

Darktrace pilotua

Ibai Peña - Xabat Zabala - Aitor Zumelaga

GIDOIA

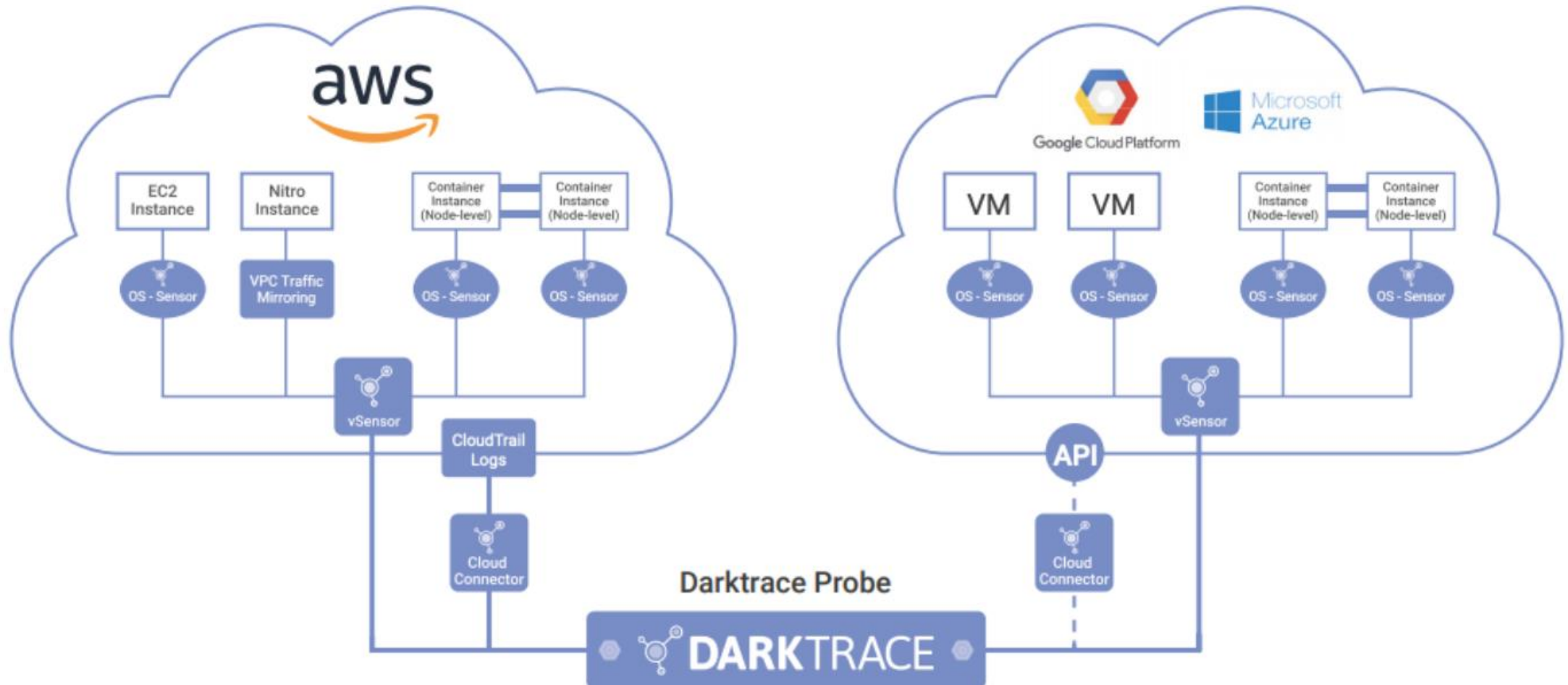
1. Sarrera
2. Arkitektura eta instalazioa
3. Jasotako emaitzak
4. Proba espezifikoak
5. Ondorioak

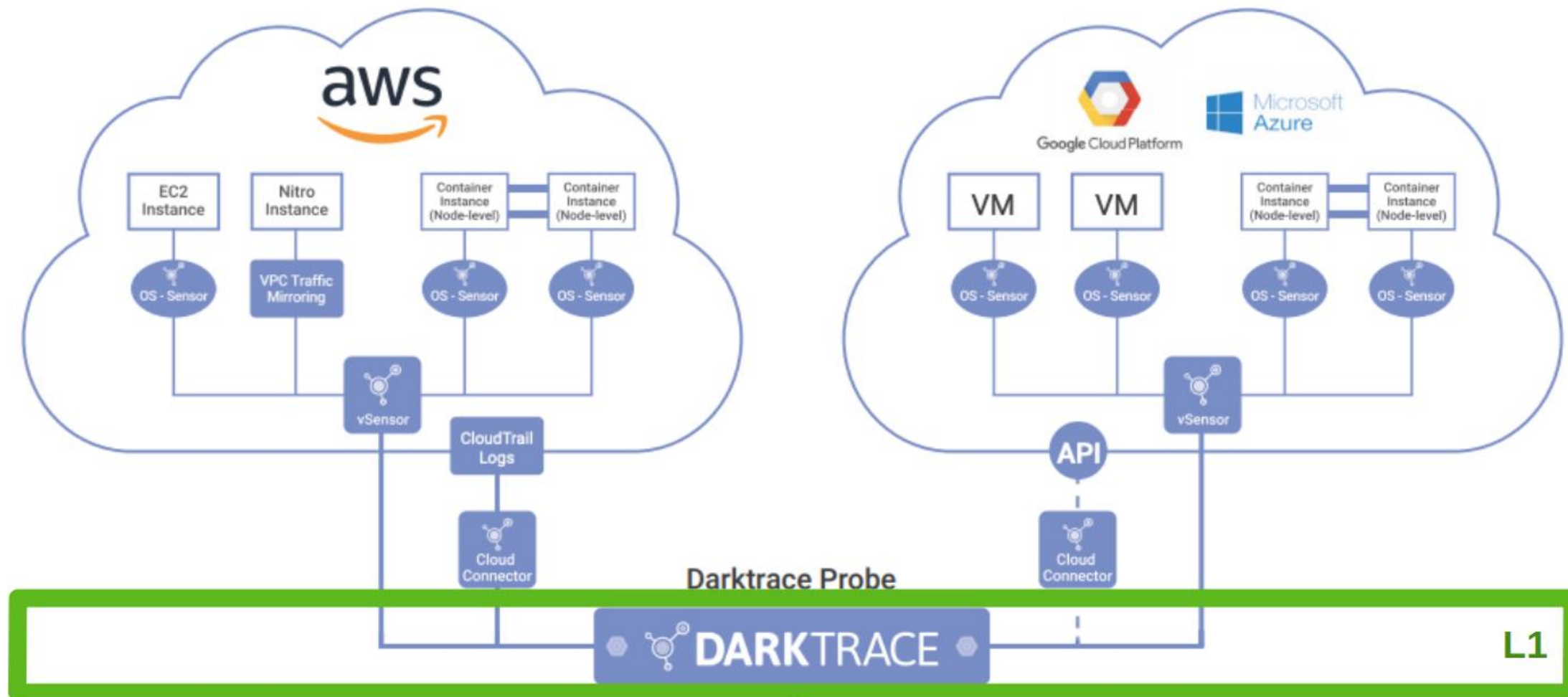
1- Sarrera

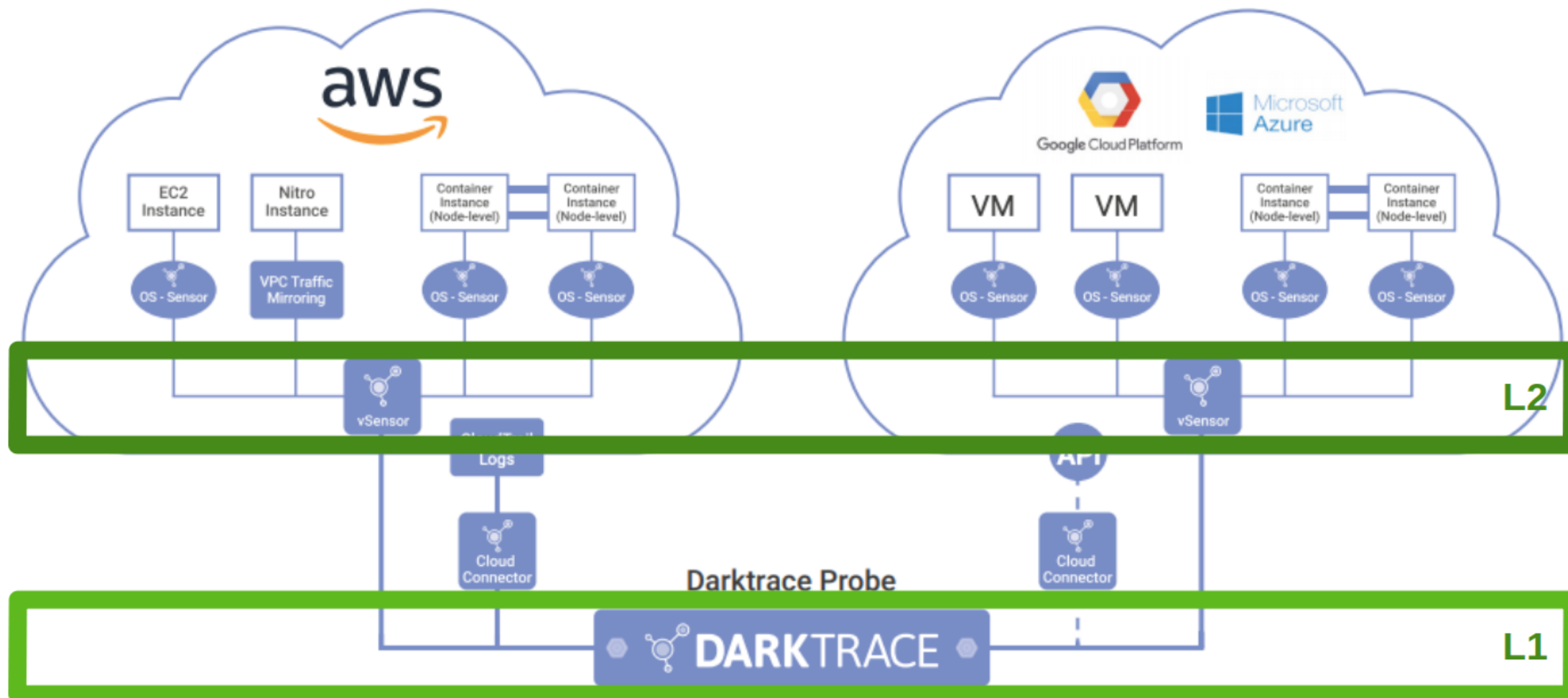
ZER DA DARKTRACE?

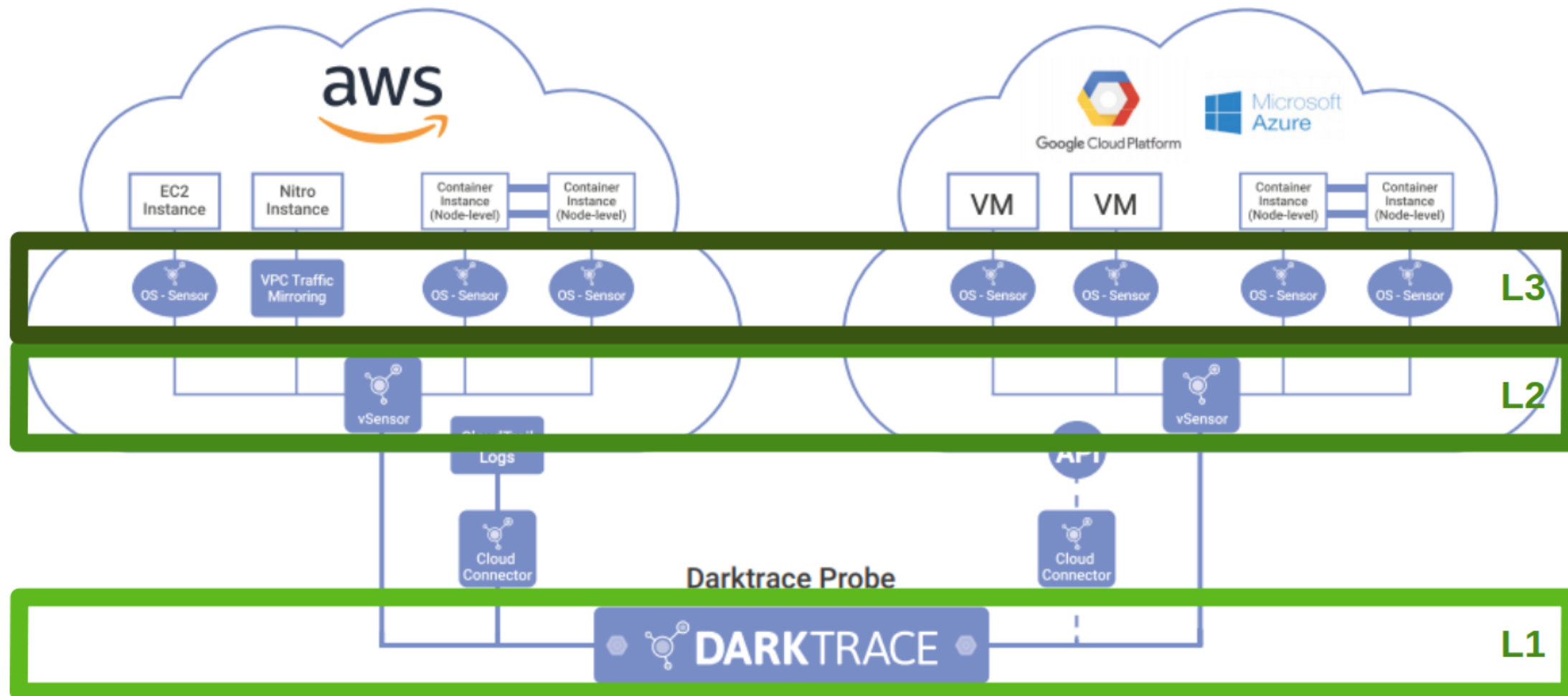
Adimen Arfifiziala erabiltzen duen SIEMa

Your Data + Our AI





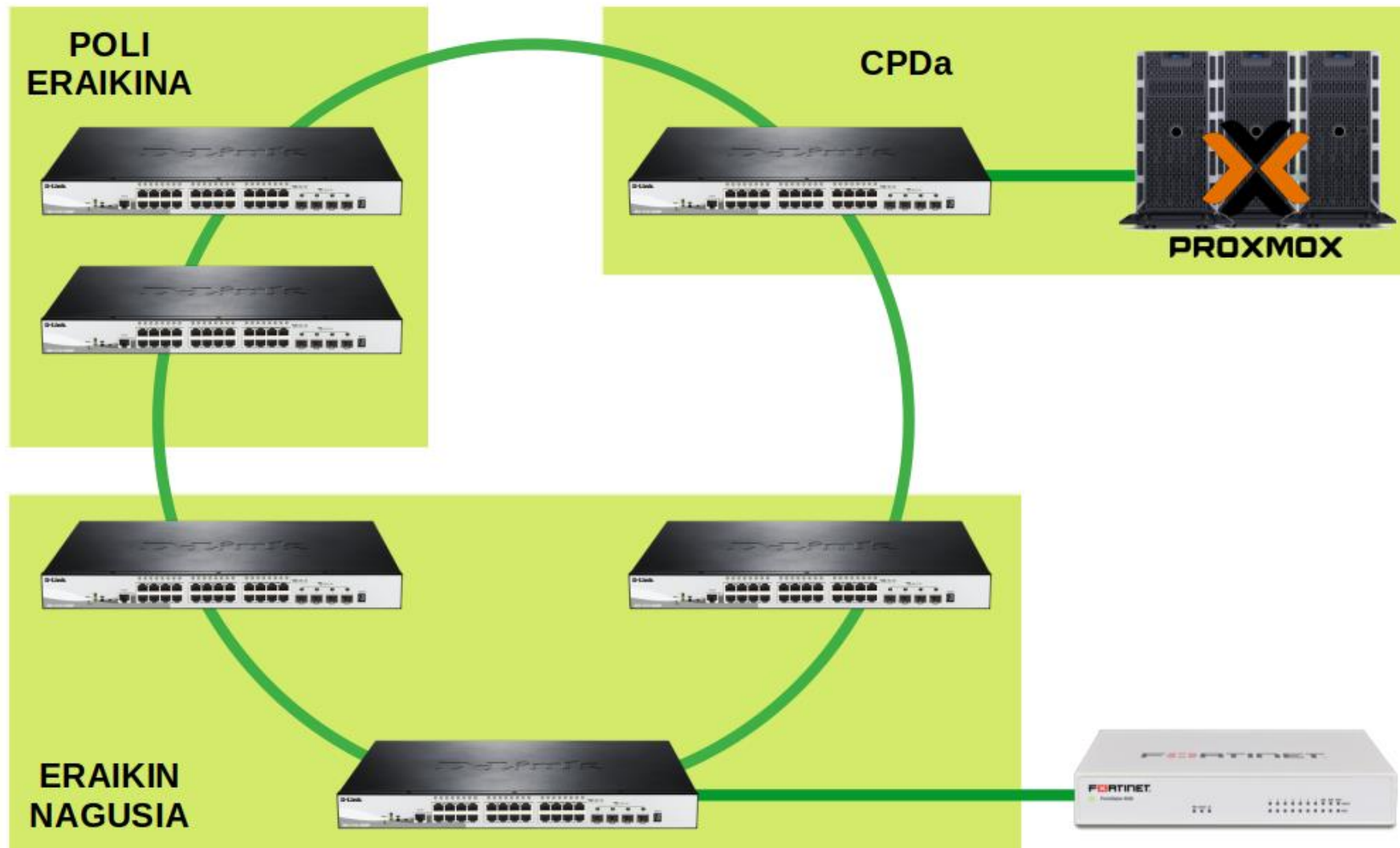


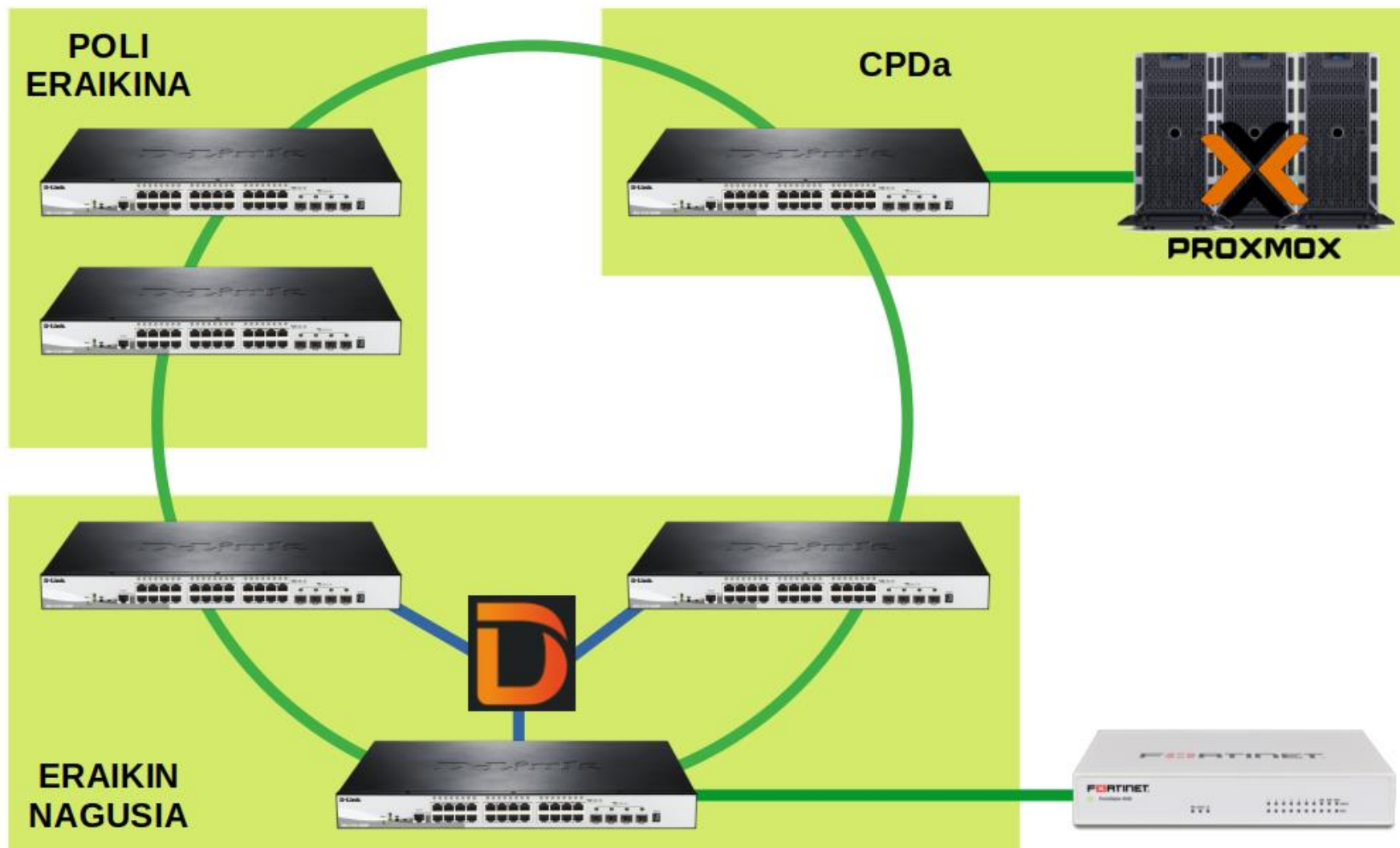


PILOTORAKO ESKAINI ZAIGUNA

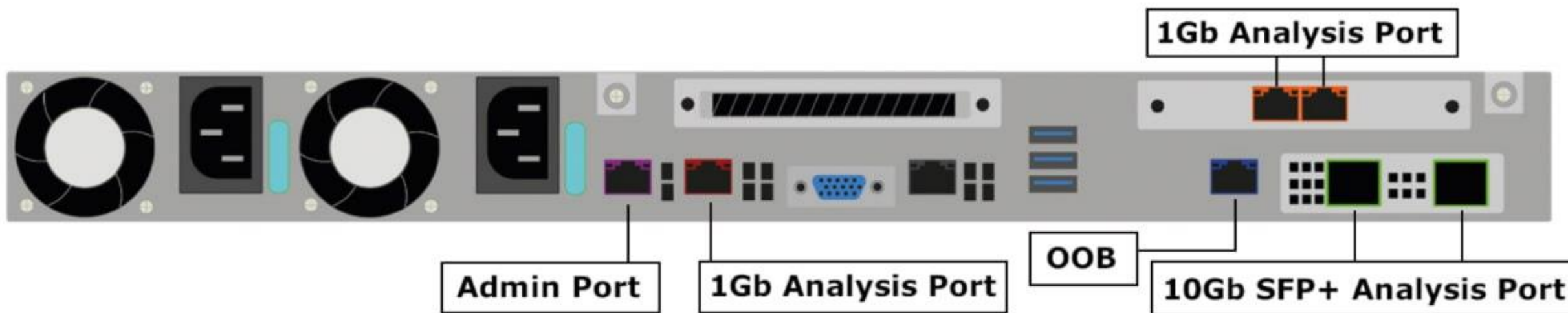
- **Appliance fisikoa ahaltsu bat**
- **Behar genuen lizentziamendua**
- **Bezeroen baliabideetara sarrera**
- **Teknikarien soportea**
- **Instalaziorako laguntza**
- **3 Jarraipen bilera (bilera bakoitzean 3 inzidentzia)**

2-Arkitektura eta instalazioa

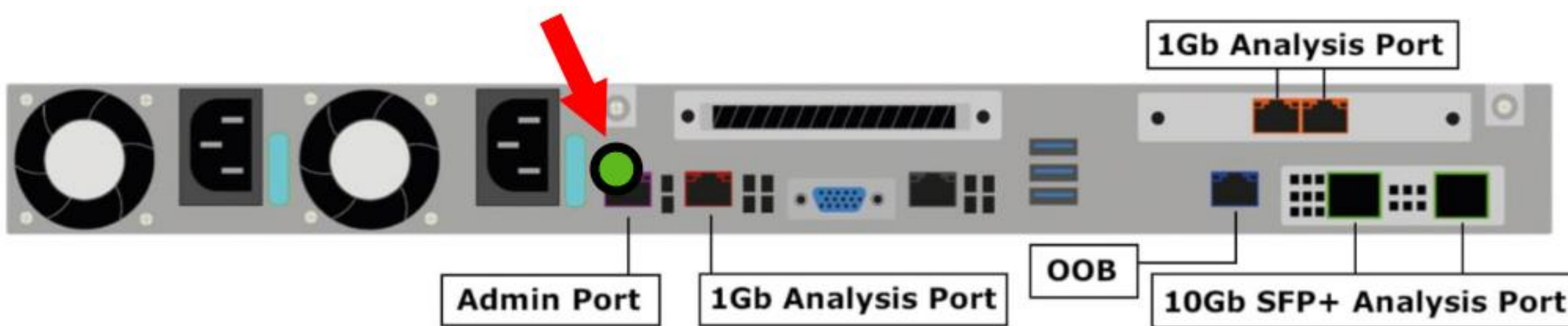




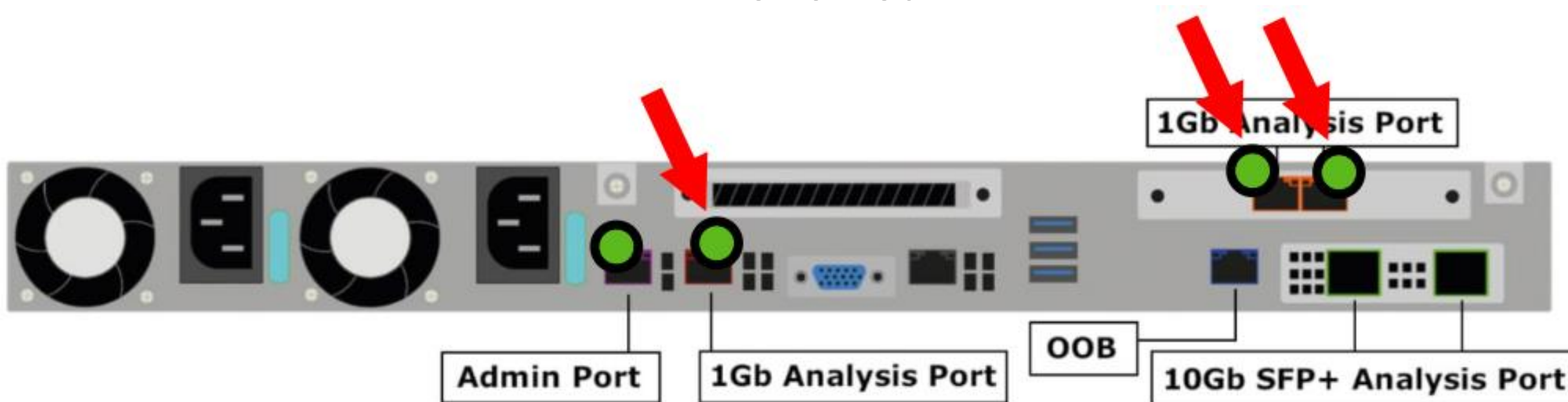
Konexioa



Konexioa



Konexioa



The screenshot shows the web management interface of a D-Link DGS-1510-28 switch. The top banner includes the D-Link logo and a physical switch image. The navigation bar contains links for Save, Tools, Wizard, Online Help, Surveillance Mode, and a language dropdown set to English. The left sidebar shows a tree view of the configuration menu, with 'Mirror Settings' selected under the 'Monitoring' section. The main content area is titled 'Mirror Settings' and contains the following fields:

- Mirror Settings**
 - Session Number: 1 (dropdown)
 - Destination: ☐ Port (dropdown)
 - Source: ☐ Port (dropdown)
- Mirror Session Table**
 - All Session (dropdown)
 - 1 (dropdown)

Mirror Settings

Mirror Settings

Session Number	<input type="text" value="2"/>						
Destination	<input checked="" type="checkbox"/> Port <input type="text" value="Port"/>	Unit	<input type="text" value="5"/>	Port	<input type="text" value="eth5/0/1"/>		
Source	<input checked="" type="checkbox"/> Port <input type="text" value="Port"/>	Unit	<input type="text" value="5"/>	From Port	<input type="text" value="eth5/0/2"/>	To Port	<input type="text" value="eth5/0/26"/>
						Frame Type	<input type="text" value="Both"/>

Add

Delete

Mirror Session Table

All Session

1

Find

Session Number	Session Type	
1	Local Session	Show Detail
2	Local Session	Show Detail

Mirror Settings

Mirror Settings

Session Number: 2

Destination: ☒ Port ☐ Unit: 5 Port: eth5/0/1

Source: ☒ Port ☐ Unit: 5 From Port: eth5/0/2 To Port: eth5/0/26 Frame Type: Both

Add

Delete

sw1.uni.lan

ERROR: The hardware resource is insufficient.

OK

Mirror Session Table

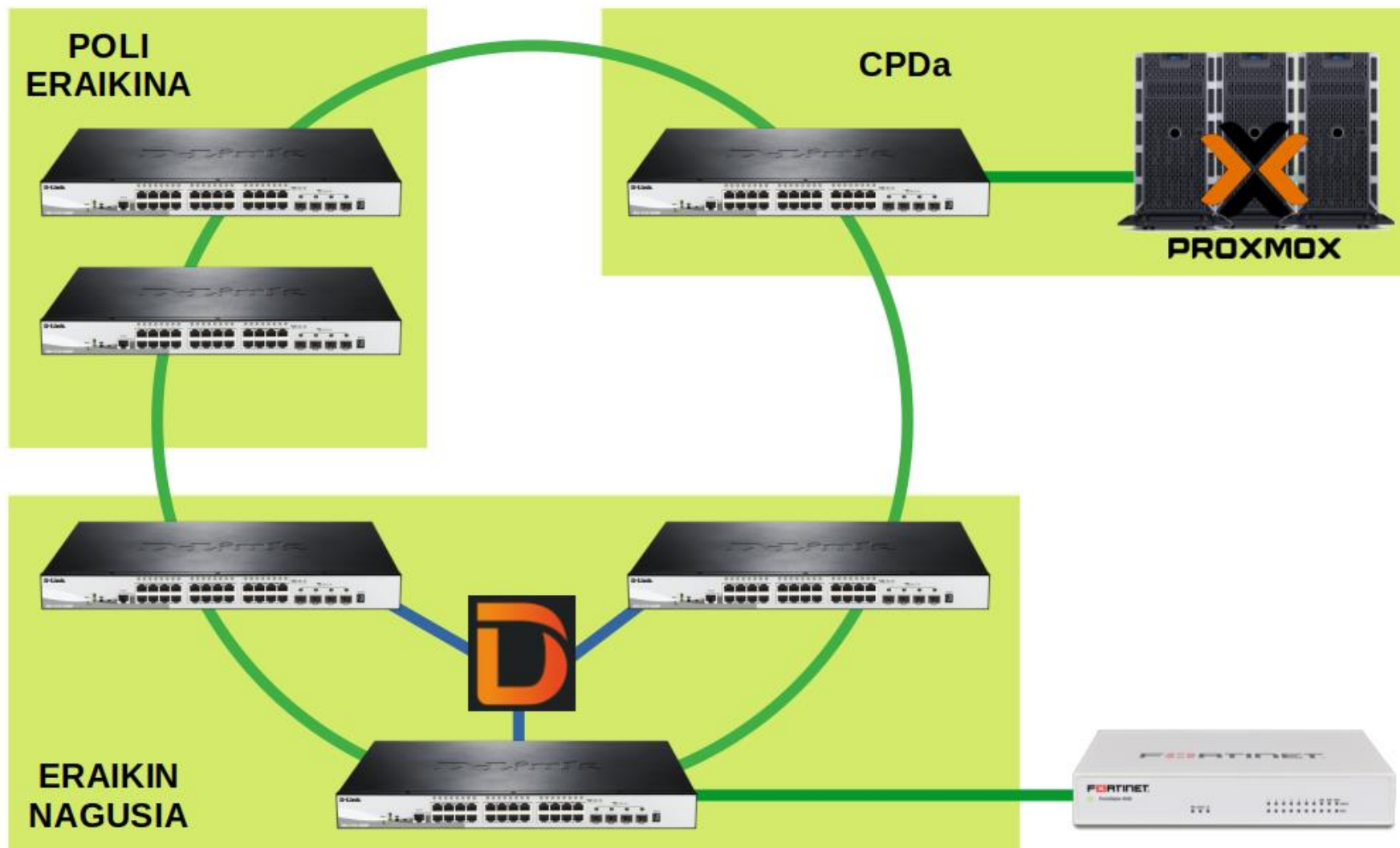
All Session

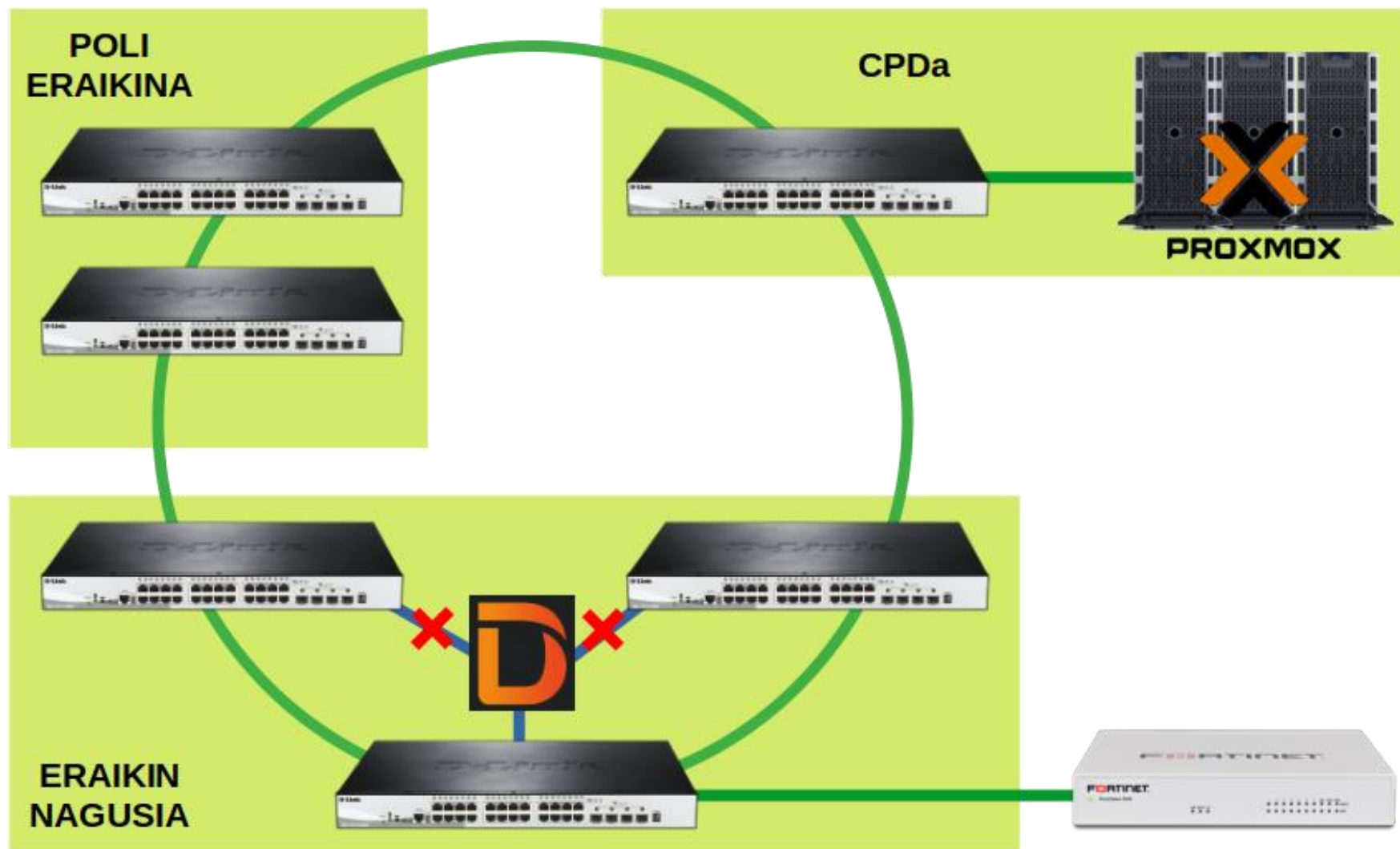
1

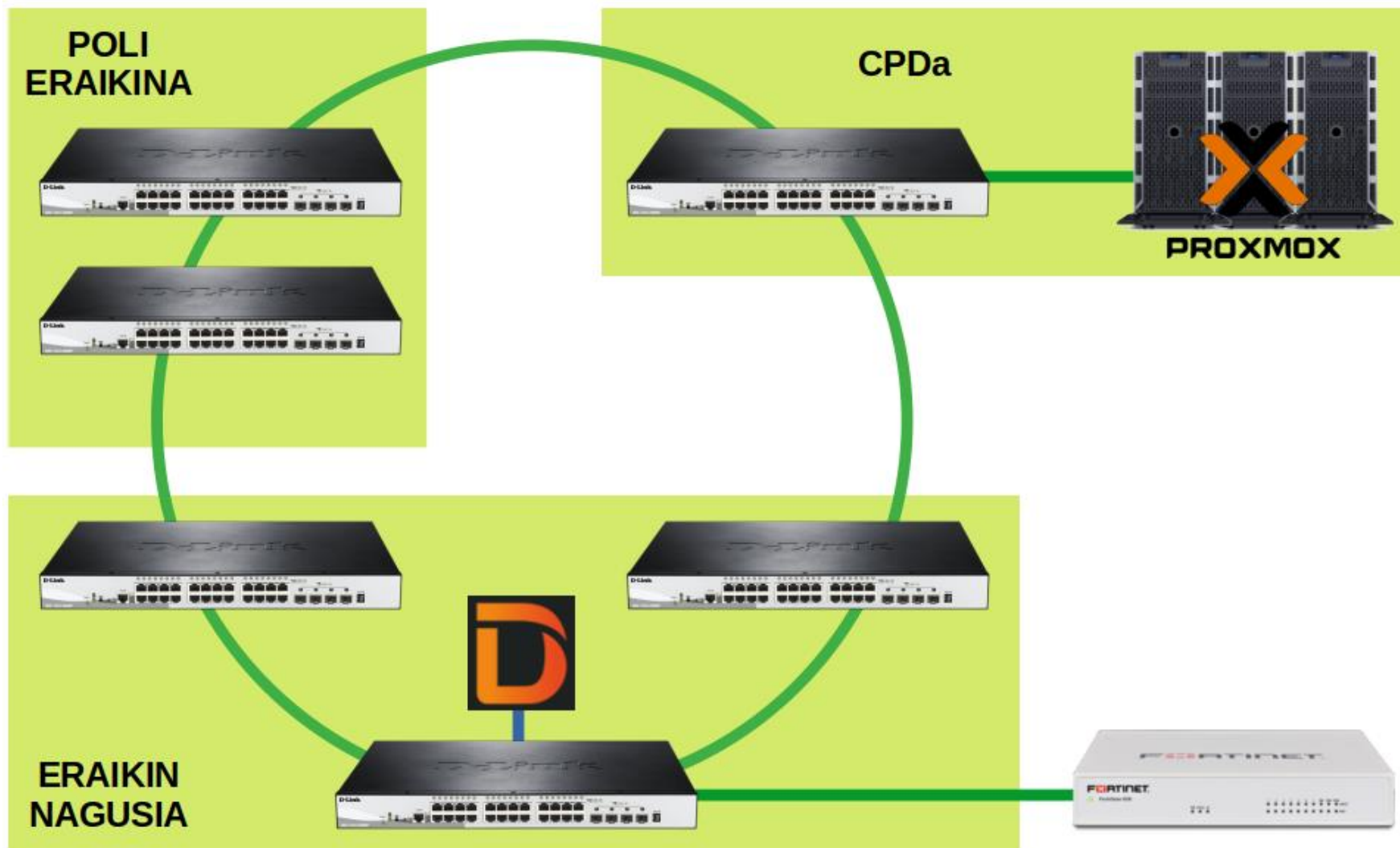
Find

Session Number	Session Name	Session Type	Session Status
1	Local Session	Local Session	Show Detail

1
Local Session
eth1/0/1-eth1/0/26,eth2/0/1-eth2/0/26,eth3/0/1-eth...
eth1/0/1-eth1/0/26,eth2/0/1-eth2/0/26,eth3/0/1-eth 3/0/26,eth6/0/1-eth6/0/26
Ethernet2/0/7

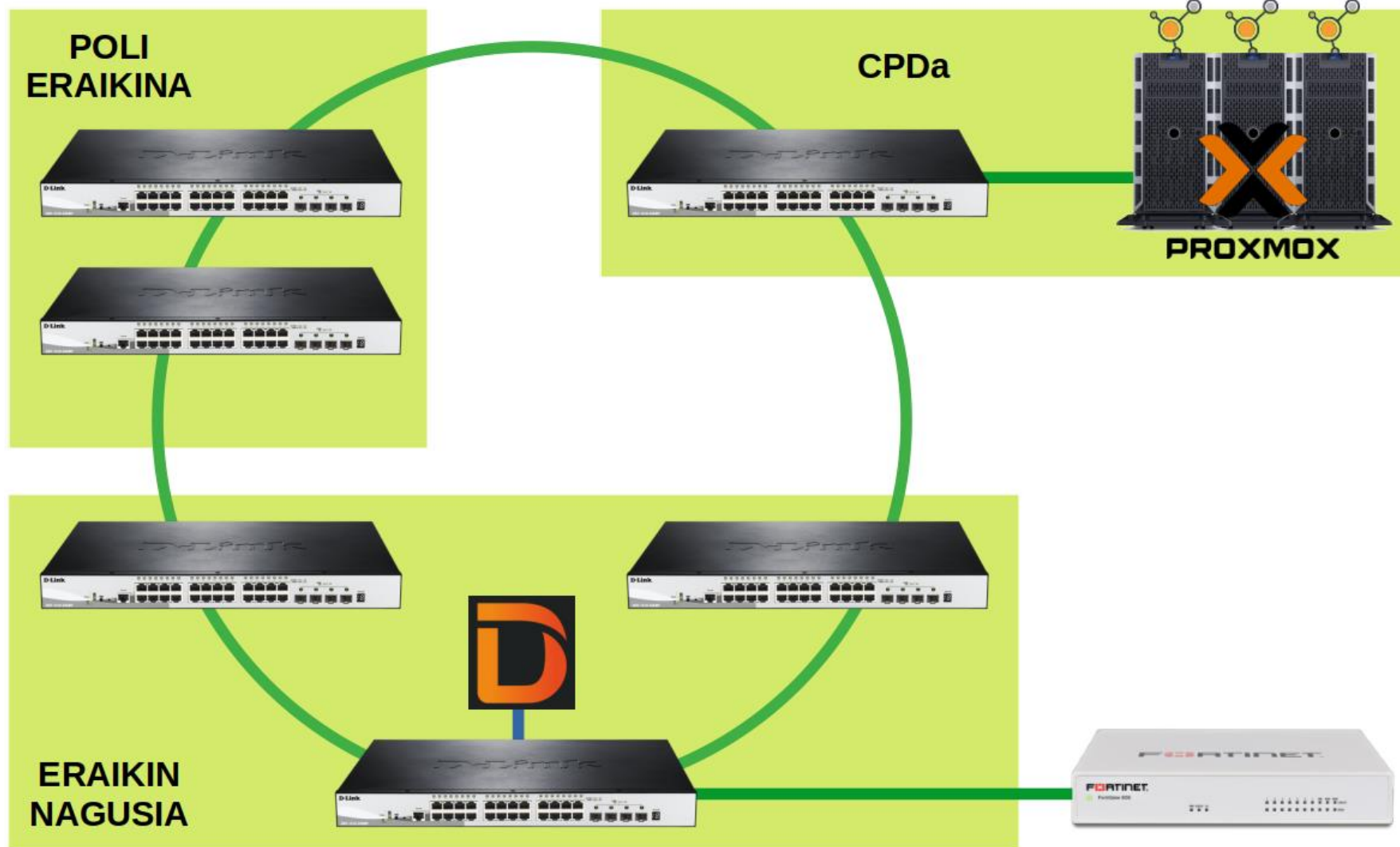






vSensor

- Makina birtual batean instalatzen da
- Montatuta datorren ova bat erabili daiteke edo Ubuntu bat montatu eta instalazioa egin
 - Guk Ubuntu+Instalazioa
- Behar den leku guztietan jarri daitezke
 - Guk Proxmoxeko nodo bakoitzean 1
- Informazioa jaso eta gailu nagusira bidaltzen dute
 - Bai sarekoa eta bai beste osSentsoreek bidaltzen diotena

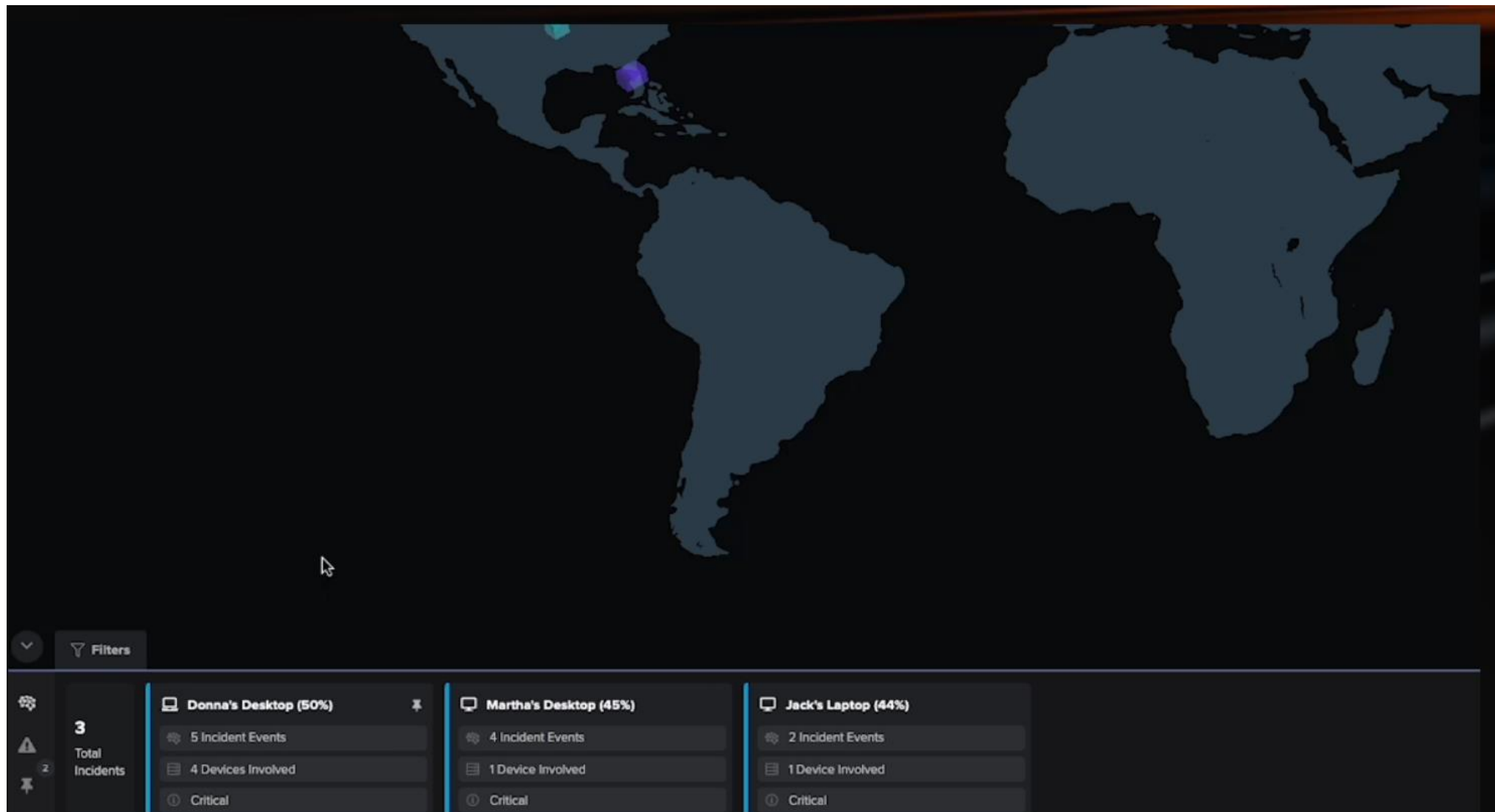


osSensor

- Lehendik dagoen zerbitzari batean ezartzen da honen informazioa jasotzeko
- Agente moduan funtzionatzen duen software instalagarria da
- Informazioa jaso eta vSensor-etara bidaltzen da
- Guk 6 ezarri genituen: 2 windows zerbitzarietan eta 4 linux zerbitzarietan

3- Jasotako emaitzak

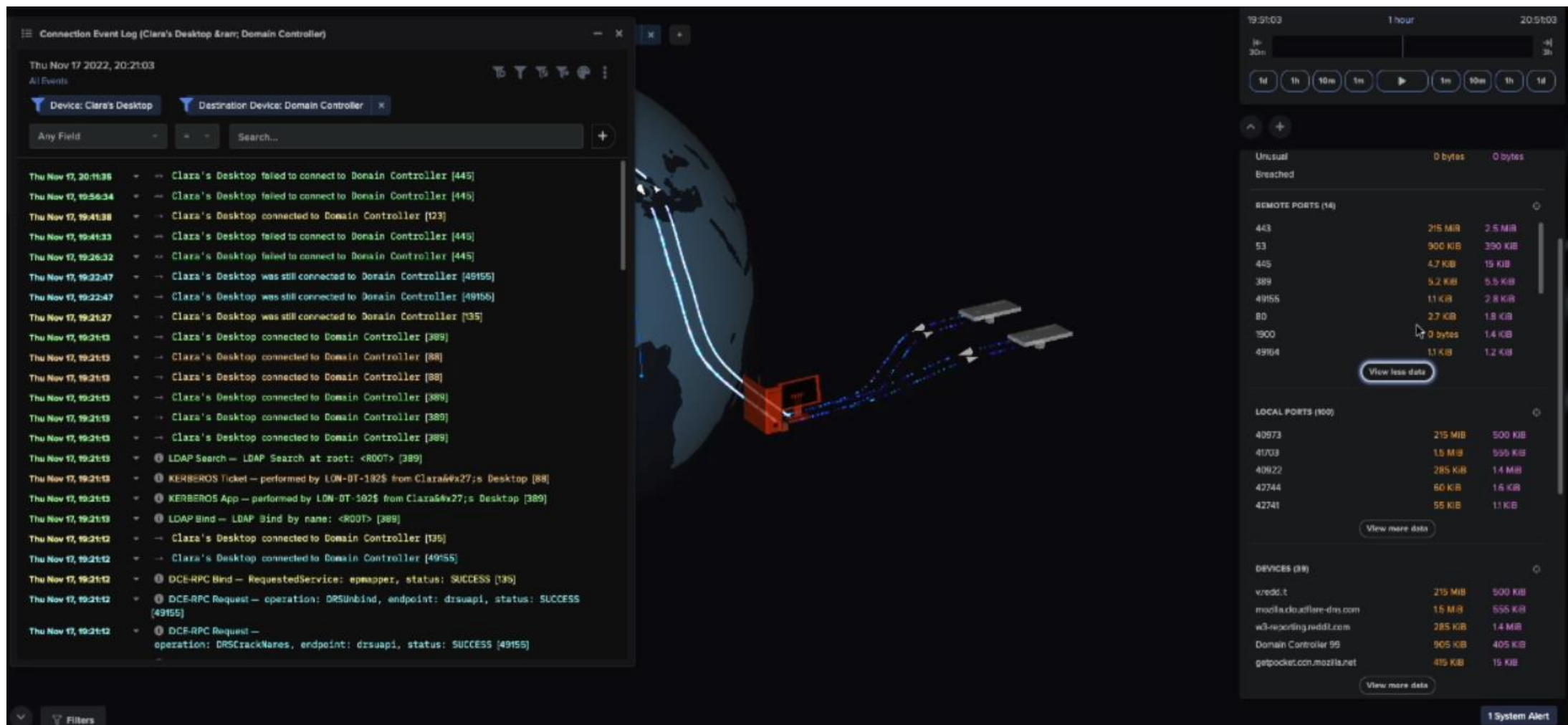




Txostenak

- [BitTorrent](#)
- [VPN](#)
- [Cryptocurrency Mining Activity](#)

Gertatutakoaren Jarraipena



4- Proba espezifikokoak

Portu Eskaneoa atzeman du.

Suspicious AI Analyst Incident

Beginning on Monday 27th March 11:57 CEST, the device 192.168.67.100 exhibited the following event worthy of investigation

Mon 27th 11:00 Mon 27th 11:15 Mon 27th 11:30 Mon 27th 11:45 Mon 27th 12:00 Mon 27th 12:15 Mon 27th 12:30 Mon 27th 12:45 Mon 27th 13:00

Port Scanning

Port Scanning

SUMMARY

The device **192.168.67.100** was observed making an unusually large number of internal connection attempts to 192.168.67.254, suggesting scanning activity.

Network scanning can be used during reconnaissance to gather information about internal devices, such as their list of open ports, and is thus a possible indicator of preparation for malicious or unauthorised internal activity.

If the activity from the device was not expected, it is recommended that the security team investigate it further to determine whether it was part of legitimate network activity.

Discovery Reconnaissance

RELATED MODEL BREACHES

ACTIONS

✓ Acknowledge this Incident Event

OVERVIEW OF SCAN

Time	27th Mar 2023 11:57:43 - 12:11:41 CEST
Source Device	192.168.67.100 Antigena All High Risk New Device
Scanned IP	192.168.67.254

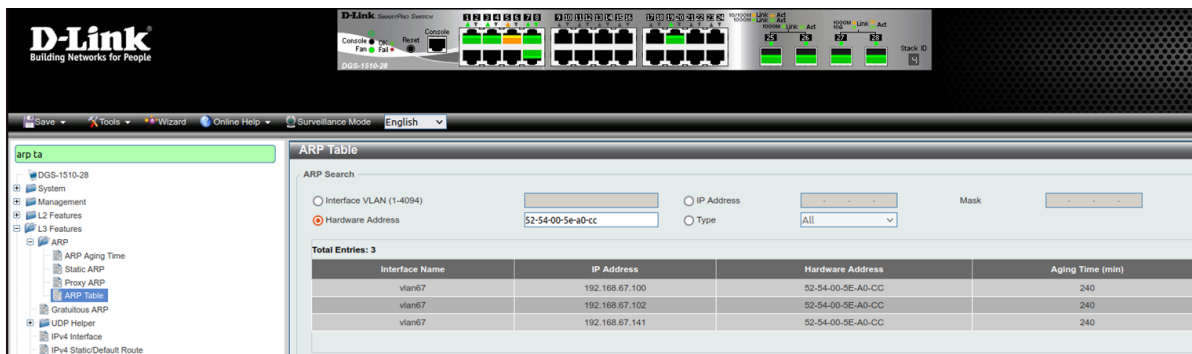
Man in the middle ez du atzeman

Kaliak 192.168.67.141 IP-a dauka, eta beste ekipoa gelatik kanpo dago. Beraz, DarkTrace ikuskatzen ari den portuetatik pasa beharko luke erasoak.

ARP Spoofing bitartez 2 ekipo suplantatu dira:

1. 192.168.67.100 (Ubuntu desktop bat)
2. 192.168.67.102 (Gelan dagoen Router bat)
3. 192.168.67.254 (Switch gelakoa)

```
uni@server:~$ arp -a
? (192.168.67.141) at 52:54:00:5e:a0:cc [ether] on ens3
_gateway (192.168.67.254) at 10:62:eb:d2:15:e0 [ether] on ens3
uni@server:~$ arp -a
? (192.168.67.141) at 52:54:00:5e:a0:cc [ether] on ens3
? (192.168.67.254) at 52:54:00:5e:a0:cc [ether] on ens3
uni@server:~$
```



D-Link Building Networks for People

arp ta

ARP Search

☐ Interface VLAN (1-4094) ☐ IP Address ☐ Hardware Address ☐ Type

Mask

Total Entries: 3

Interface Name	IP Address	Hardware Address	Aging Time (min)
vlan67	192.168.67.100	52-54-00-5E-A0-CC	240
vlan67	192.168.67.102	52-54-00-5E-A0-CC	240
vlan67	192.168.67.141	52-54-00-5E-A0-CC	240

UDP flooding ez du atzeman

```
ibai@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
Sent 268966 amount of packets to 10.15.27.2 at port 23232.
Sent 268967 amount of packets to 10.15.27.2 at port 23232.
Sent 268968 amount of packets to 10.15.27.2 at port 23232.
Sent 268969 amount of packets to 10.15.27.2 at port 23232.
Sent 268970 amount of packets to 10.15.27.2 at port 23232.
Sent 268971 amount of packets to 10.15.27.2 at port 23232.
Sent 268972 amount of packets to 10.15.27.2 at port 23232.
Sent 268973 amount of packets to 10.15.27.2 at port 23232.
Sent 268974 amount of packets to 10.15.27.2 at port 23232.
Sent 268975 amount of packets to 10.15.27.2 at port 23232.
Sent 268976 amount of packets to 10.15.27.2 at port 23232.
Sent 268977 amount of packets to 10.15.27.2 at port 23232.
Sent 268978 amount of packets to 10.15.27.2 at port 23232.
Sent 268979 amount of packets to 10.15.27.2 at port 23232.
Sent 268980 amount of packets to 10.15.27.2 at port 23232.
Sent 268981 amount of packets to 10.15.27.2 at port 23232.
Sent 268982 amount of packets to 10.15.27.2 at port 23232.
Sent 268983 amount of packets to 10.15.27.2 at port 23232.
Sent 268984 amount of packets to 10.15.27.2 at port 23232.
Sent 268985 amount of packets to 10.15.27.2 at port 23232.
Traceback (most recent call last):
  File "udp.py", line 10, in <module>
    print "Sent %s amount of packets to %s at port %s." % (sent,ip,port)
KeyboardInterrupt
```

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas: Captura de pantalla tomada

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2966...	3816.2487472...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2487669...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2487861...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2488752...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2488927...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2489908...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2490115...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2491123...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2491308...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2492272...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2492489...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2493363...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2493556...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024
2966...	3816.2493693...	192.168.67.141	10.15.27.2	UDP	1066	41456 → 23232 Len=1024

▶ Frame 77456: 1066 bytes on wire (8528 bits), 1066 bytes captured (8528 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: RealtekU_5e:a0:cc (52:54:00:5e:a0:cc), Dst: D-LinkIn_d2:15:e0 (10:62:eb:d2:15:e0)
 ▶ Internet Protocol Version 4, Src: 192.168.67.141, Dst: 10.15.27.2
 ▶ User Datagram Protocol, Src Port: 41456, Dst Port: 23232
 ▶ Data (1024 bytes)

5- Ondoriak

- **Tresna oso potentea (agian informazio gehiegi)**
- **Erabilera ez oso intuitiboa**
- **Hasieran ikasketa handia eskatzen du**
- **Gure sarean mugitzen den trafikoa ezagutzen lagundu.**
- **Suhezian erregela batzuk jarrita ia abisu denak desagertu.**
- **Ohiko ziber eraso batzuk ez ditu detektatu**
- **Zapore Gazi-Goxoa.**

HARREMANETARAKO INFORMAZIOA

Ibai Peña

ipena@tnika.eus

Xabat Zabala

xzabala@uni.eus

Aitor Zumelaga

azumelaga@uni.eus