Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2024, № 3 (115) https://doi.org/10.33108/visnyk_tntu2024.03
ISSN 2522-4433. Web: ***visnyk.tntu.edu.ua***

UDC 004.056.53

SECURITY OF REMOTE IOT SYSTEM MANAGEMENT BY INTEGRATING FIREWALL CONFIGURATION INTO TUNNELED TRAFFIC

Oleksiy Mishko[1]; Danylo Matiuk[2,1]; Maryna Derkach[2,1]

[1]Volodymyr Dahl East Ukrainian National University, Kyiv, Ukraine
[2]Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

Abstract*. The issue of increasing the security level of the IoT system is considered in this paper. To provide individual and secure access to the system remotely, firewall data packet filtering rules were integrated into the VPN connection using the WireGuard protocol. Such security mechanism was implemented and tested on the developed smart lighting system, which enables effective control of lighting brightness in real time. The IoT system is based on ESP32 microcontroller and is integrated with Home Assistant platform. Using web server and Docker technology, the system is efficient and flexible to manage various IoT devices in one centralized environment, and MikroTik Hap AC Lite router with RouterOS v7.7 operating system provides reliable network infrastructure.*

Key words: *security, IoT system, firewall, VPN, network, traffic, access, integration, protocol.*

https://doi.org/10.33108/visnyk_tntu2024.03.122 *Received 13.06.2024*

1. INTRODUCTION

Internet of Things (IoT) devices are becoming an integral part of everyday life. The number of devices in which this technology is implemented increases every year [1–3]: from home thermostats and lighting to cars and medical equipment [4, 5]. However, the problem of compatibility between different devices, as well as the issue of security of data storage and transmission, is also growing [6–8].

Home Assistant is one of the platforms that can assist in solving these problems. This free operating system offers unified environment for managing IoT devices, regardless of manufacturer or model, thereby ensuring flexible and efficient interaction between them in home environment [9]. Since Home Assistant has the ability to integrate various devices and systems, it is an excellent solution for creating home automation system with single control panel [10]. Home Assistant can be used in the local network, which additionally increases the security level. In order to use the system outside your home network, you can set up virtual private network (VPN) directly on your router [11–13].

Objective of the paper is to integrate firewall packet filtering rules into VPN connection, making it possible to redirect through the home LAN, providing individual and secure access to IoT system remotely.

2. MAIN PART

2.1. Statement of the problem. The main component of the home automation system is the web server, which is a single-board Nvidia Jetson Nano computer with Ubuntu operating system. Docker platform is used to virtualize Linux environments. Home Assistant is installed and accessible via IP address of a single-board computer and port 8123, launched as Docker container, which enables flexible deployment, scalability and consistency of operations in various environments. The IoT system also uses MikroTik Hap AC Lite router running on the RouterOS v7.7 operating system, which is used to manage networks with high efficiency and security in a variety of areas, including large corporate networks, small businesses, and home networks. IoT system also uses MikroTik Hap AC Lite router running on RouterOS v7.7 operating system, which is used to manage networks with high efficiency and security in various areas, including large enterprise networks, small businesses and home networks. This router provides not only basic routing functionality, but also offers advanced network configuration options. Due to the built-in RouterOS tools, you can deeply configure firewall rules, network connectivity, and security, including VPN connections, which makes the network environment more reliable and secure [14].

2.2. Setting up VPN connection. The general security mechanism of the home automation system is shown in Figure 1.

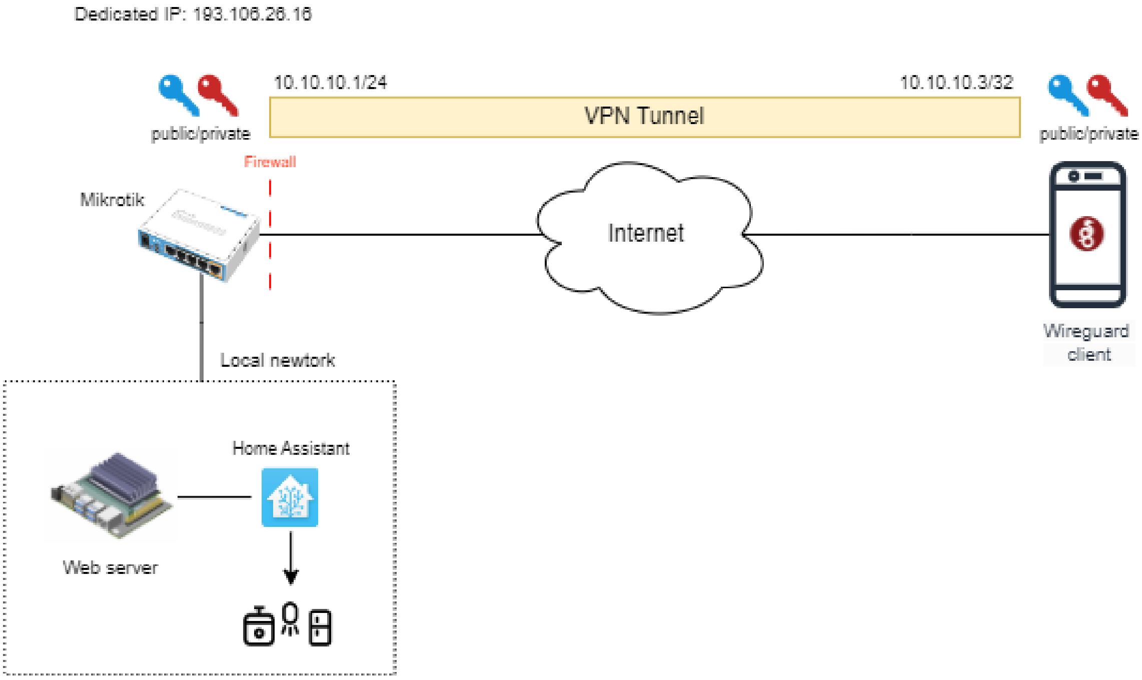


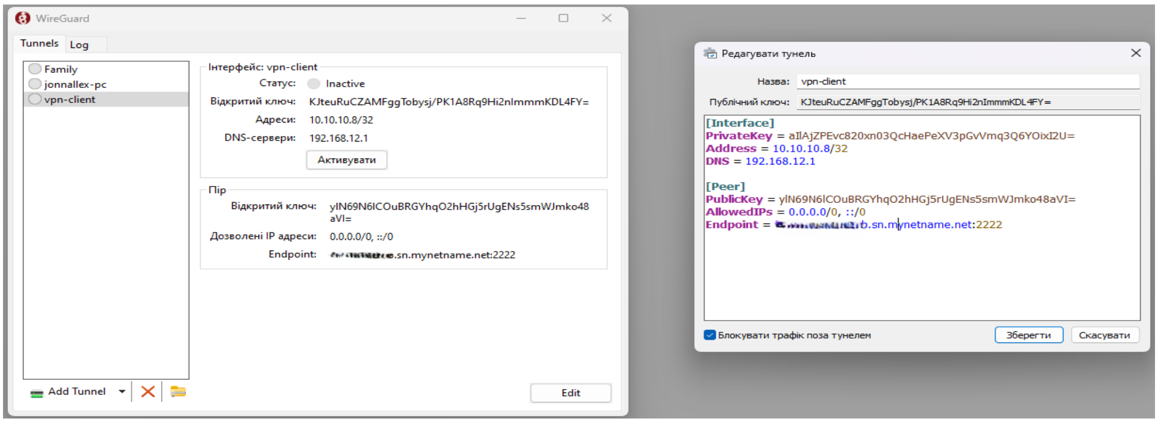
Figure 1. General security mechanism of IoT system

Access to IoT system control is limited by the local network increasing security and reducing the risk of unauthorized access from the outside. This solution makes it possible for users to control the home automation system only from devices connected to the local network, providing additional level of data protection and privacy.

Modern and efficient VPN protocol – WireGuard, was used in order to build the VPN tunnel, which was configured directly on the router, thereby creating encrypted VPN connection between two endpoints [15]. Unlike other protocols, WireGuard obfuscates packet metadata, including transmission length and IP addresses of senders and receivers, so keys for each packet are negotiated privately without third parties, making it much faster and more secure as there are no potential leaks when exchanging keys with the central server.

Public and private keys are generated automatically in the settings configuration. The port for connection was set, and then the WireGuard client was created and configured (Fig. 2).

IP address for peer-to-peer connection was entered in the WireGuard interface: 10.10.10.8/32. DNS server of the local network and the public key of the interface configured earlier were also installed. The allowed IP addresses of the local subnet and the router's DDNS address were added as endpoints.



○ Family
○ jonnallex-pc
○ vpn-client

Інтерфейс: vpn-client
Статус: ○ Inactive
Відкритий ключ: KJteuRuCZAMFggTobysj/PK1A8Rq9Hi2nlmmmKDL4FY=
Адреси: 10.10.10.8/32
DNS-сервери: 192.168.12.1
Активувати

Пір
Відкритий ключ: yIN69N6ICOuBRGYhqO2hHGj5rUgENs5smWJmko48aVI=
Дозволені IP адреси: 0.0.0.0/0, ::/0
Endpoint: [redacted].sn.mynetname.net:2222

Редагувати тунель
Назва: vpn-client
Публічний ключ: KJteuRuCZAMFggTobysj/PK1A8Rq9Hi2nImmmKDL4FY=

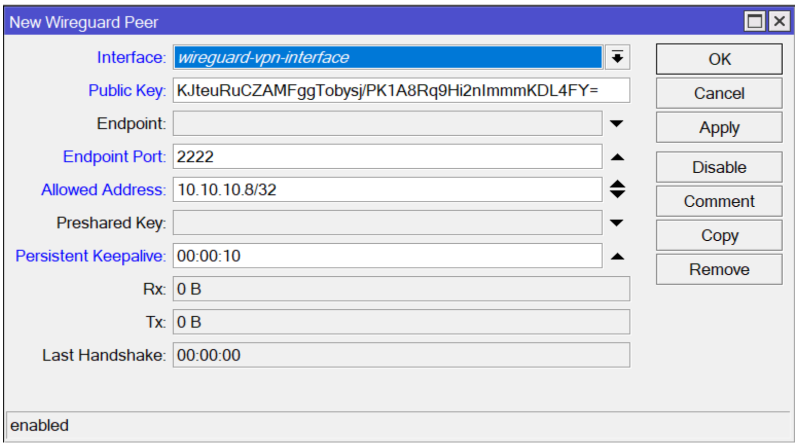
```
[Interface]
PrivateKey = aIlAjZPEvc820xn03QcHaePeXV3pGvVmq3Q6YOixI2U=
Address = 10.10.10.8/32
DNS = 192.168.12.1

[Peer]
PublicKey = ylN69N6lCOuBRGYhqO2hHGj5rUgENs5smWJmko48aVI=
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = [redacted]b.sn.mynetname.net:2222
```

☑ Блокувати трафік поза тунелем
Зберегти
Скасувати

Figure 2. Wireguard client settings

Next, we configured directly peer-to-peer connection in RouterOS. For this purpose, WireGuard interface was selected, the public key from WireGuard client was entered, IP address and port were specified, and handshake time was set to 10 seconds (Fig. 3).



New Wireguard Peer

Interface: wireguard-vpn-interface
Public Key: KJteuRuCZAMFggTobysj/PK1A8Rq9Hi2nImmmKDL4FY=
Endpoint:
Endpoint Port: 2222
Allowed Address: 10.10.10.8/32
Preshared Key:
Persistent Keepalive: 00:00:10
Rx: 0 B
Tx: 0 B
Last Handshake: 00:00:00

enabled

Figure 3. Peer connection settings

2.3. Setting up firewall data packet filtering rules. The next step was to set up the firewall for the computer network protection from unauthorized access, control traffic and filter data packets, prohibiting or allowing specific network traffic based on specified rules and security policies. For this purpose, you should enter /ip/firewall/filter and create new firewall rule, i.e., in the settings, specify «Chain» parameter, which indicates the chain, that is, where the rule will be applied in the network stack, since each chain is responsible for processing packets on a certain stage of their movement via the router. Also, you should determine the IP address that sends or receives packets to which the rule is applied (Fig. 4 a).

In general, the following rules should be set for optimized setting (Fig. 4 b):

1. The rule is intended for receiving packets in the «input» chain using UDP protocol on port 2222, for connecting Wireguard clients.

2. The rule is designed to receive packets in the «input» chain, which are related to already established or related connections. Such packets have already been pre-processed and are allowed into the network without additional verification. This is useful for handling input traffic which is the part of active connections.

3. The rule is intended for permission ICMP packets that include ping requests and responses in the «input» chain. ICMP protocol is used for remote diagnostics and testing of the availability of network devices.

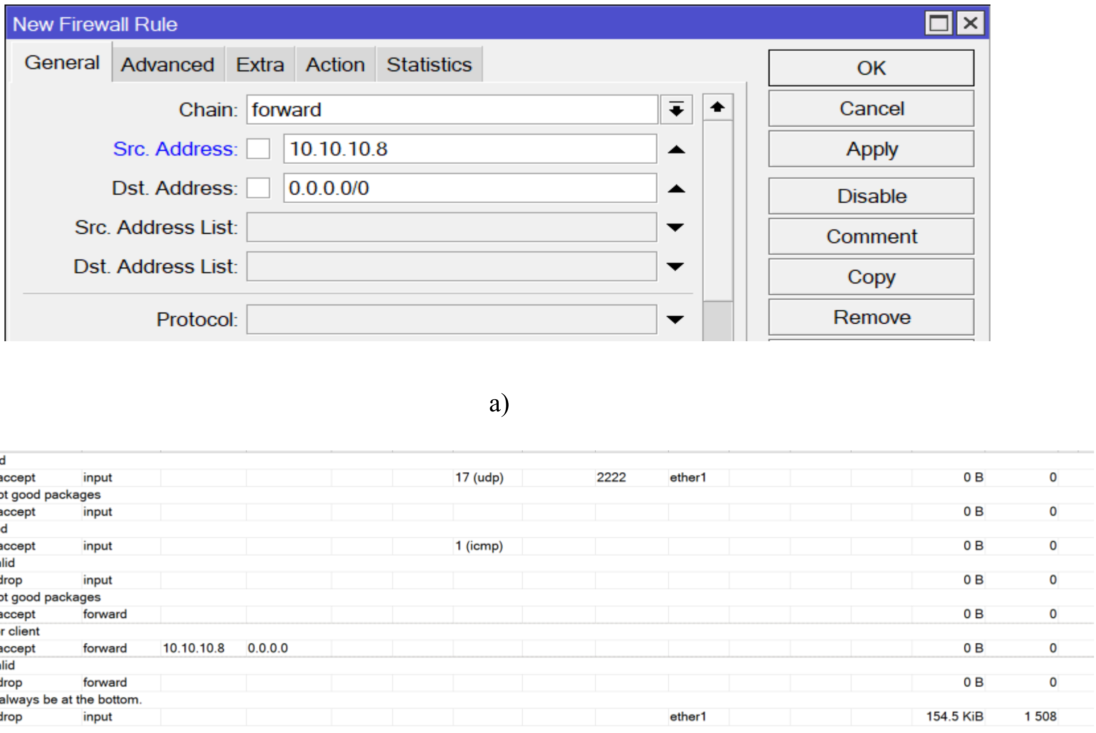
4. The rule rejects any packets in the «input» chain that are recognized as invalid for connections. Invalid packets can be attacking attempts or erroneous packets.

5. The rule is similar to the first one, but it is applied to packets forwarded via the router in the «forward» chain. Established and related connections are allowed without additional control.

6. The rule is created to receive packets in the «forward» chain for Wireguard client 10.10.10.8/32 to access the entire network.

7. The rule performs the same function as the third rule, but in the «forward» chain. All invalid packets transmitted via the router will be rejected.

8. The rule is designed to register packets in the system log and drop all incoming traffic coming through the WireGuard- interface ether1.



Chain: forward

Src. Address: □ 10.10.10.8

Dst. Address: □ 0.0.0.0/0

Src. Address List:

Dst. Address List:

Protocol:

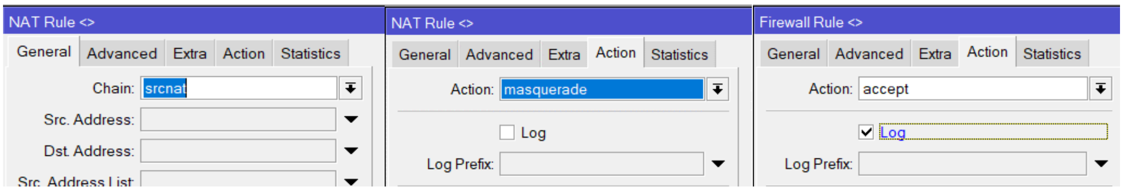
a)

;;; Wireguard									
0	✓ accept	input			17 (udp)	2222	ether1	0 B	0
;;; We accept good packages									
1	✓ accept	input						0 B	0
;;; Ping Good									
2	✓ accept	input			1 (icmp)			0 B	0
;;; Drop invalid									
3	✗ drop	input						0 B	0
;;; We accept good packages									
4	✓ accept	forward						0 B	0
;;; Accept for client									
5	✓ accept	forward	10.10.10.8	0.0.0.0				0 B	0
;;; Drop invalid									
6	✗ drop	forward						0 B	0
;;; It should always be at the bottom.									
7	✗ drop	input					ether1	154.5 KiB	1 508

b)

Figure 4. Firewall settings: a) creation of the new rule, b) all given rules

In addition, in order to have the access to the global network for all devices connected to the router, NAT rule is configured (Fig. 5). The «masquerade» rule conditionally replaces the device's local address with the external address from the provider, through which access to the global network (ip/firewall/nat) is provided. To check the rules validity, you can add logging, that is, use «Ping Good» rule and the computer command line for ping.



Chain: srcnat
Src. Address:
Dst. Address:
Src. Address List:

Action: masquerade
□ Log
Log Prefix:

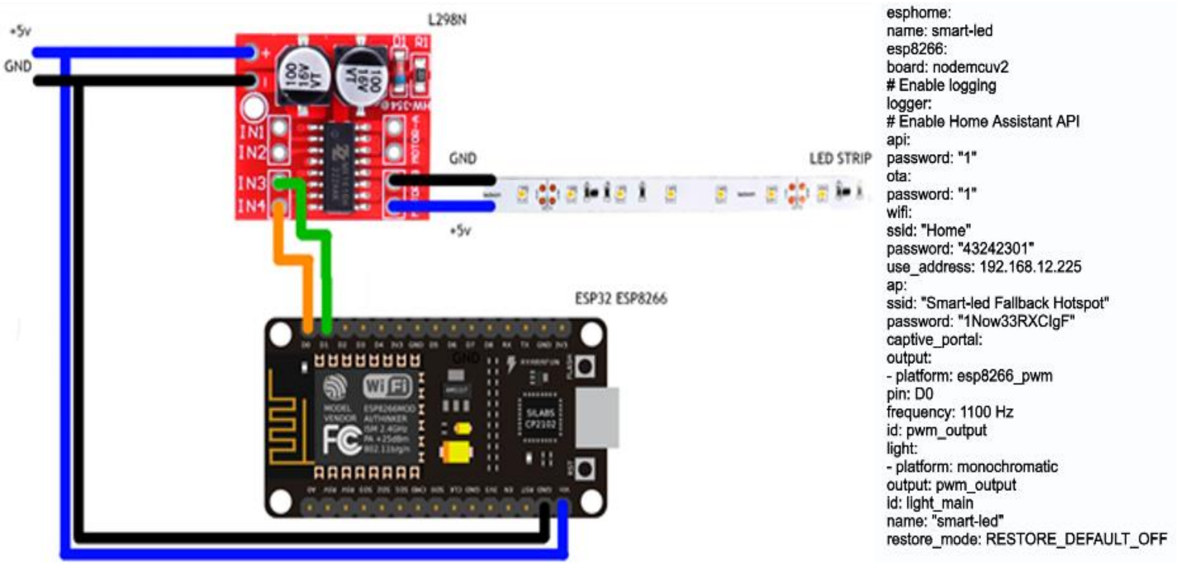
Action: accept
☑ Log
Log Prefix:

Figure 5. NAT rule settings

This completes the configuration of VPN connection to the local network with integrated firewall packet filtering rules, and by activating the configuration on Wireguard client in the mobile or desktop application, all traffic will be automatically redirected through VPN tunnel to the local network. This makes it possible to get safe and reliable access to the local network from anywhere in the world.

2.4. Home automation system testing. In order to test the safety mechanism, smart lighting system based on ESP32 ESP8266 microcontroller, L298N motor driver, and LED strip was implemented (Fig. 6). Change of the lighting brightness is provided by the motor driver that receives PWM (pulse width modulation) signal and uses it to adjust the level of illumination.

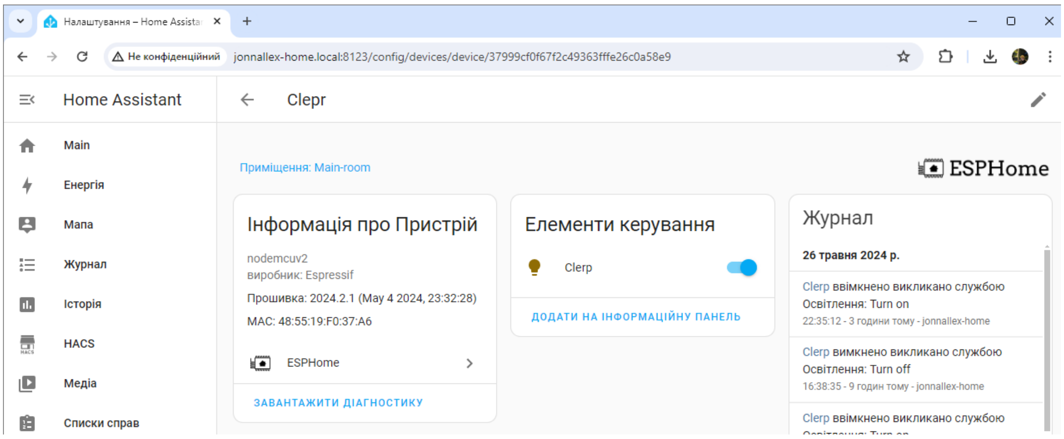
ESPHome platform, which has intuitive interface for creating firmware, was used to program and integrate the microcontroller with the home automation system. ESPHome configuration file describes the settings for ESP8266 platform that controls the lighting system using LED strips. The firmware is downloaded from single-board computer via USB cable and by means of ESPHome Docker container.



```
esphome:
name: smart-led
esp8266:
board: nodemcuv2
# Enable logging
logger:
# Enable Home Assistant API
api:
password: "1"
ota:
password: "1"
wifi:
ssid: "Home"
password: "43242301"
use_address: 192.168.12.225
ap:
ssid: "Smart-led Fallback Hotspot"
password: "1Now33RXClgF"
captive_portal:
output:
- platform: esp8266_pwm
pin: D0
frequency: 1100 Hz
id: pwm_output
light:
- platform: monochromatic
output: pwm_output
id: light_main
name: "smart-led"
restore_mode: RESTORE_DEFAULT_OFF
```

Figure 6. Smart lighting system scheme

After assembling the smart lighting system and downloading the microcontroller firmware, the system is integrated into Home Assistant and added to the control panel (Fig. 7).


Налаштування – Home Assista
jonnallex-home.local:8123/config/devices/device/37999cf0f67f2c49363fffe26c0a58e9
Не конфіденційний
Home Assistant
Clepr
Main
Енергія
Мапа
Журнал
Історія
HACS
Медіа
Списки справ
ESPHome

Приміщення: Main-room

Інформація про Пристрій

nodemcuv2
виробник: Espressif

Прошивка: 2024.2.1 (May 4 2024, 23:32:28)

MAC: 48:55:19:F0:37:A6

ESPHome

ЗАВАНТАЖИТИ ДІАГНОСТИКУ

Елементи керування

Clerp

ДОДАТИ НА ІНФОРМАЦІЙНУ ПАНЕЛЬ

Журнал

26 травня 2024 р.

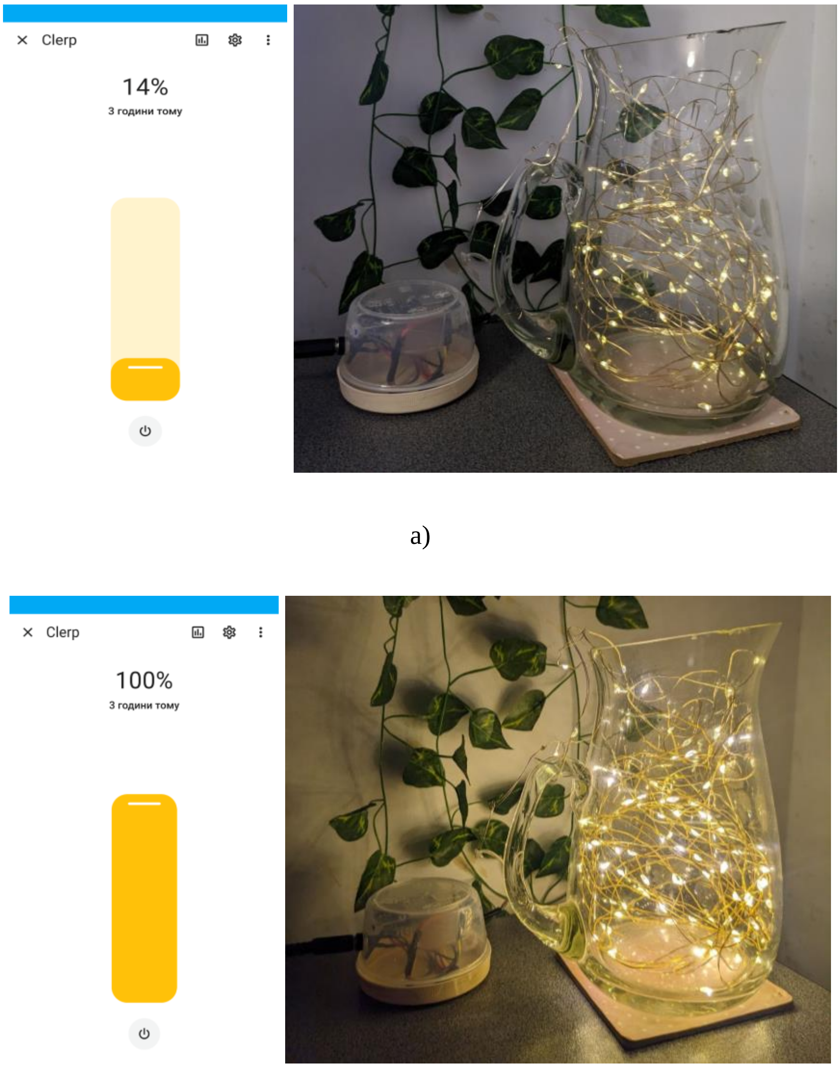
Clerp ввімкнено викликано службою Освітлення: Turn on
22:35:12 - 3 години тому - jonnallex-home

Clerp вимкнено викликано службою Освітлення: Turn off
16:38:35 - 9 годин тому - jonnallex-home

Clerp ввімкнено викликано службою

Figure 7. Integrated device in Home Assistant

In Figure 8 you can see the test results, namely, how the illumination level of IoT system changes depending on the settings in Home Assistant.



a)

b)

Figure 8. Test results: a) minimum lighting level, b) maximum lighting level

3. CONCLUSION

Thus, smart lighting system based on ESP32 microcontroller has been implemented and tested, making it possible to control effectively the lighting brightness in real time. IoT system is integrated with Home Assistant platform, which demonstrates the high level of security and reliability for creation of the smart home environment not only providing the automation routine tasks but also increasing the comfort and efficiency of various devices application in everyday life. Due to the application of web server and Docker technology, the system is efficient and flexible enough to manage a variety of IoT devices in one centralized environment. MikroTik Hap AC Lite router with RouterOS v7.7 operating system provides reliable network infrastructure and additional features to increase the level of security, such as configuration of firewall data packet filtering rules and creation of VPN tunnel by means of WireGuard protocol in order to use the system outside your home network.

Reference

1. Skarga-Bandurova I., Derkach M. (2019). Iot For Public Transport Information Service Delivering. Internet of Things for Industry and Human Applications. Volume 3. Assessment and Implementation. Intelligent Transportation Systems and IoT. Section 41. Ministry of Education and Science of Ukraine, National Aerospace University KhAI, pp. 373-401.
2. Skarga-Bandurova I., Derkach M., Kotsiuba I. The information service for delivering arrival public transport prediction. *In 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS),* 2018, pp. 191–195. https://doi.org/10.1109/IDAACS-SWS.2018.8525787
3. Palamar A., Karpinski M., Palamar M., Osukhivska H., Mytnyk M. Remote Air Pollution Monitoring System Based on Internet of Things. *In 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP),* 2022, pp. 194–204.
4. Lundin A. C., Özkil A. G., Schuldt-Jensen J. Smart cities: A case study in waste monitoring and management. *In 50th Hawaii International Conference on System Sciences (HICSS),* 2017, pp. 1392–1401.
5. Derkach M., Lysak V., Skarga-Bandurova I., Kotsiuba I. Parking Guide Service for Large Urban Areas. *In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),* 2019, vol. 1, pp. 567–571. https://doi.org/10.1109/IDAACS.2019.8924401
6. Starchenko V. (2021) Traffic optimization in wifi networks for the internet of things. *Scientific Journal of TNTU,* vol. 104, no. 4, pp. 131–142. https://doi.org/10.33108/visnyk_tntu2021.04.131
7. Fox J., Donnellan A., Doumen L. The deployment of an IoT network infrastructure, as a localised regional service. *IEEE 5th World Forum on Internet of Things (WF-IoT),* 2019, pp. 319–324. https://doi.org/10.1109/WF-IoT.2019.8767188
8. Waters D., Donnellan A., Fox J. An adaptable internet of things network infrastructure implemented for a smart building system. *In 2021 32nd Irish Signals and Systems Conference (ISSC),* 2021, pp. 1–7. https://doi.org/10.1109/ISSC52156.2021.9467837
9. Kolodiichuk L. (2023) Using the Home Assistant Digital Platform to Control the Electrical Installation. *Energy & Automation,* no. 1. https://doi.org/10.31548/energiya1(65).2023.165
10. Beshley M., Shkoropad Y., Beshley H. (2024) Development of a cyber-physical system for automation and control of the Internet of things using the Home Assistant platform. *Information and communication technologies, electronic engineering,* vol. 4, no. 1, pp. 20–30. https://doi.org/10.23939/ictee2024.01.020
11. Xu Z., Ni J. Research on network security of VPN technology. *In 2020 International Conference on Information Science and Education (ICISE-IE),* 2020, pp. 539–542. https://doi.org/10.1109/ICISE51755.2020.00121
12. Farooq M., Khan R., Khan M. H. (2023) Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices. *Indian Journal of Science and Technology,* 16 (33), pp. 2609–2621. https://doi.org/10.17485/IJST/v16i33.1262
13. Carcelén J. S. P., Parra M. G. O. (2024) Comparison of efficiency, security and stability between RouterOS from MikroTik and Cisco IOS, in network engineering environments. *Revista Científica Interdisciplinaria Investigación y Saberes,* 14 (2), pp. 42–62.
14. Vergütz A., Santos B. V. d., Kantarci B., Nogueira M. (2023) Data Instrumentation From IoT Network Traffic as Support for Security Management. *In IEEE Transactions on Network and Service Management,* vol. 20, no. 2, pp. 1392–1404. https://doi.org/10.1109/TNSM.2022.3233673

15. Donenfeld J. A. WireGuard: Next Generation Kernel Network Tunnel. Network and Distributed System Security Symposium, 2017. https://doi.org/10.14722/ndss.2017.23160

УДК 004.056.53

БЕЗПЕКА ВІДДАЛЕНОГО КЕРУВАННЯ ІОТ-СИСТЕМОЮ ЗАВДЯКИ ІНТЕГРАЦІЇ НАЛАШТУВАННЯ ФАЄРВОЛУ ДО ТУНЕЛЬОВАНОГО ТРАФІКА

Олексій Мишко[1]; Данило Матюк[2,1]; Марина Деркач[2,1]

[1]Східноукраїнський національний університет імені Володимира Даля, Київ, Україна
[2]Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

Резюме. *Розглянуто актуальне питання підвищення рівня безпеки віддаленого керування IoT-системи. Для того, щоб забезпечити індивідуальний і безпечний доступ до системи віддалено, інтегровано налаштування фаєрволу до VPN-тунелю. Фаєрвол контролює мережевий трафік і фільтрує пакети даних, забороняючи або дозволяючи специфічний мережевий трафік на основі заданих правил і політик безпеки, тим самим гарантуючи захист комп'ютерної мережі від несанкціонованого доступу, а також те, що лише авторизовані користувачі мають можливість керувати системою домашньої автоматизації дистанційно. Для побудови VPN-тунелю використано протокол WireGuard, що налаштовано безпосередньо на маршрутизаторі. Це дозволило перенаправляти трафік через домашню локальну мережу. В IoT-системі використовується маршрутизатор MikroTik Hap AC Lite, що працює на операційній системі RouterOS v7.7, яка забезпечує надійну мережеву інфраструктуру. Такий механізм безпеки реалізовано й протестовано на розробленій системі розумного освітлення, яка дозволяє ефективно керувати яскравістю освітлення в реальному часі. Для програмування й інтеграції мікроконтролера з системою домашньої автоматизації використано платформу ESPHome. Система домашньої автоматизації, що базується на основі мікроконтролера ESP32 ESP8266, драйвері двигуна L298N і світлодіодній стрічці, інтегрована з платформою Home Assistant. Home Assistant встановлена та доступна за IP-адресою одноплатного комп'ютера Nvidia Jetson Nano, що являє собою веб-сервер з операційною системою Ubuntu, і портом 8123, запущена як Docker-контейнер для віртуалізації Linux-середовищ. Усе це дає можливість гнучкого розгортання, масштабованості та узгодженості операцій задля керування різними IoT-пристроями в одному централізованому середовищі.*

Ключові слова: *безпека, система IoT, фаєрвол, VPN, мережа, трафік, доступ, інтеграція, протокол.*

https://doi.org/10.33108/visnyk_tntu2024.03.122 *Отримано 13.06.2024*