



Inhoudstafel

- H1 Inleiding
- H2 Netwerkontwerp
- H3 Ontwerp & hardware
- H4 Netwerkimplementatie
- H5 Firewall & Security
- H6 WiFi
- H7 Camerasurveillance
- H8 POS
- H9 Testing
- H10 UniFi Access
- H11 Monitoring & Logging
- H12 Theoretisch kader
- H13 Kostenprijs
- H14 Conclusie
- H15 Bronnen
- H16 Dankwoord

H1 - INLEIDING

1.1 Aanleiding & motivatie

Voor mijn eindwerk binnen de opleiding Netwerk- en Systeembeheer koos ik ervoor om een volledige IT-infrastructuur uit te werken voor een fictieve moderne nightclub: The Solus Club.

Ik koos dit onderwerp omdat een nightclub veel verschillende netwerksystemen combineert: WiFi voor bezoekers en personeel, camerabeveiliging, kassasystemen, monitoring, firewalling en centrale netwerkcontrole. Daardoor is dit een geschikte omgeving om netwerkbeheer, security en systeembeheer samen te brengen in één realistisch project.

Het doel is om niet enkel een theoretisch ontwerp te maken, maar een professionele infrastructuur uit te werken die logisch, veilig, schaalbaar en centraal beheerbaar is.

1.2 Projectomschrijving

De infrastructuur wordt opgebouwd rond het UniFi-ecosysteem van Ubiquiti. Hierbij worden routers, switches, access points en camera's centraal beheerd. Door gebruik te maken van VLANs, firewallregels en gescheiden netwerken worden bezoekers, personeel, camera's en kassasystemen logisch van elkaar gescheiden.

Dit project toont hoe een moderne hospitality-omgeving veilig en overzichtelijk ingericht kan worden volgens principes uit netwerkbeheer en systeembeheer.

De nightclub maakt gebruik van een centraal beheerd netwerk waarin gasten, personeel, camera's en kassasystemen van elkaar gescheiden worden voor betere veiligheid en prestaties.

1.3 Probleemstelling

SITUATIE & PROBLEEMSTELLING

Een moderne nightclub maakt gebruik van veel verschillende netwerktoestellen en systemen. Binnen The Solus Club moeten onder andere WiFi, camera-beveiliging, kassasystemen, monitoring en management veilig en stabiel samenwerken.

Zonder correcte netwerksegmentatie kunnen bezoekers toegang krijgen tot gevoelige systemen zoals camera's of kassasystemen. Daarnaast moet het netwerk stabiel blijven tijdens drukke evenementen met veel gelijktijdige gebruikers.

Het doel van dit project is het ontwerpen van een veilige, professionele en centraal beheerde IT-infrastructuur voor een moderne nightclubomgeving.

1.4 Doelstellingen

De belangrijkste doelstelling van dit eindwerk is het ontwerpen van een professionele netwerk- en security-infrastructuur voor The Solus Club.

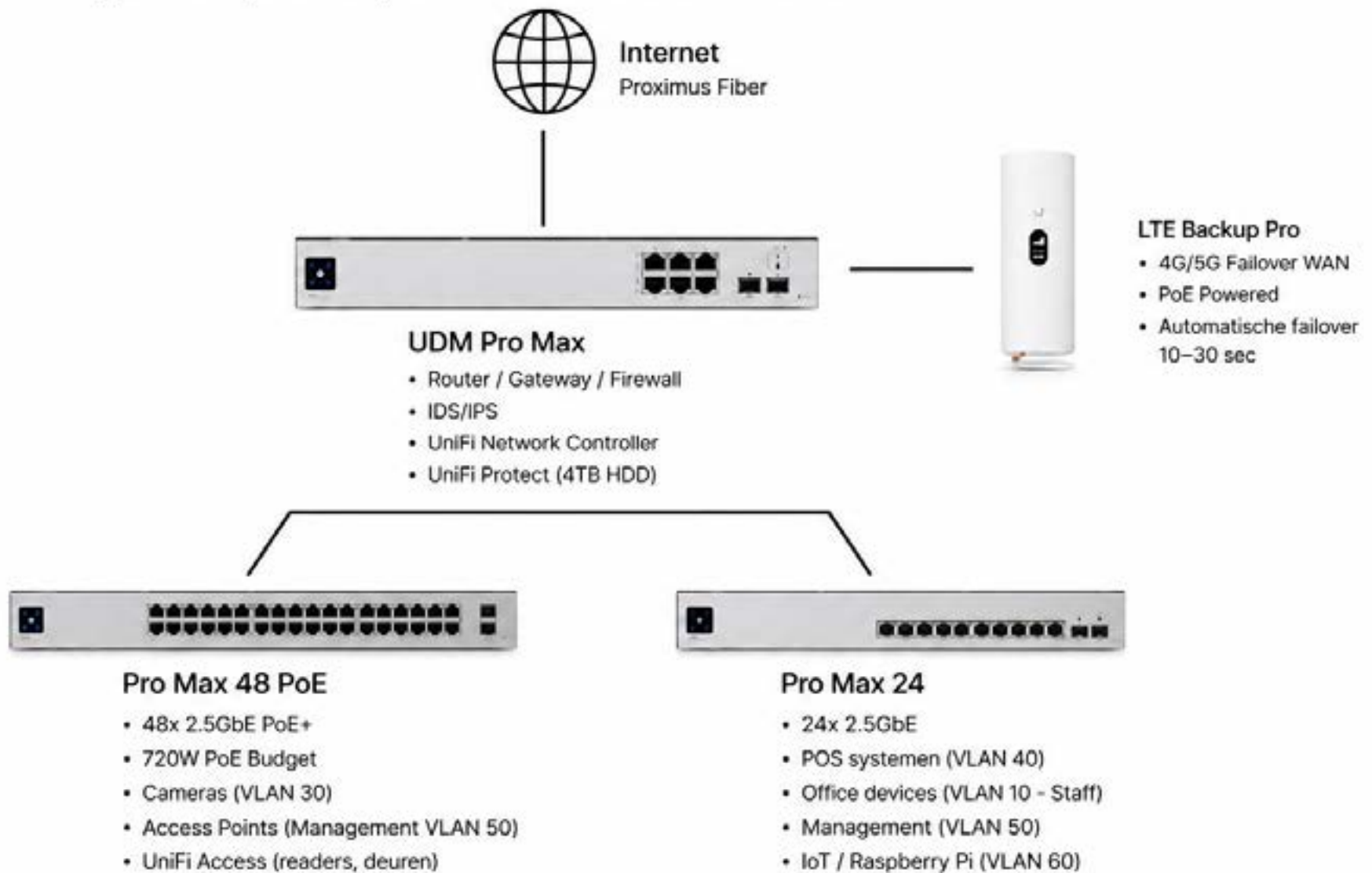
De concrete doelstellingen zijn:

- een centraal beheerd UniFi-netwerk ontwerpen;
- VLANs gebruiken om netwerksegmenten te scheiden;
- aparte netwerken voorzien voor management, personeel, gasten, camera's, POS en IoT;
- veilige WiFi voorzien voor personeel en bezoekers;
- firewallregels toepassen om ongewenste toegang te blokkeren;
- camerabeveiliging voorzien via UniFi Protect;
- POS- en kassasystemen afschermen van andere netwerken;
- monitoring en logging voorzien;
- redundantie voorzien via LTE backup en UPS;
- testing en validatie uitvoeren.

H2 - Netwerkontwerp

Network Topology

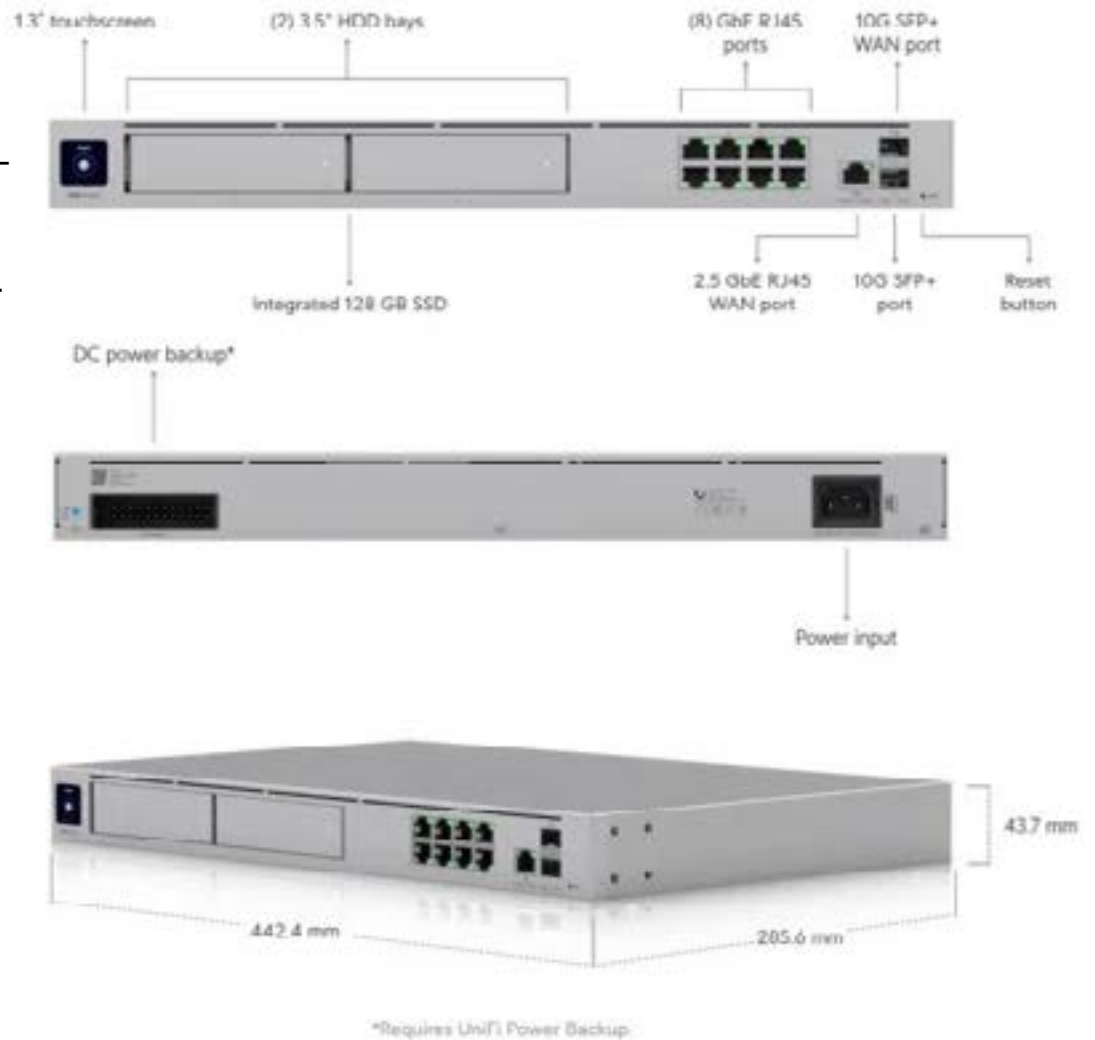
De UniFi Dream Machine Pro Max vormt het centrale netwerkpunt binnen The Solus Club en verzorgt routing, firewalling, VLAN-segmentatie, IDS/IPS, UniFi Network en UniFi Protect.



UniFi Dream Machine Pro Max

- Centrale router, firewall en UniFi controller
- Verzorgt routing tussen VLANs en netwerkbeheer
- Integreert IDS/IPS, VPN en beveiligingsregels
- Centraal beheer van switches, access points en camera's

De UniFi Dream Machine Pro Max wordt gebruikt als core router binnen The Solus Club en vormt het centrale netwerkpunt van de infrastructuur. Het toestel verzorgt routing tussen VLANs, firewalling, IDS/IPS beveiliging en centraal beheer van UniFi-apparatuur zoals switches, access points en camera's. Dankzij de 10G uplinks en geïntegreerde controller biedt de UDM Pro Max voldoende prestaties, schaalbaarheid en centraal beheer voor een moderne nachtclubomgeving.



10G Uplinks & Backbone

Backbone gebruikt 10G SFP+ DAC uplinks tussen UDM Pro Max en switches
Ondersteunt hoge bandbreedte voor camera's, backups en centrale opslag
Vermindert congestie bij piekmomenten in de nightclub
Laat toekomstige uitbreiding toe zonder bottlenecks
VLANs beperken broadcastverkeer en verbeteren prestaties
Problemen blijven geïsoleerd binnen hun eigen netwerksegment

Waarom netwerksegmentatie?

- Guest-netwerken mogen nooit toegang krijgen tot POS-systemen, camera's of managementtoestellen
- POS-systemen blijven gescheiden voor betere veiligheid en betrouwbaarheid
- Camera's worden ondergebracht binnen VLAN 30 Cameras om cameraverkeer te isoleren
- IoT-apparatuur en Raspberry Pi-systemen bevinden zich binnen VLAN 60 IoT
- Firewallregels bepalen welke communicatie tussen VLANs toegelaten of geblokkeerd wordt
- Segmentatie vermindert broadcastverkeer en verhoogt veiligheid en beheerbaarheid

H3 - Ontwerp & hardware

Floorplan

The Solus Club heeft een totale oppervlakte van 40 bij 60 meter. Het gebouw is opgedeeld in duidelijke functionele zones, elk met specifieke netwerkvereisten.

De belangrijkste zones zijn: ingang en ticketcontrole, vestiaire, barzone, dansvloer, VIP-lounge, podium, backstage, kantoorruimte, stockruimte en de technische ruimte waar het centrale rack zich bevindt.

Elke zone maakt gebruik van specifieke netwerkkapparaten zoals access points, camera's, POS-terminals en managed switches. Hierdoor kan het netwerk centraal beheerd en per zone gecontroleerd worden.



PLATTEGROND & ZONES

The Solus Club werd opgedeeld in verschillende netwerk- en beveiligingszones om een stabiele en veilige infrastructuur te creëren.

Belangrijke zones binnen de nightclub:

Ingang & ticketcontrole

Vestiaire & lockers

Barzone

Dansvloer

DJ booth

Backstage

Technische ruimte

Kantoorruimte

Elke zone maakt gebruik van specifieke netwerktoestellen zoals access points, camera's, kassasystemen en managed switches. Hierdoor kan het netwerk centraal beheerd en gecontroleerd worden.

3.2 Overzicht van de volledige infrastructuur

De infrastructuur van The Solus Club is opgebouwd rond één centraal rack in de technische ruimte.

Triton RMA 18U Rackkast

- Ubiquiti UACC-Rack-Panel-Brush-1U
- 48-Port Cat6 Patch Panel
- UniFi Dream Machine Pro Max
- Seagate SkyHawk 4TB HDD
- UniFi Switch Pro Max 48 PoE
- UniFi Switch Pro Max 24
- Digitus DN-95403 Rack PDU
- APC Smart-UPS SMT1500RMI2UC
- UniFi LTE Backup Pro
- Vrije ruimte / airflow



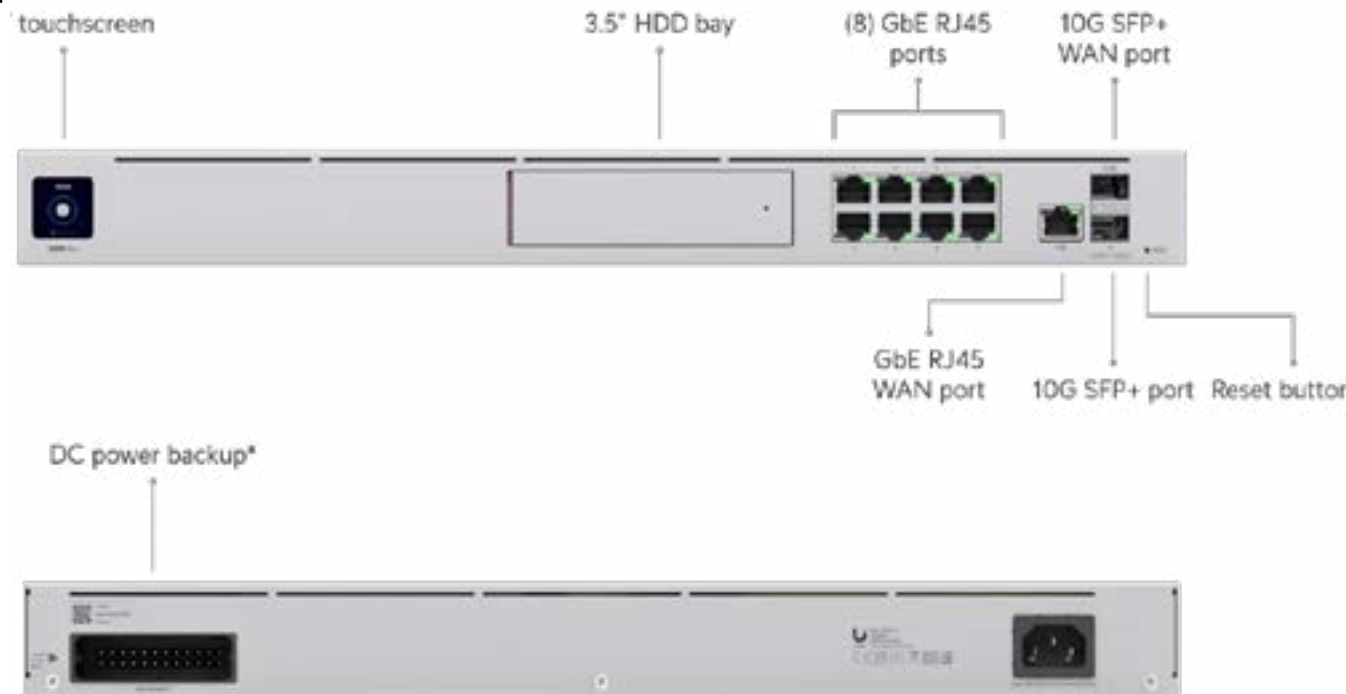
3.3 Hardwarecomponenten & technische specificaties

3.3.1 UniFi Dream Machine Pro Max

Prijs: €550-600

Waarom?

- Centrale router, firewall en controller
- IDS/IPS inspecteert verkeer op bedreigingen
- Ondersteunt UniFi Network, Protect en Access
- 10G uplinks verminderen bottlenecks
- Ondersteunt centrale VLAN-segmentatie
- IDS/IPS throughput ± 5 Gbps



De UDM Pro Max beschikt over een quad-core ARM Cortex-A57 processor op 2,0 GHz, 8 GB DDR4 werkgeheugen, 8 GbE RJ45-poorten, een 10G SFP+ WAN-poort en twee 3,5-inch NVR HDD-bays. De IDS/IPS-doorvoer bedraagt ± 5 Gbps. De richtprijs bedraagt ongeveer €684 inclusief btw.

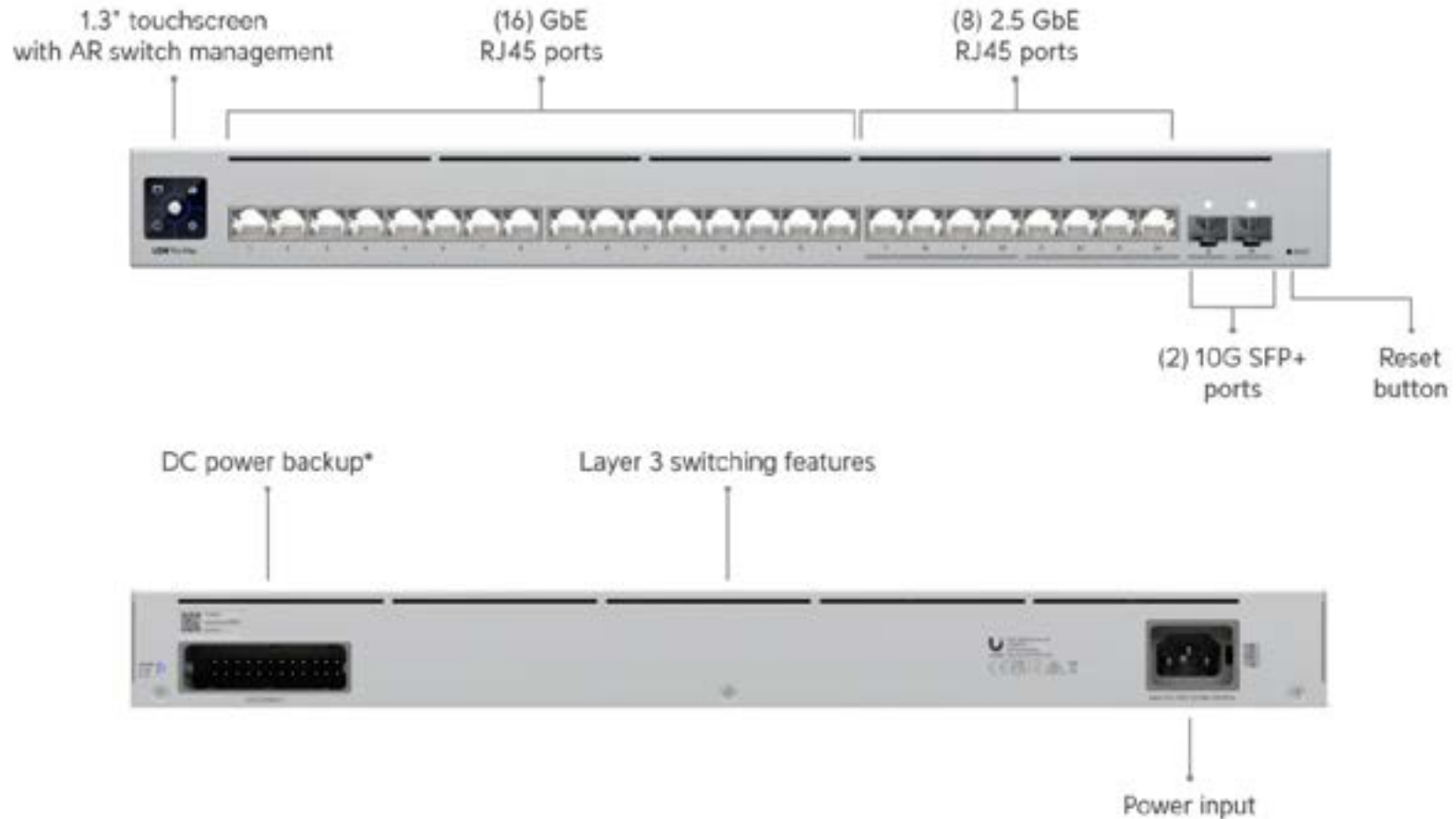
3.3 Hardwarecomponenten & technische specificaties

3.3.2 UniFi Switch Pro Max 24

Prijs: €400-500 euro

Waarom?

Verbindt vaste netwerkkapparatuur zoals POS, office en managementtoestellen en ondersteunt VLAN-segmentatie.



De UniFi Switch Pro Max 24 verbindt vaste netwerkkapparaten zoals POS-terminals, werkstations en managementtoestellen. Dit toestel beschikt over 16 GbE RJ45-poorten, 8 poorten van 2,5 GbE en twee 10G SFP+-uplinks voor de verbinding met de UDM Pro Max. De richtprijs bedraagt €400 tot €500.

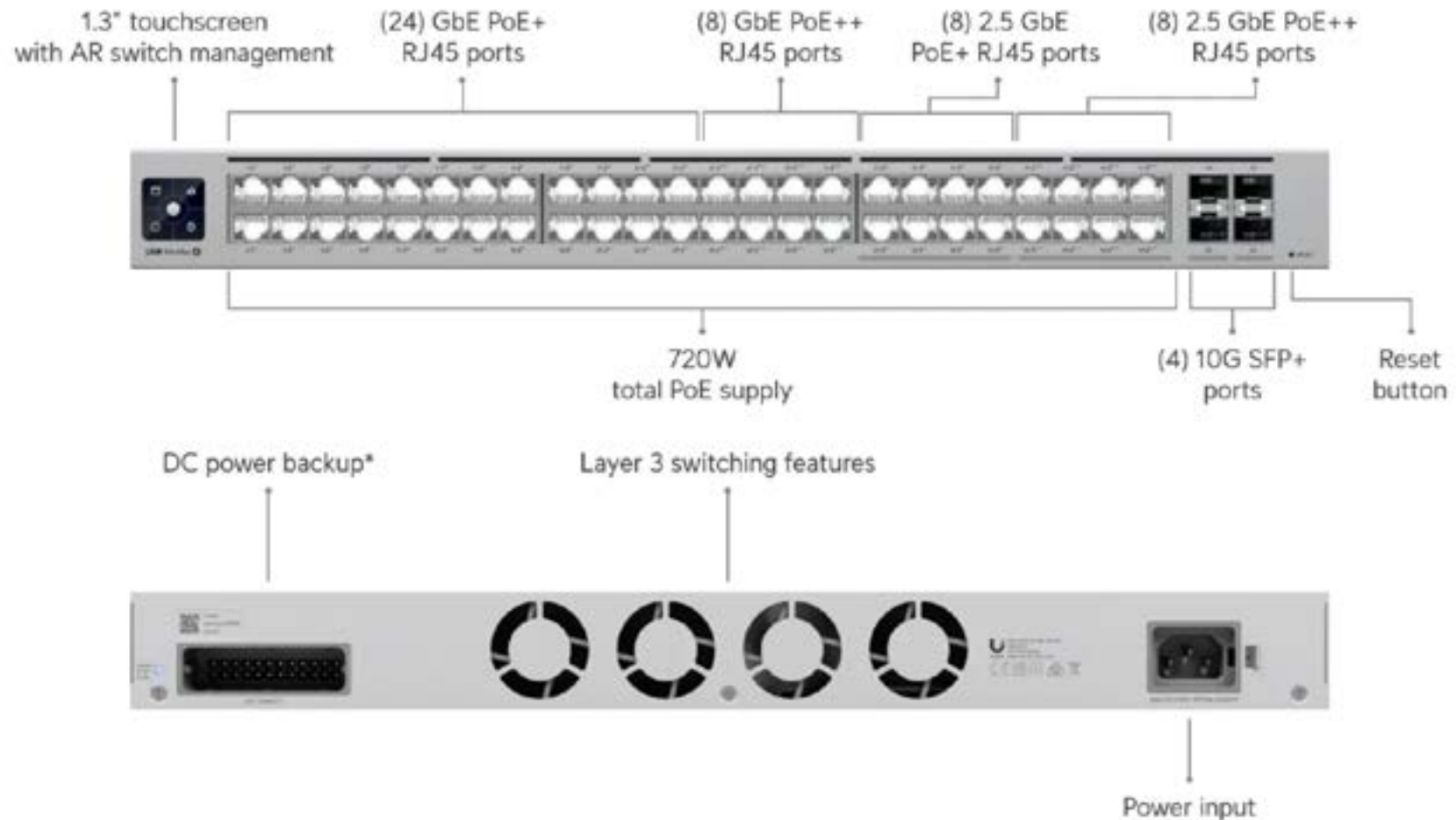
3.3 Hardwarecomponenten & technische specificaties

3.3.3 UniFi Switch Pro Max 48 PoE 720w

Prijs: €1500 euro

Waarom?

Voorziet access points, camera's en access control centraal van netwerk en stroom via PoE, wat bekabeling vermindert en installatie eenvoudiger maakt.



De UniFi Switch Pro Max 48 PoE is de centrale PoE-switch van de infrastructuur. Dit toestel voedt en verbindt alle camera's, access points en toegangscontroleleiders via PoE, wat aparte stroomkabels overbodig maakt. Het totale PoE-budget bedraagt 720 watt. De richtprijs bedraagt €1.500.

3.3 Overzicht van de volledige infrastructuur

3.3.4 Triton RMA 18U Rackkast

Triton RMA 18U Rackkast

Prijs: €300-500 euro

De Triton RMA 18U Rackkast biedt ruimte voor alle kernapparatuur in de technische ruimte. De kast biedt voldoende vrije ruimte voor toekomstige uitbreiding en goede luchtcirculatie. De richtprijs bedraagt €300 tot €500.



3.3 Overzicht van de volledige infrastructuur

3.3.5 Rack Panel

Ubiquiti UACC-Rack-Panel-Brush-1U

Prijs: €40-50

Waarom?

Zorgt voor propere kabeldoorvoer in het rack en maakt onderhoud makkelijker.



3.3 Overzicht van de volledige infrastructuur

3.3.6 Patchpaneel

Patchpaneel Cat6 FTP 48-poorts

Prijs: ± €90–€150

Waarom?

Centraliseert alle netwerkkabels in het rack zodat kabels niet rechtstreeks op de switch aangesloten moeten worden, wat onderhoud, troubleshooting en kabelbeheer eenvoudiger maakt.



3.3 Overzicht van de volledige infrastructuur

3.3.7 APC Smart-UPS

APC Smart-UPS SMT1500RMI2UC

Prijs: ± €1000–€1300

Waarom?

Beschermt kritieke netwerkapparatuur tegen stroomuitval en spanningsproblemen zodat routers, switches, camera's en opslag gecontroleerd kunnen blijven werken en niet abrupt uitvallen.



3.3 Overzicht van de volledige infrastructuur

3.3.8 Skyhawk hardeschijf

Skyhawk harde schijf 4TB 24/7

Prijs: € 199,00

Waarom?

Ontworpen voor 24/7 camerabewaking en betrouwbare opslag van continue video-opnames.



3.3 Overzicht van de volledige infrastructuur

3.3.9 Digitus 1U

DIGITUS 1U

Prijs: € 50

Waarom?

Voorziet alle rackapparatuur centraal van stroom en zorgt voor een overzichtelijke stroomverdeling in het rack.



3.3 Overzicht van de volledige infrastructuur

3.3.10 LTE failover

Prijs: €180-250

Waarom?

Biedt automatische internet failover via 4G/5G zodat kritieke diensten zoals POS, camera's en beheer online blijven bij internetstoringen.



3.3 Overzicht van de volledige infrastructuur

3.3.11 UniFi U7 Pro XGS

Prijs: €284 - €340

Waarom?

- Hoge densiteit bezoekers (zaal)
- WiFi 7 + 6 GHz ondersteuning
- Hoge doorvoer voor drukke zones
- 2.5GbE uplink
- Geschikt voor ±300 bezoekers verspreid over meerdere AP's



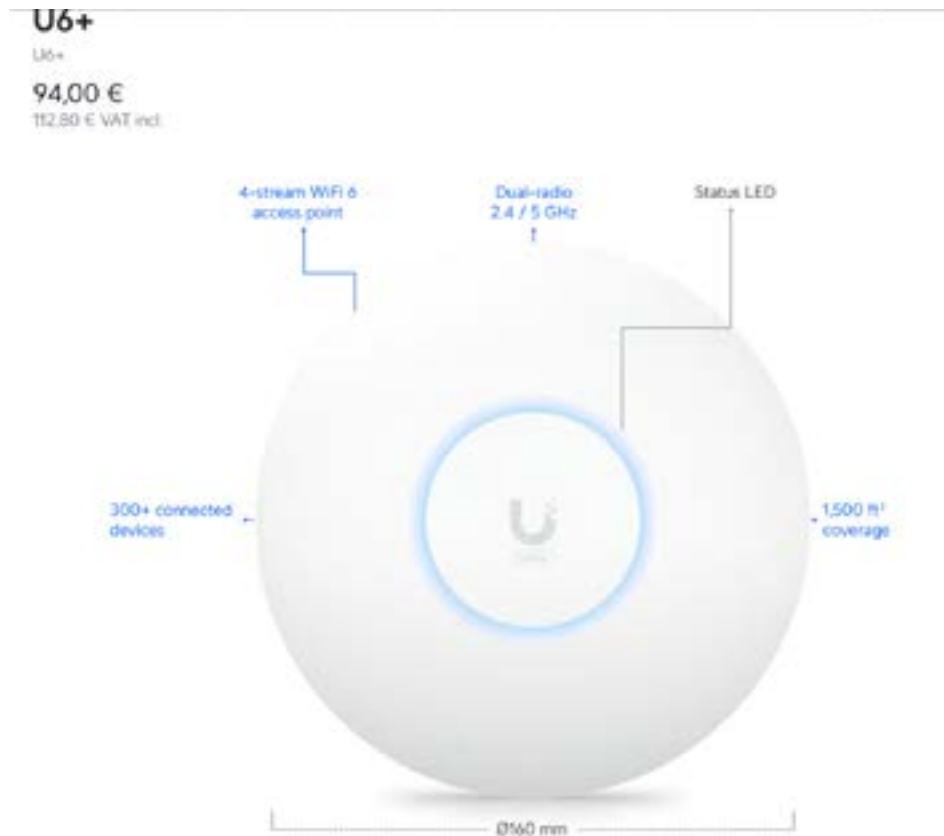
3.3 Overzicht van de volledige infrastructuur

3.3.12 UniFi U6+

Prijs: €100

Waarom?

- Kostenefficiënt voor kleinere ruimtes
- WiFi 6 ondersteuning
- PoE gevoed via netwerkkabel
- Voldoende voor office & backstage zones



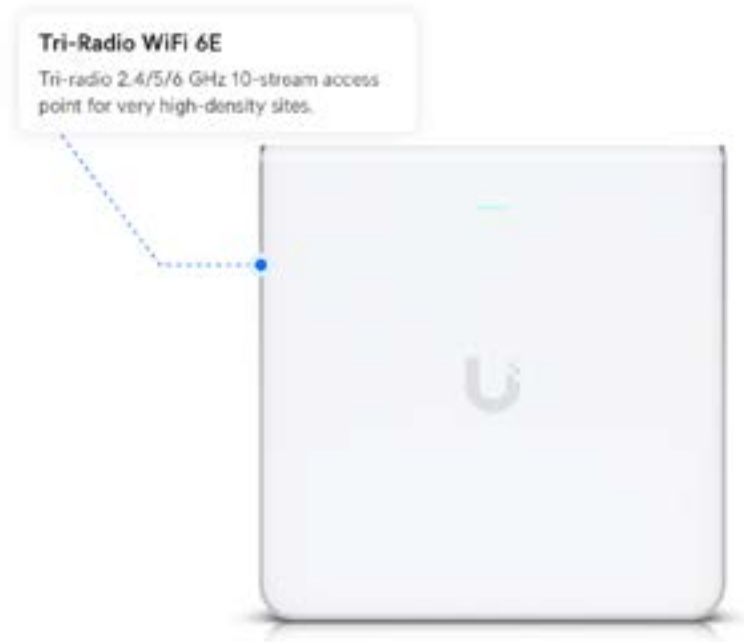
3.3 Overzicht van de volledige infrastructuur

3.3.13 UniFi U6 Enterprise in-wall

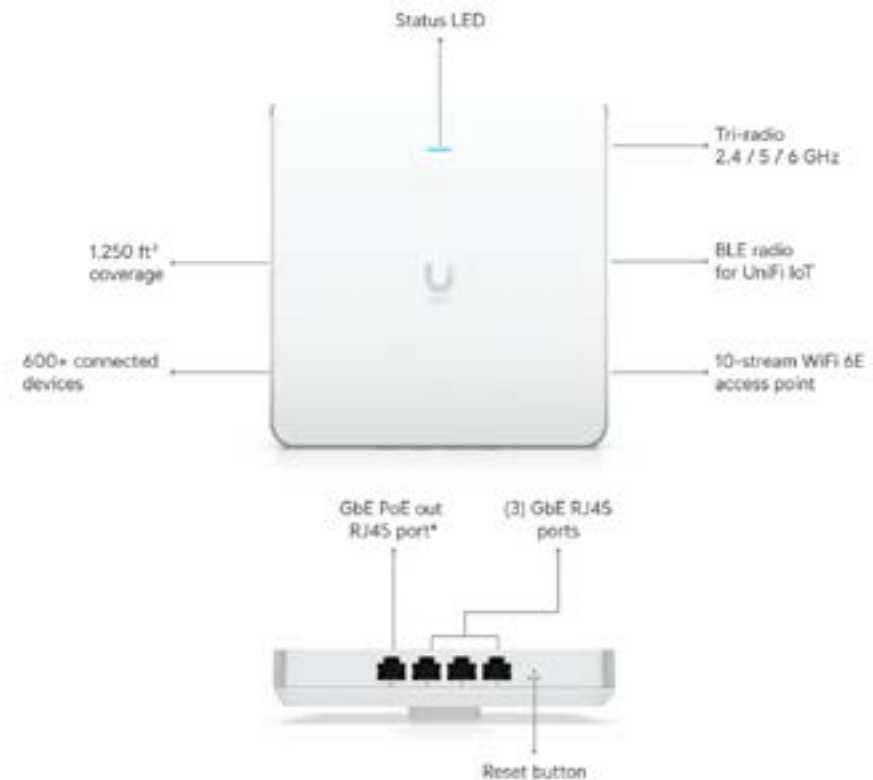
Prijs: €250–320

Waarom?

- Compact ontwerp voor VIP lounge
- WiFi 6E ondersteuning
- Extra ethernetpoorten geïntegreerd
- Hoge capaciteit voor premium zones
- Discrete plaatsing tegen muur



il



3.3 Overzicht van de volledige infrastructuur

3.3.14 G5 Pro

G5 Pro: 5 camera's

Prijs: €270-320

buiten, nachtvisie, inkom, PoE



3.3 Overzicht van de volledige infrastructuur

3.3.15 G5 Dome Ultra

G5 Dome Ultra: 15 camera's

Prijs: €80

vandalismebestendig, plafondmontage, binnengebruik, PoE



3.3 Overzicht van de volledige infrastructuur

3.3.16 AI 360

Ai 360: 3 camera's

Prijs: €400

360° overzicht, crowd monitoring, centrale dansvloer PoE



3.3 Overzicht van de volledige infrastructuur

3.3.17 Sunmi T2S Lite

POS-systeem: Sunmi T2S Lite P03130033 single screen

Prijs: €500

- Android-based POS terminal
- 15.6 inch touchscreen interface
- Compact horeca ontwerp
- Ondersteunt browser-based applicaties
- Ethernet en WiFi ondersteuning
- Draait binnen VLAN 40 (POS netwerk)



3.3 Overzicht van de volledige infrastructuur

3.3.18 Worldline Yomani XR

Prijs: €250 - 300

- Contactloos betalen
- Bancontact / Visa / Mastercard
- Gescheiden van POS software
- Ethernet connectiviteit mogelijk
- PCI veiliger betaalverkeer
- Professionele horeca terminal



3.3 Overzicht van de volledige infrastructuur

3.3.19 Epson TM-T20II

Prijs: €150-200

- Meest gebruikt bonprinter voor horeca
- Snelle afdrukken
- Lage operationele kost
- Compatibel met POS systemen
- Hoge betrouwbaarheid



3.4 PoE-budget

De UniFi Pro Max 48 PoE switch beschikt over een totaal PoE-budget van 720W.

Onderstaande berekening toont het geschatte verbruik van alle PoE-apparaten in het netwerk.

TOESTEL	AANTAL	MAX. VERBRUIK / STUK	TOTAAL VERBRUIK
 G5 Pro Camera	5	10 W	50 W
 G5 Dome Ultra Camera	15	4,2 W	63 W
 AI 360 Camera	3	8,64 W	25,92 W
 U7 Pro XGS Access Point	3	29 W	87 W
 U6+ Access Point	2	9 W	18 W
 U6 Enterprise In-Wall	1	21 W	21 W
 LTE Backup Pro	1	8,5 W	8,5 W
 UniFi Access – Door Hub Mini	4	10 W	40 W
 UniFi Access – G2 Reader	4	6 W	24 W
TOTAAL	38 PoE-toestellen	-	±337,42 W



TOTAAL POE-VERBRUIK
±337,42 W



BESCHIKBAAR POE-BUDGET
720 W



BESCHIKBARE MARGE
±382,58 W
(±53% vrij)



Conclusie: Het totale verbruik blijft ruim binnen het beschikbare PoE-budget.
Er is voldoende marge voor toekomstige uitbreidingen of piekbelasting.

H4 - Netwerkimplementatie & configuratie

VLAN Plan

Binnen The Solus Club wordt het netwerk opgesplitst in meerdere VLAN's. Hierdoor worden bezoekers, personeel, camera's, POS-systemen en IoT-toestellen van elkaar gescheiden voor extra veiligheid en betere prestaties.

Elk VLAN heeft een eigen functie binnen het netwerk. Zo krijgt het guest netwerk enkel internettoegang, terwijl camera's, servers en kassasystemen in aparte beveiligde netwerksegmenten geplaatst worden. Firewallregels zorgen ervoor dat enkel noodzakelijke communicatie toegelaten wordt.

Deze netwerkstructuur zorgt voor een stabiel, overzichtelijk en professioneel netwerk binnen de nachtclub.

 VLAN	 NAAM	 IP-NETWERK (/24)	 GATEWAY
 10	Staff	192.168.10.0/24	192.168.10.1
 20	Guest	192.168.20.0/24	192.168.20.1
 30	Cameras	192.168.30.0/24	192.168.30.1
 40	POS	192.168.40.0/24	192.168.40.1
 50	Management	192.168.50.0/24	192.168.50.1
 60	IoT	192.168.60.0/24	192.168.60.1



Belangrijk:
Native **VLAN 999** wordt gebruikt als beveiligingsmaatregel om ongewenst of ongetagd verkeer te isoleren en **VLAN 1** te vermijden.



DHCP

Elke VLAN krijgt een eigen DHCP scope. Kritieke toestellen zoals camera's, POS-systemen en netwerkapparatuur krijgen DHCP reservations.

gateway per VLAN = .1

dynamische adressen voor clients

camera's krijgen reservations

POS krijgt reservations

management toestellen gebruiken vaste adressen

Firewall regels

- Guest netwerk heeft geen toegang tot managementsystemen
- Camera VLAN wordt gescheiden van gebruikersnetwerken
- POS-systemen blijven afgeschermd van bezoekers
- IoT-toestellen hebben beperkte toegang tot kritieke infrastructuur
- Inter-VLAN filtering verhoogt de netwerkbeveiliging

All **Internet (13)** LAN (18) Guest (12) Internet v6 (6) LAN v6 (0) Guest v6 (3)

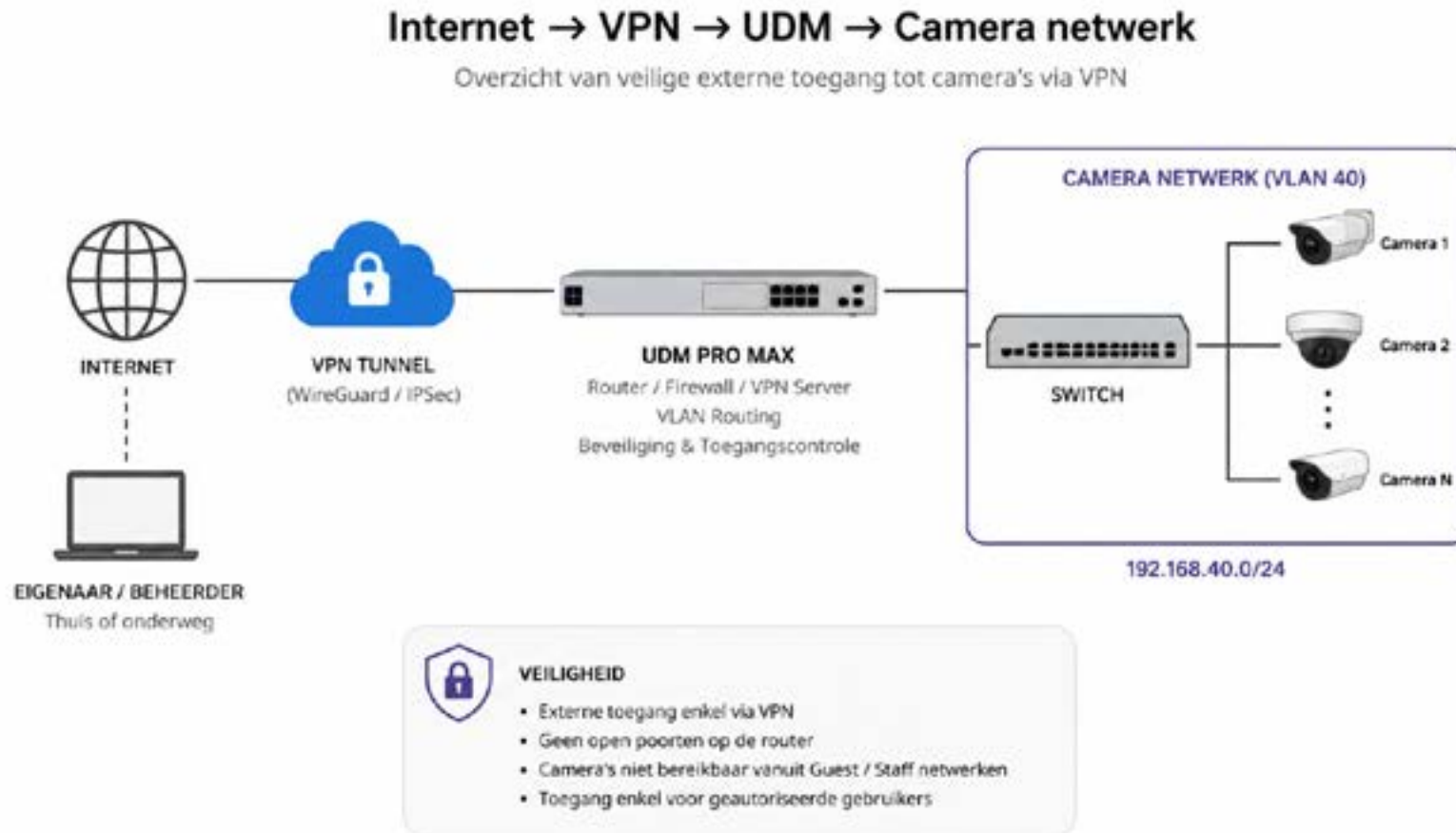
☐ Internet In ☐ Internet Local

Name	Action	Type	Protocol	Source	Port	Destination
 Block geust to management	Drop	Internet In	All	GUEST	Any	MANAGEMENT
 Block Guest to Cameras	Drop	Internet In	All	GUEST	Any	CAMERAS
 Block Guest to POS	Drop	Internet In	All	GUEST	Any	POS
 Block Guest to Staff	Drop	Internet In	All	GUEST	Any	STAFF
 Block Guest to IoT	Drop	Internet In	All	GUEST	Any	IoT
 Block Guest to Default LAN	Drop	Internet In	All	GUEST	Any	Default
 Block IoT to Management	Drop	Internet In	All	IoT	Any	MANAGEMENT
 Block Cameras to Management	Drop	Internet In	All	CAMERAS	Any	MANAGEMENT
 Block POS to Management	Drop	Internet In	All	POS	Any	MANAGEMENT
 Allow Established/related Sessions	Accept	Internet In	All	Any	Any	Any
 Drop Invalid State	Drop	Internet In	All	Any	Any	Any
 Allow Established/related Sessions	Accept	Internet Local	All	Any	Any	Any
 Drop Invalid State	Drop	Internet Local	All	Any	Any	Any

[Create Entry](#) [Create List](#) [Manage](#)

Remote access

Externe toegang gebeurt via een beveiligde VPN-verbinding zodat de eigenaar en beheerders camera's, beheerplatformen en netwerkdiensten veilig extern kunnen bereiken zonder onveilige port forwarding toe te passen. De UDM Pro Max ondersteunt VPN-technologieën zoals WireGuard en IPsec, waardoor versleutelde communicatie mogelijk wordt tussen externe gebruikers en het interne netwerk. Door gebruik te maken van VPN blijft het cameranetwerk afgeschermd van het publieke internet en krijgen enkel geautoriseerde gebruikers toegang tot kritieke systemen buiten de nightclubomgeving.



H5 - Firewall & Security

Network Security

Om kritieke systemen te beschermen wordt gebruik gemaakt van netwerksegmentatie, firewallregels en toegangscontrole. Hierdoor wordt ongewenst verkeer beperkt en blijven gevoelige systemen beter beschermd.

Bullets:

- VLAN-segmentatie
- Inter-VLAN filtering
- Gescheiden netwerkzones
- Beperken laterale beweging
- Least privilege principe

6.2 Voorbeeld firewallregels

UniFi firewalls werken met firewallregels binnen de UniFi Controller. Deze regels controleren verkeer tussen VLANs en netwerksegmenten. Elke regel bevat een source netwerk, destination netwerk, protocol, poort en een actie.

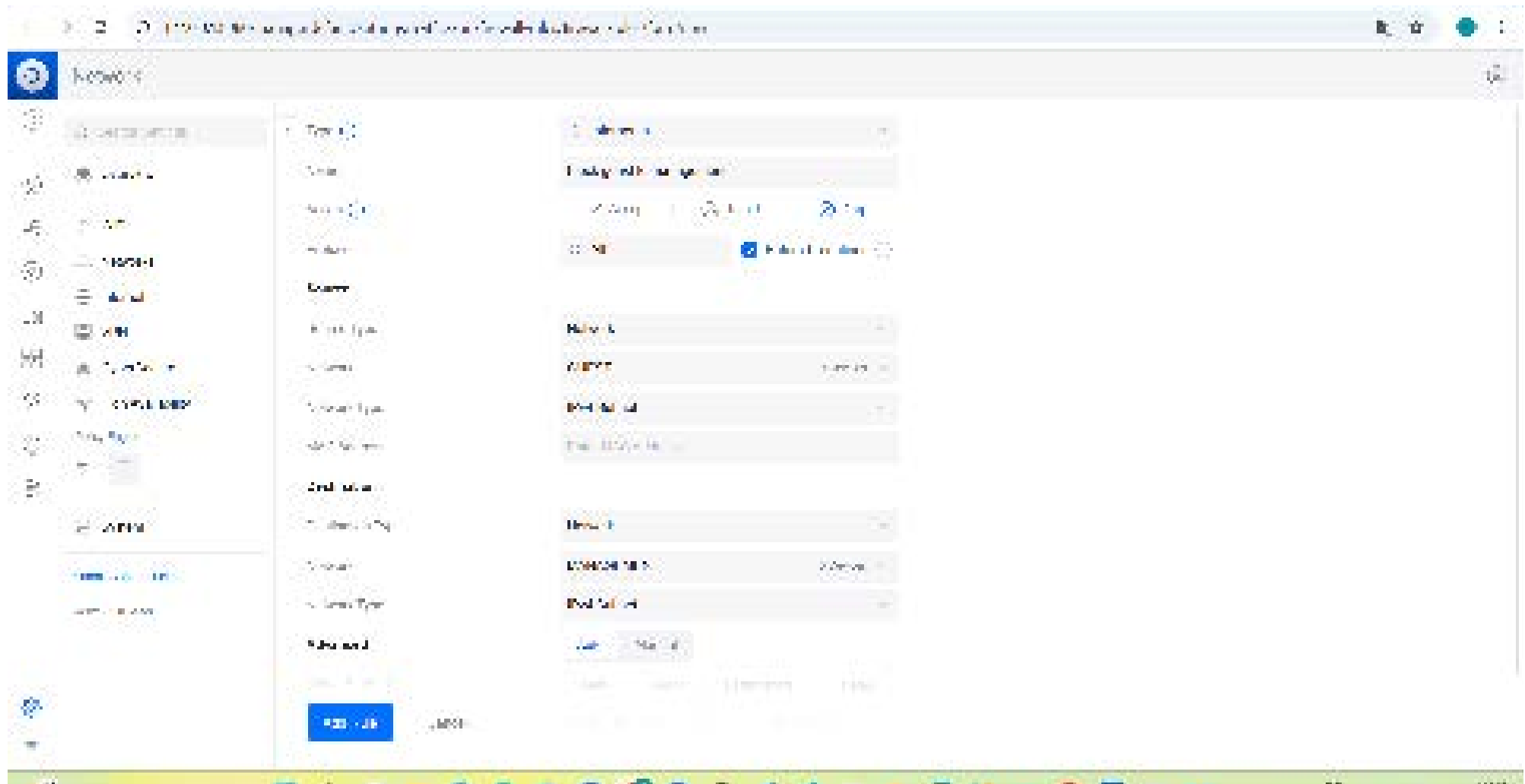
Binnen UniFi bestaan verschillende acties:

Allow / Accept → verkeer wordt toegelaten

Drop → verkeer wordt stil geblokkeerd zonder antwoord

Reject → verkeer wordt geblokkeerd met een foutmelding terug naar de client

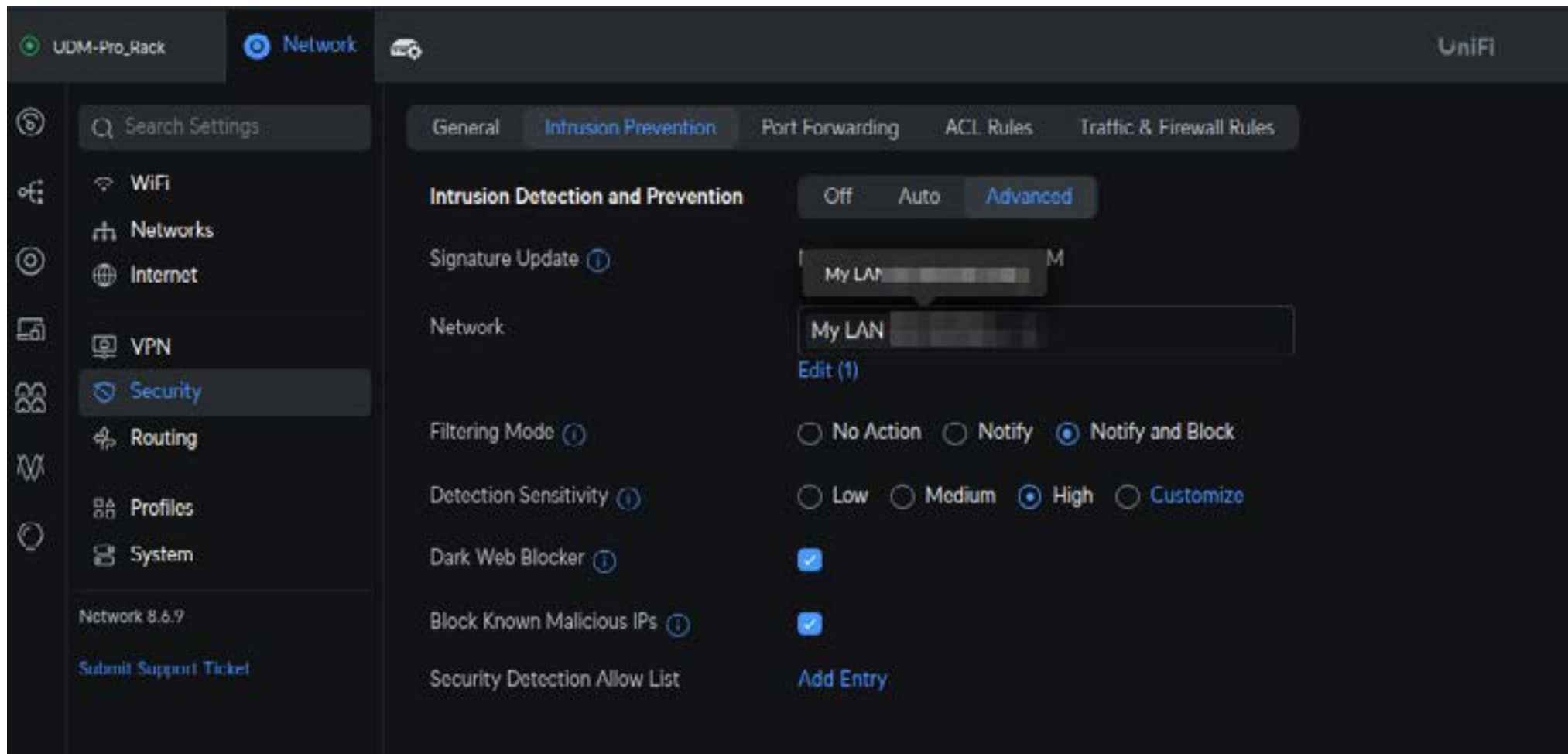
Binnen The Solus Club worden voornamelijk DROP-regels gebruikt om verkeer van het GUEST VLAN naar management, camera's, POS-systemen en IoT-toestellen te blokkeren. Hierdoor blijven gevoelige systemen veilig gescheiden van bezoekersverkeer.



Intrusion Detection & Prevention

De UDM Pro Max ondersteunt IDS/IPS functionaliteiten waarmee verdacht netwerkverkeer gedetecteerd en geblokkeerd kan worden. Hierdoor kunnen potentiële aanvallen sneller geïdentificeerd worden.

- Deep Packet Inspection (DPI) analyseert netwerkverkeer
- Signature-based detection detecteert gekende bedreigingen
- Notify and Block modus blokkeert verdachte verbindingen automatisch
- Detectiegevoeligheid ingesteld op High
- Dark Web Blocker en malicious IP blocking ingeschakeld
- Centrale configuratie via UniFi Controller



LTE Failover & Redundancy

Om beschikbaarheid te verhogen wordt LTE failover gebruikt als redundante WAN-verbinding. Bij uitval van de primaire internetverbinding schakelt het netwerk automatisch over naar de secundaire verbinding.



UPS bescherming

UPS-systemen (Uninterruptible Power Supply) beschermen kritieke netwerkapparatuur tegen stroomuitval, spanningspieken en korte onderbrekingen in de elektriciteitsvoorziening. Binnen de infrastructuur wordt gebruik gemaakt van een APC Smart-UPS SMT1500RMI2UC die tijdelijke batterijvoeding levert wanneer de primaire stroomvoorziening uitvalt.

De UPS wordt in het rack geplaatst tussen de stroomvoorziening en de kritieke netwerkcomponenten. Apparatuur zoals de UDM Pro Max, UniFi Pro Max switches, opslagapparatuur en andere essentiële infrastructuurcomponenten worden via de UPS gevoed zodat deze operationeel blijven tijdens een stroomonderbreking. Omdat access points, camera's en toegangscontrole via PoE door de switches worden gevoed, blijven ook deze systemen tijdelijk actief zolang de switches van stroom voorzien blijven.

Naast noodstroom biedt de UPS bescherming tegen spanningsschommelingen en piekspanningen die gevoelige netwerkapparatuur kunnen beschadigen. Afhankelijk van de effectieve belasting kan de UPS de infrastructuur gedurende ongeveer 15 tot 30 minuten operationeel houden. Hierdoor wordt downtime beperkt en krijgen systemen voldoende tijd om gecontroleerd uit te schakelen of operationeel te blijven tot de stroomvoorziening hersteld is.



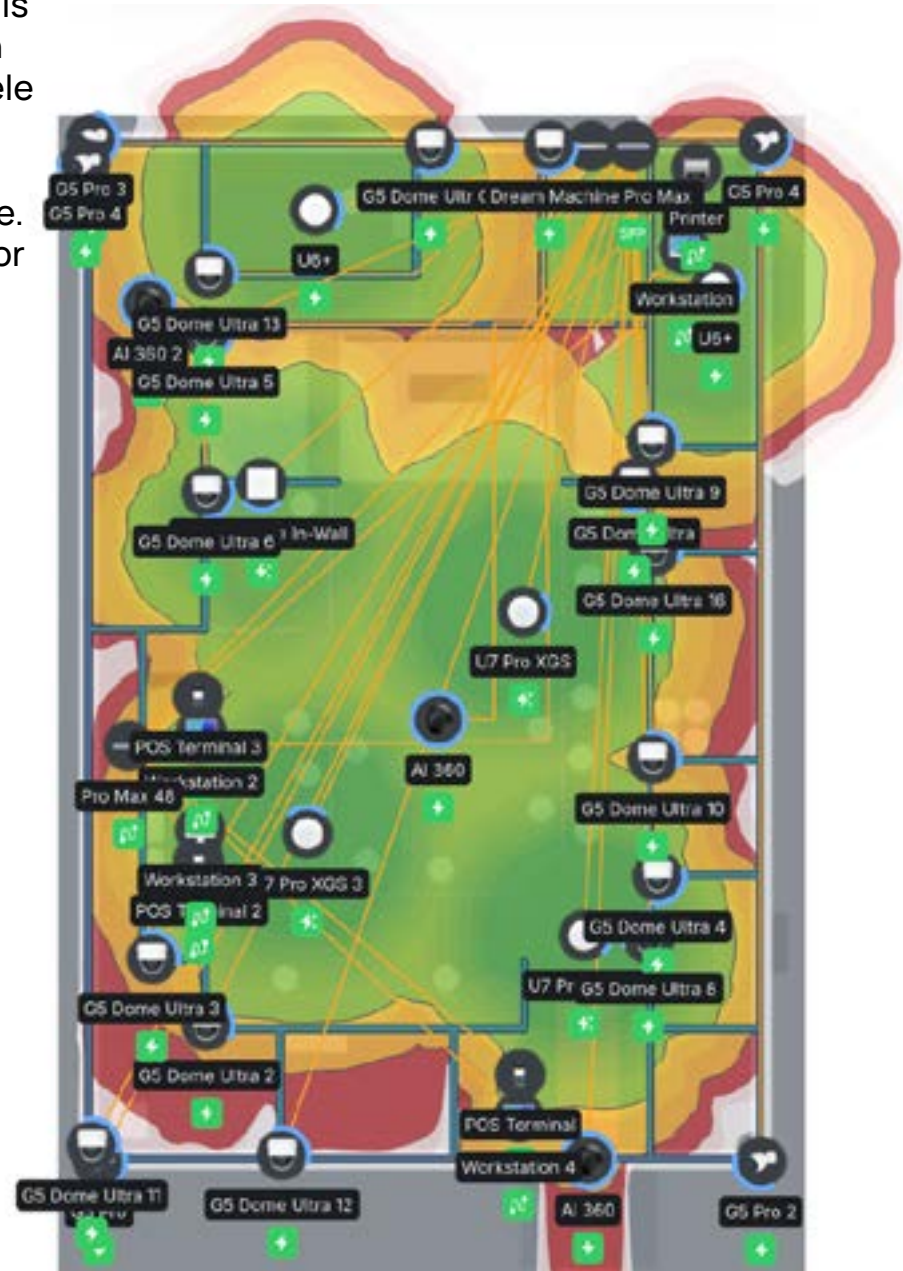
H6 - Wifi infrastructuur

WiFi Coverage / Access Points Placement

Op basis van de uitgevoerde WiFi-planning bieden de access points een vrijwel volledige dekking van de nightclub. De belangrijkste zones zoals de dansvloer, bar, VIP-ruimte, ingang, backstage en kantoor bevinden zich volledig binnen het groene dekkingsgebied, waardoor een stabiele draadloze verbinding gegarandeerd kan worden.

Enkele beperkte zones, voornamelijk in de stockruimte en delen van de sanitaire voorzieningen, beschikken over een lagere signaalsterkte. Deze ruimtes vereisen echter geen intensief netwerkgebruik waardoor bijkomende access points niet noodzakelijk zijn.

Door de strategische plaatsing van de access points wordt een optimale balans bereikt tussen dekking, capaciteit en kostenefficiëntie.



WiFi Settings / SSIDs

Het SSID Solus-Guest wordt uitsluitend uitgezonden door het access point in de hoofdzaal. Hierdoor blijft het gasten-netwerk beperkt tot de zones waar bezoekers zich bevinden. Het SSID Solus-Staff wordt daarentegen op alle access points uitgezonden zodat personeel steeds toegang heeft tot het interne netwerk, ongeacht hun locatie binnen het gebouw.

Door SSID's te koppelen aan afzonderlijke VLAN's wordt netwerksegmentatie ook draadloos doorgetrokken. Hierdoor blijven bezoekers, personeel en interne systemen logisch van elkaar gescheiden.

Network

Search Settings

Overview

WiFi

Networks

Internet

VPN

CyberSecure

High Availability

Policy Engine

System

Submit Support Ticket

Network 90.1.55

Name	Network	Broadcasting APs	Radio Band	Clients	Security
Solus-Guest	GUEST (20)	UAP Pro	2.4 GHz 5 GHz	-	Open
Solus-Staff	STAFF (10)	All APs	2.4 GHz 5 GHz	-	WPA2

Create New Manage

Channel Plan

Click on a channel to exclude it from use

2.4 GHz 2412-2484 MHz

5 GHz 5180-5856 MHz

Channels 1 2 3 4 5 6 7 8 9 10 11 12 13 14

20 MHz 40 MHz 80 MHz 160 MHz

Legend: In Use, Enabled, LPTs, Not available, Excluded

Restore to Defaults

Default WiFi Speeds

Maximum Speed Conservative Custom Apply to All APs

Channel Width (MHz)

2.4 GHz 5 GHz 6 GHz

20 40 80 160 20 40 80 160 320

WiFi Security & VLAN Integration

Binnen de infrastructuur worden meerdere SSID's gekoppeld aan verschillende VLAN's zodat gebruikers automatisch in het correcte netwerksegment terechtkomen.

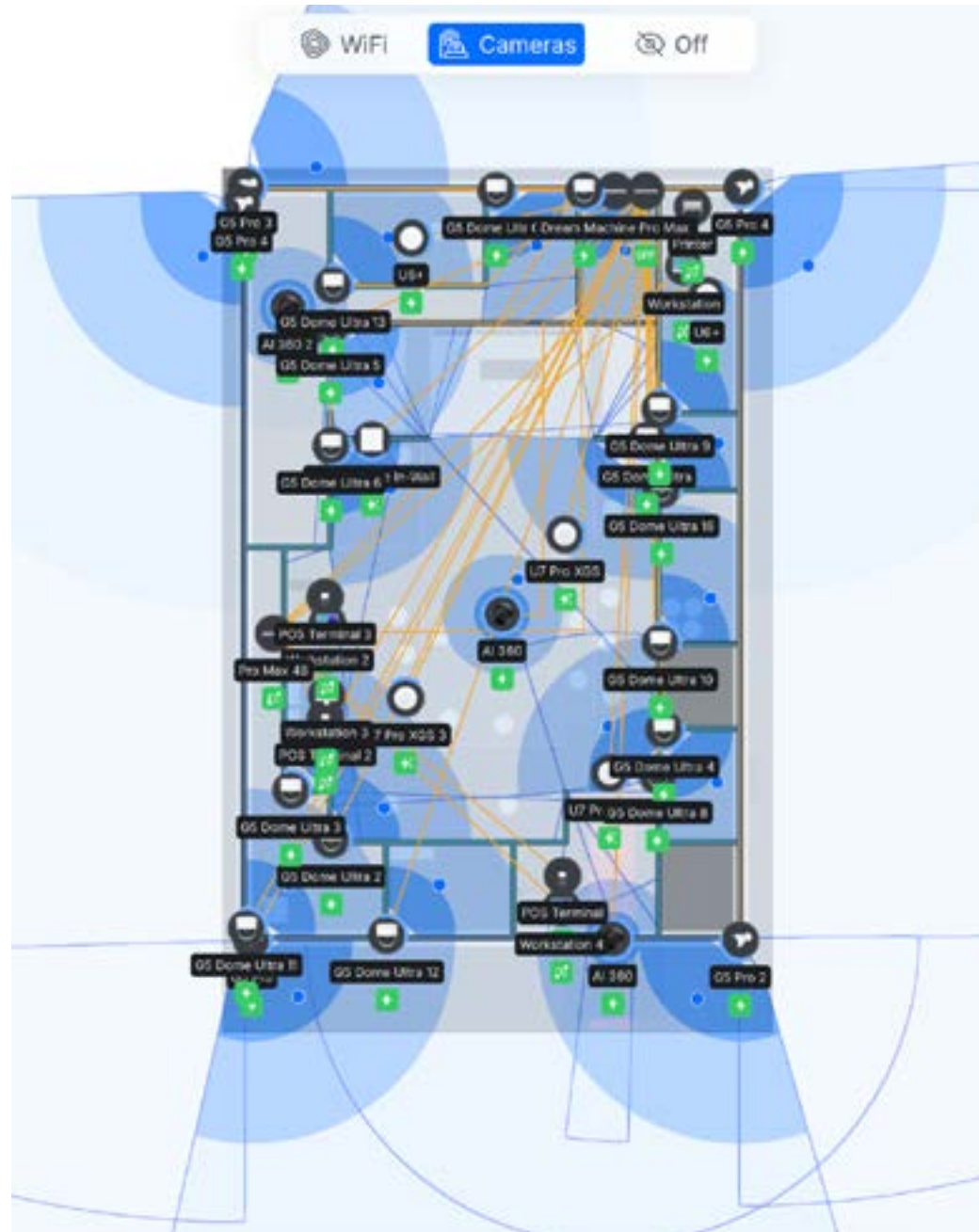
Solus-Guest is gekoppeld aan VLAN 20 Guest en biedt uitsluitend toegang tot het internet. Solus-Staff is gekoppeld aan VLAN 10 Staff en geeft personeel toegang tot interne diensten waarvoor expliciete firewalltoelatingen voorzien zijn. De access points sturen draadloos verkeer via trunkverbindingen naar de switches. Dankzij 802.1Q VLAN-tagging blijft het verkeer van bezoekers en personeel correct gescheiden binnen dezelfde fysieke infrastructuur. AP-MAINHALL zendt zowel guest- als staffnetwerken uit, terwijl AP-OFFICE uitsluitend staffverkeer uitzendt.

Voor de beveiliging van het draadloze netwerk wordt gebruik gemaakt van WPA2/WPA3-authenticatie. Daarnaast wordt client isolation toegepast op het gastennetwerk zodat bezoekers onderling geen directe verbinding kunnen maken. Hierdoor blijft het netwerk veiliger en stabiel tijdens drukke evenementen.

H7 - Camerasurveillance

8.1 Camera plan

Op deze foto kan je de planning zien van de cameras in de nachtclub, ik heb dit plan kunnen maken met UniFi Design center.



8.2 AI Cameras

Binnen The Solus Club worden drie UniFi AI 360 camera's gebruikt binnen VLAN 30 Cameras. Eén camera wordt geplaatst aan de inkom, één centraal boven de dansvloer en één in de backstagezone voor full-room surveillance zonder dode hoeken.

De UniFi AI 360 beschikt over een 5MP CMOS sensor met een 360° fisheye lens en ondersteunt een resolutie van 1920x1920 aan 30 FPS. Binnen UniFi Protect wordt gebruik gemaakt van dewarping waardoor één fisheye-camera softwarematig opgesplitst kan worden naar meerdere virtuele camerazichten.

De camera ondersteunt edge AI processing voor person detection en motion events. Alle videostreams worden via H.264-compressie doorgestuurd naar de UniFi Protect omgeving op de UDM Pro Max, terwijl het cameraverkeer gescheiden blijft binnen VLAN 30 Cameras.

De AI 360 camera's worden aangesloten via IEEE 802.3af PoE waardoor zowel voeding als netwerkverkeer via één Cat6 FTP-kabel verlopen vanuit de UniFi Pro Max PoE-switches.

8.3 UniFi Protect

Binnen The Solus Club wordt UniFi Protect gebruikt voor het centraal beheren van alle beveiligingscamera's. Via UniFi Protect kunnen live camerabeelden bekeken worden, motion events gedetecteerd worden en opnames terug opgezocht worden via een tijdlijninterface.

Alle camerabeelden worden opgeslagen binnen de UniFi Protect omgeving op de UDM Pro Max. Hierdoor kunnen opnames centraal beheerd worden en blijven camerabeelden eenvoudig raadpleegbaar vanuit één beheersplatform.

Omdat alle camera's zich binnen VLAN 30 Cameras bevinden, blijft het cameraverkeer volledig gescheiden van andere netwerksegmenten zoals guest, POS en IoT. Enkel managementtoestellen binnen VLAN 50 Management krijgen toegang tot UniFi Protect en de camerastreams.

Daarnaast ondersteunt UniFi Protect AI-functionaliteiten zoals person detection en motion events op compatibele camera's zoals de UniFi AI 360. Hierdoor kunnen beveiligingsincidenten sneller gedetecteerd worden binnen de nightclubomgeving.

8.4 Camera-retentie

De camerabewakingsinfrastructuur maakt gebruik van een Seagate SkyHawk 4TB surveillance hardeschijf voor de opslag van camerabeelden. Binnen het ontwerp worden in totaal 23 camera's ingezet:

- 5x UniFi G5 Pro
- 15x UniFi G5 Dome Ultra
- 3x UniFi AI 360
- Totaal: 23 camera's

De effectieve retentieperiode is afhankelijk van verschillende factoren zoals resolutie, bitrate, framerate, opname-instellingen en het gebruik van motion recording. Door het grote aantal camera's dat gelijktijdig beelden opslaat, biedt een opslagcapaciteit van 4TB slechts een beperkte bewaartermijn.

Binnen dit project wordt de 4TB SkyHawk-schijf gebruikt als proof-of-concept en basisconfiguratie. In een productieomgeving wordt aanbevolen om extra opslagcapaciteit of meerdere harde schijven te voorzien om langere retentieperiodes mogelijk te maken.

Door gebruik te maken van motion detection, slimme detectieprofielen en geoptimaliseerde opname-instellingen kan de beschikbare opslagcapaciteit efficiënter benut worden en kan de retentieperiode aanzienlijk verlengd worden.

23 camera's × 2 Mbps = ±497 GB per dag

4TB opslag = ±8 dagen continu

Met motion detection: ±14–20 dagen

H8 – POS & bedrijfsinfrastructuur

9.1 Wat is een POS-systeem?

POS-systemen (Point of Sale) worden gebruikt voor het verwerken van verkopen, betalingen en transacties. Moderne POS-oplossingen combineren hardware en software om producten te registreren, betalingen te verwerken en verkoopgegevens centraal op te slaan.

Een modern POS-systeem bestaat typisch uit:

- kassaterminals

- betaalterminals

- bonnenprinters

- netwerkverbindingen

- centrale beheerssoftware en databanken

In deze proof-of-concept wordt gebruik gemaakt van een webgebaseerde POS-applicatie gekoppeld aan een MariaDB-database. Producten, bestellingen en transacties worden opgeslagen in MariaDB en beheerd via phpMyAdmin. Hierdoor kunnen orders centraal opgeslagen, beheerd en geraadpleegd worden.

9.2 Welke POS gebruiken wij in nachtclub

De gekozen POS-oplossing bestaat uit de Sunmi T2S Lite kassaterminals. Deze Android-gebaseerde toestellen combineren een touchscreen, netwerkconnectiviteit en kassafunctionaliteiten binnen één systeem. Hierdoor kunnen verkopen, bestellingen en transacties centraal verwerkt worden.

De POS-systemen worden ondergebracht binnen VLAN 40 POS zodat financiële transacties gescheiden blijven van andere netwerksegmenten. Via firewallregels wordt ongewenste toegang vanuit andere VLAN's beperkt om de beveiliging van transactiedata te verhogen.

De Sunmi-terminals worden via bekabelde ethernetverbindingen aangesloten voor maximale stabiliteit en een lagere kans op verbindingsproblemen tijdens piekmomenten. WiFi kan beschikbaar blijven als tijdelijke backupverbinding indien nodig.

Bestellingen en transacties worden opgeslagen in een MariaDB-database en beheerd via phpMyAdmin. Hierdoor kunnen producten, orders en verkoopgegevens centraal opgeslagen, beheerd en geraadpleegd worden. Daarnaast worden bonnenprinters en betaalterminals gekoppeld aan hetzelfde netwerksegment zodat kassacommunicatie overzichtelijk en centraal beheerd blijft.

9.3 Worldline Yomani XR

Binnen The Solus Club worden elektronische betalingen verwerkt via de Worldline Yomani XR betaalterminal. Deze ondersteunt Bancontact, kredietkaarten en contactloze betalingen.

De Sunmi T2S Lite terminals en betaalterminals worden via RJ45 ethernet aangesloten op de UniFi switchinfrastructuur binnen VLAN 40 POS. Hierdoor blijven financiële transacties gescheiden van andere netwerksegmenten en wordt een stabiele netwerkverbinding gegarandeerd.

Bij internetuitval schakelt de UniFi LTE Backup Pro automatisch over naar LTE-failover zodat kritieke diensten zoals betalingen operationeel blijven.



2 Product info

2.1 CUSTOMER TERMINAL



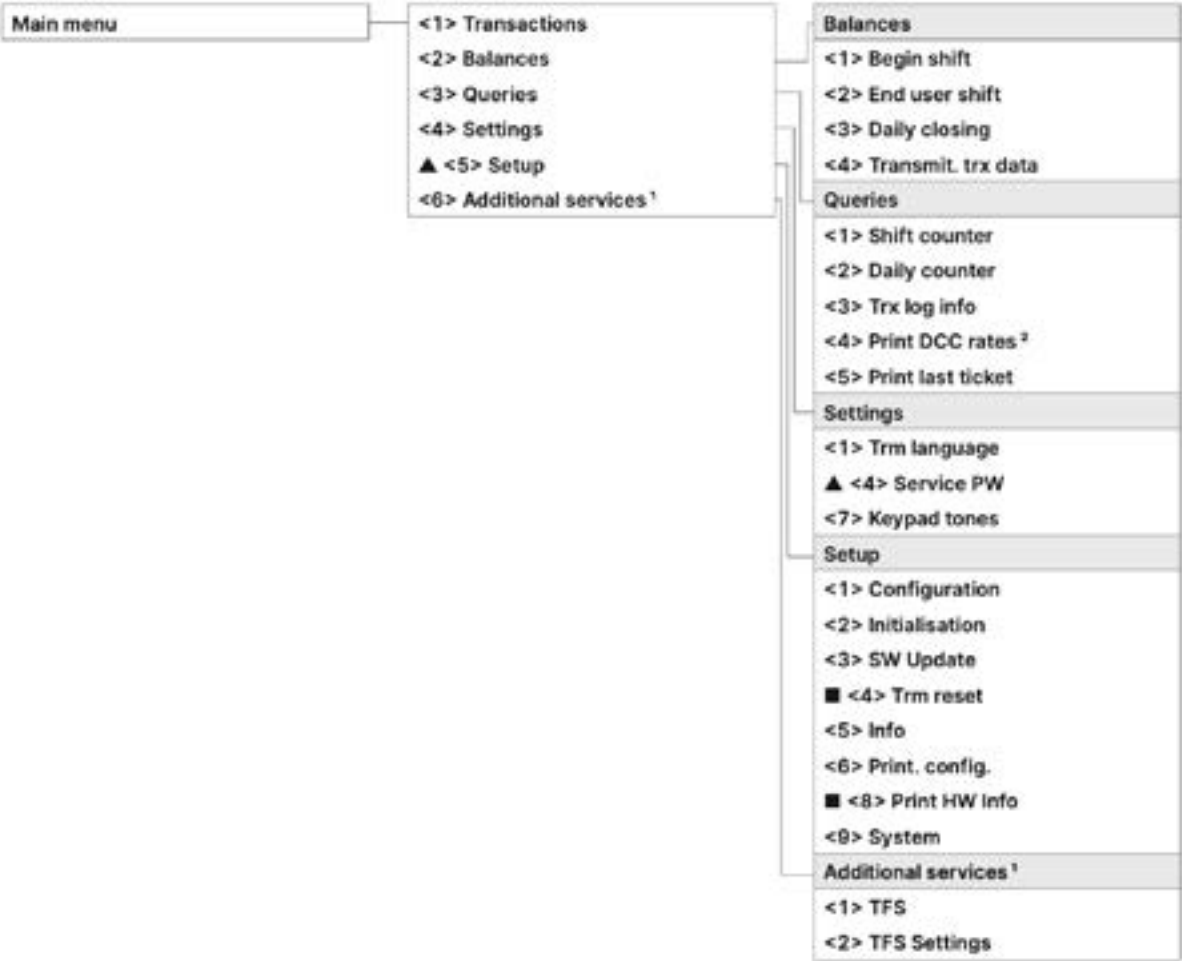
- 1 **Thermal printer**
(YOMANI XR Compact only)
- 2 **Chip reader**
For chip cards
- 3 **Magnetic strip reader**
For cards with magnetic strips
- 4 **Display**
The next step to be taken is always shown on the display.
- 5 **Navigation buttons**
You can use these three buttons to navigate through the menu (up/down/confirm).
- 6 **Contactless reader (RFID)**
For contactless paying
- 7 **<OK> button**
All entries must be confirmed using the <OK> button.
- 8 **<CORR> button**
Incorrect entries can be corrected using the <CORR> button.
- 9 **<STOP> button**
Active procedures can be stopped using this button.

9.3 Product info Worldline Yomani XR

4 Menu tree (illustration)

4.1 MAIN MENU

To enter the menu tree below, press the <STOP> button.



9.3 Product info Worldline Yomani XR

3.1 INSTALLATION

- Position the device at its intended location
- Connect the device.
Always plug in the power supply last!
- Cable:

Only the original cables delivered with the product should be used.

Customer terminal



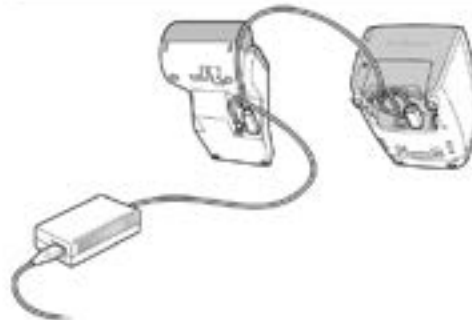
- 1 Port for NFC antenna (for contactless paying)
- 2 Serial RS-232 port
- 3 USB port
- 4 YOMANI XR Pinpad and Compact only
- 5 Ethernet/LAN port

Cash register terminal (YOMANI XR Autonom)



- 1 Cable guides
- 2 Power supply port
- 3 Customer terminal port

Completed installation



The terminal starts up and reports with an acoustic signal when it is ready to operate.

9.4 Bonnenprinters

Binnen The Solus Club worden Epson TM-T20II bonnenprinters gebruikt voor het automatisch afdrukken van kassabonnen.

De printer wordt via USB-A verbonden met de Sunmi T2S Lite POS-terminal. Wanneer een bestelling verwerkt wordt stuurt het kassasysteem automatisch een printopdracht naar de printer.

De kassalade wordt aangesloten via de RJ12 Cash Drawer Port op de Sunmi terminal. Hierdoor vormt de POS-terminal het centrale punt van de volledige kassainfrastructuur.



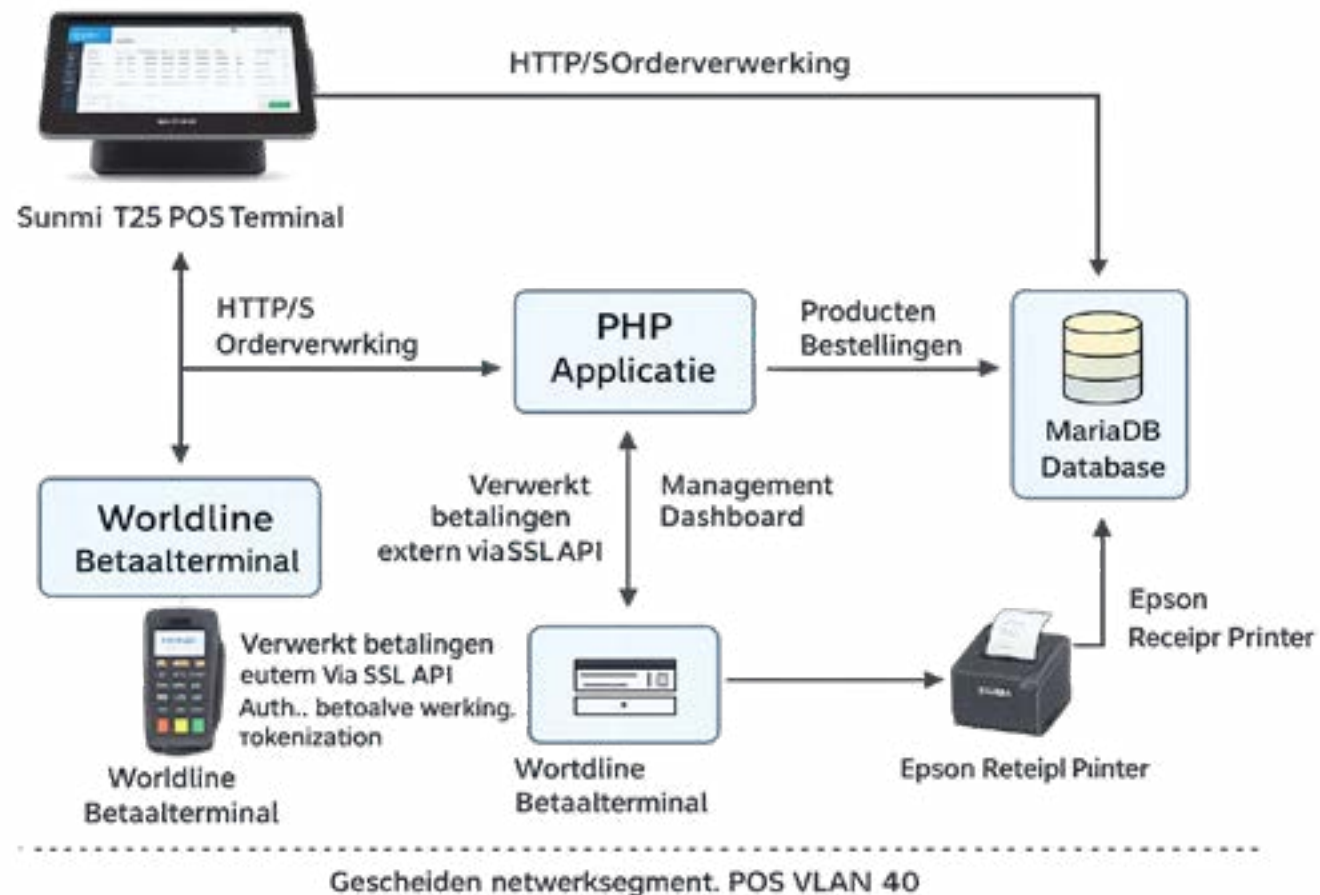
9.5 POS Netwerkarchitectuur

De POS-infrastructuur van The Solus Club werd ondergebracht in een afzonderlijk netwerksegment op VLAN 40. Door kassystemen te scheiden van gasten, camera's en IoT-toestellen wordt ongewenste toegang beperkt en blijft het netwerk overzichtelijk beheerd.

De POS-systemen worden bekabeld aangesloten via Cat6 in plaats van WiFi. Een bekabelde verbinding biedt meer stabiliteit, lagere latency en minder kans op interferentie of pakketverlies tijdens drukke evenementen. Binnen een nightclubomgeving primeert betrouwbaarheid boven flexibiliteit.

Binnen VLAN 40 worden DHCP reservations gebruikt zodat POS-terminals, printers en betaalterminals steeds hetzelfde IP-adres behouden. Dit vereenvoudigt troubleshooting, monitoring en firewallbeheer.

De infrastructuur bestaat uit Sunmi T2S Lite POS-terminals, Worldline betaalterminals en Epson-printers. De datastroom verloopt van de POS-terminal naar de PHP-applicatie en vervolgens naar de MariaDB-database voor opslag en rapportage. Betalingen worden extern verwerkt via Worldline waardoor betaalgegevens niet lokaal opgeslagen worden.



9.6 POS Security

De beveiliging van de POS-infrastructuur speelt een belangrijke rol omdat kassasystemen gevoelige bedrijfsinformatie verwerken. Daarom werd het POS-netwerk ondergebracht op VLAN 40 zodat het logisch gescheiden blijft van gasten, camera's en IoT-toestellen.

Via firewallregels wordt verkeer vanuit het gastennetwerk geblokkeerd naar het POS-segment. Hierdoor kunnen bezoekers geen verbinding maken met kassasystemen of betaalinfrastructuur. Enkel beheer-toestellen binnen het managementsegment krijgen toegang indien nodig voor onderhoud of troubleshooting.

Betaalgegevens worden niet lokaal opgeslagen binnen de infrastructuur. Transacties worden extern verwerkt via Worldline betaalterminals waardoor gevoelige betaalinformatie buiten het interne netwerk verwerkt blijft.

9.7 Redundantie

Binnen een nightclubomgeving heeft uitval van kassasystemen directe impact op omzet en dienstverlening. Daarom werden meerdere redundantiemechanismen voorzien binnen de POS-infrastructuur.

Bij internetstoringen zorgt de UniFi LTE Backup Pro voor automatische failover zodat betaalterminals, cloudtoepassingen en beheerfuncties online blijven. Daarnaast beschermt een APC Smart-UPS kritieke netwerkkapparatuur tegen stroomuitval en spanningsproblemen.

De POS-systemen maken gebruik van bekabelde verbindingen via Cat6 in plaats van WiFi. Hierdoor blijft de kans op verbindingsproblemen tijdens drukke evenementen beperkt en wordt een stabiele werking gegarandeerd.

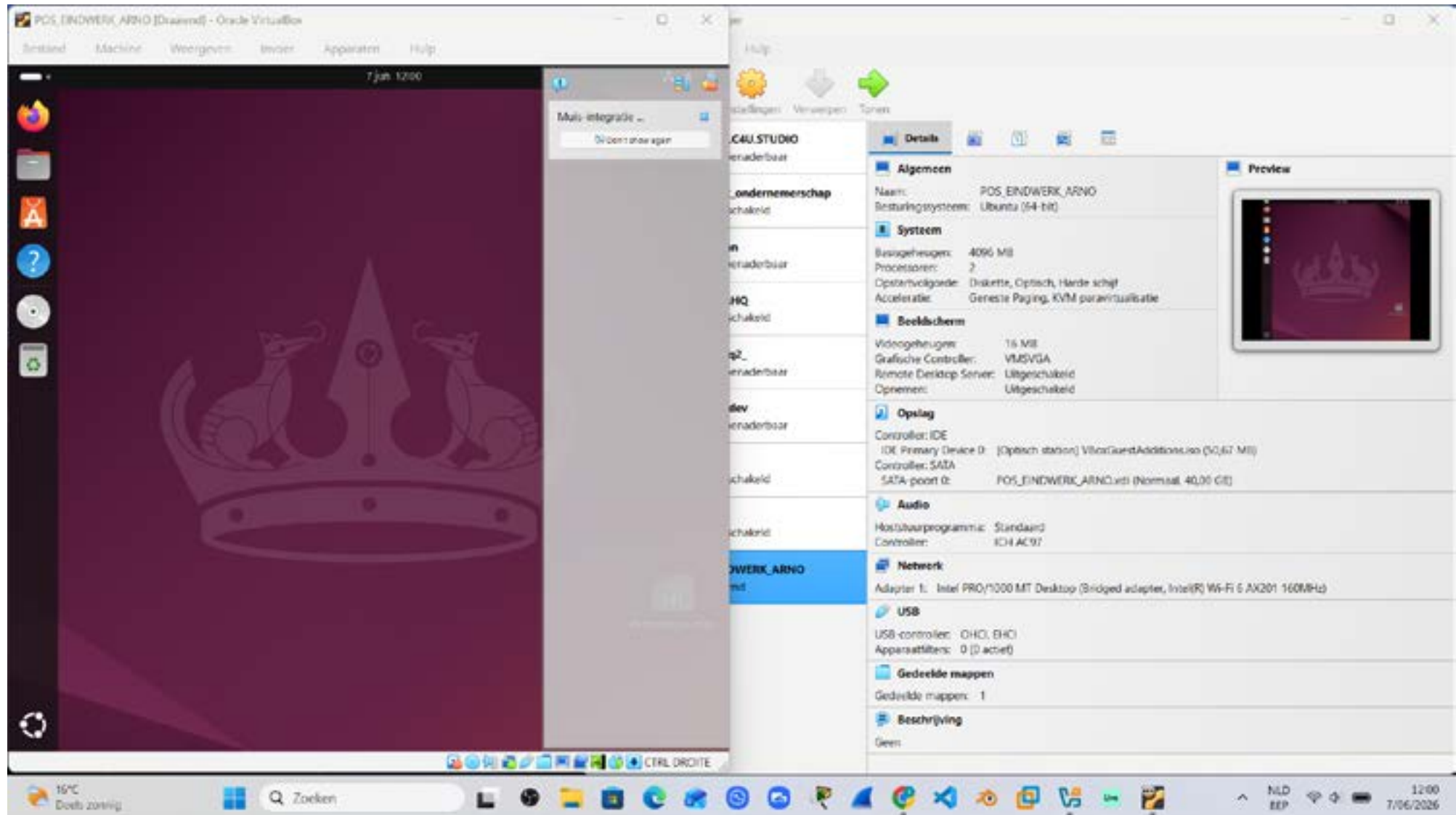
9.8 Dataflow

De verwerking van bestellingen binnen The Solus Club verloopt via een centrale datastroom tussen de POS-terminals, applicatielaag en database. Wanneer een medewerker een bestelling invoert via de Sunmi T2S Lite POS-terminal wordt deze via de PHP-applicatie verwerkt.

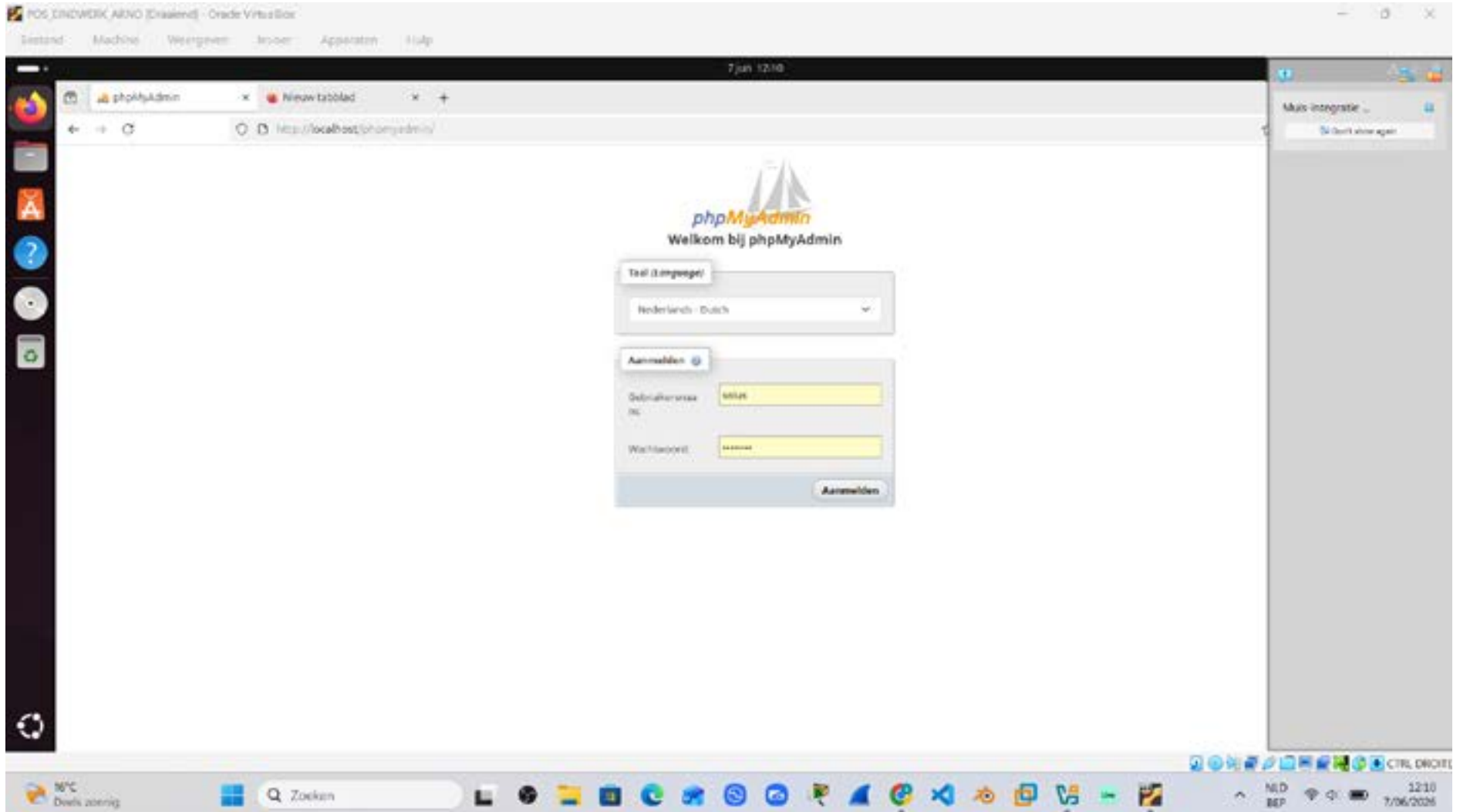
De PHP-applicatie communiceert vervolgens met de MariaDB-database waar bestellingen, producten en rapportagegegevens opgeslagen worden. Hierdoor kunnen verkopen centraal beheerd en later geanalyseerd worden.

Betalingen worden afzonderlijk verwerkt via de Worldline betaalterminal. Hierdoor worden gevoelige betaalgegevens niet lokaal opgeslagen binnen de infrastructuur. Door applicatie-, database- en betaalverwerking logisch te scheiden ontstaat een veiligere en overzichtelijke architectuur.

Demo



Phpmyadmin



Phpmyadmin producten

The screenshot shows a Windows 10 virtual machine environment. A web browser is open to the phpMyAdmin interface at `http://localhost/phpmyadmin/index.php?route=sql&pos=0&db=solusclub_pos&table=products`. The interface displays the 'products' table with the following data:

	id	product_name	price	category
☐	1	VIP Ticket	25.00	Ticket
☐	2	Vodka Redbull	12.00	Drink
☐	3	Venture Ticket	5.00	Service
☐	4	Pornstar March	12.00	Cocktail
☐	5	Juglax	2.00	Drink

The interface includes a sidebar with a database tree, a top navigation bar with various tools (Verkennen, Structuur, SQL, etc.), and a bottom status bar showing system information like temperature and time.

Phpmyadmin orders

The screenshot displays a Windows virtual machine environment. The primary application window is a web browser showing the phpMyAdmin interface. The browser's address bar indicates the URL: `http://localhost/phpmyadmin/index.php?route=/tools/pos/sales/salesable/orders`. The phpMyAdmin interface shows a table of orders with the following columns: `id`, `product_name`, `quantity`, `total price`, and `timestamp`. The table contains 18 rows of order data. The left sidebar of phpMyAdmin shows the database structure, with the `salesclub_pos` database selected. The bottom taskbar of the virtual machine shows the Windows taskbar with various application icons and the system clock displaying 12:11 on 7/05/2026.

id	product_name	quantity	total price	timestamp
1	VP Ticket	1	25.00	2026-05-31 22:38:46
2	Voeds Redbull	1	12.00	2026-05-31 22:38:46
3	Versure Ticket	1	5.00	2026-05-31 22:38:46
4	Pomstar Maroni	1	12.00	2026-05-31 22:38:46
5	Jupier	1	2.00	2026-05-31 22:38:46
6	VP Ticket	1	25.00	2026-05-31 23:34:08
7	VP Ticket	1	25.00	2026-05-31 23:34:13
8	Jupier	1	2.00	2026-05-31 23:34:20
9	Jupier	1	2.00	2026-05-31 23:34:23
10	Voeds Redbull	1	12.00	2026-05-31 23:35:31
11	Versure Ticket	1	5.00	2026-05-31 23:35:40
12	Voeds Redbull	1	12.00	2026-05-31 23:41:07
14	VP Ticket	3	75.00	2026-05-31 23:43:47
15	Voeds Redbull	2	24.00	2026-05-31 23:43:57
16	VP Ticket	1	25.00	2026-06-01 13:51:03
17	Pomstar Maroni	1	12.00	2026-06-01 13:51:08
18	VP Ticket	2	50.00	2026-06-01 13:51:08

.php dashboard

POS_FRAMEWORK_ARNO [Desktop] - Google Chrome

Bestand Machine Weergave Invoer Apparaat Help

7 jun 12:11

phpMyAdmin The Solus Club POS

http://localhost/pos.php

The Solus Club POS

Werkende demo: producten toevoegen aan bestelling, daarna betaling opslaan in MySQL.

VIP Ticket toegevoegd aan bestelling.

Producten

VIP Ticket Categorie: Ticket Prijs: €25.00 + Toevoegen	Vodka Redbull Categorie: Drink Prijs: €12.00 + Toevoegen	Vestaire Ticket Categorie: Service Prijs: €5.00 + Toevoegen	Pornstar Martini Categorie: Cocktail Prijs: €12.00 + Toevoegen	Jupiler Categorie: Drink Prijs: €2.00 + Toevoegen
--	--	---	--	---

Bestelling / winkelmandje

Product	Aantal	Prijs/stuk	Totaal	Actie
VIP Ticket	1	€25.00	€25.00	- Verwijder 1

Totaal te betalen: €25.00

Betalen Bestelling afsluiten

16°C Deurs zonnig

Zoeken

NLD BEP 12:11 7/06/2025

```
POS_EINDWERK_ARN0 [Draient] - Oracle VirtualBox
Bestand  Machine  Weergeven  Invoers  Apparaten  Help

7 jun 12:14
arno@arno-VirtualBox: /var/www/html

arno@arno-VirtualBox: /var/www/html$
arno@arno-VirtualBox: /var/www/html$ sudo systemctl st
start status stop
arno@arno-VirtualBox: /var/www/html$ sudo systemctl st
start status stop
arno@arno-VirtualBox: /var/www/html$ sudo systemctl status ap
apache2.service          apport-autoreport.path    apport-forward.socket     apt-daily.timer          apt-news.service
apache-htcacheclean.service  apport-autoreport.service  apport.service            apt-daily-upgrade.service
apparmor.service          apport-autoreport.timer    apt-daily.service         apt-daily-upgrade.timer
arno@arno-VirtualBox: /var/www/html$ sudo systemctl status apache2
[sudo] wachtwoord voor arno:
Warning: The unit file, source configuration file or drop-ins of apache2.service changed on disk. Run 'systemctl daemon-reload' to reload units.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-06-07 12:00:00 CEST; 10min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 1365 (apache2)
    Tasks: 11 (limit: 4596)
   Memory: 57.5M (peak: 62.1M)
      CPU: 1.123s
   CGroup: /system.slice/apache2.service
           └─1365 /usr/sbin/apache2 -k start
             1376 /usr/sbin/apache2 -k start
             1377 /usr/sbin/apache2 -k start
             1378 /usr/sbin/apache2 -k start
             1381 /usr/sbin/apache2 -k start
             4630 /usr/sbin/apache2 -k start
             4647 /usr/sbin/apache2 -k start
             4648 /usr/sbin/apache2 -k start
             4747 /usr/sbin/apache2 -k start
             4748 /usr/sbin/apache2 -k start
             4749 /usr/sbin/apache2 -k start

jun 07 11:59:59 arno-VirtualBox systemd[1]: Starting apache2.service - The Apache HTTP Server...
jun 07 12:00:00 arno-VirtualBox apache2[1346]: AH00557: apache2: apr_sockaddr_info_get() failed for arno-VirtualBox
jun 07 12:00:00 arno-VirtualBox apache2[1346]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directi
jun 07 12:00:00 arno-VirtualBox systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-26/26 (END)
```

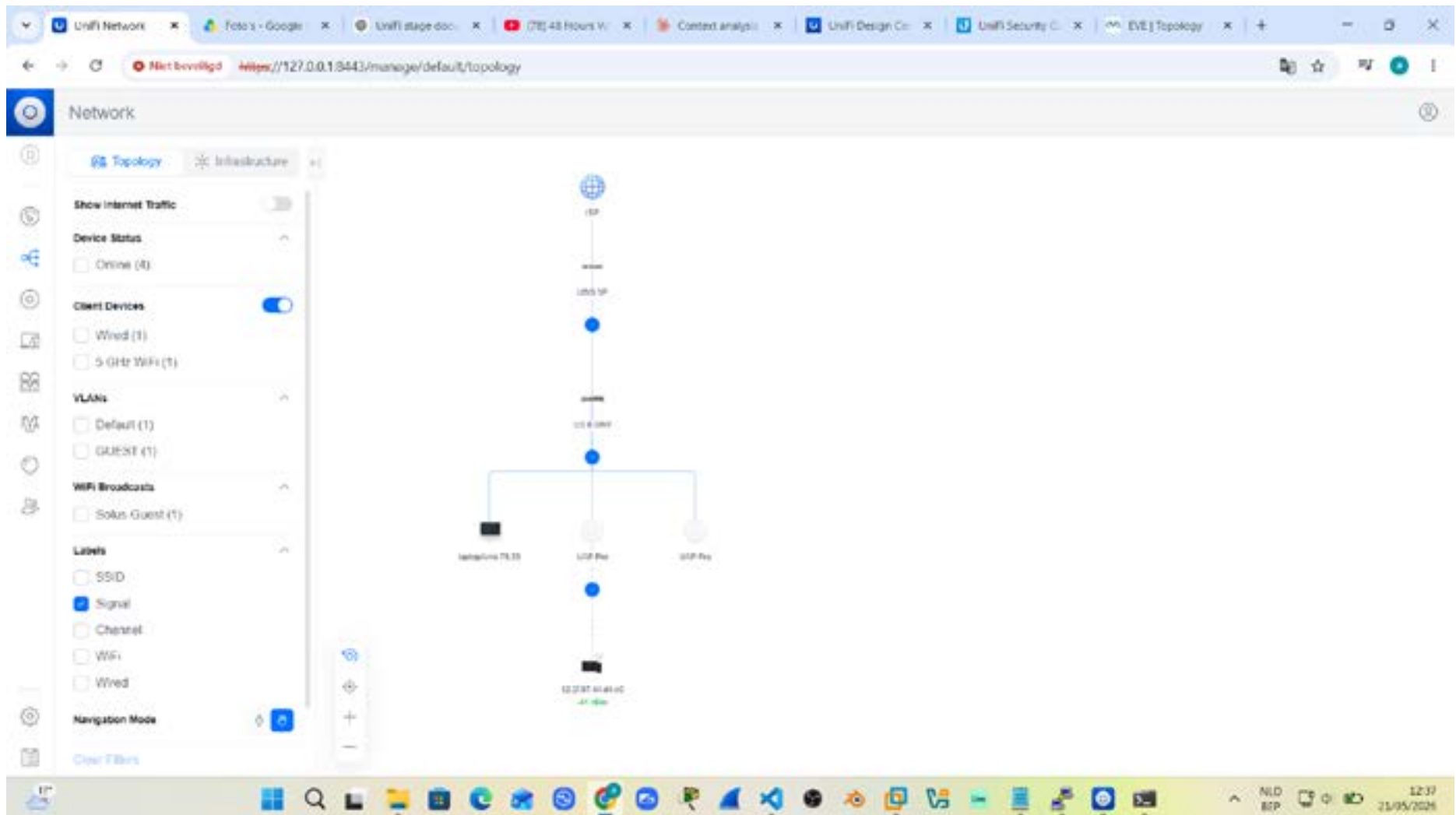
```
POS (NETWORK_ARNO) [Charles] - Oracle VM VirtualBox
Bestand Machine Weergeven Invoer Apparaten Help
7 jun 12:14
arno@arno-VirtualBox: /var/www/html$
arno@arno-VirtualBox: /var/www/html$
arno@arno-VirtualBox: /var/www/html$ sudo systemctl status mariadb
Warning: The unit file, source configuration file or drop-ins of mariadb.service changed on disk. Run 'systemctl daemon-reload' to reload units.
● mariadb.service - MariaDB 10.11.14 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: enabled)
   Active: active (running) since Sun 2026-06-07 12:00:01 CEST; 14min ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 1445 (mariadb)
   Status: "Taking your SQL requests now..."
     Tasks: 11 (limit: 3038)
   Memory: 128.5M (peak: 136.4M)
      CPU: 1.636s
   CGroup: /system.slice/mariadb.service
           └─1445 /usr/sbin/mariadb

jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] InnoDB: log sequence number 72545; transaction id 82
jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/lb_buffer_pool
jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] Plugin 'FEEDBACK' is disabled.
jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Warning] You need to use --log-bin to make --expire-logs-days or --binlog-expire-logs-seconds work.
jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] Server socket created on IP: '127.0.0.1', port: '3306'.
jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] InnoDB: Buffer pool(s) load completed at 260697 12:00:01
jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] /usr/sbin/mariadb: ready for connections.
jun 07 12:00:01 arno-VirtualBox system[1]: Started mariadb.service - MariaDB 10.11.14 database server.
jun 07 12:00:01 arno-VirtualBox /etc/mysql/debian-start[1499]: Upgrading MariaDB tables if necessary.
arno@arno-VirtualBox: /var/www/html$
```

H9 - Testing & Validatie

9.1 VLAN & Firewall regels aanmaken test op stage

Op stage kreeg ik de kans om te testen met een USG 3P router en US 8 60W switch, en 2 UAP Pro access points. Ik heb deze devices succesvol kunnen adopteren.



Hier zie je mijn device list van het test op lab op stage, na succesvol alle devices te adopteren staat er bij de status van elk device nu Up To Date

The screenshot shows the UniFi Network management interface in a web browser. The left sidebar contains navigation options: Status, UniFi Devices, Models, Supervision, Uptime, and Install Date. The main area displays a table of devices with the following columns: Type, Name, Application, Status, IP Address, Uplink, Parent Device, Ch. 2.4 G..., Ch. 5 GHz, and Ch. 5 GHz. All devices listed have a status of 'Up to date'.

Type	Name	Application	Status	IP Address	Uplink	Parent Device	Ch. 2.4 G...	Ch. 5 GHz	Ch. 5 GHz
USG 3P	USG 3P	Network	Up to date	192.168.1.1	E	-	-	-	-
US 8 60W	US 8 60W	Network	Up to date	192.168.1.7	GbE	USG 3P Port 1	-	-	-
UAP Pro	UAP Pro	Network	Up to date	192.168.1.8	-	-	-	-	-
UAP Pro	UAP Pro	Network	Up to date	192.168.1.9	GbE	US 8 60W Port 6	11 (20 MHz)	36 (40 MHz)	-

Binnen deze testomgeving werden verschillende VLANs aangemaakt voor personeel, gasten, camera's en POS-systemen. Elke VLAN kreeg een eigen subnet en DHCP-configuratie. Hierdoor konden netwerksegmenten logisch van elkaar gescheiden worden. Deze testomgeving werd gebruikt om VLAN-configuratie, routing en netwerksegmen-

The screenshot displays the UniFi Network Manager web interface. The left sidebar contains navigation options: Overview, WiFi, Networks (selected), Internet, VPN, CyberSecure, High Availability, Policy Engine, and System. The main content area shows a table of configured networks.

Name	VLAN ID	Router	Subnet	IPv6 Subnet	DHCP	IP Leases	Available
Default	1	USG 3P	192.168.1.0/24	-	Server	- /2	240
STAFF	10	USG 3P	192.168.2.0/24	-	Server	- /2	240
GUEST	20	USG 3P	192.168.3.0/24	-	Server	- /2	240
CAMERAS	30	USG 3P	192.168.4.0/24	-	Server	- /2	240
POS	40	USG 3P	192.168.5.0/24	-	Server	- /2	240

Below the table, there are sections for 'Default Security Posture' (Allow All selected), 'Gateway mDNS Proxy' (Auto selected), 'iCMP Snooping' (unchecked), 'L3 Network Isolation (ACL)' (unchecked), 'Device Isolation (ACL)' (unchecked), 'Network Lists' (Create New), and 'RADIUS Servers' (Create New, Local Credentials, Manage). The bottom status bar shows the time as 12:00 on 21/05/2024.

Tijdens de implementatie werden firewallregels geconfigureerd binnen de Uni-Fi Controller om de verschillende VLANs van elkaar te scheiden. Door gebruik te maken van LAN IN-regels wordt ongewenste communicatie tussen netwerksegmenten geblokkeerd.

The screenshot displays the UniFi Network Controller web interface. The browser address bar shows the URL <https://127.0.0.1:8443/manage/default/settings/traffic-and-firewall-rules/firewall-rules>. The left sidebar contains navigation options: Overview, WiFi, Networks, Internet, VPN, CyberSecure, High Availability, Policy Engine, and System. The main content area is titled 'Network' and shows a list of firewall rules. The 'LAN (13)' tab is selected. The rules are categorized by 'LAN In' and 'LAN Out'. The table below lists the rules:

Name	Action	Type	Protocol	Source	Port	Destination	Port	ID
BLOCK_GUEST_TO_DEFAULT	Drop	LAN In	All	GUEST	Any	Default	Any	2000
BLOCK_CAMERAS_TO_LAN	Drop	LAN In	All	CAMERAS	Any	Default	Any	2001
BLOCK_POS_TO_LAN	Accept	LAN In	All	POS	Any	Default	Any	2002
Allow Network 192.168.1.0/24 Traffic	Accept	LAN In	All	Any	Any	Any	Any	6001
Allow Network 192.168.2.0/24 Traffic	Accept	LAN In	All	Any	Any	Any	Any	6002
Allow Network 192.168.3.0/24 Traffic	Accept	LAN In	All	Any	Any	Any	Any	6003
Allow Network 192.168.4.0/24 Traffic	Accept	LAN In	All	Any	Any	Any	Any	6004
Allow Network 192.168.5.0/24 Traffic	Accept	LAN In	All	Any	Any	Any	Any	6005
Allow Network 192.168.1.0/24 Traffic	Accept	LAN Out	All	Any	Any	Any	Any	6001
Allow Network 192.168.2.0/24 Traffic	Accept	LAN Out	All	Any	Any	Any	Any	6002
Allow Network 192.168.3.0/24 Traffic	Accept	LAN Out	All	Any	Any	Any	Any	6003
Allow Network 192.168.4.0/24 Traffic	Accept	LAN Out	All	Any	Any	Any	Any	6004
Allow Network 192.168.5.0/24 Traffic	Accept	LAN Out	All	Any	Any	Any	Any	6005

At the bottom of the table, there are links: 'Create Entry', 'Create List', and 'Manage'. The bottom status bar shows the time as 12:21 on 21/05/2026.

Binnen de UniFi TEST omgeving werden twee SSID's aangemaakt: Solus-Guest (VLAN 20) en Solus-Staff (VLAN 10).

Het gastennetwerk werd enkel uitgezonden via de UAP Pro access point voor bezoekers, terwijl het personeelsnetwerk beschikbaar bleef op alle access points. Hierdoor wordt de Wi-Fi-dekking afgestemd op de gebruikers en blijft het netwerk beter beheerbaar en beveiligd.

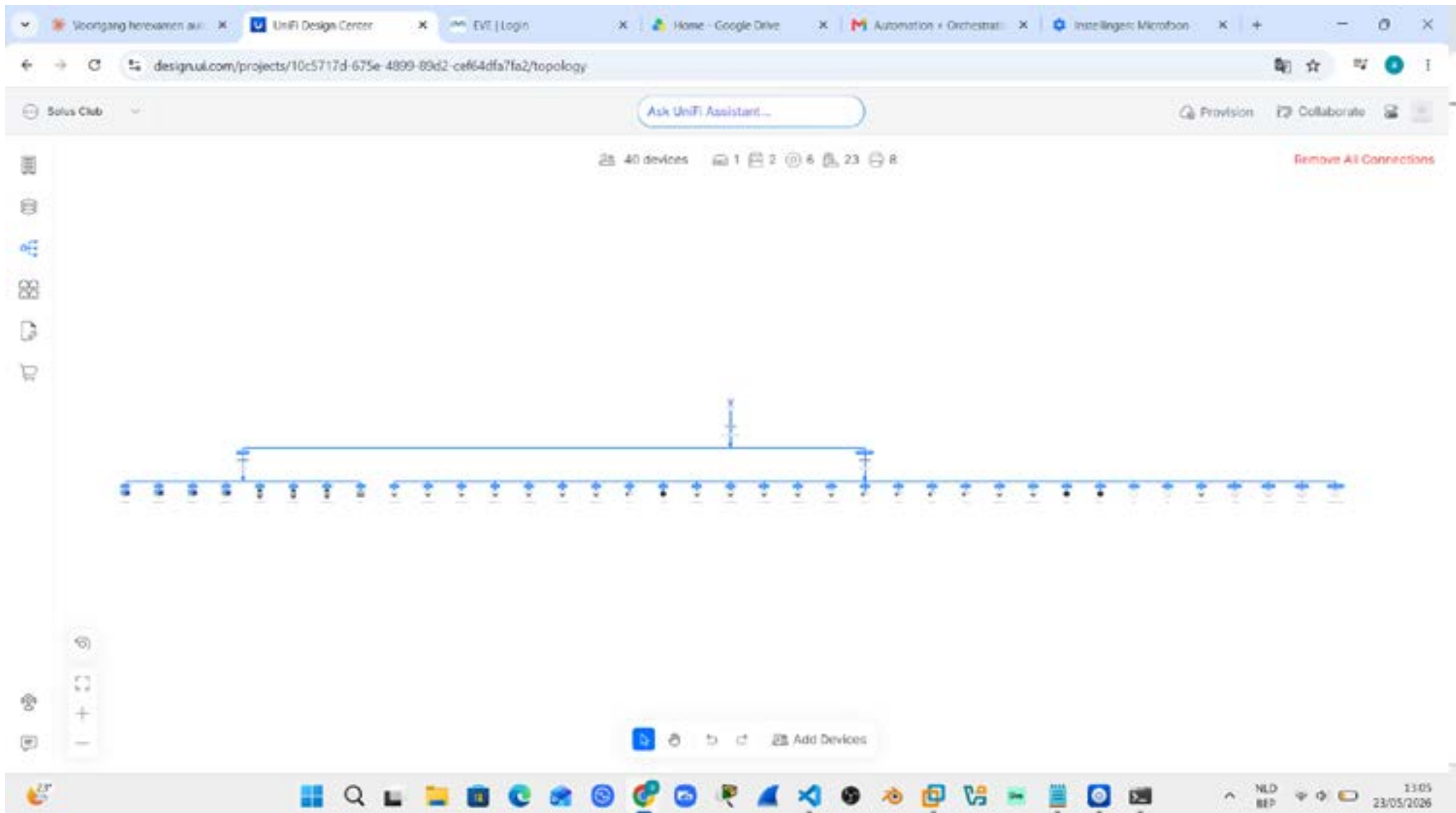
The screenshot shows the UniFi Network Controller interface. The left sidebar contains navigation options: Overview, WiFi, Networks, Internet, VPN, CyberSecure, High Availability, Policy Engine, and System. The main content area is titled 'Network' and shows a table of configured networks.

Name	Network	Broadcasting APs	Radio Band	Clients	Security
Solus-Guest	GUEST (20)	UAP Pro	2.4 GHz 5 GHz	-	Open
Solus-Staff	STAFF (10)	All APs	2.4 GHz 5 GHz	-	WPA2

Below the table, there are links for 'Create New' and 'Manage'. The 'Channel Plan' section shows a visual representation of the 2.4 GHz and 5 GHz frequency bands, with channels 1-14 for 2.4 GHz and channels 36-160 for 5 GHz. The 'Default WiFi Speeds' section shows options for 'Maximum Speed', 'Conservative', and 'Custom', with 'Conservative' selected.

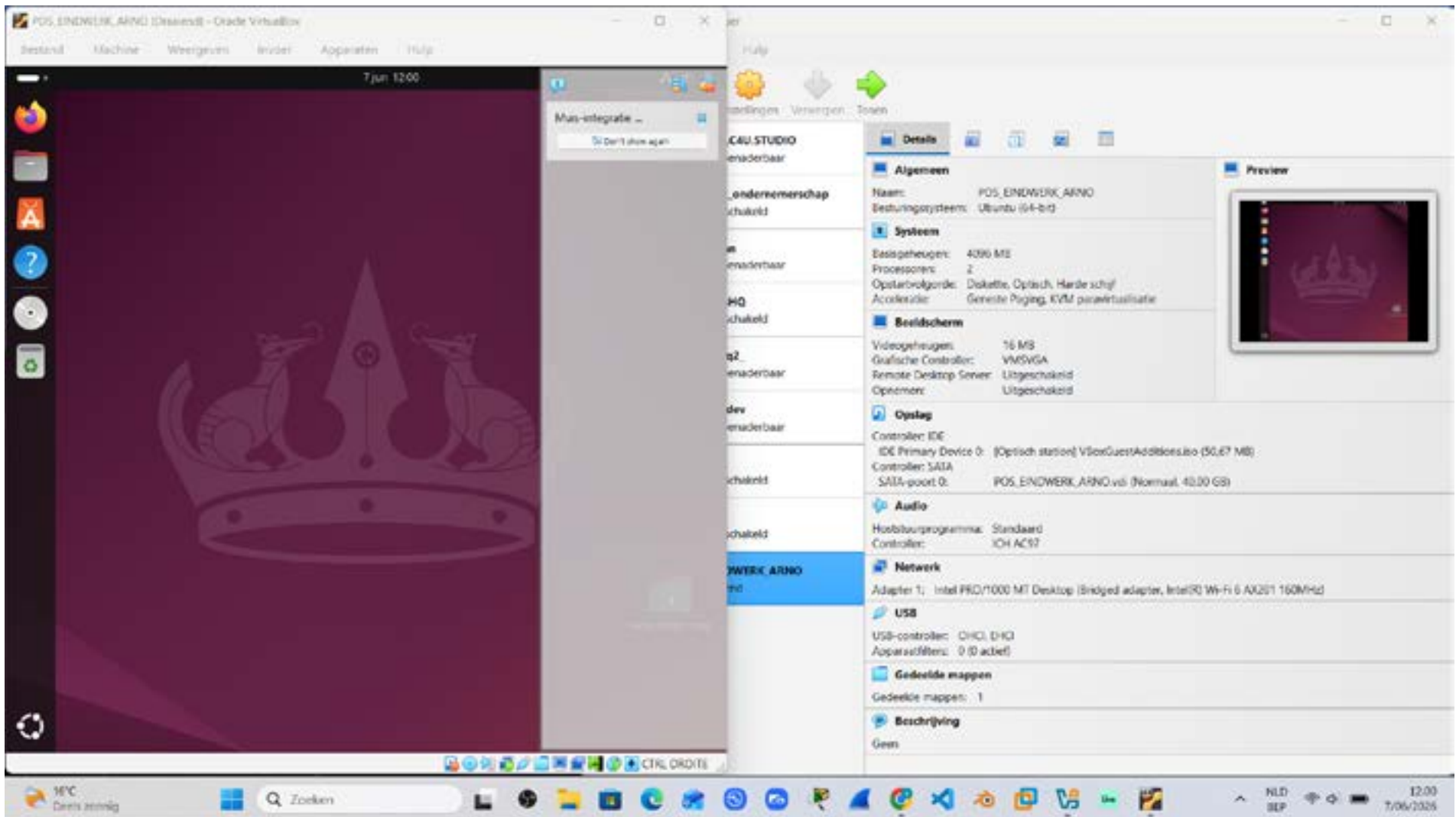
9.2 UniFi Testing

Alle devices in UniFi design center gebruikt om zo deze topology te zien te krijgen



9.3 POS Testing

Ubuntu desktop draait in virtualbox als test omgeving



Apache2 service active

The screenshot shows a terminal window titled "POS_JINOWEB_ARNO [Draaien] - Oracle VM VirtualBox". The user is logged in as arno@arno-VirtualBox. The terminal shows the following commands and output:

```
arno@arno-VirtualBox: /var/www/html$ sudo systemctl start status stop
arno@arno-VirtualBox: /var/www/html$ sudo systemctl status ap
apache2.service                                apt-daily.timer                                apt-news.service
apache2.service                                apt-daily-upgrade.service
apparmor.service                                apt-daily-upgrade.timer
```

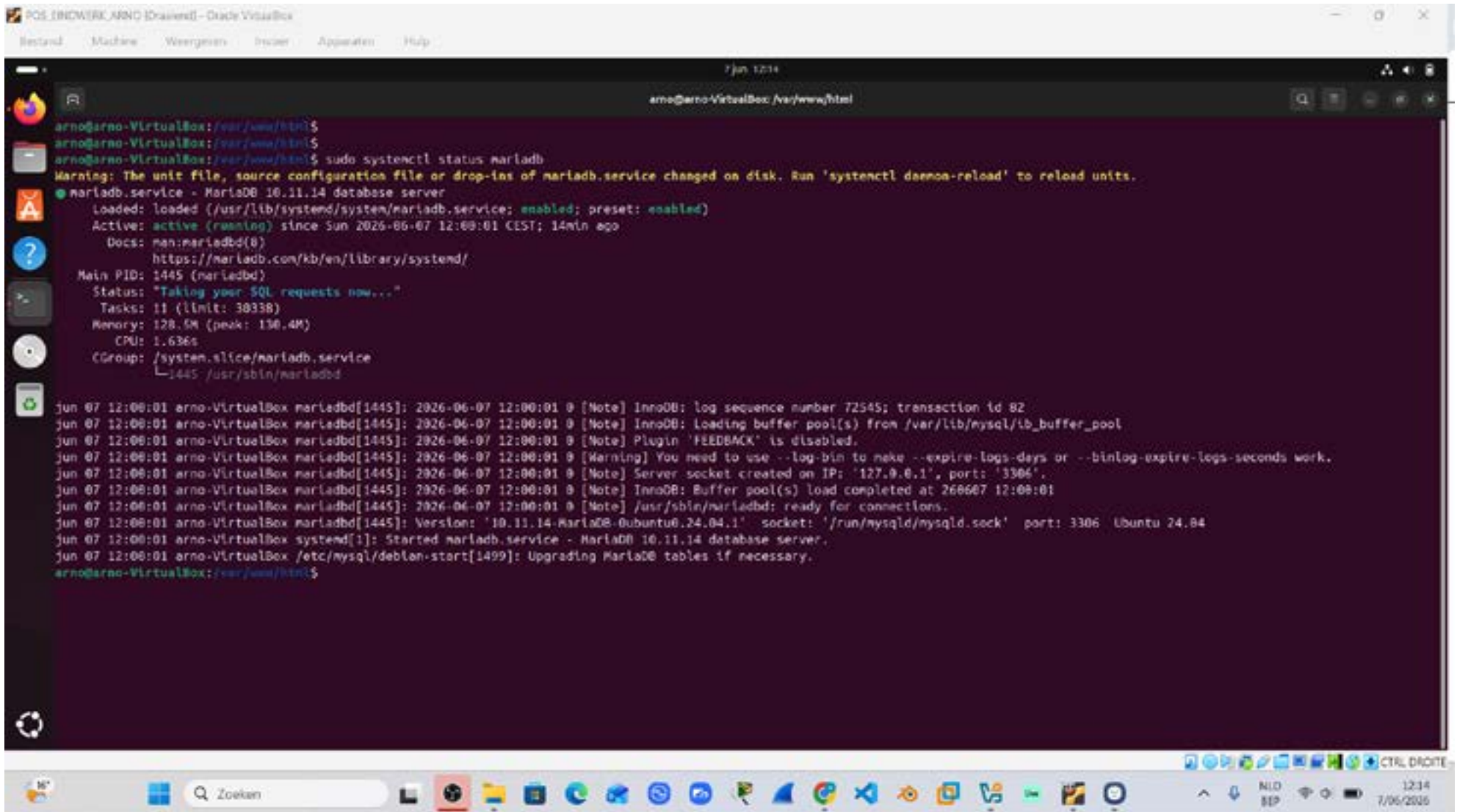
The user then runs `sudo systemctl status apache2`, which shows the service is active and running. The output includes a warning about unit file changes and a list of tasks for the service.

```
[sudo] wachtwoord voor arno:
Warning: The unit file, source configuration file or drop-ins of apache2.service changed on disk. Run 'systemctl daemon-reload' to reload units.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Sun 2026-06-07 12:09:00 CEST; 14min ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 1365 (apache2)
      Tasks: 11 (limit: 4596)
     Memory: 57.5M (peak: 62.1M)
        CPU: 1.123s
    CGroup: /system.slice/apache2.service
            └─1365 /usr/sbin/apache2 -k start
              1376 /usr/sbin/apache2 -k start
              1377 /usr/sbin/apache2 -k start
              1378 /usr/sbin/apache2 -k start
              1381 /usr/sbin/apache2 -k start
              1638 /usr/sbin/apache2 -k start
              1647 /usr/sbin/apache2 -k start
              1648 /usr/sbin/apache2 -k start
              1747 /usr/sbin/apache2 -k start
              1748 /usr/sbin/apache2 -k start
              1749 /usr/sbin/apache2 -k start

jun 07 11:59:59 arno-VirtualBox systemd[1]: Starting apache2.service - The Apache HTTP Server...
jun 07 12:09:00 arno-VirtualBox apache2[1346]: AH00557: apache2: apr_sockaddr_info_get() failed for arno-VirtualBox
jun 07 12:09:00 arno-VirtualBox apache2[1346]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive
jun 07 12:09:00 arno-VirtualBox systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-26/26 (END)
```

The terminal window also shows the system's taskbar at the bottom with various application icons and the date/time (12:14 7/06/2026).

Mariadb active

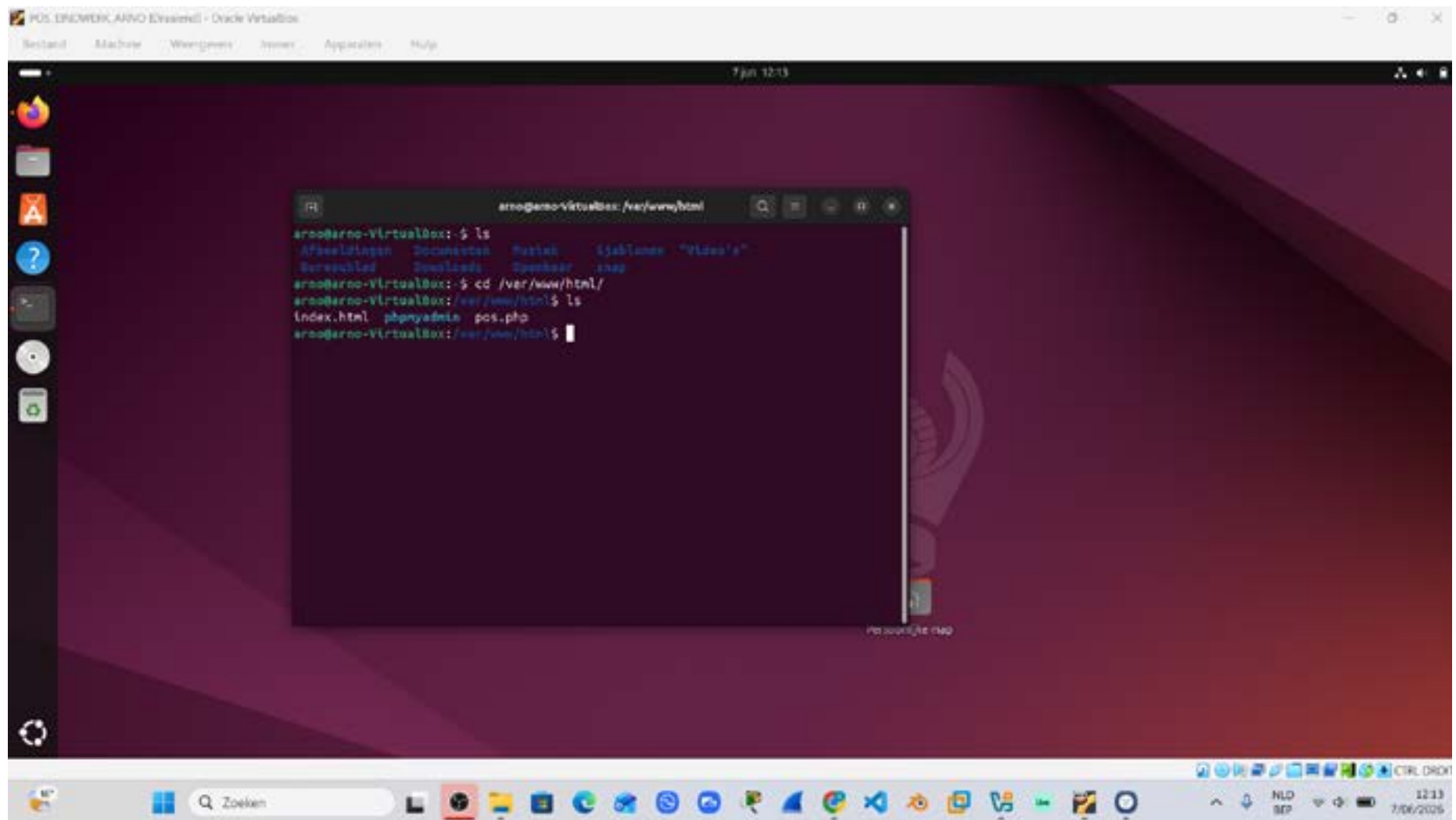


```
PS: [BROWSE_ARNO] (Drawn) - Oracle VM VirtualBox
File Transfer Machine Weergaven Invoer Apparaten Help

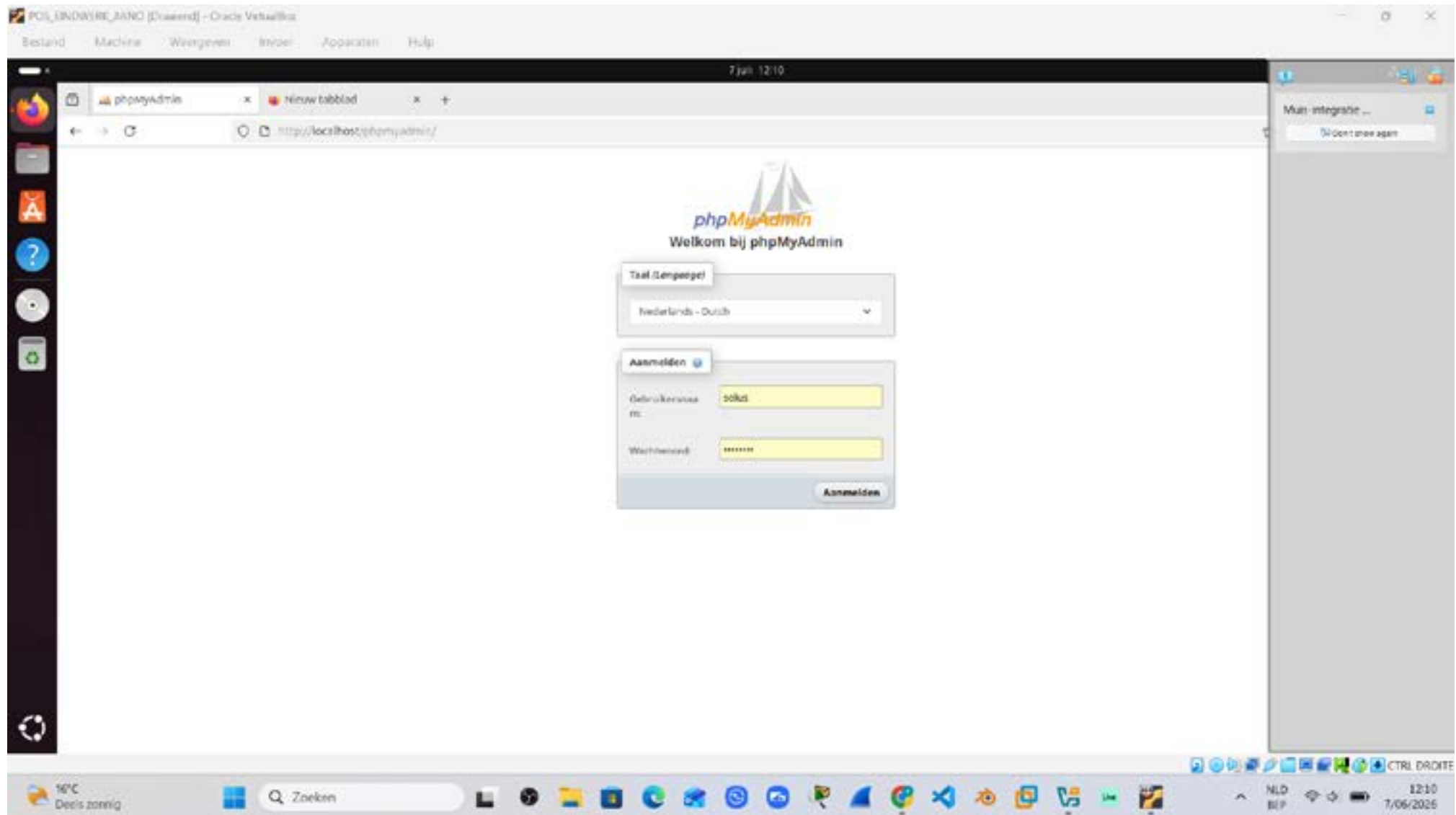
7 Jun 12:14
arno@arno-VirtualBox: /var/www/html

arno@arno-VirtualBox: /var/www/html$
arno@arno-VirtualBox: /var/www/html$
arno@arno-VirtualBox: /var/www/html$ sudo systemctl status mariadb
Warning: The unit file, source configuration file or drop-ins of mariadb.service changed on disk. Run 'systemctl daemon-reload' to reload units.
● mariadb.service - MariaDB 10.11.14 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: enabled)
   Active: active (running) since Sun 2026-06-07 12:00:01 CEST; 14min ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 1445 (mariadb)
   Status: "Taking your SQL requests now..."
     Tasks: 11 (limit: 30338)
    Memory: 128.5M (peak: 130.4M)
       CPU: 1.636s
   CGroup: /system.slice/mariadb.service
           └─1445 /usr/sbin/mariadb

Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] InnoDB: log sequence number 72545; transaction id 82
Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/ib_buffer_pool
Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] Plugin 'FEEDBACK' is disabled.
Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Warning] You need to use --log-bin to make --expire-logs-days or --binlog-expire-logs-seconds work.
Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] Server socket created on IP: '127.0.0.1', port: '3306'.
Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] InnoDB: Buffer pool(s) load completed at 260607 12:00:01
Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: 2026-06-07 12:00:01 0 [Note] /usr/sbin/mariadb: ready for connections.
Jun 07 12:00:01 arno-VirtualBox mariadb[1445]: Version: '10.11.14-MariaDB-0ubuntu0.24.04.1' socket: '/run/mysqld/mysqld.sock' port: 3306 Ubuntu 24.04
Jun 07 12:00:01 arno-VirtualBox systemd[1]: Started mariadb.service - MariaDB 10.11.14 database server.
Jun 07 12:00:01 arno-VirtualBox /etc/mysql/debian-start[1499]: Upgrading MariaDB tables if necessary.
arno@arno-VirtualBox: /var/www/html$
```



Phpmyadmin inlog scherm



Solus Club POS dashboard: pos.php

The screenshot shows a web browser window displaying the 'The Solus Club POS' dashboard. The browser's address bar shows the URL 'http://localhost/pos.php'. The dashboard has a dark theme and a sidebar on the left with icons for home, help, and other functions. The main content area is divided into sections: a header with the title 'The Solus Club POS' and a subtitle 'Werken de dier: producten toevoegen aan bestelling, daarna betaling opslaan in MariaDB.', a green notification bar stating 'VIP Ticket toegevoegd aan bestelling.', a 'Producten' section with five product cards, and a 'Bestelling / winkelmandje' section with a table of the current order.

Producten

Product	Categorie	Prijs	Actie
VIP Ticket	Ticket	€25.00	+ Toevoegen
Vodka Redbull	Drink	€12.00	+ Toevoegen
Vestaire Ticket	Service	€5.00	+ Toevoegen
Pornstar Martini	Cocktail	€12.00	+ Toevoegen
Jupiler	Drink	€2.00	+ Toevoegen

Bestelling / winkelmandje

Product	Aantal	Prijs/stuk	Totaal	Actie
VIP Ticket	1	€25.00	€25.00	- Verwijder 1

Totaal te betalen: €25.00

Buttons: Betalen, Bestelling wissen

Products

The screenshot shows the phpMyAdmin interface for a database named 'solus'. The 'products' table is selected, and its structure is displayed. The table has the following columns: **id**, **product_name**, **price**, and **category**. There are 5 records in the table.

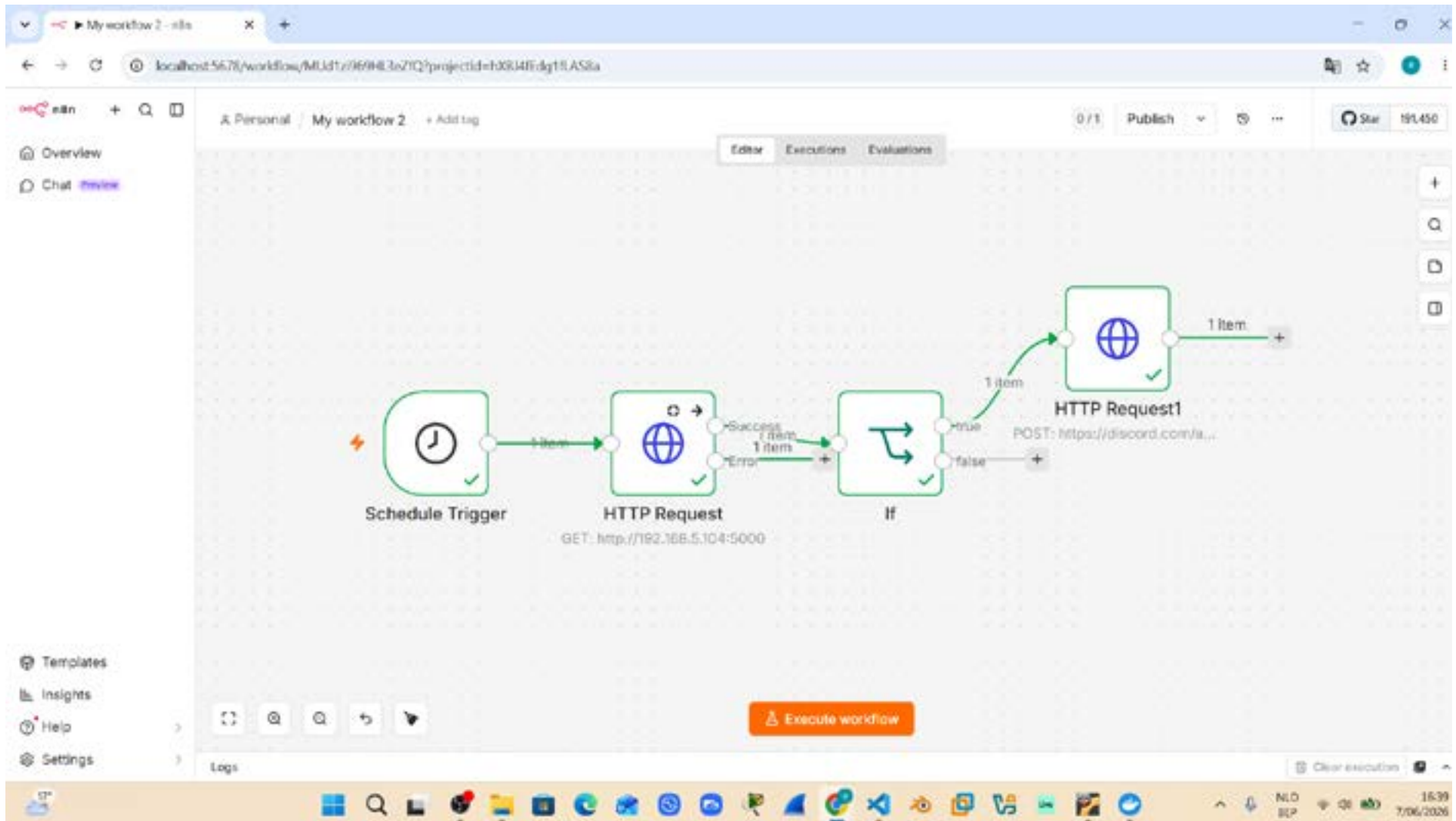
id	product_name	price	category
1	VIP Ticket	25.00	Ticket
2	Vodka Redbull	12.00	Drink
3	Vestaire Ticket	5.00	Service
4	Pornstar Martini	12.00	Cocktail
5	Jupiler	2.00	Drink

Orders

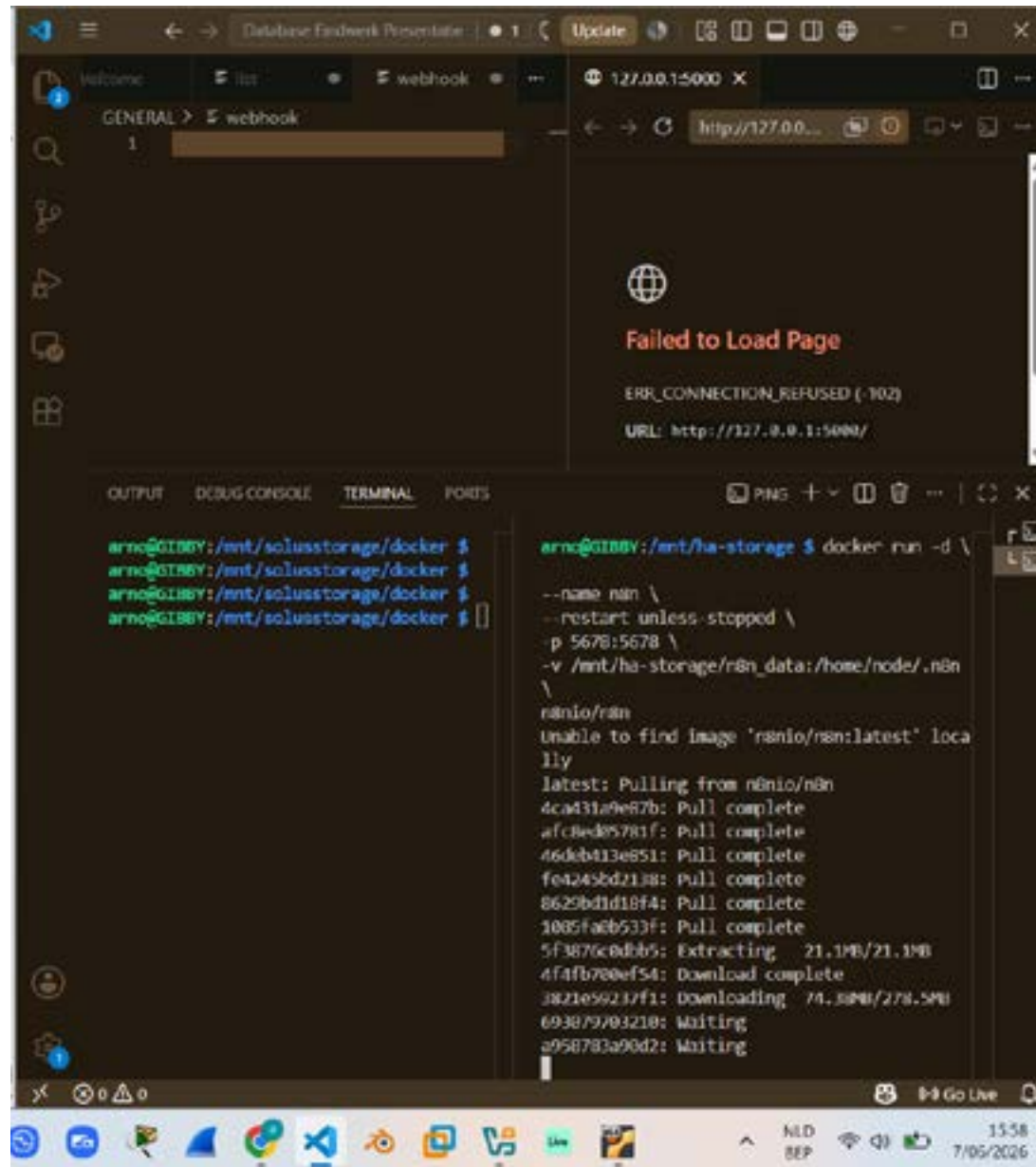
The screenshot shows a web browser window displaying the phpMyAdmin interface. The browser address bar shows the URL: `http://localhost:8080/phpmyadmin/index.php?route=/solusclub_pos/solusclub_pos/solusclub_pos/orders`. The phpMyAdmin interface is open, showing the 'orders' table selected. The table structure is as follows:

id	product name	quantity	total price	timestamp
1	VIP Ticket	1	25.00	2025-05-31 22:38:46
2	Vodka Redbull	1	12.00	2025-05-31 22:38:46
3	vinstalen Ticket	1	5.00	2025-05-31 22:38:46
4	Purestar Martini	1	12.00	2025-05-31 22:38:46
5	jupiler	1	2.00	2025-05-31 22:38:46
6	VIP Ticket	1	25.00	2025-05-31 23:34:08
7	VIP Ticket	1	25.00	2025-05-31 23:34:13
8	jupiler	1	2.00	2025-05-31 23:34:29
9	jupiler	1	2.00	2025-05-31 23:34:29
10	Vodka Redbull	1	12.00	2025-05-31 23:35:31
11	vinstalen Ticket	1	5.00	2025-05-31 23:35:40
12	Vodka Redbull	1	12.00	2025-05-31 23:41:00
13	Vodka Redbull	1	12.00	2025-05-31 23:41:00
14	VIP Ticket	3	75.00	2025-05-31 23:43:47
15	Vodka Redbull	2	24.00	2025-05-31 23:43:47
16	Vodka Redbull	1	12.00	2025-06-03 13:51:03
17	Purestar Martini	1	12.00	2025-06-03 13:51:03
18	VIP Ticket	2	50.00	2025-06-03 13:51:03

9.4 Raspberry Pi server discord notification



Download N8N met docker container



Schedule trigger

Binnen n8n werd een Schedule Trigger gebruikt om de workflow automatisch op vaste tijdsintervallen uit te voeren. Hierdoor kan de status van de Raspberry Pi en de gate controller periodiek gecontroleerd worden zonder manuele tussenkomst.

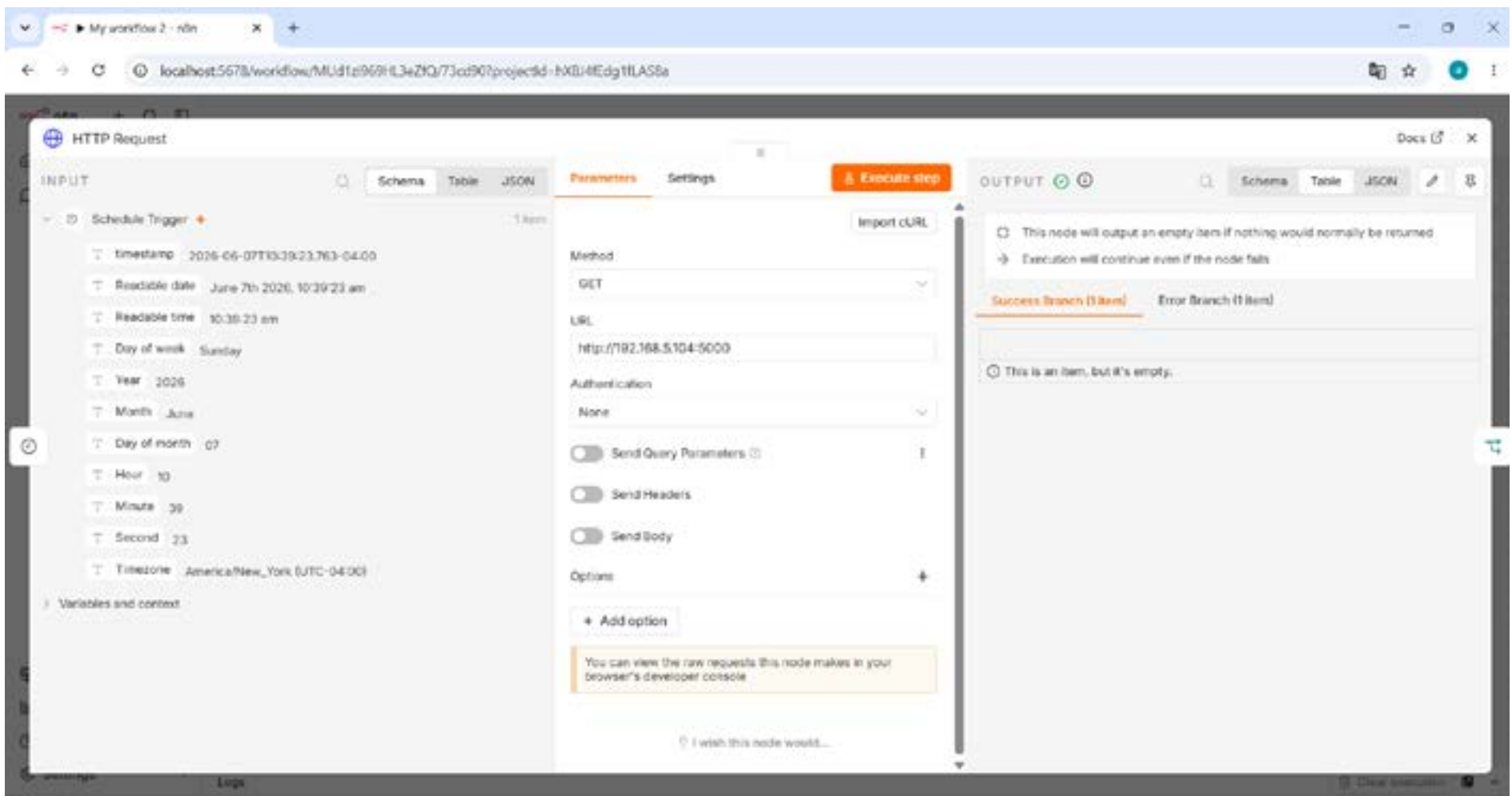
The screenshot shows the n8n web interface in a browser. The 'Schedule Trigger' node is selected, and its 'Settings' tab is active. The 'Trigger Rules' section shows a single rule with a 'Trigger Interval' of 'Minutes' and 'Minutes Between Triggers' set to '1'. The 'Execute step' button is visible. The 'OUTPUT' section displays a table with the following data:

timestamp	Readable date	Readable time	Day of week	Year	Month	Day of month	Hour	Minute	Second	Timezone
2026-06-07T10:39:23.763-04:00	June 7th 2026, 10:39 am	10:39:23 am	Sunday	2026	June	07	10	39	23	America (UTC-04:00)

The interface also includes a 'Parameters' tab, a 'Settings' tab, and an 'Execute step' button. A note states: 'This workflow will run on the schedule you define here once you publish it. For testing, you can also trigger it manually by going back to the canvas and clicking "execute workflow".'

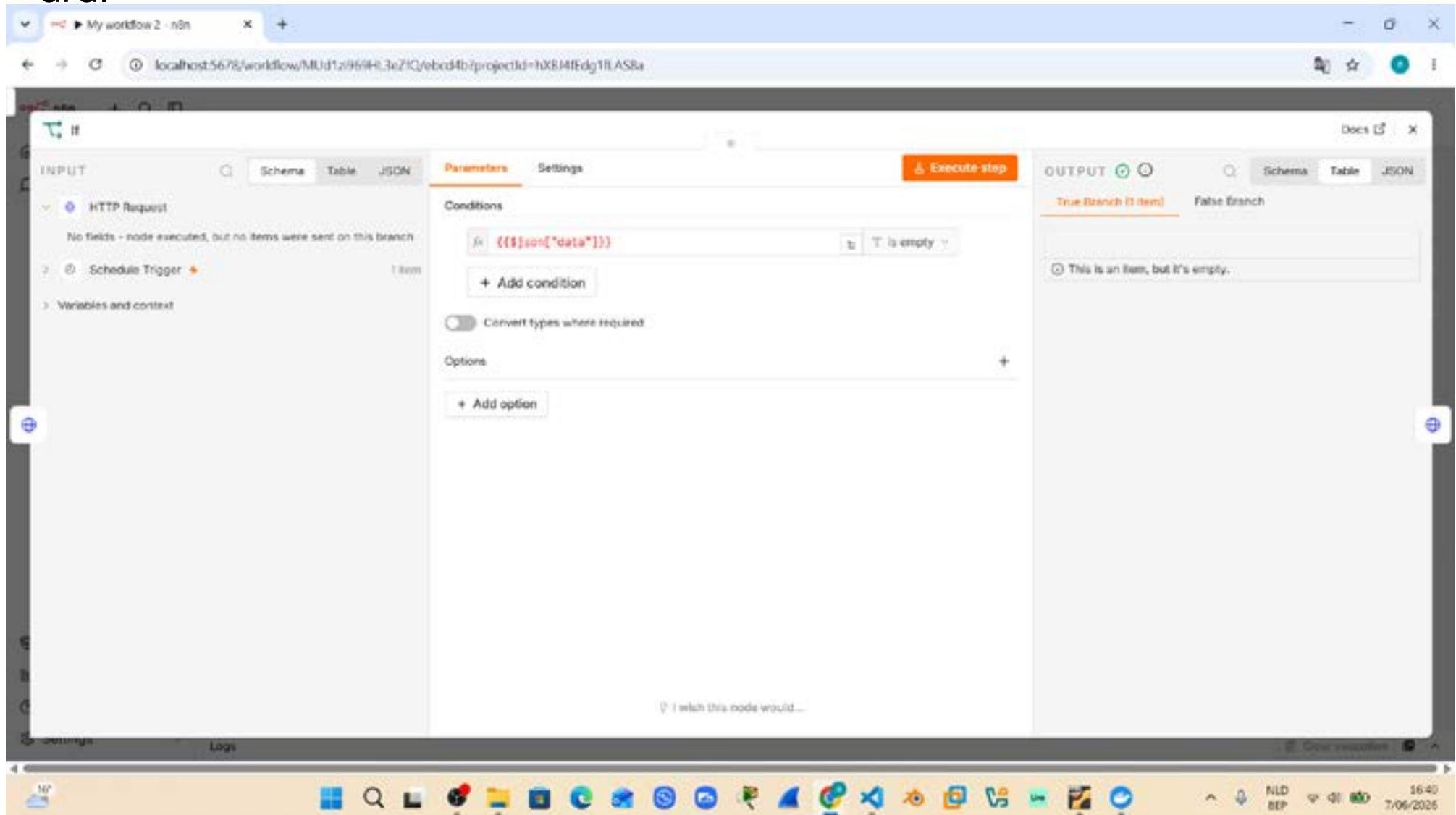
HTTP request

Via een HTTP Request controleert n8n of de Flask-webserver op de Raspberry Pi bereikbaar is. Indien de server niet reageert, wordt de workflow automatisch doorgestuurd naar de foutafhandeling.



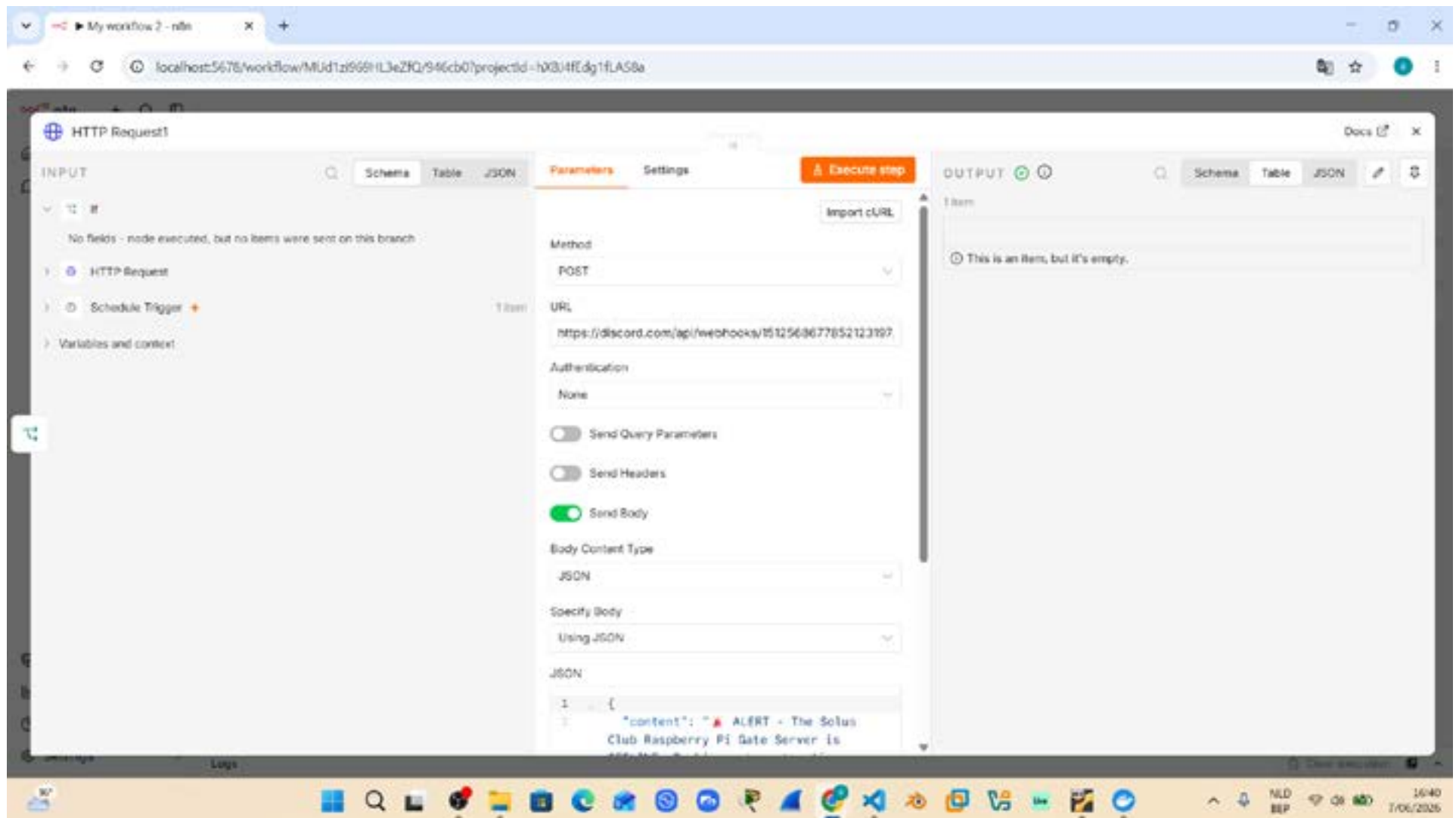
IF Node

Met behulp van een IF-node wordt gecontroleerd of de Raspberry Pi een geldige respons terugstuurt. Op basis van deze controle bepaalt n8n of de infrastructuur operationeel is of dat een waarschuwing moet worden verstuurd.



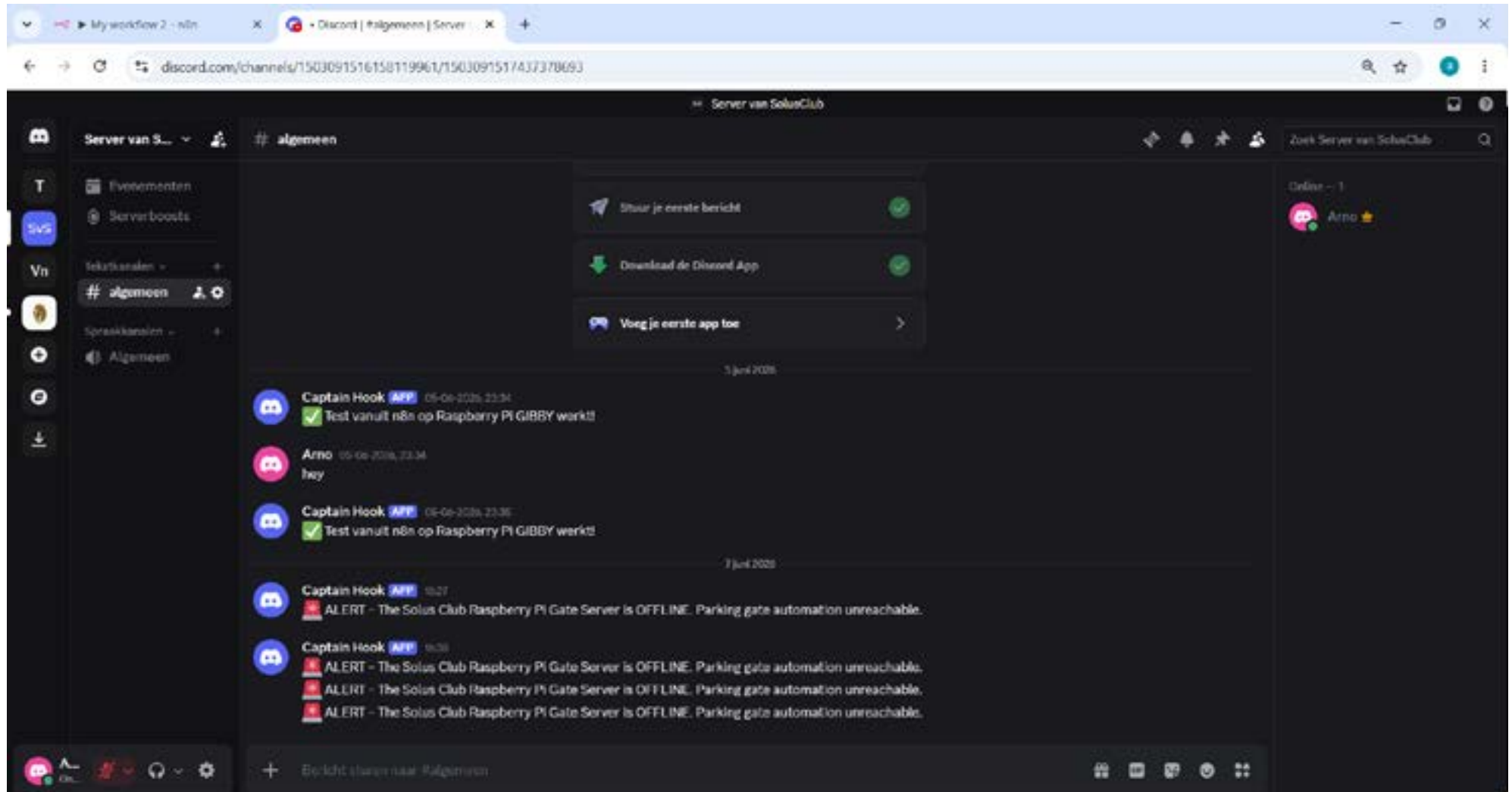
IF Node

Wanneer de Raspberry Pi niet bereikbaar is, verstuurt n8n automatisch een melding via een Discord webhook. Hierdoor kunnen problemen snel gedetecteerd worden zonder voortdurend de systemen handmatig te controleren.



Resultaat in Discord

Tijdens de test werd succesvol een Discord-melding gegenereerd wanneer de Raspberry Pi niet bereikbaar was. Hiermee werd aangetoond dat de monitoringworkflow correct functioneert en automatisch waarschuwingen kan versturen bij storingen.



H10 – UniFi Access

Wat is UniFi Access

UniFi Access is een fysiek toegangscontrolesysteem ontwikkeld door Ubiquiti waarmee deuren, poorten en beveiligde ruimtes centraal beheerd kunnen worden. Het systeem maakt gebruik van controllers, badgelezers en toegangsrechten om te bepalen welke gebruikers toegang krijgen tot specifieke locaties.

Het platform maakt deel uit van het bredere UniFi-ecosysteem en kan geïntegreerd worden met andere UniFi toepassingen zoals netwerkbeheer en camerabewaking. Hierdoor ontstaat één centraal beheersplatform voor meerdere beveiligingscomponenten.

Authenticatie kan gebeuren via NFC-badges, kaarten, mobiele toepassingen of andere ondersteunde identificatiemethoden. Toegangsrechten worden centraal beheerd waardoor wijzigingen snel kunnen worden toegepast.



Hoe maak je nieuwe badges/gebruikers aan in UniFi Access

UniFi Access maakt het mogelijk om gebruikers, bezoekers en medewerkers centraal te beheren via de UniFi Access applicatie.

Beheerders kunnen nieuwe gebruikers aanmaken en toegangsrechten toekennen op basis van functie of locatie. Per gebruiker kunnen één of meerdere NFC-badges, mobiele credentials of toegangscode's gekoppeld worden.

Daarnaast kunnen toegangsschema's worden ingesteld zodat bepaalde deuren enkel toegankelijk zijn tijdens specifieke tijdsvensters. Alle toegangsgebeurtenissen worden geregistreerd waardoor beheerders kunnen controleren wie wanneer een ruimte heeft betreden.

Door gebruik te maken van gecentraliseerd toegangsbeheer wordt het beheer van badges en toegangsrechten aanzienlijk vereenvoudigd.



<https://www.youtube.com/watch?v=EbolyOTDwRk>

In deze video wordt duidelijk uitgelegd hoe unifi access application 1.5.9 werkt en er uit ziet

Register admin access card

UniFi Access ondersteunt het gebruik van NFC-kaarten voor authenticatie en toegangscontrole. Nieuwe toegangskaarten kunnen eenvoudig worden geregistreerd via de UniFi Access Controller en vervolgens gekoppeld worden aan specifieke gebruikers of medewerkers. Tijdens de registratie wordt een unieke NFC-kaart toegewezen aan een gebruiker waarna toegangsrechten kunnen worden ingesteld op basis van deuren, zones of tijdschema's. Hierdoor kan bepaald worden welke personen toegang hebben tot specifieke ruimtes binnen een gebouw.

Alle kaartactiviteiten worden centraal geregistreerd binnen het systeem waardoor toegang-slogs, toegangsaanvragen en beveiligingsincidenten eenvoudig opgevolgd kunnen worden. Bij verlies van een kaart kan deze onmiddellijk gedeactiveerd worden zonder fysieke aanpassingen aan het toegangscontrolesysteem.



Step 2 of 4

Register Admin Access Card

Provision UniFi Access Card for the best security of any NFC cards.

Choose a reader, and tap an NFC card on it.



Main Door - 1F - Enter



NFC Card Number

100001



[Register Access Cards for More People](#)

< Back

Next >

UniFi Access

UBIQUITI UniFi UA Hub Door Mini Access Network Controller | Door Hub Mini

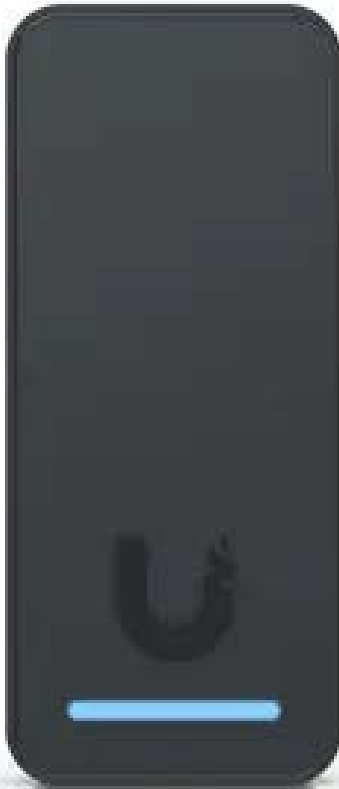
Prijs: €108



UniFi Access

UBIQUITI UniFi UA-G2-Black PoE NFC Card Reader

Prijs: €175



UBIQUITI UniFi UA-Card-B-10 Access Card

Prijs: €30 voor 10 stuks



UniFi Access

Ubiquiti Fail-Safe Strike Lock

Prijs: €100



UBIQUITI UniFi UA Button Access Button

Prijs: €40

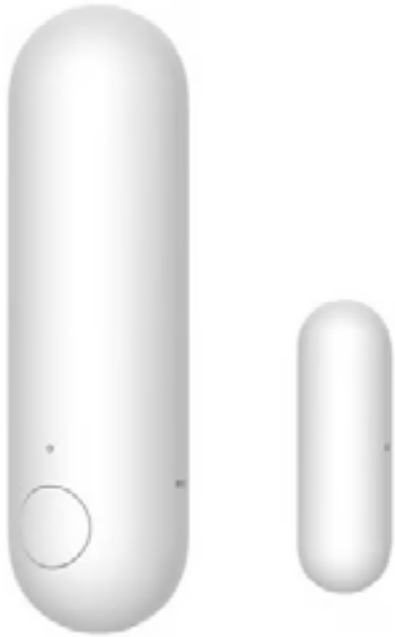


UniFi Access

Aqara door sensor

Prijs: €30

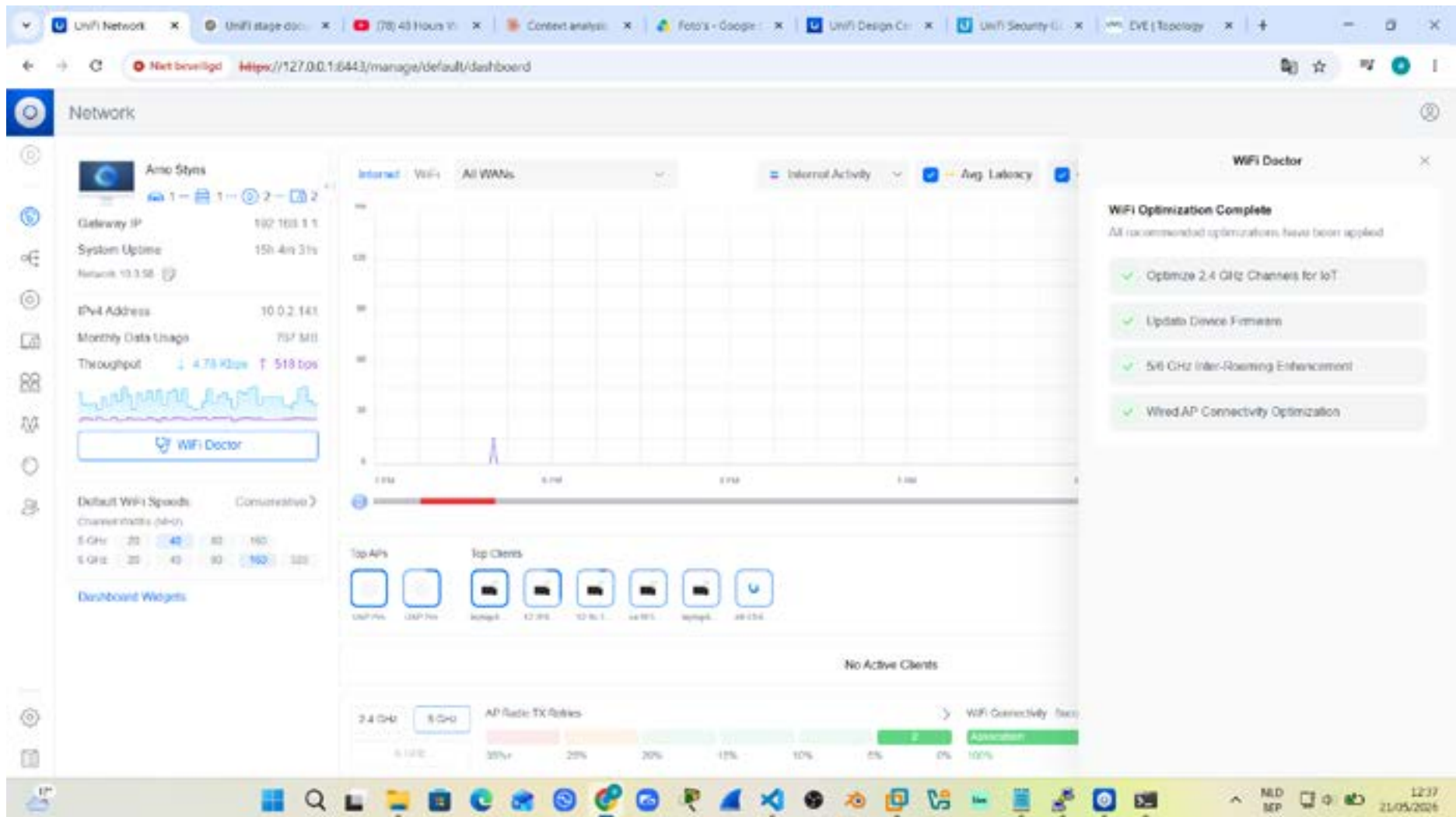
Home assistant toont welke deuren open en gesloten zijn.



H11 – Monitoring & logging

UniFi Dashboard & netwerkmonitoring

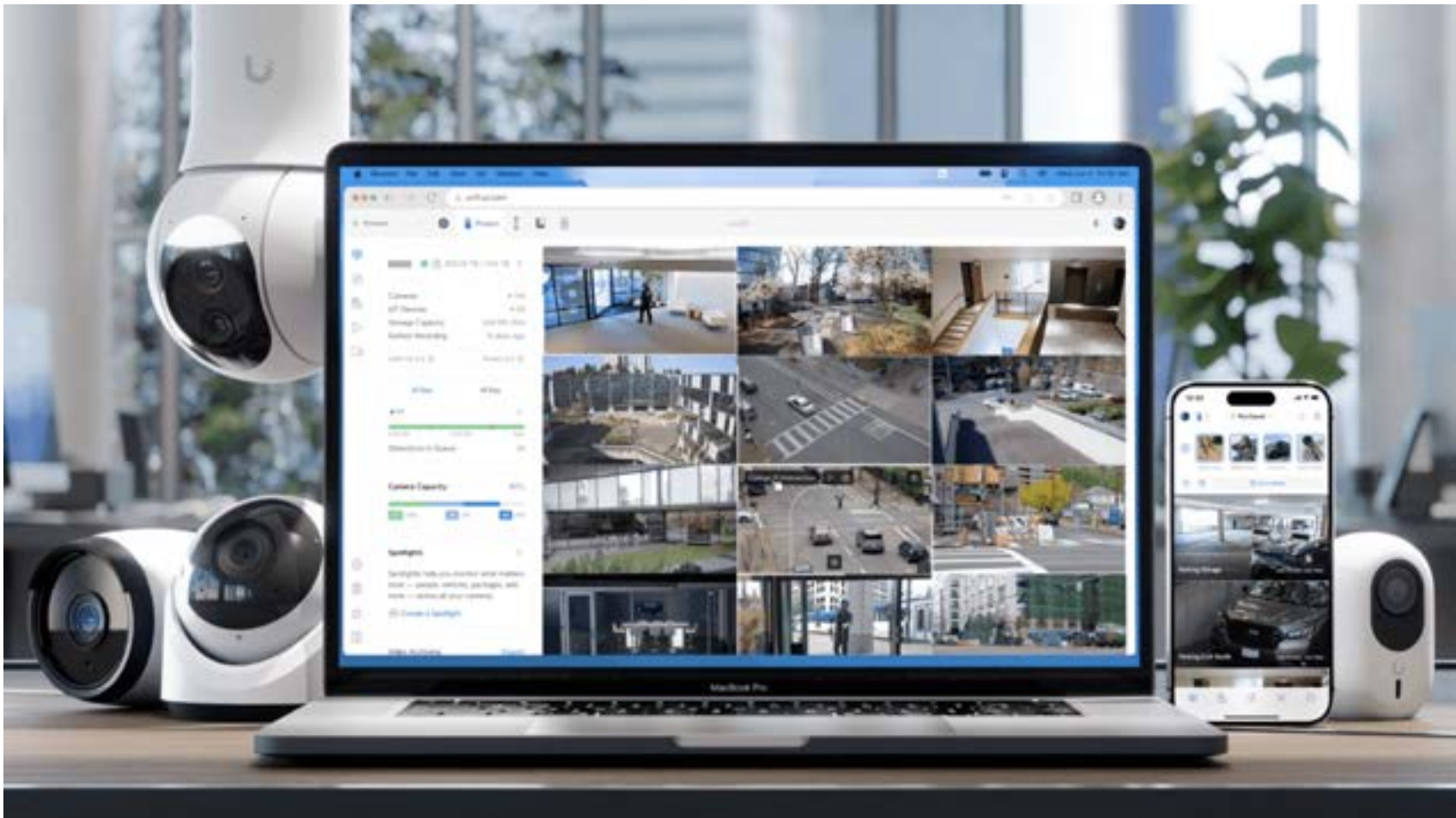
Via de UniFi Controller kan de volledige netwerkinfrastructuur centraal gemonitord worden. De beheeromgeving toont live statistieken zoals netwerkactiviteit, verbonden clients, throughput, latency en WiFi-prestaties. Hierdoor kunnen problemen sneller opgespoord en opgelost worden.



UniFi protect

UniFi Protect is het videobeheerplatform van Ubiquiti waarmee camerabeelden centraal beheerd en opgeslagen kunnen worden. Via één centrale interface kunnen beheerders live camerabeelden bekijken, opnames raadplegen, gebeurtenissen terugzoeken en meldingen ontvangen bij gedetecteerde activiteiten.

Dankzij de integratie met het UniFi-ecosysteem kunnen camera's, opslag en netwerkapparatuur centraal beheerd worden vanuit één beheeromgeving. Dit vereenvoudigt het beheer en verhoogt de overzichtelijkheid van de volledige beveiligingsinfrastructuur.



Monitoring & Logging

Het monitoren van netwerkapparatuur is essentieel om storingen snel te detecteren en de beschikbaarheid van kritieke systemen te garanderen. Binnen de infrastructuur worden routers, switches, access points, camera's en andere netwerkcomponenten centraal beheerd via de UniFi Controller.

De UniFi Controller biedt realtime inzicht in de status van alle netwerkapparatuur. Beheerders kunnen onder andere de netwerkbelasting, verbonden clients, PoE-verbruik, internetverbinding, apparaatstatus en eventuele storingen opvolgen vanuit één centraal dashboard.

Voor kritieke meldingen kan gebruik gemaakt worden van automatisatieplatformen zoals N8N. Wanneer een toestel offline gaat of een belangrijke gebeurtenis plaatsvindt, kan automatisch een melding verstuurd worden naar Discord zodat beheerders onmiddellijk op de hoogte gebracht worden.

Door monitoring, logging en automatische notificaties te combineren wordt de betrouwbaarheid van de infrastructuur verhoogd en kunnen problemen sneller opgespoord en opgelost worden.

Monitoring & Logging

N8N is een open-source automatisatieplatform waarmee verschillende systemen en applicaties met elkaar verbonden kunnen worden. Tijdens dit project werd een proof-of-concept uitgewerkt waarbij automatisch meldingen naar Discord worden verstuurd.

Naast notificaties biedt N8N tal van mogelijkheden voor automatisatie. Het platform kan geïntegreerd worden met systemen zoals UniFi, Odoo, Microsoft 365, databases, webhooks en IoT-toestellen. Hierdoor kunnen processen zoals monitoring, rapportering, ticketing en gebruikersbeheer gedeeltelijk of volledig geautomatiseerd worden.

Binnen een productieomgeving kan N8N bijvoorbeeld meldingen versturen wanneer een access point offline gaat, een camera uitvalt of een internetverbinding wordt onderbroken. Door monitoring en automatisatie te combineren kunnen problemen sneller gedetecteerd worden en kunnen beheerders efficiënter reageren op kritieke gebeurtenissen.



H12 - Theoretisch kader

12.1 VLANs & netwerksegmentatie

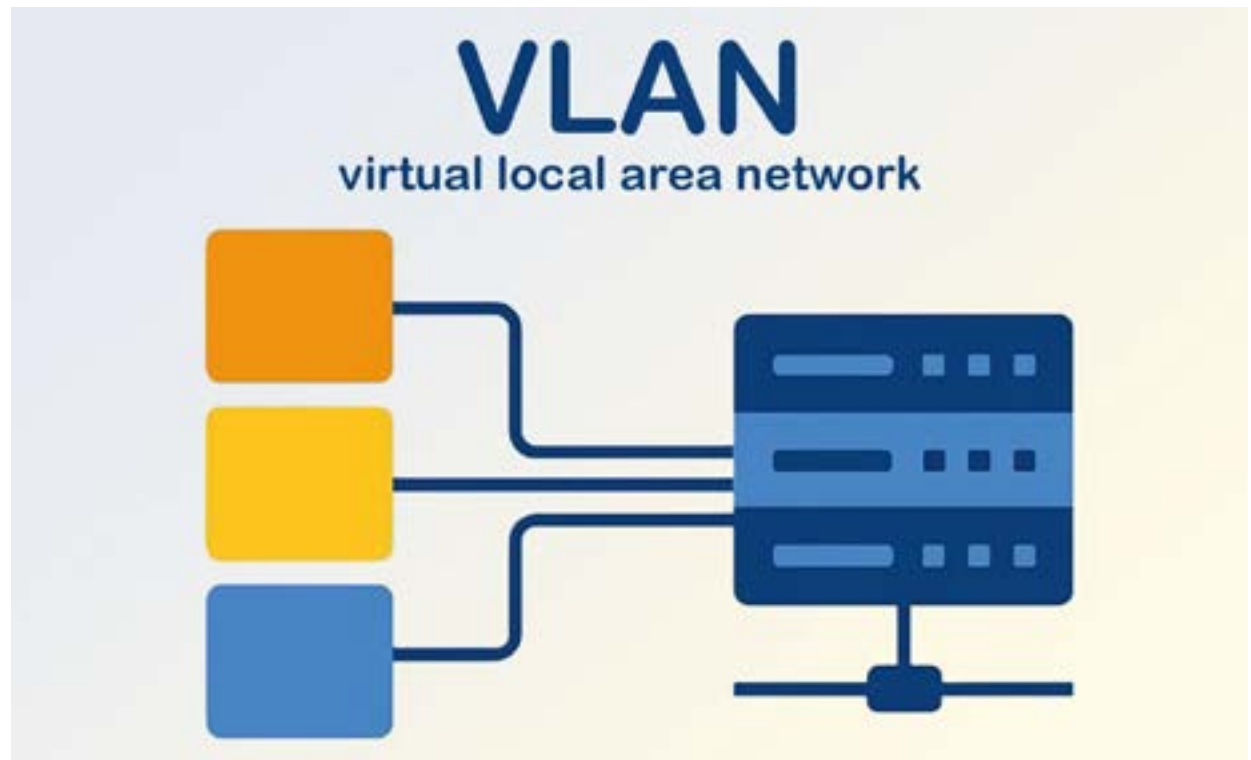
wat zijn VLANs?

Een VLAN of Virtual Local Area Network wordt gebruikt om netwerken op te splitsen in meerdere logische virtuele netwerken. Hierdoor kunnen toestellen van elkaar gescheiden worden terwijl ze toch gebruik maken van dezelfde switches en kabels.

Devices in een zelfde VLAN kunnen met elkaar communiceren. Verkeer tussen VLANs moeten via een router of firewall gaan.

Binnen professionele netwerkomgevingen worden VLANs gebruikt voor:

- Veiligheid
- Netwerkverkeer te scheiden
- Overzichtelijker te maken



Waarom zijn VLANs zo belangrijk?

Zonder VLANs zouden toestellen allemaal in hetzelfde netwerk zitten, en in bijvoorbeeld een nachtclubomgeving kan dit voor problemen zorgen

Voorbeelden

- Bezoekers kunnen kassasystemen bereiken
- cameras zouden zichtbaar zijn voor guests
- malware kan zich sneller verspreiden
- troubleshooting is moeilijker

Dus door VLAN-segmentatie te gebruiken worden gevoelige systemen van elkaar gescheiden

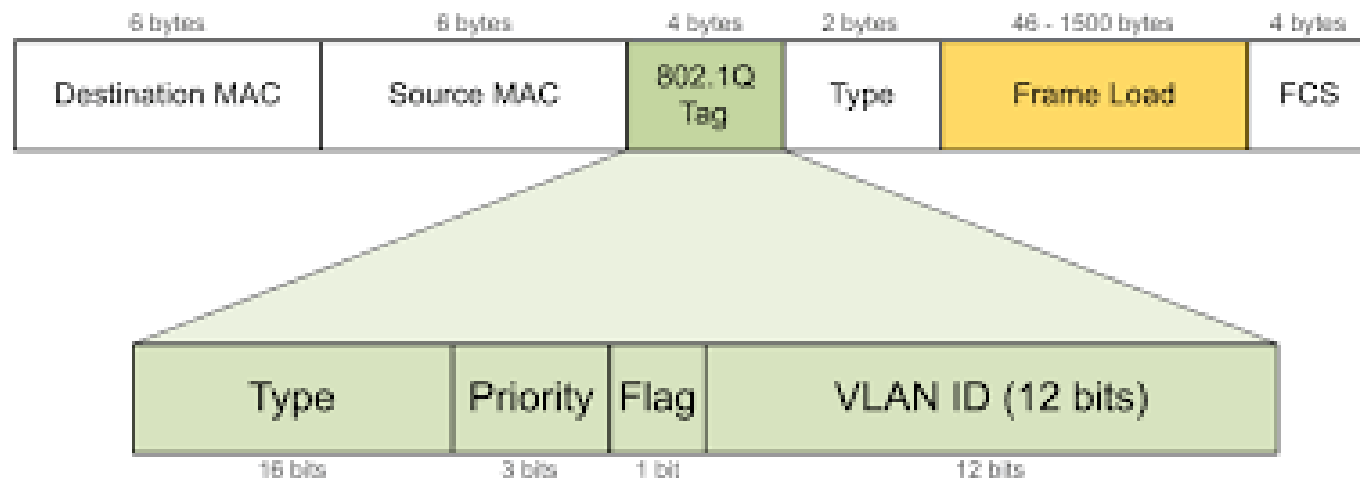
Wat is 802.1Q Tagging?

Om meerdere VLANs over dezelfde fysieke netwerkverbinding te transporteren wordt gebruik gemaakt van IEEE 802.1Q tagging. Bij 802.1Q krijgt netwerkverkeer een VLAN-tag mee zodat switches, access points en routers weten tot welk VLAN het verkeer behoort.

Binnen The Solus Club worden trunkpoorten gebruikt tussen de UniFi Dream Machine Pro Max, UniFi Pro Max switches en de UniFi access points. Hierdoor kunnen meerdere VLANs tegelijk over één enkele Cat6 trunkverbinding verzonden worden zonder aparte fysieke kabels per netwerksegment.

Wanneer bijvoorbeeld een toestel verbinding maakt met het Solus-Guest SSID, wordt het draadloze verkeer door het access point automatisch getagd met VLAN 20 Guest. Hetzelfde principe wordt gebruikt voor Solus-Staff op VLAN 10 Staff. De UniFi switches herkennen deze VLAN-tags en sturen het verkeer correct door naar het juiste netwerksegment.

Bekabelde toestellen zoals camera's, POS-systemen en IoT-apparatuur worden via switchpoorten gekoppeld aan hun respectievelijke VLANs zodat ook daar netwerksegmentatie behouden blijft.



12.5 Het UniFi Ecosysteem

Voor The Solus Club heb ik gekozen voor het UniFi ecosysteem van Ubiquiti vanwege het makkelijk beheer.

Het UniFi ecosysteem bestaat uit verschillende netwerktoestellen die centraal beheerd kunnen worden vanuit één interface. Hierdoor kunnen routers, switches, access points en camera's eenvoudiger geconfigureerd en gemonitord worden.



12.6 UniFi Controller

Binnen The Solus Club wordt de volledige netwerkinfrastructuur centraal beheerd via de UniFi Controller. Via deze beheeromgeving kunnen routers, switches, access points en camera's vanuit één interface geconfigureerd en gecontroleerd worden.

Binnen de controller worden onder andere:

- VLANs
- firewallregels
- WiFi-netwerken
- access points
- clients
- netwerkverkeer

beheerd en gemonitord.

Daarnaast biedt de UniFi Controller live statistieken zoals:

- verbonden clients
- WiFi prestaties
- PoE-verbruik
- CPU- en RAM-gebruik
- netwerkactiviteit

Binnen The Solus Club worden verschillende SSID's gebruikt zoals STAFF, GUEST en MANAGEMENT WiFi. Elke SSID wordt gekoppeld aan een apart VLAN zodat netwerkverkeer veilig gescheiden blijft.

Dankzij de centrale beheeromgeving kunnen netwerkproblemen sneller opgespoord en opgelost worden binnen de nightclubomgeving.

12.7 Firewalling & netwerksecurity

Binnen een moderne netwerkinfrastructuur is een firewall een essentieel onderdeel van de beveiliging. Een firewall controleert al het inkomende en uitgaande netwerkverkeer op basis van vooraf gedefinieerde regels en beslist welk verkeer toegelaten of geblokkeerd wordt.

In een omgeving zoals The Solus Club, waar bezoekers, personeel, kassasystemen en beveiligingscamera's allemaal gebruikmaken van hetzelfde fysieke netwerk, is firewalling cruciaal. Zonder firewallregels zou een bezoeker die verbonden is met het gastnetwerk in theorie toegang kunnen krijgen tot interne systemen zoals de kassaterminals of de camerabeelden. Een goed geconfigureerde firewall voorkomt dit door verkeer tussen netwerksegmenten strikt te controleren.

Binnen het UniFi-ecosysteem wordt firewalling uitgevoerd door de UniFi Dream Machine Pro Max. Deze fungeert als centrale router én firewall voor de volledige infrastructuur van The Solus Club. Alle firewallregels worden centraal beheerd via de UniFi Controller en gelden voor al het verkeer dat tussen de verschillende VLANs beweegt.

De firewallregels binnen UniFi werken op basis van drie richtingen: LAN IN, LAN OUT en LAN LOCAL. LAN IN-regels controleren verkeer dat vanuit een intern netwerksegment binnenkomt op de firewall. LAN OUT-regels controleren verkeer dat de firewall verlaat richting een intern netwerksegment. LAN LOCAL-regels controleren verkeer dat gericht is naar de firewall zelf, zoals beheerverkeer.

Binnen The Solus Club worden voornamelijk LAN IN-regels gebruikt om inter-VLAN verkeer te controleren en te blokkeren waar nodig.

12.8 Stateful firewalls

Een stateful firewall houdt de toestand van actieve netwerkverbindingen bij. Dit betekent dat de firewall niet enkel individuele pakketjes beoordeelt, maar de volledige context van een verbinding in overweging neemt.

Wanneer een toestel een verbinding opstart, registreert de stateful firewall de toestand van die verbinding in een zogenaamde connection state table. Antwoordverkeer dat hoort bij een reeds toegelaten verbinding wordt automatisch doorgelaten, zonder dat daarvoor een aparte regel nodig is. Dit is het grote verschil met een stateless firewall, die elk pakket afzonderlijk beoordeelt zonder rekening te houden met de context van de verbinding.

Het voordeel van stateful firewalling is dat de regels eenvoudiger en overzichtelijker blijven. Een beheerder hoeft enkel de uitgaande verbindingen toe te staan – het bijbehorende antwoordverkeer wordt automatisch toegelaten. Dit vermindert de kans op configuratiefouten en maakt het beheer van firewallregels eenvoudiger.

De UniFi Dream Machine Pro Max maakt gebruik van stateful firewalling. Alle verbindingen die door de firewall gaan worden bijgehouden in een connection table. Wanneer een verbinding wordt opgezet vanuit een toegelaten bron naar een toegelaten bestemming, wordt het bijbehorende retourverkeer automatisch doorgelaten. Verbindingen die niet overeenkomen met een toegelaten regel worden geblokkeerd en optioneel gelogd voor verdere analyse.

Binnen The Solus Club is stateful firewalling essentieel omdat het netwerk bestaat uit meerdere gescheiden segmenten die elk hun eigen verkeersregels hebben. De firewall zorgt ervoor dat enkel legitiem en geautoriseerd verkeer tussen deze segmenten kan bewegen.

12.9 Inter-VLAN blocking

Inter-VLAN blocking is de techniek waarbij verkeer tussen twee of meer VLANs geblokkeerd wordt via firewallregels op de router of firewall. Hoewel VLANs netwerken logisch van elkaar scheiden, betekent dit niet automatisch dat communicatie tussen VLANs onmogelijk is. Zonder expliciete firewallregels kan een router verkeer tussen verschillende VLANs blijven doorsturen.

Binnen The Solus Club is inter-VLAN blocking een belangrijke beveiligingsmaatregel. De verschillende netwerksegmenten moeten strikt van elkaar gescheiden blijven. Bezoekers binnen VLAN 20 (Guest) mogen onder geen enkele omstandigheid communiceren met POS-systemen binnen VLAN 40, camera's binnen VLAN 30, managementsystemen binnen VLAN 50, staff devices binnen VLAN 10 of IoT-apparatuur binnen VLAN 60.

De inter-VLAN blocking wordt gerealiseerd via LAN IN-firewallregels op de UniFi Dream Machine Pro Max. De standaardregel binnen de infrastructuur is dat netwerksegmenten enkel toegang krijgen tot het internet, tenzij communicatie tussen specifieke VLANs expliciet toegelaten wordt. Hierdoor blijven gevoelige systemen zoals kassasystemen, camerabeveiliging en managementapparatuur afgeschermd van bezoekersverkeer.

12.10 WiFi & draadloze beveiliging

Draadloze netwerken vormen een bijzondere uitdaging op het vlak van beveiliging. In tegenstelling tot bekabelde verbindingen is een draadloos signaal in principe bereikbaar voor iedereen die zich binnen het bereik van een access point bevindt. Dit maakt het des te belangrijker om draadloze netwerken correct te beveiligen.

Binnen The Solus Club wordt gebruik gemaakt van meerdere gescheiden draadloze netwerken, elk gekoppeld aan een apart VLAN. Hierdoor worden bezoekers, personeel en beheerders automatisch in het juiste netwerksegment geplaatst op basis van het WiFi-netwerk waarmee ze verbinden.

Draadloze beveiliging steunt op verschillende mechanismen. Ten eerste wordt gebruik gemaakt van sterke encryptie via WPA3 om te voorkomen dat draadloos verkeer onderschept en gelezen kan worden. Ten tweede worden SSID's gekoppeld aan specifieke VLANs zodat toestellen automatisch in het juiste netwerksegment terechtkomen. Ten derde wordt client isolation toegepast op het gastnetwerk, waardoor bezoekers onderling niet met elkaar kunnen communiceren via het WiFi-netwerk.

Access points spelen een centrale rol in de draadloze infrastructuur. Binnen The Solus Club worden UniFi access points gebruikt die centraal beheerd worden via de UniFi Controller. Elk access point zendt meerdere SSID's uit, elk gekoppeld aan een apart VLAN. Het access point zorgt ervoor dat het verkeer van elk draadloos toestel correct getagd wordt met het bijbehorende VLAN-ID voordat het via de trunkverbinding naar de switch en firewall gestuurd wordt.

12.11 Guest portals & captive portals

Een captive portal is een webpagina die automatisch getoond wordt aan een gebruiker die verbindt met een draadloos netwerk, voordat deze toegang krijgt tot het internet. Captive portals worden veel gebruikt in horeca-omgevingen zoals hotels, restaurants en nightclubs om gasten te authenticeren of te laten akkoord gaan met gebruiksvoorwaarden.

Binnen The Solus Club biedt een captive portal op het gastnetwerk verschillende voordelen. Bezoekers kunnen verwelkomd worden met een gepersonaliseerde landingspagina in de huisstijl van The Solus Club. Via de captive portal kunnen gebruiksvoorwaarden gepresenteerd worden die bezoekers moeten accepteren voordat ze internettoegang krijgen. Optioneel kan een captive portal ook gebruikt worden voor eenvoudige authenticatie via een wachtwoord of voucher. Het UniFi-ecosysteem biedt ingebouwde ondersteuning voor captive portals via de UniFi Controller. De captive portal kan volledig gecustomiseerd worden met logo, kleuren en tekst. Wanneer een bezoeker verbindt met het GUEST WiFi-netwerk, wordt deze automatisch doorgestuurd naar de captive portal. Pas na het accepteren van de voorwaarden of het invoeren van de juiste inloggegevens krijgt de bezoeker toegang tot het internet. Vanuit beveiligingsperspectief is de captive portal ook nuttig omdat het een extra laag van controle toevoegt aan het gastnetwerk. Ongeautoriseerde toegang tot het gastnetwerk wordt bemoeilijkt doordat elke gebruiker de portal moet doorlopen.

12.12 WPA2/WPA3 beveiliging

WPA staat voor Wi-Fi Protected Access en is de standaard voor draadloze netwerkbeveiliging. WPA2 en WPA3 zijn de meest recente versies van deze standaard en bieden sterke encryptie voor draadloos netwerkverkeer.

WPA2 maakt gebruik van het AES-encryptieprotocol en is sinds 2004 de industriestandaard voor draadloze beveiliging. Hoewel WPA2 nog steeds als veilig beschouwd wordt, heeft het enkele kwetsbaarheden die ontdekt werden in de loop der jaren, zoals de KRACK-aanval die in 2017 aangetoond werd.

WPA3 is de opvolger van WPA2 en werd in 2018 geïntroduceerd. WPA3 biedt verschillende verbeteringen ten opzichte van WPA2. Het maakt gebruik van Simultaneous Authentication of Equals, een veiliger authenticatieprotocol dat beschermt tegen offline woordenboekaanvallen op wachtwoorden. Daarnaast biedt WPA3 forward secrecy, wat betekent dat eerder onderschept verkeer niet ontsleuteld kan worden zelfs als het wachtwoord later gekend raakt. WPA3 biedt ook verbeterde beveiliging voor open netwerken via Opportunistic Wireless Encryption.

Binnen The Solus Club wordt WPA3 gebruikt voor alle draadloze netwerken waar dit ondersteund wordt. Voor oudere toestellen die enkel WPA2 ondersteunen wordt een WPA2/WPA3 transitie-modus gebruikt zodat compatibiliteit gegarandeerd blijft. Het gastnetwerk maakt gebruik van WPA3-Personal, terwijl het personeelsnetwerk gebruik kan maken van WPA3-Enterprise voor sterkere authenticatie.

12.13 PoE technologie

Power over Ethernet, afgekort als PoE, is een technologie die het mogelijk maakt om elektrische stroom te leveren via een standaard netwerkkabel. Hierdoor kunnen netwerkapparaten zoals access points, IP-camera's en IP-telefoons gevoed worden via dezelfde kabel die gebruikt wordt voor de dataverbinding, zonder dat een apart stroomkabel nodig is.

PoE is gestandaardiseerd door de IEEE en bestaat in verschillende varianten. IEEE 802.3af, ook bekend als PoE, levert maximaal 15,4 watt per poort en werd geïntroduceerd in 2003. IEEE 802.3at, ook bekend als PoE+, levert maximaal 30 watt per poort en is geschikt voor veeleisendere toestellen. IEEE 802.3bt, ook bekend als PoE++ of 4PPoE, levert maximaal 60 of 90 watt per poort en is bedoeld voor toestellen met een hoog stroomverbruik zoals PTZ-camera's en videoconferentiesystemen.

Binnen The Solus Club wordt PoE op grote schaal gebruikt. Alle UniFi access points worden gevoed via PoE via de UniFi Pro Max switches. De UniFi beveiligingscamera's worden eveneens gevoed via PoE, wat de installatie aanzienlijk vereenvoudigt omdat geen aparte stroomkabels naar elke cameraplocatie getrokken moeten worden. De UniFi Pro Max switches beschikken over voldoende PoE-budget om alle aangesloten toestellen te voeden.

Het gebruik van PoE biedt ook voordelen op het vlak van redundantie. Omdat de netwerkapparatuur gevoed wordt via de switches, kan een UPS-noodstroomvoorziening aangesloten op de switches ervoor zorgen dat alle PoE-toestellen actief blijven bij een stroomstoring.

12.14 IP-camerabeveiliging

IP-camera's zijn netwerkkamera's die beeldmateriaal digitaal verwerken en via het netwerk verzenden. In tegenstelling tot analoge camera's kunnen IP-camera's rechtstreeks aangesloten worden op een netwerk en zijn ze op afstand bereikbaar via een netwerkkapplicatie of webbrowser.

Vanuit beveiligingsperspectief zijn IP-camera's zelf potentieel kwetsbare toestellen. Slecht beveiligde IP-camera's met standaardwachtwoorden of verouderde firmware zijn een bekend doelwit voor cyberaanvallen. Er zijn tal van gedocumenteerde gevallen waarbij hackers toegang kregen tot camerabeelden via onbeveiligde netwerkkamera's. Bovendien kunnen gecompromitteerde camera's gebruikt worden als toegangspunt tot het bredere bedrijfsnetwerk.

Om deze risico's te beperken worden binnen The Solus Club verschillende maatregelen genomen. Alle camera's bevinden zich in een apart VLAN dat strikt gescheiden is van andere netwerksegmenten. Firewallregels zorgen ervoor dat de camera's enkel bereikbaar zijn vanuit het management- en personeelsnetwerk. De camera's hebben zelf geen toegang tot andere netwerksegmenten en kunnen geen verbindingen initiëren naar andere VLANs.

Daarnaast worden alle camera's beheerd via UniFi Protect, de geïntegreerde camerabeveiligingsoplossing van Ubiquiti. UniFi Protect zorgt voor centrale opslag van camerabeelden, beheer van camera-instellingen en toegangscontrole voor het bekijken van beelden. Camerabeelden worden opgeslagen op de lokale UNVR-opslagserver, waardoor geen gevoelige beelden naar externe cloudservers gestuurd worden.

12.15 UniFi Protect & UNVR

UniFi Protect is de camerabeveiligingsoplossing van Ubiquiti die volledig geïntegreerd is binnen het UniFi-ecosysteem. Via UniFi Protect kunnen IP-camera's centraal beheerd, gemonitord en geconfigureerd worden vanuit dezelfde interface als de rest van de netwerkinfrastructuur.

UniFi Protect biedt een breed scala aan functies. Live camerabeelden kunnen bekeken worden via de UniFi Protect applicatie op desktop of mobiel toestel. Opnames worden automatisch opgeslagen op basis van bewegingsdetectie of continue opname, afhankelijk van de configuratie. Via de tijdlijnfunctie kunnen opnames snel teruggevonden worden. Slimme detectiefuncties zoals AI-gebaseerde personendetectie zijn beschikbaar op compatibele camera's zoals de UniFi AI 360.

De UniFi Network Video Recorder, afgekort als UNVR, is de lokale opslagserver voor camera-beelden binnen het UniFi Protect ecosysteem. De UNVR wordt aangesloten op het netwerk en fungeert als centrale opslag voor alle camerabeelden. Binnen The Solus Club wordt een UNVR gebruikt om camerabeelden lokaal op te slaan, zonder afhankelijkheid van externe cloudopslag. Dit biedt voordelen op het vlak van privacy, databeveiliging en beschikbaarheid.

De UNVR ondersteunt meerdere harde schijven voor uitgebreide opslagcapaciteit en RAID-configuraties voor redundantie. De retentieperiode van camerabeelden kan per camera ingesteld worden op basis van beschikbare opslagruimte en wettelijke vereisten.

12.16 POS-systemen

Een Point of Sale systeem, afgekort als POS, is het geheel van hardware en software dat gebruikt wordt voor het afhandelen van verkooptransacties. In een horecaomgeving zoals The Solus Club omvat een POS-systeem kassaterminals, bonnenprinters, betaalterminals voor contactloze betalingen en kassalades.

POS-systemen verwerken gevoelige financiële transacties en bevatten persoonsgegevens van klanten die betalen met een bankkaart of kredietkaart. Dit maakt POS-systemen tot een aantrekkelijk doelwit voor cyberaanvallen. Bekende aanvalstechnieken gericht op POS-systemen zijn onder andere RAM-scraping malware die betaalkaartgegevens onderschept tijdens de verwerking, en netwerkaanvallen waarbij aanvallers proberen toegang te krijgen tot het POS-netwerk via andere netwerksegmenten.

Om POS-systemen te beveiligen worden ze binnen The Solus Club geplaatst in een apart VLAN dat volledig geïsoleerd is van andere netwerksegmenten. Enkel het managementnetwerk heeft toegang tot het POS-netwerk voor beheerdoeleinden. Bezoekers, personeelsleden op het staff-netwerk en IoT-toestellen hebben geen toegang tot het POS-netwerk.

Daarnaast is het belangrijk dat POS-systemen altijd beschikbaar blijven tijdens evenementen. Een POS-systeem dat uitvalt tijdens een druk evenement leidt tot inkomstenverlies en ontevreden bezoekers. De LTE backup-verbinding binnen The Solus Club zorgt ervoor dat betalingstransacties kunnen blijven doorgaan zelfs als de primaire internetverbinding uitvalt.

12.17 LTE failover & redundantie

Redundantie in een netwerkinfrastructuur betekent dat er reservesystemen of alternatieve verbindingen aanwezig zijn die automatisch overnemen wanneer een primair systeem uitvalt. In een professionele horecaomgeving is netwerkredundantie essentieel omdat een netwerkstoring directe operationele en financiële gevolgen kan hebben.

LTE, wat staat voor Long-Term Evolution, is een draadloze mobiele communicatiestandaard die hoge datasnelheden biedt via het mobiele netwerk. Een LTE-verbinding kan gebruikt worden als backup internetverbinding wanneer de primaire vaste internetverbinding uitvalt.

Binnen The Solus Club wordt een UniFi LTE Backup Pro gebruikt als redundante internetverbinding. Dit toestel wordt aangesloten op de UniFi Dream Machine Pro Max en geconfigureerd als failover-verbinding. Wanneer de primaire WAN-verbinding uitvalt, detecteert de Dream Machine Pro Max dit automatisch en schakelt over naar de LTE-verbinding. Dit proces verloopt automatisch en zonder handmatige tussenkomst.

De LTE failover zorgt ervoor dat kritieke systemen zoals kassaterminals, betalingsterminals, camerabeveiliging en management op afstand actief blijven tijdens een internetstoring. De LTE-verbinding is bedoeld als tijdelijke backup en niet als primaire verbinding, omdat de bandbreedte en latency van LTE minder voorspelbaar zijn dan een vaste internetverbinding.

12.18 UPS systemen

Een Uninterruptible Power Supply, afgekort als UPS, is een noodstroomvoorziening die netwerkkapparatuur beschermt tegen stroomstoringen en stroomschommelingen. Een UPS bevat een ingebouwde batterij die automatisch de stroomtoevoer overneemt wanneer de netspanning uitvalt of te ver afwijkt van de normale waarde.

Binnen een professionele netwerkinfrastructuur is een UPS om meerdere redenen essentieel. Bij een plotse stroomstoring kunnen netwerkkapparaten beschadigd raken door een abrupte afsluiting zonder dat lopende processen correct afgesloten worden. Een UPS geeft de apparatuur de tijd om gecontroleerd af te sluiten of biedt voldoende tijd om over te schakelen op een noodgenerator. Bovendien beschermt een UPS tegen stroompieken en -dalingen die elektronische apparatuur kunnen beschadigen.

Binnen The Solus Club wordt een UPS gebruikt om de kernapparatuur in het centrale rack te beschermen. Dit omvat de UniFi Dream Machine Pro Max, de core switch, de UNVR-opslagserver en het patchpaneel. Doordat de core switch gevoed wordt via de UPS, blijven ook alle PoE-toestellen zoals access points en camera's actief bij een stroomstoring.

De autonomie van de UPS bepaalt hoe lang de apparatuur actief blijft bij een stroomstoring. Voor The Solus Club is een autonomie van minimaal 15 tot 30 minuten wenselijk, zodat er voldoende tijd is om het probleem te detecteren en op te lossen of om een generator op te starten.

12.19 Monitoring & logging

Netwerkmonitoring is het continu bewaken van een netwerkinfrastructuur om de beschikbaarheid, prestaties en beveiliging van alle netwerkapparaten en -verbindingen te garanderen. Via monitoring kunnen problemen snel gedetecteerd en opgelost worden voordat ze een grote impact hebben op de werking van het netwerk.

Logging is het registreren van gebeurtenissen binnen een netwerk of systeem. Logbestanden bevatten informatie over verbindingen, fouten, waarschuwingen en beveiligingsgebeurtenissen. Deze informatie is essentieel voor troubleshooting, maar ook voor security-analyse en het opsporen van ongebruikelijke activiteiten.

Binnen The Solus Club wordt monitoring en logging gerealiseerd via meerdere lagen. De UniFi Controller biedt ingebouwde monitoring van alle netwerkapparaten en geeft real-time inzicht in verbonden clients, WiFi-prestaties, PoE-verbruik en netwerkactiviteit. Alerts kunnen geconfigureerd worden om automatisch te waarschuwen bij bepaalde gebeurtenissen, zoals een netwerkapparaat dat offline gaat of een ongewone stijging in netwerkverkeer.

Syslog is een standaardprotocol voor het versturen van logberichten van netwerkapparaten naar een centrale logserver. Via syslog kunnen logberichten van alle UniFi-apparaten gecentraliseerd worden voor verdere analyse. SNMP, wat staat voor Simple Network Management Protocol, is een protocol dat gebruikt wordt voor het opvragen van statusinformatie van netwerkapparaten en het instellen van drempelwaarden voor automatische waarschuwingen.

12.20 Raspberry Pi & IoT

De Raspberry Pi is een compacte, energiezuinige single-board computer die ontwikkeld werd door de Raspberry Pi Foundation. Ondanks zijn kleine formaat beschikt de Raspberry Pi over voldoende rekenkracht voor een breed scala aan toepassingen, waaronder netwerkmonitoring, domotica, dashboards en IoT-integraties.

IoT staat voor Internet of Things en verwijst naar het netwerk van fysieke toestellen die verbonden zijn met het internet en onderling gegevens uitwisselen. In een horecaomgeving kunnen IoT-toestellen gebruikt worden voor slimme deursensoren, omgevingsmonitoring, energiebeheer en automatische meldingen.

Binnen The Solus Club wordt de Raspberry Pi 4 ingezet als monitoring node en IoT-gateway. De Pi draait een lichtgewicht Linux-omgeving en kan gebruikt worden voor het verzamelen en visualiseren van netwerkstatistieken, het aansturen van slimme sensoren en het weergeven van informatie op een intern dashboard.

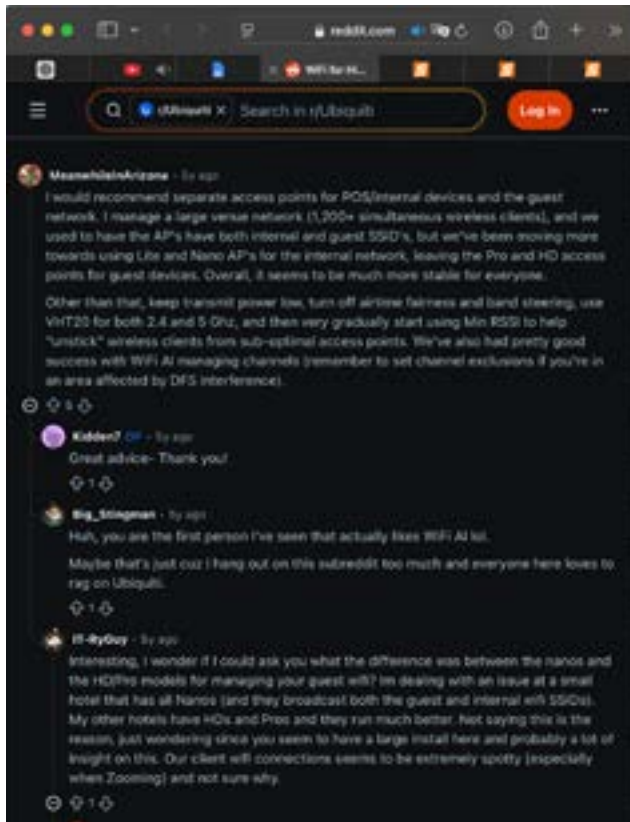
Vanuit beveiligingsperspectief is het belangrijk dat IoT-toestellen gescheiden worden van andere netwerksegmenten. IoT-toestellen hebben vaak een eenvoudigere software-architectuur en worden minder frequent bijgewerkt, wat ze kwetsbaarder maakt voor aanvallen. Door alle IoT-toestellen en de Raspberry Pi in een apart VLAN 60 te plaatsen, wordt het risico beperkt dat een gecompromitteerd IoT-toestel toegang krijgt tot andere netwerksegmenten.

ook gebruiken we badges om binnen te gaan in bepaalde deuren, zodat enkel medewerkers binnen kunnen in het gebouw.

12.21 Reddit page

Tijdens het uitwerken van The Solus Club heb ik ook online praktijkervaringen en community-discussies onderzocht rond high-density WiFi omgevingen zoals bars, restaurants en eventlocaties. Op Reddit en Ubiquiti-forums delen netwerkbeheerders vaak hun ervaringen met grote aantallen gelijktijdige draadloze clients.

Die persoon legt uit dat ze in grote drukke locaties met meer dan 1200 gelijktijdige WiFi-clients vroeger dezelfde access points gebruikten voor zowel gasten als interne toestellen zoals POS-systemen en personeel. Dit werkte minder stabiel. Daarom zijn ze later aparte access points beginnen gebruiken: Lite- en Nano-AP's voor interne toestellen en krachtigere Pro- en HD-modellen voor guest WiFi. Hierdoor werd het netwerk veel stabiel tijdens drukke momenten.



https://www.reddit.com/r/Ubiquiti/comments/l5b733/wifi_for_high_density_restaurant_bar_environment/

12.22 NFC

NFC (Near Field Communication) is een draadloze communicatietechnologie waarmee apparaten op zeer korte afstand (ongeveer 4 cm) gegevens kunnen uitwisselen. Binnen The Solus Club wordt NFC gebruikt voor toegangscontrole via badges en kaarten.

Toepassing binnen The Solus Club:

- Personeel krijgt een NFC badge of kaart
- Badge wordt gescand aan de deurlezer
- UniFi Access controleert toegangsrechten
- Bij geldige rechten opent het elektrisch slot automatisch
- Alle toegangspogingen worden gelogd in UniFi Access

Voordelen van NFC:

- Snelle authenticatie
- Contactloze werking
- Moeilijker te kopiëren dan klassieke sleutels
- Centrale toegangscontrole
- Mogelijkheid tot intrekken/vervangen van badges

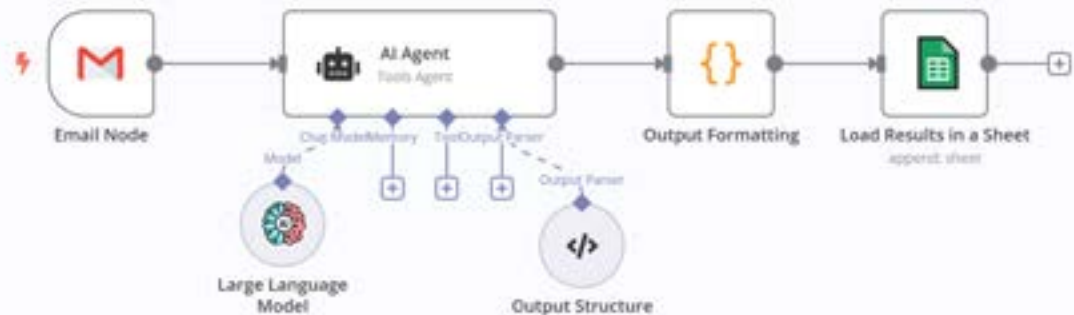
12.23 N8N

N8N is een open-source automatisatieplatform waarmee verschillende systemen, applicaties en diensten met elkaar verbonden kunnen worden via workflows. Door gebruik te maken van visuele workflows kunnen taken automatisch uitgevoerd worden zonder manuele tussenkomst.

Binnen een netwerkomgeving kan N8N gebruikt worden voor meldingen, monitoring, rapportering en integraties tussen verschillende systemen. Zo kunnen netwerkgebeurtenissen automatisch verwerkt worden en kunnen waarschuwingen verstuurd worden naar beheerders wanneer bepaalde acties plaatsvinden.

N8N ondersteunt honderden integraties waaronder Discord, e-mail, databases, webhooks, API's en cloudplatformen. Hierdoor vormt het een flexibel automatisatieplatform voor zowel netwerkbeheer als systeembeheer.

Voorbeelden van toepassingen zijn automatische meldingen bij storingen, waarschuwingen bij netwerkproblemen, verwerking van sensorgegevens en het uitvoeren van repetitieve beheertaken via workflows.



H13 - Kostenprijs

Kostenprijs Hardware + installatie-uren

Onderstaande offerte geeft een overzicht van de geschatte hardware-, installatie- en configuratiekosten voor de volledige IT-infrastructuur van The Solus Club. De totale projectkost bedraagt €21.248 excl. btw of €25.710 incl. btw.

Aantal	Product	Prijs/stuk	Totaal
1	UniFi Dream Machine Pro Max	€684	€684
1	UniFi Switch Pro Max 48 PoE	€1.500	€1.500
1	UniFi Switch Pro Max 24	€450	€450
1	UniFi LTE Backup Pro	€250	€250
3	UniFi U7 Pro XGS	€220	€660
2	UniFi U6+	€120	€240
1	UniFi U6 Enterprise In-Wall	€320	€320
5	UniFi G5 Pro	€420	€2.100
15	UniFi G5 Dome Ultra	€135	€2.025
3	UniFi AI 360	€450	€1.350
1	UniFi UNVR	€350	€350
1	Seagate SkyHawk 4TB	€199	€199
1	UniFi Gate Hub	€330	€330
2	UniFi G3 Reader Pro	€300	€600
1	UniFi Reader Flex	€130	€130
1	Triton RMA 18U Rackkast	€450	€450
1	Patch Panel 48-Port Cat6	€120	€120
3	UACC Rack Brush Panel	€50	€150
1	Digitus Rack PDU	€50	€50
1	APC Smart-UPS SMT1500RMI2UC	€1.200	€1.200
1	Raspberry Pi 4	€90	€90
4	Aqara Sensor	€25	€100
1	Cat6 bekabeling + accessoires	€1.000	€1.000
HARDWARE TOTAAL EXCL. BTW			€14.348
Installatie-uren			92 uur
Uurtarief			€75 / uur
Arbeidskost			€6.900
Totaal Hardware			€14.348
Totaal Arbeid			€6.900
Totaal Exclusief BTW			€21.248
BTW (21%)			€4.462
TOTAAL INCLUSIEF BTW			€25.710

H14 - Conclusie

Conclusie

Binnen dit eindwerk werd een volledige netwerk- en systeembeheerinfrastructuur ontworpen voor The Solus Club. Het doel was het uitwerken van een veilige, schaalbare en centraal beheerde omgeving waarin verschillende systemen zoals WiFi, camerabewaking, toegangscontrole, POS-systemen en IoT-toestellen samen functioneren.

Door gebruik te maken van VLAN-segmentatie werden bezoekers, personeel, camera's, kassasystemen, managementtoestellen en IoT-apparatuur logisch van elkaar gescheiden. Hierdoor wordt de veiligheid verhoogd en blijft het netwerk overzichtelijk beheersbaar.

Als centrale infrastructuur werd gekozen voor het UniFi-ecosysteem met een UniFi Dream Machine Pro Max, managed switches, access points, UniFi Protect-camera's en UniFi Access toegangscontrole. Daarnaast werden redundantie-oplossingen voorzien via een UPS en LTE Failover.

Tijdens het project werden verschillende onderdelen praktisch getest, waaronder UniFi-configuraties, VLAN-segmentatie, firewallregels, WiFi-dekking, een POS proof-of-concept, Raspberry Pi automatisatie en N8N workflows.

Dit eindwerk toont aan hoe netwerkbeheer, systeembeheer, security en automatisatie gecombineerd kunnen worden binnen één professionele omgeving. In een toekomstige productieomgeving kunnen bijkomende uitbreidingen zoals extra opslag, geavanceerde monitoring en verdere automatisatie toegevoegd worden.

H15 - Bronnen

Bronnen

Dream machine pro max: <https://eu.store.ui.com/eu/en/products/udm-pro-max>

Unifi OS download: <https://ui.com/download/unifi-protect>

Pro max 48 PoE: <https://eu.store.ui.com/eu/en/products/usw-pro-max-48-poe>

Seagate Skyhawk 4TB; <https://www.alternate.be/Seagate/SkyHawk-4-TB-harde-schijf/html/product/1853612>

APC Smart-UPS SMT1500RMI2UC: <https://www.se.com/be/nl/product/SMT1500RMI2UC/apc-smartups-line-interactive-1500va-rack-mount-2u-230v-4x-iec-c13-uitgangen-smartconnect-port+smartslot-avr-lcd/>

Worldline Yomani XR: https://support.worldline.com/content/dam/support-worldline/local/en-ch/documents/manuals/110071402_MA_yomani_INT_EN_opt.pdf

Sunmi T2s lite: https://www.bypos.nl/sunmi-t2s-lite-39-6-cm-15-6-android-black-or-ange-p03130033?srsId=AfmBOorhdVRYL9AiZkKqc4sc3Y6V5Ve_SY_TwT-taYS0xs8HSNhBlmJEPPY

H16 - Dankwoord

Dankwoord

Als laatste wil ik Johan en William enorm bedanken voor de passie voor IT & netwerk-beheer die ze in al hun lessen staken.

Het is door deze passie dat ik nu ook een enorme passie en leergierigheid heb gekregen voor Netwerk en systeembeheer en al de geleerde leerstof neem ik absoluut mee neem in mijn verdere carrière in IT.

Bedankt!