

UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORKS AND COMMUNICATIONS



NETWORKS SECURITY
PROJECT FINAL REPORT

GROUP 16:

ZERO TRUST NETWORK ACCESS

Lecturer: PhD. Nguyễn Ngọc Tự

Students: Nguyễn Đại Nghĩa - 21521182

Phạm Hoàng Phúc - 21521295

Hoàng Gia Bảo - 21521848

Table of contents

I. INTRODUCTION	3
II. SCENARIO	3
III. SOLUTION	4
IV. SECURITY GOALS	9
V. REFERENCES	9

I. Introduction

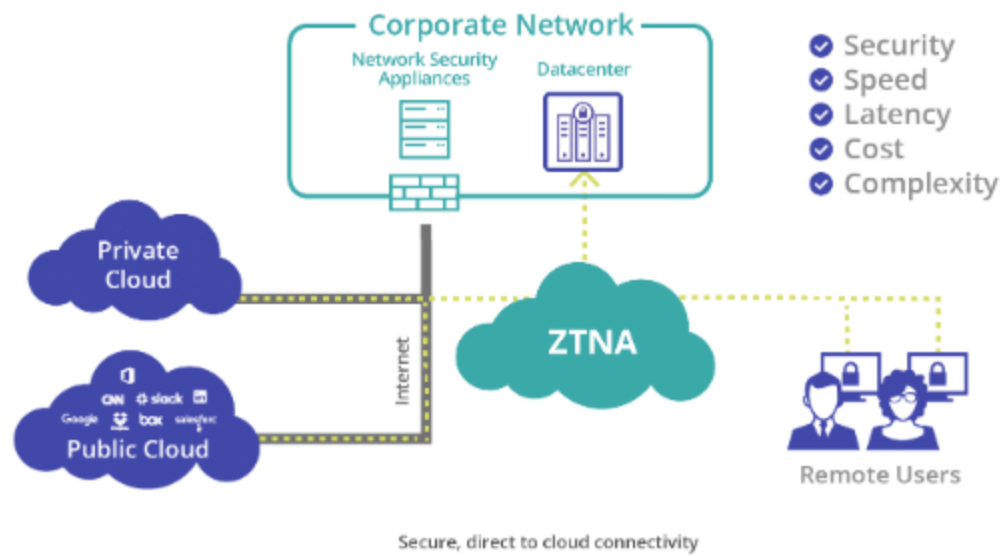
NIST defines both Zero Trust and a Zero Trust Architecture as: "Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero Trust Architecture (ZTA) is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan." Zero Trust Network Access (ZTNA) is a cybersecurity solution that embodies the principle of "never trust, always verify." It's part of the broader Zero Trust security model, which assumes that threats can exist both outside and inside the network. ZTNA specifically focuses on controlling access to network resources based on strict identity verification and context-aware policies.

II. Scenario

Most organizations already have some elements of zero trust in their enterprise infrastructure or are on their way through implementation of information security and resiliency policies and best practices. Here is one example deployment scenarios that lend themselves readily to a zero trust architecture:

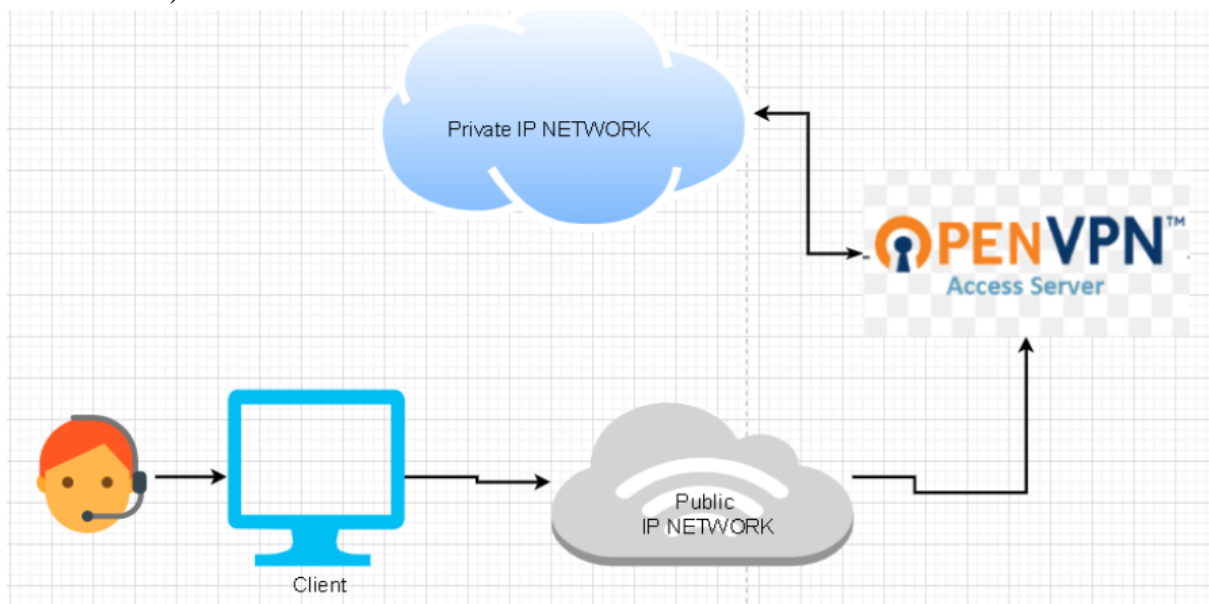
An enterprise with a single headquarters and one or more geographically dispersed locations that are not joined by an enterprise-owned physical network connection. Employees at the remote location may not have a full enterprise owned local network but still need to access enterprise resources to perform their tasks. In this case, Enterprises may wish to grant access to some resources but deny access or restrict actions to more sensitive resources (e.g., HR database).

ZTNA flow for Remote Users



III. Solution

a) Architect



After all of that, it not enough to deploy “zero trust “

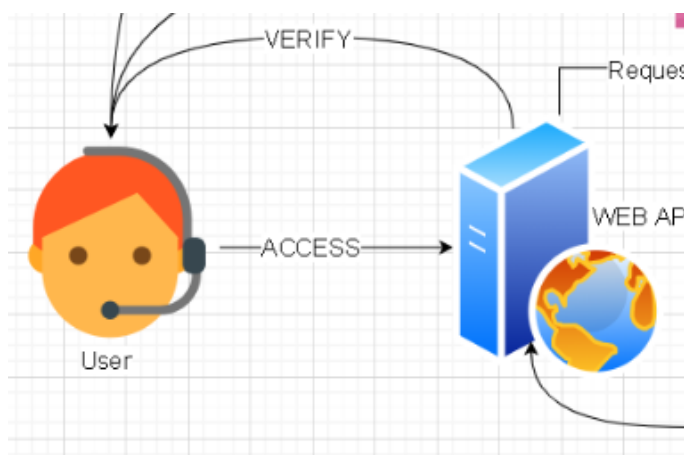
After the aforementioned steps, we perform additional verification to ensure the security of both users and resources. We utilize session tokens with expiration periods; these tokens are continuously encrypted and change every time a user clicks. If a user clicks on the login token, it is altered to prevent session hijacking from third parties or middleware. Additionally, we use tokens to record user actions on the website. **BUT** we also keep a record of each user's activities and interactions with the system on our web platform

PHOTO UPLOAD SETTINGS LOG HISTORY Đăng Xuất		
Thời gian	Hành động	Người thực hiện
1/3/2024 12:49:51 PM	Tài khoản "ngianguyen3092009@gmail.com" đăng nhập	
1/3/2024 12:51:45 PM	Tài khoản "ngianguyen3092009@gmail.com" đăng nhập	
1/3/2024 1:05:22 PM	Tài khoản "ngianguyen3092009@gmail.com" đăng nhập	
1/3/2024 1:07:47 PM	Tài khoản "hoangphuc@gmail.com" đăng nhập	
1/3/2024 1:08:10 PM	Tài khoản "ngianguyen3092009@gmail.com" đăng nhập	

However, there are still some aspects that have not been fully completed in the demo below.

We have only draw architecture :

- For session tokens :



When a user accesses the system, if the server verifies that the account exists on Firebase, it will create a login session and record it in the system to allow user access. The content of the session before encryption will include the user's name and permissions.

This session will have a 5-minute expiration and will automatically be deleted if exceeded. The time will follow the real-time network to prevent attacks by adjusting the local clock.

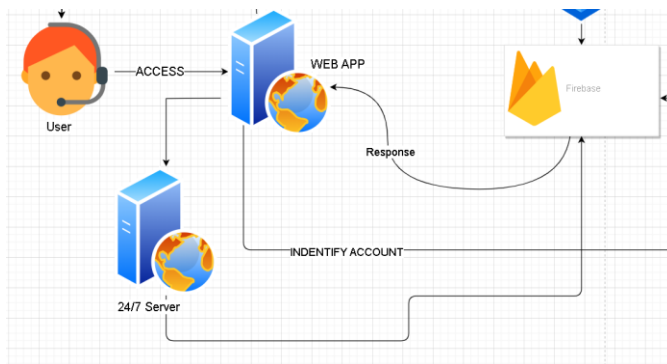
During this 5-minute period, each time the user continuously double-clicks the mouse, the login session will be altered, ensuring safety for the user.

Simultaneously, we will use RSA256 encryption for this session. The private key will be generated using the timestamp when the user logs in, and the public key will be the username plus their permissions.

However, there is no need to encrypt the data on the local storage. All necessary security operations can be performed on our backend. On local storage or session storage, we only store a randomly generated numeric value, which serves as a verification link between the user and the database. This value must be securely written to Firebase.

Certainly! When users log out before the expiration time, the login session will also be deleted



In this case I propose use second server support for that



At times, we may face security threats from third parties. In the event that the web app used by users fails to adequately secure our resources, having a dedicated 24/7 server solely responsible for managing tokens and sessions can significantly enhance the

effectiveness of securing both our resources and user accounts

Scenario :

PHOTO UPLOAD SETTINGS LOG HISTORY Đăng Xuất	
Ảnh	Nội dung
	Sơn Tùng MTP
	

Storage	Key	Value
Local storage		
Session storage		
IndexedDB		
Web SQL		



Storage	Key	Value
Local storage		
Session storage		
IndexedDB		
Web SQL		

VIDEO DEMO : [DEMO ZTNA](#)




In this case we use :

- Service of azure to host Web, and a public VPN

The screenshot displays the Azure portal interface for a Web app named 'NetworkSecurity'. The left sidebar shows the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Microsoft Defender for Cloud, Events (preview), Deployment, Deployment slots, Deployment Center, Settings, Configuration, Authentication, Application Insights, Identity, Backups, Custom domains, Certificates, Networking, Scale up (App Service plan), Scale out (App Service plan), Service Connector, and Locks. The main content area is divided into several sections:

- Essentials:** Shows the resource group 'FinalProject_NetworkSecurity', status 'Running', location 'Southeast Asia', subscription 'Azure for Students', and subscription ID '67155ecc-4d9a-4868-b0b7-f153dc8e88a2'.
- Properties:** Displays the web app name 'NetworkSecurity', publishing model 'Container', and container image 'nghianguyen/antoanmang'.
- Domains:** Shows the default domain 'networksecurity.azurewebsites.net' and an option to add a custom domain.
- Hosting:** Displays the plan type 'App Service plan', name 'ASP-FinalProjectNetworkSecurity-a038', operating system 'Linux', instance count '1', and SKU and size 'Basic (B1) Scale up'.
- Deployment Center:** Provides links for deployment logs and view logs.
- Application Insights:** Offers an option to enable application insights.
- Networking:** Shows the virtual IP address '52.187.36.104', outbound IP addresses, and virtual network integration status 'Not configured'.

- Database : Firebase (firebase support any service about protect our account like two step factor authentication,store resources)

Identifier	Providers	Created ↓	Signed In	User UID
nghianguyen3092003@...		Jan 3, 2024	Jan 3, 2024	DaH9V9RHfeSffntZJCYvabXrt...
hp249@gmail.com		Jan 3, 2024	Jan 3, 2024	W4Z5M75kwmP77es3BwTx7...
hoangphuc249@gmail....		Jan 3, 2024	Jan 3, 2024	6YE3W24f8XN8PAmAyuigZYP...
baohoanggia9@gmail.c...		Jan 2, 2024	Jan 8, 2024	x8kh5pXb8pM03PkuBufNzFu...

IV. SECURITY GOALS

- User Authentication
- Role-Based Access Control
- Reauthentication Before Certain Actions
- Secure Remote Access
- Zero Trust

V. References

NIST Special Publication 800-207 Zero Trust Architecture