business owners avoid a bigger disaster in the future.

References

1 Mitchell, John Arnold & Thomson, Magdalena. 2017. A guide to citation. London: London Publishings.

2 [online] Forcepoint. What is Network Security? Available at https://www.forcepoint.com/cyber-edu/network-security

3 [online] geek-university.com Available at https://geek-university.com/confidentiality-integrity-and-availability-cia-triad/

4 Provided by HG.org. Small Businesses Are Often a Target for Hackers.[online] HG.org. Available at https://www.hg.org/legal-articles/smallbusinessesareoften-a-target-for-hackers-50136

5 Provided by sba.gov. Stay safe from cybersecurity threats [online] sba.gov Available at https://www.sba.gov/businessguide/manage-your-business/stay-safe-cybersecurity-threats KENTON WILL. Sep 28, 2020.

6 Two-Factor Authentication (2FA) [online] investopedia.com Available at https://www.investopedia.com/terms/t/twofactorauthentication2fa.asp

7 Provided by Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas an Implementation of Intrusion Detection System Using Genetic Algorithm. 2012. Available at https://arxiv.org/ftp/arxiv/papers/1204/1204.1336.pdf

8 Provided by Swati Paliwal and Ravindra Gupta Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.303.3876&rep=rep1&type=pdf

9 Cisco, Principles of Network Security, Attackers and Their Tools Available at https://hacc.hawaii.gov/wp-content/uploads/2020/05/CyOps-Presentation.pdf

10 Provided by Mara Calvello. Virtual Private Network (VPN), Category VPN Protocols: Are You Using the Right One? 2020 Available at https://www.g2.com/articles/vpn-protocols

11 Enterprise Campus 3.0 Architecture: Overview and Framework. 2008 Available at https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html

12 Zero Trust security | What is a Zero Trust network?

Available at https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

13 Fawad Ali. Everything You Need to Know About Operation Aurora.2022 Available at https://www.makeuseof.com/operation-aurora/

14 Zero Trust Architecture. provided by Rose, Scott. Borchert, Oliver. Mitchell, Stu. Connelly, Sean.2020.) Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

15 prowritersins.com. What's The Expected Cost of a Data Breach for Small Businesses? Available at https://prowritersins.com/cyber-insurance-blog/average-cost-of-a-data-breach-for-small-businesses/

16 www.fortinet.com.Why Are SMBs Most Vulnerable to Cyberattacks)

Available at https://www.fortinet.com/resources/cyberglossary/smb-cyberattacks

17 Erin Risk. DMZ Network: Is It Necessary to Secure Company Resources? Dec 17th, 2021, Available at https://www.twingate.com/blog/dmz-network/

18 Chiradeep BasuMallick. What Is a Demilitarized Zone (DMZ)? June 16, 2022, Available at https://www.spiceworks.com/it-security/network-security/articles/what-is-demilitarized-zone/

19 Michel Cukier.Hackers Attack Every 39 Seconds. February 9, 2007, Available at https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds