ZTA-based Federated Policy Control Paradigm for Enterprise Wireless Network Infrastructure

Boo Geum Jung, Yoon-Sik Yoo, Kiwon Kim, Byoung-Sik Kim, Hyungkyu Lee and HeaSook Park
Defense ICT Convergence Research Section, Electronics and Telecommunications Research Institute
{bgjung, ys5315, kiwon, bskim25, leehk, parkhs}@etri.re.kr

***Abstract*—The increasing use of wireless devices comes with advances in Wi-Fi technology. Devices with a Wi-Fi interface use the wireless network for convenient connection. Wireless networks face a variety of security threats, such as mac spoofing, rogue twins, DDoS attack and sniffing. We propose a Zero Trust Architecture (ZTA) paradigm to supplement enterprise wireless network control and to enhance security. ZTA can protect enterprise network resources by authorizing only authenticated users and devices to access enterprise services. ZTA in this paper is implemented within Wi-Fi Protected Access (WPA) enterprise network environment and is named wireless-ZTA. After analyzing the implementation performance, it conducts a DDoS attack to prove a stealth enterprise service invisible to malicious adversaries. To verify the effectiveness of the proposed Wireless-ZTA, additional analysis such as a network blacken test that cannot be accessed except for authorized services was performed. This analysis leads to conclusions, along with insights into the future of ZTA in enterprise wireless networks.**

***Index Terms*—Zero Trust Architecture(ZTA), WPA-Enterprise, Wi-Fi, VPN, 802.1x, JSON-RPC, OpenWRT, IKEv2 EAP.**

I. Introduction

Today's wireless networks are no longer slower than wired networks. Wi-Fi 6, also known as 802.11ax, is the sixth generation of Wi-Fi with enhanced features that can effectively respond to increases in traffic demand, capacity, coverage and network intelligence. Shipments (cumulative) of Wi-Fi 6 and Wi-Fi 6E compatible devices are expected to reach more than 13 billion units by 2026 [1]. However, because wireless networks are more vulnerable than wired networks, they have more inherent security challenges [2].

Enterprise wireless network infrastructure requires a framework to mitigate the security threats. One framework can do this is Zero Trust Architecture (ZTA) [3]. Another security model, Cloud Security Alliance (CSA) Software Defined Perimeter(SDP) [4] is a kind of the ZTA concept implementation. Because of the way the SPA (Single Packet Authorization)[1], the most important concept of SDP, works, the SDP is more suitable for system devices (desktops or servers) using fixed public IP.

NIST has defined ZTA to plan the enterprise's network infrastructure according to a zero trust model. US government agencies are also preparing to adopt a zero trust network architecture [6]. Therefore, to maintain a secure wireless network,

[1]SPA is a method of limiting access to server and network resources by cryptographically authenticating users before any type of TCP/IP stack access is allowed. https://help.ubuntu.com/community/SinglePacketAuthorization

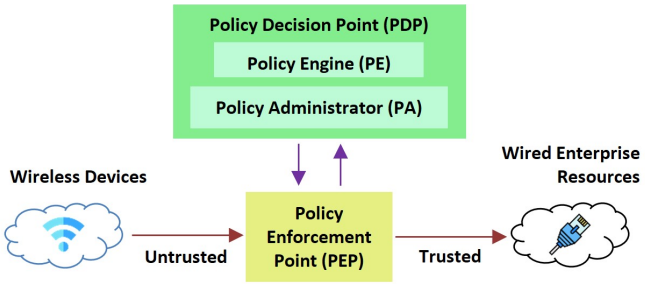

Fig. 1. Zero Trust Architecture(ZTA) on Wireless Network

we propose the Wireless-ZTA paradigm to block malicious traffic before attacking enterprise resources. The main contributions of our research are:

- Propose a wireless-ZTA architecture model based on unified policy deploy through network and security entity federation for secure enterprise wireless network infrastructure.
- Check the end-to-end security of the proposed paradigm.
- Verify the effectiveness of our model against DDoS attacks and unauthorized access by unauthenticated users.

After the introduction, we describe the basic concept of ZTA for wireless network infrastructure in Section II and federated policy control on wireless-ZTA combined architecture is presented in Section III. In Section IV, we discuss the verification results of the proposed model and we conclude our paper in Section V.

II. Wireless-ZTA

The main purpose of ZTA is to reduce the implied zone of trust within the enterprise network by protecting enterprise services from unauthorized users through authorization and authentication procedures.

In the conceptual model shown in Figure 1, wireless devices need access to enterprise resources. Policy Decision Points (PDPs) grant access through an enterprise's policies and PEP enforces policies. The system must ensure that the subject(end users, applications and other non-application, virtual components) is authentic and the request is valid. PDP/PEP, in good judgment, controls whether a subject can access a resource. This means that zero trust applies to two main areas: authentication and authorization. The Policy Decision Point (PDP) is

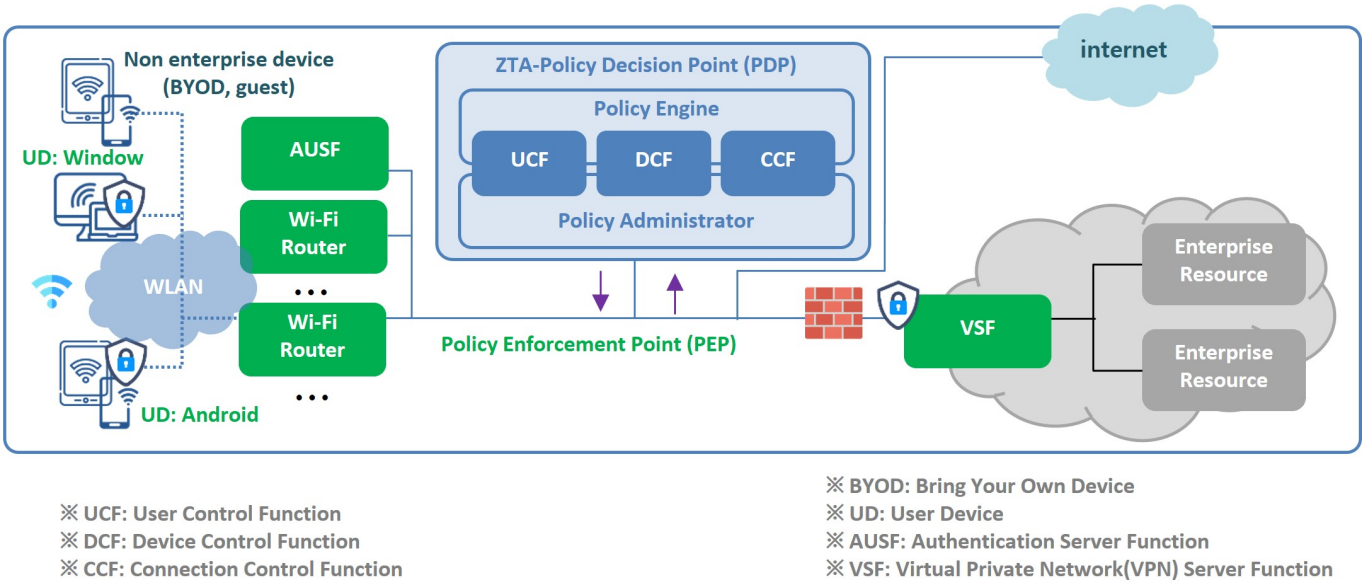

Fig. 2. Enterprise Network Protected with Wireless-ZTA

divided into two logical parts: the policy engine and the policy administrator.

A. Policy Engine (PE)

The policy engine is the core brain that makes decisions about granting legitimate users access to network services. The policy engine approves, denies, or revokes access to enterprise resources using the entered enterprise policy. PE works in pairs with the components of the PA. The PE also records a history of decisions (approval or denial) so that decisions in progress can be implemented.

B. Policy Administrator(PA)

The policy administrator works closely with the policy engine to generate credentials and certificates used to approve access to legitimate user devices. PA also serves to establish a connection between normal enterprise user devices and resources(ip:protocol:port). The PA is responsible for establishing and/or blocking communication paths between user devices and enterprise resources through commands to the PEP. PA also generates per-session authentication and grants the authentication token or credentials that clients use to access enterprise resources(ex: server ip:ssh, dbms server ip:port). The PA is closely tied to the PE and ultimately decides whether a session is allowed or not. If the request is authenticated, the PA instructs the PEP to start this session. If the session is rejected, the PA signals the PEP to close the connection. The PA communicates with the PEP when creating a communication path. This communication is done through the control plane.

C. Policy Enforcement Point(PEP)

The policy enforcement point's responsibility is to enable, monitor, and terminate connection paths between legitimate user devices and enterprise resources. The PEP communicates with the PA to forward requests or receive policy updates from the PA. Although PEP appears as a single logical component in ZTA, it can be divided into two components: the client and the resource side. Thus, it acts as a gatekeeper for the communication path. Beyond the PEP is the Trusted Zone with enterprise resources.

III. Unified Policy Control on Wireless-ZTA

In this paper, we propose a combined Wireless-ZTA architecture. Wireless access provides convenience but has some security disadvantages compared to wired access. ZTA authenticates before accessing services and provides an additional layer of security using policy-based controls, enabling us to secure enterprise resources from the wireless network.

The proposed architecture, porposed in Figure 2 consists of user control function(UCF), device control function(DCF), connection control function(CCF) engine and administrator as policy decision point (PDP) and authentication server function(AUSF), Wi-Fi router and VPN server function(VSF) as policy enforcement point (PEP). All these entities are federated and participate in unified control. The user device (UD) acts as a client and connects to the VPN server (VSF). The Wi-Fi router sends traffic to WAN, and the traffic arrives at VPN server. To access the resource which has been deployed in the enterprise, all UDs must be authenticated by the PDP at the enterprise first. Without policy deployed by PDP, no enterprise service access is approved at all.

The sequence diagram of each entity's operation under wireless-ZTA is shown in Figure 3. The PDP deploys predefined policies to the PEPs such as VSF, AUSF, Wi-Fi router and UDs. The predefined policy is for example UD1 can access service1 and not service2, UD2 can access service2 but not service1. Then UD1 and UD2 are authenticated by the authentication server and associate to the enterprise Wi-Fi

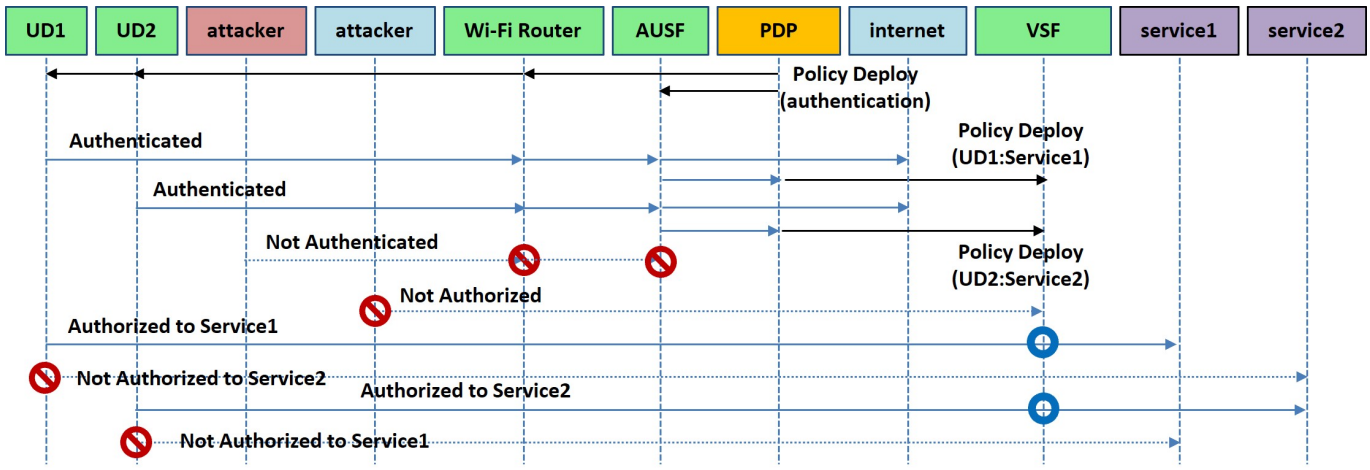

Fig. 3. Sequence Diagram of Each entity's Operation under Wireless-ZTA

routers, the attacker cannot associate with the enterprise Wi-Fi router. An external attacker cannot be authorized by the VSF. VSF authorizes service1, not service2 to UD1. The same goes for UD2.

A. User Control Function (UCF) and Authentication Server Function (AUSF)

The user control Function (UCF) manages the user IDs and passwords of enterprise members and deploys them to the authentication server. The authentication server function (AUSF) builds a user database using them. Enterprise users can log in to a wireless network using 802.1x authentication. UCF manages authentication server through AUSF and provides CRUD(create, read, update, delete) restful APIs for the enterprise network administrators. UCF also provides various APIs for the user account and connection information.

We use "freeradius" server [8]. We developed a backend server named AUSF that provides RESTful APIs (CRUD for radcheck(radius user database table name in freeradius), RD for radacct(user account database table name in freeradius) and additional combined query capabilities on the freeradius server. This backend server notifies the CCF front-end server whenever a user logs in or logs out, allowing CCF to take control of the VPN channel.

B. Device Control Function (DCF)

The device control Function (DCF) manages users' enterprise devices. One user may have one id but can have many devices. Any devices to access enterprise service should be registered to DCF's database. When the DCF receives the login notification from UCF, DCF can check whether the user device is legitimate or not. And DCF can check the status of the user devices using the RESTful API of UCF.

The device control function (DCF) also manages enterprise Wi-Fi routers. DCF controls Wi-Fi routers remotely to get and set the status and values. There are over 2,000 types of OpenWRT-supported hardwares [7]. OpenWRT has embedded RESTful APIs using JSON-RPC[2]. DCF can control OpenWRT routers with this RESTful API. We define various additional control functions such as assigning static IPs to UDs, mac filtering and checking the status of the system using this JSON-RPC API.

C. Connection Control Function (CCF) and VPN Server Function (VSF)

The connection control Function (CCF) manages UD's access to enterprise services. Wireless devices have private IP addresses behind NAT. Enterprise services are in public network areas. To access the public area from private IP securely, we use a virtual private network (VPN) server and control it through VSF. VPN provides end-to-end encryption for secure communications. There are many VPN methods. We chose IKEv2 EAP(Extensible Authentication Protocol), which is known as the best method for wireless devices and for common use on Windows and Android devices. Controlling the VPN server requires an additional agent software(back-end server) that provides RESTful APIs. We have developed back-end(VSF) and front-end(CCF) server function for user-server connection control using java on the spring framework.

VSF also has the server's PKI (Public Key Infrastructure) credential and we deploy it to enterprise staff using secure offline channels such as enterprise e-mail. We manage EAP[3] id and password for each user device based on the authentication id and password. The unified EAP id and password are managed in common with DCF (Device Control Function) and UCF (User Control Function).

User devices can access the enterprise service using the native client(windows) or app(Android) with an end-to-end secure path. Enterprise staffs using enterprise devices must know the id and password of device EAP for their devices (Type 1 authentication: something you know) and have the server's credential(Type 2 authentication: something you have).

[2]https://documenter.getpostman.com/view/14290/SzKPUgEo
[3]Extensible Authentication Protocol

IV. Verification Results

We built a testbed and developed core software for our paradigm's proof-of-concept (PoC). End-to-end security, stealth (not visible to unauthenticated users) service and black(unaware of existence) network capabilities are tested. We have developed a back-end server using JAVA and spring framework on top of the authentication server named AUSF (authentication server function) as one of the ZTA-PEP elements. Using this, a front-end server called User Control Function (UCF) was developed as one of the ZTA-PDP components. We use Linksys E8450 Wi-Fi 6 router and installed OpenWRT on it. Wi-Fi router has its own back-end server called Luci-RPC-mode. So, we wrote core JAVA functions to control the Wi-Fi router in DCF (Device Control Function), another component of ZTA-PDP. We also developed a backend server as VSF (VPN server function) on top of the IKEv2 EAP(strongswan) Ubuntu server. As a result of verifying the CCF (Connection Control Function) and VSF functions, it was confirmed that a notification is sent to the IKEv2 EAP server when the user device logs in and out, and the tunnel is automatically established and deleted.

A. Testbed

The testbed used in this paper is comprised of 7 physical machines (android phone as user device, Wi-Fi router, authentication server(AUSF), policy decision point server(PDP) and VPN server(VSF), 2 enterprise servers), 3 L2 switches and 1 L3 switch. Table I shows the descriptions of components of the testbed. Figure 4 displays the actual machines composed of wireless network and ZTA environment. Figure 5 shows the testbed configuration.

B. Test Results

Encryption-protected packet using ZTA is captured in Figure 6. The packets are all encrypted with ESP (Encapsulated Security Payload). Traffic was monitored as it flows between user devices and servers shown in Figure 7.

Without ZTA, a DDoS attack as shown in Figure 8 can severely degrade the quality of service because of numerous TCP errors, as shown in Figure 9. But with ZTA, there is no DDoS impact as there are no TCP errors as shown in Figure 10. This demonstrates the ZTA's stealth service ability to hide from foe's attacks.

An example predefined policy is that UD1 can access port 22 (ssh) of server1 (172.16.0.2) and cannot access server2 (172.16.0.3) shown in Figure 11 (using JuiceSSH on Android phone). And UD2 can access port 22 (ssh) of server2 but cannot access server1. So, we cannot run ssh from UD1 to server2 and from UD2 to server1. This confirms ZTA's black network ability to block any traffic from unauthenticated devices.

V. Conclusion

This paper describes the Wireless-ZTA architecture paradigm for securing enterprise wireless network infrastructure. Wireless-ZTA is a proposed framework for mitigating threats in wireless networks. After detailing the architecture and implementation, the test results were described. The proposed ZTA was capable of protecting enterprise resources. ZTA was able to prevent DDoS attacks. Unauthorized access was also performed in the ZTA framework to check for the darkening of the network. The attacker was unaware of the ports and services and even if they did, they would not be able to access them without deploying a proper policy. The purpose of ZTA is not to create a completely new concept or system, but to build a reliable system by integrating proven technologies and systems. This study and its findings provide a gradual adoption model

TABLE I
Description of the Testbed

Machine	Description
Android phone	Galaxy S22 Ultra, IKEv2 EAP client(App)
Wi-Fi Router	Linksys E8450, OpenWRT
AUSF server	Ubuntu20.04, freeradius3.0, Spring Framework
VSF server	Ubuntu20.04, IKEv2 EAP server, Spring Framework
PDP server	Ubuntu20.04, Spring Framework
3 L2 switches	Wireless/Wired/Private Network
L3 switch	Inter-working Wireless and Wired Network

Fig. 4. Testbed Setup

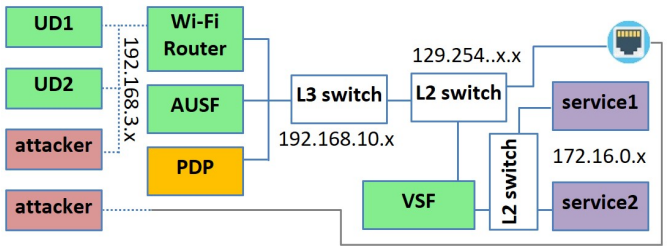

Fig. 5. Testbed Configuration

```
IP 129.254.[redacted].47124 > ZTA-VSF.ipsec-nat-t: UDP-encap: ESP
IP 129.254.[redacted].47124 > ZTA-VSF.ipsec-nat-t: UDP-encap: ESP
IP 129.254.[redacted].47124 > ZTA-VSF.ipsec-nat-t: UDP-encap: ESP
IP ZTA-VSF.ipsec-nat-t > 129.254.[redacted].47124: UDP-encap: ESP
IP ZTA-VSF.ipsec-nat-t > 129.254.[redacted].47124: UDP-encap: ESP
IP ZTA-VSF.ipsec-nat-t > 129.254.[redacted].47124: UDP-encap: ESP
IP 129.254.[redacted].47124 > ZTA-VSF.ipsec-nat-t: UDP-encap: ESP
```

Fig. 6. End-to-End security(Encap by ESP) with ZTA

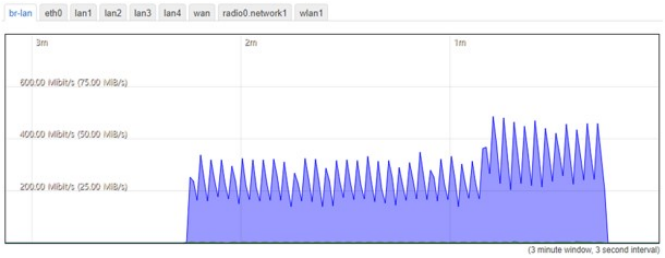

Fig. 7. Real-Time Traffic of WLAN Graph on OpenWRT

```
root@ZTA-VSF:~# hping3 -S 172.16.0.2 -p 5001 --flood -I enp5s0
HPING 172.16.0.2 (enp5s0 172.16.0.2): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Fig. 8. DDoS Attack Execution using syn flooding on Ubuntu OS

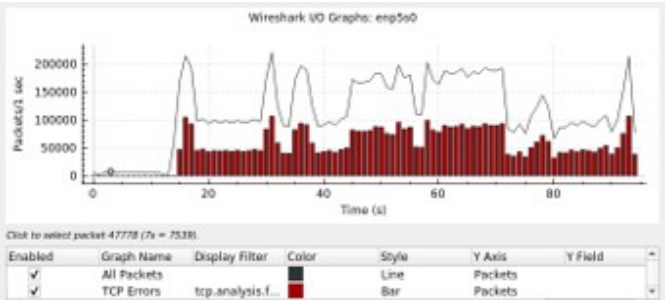

Fig. 9. Many TCP errors Occurred due to DDoS attack without ZTA

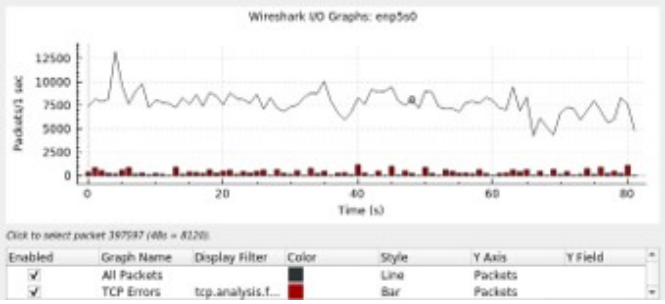

Fig. 10. No TCP errors Appeared due to DDoS attack with ZTA

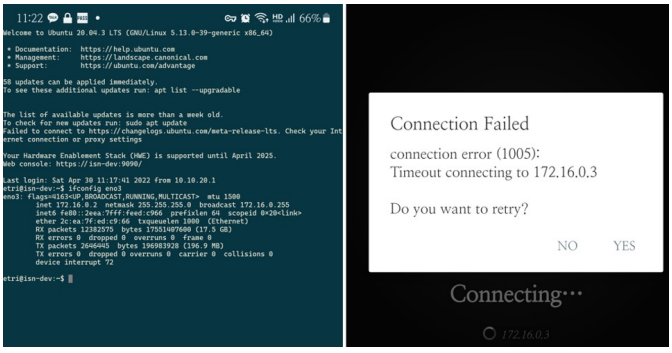

Fig. 11. Traffic accepted & connected to server from authorized device(left), traffic blocked & can't be connected to server from unauthorized device(right)

for enterprises looking to transition their existing wireless infrastructure to ZTA. By adding some back-end servers to existing network and security entities and adding a ZTA-PDP function as a controller, Wireless-ZTA can be applied without replacing the entire system.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (2021-0-00040, Development of intelligent stealth technology for information and communication resources for public affairs and missions)

REFERENCES

[1] LogisticsIQ, "Wi-Fi 6 and 6E - Forecast to 2026: An Analysis of Market Trends, Key Players and Revenue Forecasts," Mar. 2021.
[2] Mir, R.N. (2021) WiNajar, Z.A. and Fi: WPA2 Security Vulnerability and Solutions. Wireless E ngineering and Technology, 1 2, 15-22. https://doi.org/10.4236/wet.2021.122002
[3] SP 800-207, "Zero trust architecture," August. 2020. The official publication is available at: https://doi.org/10.6028/NIST.SP.800-207.
[4] Cloud Security Alliance (CSA), SDP Architecture Guide version 2.0, May 2019. [Online]. Available: https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/
[5] Sukhraj Singh Brar, Additional Security Mechanism in Single Packet Authorization, Department of Information Systems Security & Assurance Concordia University of Edmonton, Edmonton, Alberta, Canada, April 2021.
[6] EXECUTIVE OFFICE OF THE PRESIDENT, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles ," January 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[7] OpenWRT, "Table of Hardware: Firmware downloads," [Online]. https://openwrt.org/toh/views/toh_fwdownload
[8] FreeRAIUDS, [Online]. https://freeradius.org/