Secured Internet Office Network with the Internet of Things Using Packet Tracer Analysis

Azrai Danial Azhari, Norakmar Arbain Sulaiman, Murizah Kassim

School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia
norakmar7222@uitm.edu.my

2021 IEEE 11th International Conference on System Engineering and Technology (ICSET) | 978-1-6654-3766-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICSET53708.2021.9612554

Abstract— Internet of Things (IoT) communication provides connections of more objects and services to the Internet which involves a Secured Internet Office Network environment. Internet office is an important environment where issues on security have been regularly discussed which impact education, communication, business, government, and others. Recent small internet office network has implemented VLAN, DHCP, Cisco ASA Firewall, wireless access point and registration Server but IoT is enhanced from time to time. This paper presents the implementation of simulation of IoT onto a secured small office network by using the Cisco Packet Tracer a network simulator software. A simulation of Internet office network with IoT systems services on motion detection system, door lock system and smoke detection system were developed. Due to security concerns, several security protocols have been integrated such as SSL VPN, ASA Firewall security level and WPA2-PSK authentication. The result has successfully shown the data for smoke level over time taken and the door lock system's scenarios based on the RFID setup. The implementation of the IoT, network design and configuration and integration of the security protocols have been successfully implemented using the Cisco Packet Tracer.

Keywords— Internet Office Network, Packet Tracer Analysis, IoT, SSL VPN, Security, WPA2-PSK.

I. Introduction

Nowadays, a lot of residential building has integrated the IoT into their houses by applying the smart house concept. This concept can be managed and operate remotely by using smartphones and computers. Users can enjoy a lot of advantages from this concept such as remote monitoring, wireless alarm system, higher security for better safety saves a lot of money by going green [1]. In contrast, the corporate sector and business industry are still low in number in terms of IoT implementation for their office. Projects and study regarding the smart office are very limited compared to other application of this concept such as a smart house, smart campus, and smart cities. If the corporate sector still refuses to implement this concept, they will face several issues that may get worse and cannot improves their business. They would not be able to produce a conducive work environment which can lower the productivity that is essential for future profits x [2]. A study has been carried out to develop and implement the smart office concept to curb and solve this problem and improves the working environment at offices around Malaysia.

IoT plays an important role in human progression. With the combination of the ability of IoT to sense, collect, transmit, analyze and distribute data on a large scale with the way people process information, humanity will have the knowledge and wisdom to survive and thrive for the coming years [2]. He also found out that the power of sensors has the potential to slow the development of IoT. Sensors will need to be self-sustaining for IoT to reach its full potential while current sensors can last long enough to fulfill the requirement. Research on the events processing and device interoperability in a smart office IoT application. This paper shows that Smart Office will be focused on facilitating user interactions driven by business processes or workflow sequences in the environment [3]. The application of Smart Office will provide benefits on business process optimization, improvement of working conditions for employees, or an overall increase of work effectiveness can be achieved.

The feature that Smarts Office can offer is energy savings achieved by optimized use of the office room equipment, alignment of the office room environment to business process based on the adaptation of the office work environment and comfort of individual users by Exploration of a suitable occupancy sensing devices [4]. Some of the previous work that is related to this paper researches on designing smart campuses using the Internet of Things. This paper studies that Smart Campus will contain progressed ICT's to consequently screen and control each activity within the campus using IoT smart devices. A Smart Campus portion named Smart Office causes to show the feasibility of the work simulation tool for designing the concept [5]. The other research on implementing smart college using Cisco Packet Tracer Simulator.

This paper shows that a smart college network can be implemented through the simulation concept designed on Cisco Packet Tracer. The Home Gateway was used as a transmission media path and provide automatic addressing to multiple devices connected via wireless networks, IoT server and smartphone that serve as interfaces in controlling and monitoring electronic devices and Microcontroller (MCU) to register IoT device on it to control them [6, 7]. More research was presented on using Cisco Packet Tracer to simulate smart homes. This paper shows the simulation of smart home devices such as air conditioning, alarm, lighting, and doors that can be controlled by the end-user smart device remotely which produces the concept called smart home [8]. The use of Cisco Packet Tracking features which can simulate the smart home concept and IoT devices can be monitored. Simulation results show that smart objects can be connected to the home portal and objects can be successfully monitored which leads to the idea of real-life implementation. A study on Cisco ASA all-in-one firewall, IPS, and VPN adaptive security appliance. This paper indicates that the Cisco ASA Firewall is a security appliance used to control network traffic and order to allow or deny access to the network based on security rules [9]. To provide additional security functionalities, add-on modules can be included.

This paper studies developing an office network environment with the implementation of the Internet of Things and several security protocols using Cisco Packet Tracer software. An office network equipped with Cisco

ASA Firewall as its main security device that connects the office network with an external network.

The SSL Virtual Private Network (VPN) also has been integrated into the ASA firewall as one of the security protocols. The office network is also equipped with several IoT systems such as the motion detection system, door lock system and smoke detection system. The network is segmented using VLAN to provide communication between grouped devices and enhance the management of the network traffic. DHCP is also configured into the network to allow an automated assignment of the IP addresses for each device. Registration server has been used to manage and configure IoT devices in the office network.

II. Methodology

Figure 1 shows the design and implements an IoT network into a secured office network. Several steps have been taken and details are explained.

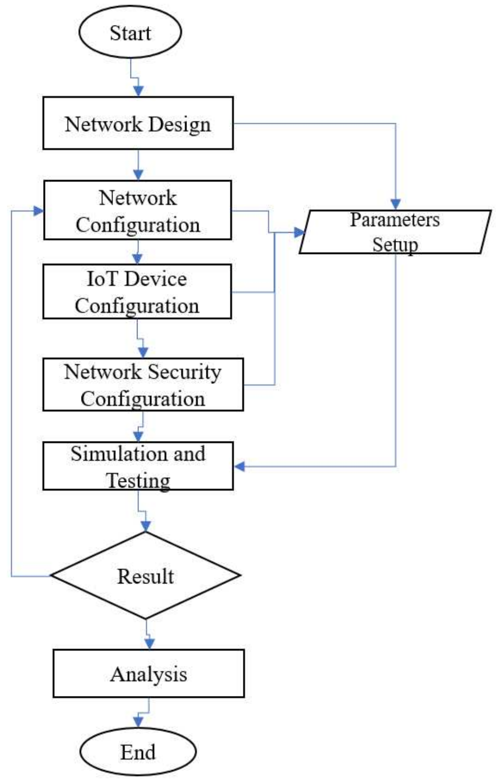


Fig. 1. Flow chart for the project development.

A. Designing Network Topology and Specification

The networks that are suitable for a small to medium scale office are Local Area Network (LAN) as they can be managed by one person with only moderate accessibility and scalability. A group of computers and mobile devices that shares the same communications line or network to a server are in LAN [10]. Offices tend to have more than one department and to separate those department's networks, the Virtual Local Area Network (VLAN) will be implemented. Interfaces or end devices can be assigned to VLAN based on their department which enables the system to be divided into logical groups. The tree topology has been implemented in this project where it is considered the best among other topologies because it can contain a few branches of network connected by a central hub. The tree topology is flexible and scalable because it accommodates more nodes in the hierarchy chain. The fault finding and troubleshooting are easy in this topology because each branch can be assessed individually. The devices used in this network design include a Cisco ASA 5505 firewall, a router model 2621XM, two servers, a switch model 2960-24TT, a few PC and 3 access points. As for the design for the IoT network, several systems have been implemented which are:

- Motion Detection System: Consists of a trip sensor as an input while the output consists of an alarm, webcam, and a spotlight. The purpose of this system is to detect trespassing in the office.
- Door Lock System: The input consists of an RFID reader and the output includes an RFID card and a smart door which are used to allow employees and authenticate guests only to enter the office.
- Smoke Detection System: Consists of a smoke detector, smart window, fire sprinkler and an alarm that will be to detect fire in the office and alarming surrounding environment.

B. Network Configuration

The configuration for the whole network in this design consists of several features which are the Cisco ASA firewall, access point and Registration Server.

- *Cisco Asa Firewall*

The Cisco ASA Firewall's complete traffic flow is governed by the following four default security policy regulations [11].

- Traffic flow from a higher-level security interface to a lower-level security interface is permitted.
- Traffic flow from a lower-level security interface to a higher-level security interface is not permitted.
- Traffic flow is prohibited from any interface to any other interface with the same security level.
- Traffic flows in and out from the same interface are also denied.

Figure 2 shows the basic topology of the network that consists of the ASA Firewall, a router, a server, a switch and two computers.

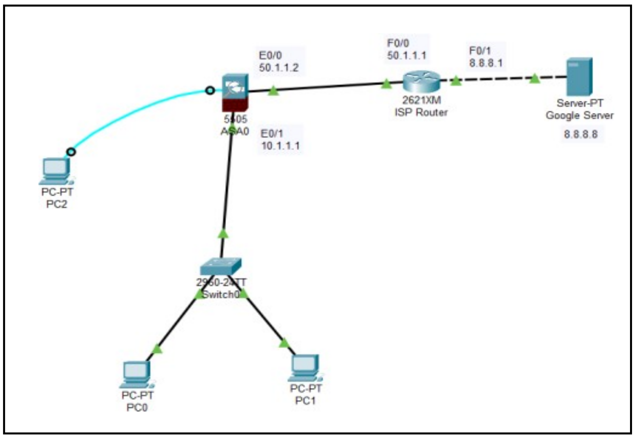


Fig. 2. Basic topology of the office network.

There are a few steps to configure the ASA firewall:

- Connects all the devices in the topology. The switch will be connected to the Ethernet0/1 port while the ISP router will connect to the Ethernet0/0 port of the firewall. The Google Server will be connected to the ISP router.
- Assign IP Addresses on the ASA Firewall and ISP Router.
- Set the interface inside and outside and security level on the ASA Firewall.
- Configure DHCP server and DNS server on CISCO.
- Registration Server

Registration server is used to communicate and control the IoT devices which are connected to it. The registration server can be accessed by using its IP address. Then it will prompt the user to enter the username and password to access the website. Once the username and password have been set, the end devices will be able to access and monitor the wireless IoT devices through the web.

C. *IoT Device Configuration*

All devices should get the IP address from the DHCP that has been configured on the ASA firewall in the network has been designed and configured. All IoT devices should be connected to the registration server by using the registration server IP address and provide a username and password for the authentication process. Figure 3 shows the IoT monitor on the administrator computer that contains all the IoT devices that have been connected to the registration server.

- Door Close: When the RFID reader was in invalid status the Main Door will be locked or remain locked. The RFID reader will turn invalid when it detects no card or card with a value other than 1001. Smoke Detection System consists of two different conditions which are:
- Sprinkler ON: When the smoke detector reading was equal to or more than 2 ppm it will switch on the fire sprinkler, alarm and the smart window forsafety purposes.
- Sprinkler OFF: When the smoke detector reading was below 2 ppm it will switch off the fire sprinkler, alarm and the smart window.

D. *Network Security Configuration*

- *Asa Security Level*

The basic security policy of the Cisco ASA Firewall depends on the relative trust known as Security Levels. These security levels are numbered from 0 to 100, where level 0 is used for the least trusted network and level 100 for the highest trusted. The default settings on the Cisco ASA Firewall are level 0 for the public network and level 100 for the private network [11]. Any other network can be assigned a level number depending on its trust level. This security policy has been implemented in this network to provide security on the office network and outside network.

- *Secured Socket Layer (SSL) VPN*

Clientless SSL VPN is a technology allowing limited but secure access to internal network resources from any location using a web browser. No specific VPN client is needed, a remote user only needs any device that has an SSL-enabled web browser to access HTTP or HTTPS-enabled web servers on the internal network [12]. To create an SSL VPN, an HTTP server is required within the office network and switch on the HTTP and HTTPS services. Then the user needs to create a username and a password at the ASA firewall CLI. Then using the User Manager tab at the Clientless section in the ASA firewall user need to create a bookmark with a title and a URL that links to the HTTP server IP address. Next, the user needs to create a profile using the User Manager tab at the Clientless section that requires a username, bookmark, profile name and VPN group policy name where the username and bookmark are based on the configured before.

- *Wpa2-Psk with AES Encryption for Access Point*

WPA2/PSK is usually implemented for home use or small office networks. AES is typically utilized for encryption. All clients of the same network use the shared passphrase to access the same network. The shared passphrase is used with other variables like Service Set Identifier (SSID) and SSID length to produce Pairwise Master Key (PMK), which is used for authentication and production of unicast protection keys [13]. There are three different access points used in this network each for the three IoT systems. Each access point has a different Service Set Identifier (SSID) and uses the WPA2-PSK as its authentication with AES encryption type. The Pre-Shared Key (PSK) contains from 8 to 9 characters varies to the access point.

E. *Simulating And Network Testing*

The network has been simulated and tested on the connection between the devices, security protocol implemented and access to the registration server. The IoT device had also been tested if it would run the way it has been configured based on the scenarios and conditions. The testing results will be presented in the results and discussion section.

III. Result and Analysis

This section shows the result of the implementation of IoT into a secured office network. The result will be explained in detail by referring to the picture of the design topology. The resulting framework includes Dynamic Host Configuration Protocol (DHCP), IoT Devices Implementation, Communication and Security Protocol Implementation.

A. *Dynamic Host Configuration Protocol DHCP*

TABLE I. DHCP POOL

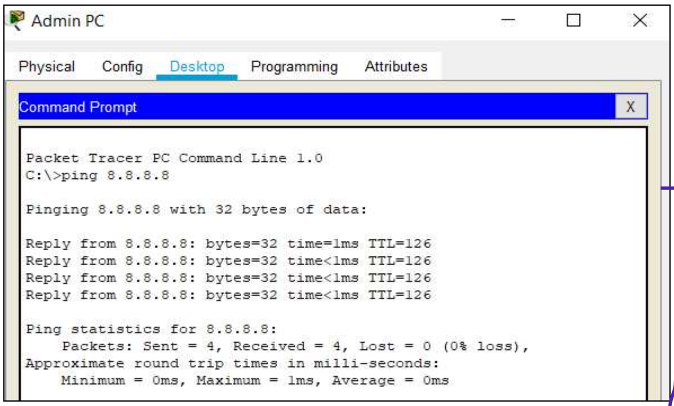
Device Type **Device Name**	**End Device**	**Server**	**IoT Device**
Admin PC	10.1.1.1/01	-	-
User PC	10.1.1.1/02	-	-
HTTP Server	-	10.1.1.1/00	-
Registration Server	-	10.1.1.1/03	-
Spotlight	-	-	10.1.1.1/04
CCTV	-	-	10.1.1.1/05
Alarm	-	-	10.1.1.1/06
Trip Sensor	-	-	10.1.1.1/07
RFID Reader	-	-	10.1.1.1/08

Main_Do or	-	-	10.1.1.1/09
Fire Sprinkler	-	-	10.1.1.1/10
Alarm 2	-	-	10.1.1.1/11
Smoke Detector	-	-	10.1.1.1/12

The ASA Firewall interface has been configured to perform Dynamic Host Configuration Protocol (DHCP) features. Table 1 shows the DHCP pool provides IP addresses automatically for all the devices within the inside network. This protocol helps to assign IP addresses and default gateway parameters to hosts that are trying to connect to the network automatically. Therefore, using this will help the users by not configure manually the IP addresses on their device when they want to connect to the office network.

B. Communication

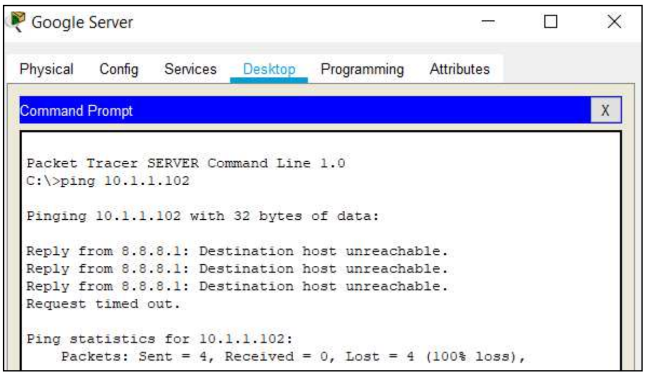
There are two different VLANs in this network which are Vlan 1 for the inside network and Vlan 2 for the outside network. Devices from Vlan 1 can communicate with devices on the Vlan 2 while devices in Vlan 2 cannot reach devices from Vlan 1. Figure 3 shows that Admin PC which is within Vlan 1 can communicate with Google Server with no packet loss after a ping from address 10.1.1.102 to 8.8.8.8.



```
Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fig. 3. Communication between Admin PC and Google Server.

Figure 4 shows Google server failed to communicate with Admin PC with all 4 packets loss after a ping from address 8.8.8.8 to 10.1.1.102 because the ASA Firewall has blocked any device from lower security level to communicate to higher security level.



```
Packet Tracer SERVER Command Line 1.0
C:\>ping 10.1.1.102

Pinging 10.1.1.102 with 32 bytes of data:

Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.
Request timed out.

Ping statistics for 10.1.1.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 4. Communication between Admin PC and Google Server.

C. IoT devises Implementation

This section presents the result of the implementation of IoT devices by using the registration server. There are 3 different case studies carried on IoT devices.

- Case Study 1: Smoke Detection System

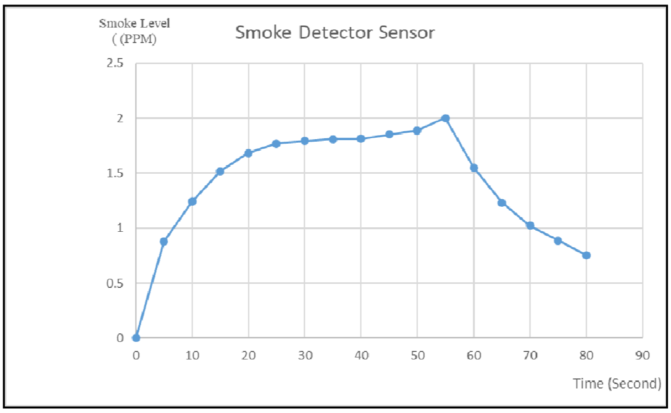


Fig. 5. Smoke level (ppm) over time (second) graph.

Figure 5 shows the graph of smoke level (ppm) over time recorded by the smoke detector sensor. The sensor detected smoke indicating there is a fire inside the office the smoke level reading will start to increase. For the first 20 seconds, the smoke level increases rapidly from 0 ppm to 1.65 ppm. However, the smoke level starts to increase slowly until its reaches the threshold value of 2 ppm at 55 seconds and begins to drop significantly after that. When the smoke level reading hits the threshold point, all the outputs will switch on as a fire prevention method. The smart window, fire sprinkler and alarm will switch on to release the smoke, puts out the fire and notify surrounding people of the fire respectively.

- Case Study 2: Intruder Access Prevention

TABLE II. DOOR LOCK SYSTEM'S SCENARIOS.

System	Scenario	Action
Door Lock System	Door Locked	RFID Reader status invalid and Smart Door remain locked.
	Door Unlocked	RFID Reader status turns to valid and Smart Door will be unlocked.

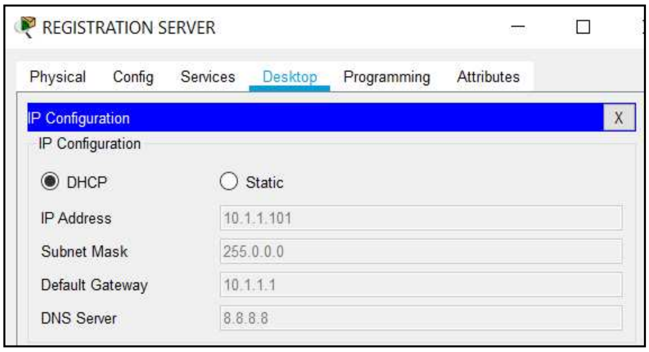
Table 2 shows the Door Lock System's scenarios and their outputs. When the RFID reader reads an RFID card that the ID is above the value of 1000 it will display an invalid status and the Smart Door remains locked. If the RFID reader reads an RFID card with an ID value below 1000 it will display valid status and the Smart Door will be unlocked.

TABLE III. MOTION DETECTION SYSTEM'S SCENARIOS.

System	Scenario	Action
Motion Detection System	No Motion Detected	The alarm, spotlight, and webcam switch off.
	Motion Detected	The alarm, spotlight, and webcam switch on.

Table 3 shows the Motion Detection System's outputs based on the scenarios that applied to them. The first scenario is when there is no movement detected at the laser beam therefore the alarm, spotlight and webcam will be switch off. But if the trip sensor detects movement across the laser beam it will activate the alarm, spotlight, and webcam.

- Case Study 3: Registration Server risk management



IP Configuration

IP Configuration

● DHCP ○ Static

IP Address: 10.1.1.101

Subnet Mask: 255.0.0.0

Default Gateway: 10.1.1.1

DNS Server: 8.8.8.8

Fig. 6. Registration Server IP configuration.

Figure 6 shows the IP configuration for the Registration Server which used the Dynamic Host Configuration Protocol (DHCP). The DHCP will automatically assign all the IP addresses, subnet mask, default gateway and DNS Server to the Registration server. In case of a power outage, the risk of the IP address of the registration server changing will be very high. Therefore, all the IoT devices will lose connection to the Registration Server. To overcome this problem, the user needs to manually connect all the IoT devices to the Registration Server's new IP address.

D. *Security Protocol*

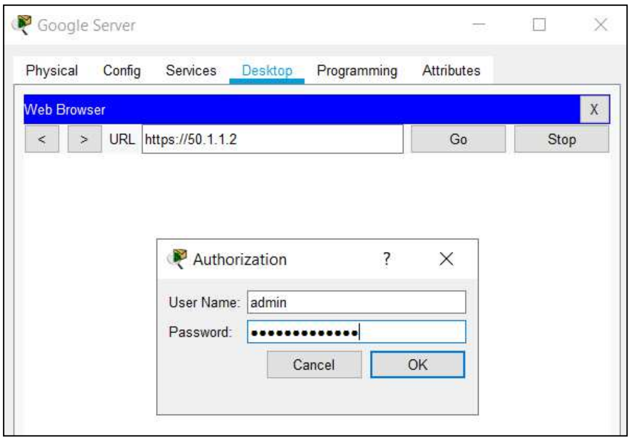
- ASA Firewall Security Level

TABLE IV. ASA FIREWALL SECURITY LEVEL.

Interface	Name	Security Level	Ip Address
VLAN 1	Inside	100	10.1.1.1
VLAN 2	Outside	0	50.1.1.2

Table 4 above shows the security level of the ASA Firewall implemented in this topology. Vlan 1 has a security level of 100 and Vlan 2 with a security level of 0. Security level 100 is the highest security level where it is considered the most trusted while security level 0 is the lowest in the firewall. Therefore, traffic can pass through from interfaces with higher security levels to interfaces with lower security levels. And the firewall blocks traffic from interfaces with lower security levels from passing through to interfaces with a higher security level.

- Secured Socket Layer (SSL) VPN



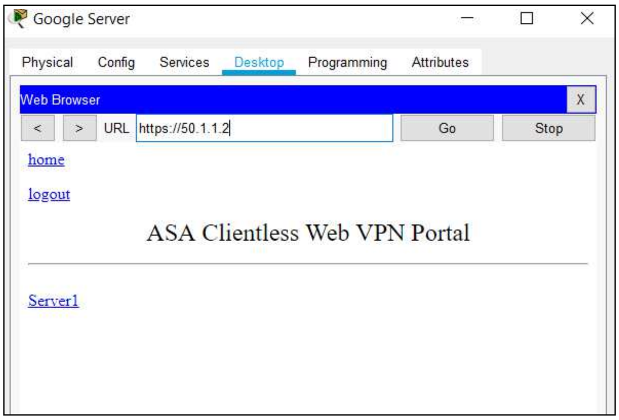
URL: https://50.1.1.2

User Name: admin

Password: ••••••••••••••

Fig. 7. Authorization Process to access the internal network.

Figure 7 shows that the user needs to provide the correct username and password that has been configured to access the internal network using the clientless SSL VPN. The user only needs an SSL-enabled web browser to access HTTP- or HTTPS-enabled web servers on the internal network.



URL: https://50.1.1.2

ASA Clientless Web VPN Portal

Fig. 8. The Company Webpage through the SSL VPN.

Figure 8 shows the company webpage that can be accessed by a user from the outside network after providing the correct username and password during the authorization process.

- *Light Weight Access Point Security*

TABLE V. LIGHTWEIGHT ACCESS POINT DETAILS

Access Point Name	SSID	Pre-Shared Key
Motion Detection System	MOTION	motion123
Main Door	DOOR	door1234
Smoke Detection System	SMOKE	smoke123

Table 5 shows the Access points used and their security features. The access point uses the WPA2-PSK as their security measure where the WPA2-PSK provides authentication for the IoT devices. Each access point has its SSID and Pre-Shared Key where it acts as a password. The minimum length for the Pre-Shared Key is 8 characters and can supports up to 63 characters.

IV. Conclusion

The implementation of IoT into a secured small office network has been successfully developed using the Cisco Packet Tracer software. The network design incorporates the VLAN and DHCP technology into the office network that will ease the management of the devices and providing connectivity throughout the network. The ASA Firewall also has been used as the medium to connects the office network to outside or external networks. The SSL VPN has been integrated into the firewall providing users from outside networks limited but secure access to the office network. All the IoT system has been implemented into the office network through the registration server that will manage and monitor all the IoT devices. In a conclusion, the scope of work is a practical proof-of-concept to implement an industrial control system into a real-life office network as part of the IoT framework.

Acknowledgment

The authors would like to thank the College of Engineering, Universiti Teknologi MARA, 40450 UiTM Shah Alam for the support grant in publishing this paper.

REFERENCES

[1] H. N. Rafsanjani and A. Ghahramani, "Towards utilizing internet of things (IoT) devices for understanding individual occupants' energy usage of personal and shared appliances in office buildings," *Journal of Building Engineering,* vol. 27, p. 100948, 2020.

[2] M. Ezechina, K. Okwara, and C. Ugboaja, "The Internet of Things (Iot): a scalable approach to connecting everything," *The International Journal of Engineering and Science,* vol. 4, no. 1, pp. 09-12, 2015.

[3] K. Furdík and G. Lukác, "Events processing and device interoperability in a smart office IoT application," in *Central European Conference on Information and Intelligent Systems*, 2012: Faculty of Organization and Informatics Varazdin, p. 387.

[4] M. A. A. Razali, M. Kassim, N. A. Sulaiman, and S. Saaidin, "A ThingSpeak IoT on Real Time Room Condition Monitoring System," in *2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, 2020: IEEE, pp. 206-211.

[5] A. Abdi, "Designing smart campus using Internet of Things," *International Journal of Computer Science Trends and Technology,* vol. 6, no. 3, pp. 109-116, 2018.

[6] N. N. A. Aziz, R. M. A. Rechie, B. B. M. Bakry, R. A. Rahman, and Y. M. Yussoff, "Analysing Smart Home Security Using Packet Tracer Simulation Software," in *2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2021: IEEE, pp. 239-244.

[7] N. L. Ismail, M. Kassim, M. Ismail, and R. Mohamad, "A review of low power wide area technology in licensed and unlicensed spectrum for IoT use cases," *Bulletin of Electrical Engineering and Informatics,* Article vol. 7, no. 2, pp. 183-190, 2018, doi: 10.11591/eei.v7i2.1174.

[8] A. Jaafar, M. Kassim, C. K. Haroswati, and C. K. Yahya, "Dynamic home automation security (DyHAS) alert system with laser interfaces on webpages and windows mobile using Rasberry PI," in *2016 7th IEEE Control and System Graduate Research Colloquium, ICSGRC 2016 - Proceeding*, 2017, pp. 153-158, doi: 10.1109/ICSGRC.2016.7813319. [Online]. Available:

[9] N. Naik, C. Shang, Q. Shen, and P. Jenkins, "D-FRI-CiscoFirewall: Dynamic fuzzy rule interpolation for Cisco ASA Firewall," in *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2019: IEEE, pp. 1-6.

[10] A. H. Ahmed and M. N. Al-Hamadani, "Designing a secure campus network and simulating it using Cisco packet tracer," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 23, no. 1, pp. 479-489, 2021.

[11] M. T. Arefin, M. R. Uddin, N. A. Evan, and M. R. Alam, "Enterprise Network: Security Enhancement and Policy Management Using Next-Generation Firewall (NGFW)," in *Computer Networks, Big Data and IoT*: Springer, 2021, pp. 753-769.

[12] M. H. M. Zaharuddin, R. A. Rahman, and M. Kassim, "Technical comparison analysis of encryption algorithm on site-to-site IPSec VPN," in *ICCAIE 2010 - 2010 International Conference on Computer Applications and Industrial Electronics*, 2010, pp. 641-645, doi: 10.1109/ICCAIE.2010.5735013. [Online]. Available:

[13] Z. A. Najar and R. N. Mir, "Wi-Fi: WPA2 Security Vulnerability and Solutions," *Wireless Engineering and Technology,* vol. 12, no. 2, pp. 15-22, 2021.