

ACME Network Project

GROUP 6

External Security & Web Servers (Keyao Huang)

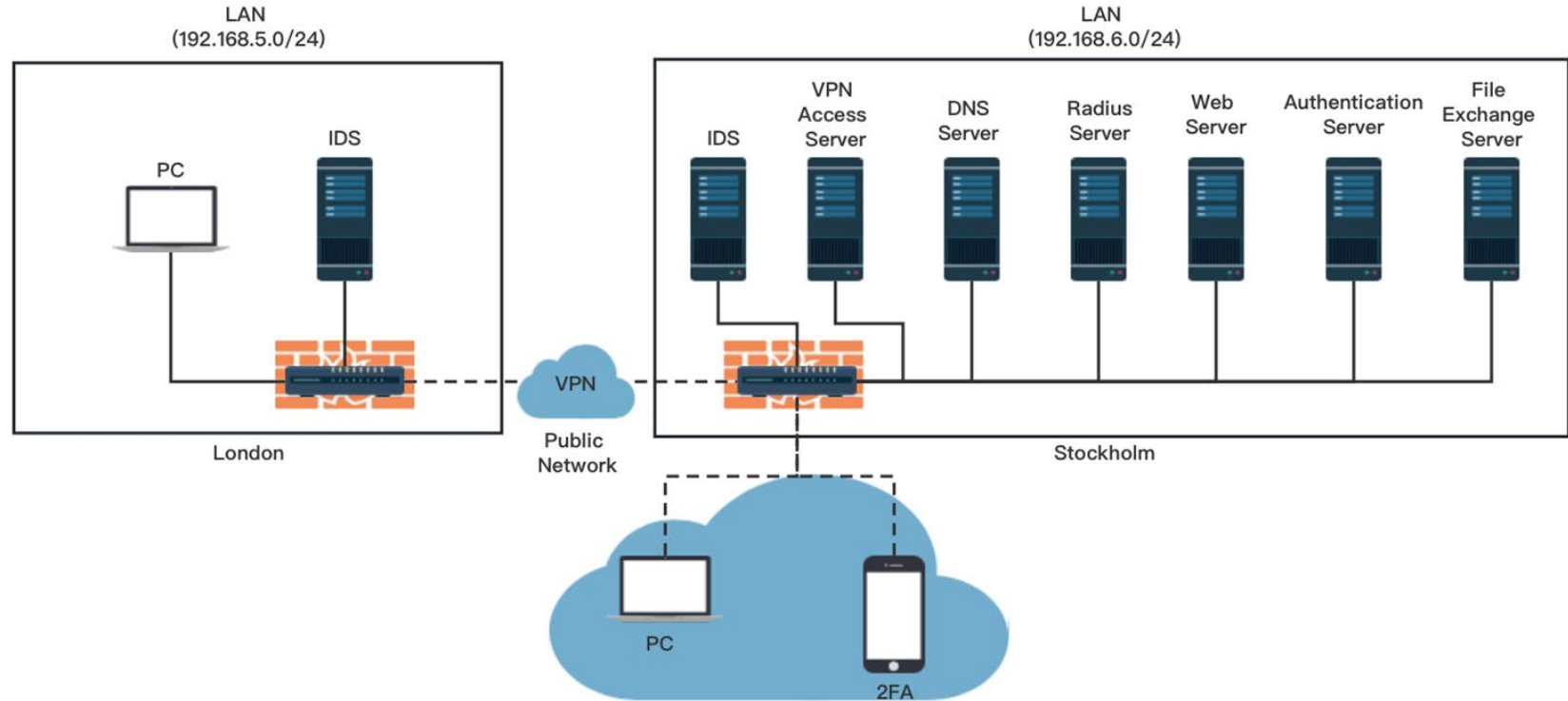
DNS & IDS (Zhiyuan Lin)

Wireless Security & File Exchange (Enze Wang)

CA & OpenSSL (Ziyang Song)

Presentation Date: March 15, 2023

Network Topology



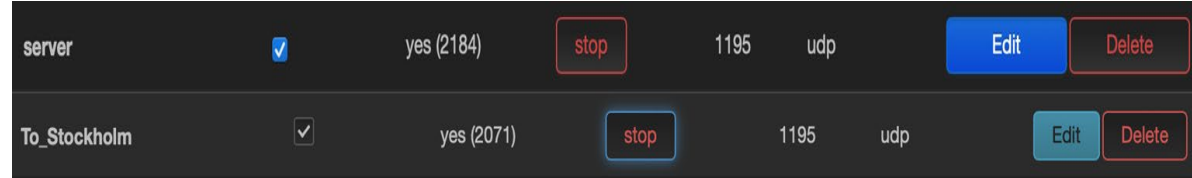
External Security - VPN & 2FA



1. Router VPN

Stockholm Router -> OpenVPN Server

Only Accept One Client (London Router)



2. VPN Access Server

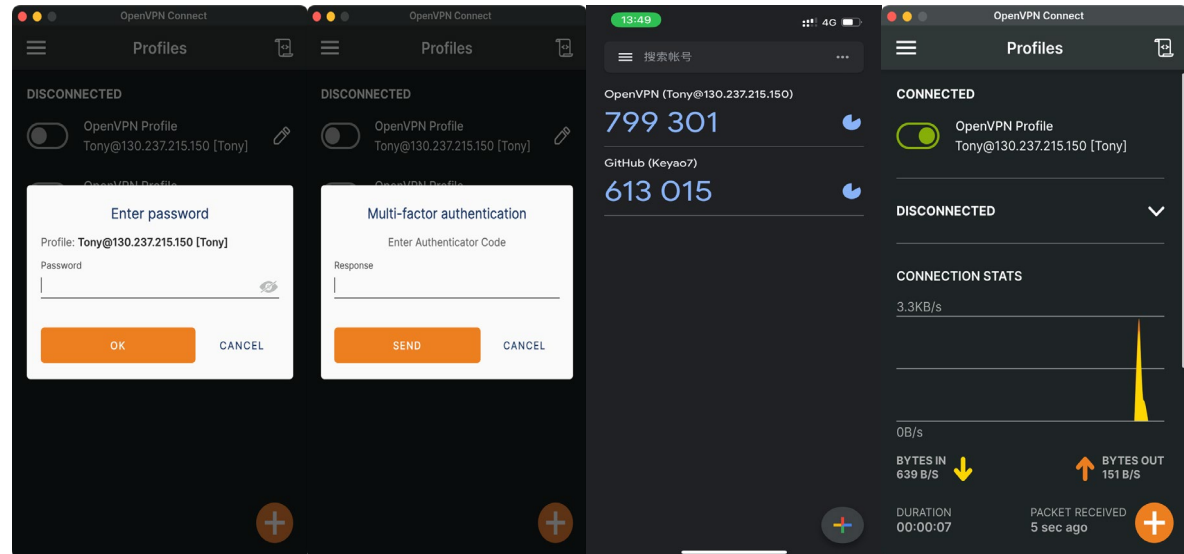
Install OpenVPN-as in VM

Accept External Client

3. VPN 2FA

One Time 6 Digit Pin-Codes

With Google Authenticator



Web Servers

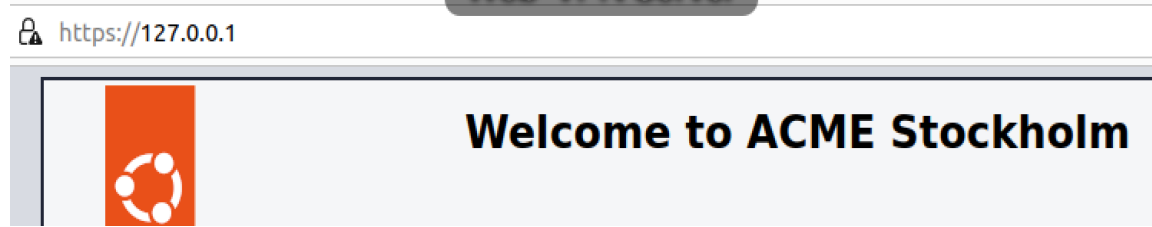
1. Normal Web Server

- Can be access by In-company users and external users
- Using HTTPS

2. Critical Web Server

- Not allow external users to access
- Using iptables to block external users

```
ubuntu@ubuntu:~$ sudo iptables -L
[sudo] password for ubuntu:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  192.168.9.0/24          192.168.6.113          tcp dpt:http-alt
```



Certificate Viewer: 172.52.30.41

General

Details

Issued To

Common Name (CN)	172.52.30.41
Organization (O)	ACME
Organizational Unit (OU)	Headquarters

Issued By

Common Name (CN)	ca.demo.com
Organization (O)	ACME
Organizational Unit (OU)	Headquarters

Validity Period

Issued On	Tuesday, March 14, 2023 at 8:48:59 PM
Expires On	Saturday, May 13, 2023 at 9:48:59 PM

Fingerprints

SHA-256 Fingerprint	F4 88 95 83 AD 6C 18 76 5A B7 51 A0 D7 5C A4 8F 6D 77 0C 1B 2B D9 AE 87 74 6E C6 33 2A 76 AC 15
SHA-1 Fingerprint	2F DA F6 20 C8 85 06 B8 52 AE 31 2C 0C 79 B2 8A 44 1E 7C 4A

Internal Security—IDS



- **Snort** as an NIDS, with mirrored traffic from router to get more coverage
- Configure the local rules file or download the rules from SNORT website.
- Set up snort.conf file, test and run

Table: Mangle

Chain *PREROUTING* (Policy: *ACCEPT*, 53435 Packets, 27.04 MB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
53.94 K	27.34 MB	TEE	all	*	*	0.0.0.0/0	0.0.0.0/0	TEE gw:192.168.6.113	-

Chain *POSTROUTING* (Policy: *ACCEPT*, 164503 Packets, 88.22 MB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
164.50 K	88.22 MB	TEE	all	*	*	0.0.0.0/0	0.0.0.0/0	TEE gw:192.168.6.113	-

```
"
#-----
# LOCAL RULES
#-----
alert icmp any any -> $HOME_NET any (msg:"ICMP Packet Detected";sid:1000001;rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH incoming"; flow:stateless; flags:S+; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"Potential SSH Brute Force Attack"; flow:to_server; flags:S; threshold:type threshold, track_by_src, count 3, seconds 60; classtype:atten
```

DNS

- BIND9 is used for deploying the DNS service for STOCKHOLM network
- Configure db.demo.com and db.168.192 and named.conf.local files



```
Open  db.168.192 /etc/bind
1 ;
2 ; BIND reverse data file for local loopback interface
3 ;
4 $TTL      604800
5 @         IN      SOA      demo.com. root.demo.com. (
6                               1          ; Serial
7                               604800     ; Refresh
8                               86400      ; Retry
9                               2419200    ; Expire
10                              604800 )    ; Negative Cache TTL
11 ;
12 @         IN      NS       localhost.
13 1.0.0     IN      PTR      localhost.
14 233.6 IN PTR demo.com ;
15 133.6.168.192.in-addr.arpa. IN PTR radius.demo.com
16 113.6.168.192.in-addr.arpa. IN PTR web.demo.com
17 184.6.168.192.in-addr.arpa. IN PTR nextcloud.demo.com
```

```
Open  db.demo.com /etc/bind Save
1 ;
2 ; BIND data file for local loopback interface
3 ;
4 ;
5 $TTL      604800
6 @         IN      SOA      demo.com. root.demo.com. (
7                               2          ; Serial
8                               604800     ; Refresh
9                               86400      ; Retry
10                              2419200    ; Expire
11                              604800     ; Negative Cache TTL
12                              )
13 @         IN      NS       localhost.
14 @         IN      A        192.168.6.233
15 web       IN      A        192.168.6.113
16 radius   IN      A        192.168.6.133
17 nextcloud IN      A        192.168.6.184
18 ;
19 * IN      A        192.168.6.233 ;
20 ; Add the DNSKEY records
21 demo.com. IN DNSKEY 257 3 8 ( AwEAAbsFZZlOofeKT2k6fQcX5DAR/R4i1FP5s8jSHUVs/VV2Vj5WT7Zn
TIW6pKlji8SNVQruC0e8WXjswlskG9Pxp4WgiIXuP5grW5TWrkme4SIE 1XldGD6B/ycyovG/nAp/
ycA6PaL8ahMBxVcGNSYthoHK8PlfCEP6Svvl 460rta/LL20UYweDi0G7Y1ak7Cnc1V4Ts6COKMLKlg+3drXS1fzv06c
l9Ev/2if7nEdyS819dTw6jGhPy+h2jgNfNex85kxJM/R70L4vQ/wJlQ8
ZPvQ1nS6D+CrTJNHNlZImL0jgSzEHveUhrXJNCWQ1ttrFBPABVFYCDL1 lZa6jZ0rA00= )
22 demo.com. IN DNSKEY 256 3 8 ( AwEAAADPT7PjlsrgNIV+weyrX0tRqvJexjg0d5VNHvb05RVZk3JRXZBu/u
VxgtlQLewIgrG0Z9TfKs3b3D0N15eKa29K17NBG00LX/8NgU8V40xzVH
8Kpj+zcBsaprAiv+WtUzP9wYCPtKacDBqEnrHhdXuTC4Per4tiwm21P3 nozFvLE0bCOMqh/ZnpH0D93L/
uI7Xg8G6DqXhLaB0XIaRDehNH17zSB ZcP3C3v45skotbnQ5TMNL1qL50DK3qFDAd5VNm9CyTYK9IRJUP1N9eRZR
DTE5JkNXpyujj09YeJpBWBdTgX7l7pmjK79X3tRokTMLaK2I+RD2aIA GYoUhh4+b7U= )
```

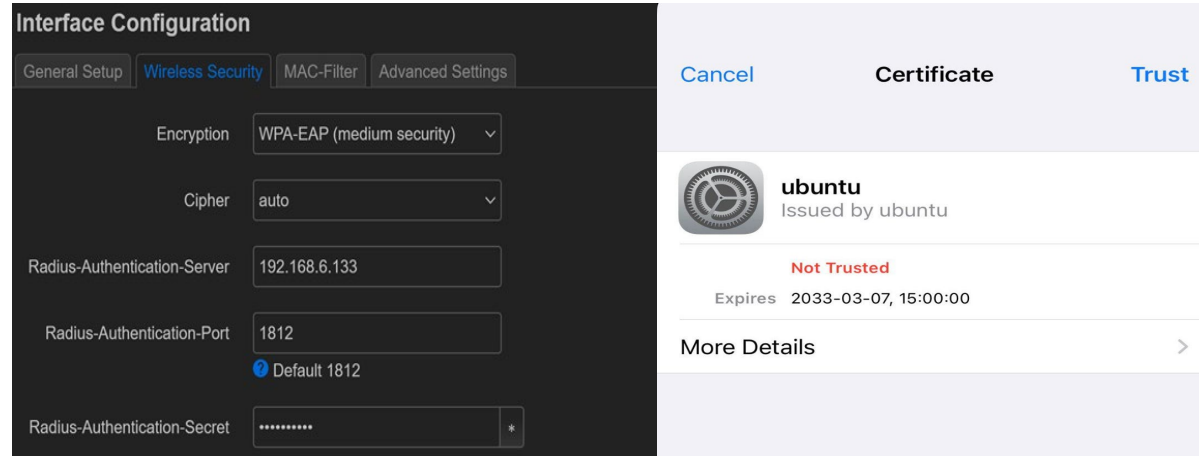
Wireless Security: Radius Server

Main configuration for freeradius :

- 1) at /freeradius/3.0/clients.conf set two routers as the NAS
- 2) edit /freeradius/3.0/users file which includes employees' user/password information
- 3) under /freeradius/3.0/certs/client.cnf, modify the cnf file and run “make” generate user certificates

Set WPA-EAP as the encryption

for router and server on OpenWRT :

The image shows two side-by-side screenshots. The left screenshot is from the OpenWRT web interface, specifically the 'Interface Configuration' page under the 'Wireless Security' tab. It shows settings for 'Encryption' set to 'WPA-EAP (medium security)', 'Cipher' set to 'auto', 'Radius-Authentication-Server' set to '192.168.6.133', 'Radius-Authentication-Port' set to '1812' (with a note 'Default 1812'), and 'Radius-Authentication-Secret' masked with dots. The right screenshot shows a system certificate for 'ubuntu' issued by 'ubuntu'. The certificate status is 'Not Trusted' in red text. It includes an expiration date of '2033-03-07, 15:00:00' and a 'More Details' link with a right-pointing arrow.

Wireless Security: Radius Server

Start the debug mode : “freeradius -X”, and “ready to process request” is shown in the terminal.

```
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on proxy address * port 40307
Listening on proxy address :: port 47073
Ready to process requests
```

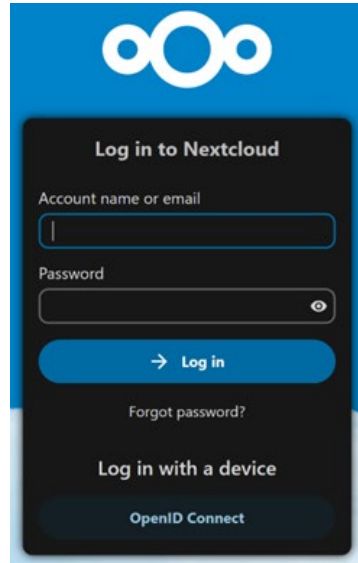
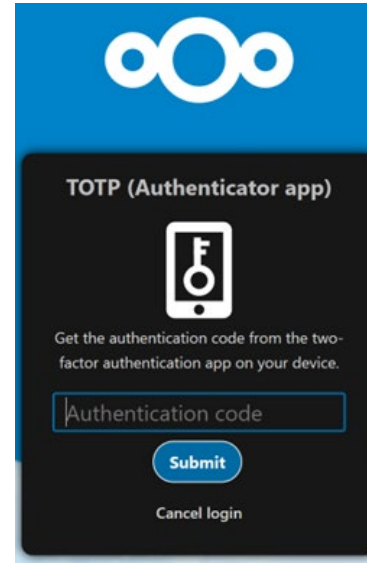
Now, employees can access the wireless internet through radius authentication:

- 1) A user connects to the Network Access Server (router) and initiates a login.
- 2) The NAS (router) communicates with the RADIUS server using a shared secret mechanism that the port 1812 is for authentication.
- 3) The NAS sends a RADIUS message (an Access-Request) to the server.

File Exchange server: Nextcloud

We run nextcloud server with docker container. So, we run the server using Docker Desktop.

Sever is running, you should be able to login Nextcloud at 192.168.6.184:9006 with 2FA. After successfully logging in, users should be able to chat and shire files. For example, one way to share files is transferring ownership.

The image shows the Nextcloud login interface. At the top is the Nextcloud logo (three interlocking circles) on a blue background. Below it, on a dark grey background, is the title 'Log in to Nextcloud'. There are two input fields: 'Account name or email' and 'Password'. Below the password field is a blue button with a right arrow and the text 'Log in'. Underneath the button is a link 'Forgot password?'. At the bottom, there is a section titled 'Log in with a device' with a button labeled 'OpenID Connect'.The image shows the Nextcloud Two-Factor Authentication (2FA) screen. At the top is the Nextcloud logo on a blue background. Below it, on a dark grey background, is the title 'TOTP (Authenticator app)'. There is an icon of a smartphone with a key symbol. Below the icon is the text 'Get the authentication code from the two-factor authentication app on your device.' There is an input field for the 'Authentication code'. Below the input field is a blue button labeled 'Submit'. At the bottom is a link 'Cancel login'.

- *.key Private Key
- *.pem Certificate or Certificate chain file
- *.csr Certificate signing request (CSR)
- *.cnf Configuration File
- *.crl Certificate revocation list (CRL)
- *.vrfy Certificate Verification

All files use PEM format.

Hierarchy:

1. Root CA
(External, with full chain)
2. Intermediate CA
(Internal, maintaining local CRL)
3. Server or User
(With mutual TLS verification)

Web Server certificate and authentication



The connection for this site is not secure

172.30.52.41 didn't accept your login certificate, or a login certificate may not have been provided.

Try contacting your organization.

ERR_BAD_SSL_CLIENT_AUTH_CERT

Select a certificate for authentication

Site 172.30.52.41:443 needs your credentials:



chiron.demo.com

ca.demo.com

ACME test

3/15/2023

Certificate information

OK

Cancel

General Structure of Trust (Imaginary)

