Aptisi Transactions on Technopreneurship (ATT)
Vol. 5 No. 2Sp 2023

P-ISSN: 2655-8807
E-ISSN: 2656-8888

Implementation of Wireless User Authentication using WLC-Forti Framework

Ignatius Agus Supriyono[1], Irwan Sembiring[2], Adi Setiawan[3], Iwan Setyawan[4], Theophilus Wellem[5], Henderi[6], Ilham Hizbuloh[7]
Faculty of Science and Technology[1,6,7], Faculty of Information Technology[2,3,4,5]
University of Raharja[1,6,7], Satya Wacana Christian University[2,3,4,5]

e-mail: ignatius@raharja.info[1], irwan@uksw.edu[2], adi.setiawan@uksw.edu[3], iwan.setyawan@uksw.edu[4], theophilus.wellem@uksw.edu[5], henderi@raharja.info[6], ilham.hizbuloh@raharja.info[7]

Author Notification
01 August 2023
Final Revised
31 August 2023
Published
06 September 2023

Supriyono, I. A., Sembiring, I., Setiawan, A., Setyawan, I., Wellem, T., Henderi, & Hizbuloh, I. (2023). Implementation of Wireless User Authentication using WLC-Forti Framework. Aptisi Transactions on Technopreneurship (ATT), 5(2sp), 234–242.

DOI: https://doi.org/10.34306/att.v5i2sp.346

Abstract

Internet access at this time is a daily necessity that cannot be denied. It is certain that most institutions and business entities require internet access in carrying out their activities, including educational institutions. With the development of mobile computer technology in which more users use mobile devices to access the internet, wireless-based network infrastructure is a demand that cannot be postponed any longer. By using a wireless connection to connect to the network, authentication becomes something that must be considered, the use of access to the network by unwanted parties can harm other parties. Changing passwords regularly is important to avoid misuse of access to the network by other parties. This paper presents a problem where when an educational institution implements the Bring Your Own Device (BYOD) program, students and teachers cannot change passwords using the personal device used, this is because the personal device is not registered with the domain controller at the institution. The solution proposed in this article is to move the NPS RADIUS server function on the local site to LDAP in the cloud using a combination of WLC which handles Wi-Fi clients and Fortinet which handles authentication to the cloud. The implementation results show that the WLC-Forti framework functions well.

Keywords: *Cloud, Authentication, LDAP, Wireless access, Wireless Controller*

1. Introduction

User access authentication [1] on a wireless network [2] becomes something very important to consider, because network access leaks can be recognized by every mobile device such as laptops, iPads, tablets, and smartphones [3]. If the user's authentication access system is not handled properly, this can create an entry point for other unauthorized parties into the wireless network so they can do undesirable things. [4]. Before cloud-based technology developed, the authentication method used the Remote Authentication Dial-In User Service RADIUS method [5] seems to be sufficient to handle this wireless user authentication problem [6]. A Wireless Controller (WLC) [7] can perform authentication by validating user and password on a RADIUS server to grant registered user access to connect

to the wireless network after validating the username and password by WLC to the RADIUS server. The user will be given access to the wireless network, get an IP address from the DHCP server [8] and be given internet access by the Firewall [9] according to the policy that applies to that user. In this study, Windows Server on premise was used, in which Active Directory (AD) and Network Policy System (NPS) services were run to authenticate wireless user access. NPS uses AD data as a reference for authentication. The drawback of this system is that changing the user password can only be done on an on-premises computer connected to the domain controller, it cannot be done on any computer including personal devices (BYOD). Limited access to changing passwords is an obstacle when school management implements the use of personal devices (BYOD) for students and teachers. Teachers, students, and staff cannot change passwords using their own devices. On the other hand, some applications require a password to access them, for example the attendance system and library require different passwords, causing teachers, students, and staff to have to remember many passwords for each application.

At this time, when the cloud-based technology offered can provide services with better features, authentication management that utilizes PaaS has become an option. In this authentication system, the process of changing the password by the user can be done anywhere if the cloud server can be accessed via the internet. In this article PaaS [10] used is Azure Active Directory which runs the LDAP service [8] where the Windows server platform that runs AAD and LDAP services is in the cloud. Even though the Windows platform on Azure offers better service features and access to servers and changing passwords by users becomes easier and more flexible, Cisco WLCs that handle Wireless Access Points (APs) cannot communicate with LDAP in the cloud [11], on the other hand the Fortinet firewall can communicate with servers in the cloud but cannot handle on-premises AP devices. The solution provided in this article is a combination of a WLC Cisco 2504 WLC that can handle Cisco APs with a Fortinet 200F firewall that can communicate with LDAP in the cloud.

Previous studies related to authentication include Talib and Salman [12] conveyed in his article proposing biometrics with finger print as user authentication. Sukarsa et al. [13] in his article, he proposes using RADIUS and Mikrotik Routerboard to perform authentication, in addition to authentication, they use it for bandwidth management. Villanueva and Gonzalez [8] proposes RADIUS and Ubuntu server to perform user authentication. Zhou and Wang [5] in his article examines the use of RADIUS and PPPoE to perform user authentication to access the internet. Assumpta Ezugwu et al. [14] in his research on password-based authentication, stated the importance of a password manager to handle multiple passwords required for several applications.

The contribution to this experiment is the implementation of a WLC-Forti framework by combining WLC which can handle APs with Fortinet which can communicate with the cloud. A virtual LAN (VLAN) is required to connect a virtual port on Fortinet so that it can be recognized by WLC as a gateway to the cloud. The experimental results show that the WLC-Forti framework functions properly, changing passwords can be done directly by the user by logging into the Microsoft cloud. This password can be used in various applications other than Microsoft cloud access, can be used for Wi-Fi authentication and various applications that refer to the LDAP authentication system.

In this article, the literature is presented in section 2, the method used in this research is presented in section 3, the results and discussion are presented in section 4, and the conclusion is presented in section 5.

2. Literature

Below is an explanation of the devices used in this paper.

2.1 Layer-3 switch

A layer-3 switch is used as a core switch that is used as a network center that functions to connect various network segments so that APs, WLCs, and firewalls can be connected to each other. In this article, Cisco Catalyst C9300 is used.

Figure 1. Cisco Catalyst C9300

2.2 Wireless Controller

Wireless Controller (WLC) is a server that manages several APs to broadcast SSID where the client will connect to the network via a certain SSID. The SSID and Wifi network segment are determined in this WLC device. In this study the SSIDs that are emitted are the SSID Wifi-Student, Wifi-Teacher, and Wifi-Staff. The WLC used in this research is Cisco 2504.

Figure 2. Wireless Controller Cisco 2504

2.3 Wireless Access Point

Wireless Access Point (AP) is a device used to transmit SSID, namely Wifi-Student, Wifi-Teacher, and Wifi-Staff which is used by clients to connect to the network via Wifi

Figure 3. Wireless Access Point Cisco 2801

2.4 Firewall Fortinet

Firewalls in computer networks are needed to manage data traffic, contain policies for each network segment to access the internet. In this paper the firewall used is Fortinet 200F which has features for connecting with servers in the cloud.

Figure 4. Fortinet 200F

2.5 Remote Authentication Dial-in User Service

Remote Authentication Dial-in User Service (RADIUS) is a server whose function is to store user data and client passwords which are used to carry out authorization when a client accesses the network. The RADIUS function in this paper is handled by a service on the local Windows Server, namely the Network Policy System (NPS). On the cloud server, the RADIUS function is handled by the LDAP service.

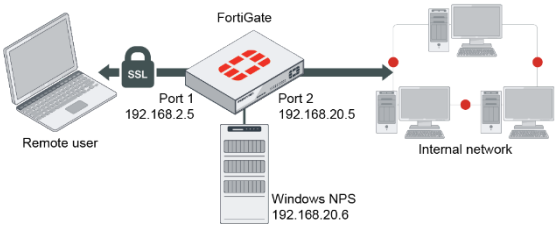

Figure 5. Network Policy System

P-ISSN: 2655-8807
E-ISSN: 2656-8888

2.6 Cloud services

Cloud services are divided into 3 main groups, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud service providers that provide these storage services include Google, AWS, and Microsoft Azure. In this article, Microsoft Azure is used, which provides Windows Server platform services. Azure Active Directory (AAD) and Lightweight Directory Access Protocol (LDAP) run on this Windows Server platform.

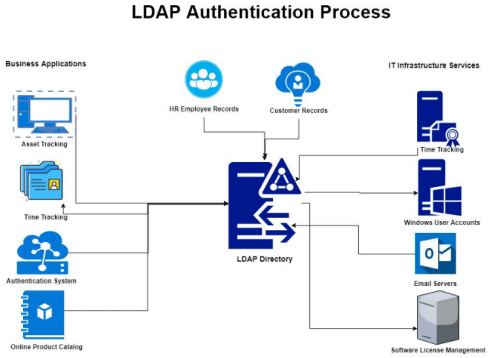

Figure 6. LDAP on cloud server platform

3. Research Methods

This research is a field experiment implemented in real activities at an educational institution. The equipment used is on premise equipment, a Cisco C9300 layer3 switch, a Cisco 2504 Wireless Controller with 50 AIR-AP2801 APs, a Fortinet 200F firewall, several local Windows Server 2016 servers, and LDAP services on Azure Active Directory in the cloud.

3.1 Evaluate the running configuration

Evaluate the running configuration where the on-premises RADIUS function is on Windows Server 2016 by running AD and NPS services on the server. WLC Cisco 2504 connected to a RADIUS server, namely a Windows Server that runs AD and NPS services [15] to perform user authentication. The user group client used by the NPS is obtained from the server based on the AD user group policy. When there is a client accessing the network using a wireless network (Wi-Fi), the username and password in the AD are required. NPS will read input from the Wi-Fi client to authenticate Wi-Fi network access. In the existing design, the firewall does not play a role in the authentication process.

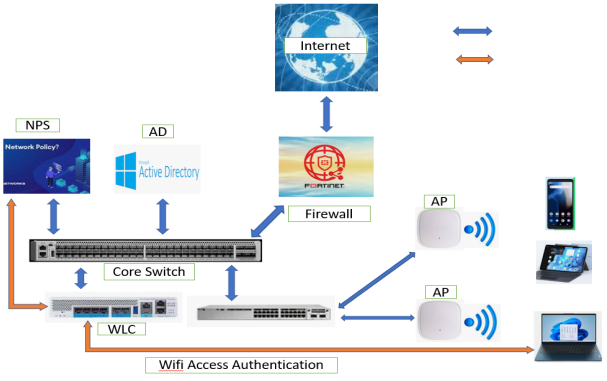

Figure 7. Existing system design

Figure 7. shows that WLC is related to NPS to authenticate Wi-Fi clients. The problem that arises in this design is that the client cannot change the password using a personal device (BYOD). Changing the password can only be done on a computer connected to the domain.

3.2 The Proposed System Design

From the case shown in Figure 7 above, it is proposed to solve the problem as follows; a). moving the authentication server, namely NPS on local to LDAP in the cloud, b). using a virtual port on Fortinet as a gateway off Wi-Fi clients, c). build a VLAN to connect virtual ports on Fortinet with virtual ports on WLC. By combining the WLC Cisco 2504 which works locally to handle Wi-Fi clients with the Fortinet 200F Firewall which has a server access feature to the cloud. In this framework, the authentication that was previously handled by the WLC Cisco 2504 was moved to the Fortinet 200F. Thus, Wi-Fi client authentication can be served by LDAP in the cloud.

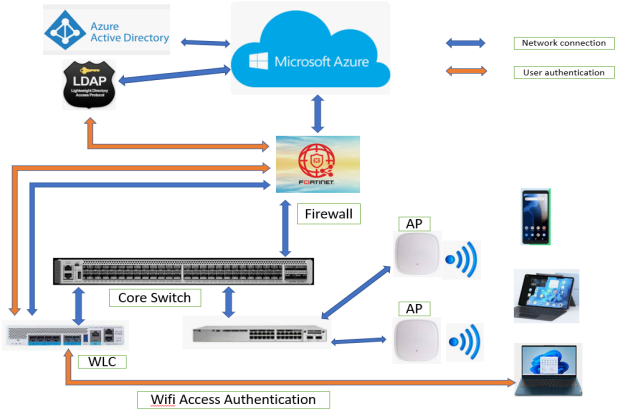

Figure 8. The proposed system design

In Figure 8 it is shown that WLC serves the Wi-Fi client in authenticating to LDAP via Fortinet.

4. Result and Discussion

From Figure 8, several steps are carried out in configuring so that the authentication process can work properly.

4.1 WLC configuration

In WLC, a trunk port is made to connect Fortinet which is used as a gateway for each SSID in WLC, the trunk is connected between WLC, core switch, and Fortinet. The virtual port on Fortinet functions as a gateway, through this virtual port authentication of Wi-Fi client to LDAP is carried out by Fortinet. The steps that must be taken in the SSID setup are to create an SSID as shown in Figure 9.

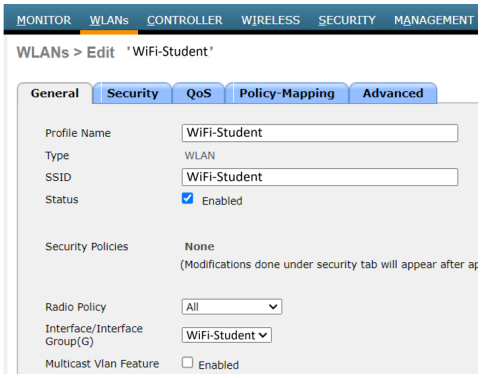

Figure 9. Create Wi-Fi SSID on WLC

P-ISSN: 2655-8807
E-ISSN: 2656-8888

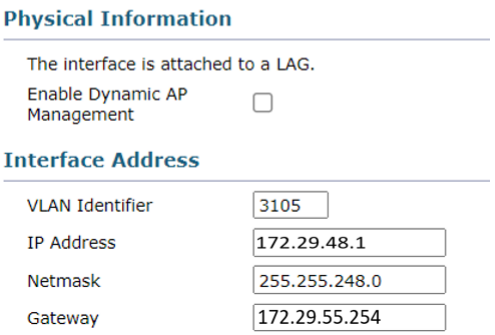

Figure 10. VLAN interface on WLC

Figure 10 shows the VLAN Identifier used in the trunk for authentication paths, IP Address 172.29.48.1 is the SSID interface for connecting Wi-Fi clients to WLC, and Gateway 172.29.55.254 is a virtual port on Fortinet as a gateway to the cloud.

Therefore, the recommendations to address these gaps are to implement live chat with sellers, enhance content personalization and recommendations, focus on responsiveness and page loading speed, prioritize security in online shopping, and improve content personalization and recommendations in engagement. By adopting these strategies, the e-commerce company can provide a more satisfying customer experience, increase engagement, and strengthen loyalty, thereby gaining a competitive advantage in the market and driving sustainable business growth.

4.2 Core switch configuration

On the Core Switch, a port is prepared to be connected to the WLC and a port to be connected to Fortinet. The port configuration is shown in Figure 11.

```
interface GigabitEthernet0/11
 description "Connect to WLC"
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 48 mode on
!
interface GigabitEthernet0/15
 description To Forti for WebAuth Wifi
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3102-3105
 switchport mode trunk
 channel-group 40 mode active
!
```

Figure 11. Layer-3 switch configuration

Figure 11 shows that the GigabitEthernet0/11 interface is assigned as a trunk for all VLANs between the WLC and the core switch, while the GigabitEthernet0/15 interface is used for VLANs 3102-3105 between the core switch and Fortinet.

4.3 Fortinet configuration

At Fortinet, a physical port is prepared to be configured with several virtual ports that are used as gateways for Wi-Fi clients. Thus, the virtual port on the Fortinet network is connected in one VLAN with the Wi-Fi client segment. Another thing that needs to be done is to configure Fortinet to be able to communicate with LDAP in the cloud.

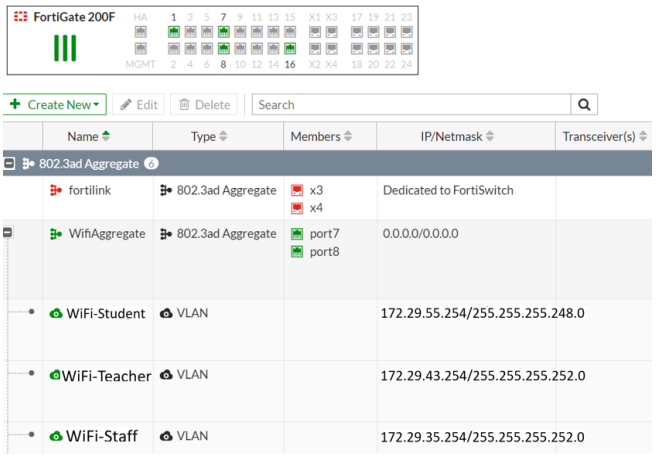

Figure 12. Configuring virtual interfaces on Fortinet

Figure 12. shows the virtual interfaces for Wifi-Student, Wifi-Teacher and Wifi-Staff, the IP address on each of these virtual interfaces is the gateway from the Wi-Fi client via WLC to be able to carry out the authentication process to LDAP in the cloud.

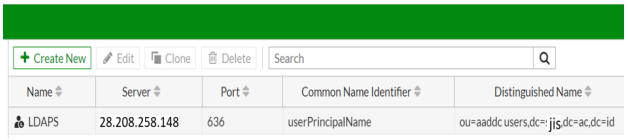

Figure 13. Connection configuration on Fortinet

Figure 13. shows the IP address of the server running the LDAP service in Figure 14, equipped with the organization unit (OU) of AAD.

4.4 Configuration on the cloud

Azure Active Directory is required to create a user group, there is a username and password in AAD. LDAP synchronizes usernames and passwords from AAD data to be used as authentication data, the results of which are sent to Fortinet. So, in this case the Wi-Fi client is connected to the WLC but authentication is done on Fortinet and LDAP.

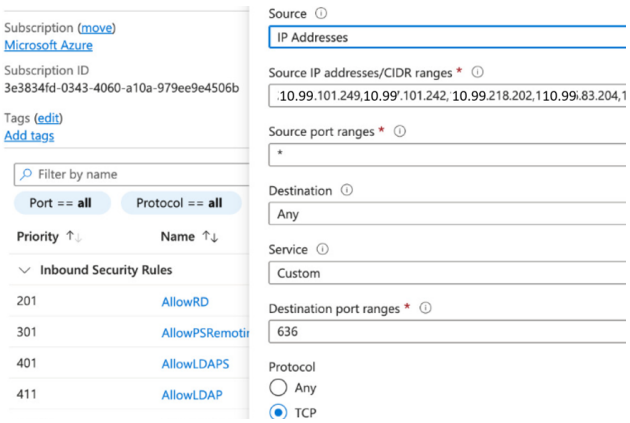

Figure 14. Configure connections on LDAP

Figure 14. shows the configuration of the source IP address from Fortinet referred to in Figure 13.The appearance of the user interface when the device is connected to Wi-Fi,

complete username followed by domain name and password is required for the authentication process.

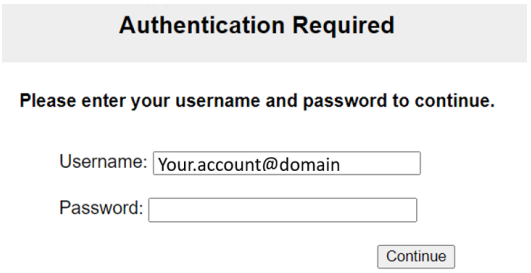

Figure 15. Wi-Fi user interface

This design has been implemented and the authentication system functions properly, the benefits obtained include, a). Wi-Fi clients can connect to a Wi-Fi network using the username and password registered in AAD and LDAP, b). Wi-Fi clients can change passwords using their own device (BYOD), 3). The same username and password can be used to authenticate other applications using the same LDAP configuration. The disadvantage of this WLC-Forti configuration is that user connection information cannot be monitored on WLC but can be monitored on Fortinet.

5. Conclusion

The results of design, experiments and implementation show that the WLC-Forti framework works well to handle Wi-Fi client authentication. Usernames and passwords registered in LDAP can be used to authenticate other applications, this is a solution for research conducted by Assumpta et al [14], which requires a password manager to handle multiple passwords on multiple applications.

The next research that can be done is to find a way for authentication to be carried out on the WLC node to LDAP in the cloud so that WiFi client monitoring can be carried out on the WLC.

References

[1] S. Pranata and H. T. Nugroho, “2FYSH : two-factor authentication you should have for password replacement,” vol. 17, no. 2, pp. 693–702, 2019, doi: 10.12928/TELKOMNIKA.v17i2.9187.

[2] S. W. Chin, K. G. Tay, C. C. Chew, A. Huong, and R. A. Rahim, “Dorsal hand vein authentication system using artificial neural network,” vol. 21, no. 3, pp. 1837–1846, 2021, doi: 10.11591/ijeecs.v21.i3.pp1837-1846.

[3] T. Mehraj, M. A. Sheheryar, S. A. Lone, and A. H. Mir, “A critical insight into the identity authentication systems on smartphones,” vol. 13, no. 3, pp. 982–989, 2019, doi: 10.11591/ijeecs.v13.i3.pp982-989.

[4] B. Hajimirzaei, “Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm,” ICT Express, vol. 5, no. 1, pp. 56–59, 2019, doi: 10.1016/j.icte.2018.01.014.

[5] J. Zhou and Q. Wang, “Lightweight Authentication Billing Enhancement Mechanism Based on the Fourier Fast Transform Algorithm,” vol. 2022, 2022.

[6] P. Wanda and H. J. Jie, “Efficient Data Security for Mobile Instant Messenger,” vol. 16, no. 3, pp. 1426–1434, 2018, doi: 10.12928/TELKOMNIKA.v16i3.4045.

[7] Z. Asmae, P. El, and O. Nabih, “Implementation of a bluetooth attack on controller area network,” vol. 21, no. 1, pp. 321–327, 2021, doi: 10.11591/ijeecs.v21.i1.pp321-327.

[8] C. Alezander, O. Villanueva, and A. Roman-gonzalez, “International Journal of

Advanced and Applied Sciences Implementation of a RADIUS server for access control through authentication in wireless networks," vol. 10, no. 3, pp. 183–188, 2023.
[9] S. J. Mohammed and S. A. Mehdi, "Web application authentication using ZKP and novel 6D chaotic system," vol. 20, no. 3, pp. 1522–1529, 2020, doi: 10.11591/ijeecs.v20.i3.pp1522-1529.
[10] D. Sudyana and N. Lizarti, "Forensic Investigation Framework on Server Side of Private Cloud Computing," vol. 10, no. 3, pp. 181–192, 2019.
[11] M. H. Mahdi and I. A. Ibrahim, "Enhancing the security of quality of service-oriented distributed routing protocol for hybrid wireless network," vol. 30, no. 1, pp. 121–128, 2023, doi: 10.11591/ijeecs.v30.i1.pp121-128.
[12] A. A. Talib and A. D. Salman, "Design and develop authentication in electronic payment systems based on IoT and biometric," vol. 20, no. 6, pp. 1297–1306, 2022, doi: 10.12928/TELKOMNIKA.v20i6.22157.
[13] I. M. Sukarsa, I. N. Piarsa, I. G. Bagus, and P. Putra, "Simple solution for low cost bandwidth management," vol. 19, no. 4, pp. 1419–1427, 2021, doi: 10.12928/TELKOMNIKA.v19i4.17109.
[14] A. Ezugwu, E. Ukwandu, C. Ugwu, M. Ezema, C. Olebara, and J. Ndunagu, "Password-Based Authentication and The Experiences of End Users," no. 2019.
[15] A. H. Aly, A. Ghalwash, M. M. Nasr, and A. A. A. El-hafez, "Formal security analysis of lightweight authenticated key agreement protocol for IoT in cloud computing," vol. 24, no. 1, pp. 621–636, 2021, doi: 10.11591/ijeecs.v24.i1.pp621-636