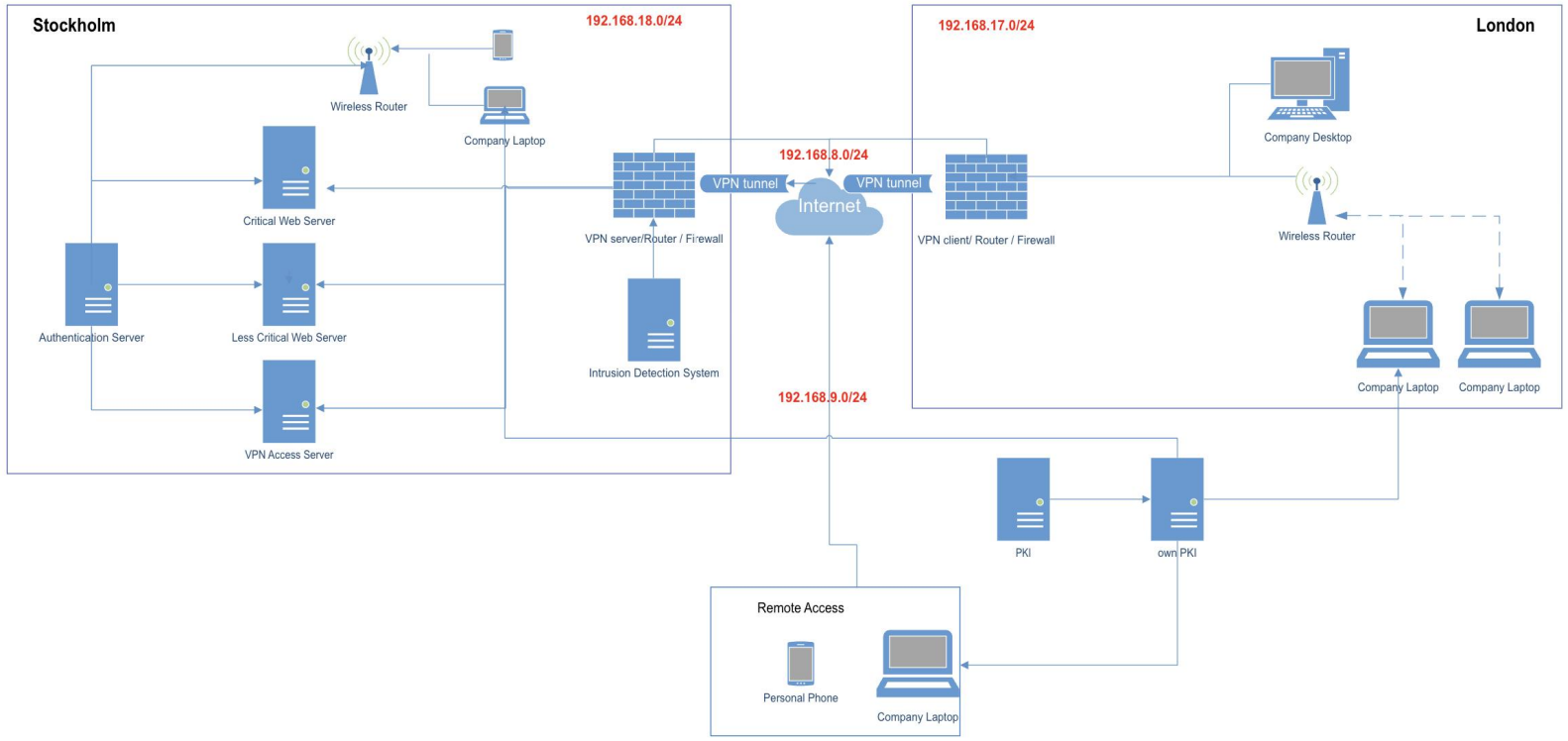
Cross-Regional Remote Access Network Solution

BNSS 2025--Group 18

Biqi Liu, Siying Chen, Tim Rundström, Yiyi Miao

Requirements and System Design

- Secure Access
- Centralized User Authentication
- Secure File Exchange
- Network Defense
- Secure Wireless Connectivity
- Robustness and Scalability



Tools and Technologies

- **VPN Solution:** OpenVPN (TUN mode)， Easy-RSA
- **Authentication:** FreeIPA, FreeRADIUS, LDAP, Certificate
- **File Exchange:** Nextcloud
- **Security protection:**
  - Firewall (OpenWRT built-in firewall, default-deny policy)
  - Intrusion Detection System (Snort)
  - DNS Security (DNSSEC in OpenWRT)

Implementation – Site-to-Site VPN Tunnel

OpenVPN (TUN mode), Easy-RSA

Stockholm

```
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'
```

London

```
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'
```

Firewall - Zone Settings

General Settings | Advanced Settings | Conntrack Settings

The options below control the forwarding policies between this zone (lan) a
lan. *Source zones* match forwarded traffic from other zones **targeted at lai**
not imply a permission to forward from wan to lan as well.

Covered devices: tun0

Allow-OpenVPN	Incoming *IPv4* and *IPv6*, protocol *TCP*, *UDP* From **wan** To *this device*, port *1194*	*Accept* input

Install OpenVPN and Easy-RSA

Stockholm server preparation

↓

Generate Security Certificates

CA certificate	server/client certificates	DH parameters

↓

Configure OpenVPN Server

TUN mode	UDP 1194 port	AES-256-GCM encryption

↓

Network Routing and Firewall

Enable IP forwarding	Firewall rules

↓

Client Configuration

Import certificates	Establish VPN tunnel connection

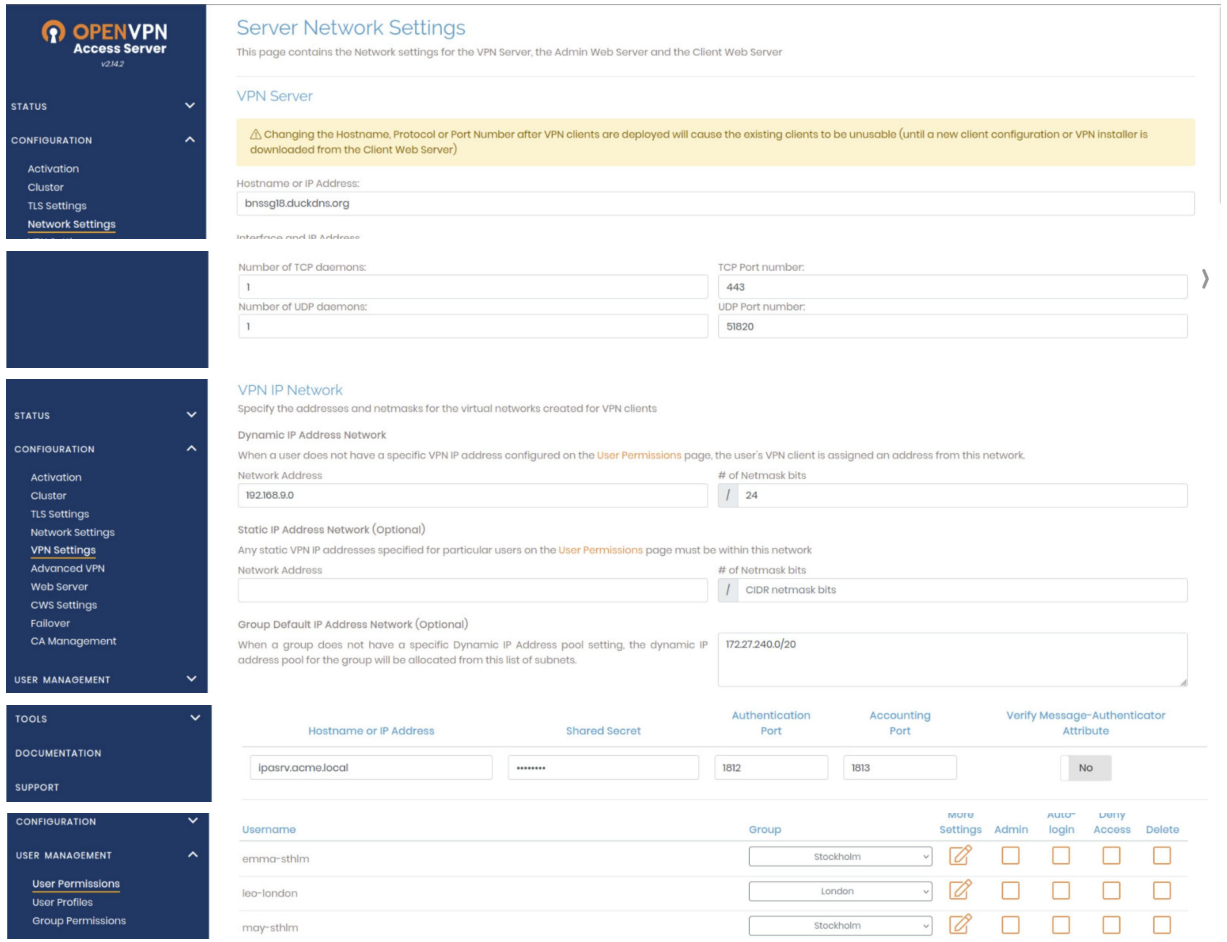
↓

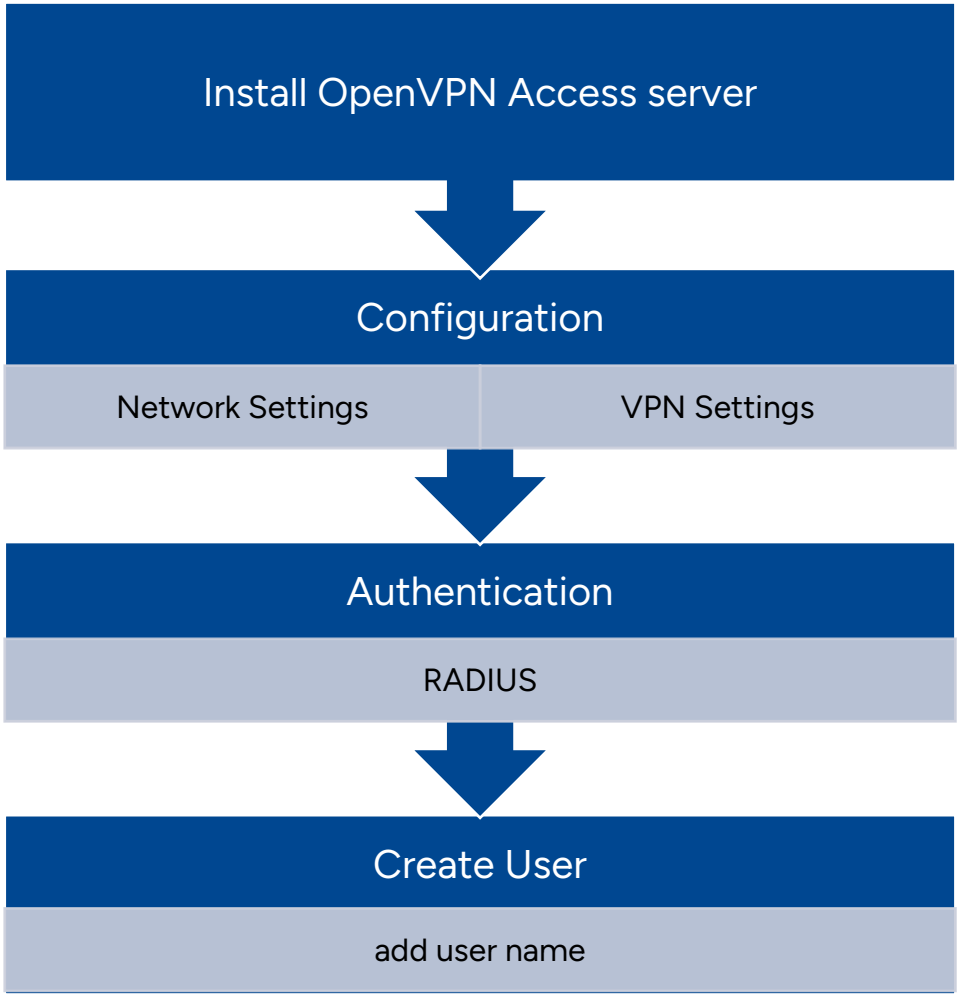
Set Up Site-to-Site Routing

Configure client-specific routes

Implementation – Remote VPN

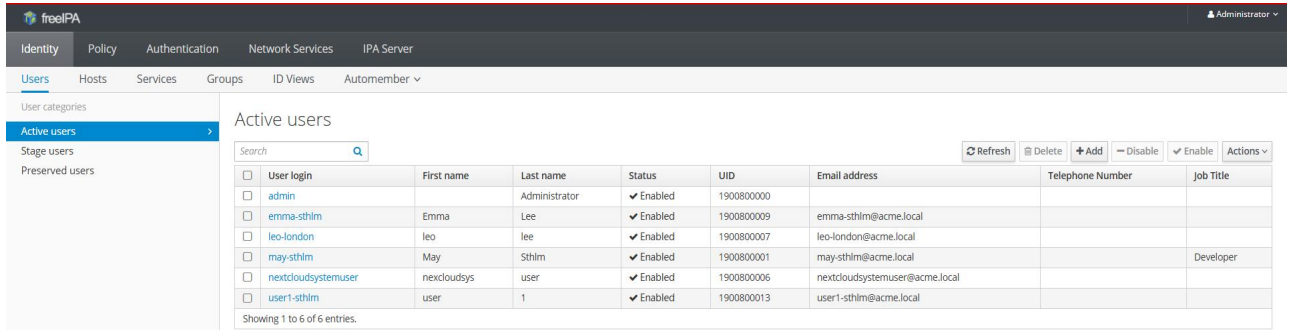
```
bash <(curl -fsS https://packages.openvpn.net/as/install.sh) --yes
```





Implementation – Authentication

FreeIPA, LDAP



HBAC Rule: sysadmin_webservers

Host Groups
stockholm

```
[ipa-server@ipasrv ~]$ ipa hbactest --user emma-sthlm --host ipa01.acme.local --service sshd
---------------------
Access granted: True
---------------------
  Matched rules: sysadmin_webservers
[ipa-server@ipasrv ~]$ ipa hbactest --user user1-sthlm --host ipa01.acme.local --service sshd
---------------------
Access granted: False
---------------------
  Not matched rules: sysadmin_webservers
[ipa-server@ipasrv ~]$ ipa hbactest --user leo-london --host ipa01.acme.local --service sshd
---------------------
Access granted: False
---------------------
  Not matched rules: sysadmin_webservers
```

Deploy FreeIPA Server

CentOS 7	IP	LDAP-based Identity Management

Configure FreeIPA Environment

FQDN	LDAP Domain	Realm (ACME.LOCAL)	DH parameters	LDAP Directory Manager	Admin User

Firewall Configuration

Open LDAP & FreeIPA required ports

Deploy and Configure

Integrate FreeIPA LDAP	Enable LDAP authentication backend

Set Multi-Factor Authentication (MFA)

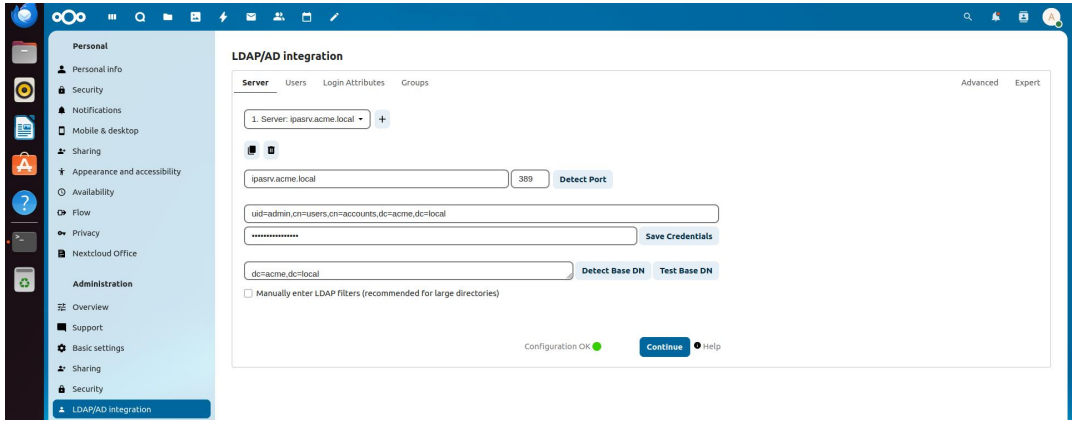
OTP tokens	Enforce MFA

Test and Validate Authentication

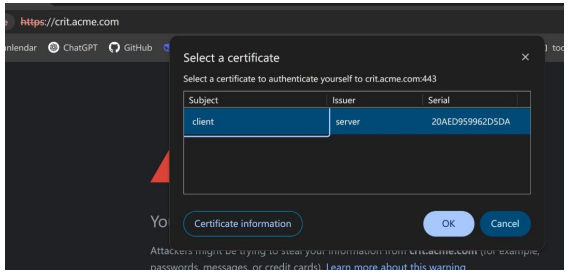
Confirm LDAP and OTP-based log

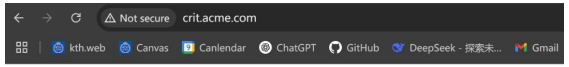
Implementation – File Exchange and Web server

Nextcloud, Certificate




```
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        ServerName crit.acme.com
        DocumentRoot /var/www/html

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine on

        SSLCertificateFile      /etc/ssl/certs/server.crt
        SSLCertificateKeyFile   /etc/ssl/private/server.key
        SSLCACertificateFile /etc/apache2/ca.crt

        SSLVerifyClient require
        SSLVerifyDepth  10

        SSLOptions +StrictRequire
        <FilesMatch "\.(?:cgi|shtml|phtml|php)$">
                SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
                SSLOptions +StdEnvVars
        </Directory>
</VirtualHost>
```





Welcome to ACME Critical Web Server

Here you can do critical actions, but only if you're coming from an office with the right credentials! :)

Install Required Packages

Apache2 / Docker

Configure Apache Web Server

- Set DocumentRoot to Nextcloud directory
- Configure domain/IP

Setup Nextcloud Configuration

- Trusted domains
- Database connection
- LDAP authentication

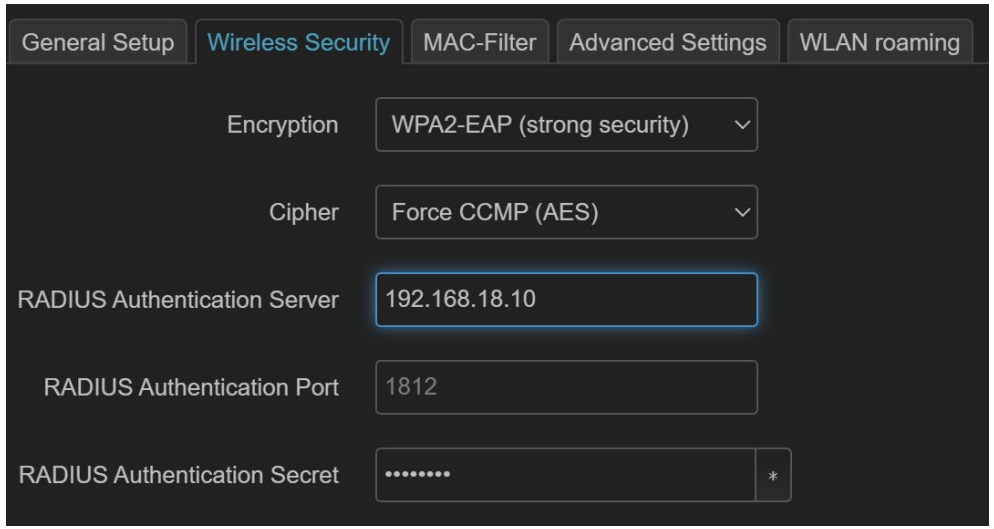
Add Self-signed Certificate / Enable Admin Security

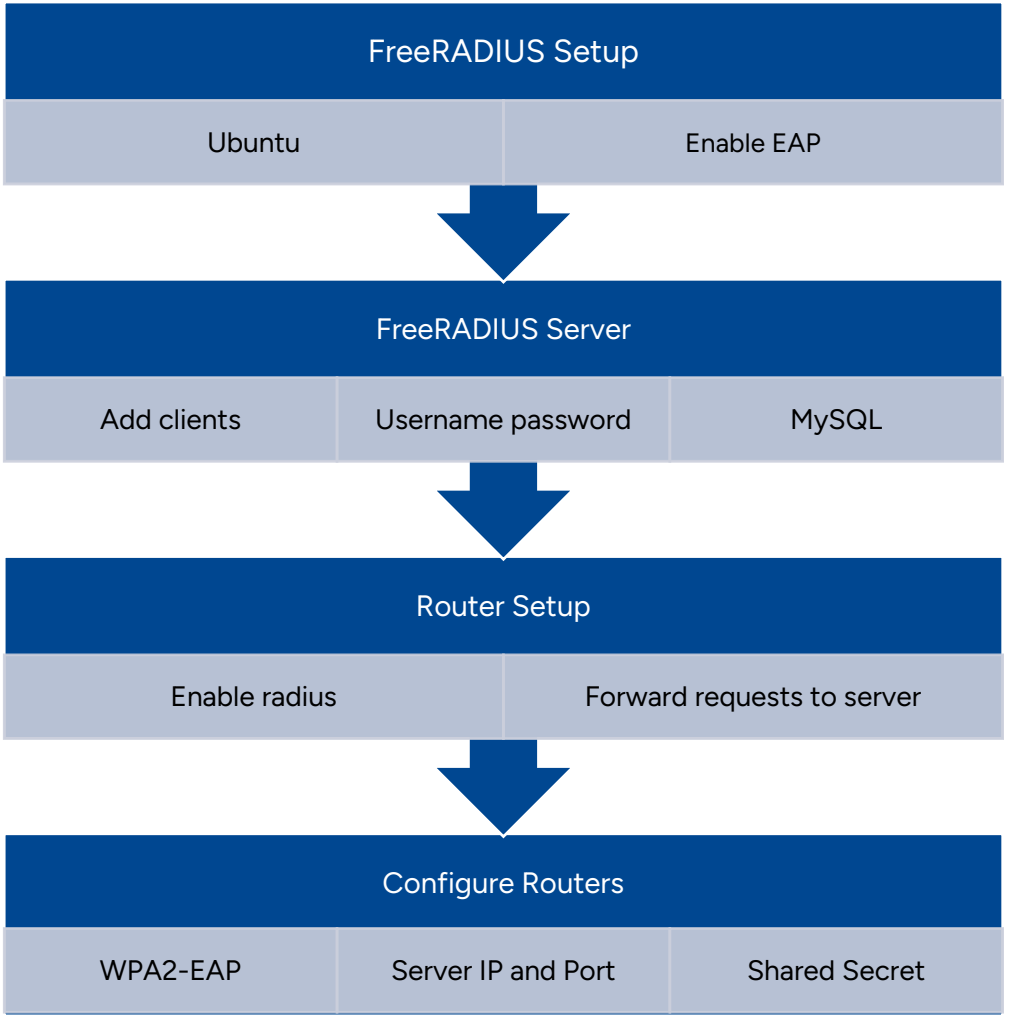
Enable HTTPS connection / Activate Two-Factor Authentication

Implementation – Wireless Authentication

FreeRADIUS, PEAP

```
mysql> select * from radcheck;
+----+----------+--------------------+----+-----------+
| id | username | attribute          | op | value     |
+----+----------+--------------------+----+-----------+
|  1 | tina     | Cleartext-Password | := | bnss2025  |
|  2 | bob      | Cleartext-Password | := | hello     |
|  3 | client1  | Cleartext-Password | := | password1 |
+----+----------+--------------------+----+-----------+
3 rows in set (0,00 sec)
```





Implementation – Security protection

stockholm Status System Services Network VPN

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for e
hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action
Restrict Crit Web From Remote	Forwarded IPv4 and IPv6 From lan, IP 192.168.18.27, 192.168.9.0/24 To lan, IP 192.168.18.12	Drop forward
Allow-DHCP-Renew	Incoming IPv4, protocol UDP From wan To this device, port 68	Accept input
Allow-Ping	Incoming IPv4, protocol ICMP From wan To this device	Accept input
Allow-IGMP	Incoming IPv4, protocol IGMP From wan To this device	Accept input
Allow-DHCPv6	Incoming IPv6, protocol UDP From wan To this device, port 546	Accept input
Allow-MLD	Incoming IPv6, protocol ICMP From wan, IP fe80::/10 To this device	Accept input
	Incoming IPv6, protocol ICMP	

Firewall
(in OpenWRT)

```
ipvar HOME_NET 192.168.18.0/24
ipvar EXTERNAL_NET any

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;)

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

sudo tail -f /var/log/snort/snort.alert.fast
```

Deploy Snort

Install on virtual machines

↓

Configuration

HOME_NET	Detection Rules	Log Alerts

↓

Configure Port Mirroring

Use iptables (MANGLE table) on routers for traffic duplication.

Intrusion Detection System
(Snort)

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 dnssecheckunsigned '1'

stockholm Status System Services Network VPN Log out REFRESHING

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

Delete

CFG01411C

General | Devices & Ports | DNSSEC | Filter | Forwards | Limits | Log | Resolv & Hosts Files
Static Leases | Hostnames | IP Sets | Relay | SRV | MX | CNAME | PXE/TFTP

DNSSEC ☑
Validate DNS replies and cache DNSSEC data, requires upstream to support DNSSEC.

DNSSEC check unsigned ☑
Verify unsigned domain responses really come from unsigned domains.

Add

DNS Security
(DNSSEC in OpenWRT)

Conclusion & Future Work

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.

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.