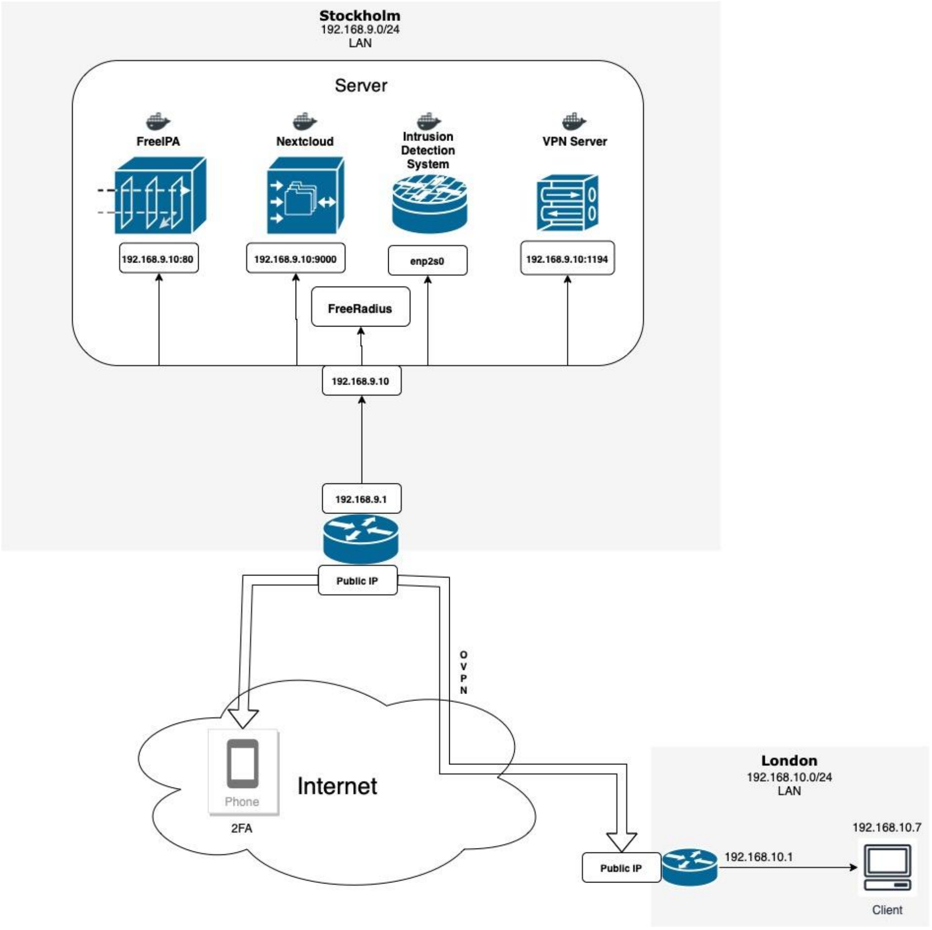
ACME

A proposal for a secure enterprise network



Group 7:
Poncet - Stournaras - Ståhl - Åström

Needs and Requirements

Specified by ACME

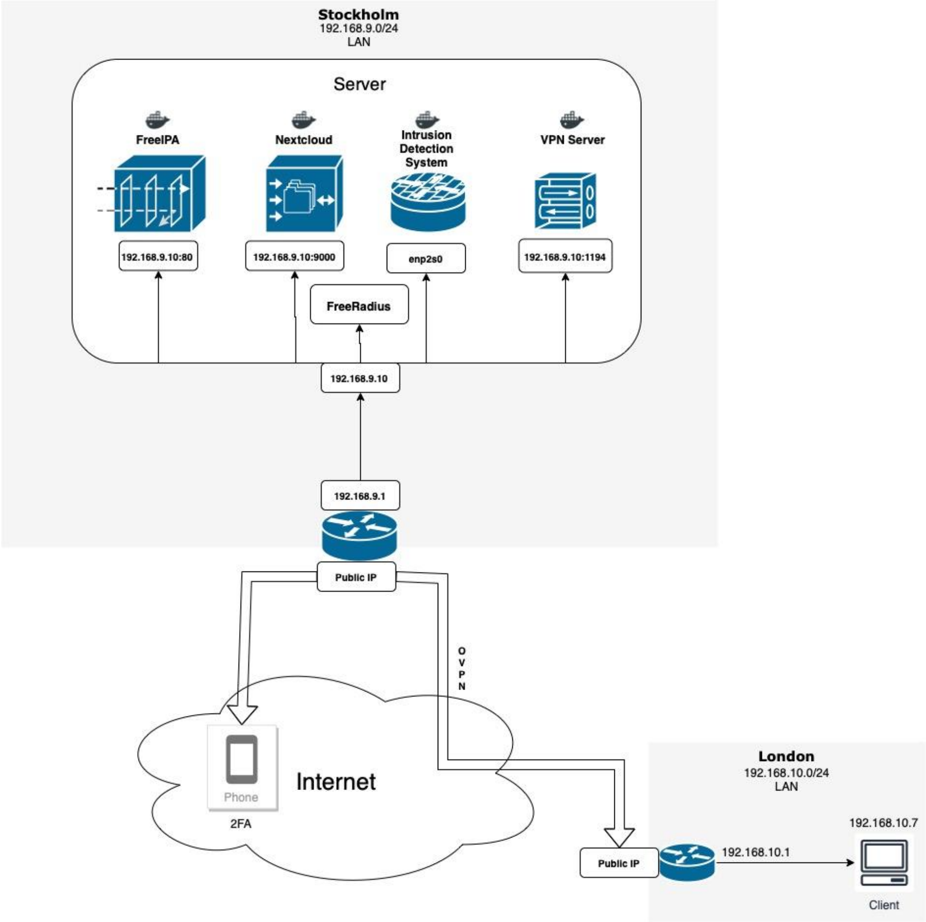
- Employee Authentication
- Confidentiality
- Secure connectivity
- Secure Wireless Access
- Secure File Exchange

Topology

- All services containerized on server in Stockholm branch

- Allows for easy expansion of infrastructure in new branches

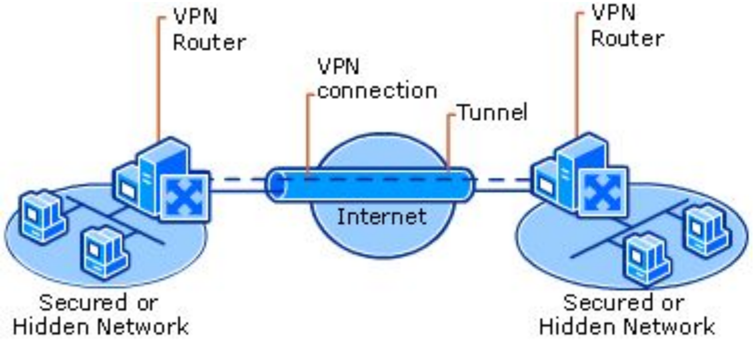
- Same containers can be spun up in other branches



VPN

Ensures confidentiality from third parties. VPN tunnel between Stockholm and London branches, as well as from employees wanting to access ACME networks from home or other locations.

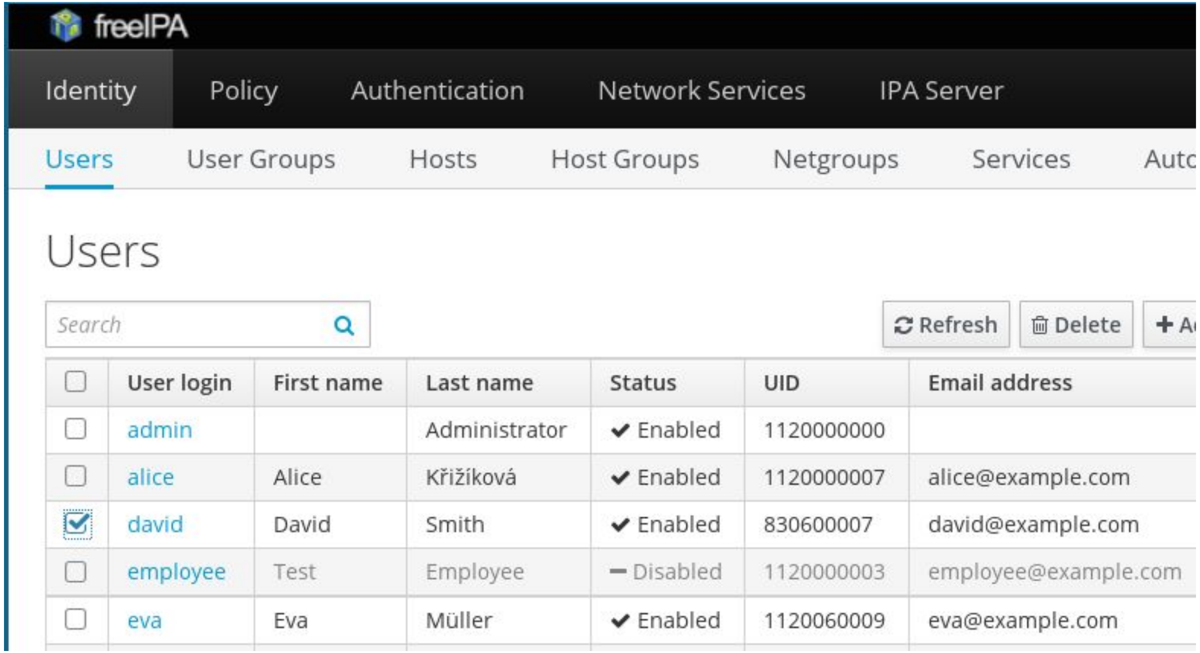
- OpenVPN free open source alternative
- Connected to FreeIPA



Identity Manager

- Needed for Employee Authentication.

- FreeIPA opensource alternative that integrates well with the file server. Easy enabling of 2FA.

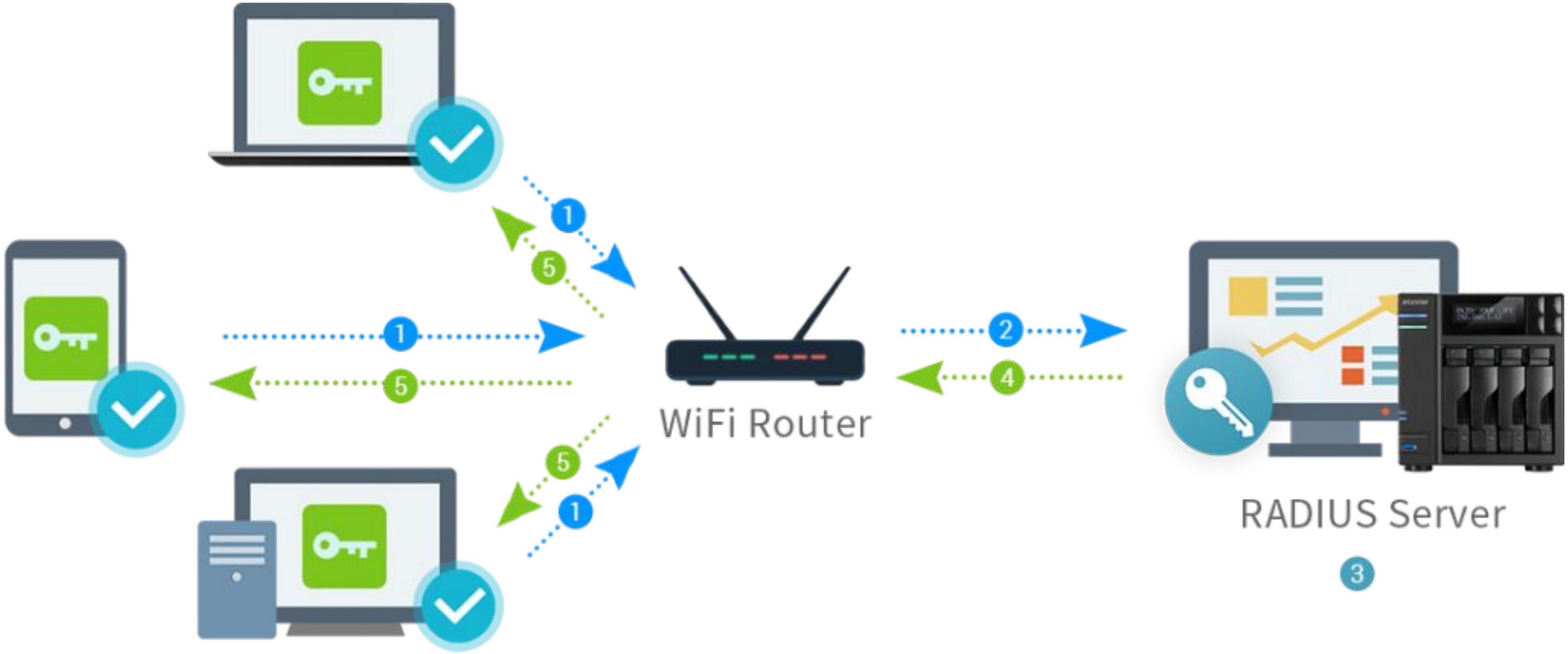


Users

□	User login	First name	Last name	Status	UID	Email address
□	admin		Administrator	✔ Enabled	1120000000	
□	alice	Alice	Křižíková	✔ Enabled	1120000007	alice@example.com
☑	david	David	Smith	✔ Enabled	830600007	david@example.com
□	employee	Test	Employee	− Disabled	1120000003	employee@example.com
□	eva	Eva	Müller	✔ Enabled	1120060009	eva@example.com

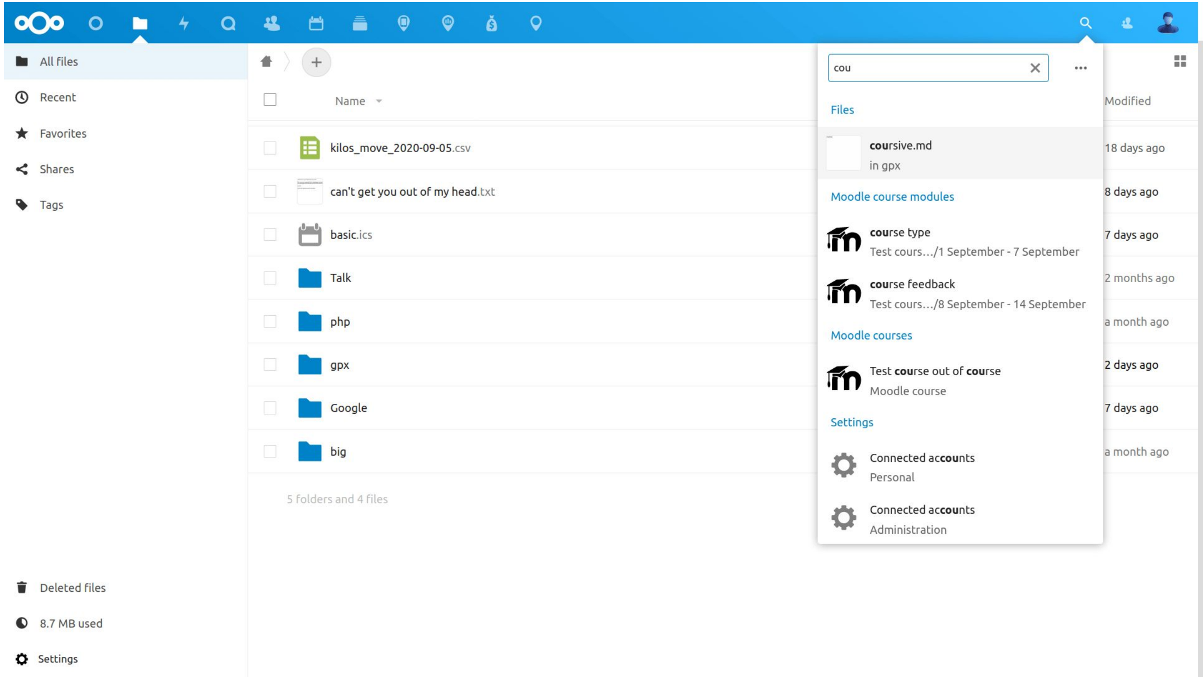
Radius server

FreeRadius for 802.1x authentication. This ensures Secure Wireless Access.



File server

Nextcloud - Ensures Secure File Exchanges. Only permissioned access allowed for the file server.



Name	Modified
kilos_move_2020-09-05.csv	18 days ago
can't get you out of my head.txt	8 days ago
basic.ics	7 days ago
Talk	2 months ago
php	a month ago
gpx	2 days ago
Google	7 days ago
big	a month ago

5 folders and 4 files

cou

Files

coursive.md
in gpx

Moodle course modules

course type
Test cours.../1 September - 7 September

course feedback
Test cours.../8 September - 14 September

Moodle courses

Test course out of course
Moodle course

Settings

Connected accounts
Personal

Connected accounts
Administration

Intrusion Detection System

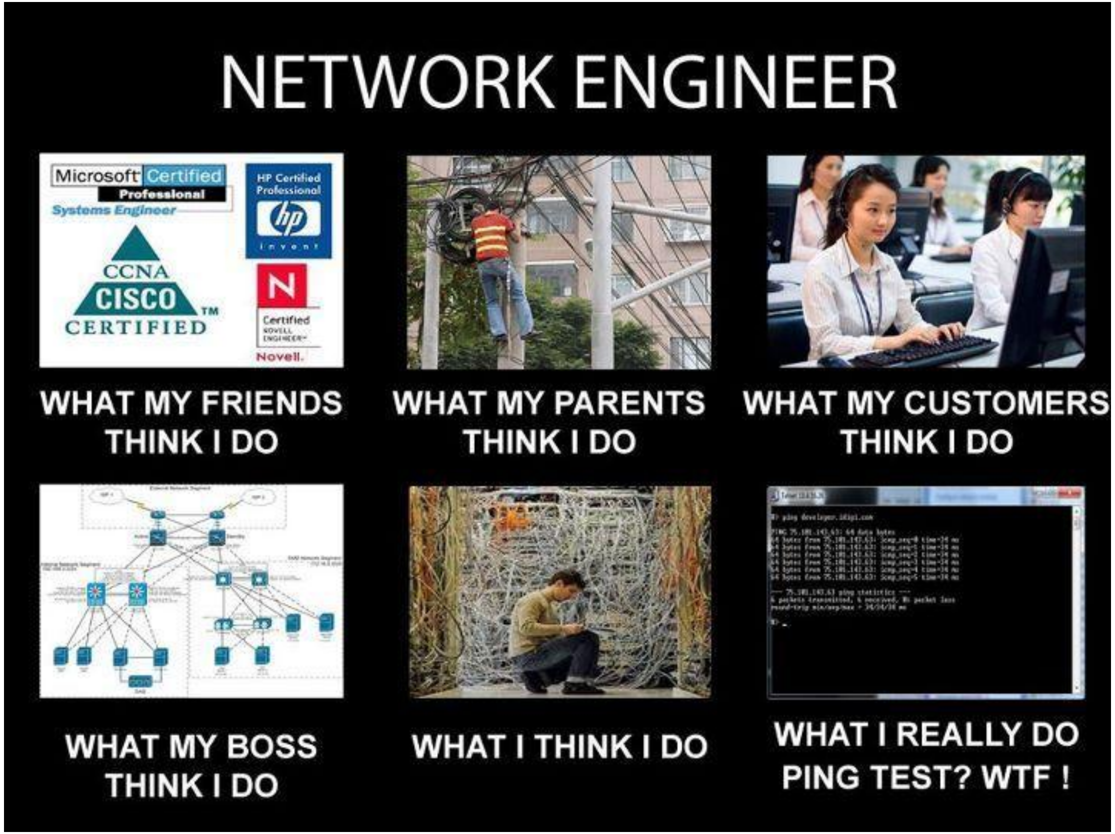
To detect attacks against our infrastructure, we use the open-source IDS software SNORT running containerized on the Stockholmserver. The IDS has rules covering:

- SSH Brute Force Attacks
- Malicious port scannings
- DDOS, including “ping of death”
- NTP
- Attack-responses

Example alert from running port scan on network

```
03/04-16:41:28.802112  [**] [1:1000004:1] SSH incoming [**] [Priority: 0] {TCP} 192.168.9.2:55338 -> 192.168.9.26:22
03/04-16:41:28.805635  [**] [1:628:8] SCAN nmap TCP [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.9.2:55338 -> 192.168.9.26:22
03/04-16:41:56.717214  [**] [1:368:6] ICMP PING BSDtype [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.9.2 -> 192.168.9.26
03/04-16:41:56.717214  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.9.2 -> 192.168.9.26
03/04-16:41:56.717273  [**] [1:1000001:0] Pinging... [**] [Priority: 0] {ICMP} 192.168.9.26 -> 192.168.9.2
03/04-16:42:15.831005  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.9.2 -> 192.168.9.26
03/04-16:42:15.851048  [**] [1:620:11] SCAN Proxy Port 8080 attempt [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.9.2:55340 -> 03/04-16:42:16.960237
03/04-16:42:17.064509  [**] [1:1000002:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.9.2:55368 -> 192.168.9.26:21
03/04-16:42:18.397314  [**] [1:1000005:4] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 192.168.9.2:55860 -> 192.168.9.26:22
03/04-16:42:18.606497  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.9.2:56020 -> 192.168.9.26:705
03/04-16:42:18.827199  [**] [1:618:10] SCAN Squid Proxy attempt [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.9.2:56207 -> 192.168.9.26:3128
```

Thanks for listening!


NETWORK ENGINEER
Microsoft Certified Professional
Systems Engineer
HP Certified Professional
hp invent
CCNA
CISCO
CERTIFIED
Certified NOVELL ENGINEER
Novell.
WHAT MY FRIENDS THINK I DO
WHAT MY PARENTS THINK I DO
WHAT MY CUSTOMERS THINK I DO
WHAT MY BOSS THINK I DO
WHAT I THINK I DO
WHAT I REALLY DO
PING TEST? WTF !

```
#> ping developer.idigi.com

PING 75.101.143.63: 64 data bytes
64 bytes from 75.101.143.63: icmp_seq=0 time=34 ms
64 bytes from 75.101.143.63: icmp_seq=1 time=34 ms
64 bytes from 75.101.143.63: icmp_seq=2 time=34 ms
64 bytes from 75.101.143.63: icmp_seq=3 time=34 ms
64 bytes from 75.101.143.63: icmp_seq=4 time=34 ms
64 bytes from 75.101.143.63: icmp_seq=5 time=34 ms

--- 75.101.143.63 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss
round-trip min/avg/max = 34/34/34 ms

#> _
```