

Practical Security Analysis and Measures for 5G Private Industrial Standalone (SA) Deployments

26. VDE/ITG Fachtagung Mobilkommunikation

Lars B. Vosteen

Kompetenzzentrum CoSA – Technische Hochschule Lübeck

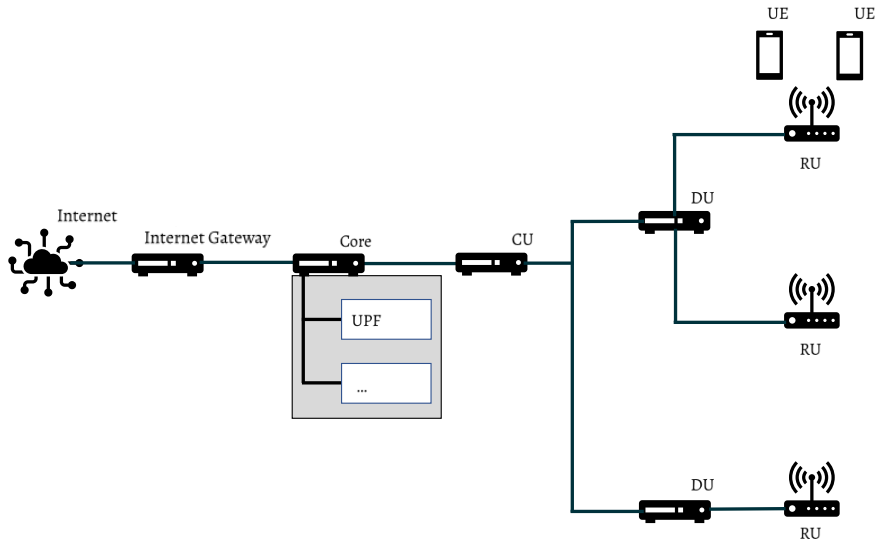
Institut für Telematik – Universität zu Lübeck

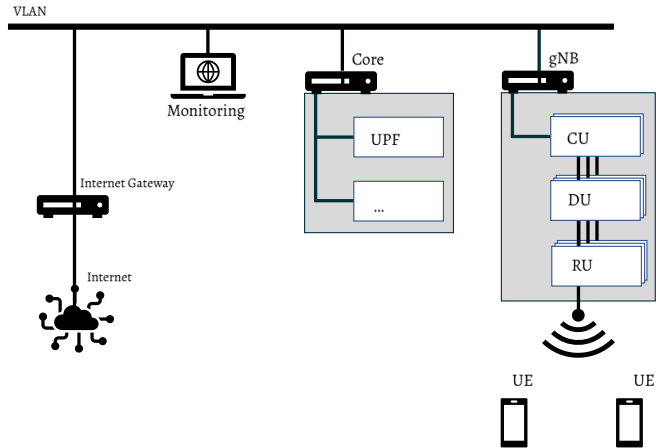
2022-05-19

1. Angriffsfläche eines 5G-Campussystems
2. Sicherheitsmaßnahmen
3. Monitoring-System

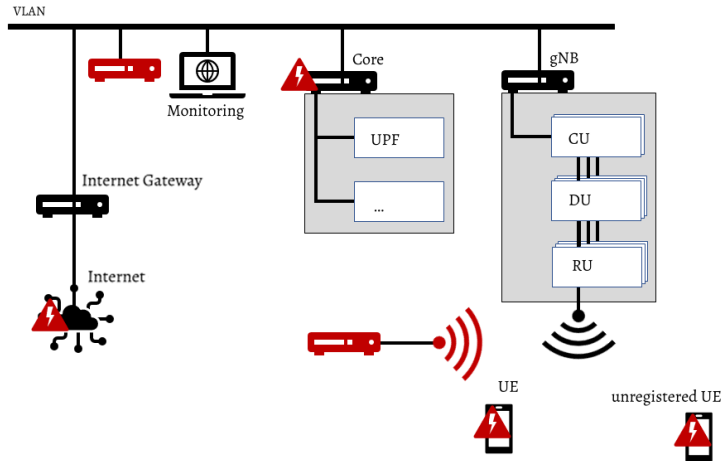


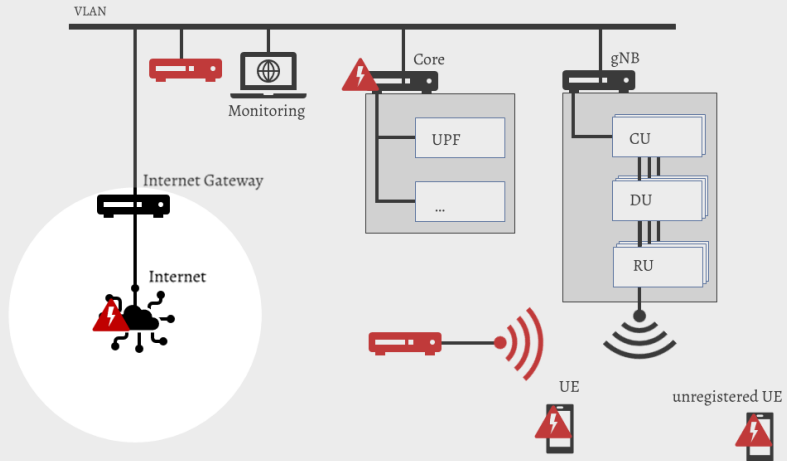
Fabian John, Jörg Schuljak, Björn Sievers, Andreas Hanemann, Horst Hellbrück

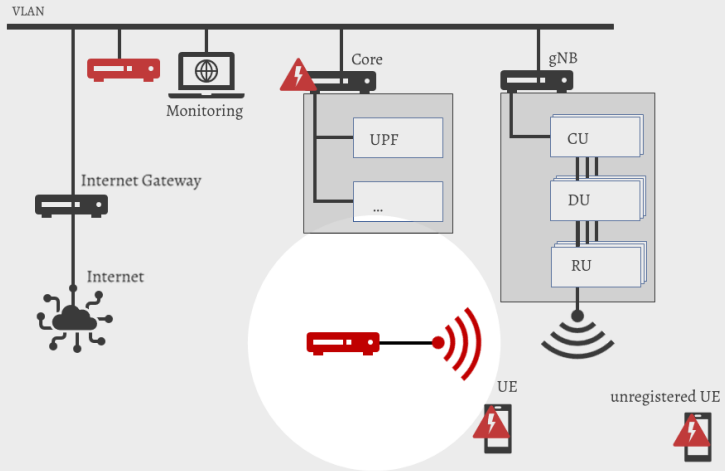


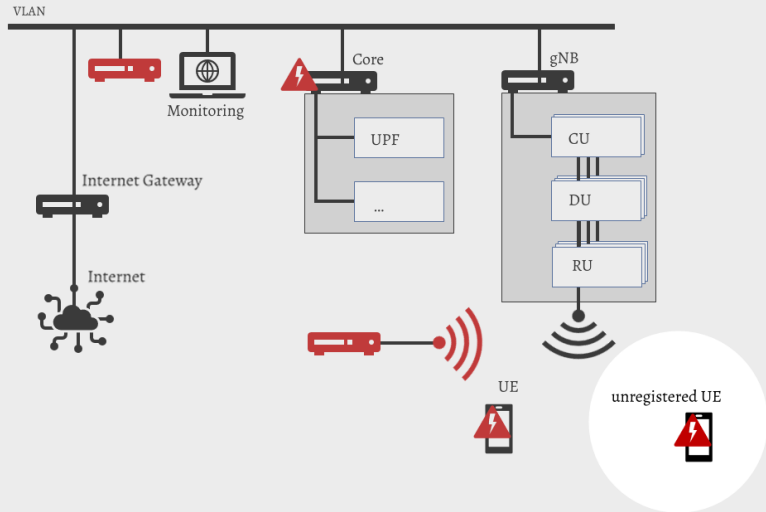


Sicherheitsanalyse









Flashing SIM Cards

Start the program OYSIMWrite4.1.5 which should be delivered with the Oyeitimes SIM card programmer. The value have to be like the ones in the following pictures:

SIM Personalize tools(Copyright:OYEITIMES Co.,Ltd Ver 4.1.5)

Reader(PC/SC): Identiv CLOUD 2700 R Smart Card Reader 0 Refresh Read Card Write Card Save Data Load Data Exit

Batch Write Card
Data File: Select File Go First Prev Next Last Find Continue Template

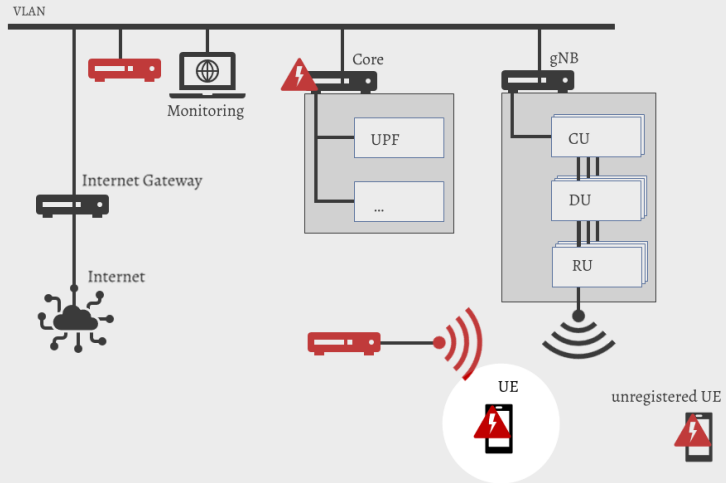
Common Parameter
ATR: 3B9F95801FC38031E073FE21135786810286984418A8 Type: LTE(LH02):LTE+GSM Language: ADN
ICCID: 89010208930000000001 Inc (DEC20) PIN1: 1234 PUK1: 88888888 PIN2: 1234 PUK2: 88888888 (ASC8) ADM: 3838383838383838 (HEX16/8)

GSM/WCDMA/LTE CDMA/EVDO/CSIM VoLTE/ISIM

GSM Parameter
☐ IMSI18: 809262950000000031 ☒ IMSI15: 2629500000000031 Inc (DEC18/15)
ACC: 0002 Input (DEC4) AD: 00000002
☐ Inc KI: 0C0A34601D4F07677303652C0462535B (HEX32)
PLMN: 46000; 46002; 46007; 46008; 45412; 41004 Auto
EHPLMN: 26295
FPLMN:
HPLMN: 00 (HEX2) GID1: GID2: (HEX)
SMSP: + MSISDN: Inc (ASC)
SPN: CoSA THL (ASC)
ECC:
Algorithm: ☐ Comp128-1 ☐ Comp128-2 ☐ Comp128-3 ☒ Milenage

LTE/WCDMA Parameter
☐ IMSI18: 809262950000000031 ☒ IMSI15: 2629500000000031 Inc (DEC18/15)
ACC: 0002 Input (DEC4) AD: 00000002
☐ Inc KI: 0C0A34601D4F07677303652C0462535B (HEX32)
☒ OPC: 638FA50EE6523365FF14C1F45F88737D (HEX32)
☐ OP: 11111111111111111111111111111111 (HEX32)
PLMNwAct: 26295:8000; 26295:0080; 26295:4000
OPLMNwAct: 26295:8000; 26295:0080; 26295:4000
HPLMNwAct: 26295:8000; 26295:0080; 26295:3400 Auto
EHPLMN: 26295
FPLMN:
HPPLMN: 00 (HEX2) GID1: GID2: (HEX)
SMSP: + (ASC) MSISDN: Inc (ASC)

<https://git.mylab.th-luebeck.de/5g/cosa-5g-private-campus-network-deployment-oai/-/blob/main/oai-network-setup.md#flashing-sim-cards>



Netzwerkscan

```
user@ue:~$ traceroute th-luebeck.de
```

```
[...]
```

```
2  192.168.70.129 (192.168.70.129)  27.053 ms  27.024 ms  26.996 ms
```

```
3  192.168.50.1 (192.168.50.1)  32.979 ms  32.954 ms  32.927 ms
```

```
[...]
```

Netzwerkscan

```
user@ue:~$ nmap 192.168.70.0/24
```

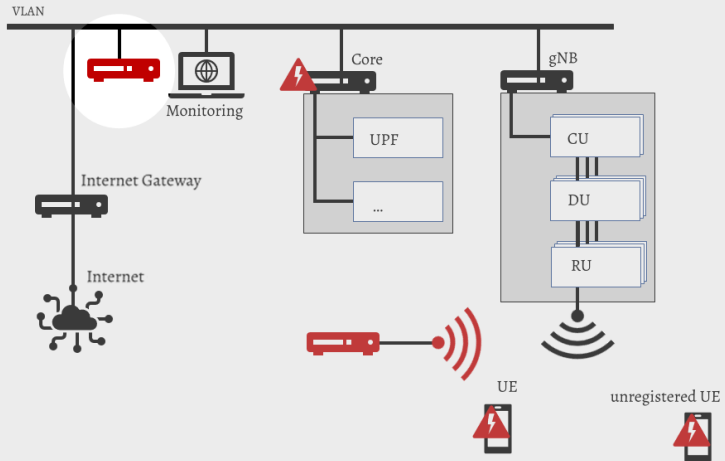
```
[...]
```

```
Nmap done: 256 IP addresses (10 hosts up) scanned in 27.29 seconds
```

```
user@ue::~~$ nmap 192.168.50.0/24
```

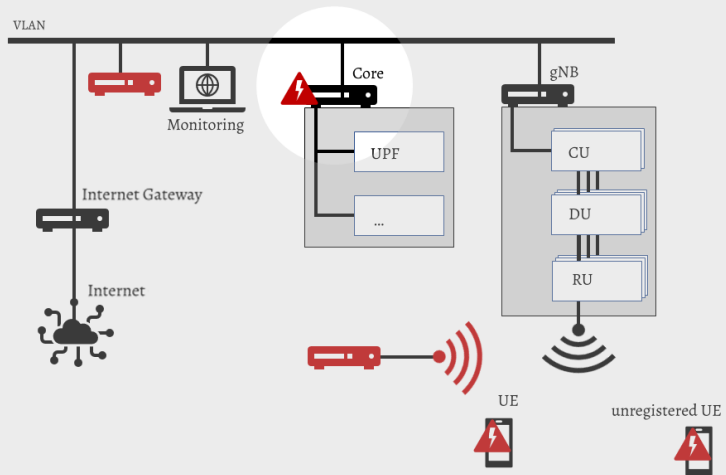
```
[...]
```

```
Nmap done: 256 IP addresses (9 hosts up) scanned in 14.48 seconds
```

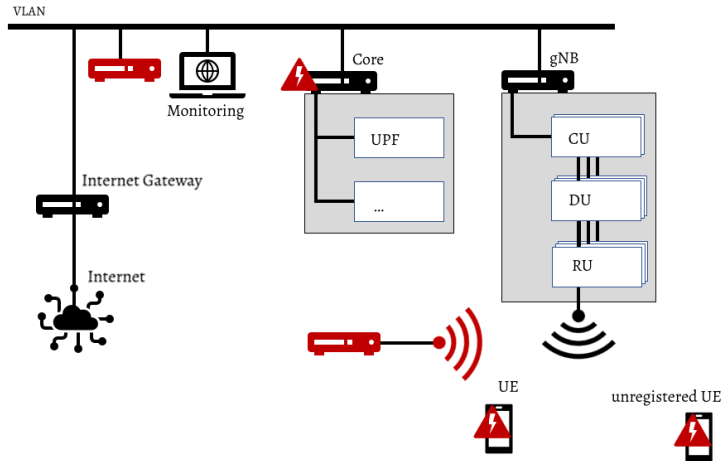


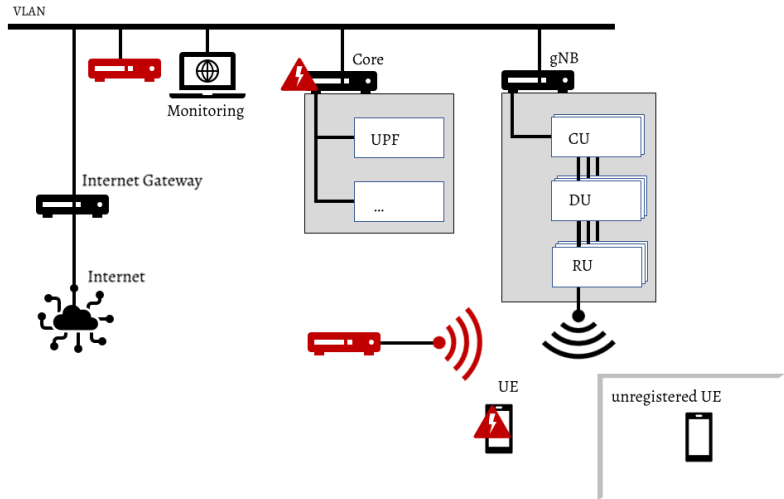
SSH-Passwort-Rateangriff

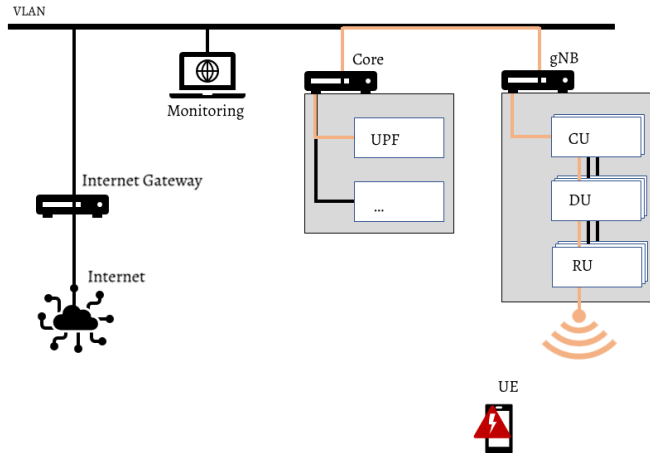
```
user@ue:~# hydra -l fiveg -x 1:4:a1 core180216.th-luebeck.de ssh  
[...]  
[22][ssh] host: core180216    login: fiveg    password: <REDACTED>  
[STATUS] 114.05 tries/min, 1497984 tries in 218:55h  
1 of 1 target successfully completed, 1 valid password found
```

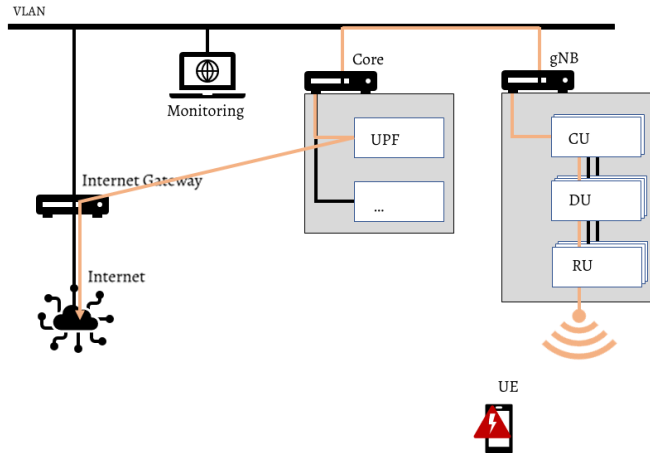



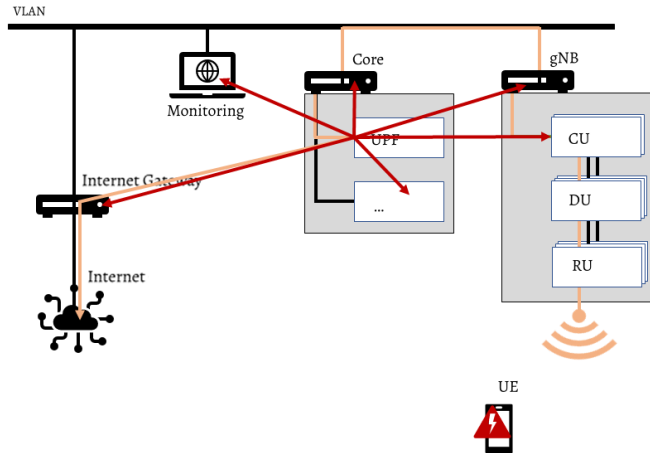
Gegenmaßnahmen

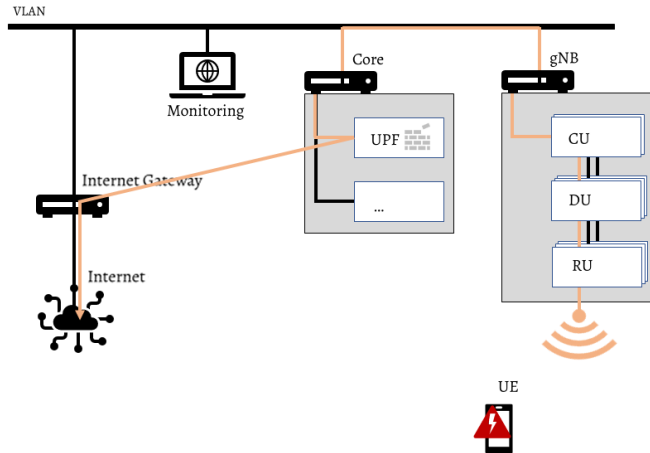


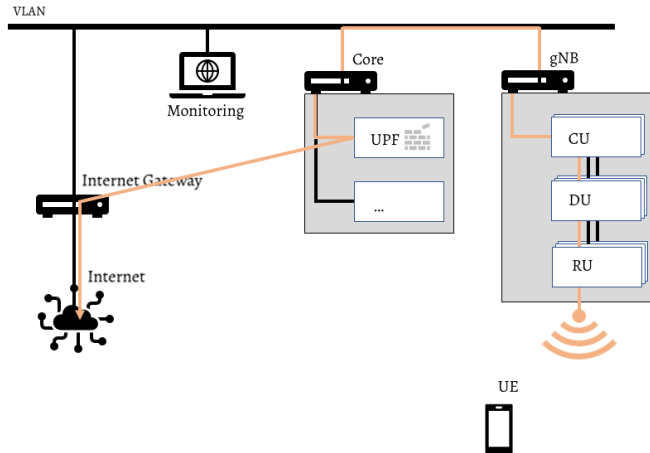


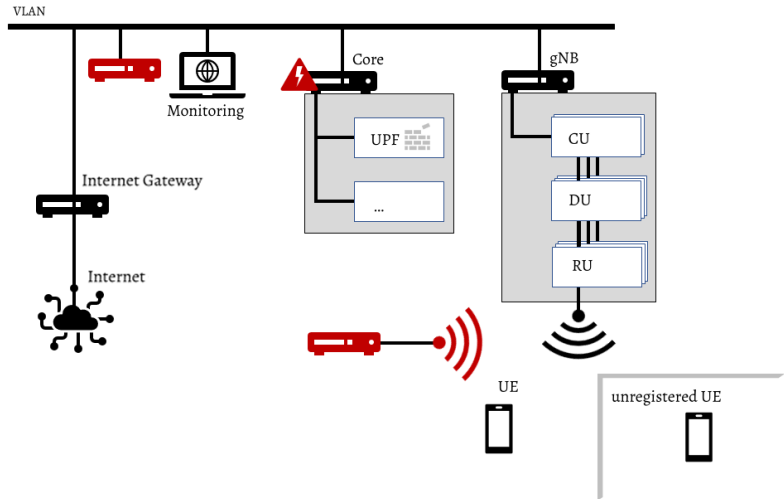


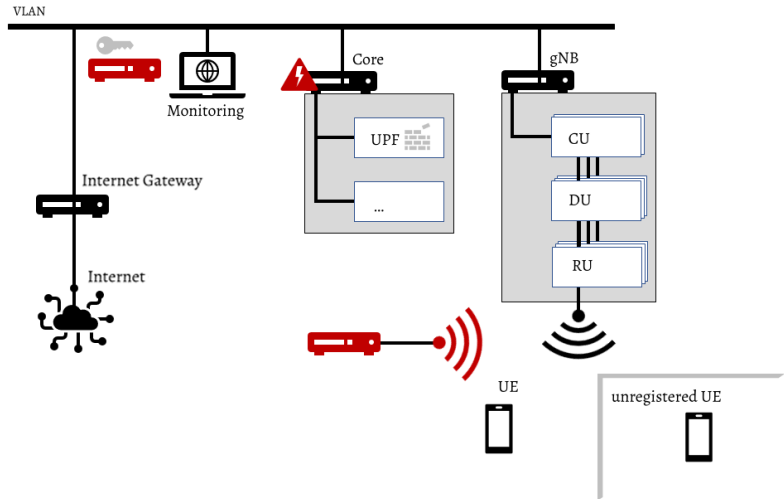


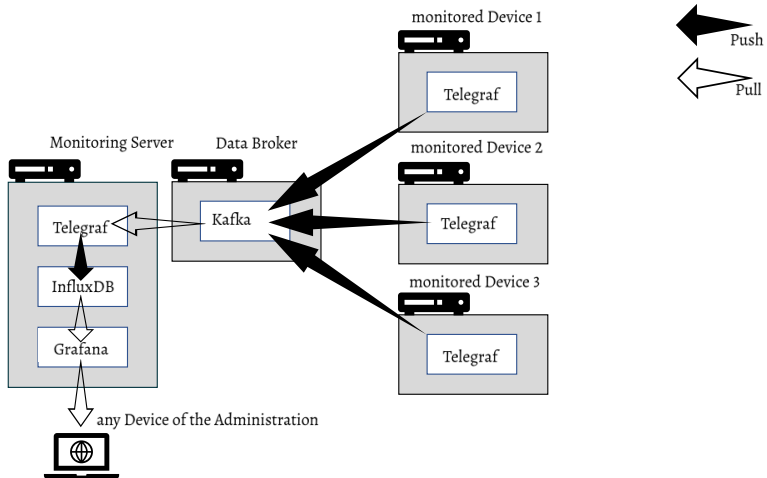












hosts

All

Row title

Load average



Disk usage



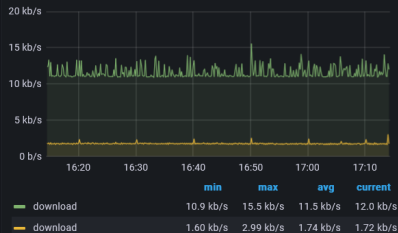
RAM



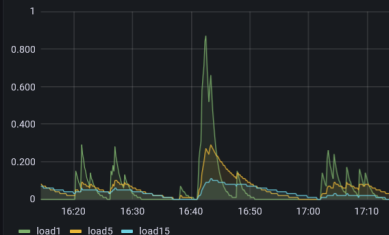
Uptime

5.0 day

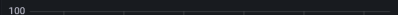
Network



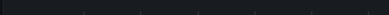
Load



CPU



RAM



Alerting

Alert rules and notifications

Alert rules

Contact points

Notification policies

Silences

Alert groups

Admin

Search by data source

All data sources

Search by label

Search

State

Firing

Normal

Pending

Rule type

Alert

Recording

View as

Groups

State

11 rules: 4 firing, 7 normal

+ New alert rule

Firing (4)

State	Name	Health	Group
> Firing for 8m	lab180215v001 – Device in VLAN dected	ok	lab180215v001
> Firing for 12m	lab180215v001 – HDD	ok	lab180215v001
> Firing for 4m	lab180215v001 – nmap	ok	lab180215v001
> Firing for 32s	lab180215v002 – device outage	ok	lab180215v001

> Pending (0)

> Normal (7)

