

Bijlage C: Huidige omgeving

Vooraf

Deze bijlage biedt Inschrijvers inzicht in de huidige technische netwerk/infrastructuur-omgeving van Stichting LVO. Het document is bedoeld om een duidelijk beeld te schetsen van de bestaande infrastructuur.

De informatie in dit document is samengesteld op basis van de meest actuele gegevens die op het moment van schrijven beschikbaar waren. Hoewel grote zorg is besteed aan juistheid en volledigheid, kunnen wijzigingen of afwijkingen in de praktijk voorkomen.

Algemeen

De netwerk-infrastructuur van Stichting LVO is opgebouwd uit een samenstel van diensten die door verschillende gespecialiseerde partijen worden geleverd.

NaaS leverancier

Deze levert en beheert de netwerkcomponenten binnen de locaties van LVO in een OPEX-model. Dit omvat de switches en access points, inclusief incident- en change-afhandeling voor netwerklraag 1, 2 en deels 3. De NaaS-dienst voorziet in een uniform uitgerolde infrastructuur met centraal beheer en monitoring, waarmee de beschikbaarheid en performance van het LAN en WLAN worden geborgd.

SIVON dienst

Via SIVON maakt LVO gebruik van de landelijke dienst 'Veilig Internet'. Deze dienst biedt filtering, beveiliging en een centrale ontsluiting naar het Internet. Iedere locatie is uitgerust met een Fortigate 100F-firewall, eveneens geleverd/beheerd via SIVON. Deze FG100's verzorgen zowel de VLAN-segmentatie als de beveiliging op de locaties verzorgt. Het WAN-verkeer wordt centraal gemonitord door SIVON.

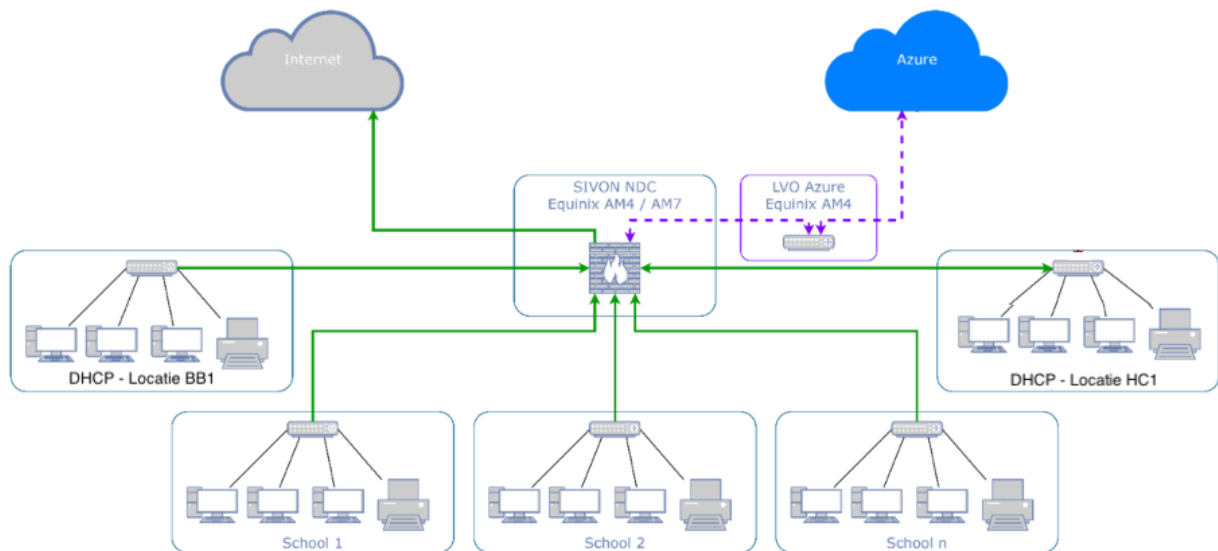
MSP partij

De MSP ondersteunt LVO met werkplekbeheer, datacenterbeheer en beheer van de apparatuur in de Equinix-locatie, die de koppeling vormt tussen het SIVON-netwerk en het LVO Azure-datacenter. Vanuit deze omgeving worden onder andere hosting- en netwerkdiensten geleverd. DE MSP verzorgt daarnaast de monitoring van overige componenten binnen de infrastructuur.

LVO regie

LVO vervult een centrale regierol over de gehele technische keten. De stichting bewaakt de architectuur, coördineert leveranciers, en beschikt over inzicht in alle monitoring-omgevingen. Operationele taken en technische wijzigingen worden via de genoemde dienstverleners uitgevoerd, onder toezicht van LVO.

High Level Design



Locaties

Het netwerk van Stichting LVO bestaat alle onderwijs- en ondersteunende locaties binnen de stichting. In totaal betreft dit meer dan twintig schoollocaties en één bureau ondersteunende diensten, verspreid over de provincie Limburg en één locatie in Noord-Brabant.

De totale infrastructuur omvat circa 13.000 LAN-poorten en 1.300 draadloze access points. Alle locaties zijn uniform aangesloten volgens de door NaaS-leverancier geleverde NaaS-oplossing en de dienst Veilig Internet van SIVON, bestaande uit een CPE, distributie- en access-laag met centrale monitoring en beheer. Deze opzet zorgt voor een gestandaardiseerde netwerkconfiguratie en consistente netwerkbeveiliging binnen het gehele LVO-domein.

Uitzondering: de locatie Milaanstraat maakt gebruik van de Wi-Fi-infrastructuur van het Vista College. Hier is momenteel enkel EDUroam actief; overige draadloze diensten worden niet vanuit LVO beheerd.

Locaties	Adres	LAN-poorten	WiFi-accesspoints	WAN-lijn
Ondersteunende Diensten	Mercator 1, 6135 KW	144	12	1gbit
Broekland College	Polderstraat 4, 6431 LE	336	16	1gbit
Bonnefanten College	Eenhoornsingel 100, 6216 CW	528	42	1gbit
Bernard Lievegoed College	Nijverheidsweg 25, 6213 GB Gebroeders van Doornelaan 124, 5961 BE	408	39	1gbit
Dendron College	5961 BE	936	86	1gbit
Emmacollege	De Weggebekker 1, Putgraaf 188, 6411GT	240	46	1gbit
Emmacollege	Putgraaf 188, 6411GT	312	41	1gbit
Grotius College	Akerstraat 117, 6417 BM	288	53	1gbit
Graaf Huyn College	Jos Klijnenlaan 683, 6164 AP	672	123	1gbit
Scholengemeenschap Groenewald	Kinskystraat 15, 6171 LX	456	64	1gbit
Het Bouwens van der Boijecollege	Minister Calsstraat 10, 5981 VT	672	69	1gbit
Het College	Parklaan 1A, 6006 NT	672	53	1gbit
Bravo! College				
Cranendonck	Jan van Schoonvorststraat 1, 6021 BP	216	18	1gbit
Het Kwadrant	Thornstraat 7, 6004 JP	792	71	1gbit
Het Kwadrant	Randweg-Oost 32, 6021 PB Budel	24	11	1gbit
Porta Mosana College	Oude Molenweg 130, 6228 XW	480	58	1gbit
SGM Philips van Horne	Wertastraat 1, 6004	672	53	1gbit
Raayland College	Leunseweg 6, 5802 CH	792	74	1gbit
Raayland College	Groenewoltsepad 2, 5801 AP Venray	48	11	1gbit
Compass	Schoolstraat 16, 6443 BT	96	11	1gbit
Sint-Janscollege	Amstenraderweg 122, 6431 EN	912	56	1gbit
Sint-Maartenscollege	Noormannensingel 50, 6224	336	30	1gbit
Sophianum	Landsraderweg 3, 6271 NT	672	90	1gbit
Stella Maris College	Parallelweg 56, 6231 CJ	552	48	1gbit
Terra Nigra	Terra Nigrastraat 5, 6216 BK Bemelerweg 1, 6226 NE,	96	25	1gbit
VMBO Maastricht	Bemelergrubbe 2 , 6226 NK	936	50	1gbit
Dacapo	Havikstraat 5, 6135 ED	528	64	1gbit
Dacapo	Milaanstraat 125, 6135 LH	192	-	1gbit
Dacapo	Einighauserweg 25, 6163 AK	144	13	1gbit
Buurt College - Agora				500
Maas en Peel	Piushof 87, 5981 VW	72	13	mbit

Totaal aantal switchpoorten = 13224

Totaal aantal accesspoints = 1340

LAN

Elke locatie binnen Stichting LVO is voorzien van een eigen Local Area Network (LAN), opgebouwd volgens een gestandaardiseerde architectuur die door NaaS-leverancier als NaaS-dienst wordt geleverd en beheerd. Het LAN vormt de ruggengraat van de lokale infrastructuur en biedt bekabelde connectiviteit voor werkplekken, randapparatuur en netwerkcomponenten.

Het LAN is opgebouwd uit een distributielaag en een access-laag. Elke locatie beschikt over één (soms twee) distributieswitch van het type Cisco Meraki MS425-16 en meerdere access-switches van het type Cisco Meraki MS250-48FP en Cisco Meraki MS250-24P. De verbinding tussen beide lagen is gebaseerd op 10 Gbps-verbindingen via multimode glasvezel. De distributieswitches zijn enkelvoudig uitgevoerd zonder redundantie. De access-switches staan in stacks tot maximaal acht units en worden gekoppeld op basis van physical stacking.

De accesspoorten van de switches zijn voorzien van PoE-poorten. Alle WiFi-accesspoint en overige randapparatuur, zoals bijv. camera's en VoIP-toestellen maken gebruik van PoE-voorzieningen. De switches en access points zijn Cisco Meraki-componenten, waardoor configuratie, beheer en monitoring centraal plaatsvinden via het Meraki-dashboard binnen de beheerdienst van NaaS-leverancier.

Binnen LVO wordt het subnets XX.XXX.X.0 /12 gebruikt om alle locaties te huisvesten, waarbij per locatie een /18-subnet wordt toegewezen. Deze logische scheiding zorgt voor overzicht en eenvoud in routing en beheer.

Het LAN maakt gebruik van een gestandaardiseerde VLAN-indeling waarmee de verschillende netwerkfuncties logisch van elkaar zijn gescheiden. De huidige configuratie is als volgt:

VLAN-ID	Toepassing	IP subnet
403	Management	/23
404	Servers	/24
405	Beveiliging	/24
406	IP-Telefonie	/23
407	Randapparatuur	/23
408	DMZ	/24
409	APs	/24
410	Educatief	/22
419	Guest - bekabeld	/23
420	Guest – Wi-Fi	/20
428	-reserve-	/23
430	-reserve-	-reserve-
431	Landing	/22
432	IOT-Private	/24
433	IOT-open	/24

Deze structuur waarborgt een duidelijke scheiding tussen beheer-, gebruikers- en gastverkeer, waardoor het netwerk veilig, overzichtelijk en goed schaalbaar blijft.

Het volledige LAN wordt beheerd door NaaS-leverancier via het centrale Meraki-dashboard, waarmee real-time inzicht wordt geboden in configuraties, prestaties en storingen. Stichting LVO heeft leesrechten tot deze omgeving en voert regie over wijzigingen en beleidskeuzes.

Wi-Fi

Alle locaties van Stichting LVO zijn uitgerust met een uniforme draadloze infrastructuur, gebaseerd op Cisco Meraki MR45 en MR46(e) access points. Deze access points ondersteunen Wi-Fi 6 (802.11ax) en opereren op zowel 2,4 GHz als 5 GHz. De draadloze infrastructuur is integraal onderdeel van de door NaaS-leverancier geleverde NaaS-omgeving en wordt centraal beheerd via het Meraki-dashboard.

De access points zijn aangesloten op de access-laag van het LAN via PoE-voorzieningen en worden volledig centraal geconfigureerd. Hiermee is op alle locaties een identieke inrichting en beveiliging gewaarborgd. Het beheer, de firmware-updates en de monitoring verlopen via het Meraki-beheerportaal van NaaS-leverancier, waarin LVO-leesrechten heeft voor inzicht en regie.

Binnen het Wi-Fi-domein wordt gebruikgemaakt van meerdere SSID's die elk een specifieke gebruikersgroep en beveiligingsmethode bedienen. De configuratie is uniform toegepast op alle LVO-locaties, met uitzondering van de locatie Milaanstraat, waar de Wi-Fi-voorziening in beheer is van Vista College en enkel EDUroam wordt aangeboden.

Frequentie	SSID	Toepassing	Authenticatie
2,4 GHz / 5 GHz	Stichting LVO	Managed devices (LVO-medewerkers)	RADIUS / EAP-TLS / PEAP / MAC auth
2,4 GHz / 5 GHz	Stichting LVO Gasten	Gastennetwerk	Splash page / gebruikersnaam + wachtwoord
2,4 GHz / 5 GHz	PUBLICroam	Publiek gastennetwerk	RADIUS / Identity PSK (via Publicroam-federatie)
2,4 GHz / 5 GHz	EDUroam	Leerlingen / onderwijs-gasten	RADIUS / PEAP / gebruikersnaam + wachtwoord
2,4 GHz / 5 GHz	IOTroam-open	IoT-netwerk (open)	RADIUS / Identity PSK
2,4 GHz / 5 GHz	IOTroam	IoT-netwerk (gesloten)	RADIUS / Identity PSK

Authenticatie vindt in de meeste gevallen plaats via de huidige Microsoft NPS-servers van LVO. Voor de SSID's PUBLICroam en IOTroam wordt authenticatie via externe federaties afgehandeld. De netwerksegmentatie sluit direct aan op de VLAN-structuur van het LAN:

- IOTroam-open en IOTroam zijn gekoppeld aan hun eigen VLAN's.
- PUBLICroam, LVO Gasten en Eduroam delen VLAN 420 (gastennetwerk).

- Voor Stichting LVO-devices wordt het VLAN dynamisch toegewezen op basis van authenticatie-attributen.

Specifieke toelichting m.b.t. de IOTroam-functionaliteit:

- Pilot i.s.m. KennisNet
- Veilige integratie van IoT-devices op de aanwezige connectiviteit
- Toepassing o.b.v. apparaat-gebonden en user-gebonden
- Potentieel ook ruimte-gebonden en/of tijd-gebonden
- Beheersbaar (vanuit ICT optiek) en gebruiksvriendelijk (vanuit onderwijs optiek)

Firewall

Elke locatie binnen Stichting LVO is voorzien van een Fortigate 100F-firewall, geleverd via de SIVON-dienst Veilig Internet-dienst. Eén locatie is tijdelijk voorzien van een FG60 en koperlijn in afwachting van nieuw schoolgebouw. Deze firewalls fungeren als Customer Premises Equipment (CPE) en vormen de lokale beveiligingslaag tussen het interne LVO-netwerk en de landelijke SIVON-infrastructuur. De inrichting is op alle locaties uniform toegepast en wordt centraal gecoördineerd binnen de dienst Veilig Internet.

De lokale Fortigate-firewalls verzorgen de VLAN-segmentatie en de laag 3-routing tussen de interne netwerken. Daarnaast handelen zij de lokale netwerkfuncties af, zoals IP-helper-configuraties voor DHCP-verkeer.

Het overige beveiligingsbeleid waaronder contentfiltering, webfiltering en internetbeveiliging wordt centraal door SIVON uitgevoerd. Deze filtering is gebaseerd op categorieën en profielen die door SIVON worden beheerd. Stichting LVO kan via een changeprocEDURE wijzigingen of uitzonderingen aanvragen.

Naast de lokale firewalls beschikt LVO over twee centrale firewalls, namelijk één in het Azure-datacenter en één in de Equinix-locatie. Deze firewalls beschermen de datacenterverbindingen en vormen samen met de SIVON-omgeving het beveiligde koppelvlak tussen het lokale netwerk en de cloud- en datacenteromgevingen.

Het verkeer tussen de LVO-locaties en de datacenteromgevingen (Azure en Equinix) verloopt volledig via het SIVON-WAN. Binnen dit WAN worden de onderlinge verbindingen en VPN-structuren beheerd door SIVON. Hierdoor zijn alle locaties veilig verbonden en wordt verkeer consistent gefilterd via de centrale infrastructuur van de Veilig Internet-dienst.

De monitoring, logging en rapportage van de Fortigate-firewalls worden uitgevoerd door SIVON. LVO ontvangt inzicht in deze gegevens voor regie- en coördinatiedoeleinden, maar voert zelf geen operationeel beheer uit. Deze centrale opzet garandeert dat beveiligingsbeleid en logging uniform worden toegepast binnen alle onderdelen van de organisatie.

DHCP

De DHCP-dienstverlening zijn binnen LVO gehost op twee locaties: het Bestuursbureau en Het College. Op beide locaties draait een virtuele DHCP-server op een lokale ESX-host. Deze opzet waarborgt de beschikbaarheid van netwerkadressering, ook in het geval van een tijdelijke onderbreking van de verbinding met het datacenter of Azure-omgeving. De MSP is verantwoordelijk voor het beheer en onderhoud van deze DHCP-servers.

DNS

De DNS-diensten zijn redundant uitgevoerd binnen de private cloudomgeving van LVO in Azure. Beide servers draaien op Windows Server en leveren interne naamresolutie voor het gehele domein. Voor externe naamresolutie maken de DNS-servers gebruik van forwarders richting de Kennisnet-DNS-servers binnen de dienst Veilig Internet van SIVON. Deze opzet zorgt voor gecontroleerde en veilige resolutie van internetverkeer, waarbij filtering en beveiliging via SIVON behouden blijven. De MSP beheert en monitort de DNS-servers als onderdeel van de centrale infrastructuurdiensten.

RADIUS

Voor netwerktoegang maakt LVO gebruik van een RADIUS-infrastructuur gebaseerd op Microsoft Network Policy Server (NPS). Deze dienst draait redundant op twee servers binnen de Azure-omgeving van LVO. De RADIUS-servers worden gebruikt voor zowel draadloze als bekabelde 802.1X-authenticatie. Ze verzorgen de autorisatie van gebruikers en apparaten voor de SSID's Stichting LVO, Eduroam en de bekabelde educatieve VLAN's. Via beleidsregels worden authenticatieattributen uit Active Directory gebruikt om dynamisch VLAN's toe te wijzen, zodat gebruikers automatisch in het juiste netwerksegment terechtkomen. Het beheer en de monitoring van de RADIUS-infrastructuur worden eveneens door de MSP uitgevoerd.

Werkplek

Stichting LVO beschikt over circa 11.500 beheerde werkplekken, die volledig zijn geïntegreerd binnen de Microsoft-tenant/cloudomgeving van de LVO organisatie. Dit betreft zowel werkplekken voor de medewerkers als t.b.v. leerlingen op de schoollocaties (bijv. computerlokalen, mediatheek, shared werkplekken, etc). Het werkplekbeheer is ingericht volgens het Modern Management-principe, waarbij inrichting, beveiliging en onderhoud grotendeels via de cloud worden uitgevoerd.

Alle werkplekken binnen LVO draaien op Windows en zijn geïntegreerd binnen Entra ID. De apparaten worden centraal beheerd via Microsoft Intune. De inrichting van nieuwe werkplekken verloopt volledig geautomatiseerd via Windows Autopilot.

Voor endpoint beveiliging maakt LVO gebruik van Microsoft Defender for Endpoint (DFE), dat actief toezicht houdt op dreigingen, antivirusstatus en compliance. Deze oplossing is geïntegreerd binnen Intune, waardoor real-time beheer en rapportage over de gehele werkplekomgeving mogelijk zijn.

Het operationele beheer van de werkplekken wordt uitgevoerd door de MSP.

MDM

Het Mobile Device Management (MDM) binnen LVO is eveneens gebaseerd op Microsoft Intune. De MDM-configuratie is momenteel gericht op werkplekken en niet op mobiele apparaten. Via Intune worden gebruikersprofielen, beleidsregels, applicaties en instellingen centraal uitgerold op basis van gebruikersgroepen en device categorieën. Dit zorgt voor een consistente configuratie en beveiligingsstandaard binnen de gehele organisatie.

CA en PKI

De certificaatinfrastructuur van LVO is ondergebracht in de Azure-omgeving van de stichting. Binnen deze omgeving draait een eigen Microsoft Certificate Authority (CA) die fungeert als Private Key Infrastructure (PKI) voor de organisatie, welke wordt gebruikt voor:

- 802.1X-authenticatie van werkplekken via EAP-TLS,
- het uitgeven en beheren van device certificaten,
- het ondersteunen van beveiligde communicatie binnen de beheerde omgeving.

De PKI-omgeving wordt beheerd door de MSP onder regie van LVO.

Datacenter

De ICT-infrastructuur van Stichting LVO is ingericht volgens een hybride model, bestaande uit een cloudomgeving in Microsoft Azure, een fysieke colocatie in Equinix AM7, evenals een beperkte on-premises component op locatie. Deze opzet combineert de schaalbaarheid van cloud met de noodzakelijke lokale beschikbaarheid voor specifieke toepassingen.

Azure

De primaire infrastructuur van LVO is ondergebracht binnen de Microsoft Azure-regio West-Europa. Deze omgeving fungeert als private cloud binnen de eigen Azure-tenant van LVO en bevat de centrale infrastructuur- en beheerdiensten van de organisatie. Het netwerkverkeer tussen Azure en het LVO-netwerk loopt via een beveiligde verbinding met de Equinix-locatie, waar de koppeling met het SIVON-WAN tot stand komt. De omgeving is redundant uitgevoerd en vormt het hart van de centrale ICT-diensten van LVO. Beheer vindt plaats door de MSP onder regie van LVO.

Equinix

LVO beschikt over een half rack in het Equinix AM7-datacenter. Deze colocatie fungeert (uitsluitend) als ontsluiting/koppel-punt tussen het SIVON-netwerk en de Azure-omgeving van LVO. Derhalve worden hier geen productiesystemen of data gehost. De opstelling bestaat uit één core switch en twee Fortigate 100F-firewalls, waarmee veilige verbindingen tussen de cloud- en WAN-omgeving worden gerealiseerd. Beheer vindt plaats door de MSP onder regie van LVO.

Onpremise

Binnen het LAN van LVO bevindt zich nog één lokale ESX-host, uitsluitend bedoeld voor het uitvoeren van FACET-examens. Deze host blijft operationeel tijdens eventuele WAN-storingen, zodat de examenfunctionaliteit onafhankelijk van de internetverbinding beschikbaar blijft. De MSP is verantwoordelijk voor het dagelijkse technisch beheer en de operationele monitoring.

WAN

Het Wide Area Network (WAN) van Stichting LVO is volledig gebaseerd op de Veilig Internet-dienst van SIVON. Deze dienst vormt de beveiligde backbone waarlangs alle onderwijs- en ondersteunende locaties van LVO met elkaar, met de cloud-omgevingen en met het Internet zijn verbonden.

Elke LVO-locatie beschikt over een eigen WAN-aansluiting via SIVON, gekoppeld aan een Fortigate 100F-firewall die lokaal als CPE fungeert. Vanuit deze firewalls loopt al het netwerkverkeer over het SIVON-WAN, waar de filtering, beveiliging en routing centraal worden afgehandeld.

Binnen het Netwerkdiensten Centrum (NDC) beschikt ieder Schoolbestuur over een eigen, modern beheerde firewall. Deze *Schoolbestuur-firewall* vormt een essentieel onderdeel van de beveiligingsarchitectuur en biedt zowel generieke als Schoolbestuur-specifieke beveiligingsmaatregelen.

SIVON past onderstaande realtime beveiligingsmaatregelen toe voor LVO:

- DDoS-filtering: bescherming tegen grootschalige aanvallen die netwerkverkeer overbelasten en de beschikbaarheid van internetdiensten verstoren.
- Intrusion Prevention System (IPS): automatische detectie en blokkering van kwaadaardig verkeer, gericht op het voorkomen van exploits en misbruik van kwetsbaarheden.

Dit zijn generieke maatregelen en worden door SIVON beheerd en waar nodig bijgesteld.

LVO heeft daarnaast de mogelijkheid om eigen beleidskeuzes en configuraties toe te passen binnen de firewalls. Deze specifieke maatregelen omvatten:

- Verkeerfilters (firewall policies): LVO bepaalt zelf welke soorten verkeer van en naar internet toegestaan zijn.
- Webfiltering: beperking van toegang tot schadelijke, ongewenste of ongeschikte websites, met doelen als anti-malwarebescherming en het bevorderen van een veilige leer- en werkomgeving.
- Application control: regulering van toegang tot applicaties en applicatiecategorieën die buiten reguliere webverkeer vallen.

De basisconfiguraties voor deze onderdelen worden door SIVON aangeboden, maar kunnen door LVO worden aangepast aan de eigen context en beleidswensen.

De dienst voorziet in een redundante landelijke infrastructuur, waarbij het internetverkeer via de beveiligde SIVON-koppelingen verloopt. Het WAN vormt tevens de verbindende laag tussen de locaties van LVO, de Equinix-ontsluiting en de Azure-omgeving.

Binnen de Veilig Internet-dienst worden web- en contentfilters toegepast op basis van categorieën, die centraal door SIVON worden beheerd. LVO kan wijzigingen of uitzonderingen aanvragen via een gestandaardiseerde changeprocedure.

Voor examenaccounts wordt gebruikgemaakt van een dienst op basis van de Forti Single Sign-On (SSO) Agent op de LVO domain controller. Bij het inloggen van een examenaccount registreert de SSO-agent de gebruiker automatisch bij de firewall en plaatst deze in een speciale examengroep. De firewall past daarop direct een beperkt internetbeleid toe, zodat alleen de voor examens toegestane diensten beschikbaar zijn. Hiermee wordt het toepassen van examenrestricties volledig geautomatiseerd en centraal beheerd.

Verkeer tussen de locaties en de centrale diensten (zoals Azure) verloopt volledig via het SIVON-WAN. VPN-tunnels tussen locaties of naar het datacenter worden binnen deze infrastructuur door SIVON beheerd. De VLAN-segmentatie van het LAN sluit direct aan op de WAN-structuur, waardoor scheiding tussen onderwijs-, beheer- en gastverkeer ook over de WAN-verbinding behouden blijft.

Het dagelijks beheer, inclusief monitoring van bandbreedte, uptime en beveiligingsincidenten, ligt bij SIVON. LVO vervult de regierol. Rapportages en netwerkstatistieken zijn voor LVO inzichtelijk via het

SIVON-portaal en via de periodieke service overleggen.

VoIP

De VoIP-omgeving maakt gebruik van Microsoft Teams Calling als telefonieplatform. Voor vaste toestellen worden Yealink-apparaten ingezet die voorzien zijn van Microsoft Teams. De toestellen worden van voeding voorzien via Power over Ethernet (PoE) en zijn aangesloten op een separaat VLAN dat specifiek is ingericht voor VoIP-verkeer. De SBC's van zijn in het beheer van Vodafone en connecteren op de LVO M365-tenant.