International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
www.computersciencejournals.com/ijcit
IJCIT 2023; 4(2): 01-11
Received: 01-05-2021
Accepted: 12-06-2021

Mohammad Anwar Hossain
Department of CSE, World University of Bangladesh, Dhaka, Bangladesh

Harun Miah
Department of CSE, World University of Bangladesh, Dhaka, Bangladesh

Rana Ahmed
Department of CSE, World University of Bangladesh, Dhaka, Bangladesh

Shayeed Anower
Department of CSE, World University of Bangladesh, Dhaka, Bangladesh

Corresponding Author:
Mohammad Anwar Hossain
Department of CSE, World University of Bangladesh, Dhaka, Bangladesh

Secure Inter-VLAN routing in multi branches office network

Mohammad Anwar Hossain, Harun Miah, Rana Ahmed and Shayeed Anower

DOI: https://doi.org/10.33545/2707661X.2023.v4.i2a.65

Abstract

In contemporary IT contexts, secure inter-VLAN communication is essential for preserving the availability, confidentiality, and integrity of network resources. Secure communication between VLANs is a vital component of network security. It limits access to resources to authorized systems and users and lessens the potential harm caused by security events. Building a solid and secure network architecture requires careful VLAN segmentation implementation. As a consequence, the authors created an adaptable and affordable data protection solution that any company may use. Fortinet Firewall assists in providing inter-VLAN security. In the cybersecurity space, fortinet firewalls are highly respected for a number of reasons, including their scalability, application control, comprehensive protection, and unified threat management (UTM). With the right authorization, an organization may readily connect with one another using this Secure Inter-VLAN.

Keywords: Secure, VLAN, routing, multi-branch, network

1. Introduction

Information or data that is confidential, private, or sensitive can be protected. use, misuse, disclosure or destruction by means of principles and methods that are designed and implemented [1].

A computer network is a system that links two or more devices so they may send and receive resources or data from one another. The network connects all computer devices, ranging from a server to a mobile phone. Physical wires or wireless connections can be used to link these devices.

Verified local area network is known as inter-VLAN. The process of communicating between two or more VLANs within the same network architecture is known as inter-VLAN routing. In a network switch, when numerous VLANs are created, they are often banned by default. The method used to route or send traffic between each other's is called inter-VLAN routing.

Utilizing ACL, firewalls, VPNs, and routing protocol authentication, secure inter-VLAN routing may be put into practice. We can perform network segmentation, device updates, traffic monitoring, user authentication, security audits, prevent unauthorized user access, and guarantee safe communication across VLANs by implementing inter-VLAN routing.

The researchers in this study created an inter-VLAN network that allows two or more branches with several departments within each branch to securely connect with one another. The administrator of the suggested system will have easy control over each department's access to sensitive data with the help of fortinet firewall.

1.1 Objective

The main focus of this research is-

*To secure inter VLAN routing with firewall in multi branches office networks for improving flexibility, easy of management, and secure the network system.

2. Literature Review

The transfer of packets between hosts in separate network corridors throughout the network is referred to as inter-VLAN routing. Given that VLANs are logical connections, they facilitate network membership, which enhances the network's flexibility and performance.

Organizations implement information security measures for a variety of reasons.

The goal of information security is to safeguard all company data. Concurrent implementation of vulnerability management, cryptography, infrastructure security, and information security is typical.

Many research works are being proposed to secure Inter-VLAN Communication.

Ahmad (2020) [2] developed a model named Design and implementation of network security using inter-VLAN-routing. The work finds the enterprise or campus networks are characterized by their large size, making them challenging to manage efficiently. So, the researcher proposed for inter-VLAN routing with DHCP. Because VLANs are widely adopted in these networks to enhance, flexibility, ease of management, and reduce broadcast traffic. They provide Layer 2 security by limiting the number of broadcast domains. This approach reduces complexity and proves to be a cost-effective solution. But In this proposed system we implement this work on layer 3 switch that easier then layer 2 switch and we also use a Fortinet firewall which gives batter security from their work.

Ramdhania *et al*. (2019) [3] Created a network infrastructure design in connectivity using inter-VLAN concept in banding district government. The research conducted at banding district government aims to optimize their network infrastructure using inter-VLAN routing. By implementing inter-VLAN, the infrastructure's single broadcast domain can be divided into multiple domains, allowing different departments to communicate effectively. This improves network performance and reduces hardware costs. Additionally, packet filtering using firewall ensures that only authorized data packets transfer the internal network. Overall, this research benefits the banding district government by enhancing network optimization, communication, and cost savings.

Gerome, M. (2023) [4] developed a model named Design and implement small business office network. This research will emulate a small office network surroundings. The design will demonstrate the process of structure and configuring the network to meet the conditions laid out in the design plan. This network includes four subnets with windows 10 end devices and a kali linux device, it also includes five cisco layer 2 switches. After the network environment is set up, colorful penetration tests are performed from the kali linux device to gather information. They used nmap surveillance tool for overlook the network security. They design this only for a small office but our work can be implementing any big organizations.

Tongkaw S & tongkaw A (2019) [5] has Proposed a system to implement multi-VLAN design over ipsec vpn for campus network. Multi-VLANs have gained significant popularity in the business and education sectors as they enable comfortable and secure network management. The research highlights three main benefits of multi-VLAN design. Firstly, it proves to be a cost-effective solution for deploying multiple applications. By segregating the network into separate VLANs, each application can be assigned to its own VLAN, optimizing resource allocation and reducing infrastructure costs. By implementing multi-VLANs in the two campuses of songkhla rajabhat university, the research demonstrates the advantages of this design approach. It allows for cost-effective deployment of multiple applications, enhances protection and security, and simplifies network administration and management. They setup multi-VLAN and it enables efficient and secure data transmission between the campuses, ensuring the overall performance and effectiveness of the network infrastructure.

Rugeles uribe *et al*. (2021) [6] Develop a technical review of wireless security for the internet of things. This research discusses the vulnerabilities in wireless technologies that provide connectivity to iot devices and evaluates the use of software defined radio (sdr) for conducting wireless attacks on iot technologies. A systematic literature review was conducted to compare the types of vulnerabilities and attacks affecting wireless technologies in the iot ecosystem and identify recent methods to mitigate these attacks. The perception layer of the iot reference model was found to be the most vulnerable, primarily due to hardware limitations, physical device exposure, and technology heterogeneity. The integration of sdr technologies in future cybersecurity systems offers advantages such as flexibility and adaptability to new communication technologies and the potential for advanced tool development. However, addressing the complex cybersecurity challenges of iot requires combining sdr hardware with cognitive and intelligent techniques, such as deep learning, to adapt mitigation systems to rapid technological changes.

3. Methodology

3.1 Methodology

In this project authors used 5 phases to describe the procedure. These phases are planning, requirement analysis, network infrastructure design, development, testing and result. In this part authors tries to clear the whole work by a diagram. In this diagram we describe our work flow.

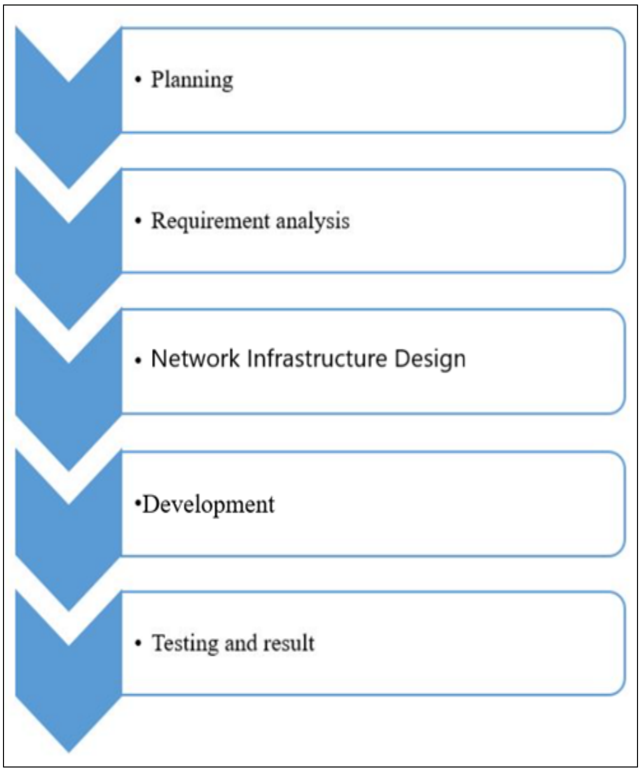


Fig 1: Proposed methodology

3.1.1 Planning

The foundation of any successful research effort is preparation. Because of this, the researchers had a well-defined plan in place before they started their inquiry. The research methodology and study subject are included in the strategy. The writers looked through several research on the same topic before creating this one. Following that, the writers developed the title using the knowledge they had gained from those articles. As the authors reviewed the research, they found that every one had a unique set of limitations. Consequently, the researchers came up with a plan to get around these limitations without sacrificing the uniqueness of the study.

3.1.2 Requirement analysis

Each project has a unique set of requirements that change based on the work being done. The project description contains information about the resources needed for the suggested project.

A. System requirements: System requirement can be divided into two types.

- Software requirements.
- Hardware requirements.

Software requirements

- Eve-ng network simulator.
- VM ware.
- Fortunate image

Hardware requirements

- Laptop or Desktop

B. User Requirements: - user requirements include what the user wants from system. The user need integrity, secrecy, and authentication in addition to other VLAN security features for this.

3.1.3 Network infrastructure design

Network infrastructure depend on organization need. It's a raw design that can be explain the total work. For this we have to discuss with the organization and we have to understand their need and requirements. After this we proposed a design to the organization and explain this proposed properly. If they accept our design we can go ahead to our main work. After getting permission we design this infrastructure in eve-ng network simulator.

3.1.4 Development

In this part authors configured the Switch and firewall in eve-ng network emulator with the proper command. Then need to configure firewall and create different VLAN for different department. Then we implement our selecting ACL in different VLAN. Then we configure inter VLAN access for each other's.

3.1.5 Testing and Result

After implementation, we obtained the outcome that satisfied the organization's needs. Upon implementation, the authors found that what they had been looking for had been accomplished.

4. Analysis, Design and Development

4.1 Requirement gathering technique

4.1.1 Stockholder identification

We know that there are several investors in this kind of network model after analyzing multiple network models. These days, a network system is necessary for any business or organization to do daily tasks. Furthermore, for the protection of its data, every firm needs a secure network infrastructure. We create a contemporary network model. Our network approach is applicable to any type of organization, whether it be government or non-government, school, college, or multi-branch office.

4.1.2 Stakeholder Interview and Question

We arrange several interviews with several organizations. Here is some sample question asked during the interview: -

- Is this easier from our existing system?
- What type of technology do you uses?
- What type of security or device you used for secure our system?
- Could we implement different policy for our different department or user?
- Is it easier to maintenance?
- Is it updated from our current model?
- In this system could we protect our network from unauthorized access from outside?

4.1.3 Legacy system review

The existing legacy system makes use of antiquated network infrastructure, which has drawbacks that render it vulnerable to cyber-attacks, phishing scams, and hacking. Nowadays, the majority of organizations using this kind of network architecture employ layer two switches instead of robust firewalls to safeguard their networks. Its upkeep is also considerably more challenging than our network model. We look for weaknesses in the present network infrastructure and seek to fix them in order to create a more straightforward and safe network infrastructure.

4.2 Design

The authors devised a method that will provide greater security with less complexity, all the while taking into consideration the current system. Any corporation may maintain its departments more effectively and with more security using this suggested model.

4.2.1 Block Diagram

In this diagram authors created a demo diagram for their project.

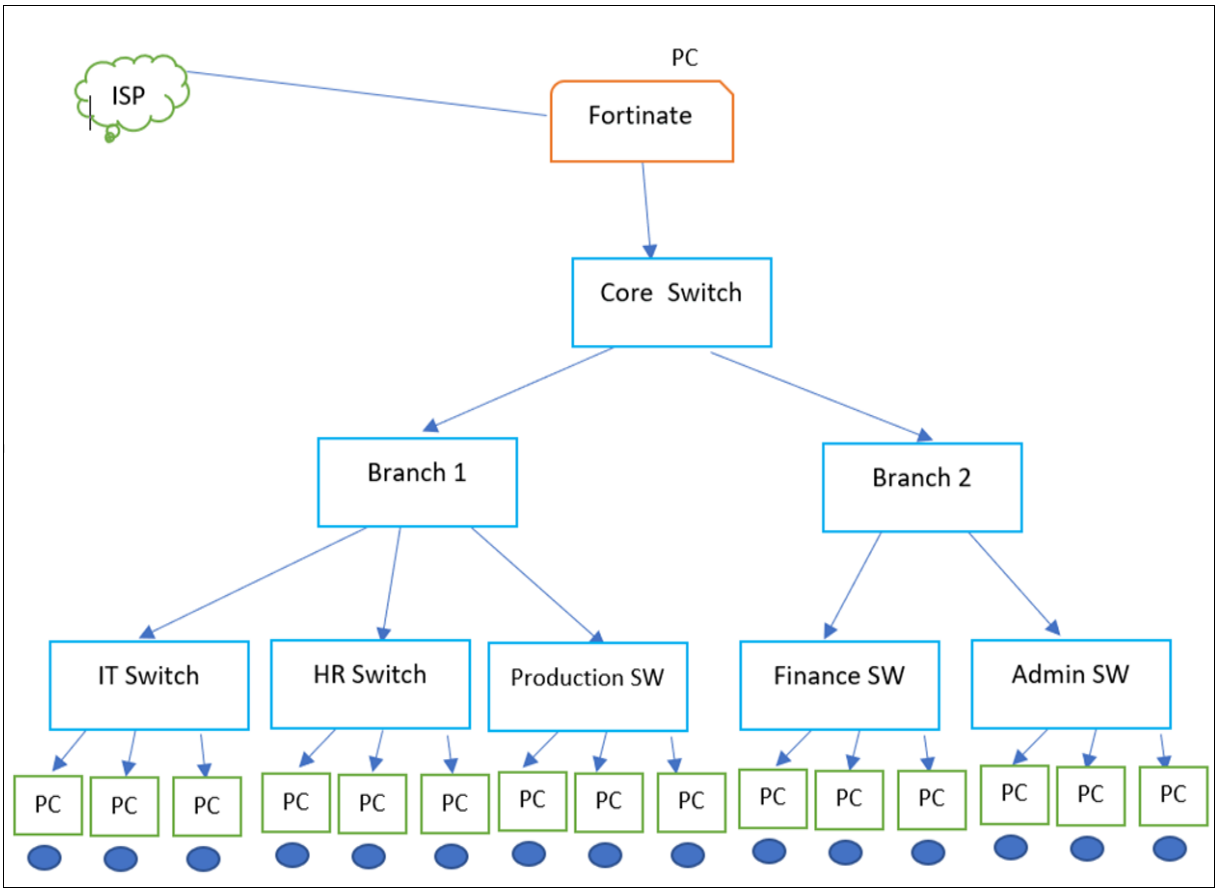
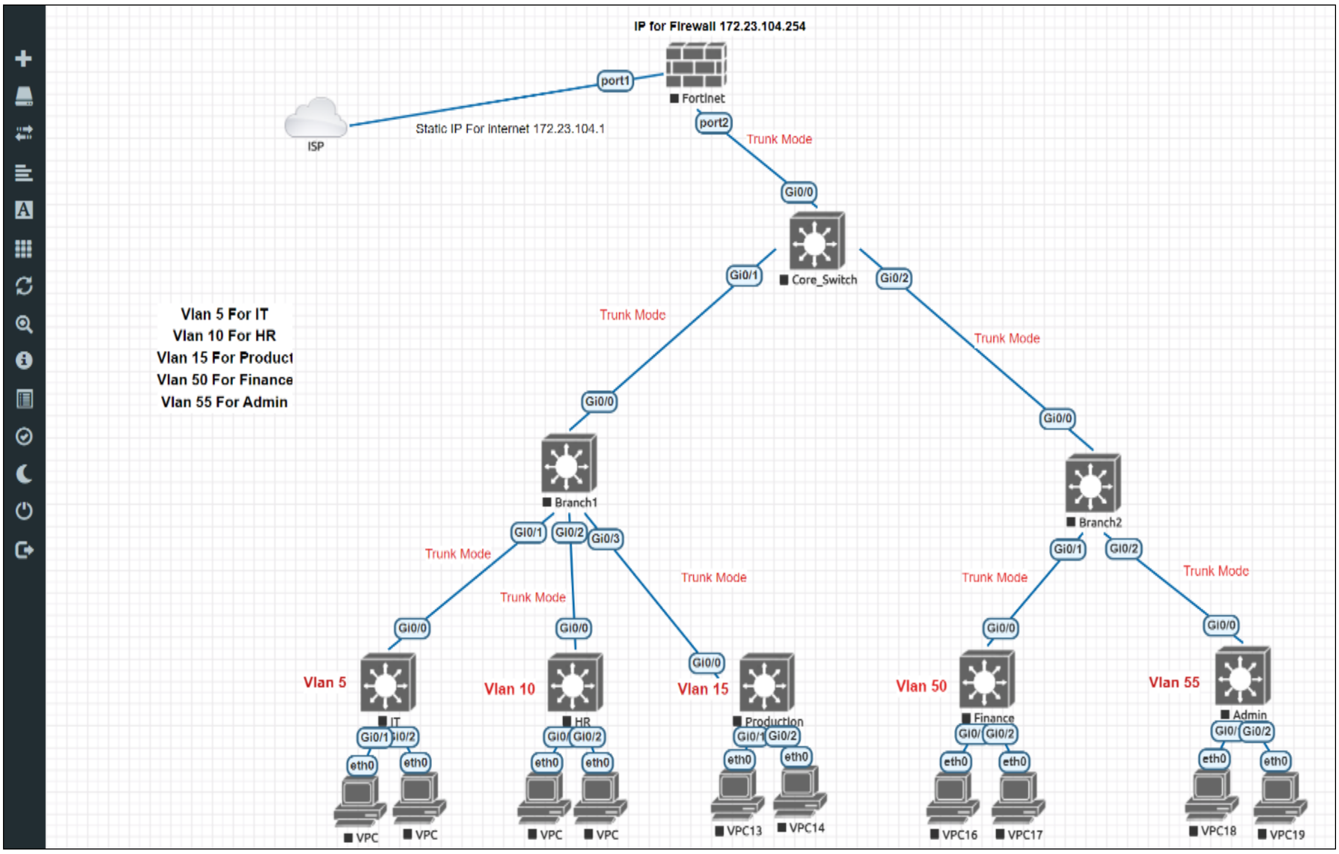


Figure 2. Block Diagram

4.2.2 Network topology

In this section, we use the Eve-ng network simulator to create our network infrastructure. In order to carry out our project, we create our block diagram on an emulator. This is the network emulator version of our infrastructure.


IP for Firewall 172.23.104.254

Static IP For internet 172.23.104.1

Vlan 5 For IT
Vlan 10 For HR
Vlan 15 For Product
Vlan 50 For Finance
Vlan 55 For Admin

Fig 3: Network Topology

4.2.3 Device and technologies implementation

Devices uses: - authors used cisco layer3 switch, Fortinet firewall to execute the design on eve-ng network emulation which gives a real device feel.

Technologies Implemented

- Creating a network topology using eve-ng network emulator software.
- Connecting Networking devices with correct cabling.
- Configure firewall.
- Creating VLANs and assigning ports VLAN numbers.
- Subnetting and IP Addressing.
- Configuring Inter-VLAN Routing.
- Configuring DHCP with each VLAN
- Configuring SSH for secure Remote access.
- Assign switch port on trunk and access mode.
- Create multiple policy for multiple VLAN.
- Test and Verifying Network Communication

4.2.4 Development

Authors setup their gadgets in this section. Initially, they set up their switch. Then established many VLANs that correspond to their department, each with a unique name. Next, they set up the switch port modes so that they can distinguish between access and trunk. Next, they set up their department-based network and security policies as well as firewall. Authors has set up web base access on their fortinet firewall as well. In order to access the online portal, they configured a static IP for our firewall. They also open port 1 to HTTP, SSH, and PING.

5. Project Description

5.1 Fortinet Firewall Configuration

After adding fortinet firewall in network emulator at first, authors configured fortinet port1 which connected with ISP. Then setup a static IP for fortinet and we can access the fortunate web with this IP with username and password.

5.2 Fortinet Firewall Web Login Page

This is Fortinet firewall login page. You have to give your username and password in this page then login.

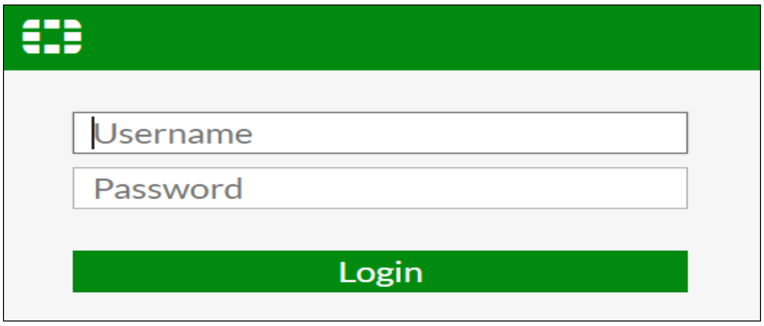
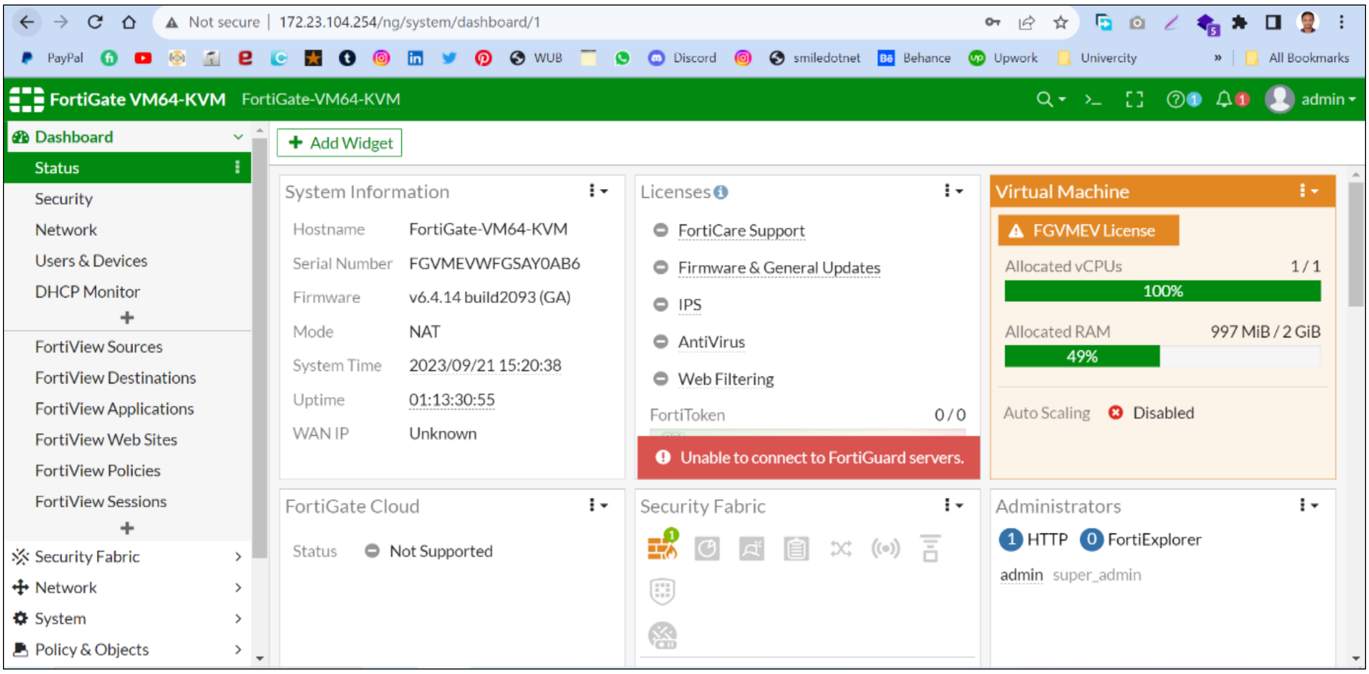


Fig 4: Fortinet Web Login page

5.3 Fortinet Firewall Main Dashboard

After login we can see the dashboard. Its fortinet firewall main dashboard. We can see the all features in left side.



Hostname FortiGate-VM64-KVM
Serial Number FGVMEVWFGSAY0AB6
Firmware v6.4.14 build2093 (GA)
Mode NAT
System Time 2023/09/21 15:20:38
Uptime 01:13:30:55
WAN IP Unknown

FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken 0 / 0
Unable to connect to FortiGuard servers.

FGVMEV License
Allocated vCPUs 1 / 1
100%
Allocated RAM 997 MiB / 2 GiB
49%
Auto Scaling Disabled

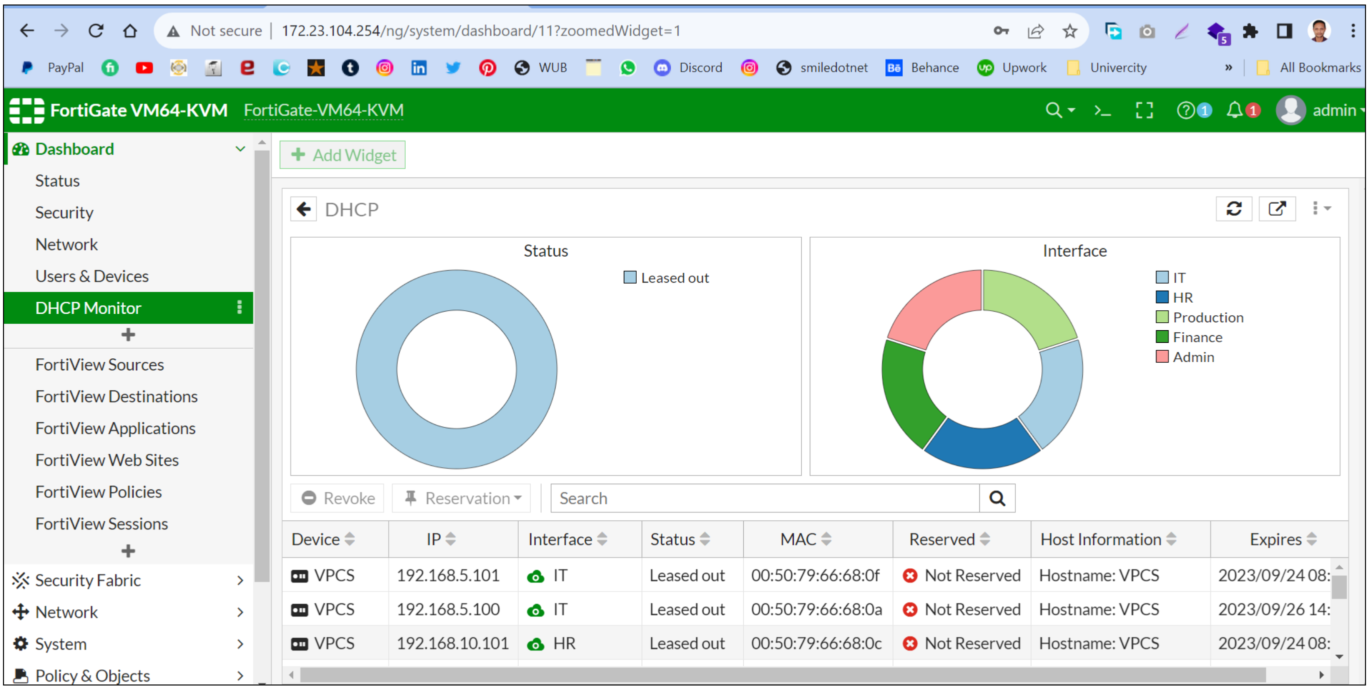
Status Not Supported

1 HTTP 0 FortiExplorer
admin super_admin

Fig 5: Fortinet firewall Main dashboard

5.4 Fortinet Firewall DHCP Dashboard

This is DHCP monitoring dashboard. In this page we can see all of the pc which is under the DHCP. We can see the status, IP, MAC and hostname also.

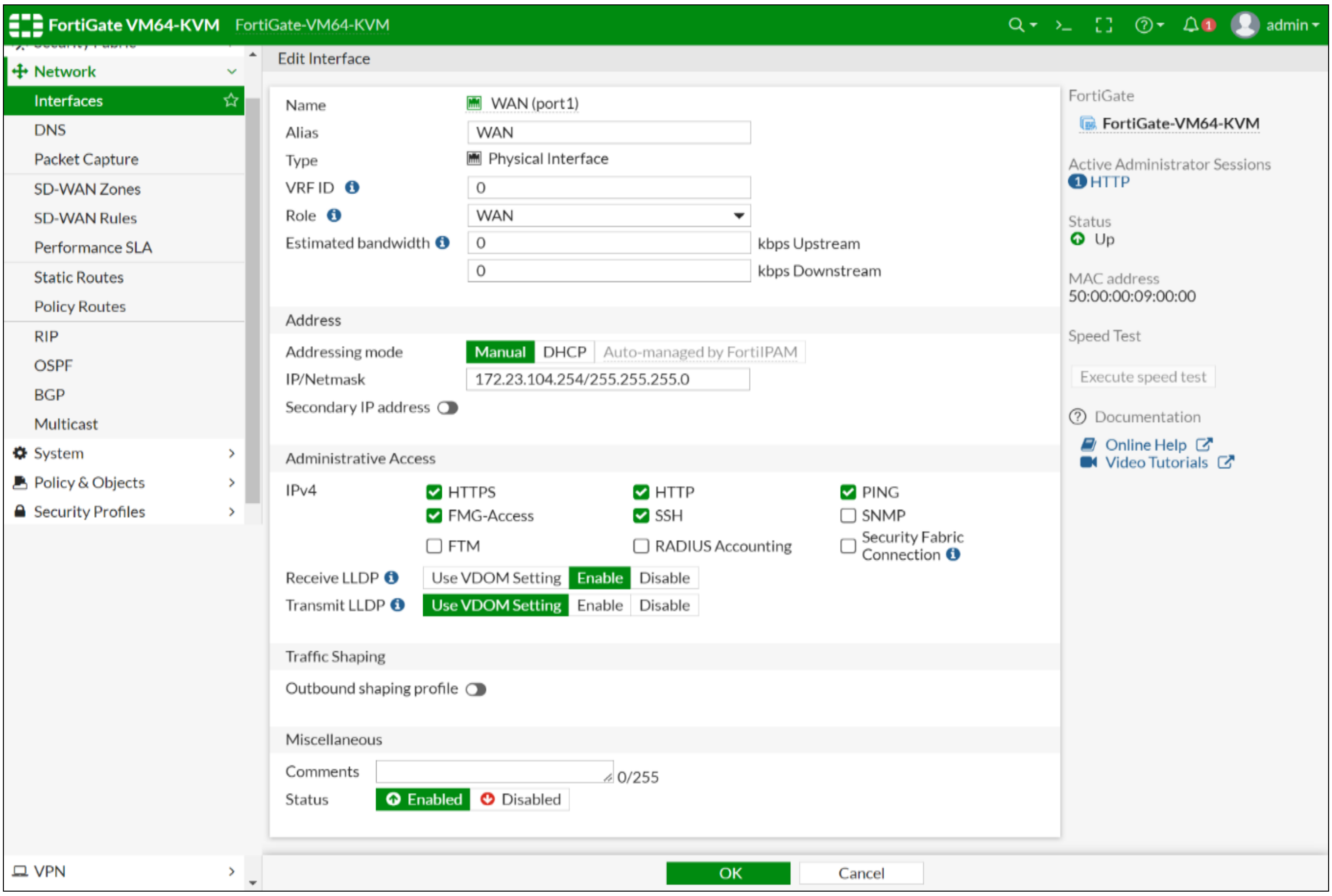


Device	IP	Interface	Status	MAC	Reserved	Host Information	Expires
VPCS	192.168.5.101	IT	Leased out	00:50:79:66:68:0f	Not Reserved	Hostname: VPCS	2023/09/24 08:
VPCS	192.168.5.100	IT	Leased out	00:50:79:66:68:0a	Not Reserved	Hostname: VPCS	2023/09/26 14:
VPCS	192.168.10.101	HR	Leased out	00:50:79:66:68:0c	Not Reserved	Hostname: VPCS	2023/09/24 08:

Fig 6: Fortinet Firewall DHCP Dashboard

5.5 Fortinet Firewall WAN Port Configuration

In this page we can see how authors configured their fortinet firewall WAN port in which one connected with the ISP. In this part they configure their fortinet WAN port for internet access. Here we can select the port role as WAN which connected with ISP or internet.



Edit Interface

Name: WAN (port1)
Alias: WAN
Type: Physical Interface
VRF ID: 0
Role: WAN
Estimated bandwidth: 0 kbps Upstream
0 kbps Downstream

Address
Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM
IP/Netmask: 172.23.104.254/255.255.255.0
Secondary IP address ○

Administrative Access
IPv4: ☑ HTTPS ☑ HTTP ☑ PING
☑ FMG-Access ☑ SSH □ SNMP
□ FTM □ RADIUS Accounting □ Security Fabric Connection
Receive LLDP: Use VDOM Setting [✓ Enable] Disable
Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

Traffic Shaping
Outbound shaping profile ○

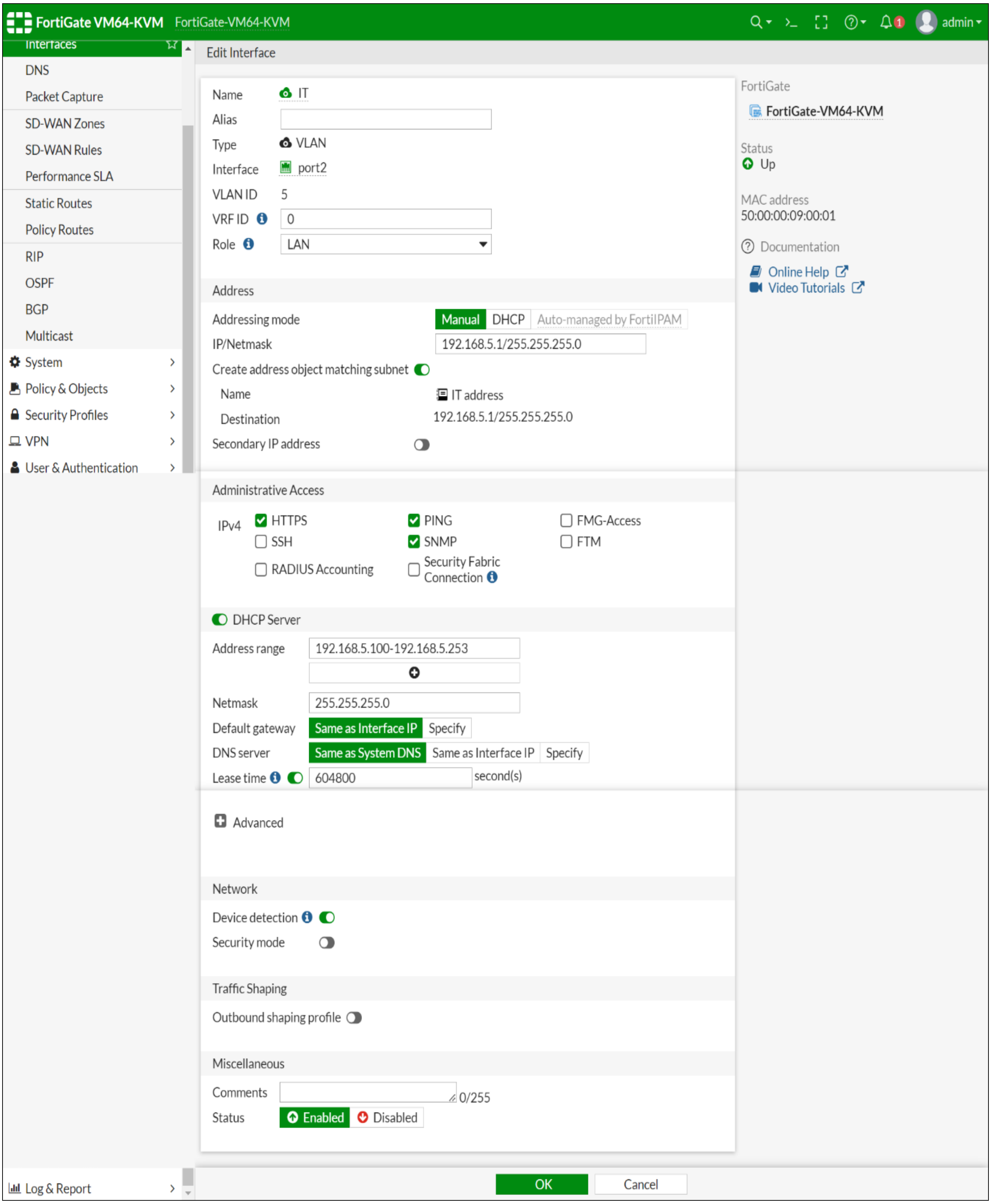
Miscellaneous
Comments: 0/255
Status: [✓ Enabled] Disabled

FortiGate
FortiGate-VM64-KVM
Active Administrator Sessions
1 HTTP
Status
Up
MAC address
50:00:00:09:00:00
Speed Test
Execute speed test
Documentation
Online Help
Video Tutorials

Fig 7: Fortinet Firewall WAN Port Configuration

5.6 VLAN Creation and Configuration

Here VLAN is created and VLAN wise department configuration is also done here. Here authors created a VLAN and set an IP address and enable DHCP mode for each VLAN and select DHCP range and here they also configure administrative access list.



Edit Interface

Name: IT
Alias:
Type: VLAN
Interface: port2
VLAN ID: 5
VRF ID: 0
Role: LAN

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM
IP/Netmask: 192.168.5.1/255.255.255.0
Create address object matching subnet: ●
Name: IT address
Destination: 192.168.5.1/255.255.255.0
Secondary IP address: ○

Administrative Access

IPv4: ☑ HTTPS ☑ PING □ FMG-Access □ SSH ☑ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection

● DHCP Server

Address range: 192.168.5.100-192.168.5.253
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify
Lease time ●: 604800 second(s)

Advanced

Network

Device detection: ●
Security mode: ○

Traffic Shaping

Outbound shaping profile: ○

Miscellaneous

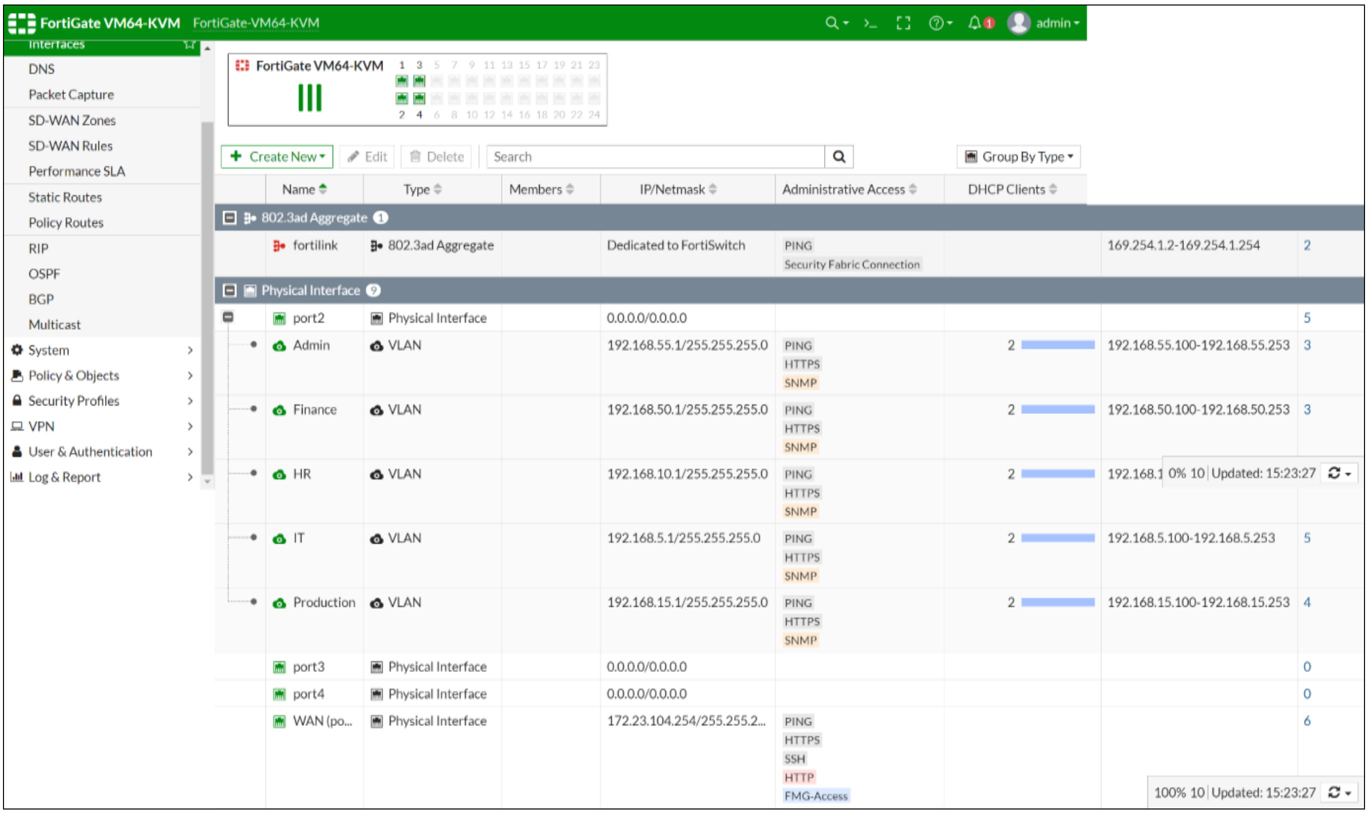
Comments: 0/255
Status: [✓ Enabled] Disabled

FortiGate: FortiGate-VM64-KVM
Status: Up
MAC address: 50:00:00:09:00:01
Documentation: Online Help, Video Tutorials

Fig 8: VLAN Creation and DHCP Configuration for Each VLAN

5.7 All VLAN List Dashboard

Here shows all VLAN which was created for different department. We create our all VLAN under the fortinet port2.



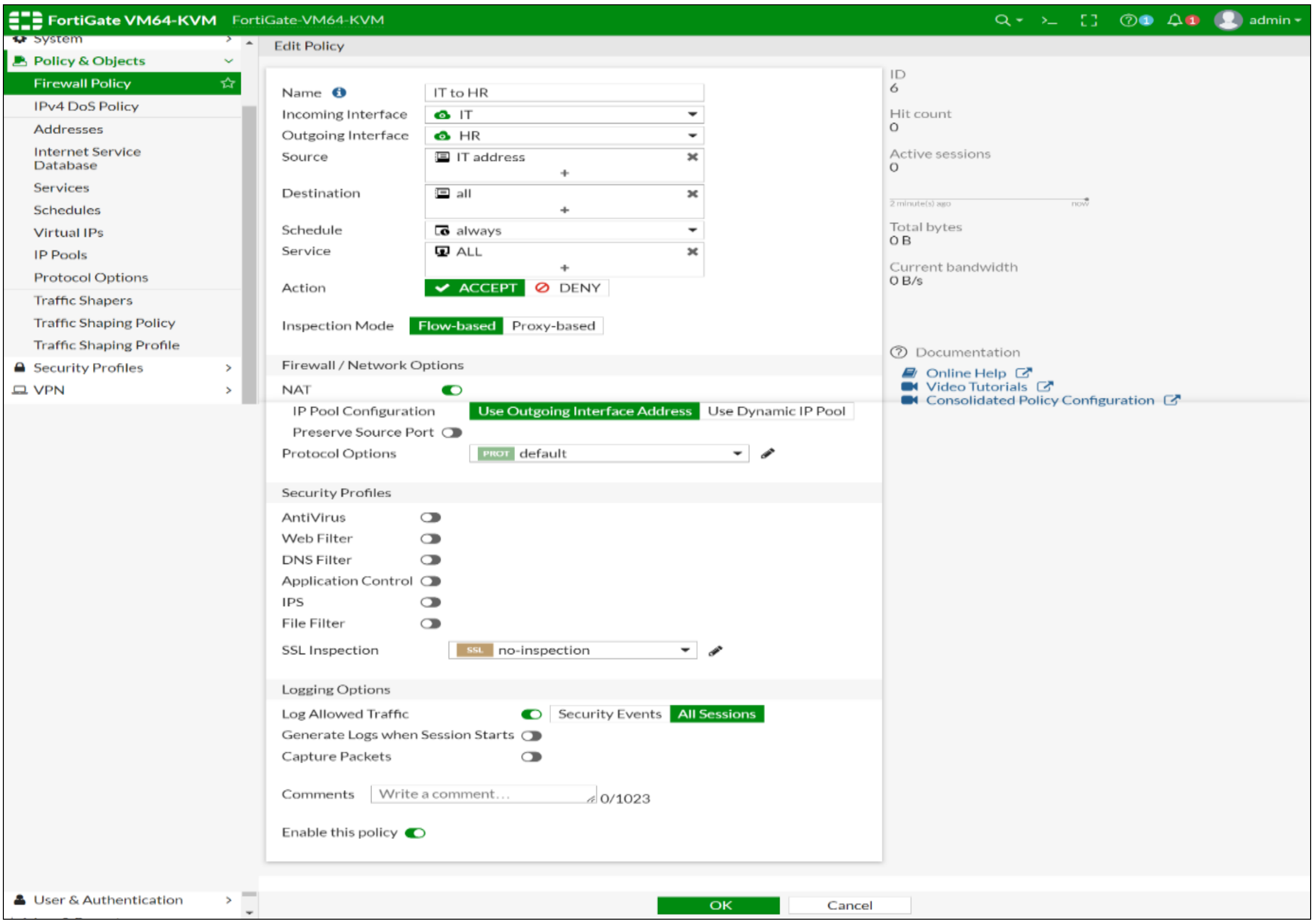
Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients		
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Physical Interface 9							
port2	Physical Interface		0.0.0.0/0.0.0.0				5
Admin	VLAN		192.168.55.1/255.255.255.0	PING HTTPS SNMP	2	192.168.55.100-192.168.55.253	3
Finance	VLAN		192.168.50.1/255.255.255.0	PING HTTPS SNMP	2	192.168.50.100-192.168.50.253	3
HR	VLAN		192.168.10.1/255.255.255.0	PING HTTPS SNMP	2	192.168.1 0% 10 Updated: 15:23:27	
IT	VLAN		192.168.5.1/255.255.255.0	PING HTTPS SNMP	2	192.168.5.100-192.168.5.253	5
Production	VLAN		192.168.15.1/255.255.255.0	PING HTTPS SNMP	2	192.168.15.100-192.168.15.253	4
port3	Physical Interface		0.0.0.0/0.0.0.0				0
port4	Physical Interface		0.0.0.0/0.0.0.0				0
WAN (po...	Physical Interface		172.23.104.254/255.255.2...	PING HTTPS SSH HTTP FMG-Access			6

100% 10 Updated: 15:23:27

Fig 9: All VLAN List Dashboard

5.8 VLAN to VLAN Access Configuration

In this part authors configured inter VLAN routing. Here they configured which VLAN can communicate with other VLAN in the organization.



Edit Policy

Name: IT to HR
Incoming Interface: IT
Outgoing Interface: HR
Source: IT address
Destination: all
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options: PROT default

Security Profiles

AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
File Filter ○
SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]
Generate Logs when Session Starts ○
Capture Packets ○

Comments: Write a comment... 0/1023

Enable this policy ●

ID
6

Hit count
0

Active sessions
0

2 minute(s) ago now

Total bytes
0 B

Current bandwidth
0 B/s

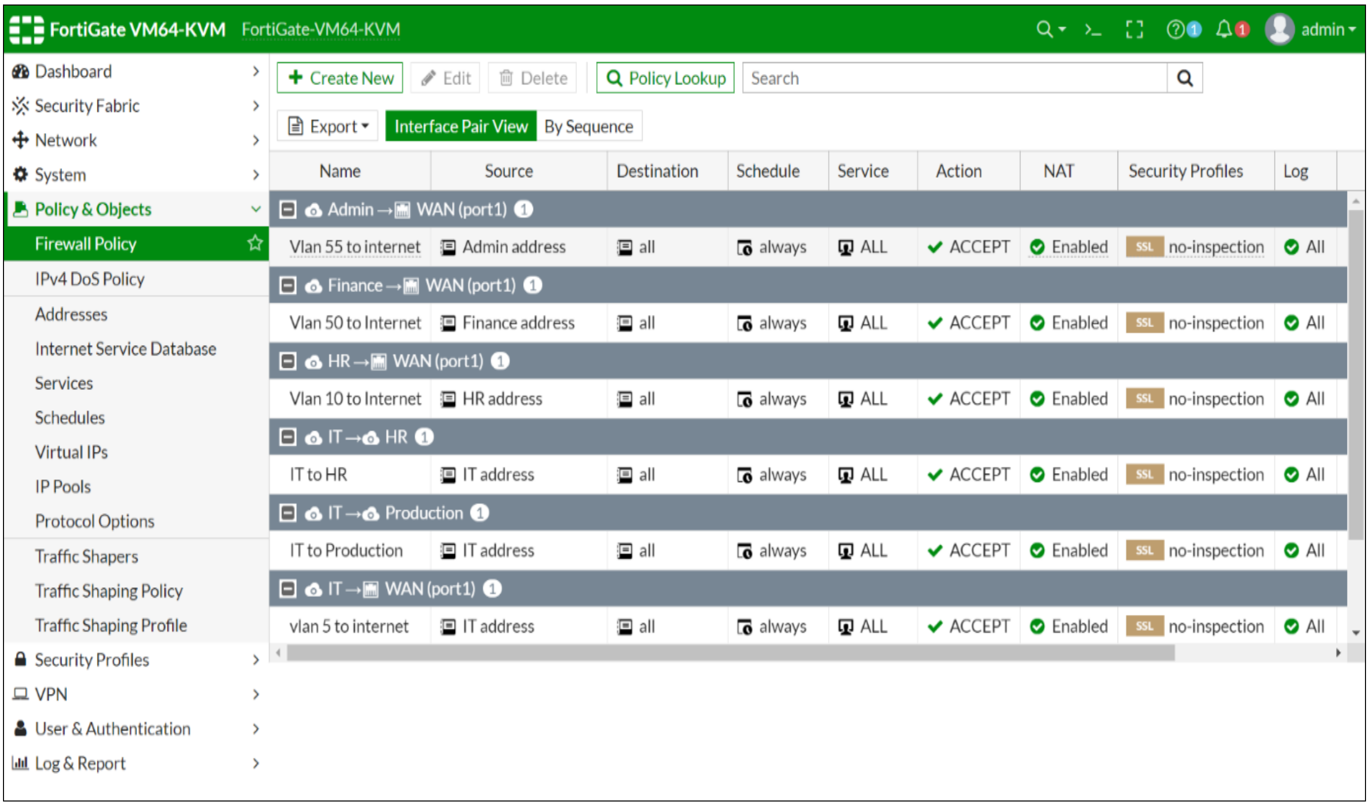
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration

OK Cancel

Fig 10: VLAN to VLAN Access

5.9 All Policy Dashboard

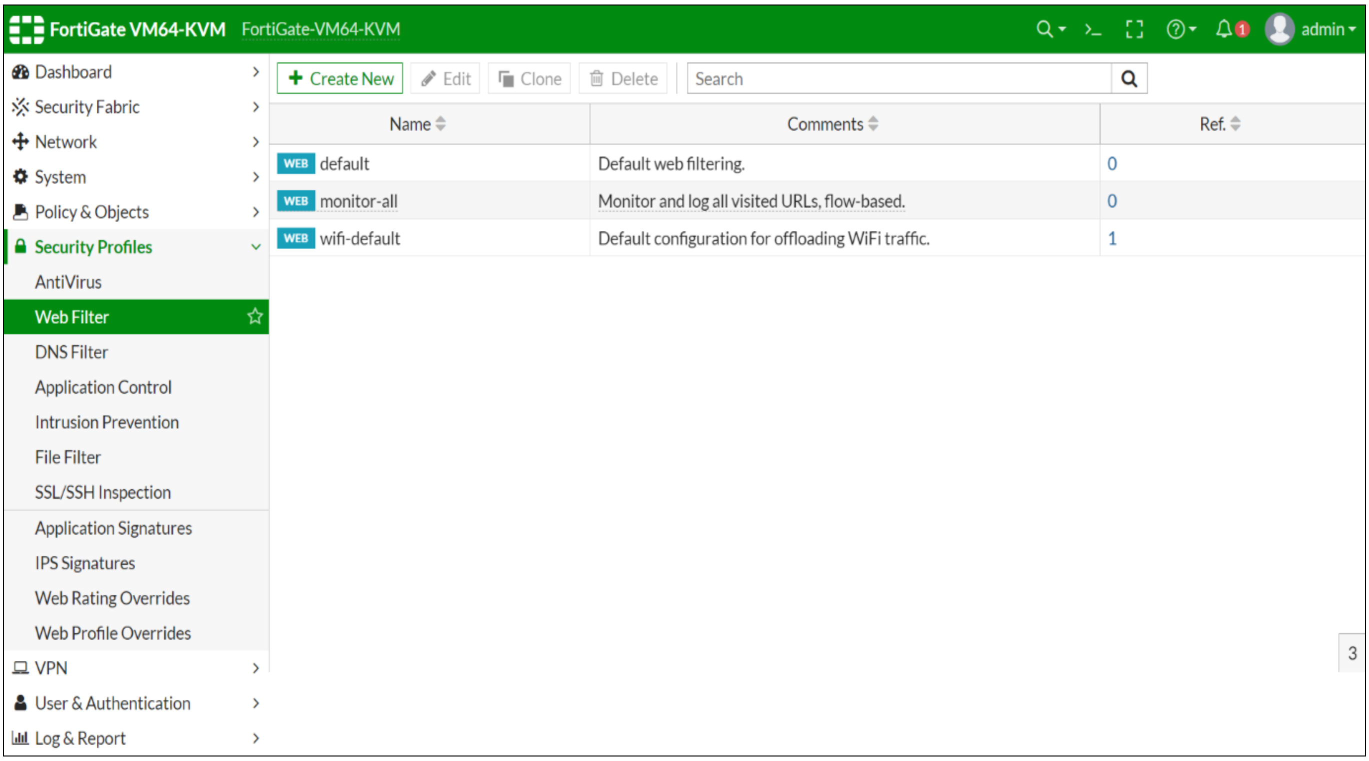
In this page we can see firewall all policy which one created before. From this page we can also create a new policy and we can edit existing policy also.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Admin → WAN (port1) 1								
Vlan 55 to internet	Admin address	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All
Finance → WAN (port1) 1								
Vlan 50 to Internet	Finance address	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All
HR → WAN (port1) 1								
Vlan 10 to Internet	HR address	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All
IT → HR 1								
IT to HR	IT address	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All
IT → Production 1								
IT to Production	IT address	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All
IT → WAN (port1) 1								
vlan 5 to internet	IT address	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All

Fig 11: All Policy Dashboard

5.10 Web Policy Dashboard

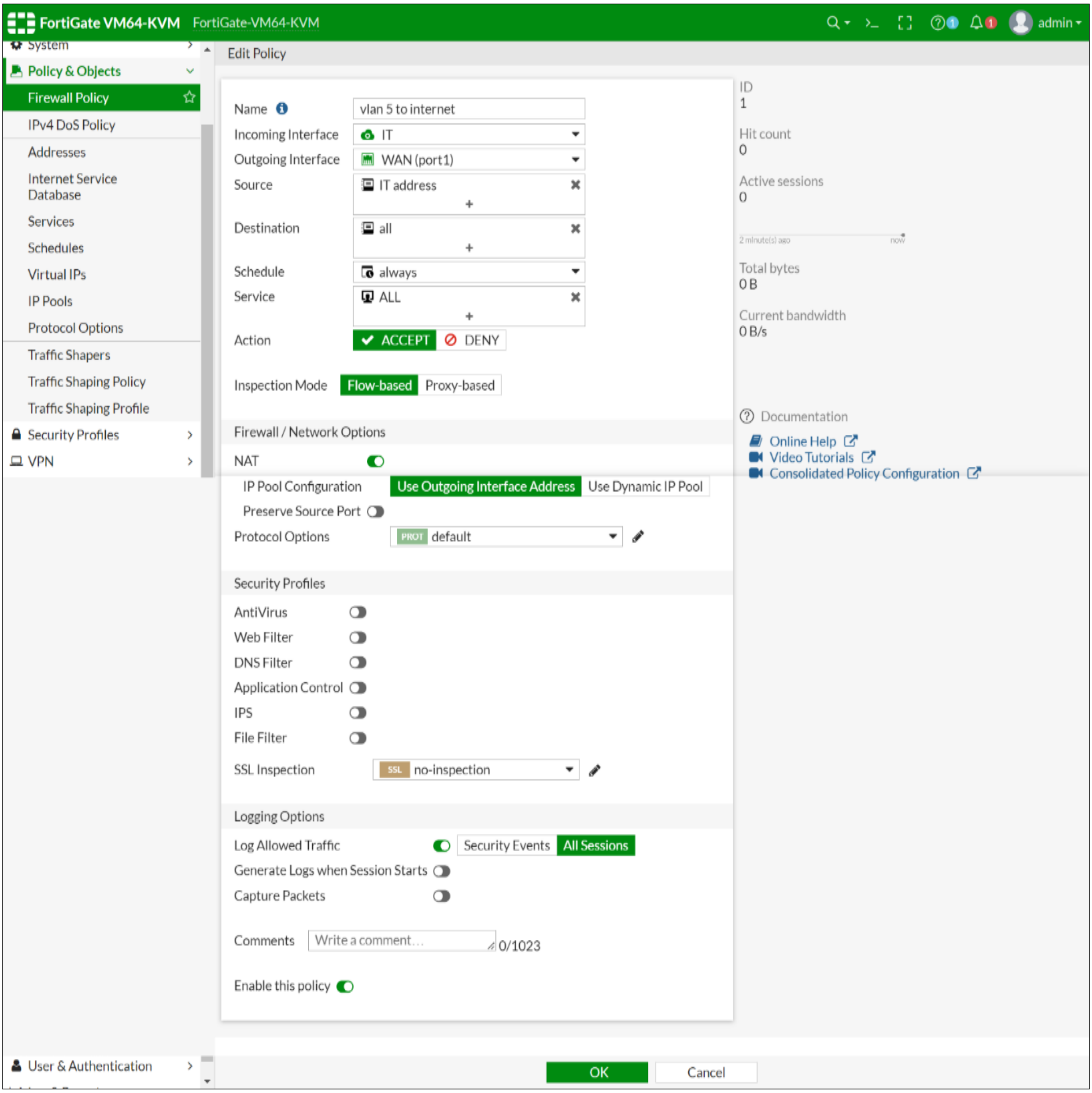


Name	Comments	Ref.
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

Fig 12: Web Policy Dashboard

5.11 Policy Creation for Internet

Here authors created a policy for internet access. They selected a VLAN as incoming interface and selected WAN (port1) as outgoing interface.



Edit Policy

Name: vlan 5 to internet
Incoming Interface: IT
Outgoing Interface: WAN (port1)
Source: IT address
Destination: all
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options: PROT default

Security Profiles

AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
File Filter ○
SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]
Generate Logs when Session Starts ○
Capture Packets ○

Comments: Write a comment... 0/1023

Enable this policy ●

ID
1

Hit count
0

Active sessions
0

Total bytes
0 B

Current bandwidth
0 B/s

Fig 13: Policy Creation for Internet

5.12 Core switch configuration

This is where authors set up their main switch. In order to tag this switch, they first modify its hostname. Next, each VLAN is created and given a name and number. Next, they set up a trunk mode on its linked ports, which enables us to send all of the signals for every switch and router via a single link and the primary switch on the branch is set up the same way.

5.13 Department switch configuration

Every department is assigned a single switch. Thus, authors establish a single VLAN with the number that is configured or chosen in the branch and core switches. Next, they establish a trunk port that is linked to the main switch of the branch or its uplink port. The others, which were connected to the user, were all made to port as access. Additionally, they set up which VLAN is accessible on this port.

6. Conclusion

Through the use of Inter-VLAN routing in a multi-branch office network, businesses may build a resilient and adaptable network architecture that changes with their demands. This technique ensures that data flows easily and securely while supporting the organization's development and compliance needs. It also makes communication between various branches and departments safe and effective. Inter-VLAN routing is a critical component of a contemporary, networked, and highly effective multi-branch office network in the ever changing corporate environment.

The entire inter-VLAN routing functionality is offered by the suggested solution. You may simply communicate between departments in your business with this proposed solution. In addition to controlling their access list, you may see their activity. You can guarantee the security and privacy of every department in accordance with their requirements with the aid of this system. As a result, this system offers strong security and improved internal communication.

6.1 Future work: The project can be added some technology such as: -

- Implement secure remote access solutions for branches remote access connectivity.
- Content filtering option can be used.
- Different type of tunneling

7. Acknowledgments

This paper and the research behind it would not have been possible without the exceptional support of our supervisor, Mohammad Anwar Hossain. His enthusiasm, knowledge and exacting attention to detail have been an inspiration and kept our work. Harun Miah, Rana Ahmed and Shayeed Anower, my colleagues at World University of Bangladesh, have also looked over my transcriptions and answered with unfailing patience numerous questions about the Paper. I am grateful to all of those with whom I have had the pleasure to work during this.

8. References

1. https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html
2. Ahmad I. Design and implementation of network security using inter-VLAN-routing and DHCP, SSRN. Asian Journal of Applied Science and Technology. 2020 July-September;4(3):37-44.
3. Ramdhania AN, Kurniawan MT, Hediyanto UYKS. “Network Infrastructur Design in connectivity using Inter-VLAN concept in Bandung District Government” ICTCE '19: Proceedings of the 3rd International Conference on Telecommunications and Communication Engineering, November 2019, 111–115. DoI: https://doi.org/10.1145/3369555.3369562
4. Gerome M. Small Business Office Network; c2023. IdeaExchange@UAkron. Available at: https://ideaexchange.uakron.edu/honors_research_projects/1688/
5. Tongkaw S, Tongkaw A. Multi-VLAN design over IPSec VPN for Campus Network. IEEE Xplore, IEEE; c2019. DOI: 10.1109/ICWISE.2018.8633293
6. Rugeles Uribe J de J, Guillen EP, Cardoso LS. A technical review of wireless security for the internet of things: Software defined radio perspective. Journal of King Saud University - Computer and Information Sciences. 2021-2022 July;34(7):4122-4134.