Cross-Regional Remote Access Network Solution

Biqi Liu | Siying Chen | Tim Rundström | Yiyi Miao

1. Analysis

This project designs a secure, scalable network connecting ACME's Stockholm headquarters with its London branch. It ensures safe access to company resources, supports remote work, and reduces security risks.We propose a VPN with SSL/TLS encryption and Multi-Factor Authentication (MFA) for secure remote access. PKI provides flexible user credentials, while firewalls and IDS protect against threats. Wireless networks will use WPA3 and 802.1X authentication. File sharing will be secured via Nextcloud.Combining VPN, firewall, IDS, PKI, secure wireless, and RBAC, this solution meets ACME's operational needs.

2. System Design

2.1 Employee Authentication

To ensure secure and reliable authentication, a robust identity verification system will be implemented using digital certificates. Each employee will be assigned a unique digital identity through OpenSSL and PKI, authenticated via an authentication server using RADIUS. The PKI system will support two types of credentials:

(1) Traditional Credentials – Long-term digital certificates used for persistent identity verification across company systems.

(2) Pseudonymous Credentials – Short-lived, anonymized certificates designed for enhanced privacy in scenarios such as employee travel.

When employees use corporate devices, local certificates will be used for authentication, and employees will only need to enter their passwords.

When employees use personal devices, multi-factor authentication (MFA) will be required. Each user will authenticate using their PKI digital certificate and an additional TOTP (Time-based One-Time Password), as employees are provided with corporate phones. OCSP (Online Certificate Status Protocol) will be enabled on the CA server to allow real-time certificate revocation in case of compromise, ensuring that invalid credentials are immediately rejected.

2.2 Secure Connectivity

To ensure secure network access, only authorized traffic from ACME's Stockholm and London offices will be permitted. All other incoming traffic will be dropped by the firewall, configured with iptables.

For remote access, only non-sensitive operations will be allowed, while highly sensitive internal servers will remain inaccessible. Employees must connect via OpenVPN using PKI credentials and MFA. Pseudonymous certificates will be issued when employees require privacy, ensuring their identities remain protected when accessing company resources during travel or remote work.For visiting employees in London, full access to the Stockholm internal network will be granted through a VPN tunnel, provided the connection originates from the London office network.

2.3 Confidentiality and Anonymity

To protect corporate data, all communications between Stockholm and London will be encrypted using VPN tunnels secured with TLS encryption. The VPN gateway will encrypt all traffic, authenticate devices using PKI-based authentication.

Confidentiality will be maintained by differentiating access between critical and non-critical systems. The main web server, containing sensitive corporate data, will only be accessible via VPN authentication and PKI certificates, and restricted to trusted internal users within the corporate

network. A secondary web server, hosting less critical resources, will allow remote access from personal devices.
Upon connecting to the VPN server, a secure encrypted tunnel will be established between the employee's device and the corporate network. The VPN server, using a DHCP server, will assign an internal IP address to authenticated users, granting access based on role-based permissions. FreeRADIUS, integrated with LDAP, will manage authorization policies, ensuring employees can securely work as if they were inside the corporate network.
To prevent remote employees' activities from being traced by curious observers, short-term anonymous certificates are used to ensure privacy and anonymity.

2.4 Secure Wireless Access

Employees connecting to Wi-Fi at the London branch will have their authentication requests forwarded to Stockholm, where the central FreeRADIUS server is located. The authentication process begins when a device initiates a connection request, which is forwarded by the access point. The RADIUS server in Stockholm, utilizing EAP-TLS authentication and SSL certificates, will handle the secure authentication of devices.
If WPA2-PSK/WPA3-SAE Mixed mode authentication is used, the AP (Access Point) will initiate the connection process and ensure that all wireless connections are encrypted, protecting them against brute-force attacks. The AP forwards the authentication request to the RADIUS server, where the server verifies the device's credentials using the certificates. Once verified, the RADIUS server returns an Access-Accept or Access-Reject response. Only successfully authenticated devices will be granted access to the internal network. This same authentication process is applied locally at Stockholm headquarters, where the RADIUS server processes requests directly.

2.5 Secure File Exchange

A Nextcloud server will be deployed internally at ACME to ensure secure, controlled file sharing while maintaining confidentiality. All file transfers will be encrypted using TLS, preventing data interception.To maintain file integrity, Nextcloud will automatically calculate hash values and log all file activities, including uploads, downloads, and modifications, in the File Access Log. This ensures that files remain untampered and unauthorized modifications can be traced.
For authentication, LDAP integration with the RADIUS server will restrict access to verified ACME employees only, preventing unauthorized users from accessing corporate files. Additionally, IP access control on the firewall will limit access to company VPN IPs, ensuring that only employees connected through the corporate VPN can reach the Nextcloud server.
To further enhance file-sharing security, controlled file-sharing policies and a sharing approval mechanism will be implemented, ensuring that only ACME employees can exchange files, while external access is entirely blocked. End-to-end encryption (E2EE) will be enabled for sensitive files, ensuring that even server administrators cannot access protected documents.

2.6 Other Security Measures

To enhance intrusion detection and response, Snort will be deployed as an IDS beside the firewall to monitor and log suspicious traffic in real time. Upon detecting an attack, automated alerts will be generated for immediate administrative action.
To mitigate DoS attacks, firewall-level DoS protection will be enabled in OpenWRT, with SYN flood protection configured to limit excessive connection requests. Traffic rate limiting will also be enforced on both the VPN gateway and firewall to prevent attackers from overwhelming network resources.
DNS security will be enforced by directing all devices to use OpenWRT for DNS resolution, with firewall rules ensuring compliance. DNSSEC validation will be enabled to protect against DNS hijacking and cache poisoning, ensuring the authenticity of DNS records.
To address potential stolen devices or credential leaks, MFA will be enforced for all employees, preventing unauthorized access even if credentials are compromised.

3. Topology

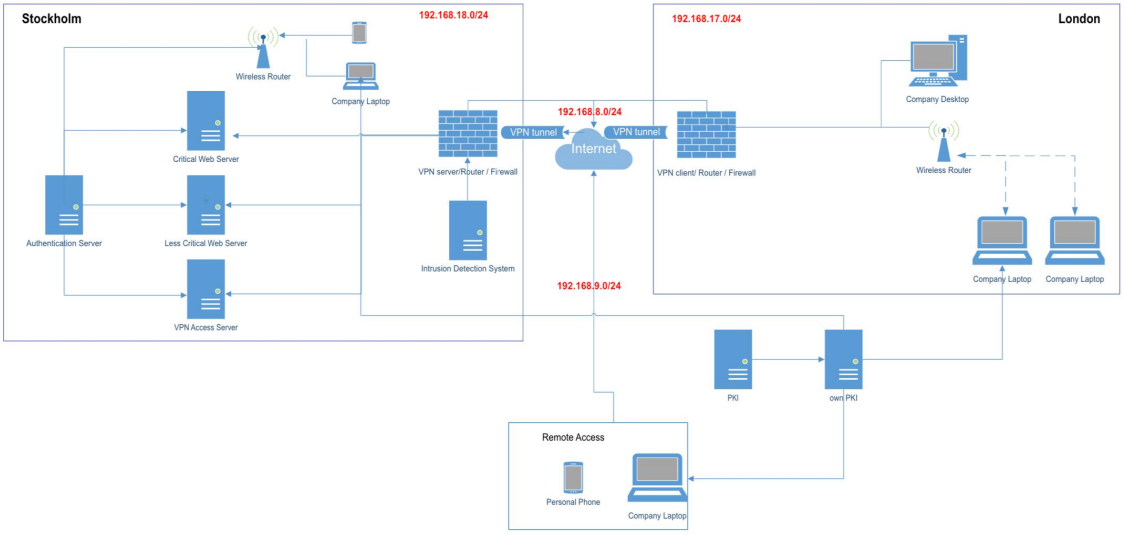

Figure 1: Topology of System

4. Implementation

4.1 General Design Router and Firewall

We have four subnets:

Stockholm	192.168.18.0/24	**site-to-site VPN tunnel**	192.168.8.0/24
London	192.168.17.0/24	**remote access VPN tunnel**	192.168.9.0/24

The VPN tunnel encrypts communication between Stockholm and London, making both networks act as one. Remote employees connect via a VPN server in Stockholm, which forwards their traffic securely to the internal network after authentication.

4.2 Router and Firewall

We have flashed both routers with OpenWrt, as it offers enhanced network functionality and greater customization options. Our implementation on OpenWrt includes static IP addressing, DNS server, firewall rules and VPN tunnel setup.

For the firewall configuration, we follow a default-deny approach, meaning all traffic is blocked by default, and we explicitly add rules to allow necessary connections. Since we have set up a VPN tunnel using OpenVPN, which operates on port 1194, we add a rule to allow the router to listen on this port, enabling VPN tunnel establishment.

Additionally, to restrict remote employees from directly accessing the main web server, we enforce a policy where their traffic is redirected through a proxy server. To achieve this, we add a reject rule that blocks any traffic originating from the VPN access server when the destination is the critical web server.

4.3 OpenVPN

4.3.1 OpenVPN Site-to-Site Tunnel

In this VPN deployment, we set up an OpenVPN Tun Route between two OpenWRT routers. This ensures that the London office can securely access resources at the Stockholm headquarters.

First, we install OpenVPN on the Stockholm server and use Easy-RSA to create the CA certificate, server certificate, client certificates, and Diffie-Hellman parameters. Then we configure the OpenVPN server to listen on UDP port 1194, using AES-256-GCM encryption. We also enable IP forwarding and set firewall NAT rules for VPN network communication.
On the client side, we install and configure OpenVPN, import certificates, and connect to the server to establish the VPN tunnel. Additionally, we set up site-to-site routing to allow efficient communication between different subnets.
Finally, this VPN deployment provides secure remote access with low overhead, supports multiple user authentication, and ensures end-to-end encryption. It helps keep the company's internal network safe and stable.

4.3.2 OpenVPN Access Server

To enable remote users to access the internal network, an OpenVPN access server was set up. Running on an ubuntu 24.04, the remote access server was installed using the command provided by the Access Server Portal as root.
The access server was then set up using the web interface, available on <local IP>:943/admin. Configuration included setting the public hostname of the access server to the public IP address of the router, which was later changed to the public hostname to accommodate whenever the public IP changes. The UDP port number was changed to 51820 (wireguard default UDP port number, one of the allowed ports), so as not to conflict with the site-to-site tunnel. The VPN IP network was also set to 192.168.9.0/24. Finally, on the router, the port 51820 was set up to be forwarded to the static local IP address of the VM running the Access Server.
Users, and user profiles, can be created using the access server web interface. They are set up to require MFA (Google Authenticator) and the profiles are installed on company devices by the IT department.

4.4 DNS, DDNS, and DNSSEC

4.4.1 DNS

Using OpenWRT LuCi, the included lightweight DHCP server and DNS forwarder Dnsmasq was used to bind the MAC address(es) of the services (virtual machines) to static local IP addresses, and then those static addresses were bound to hostnames.

4.4.2 DDNS

To circumvent having to set up the VPN tunnels and redistribute user profiles each time the public IP address changes, we set up a DDNS on the Stockholm router. Using the OpenWrt LuCi interface, the ddns-scripts and luci-app-ddns add-ons were installed. A domain was registered using DuckDNS and the service was set up on the router using the LuCi add-on and DuckDNS credentials.

4.4.3 DNSSEC

In order to protect the network and ensure authentic results from DNS queries, DNSSEC was set up on the OpenWrt router. The lightweight version of dnsmasq included in OpenWrt was upgraded to the full version of dnsmasq and DNSSEC was enabled in the configuration file.

4.5 IDS – Snort

We have Snort deployed on virtual machines in both Stockholm and London, where it monitors network traffic through its own interface. After configuring local Snort rules and specifying an output log file, we can start running Snort.
To monitor traffic on the LAN port of our local router, we take an additional step—port mirroring. This process copies traffic from the router’s LAN port to the local Snort server for analysis. To achieve this, we install iptables on the router and use the MANGLE table to configure port mirroring.

For Snort rules, we focus on detecting key security threats such as DDoS attacks, implementing rules to identify ICMP floods and SYN floods. Additionally, to monitor network administrator activities, we add rules to log SSH login attempts on the router.

4.6 FreeIPA and FreeRadius

We implemented FreeIPA in Centos 7 with IP address 192.168.18.11 as an identity management system and integrated it with FreeRADIUS for authentication services. In FreeIPA, users are authenticated using both passwords and OTP for an extra layer of security. We can easily add and manage users on the GUI. After we connect the services with FreeIPA via LDAP (like Nextcloud), we can directly use FreeIPA users in the database instead of creating new ones for the service.
In order to configure the RADIUS server to authenticate with the software token provided by the IPA server, we must let RADIUS accept requests from the clients (including the IPA server itself), enable the default configuration to search for users in the IPA server with LDAP protocol and try to authenticate them with an LDAP bind() operation.

4.7 Nextcloud

We deployed nextcloud: latest image in Ubuntu 24.04 with domain name: http://nextcloud.acme.com/ and IP address: 192.168.18.17/24. It connects to the FreeIPA's database and only allows users with permission to share files with it. With built-in functions, users can easily upload and share files. In addition, there is an admin user, where the 2FA (Google Authenticator) for admin user is enabled.

4.8 Web Servers

Both the critical web server, and the less critical web server are hosted using Apache2 on separate virtual machines. The web pages are for demonstrational purposes and do not contain any sensitive data or capabilities. The index pages were edited and stored in /var/www/html on the servers hosting them.
To restrict access to the critical web server from remote access, a firewall rule was set up to drop any requests originating from the remote access VPN to the critical web server. This way, any requests from a remotely connected device to the critical web server will be dropped.

5. Technical Appendix

5.1 OpenVPN

5.1.1 Stockholm's configuration

```
config openvpn 'VPN_Tun_Server'
        option cipher 'AES-256-GCM'
        option client_config_dir '/etc/openvpn/ccd'
        option client_to_client '1'
        option comp_lzo 'no'
        option dev 'tun0'
        option ifconfig_pool_persist '/etc/openvpn/ipp.txt'
        option keepalive '10 60'
        option mssfix '1420'
        option mode 'server'
        option persist_key '1'
        option persist_tun '1'
        option port '1194'
        option proto 'udp'
        option remote_cert_tls 'client'
        option reneg_sec '0'
        option route '192.168.17.0 255.255.255.0'
        option server '192.168.8.0 255.255.255.0'
        option topology 'subnet'
        option verb '3'
```

5.1.2 London's configuration

```
config openvpn 'VPN_Tun_Client'
        list remote 'bnssg18.duckdns.org'
        option auth_nocache '1'
        option cipher 'AES-256-GCM'
        option client '1'
        option comp_lzo 'no'
        option connect_retry '5 60'
        option dev 'tun0'
        option nobind '1'
        option persist_key '1'
        option persist_tun '1'
        option port '1194'
        option proto 'udp'
        option remote_cert_tls 'server'
        option reneg_sec '0'
        option verb '3'
        option ca '/etc/openvpn/ca.crt'
        option cert '/etc/openvpn/Client_London_Stockholm.crt'
        option key '/etc/openvpn/Client_London_Stockholm.key'
        option enabled '1'
```

5.2 DNSSEC

Swap dnsmasq for dnsmasq-full (-full includes DNSSEC support) and remove odhcpd-ipv6only:
`opkg install dnsmasq-full --download-only && opkg remove dnsmasq odhcpd-ipv6only && opkg install dnsmasq-full --cache . && rm *.ipk`
In the config dnsmasq section, add these settings:

```
option dnssec '1'
option dnsseccheckunsigned '1'
```

5.3 Snort

$HOME_NET is the subnet we want to analyze.And we can specify which IP range the $EXTERNAL_NET shall correspond to, the default is the inverse of the $HOME_NET, meaning all adresses except the $HOME_NET.

```
ipvar HOME_NET 192.168.18.0/24
ipvar EXTERNAL_NET any
```

Example of alert rules :

```
alert icmp any any -> $HOME_NET any (msg:”ICMP Detected”; sid: 1000001; rev: 1)
alert tcp any any -> $HOME_NET 80 (msg:"Possible SYN Flood DoS Attack"; flags:S,12; threshold:
type both, track by_src, count 100, seconds 10; sid:1000002; rev:1;)
alert icmp any any -> $HOME_NET any (msg:"Possible Ping of Death DoS Attack"; icmp_type:8;
dsize:>1400; sid:1000003; rev:1;)
```

As default, Snort writes alerts to the console. To write to log file, execute:

```
sudo snort -q -l /var/log/snort -i enp0s1 -A console -c /etc/snort/snort.conf
```

5.4 Nextcloud

Step1: Install Required Packages; Step2. Configure MySQL Server: Login to MySQL Prompt, Just type: mysql; Create MySQL Database and User for Nextcloud and Provide Permissions; Step3. Download, Extract, and Apply Permissions; Step4. Install NextCloud From the Command Line. Configure Apache to load Nextcloud from the /var/www/nextcloud folder.

```
vi /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/nextcloud
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
:x
```

Configuration in /var/www/nextcloud/config/config.php is as:

```
<?php
$CONFIG = array (
  'passwordsalt' => '1sNBk6BnBbllOKc7ln7pkaOCI8af9R',
  'secret' => 'qbmeY4vqIXIvcuD46nx0XyWFBESwxPJTzbyAG9xFC91f/r7H',
  'trusted_domains' =>
  array (
    0 => 'localhost',
    1 => '192.168.18.17',
    2 => 'nextcloud.acme.com',
  ),
  'datadirectory' => '/var/www/nextcloud/data',
  'dbtype' => 'mysql',
  'version' => '31.0.0.18',
  'overwrite.cli.url' => 'http://localhost',
  'dbname' => 'nextcloud',
  'dbhost' => 'localhost',
  'dbport' => '',
  'dbtableprefix' => 'oc_',
  'instanceid' => 'ocwd8st6dd39',
  'mysql.utf8mb4' => true,
```

```
  'dbuser' => 'nextcloud',
  'dbpassword' => 'passw@rd',
  'installed' => true,
  'ldapProviderFactory' => 'OCA\\User_LDAP\\LDAPProviderFactory',
);
```

5.5 FreeIPA and FreeRadius

We follow the guide in the link mainly:

https://www.freeipa.org/page/Using_FreeIPA_and_FreeRadius_as_a_RADIUS_based_software_token_OTP_system_with_CentOS/RedHat_7#install-configure-and-test-radius-server-as-a-frontend-to-ipa

During the install, we need to manually enter the FQDN for Server host name, confirm the domain name, and the realm name, enter the passwords for the LDAP Directory Server admin user (“cn=Directory Manager”) and for the IPA admin user (admin):

Add the required ports to the firewall public zone and then restart the firewall service:firewall-cmd --permanent --zone=public --add-port=80/tcp --add-port=443/tcp --add-port=389/tcp --add-port=636/tcp --add-port=88/tcp --add-port=464/tcp --add-port=88/udp --add-port=464/udp --add-port=123/udp
systemctl restart firewalld.service

Now, if everything is correctly configured and running, you should be able to reach the web management interface at https://ipasrv.acme.local

configuration of FreeIPA in /etc/ipa/default.conf:

```
[global]
host = ipasrv.acme.local
basedn = dc=acme,dc=local
realm = ACME.LOCAL
domain = acme.local
xmlrpc_uri = https://ipasrv.acme.local/ipa/xml
ldap_uri = ldapi://%2fvar%2frun%2fslapd-ACME-LOCAL.socket
enable_ra = True
ra_plugin = dogtag
dogtag_version = 10
mode = production
```

In order to configure the RADIUS server to authenticate with the software token provided by the IPA server, we must let RADIUS accept requests from your clients (including the IPA server itself), enable the default configuration to search for users in the IPA server with LDAP protocol and try to authenticate them with an LDAP bind() operation.

All the RADIUS configuration files are in /etc/raddb, and most of the configuration is done by linking files from the mod-available directory to mod-enabled and then editing them as needed. There are also some codes needed to be commented and uncommented. To reach the RADIUS server from other clients, we must also open the firewall for the required ports.

5.6 Web Servers

Both servers were set up using the following commands.

```
sudo apt update
sudo apt install apache2
sudo systemctl start apache2
sudo systemctl enable apache2
```

6. README.md

6.1 How to Connect Remotely

To connect to the internal network remotely, all company devices are pre equipped with a VPN to enable any employee to connect to Stockholm Headquarters. Connecting to the network also requires a password and MFA in the form of Google Authenticator, both of which are provided by IT on the device. To connect through the VPN, simply open the OpenVPN Connect application on your device, and connect to the pre-made profile. Password and MFA code will need to be provided. See figure 2-4. Once connected through to the VPN, the user can access service in the Stockholm network except those deemed too sensitive for remote access (Critical Web Server).

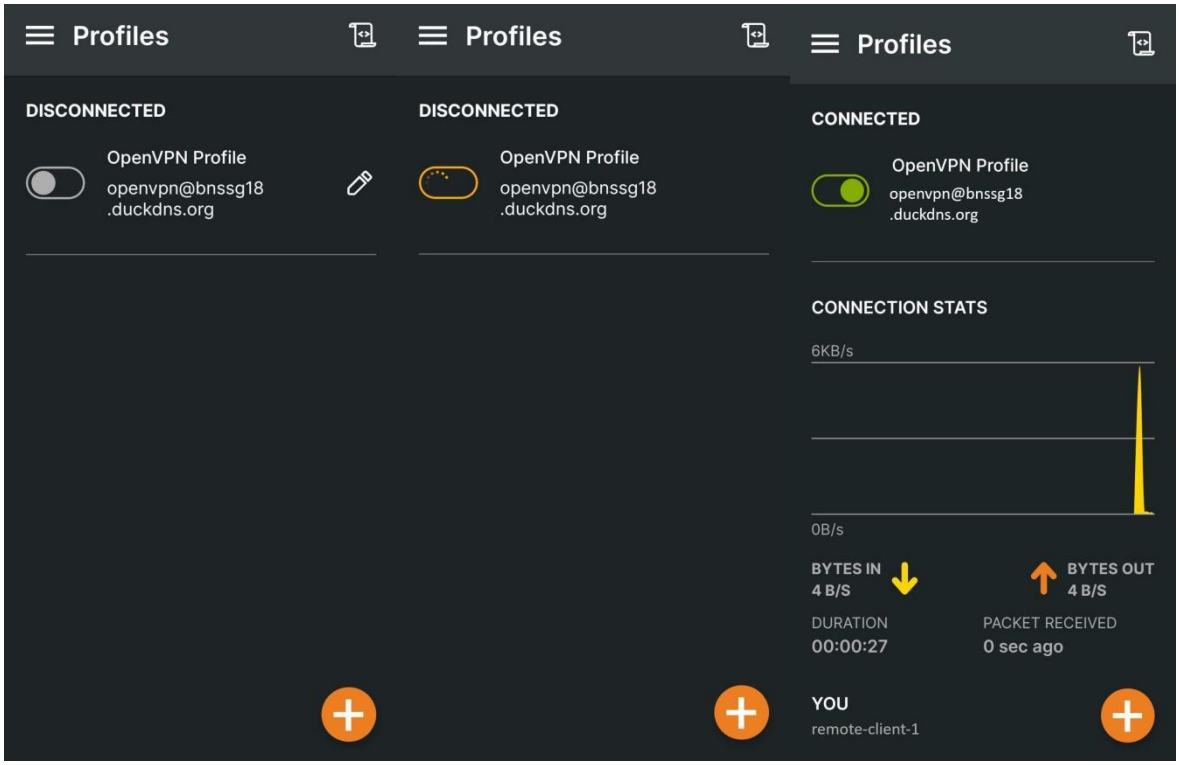

Figure 2, 3, 4: OpenVPN Connect process of connecting

6.2 Create and Revoke Remote Certificates

Creating VPN profiles which include certificates can be done at the access server web interface, found at remote.acme.com. Users and profiles for them to use for remote connections can easily be done with a push of a button, and can as easily be revoked. When logged in as admin, a user can be created under User Management, and their profiles can be created and revoked under User Permissions.

6.3 Log in to Nextcloud or FreeIPA

Now for employees to transfer files, the domain name for Nextcloud is: nextcloud.acme.com. We could use the same company accounts and passwords for FreeIPA (ipasrv.acme.local) directly.

6.4 Snort log file

The Snort log is in the file snort.alert.fast, you can use this command to get it: `sudo tail -f /var/log/snort/snort.alert.fast`

6.5 Web servers

There are 2 web servers. Only employees in Stockholm and London can access the critical web server and the remote employees can only visit the less critical web server. A web server can be controlled through the following commands:
`sudo systemctl status apache2`
`sudo systemctl stop apache2`
`sudo systemctl start apache2`
`sudo systemctl restart apache2`
The page contents can be edited in the following directory: `/var/www/html`

7. Reflection

7.1 Solution Advantages

Highly compatible, feature-rich, and easy to deploy: Supports dynamic IP allocation and DNS protection, offers excellent scalability and maintainability, making it suitable for complex enterprise networks and diverse environments.
Strong security with robust authentication: Integrates username/password, RADIUS, LDAP, and 2FA authentication mechanisms to ensure secure access.
Efficient and reliable for cross-regional office connectivity: Utilizes TUN mode (Layer 3 - IP layer) to reduce network overhead, enhance data processing speed, and enable secure interconnectivity.

7.2 Future Enhancements

Upgrade IDS to IPS: Enhance security by not only detecting attacks but also proactively preventing threats and blocking malicious traffic.
Enhance RBAC for finer access control: Use LDAP/RADIUS for role assignment and enforce RBAC across firewalls, VPNs, and applications for better security management.