

DIENSTBESCHRIJVING

DELTA Zakelijk Managed SDN

(Software Defined Networking)

NOVEMBER 2025 | VERSIE 3.0
DOCUMENT 20251114





DELTA en DELTA Zakelijk zijn handelsnamen van DELTA Fiber Nederland B.V. en van enkele groepsmaatschappijen. DELTA Fiber Nederland B.V. is een besloten vennootschap met statutaire zetel in Middelburg en geregistreerd bij de Kamer van Koophandel onder nummer 22051676. DELTA Fiber Nederland B.V. is de moedermaatschappij van DELTA Mobiel B.V. Voor verdere informatie zie www.delta.nl.

Inhoud

Algemeen _____	3	3.10 SD-Cloud _____	13
1.1 DELTA Zakelijk Managed SDN _____	3	3.10.1 Aanvullende Diensten SD-Cloud _____	13
1.2 Dienstbeschrijving _____	3	3.10.2 Hub-and-Spoke VPN _____	13
1.3 Contractuele looptijd _____	3	3.10.3 Internet Toegang Cloud Gateway _____	14
Standaard Diensten _____	3	3.10.4 MPLS-migratie _____	14
2.1 Introductie _____	3	Aanvullende diensten _____	14
2.2 Connectiviteit _____	3	4.1 Internet _____	14
2.3 Gateway _____	4	4.2 Managed Voice _____	14
2.4 Koppelvlakken _____	4	4.3 TV _____	15
2.5 Router _____	4	Installatie _____	15
2.6 Firewall _____	4	5.1 Implementatie _____	15
2.7 Site-to-Site VPN _____	4	5.1.1 Stappenplan _____	15
2.8 WAN Redundancy _____	5	5.2 Levering _____	15
2.9 Beheer _____	5	5.3 Beheer _____	16
2.10 Rapport _____	5	5.4 Wijzigingen _____	16
Opties _____	6	Service _____	18
3.1 Advanced Firewall _____	6	6.1 Algemeen _____	18
3.2 Mobile WAN redundancy _____	7	6.2 Zakelijke Helpdesk _____	18
3.3 SDN Cloud-Connect _____	7	Product voorwaardelijk _____	18
3.4 IP- en E-VPN _____	7	7.1 SDN _____	18
3.5 Remote Access _____	7	7.2 SD-WAN _____	19
3.6 High Availability Cluster _____	8	7.3 SD-(W)LAN _____	19
3.7 Periodiek Veiligheidsgesprek _____	8	7.4 SD-Cloud _____	20
3.8 Advanced Analytics _____	8		
3.9 SDN LAN en WLAN _____	8		
3.9.1 Onderdelen _____	9		
3.9.2 Bedraad netwerk (LAN Switches) _____	9		
3.9.3 Draadloos Netwerk (SD-WLAN) _____	10		
3.9.4 Optionele Verbindingsmodules _____	11		
3.9.5 Radioplan _____	11		
3.9.6 Captive portal _____	12		

Algemeen

1.1 DELTA Zakelijk Managed SDN

DELTA Zakelijk Managed Software Defined Networking (SDN) is een verzamelnaam voor de telecommunicatiedienst die in een breed scala van netwerkdiensten voorziet, zowel op Local Area Network (LAN) als op Wide Area Network (WAN) niveau. Deze Dienst is door DELTA Zakelijk ontwikkeld en bedoeld voor Zakelijke toepassingen. U kunt de SDN-dienst uitbreiden met opties zoals Internet-, Ethernet VPN- en/of IP-VPN verbindingen.

1.2 Dienstbeschrijving

Deze Dienstbeschrijving is aanvullend op de Algemene Leveringsvoorwaarden DELTA Zakelijk 2023. Beide vindt u op de website van DELTA Zakelijk. Het webadres is www.delta.nl/klantenservice/algemene-voorwaarden. Daar waar de dienstbeschrijving en de Algemene Leveringsvoorwaarden elkaar tegenspreken, refereert deze dienstbeschrijving.

1.3. Contractuele looptijd

De looptijd van uw DELTA Zakelijk Managed SDN abonnement staat vermeld in uw overeenkomst.

Standaard Diensten

2.1 Introductie

SDN van DELTA Zakelijk geeft inzicht in en controle over de verkeersstromen, de gebruikers en de applicaties. De basis is voorzien van een groot aantal securityonderdelen en intelligentie die met elkaar de beveiliging van het netwerk versterken. Dat betekent dat ze slim inspelen op de daadwerkelijke bedreigingen op dat moment. Hiermee wordt de kans op herkenning van mogelijke risico's vergroot en kunnen er mitigerende maatregelen genomen worden om (ernstige) impact te voorkomen.

SDN van DELTA Zakelijk is in staat om applicaties, locaties en gebruikers te herkennen en daarop verkeersstromen aan te passen. Ook zorgt de intelligentie in het netwerk ervoor dat verkeersstromen automatisch de beste weg vinden en transport zichzelf kan herstellen.

De intelligentie in het SD-WAN van DELTA Zakelijk zorgt niet alleen voor het optimaal gebruiken van de bandbreedte, het stuurt ook het verkeer via de beste route, om eventuele netwerkproblemen te voorkomen. Omdat het netwerk flexibel te configureren is, kunt u bepalen welke verkeersstromen voorrang krijgen boven andere. Zo kan telefonie voorrang krijgen op data, of Microsoft 365 op YouTube-verkeer.

2.2 Connectiviteit

DELTA Zakelijk SD-WAN maakt het mogelijk een veilig bedrijfsnetwerk (WAN) te maken met meerdere locaties. Hiervoor is connectiviteit nodig ofwel 'data-transport'. Qua onderliggende netwerktopologie maakt het niet uit, het kan regulier internet zijn of een Ethernet- of IP-VPN dienst.

Het maakt niet uit of de connectiviteit bij DELTA Zakelijk wordt afgenomen of dat de verbinding via een andere provider is ingekocht. Zelfs mobiel internet kan gebruikt worden om een veilig WAN te maken. Aan de inbreng van bij derden ingekochte verbindingen zijn wel voorwaarden verbonden. Bijvoorbeeld dat uw primaire netwerk voor het grootste deel uit DELTA Zakelijk verbindingen moet bestaan en dat DELTA uit naam van de Contractant technische beslissingen mag maken richting de Service Provider aangaande verstoringen.

Underlay is geen onderdeel van de SDN-dienstverlening. Underlay als in Internet, E-VPN en of IP-VPN van DELTA Zakelijk kennen eigen dienstbeschrijvingen.

2.3 Gateway

Op elke locatie van uw organisatie wordt een SD-WAN gateway in bruikleen geplaatst. De SD-WAN gateway fungeert op de bedrijfslocatie als een basis voor alle SDN-diensten die daar worden afgenomen. De beschikbare standaard gateways waaruit gekozen kan worden zijn:

Gateways	Type 1	Type 2	Type 3
WAN	1GE	10GE	10GE
Firewall capaciteit	5.000 Mbit/s	28.000 Mbit/s	39.000 Mbit/s
Advanced firewall capaciteit	1.000 Mbit/s	2.200 Mbit/s	2.800 Mbit/s

Maatwerk gateways zijn beschikbaar voor speciale oplossingen. Optioneel kan ook een high-availability setup gekozen worden met een active/passive failover.

2.4 Koppelvlakken

Snelheid		IEEE-Standaard	Patchkabel
1.000 Mbit/s	1000Base-T	802.3ab	Cat.6a of hoger
1.000 Mbit/s	1000Base-SX	802.3z	Multimode-glasvezel
10.000 Mbit/s	10GBase-T	802.3an	Cat.6a of hoger
10.000 Mbit/s	10GBase-SR	802.3ae	Multimode-glasvezel

2.5 Router

De router regelt het dataverkeer tussen het WAN en het LAN. DELTA Zakelijk verzorgt de provisioning, configuratie, wijzigingsbeheer en monitoring voor de router op locatie. De managed router is geïntegreerd in de SD-WAN gateway.

2.6 Firewall

Firewalls vormen de eerste verdedigingslinie binnen netwerk security. Ze vormen een barrière tussen beveiligde en beheerde interne netwerken die kunnen worden vertrouwd en niet-vertrouwde externe netwerken, zoals het internet.

Uw SD-WAN gateway beschikt over een krachtige Next Generation Firewall die inkomend en uitgaand netwerkverkeer bewaakt en bepaalt welk verkeer wordt toegestaan of geblokkeerd op basis van een vooraf gedefinieerde set securityregels.

Standaard voert de firewall stateful inspection uit en laat verkeer toe of blokkeert dit op basis van status, poort en protocol. Al het netwerkverkeer wordt bewaakt, vanaf het moment dat een verbinding wordt geopend totdat deze wordt gesloten. Filter beslissingen worden genomen op basis van zowel door de beheerder gedefinieerde regels als context, dat wil zeggen het gebruik van informatie van eerdere verbindingen en pakketten die tot dezelfde verbinding behoren.

Het is mogelijk om optioneel de firewall te upgraden naar een advanced firewall. Deze combineert de functies van een stateful inspection firewall met onder andere inbraakpreventie en antimalware.

2.7 Site-to-Site VPN

VPN staat voor Virtual Private Network en zorgt voor een besloten bedrijfsnetwerk. Naast het virtueel koppelen van locaties kunnen ook medewerkers die hybride werken of gebruik maken van Clouddiensten gebruik maken van deze VPN dienst.

Een SD-WAN VPN is flexibeler dan bestaande MPLS-netwerken, omdat het netwerk altijd softwarematig aangepast kan worden, snel kan op- en afschalen in bandbreedte en nieuwe locaties veilig kan aansluiten of ontsluiten.

SD-WAN optimaliseert de netwerkprestaties van uw VPN door dynamische routing van verkeer over verschillende paden op basis van real-time omstandigheden, zoals bandbreedte, latency en packet loss.

2.8 WAN Redundancy

SD-WAN biedt flexibiliteit om verbindingen van verschillende providers en technologieën te gebruiken, waardoor organisaties niet afhankelijk zijn van één enkele provider. Dit biedt meer keuzevrijheid en kan kostenbesparingen opleveren.

Via WAN Redundancy maakt u gebruik van meerdere internetverbindingen, zoals glasvezel, DSL of Coax, en wordt gebruik gemaakt van automatische failover-mechanismen om de WAN-beschikbaarheid te optimaliseren. Hierdoor blijven bedrijfskritieke applicaties beschikbaar, zelfs bij uitval van een netwerkverbinding.

Daarnaast is het mogelijk om verschillende vormen van verkeer via verschillende WAN-verbindingen te routeren om zo verkeerstromen te prioriteren. SD-WAN optimaliseert de netwerkprestaties door dynamische routing van verkeer, over verschillende WAN-koppelingen en op basis van real-time omstandigheden, waardoor de netwerkprestaties en uptime optimaal zijn.

De optie voor het aansluiten van 2 WAN lijnen is standaard voorzien in de SD-WAN gateway, er zijn geen extra maandelijkse kosten verbonden aan deze optie zolang het standaard koppelvlak 1000Base-T gebruikt wordt.

2.9 Beheer

Deze zakelijke dienst wordt geleverd als “managed service”. Hierbij inbegrepen zijn aanschaf, onderhoud, configuratie, beheer en vervanging (in geval van defect zonder opzet) van de voor deze dienst geïnstalleerde eindapparatuur op de klantlocatie.

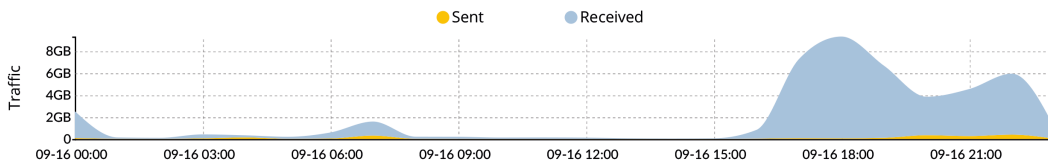
DELTA Zakelijk draagt zorg voor proactief beheer, software updates en patches, waardoor u verzekerd bent van een hoge beschikbaarheid.

2.10 Rapport

U krijgt maandelijks een pdf-rapport met daarin uitgebreide informatie en analyses over de prestaties van uw SDN-omgeving. De onderwerpen die in het rapport aan bod komen zijn afhankelijk van de door u gekozen dienstonderdelen.

Dit rapport is waardevol voor uw netwerkbeheerders, IT-managers en andere belanghebbenden om geïnformeerde beslissingen te nemen over netwerkbeheer, beveiliging en optimalisatie. Het rapport draagt ook bij in het aantonen van beveiligingsmaatregelen richting derden voor bijvoorbeeld NIS2-compliance.

Daily Summary Report Data between 2024-09-16 00:00:00 and 2024-09-16 23:59:59CEST



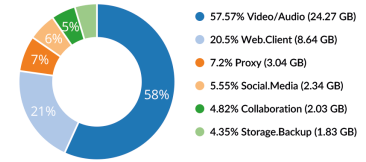
46.33 GB

Traffic Usage

Top Application by Severity

#	Application	Category	Risk	Sessions	Blocked	Allowed	Bytes	Sent	Received
1	Proxy.HTTP	Proxy	5	308	308	0	308	1.34 MB	1.34 MB
2	SOCKS5	Proxy	5	28	28	0	28	51.04 KB	51.04 KB
3	SOCKS4	Proxy	5	3	3	0	3	5.14 KB	5.14 KB
4	RDP	Remote.Access	4	330	330	0	330	15.28 KB	15.28 KB
5	VNC	Remote.Access	4	75	75	0	75	2.36 KB	2.36 KB

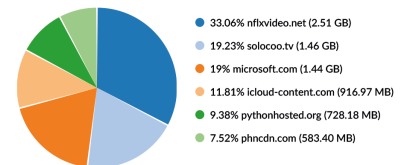
Top Application Category



Top Threat

#	Threat	Category	Threat Score	Blocked	Allowed	Incidents	Blocked	Allowed
1	Failed Connection	Failed Connection	102,165	102,165	0	20,433	20,433	0
2	mask-h2[dot]icloud[dot]com	Proxy Avoidance	7,090	7,090	0	709	709	0
3	mask[dot]icloud[dot]com	Proxy Avoidance	4,860	4,860	0	486	486	0
4	api[dot]mullvad[dot]net	Proxy Avoidance	1,080	1,080	0	108	108	0
5	Proxy[dot]HTTP	Proxy	970	970	0	97	97	0

Top Website by Traffic



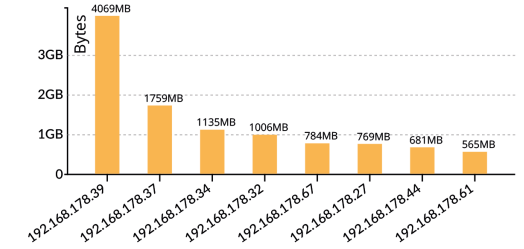
Incidents by Severity

No matching log data for this report

Compromised Host

No matching log data for this report

Top User by Traffic



Opties

3.1 Advanced Firewall

Cybercriminelen vinden steeds creatievere manieren om ongeautoriseerde toegang tot bedrijfsmiddelen te verkrijgen. Ze brengen de veiligheid en continuïteit van bedrijfsvoeringen in gevaar door bekende en onbekende kwetsbaarheden te misbruiken. Hackers vallen niet alleen bedrijfsnetwerken aan, zij proberen ook met geavanceerde malware, ransomware, bots, drive-by-downloads en phishing medewerkers te misleiden.

DELTA Zakelijk heeft voor de versterkte beveiligingstoepassingen de Advanced Firewall met de volgende extra faciliteiten ten opzichte van de basis Firewall:

- **Identity Awareness:** Met de Identity Awareness-functie kunt u voor verschillende doelgroepen andere (beleid)regels of policies gebruiken. De toegestane mogelijkheden in het gebruiken van het internet is bijvoorbeeld voor gasten of leerlingen anders in te stellen dan die voor vaste werknemers of docenten.
- **Blokkering kwaadwillend verkeer (IPS):** Standaard bevat de firewall al een signalering op kwaadwillend gedrag en verkeer. Hiermee wordt veel kwaadwillend verkeer dat uw netwerk probeert binnen te dringen, gesignaleerd. Met de advanced firewall wordt dat gesignaleerde verkeer ook vaak tegengehouden.
- **Anti-Malware:** Malware is een verzamelnaam voor veel soorten bedreigingen zoals: virussen, wormen, spyware, ransomware, Trojan horses, adware en key-loggers. De optie Anti-Malware biedt daar een betere bescherming tegen.
- **Anti-Bot:** Als apparatuur op het interne netwerk onbedoelde of onwenselijke software bevat, kan deze software, zodra er contact gemaakt wordt met het netwerk, op zoek gaan naar een externe online command-and-control-server. Als de software daarin slaagt, ontstaat het risico dat de omgeving wordt overgenomen door een externe partij, meestal een kwaadwillende. De Antibot-functionaliteit herkent dit type verkeer en kan dit stoppen, voordat deze software ongewenst verkeer gaat generen, waardoor netwerkapparatuur bijvoorbeeld de bron kan worden van D(D)oS-aanvallen.

- **Application Control:** Application Control zorgt voor het besturen en controleren van het gebruik van applicaties. Op applicatieniveau kan bepaald worden of deze gebruikt mogen worden of niet. Zo kan het gebruik van YouTube of televisiekijken in een zakelijke omgeving worden uitgezet, terwijl conferentieapplicaties wel zijn toegestaan.
- **Web Filtering:** Blokkeert toegang tot kwaadaardige domeinen/websites (malware, phishing, spam).
- **Anti-Spam:** Verminder de hoeveelheid spam en beschermd tegen e-mailbedreigingen.

DELTA Zakelijk hanteert het beleid dat de advanced firewall optie niet per individuele SD-WAN-locatie kan worden afgenomen, maar alleen voor alle locaties (dus voor alle SD-WAN gateways). Verrekening vindt dan plaats per locatie. Bij een actieve-/passive- configuratie betaalt u alleen voor de locatie (dus per active-/ passive-SD-WAN-configuratie).

3.2 Mobile WAN redundancy

Om in geval van een onverhoopte storing aan de (internet) connectiviteit toch beschikbaarheid van data-transport te garanderen biedt Mobile WAN redundancy uitkomst. DELTA Zakelijk biedt een effectieve WAN- failover oplossing via het mobiele netwerk. Als de primaire lijnverbinding uitvalt, zorgt deze voorziening ervoor dat het SD-WAN-verkeer wordt overgenomen door de secundaire mobiele-verbinding. Als de primaire verbinding weer is hersteld, schakelt het verkeer weer terug en dient de mobiele verbinding weer als back-up. Zo zal uw bedrijf zelden offline raken en verkleint u de kans dat uw kritische bedrijfsprocessen stilliggen.

Naast de mogelijkheid van een back-up-voorziening, kunt u er ook voor kiezen om een primaire voorziening over het mobiele netwerk te laten realiseren door DELTA Zakelijk. Op deze manier biedt DELTA Zakelijk u een alternatief voor een vaste lijnverbinding. Voorbeelden hiervan zijn locaties waar u tijdelijk een verbinding nodig hebt en waar de aanleg van een vaste verbinding veel doorlooptijd kent of als primaire mobiele- verbinding.

DELTA Zakelijk levert de simkaart die nodig is om de mobiele WAN redundancy in te richten. De Simkaart met het dataabonnement kent haar eigen voorwaarden, deze zijn te downloaden via www.delta.nl/klantenservice/algemene-voorwaarden.

3.3 SDN Cloud-Connect

De SDN Cloud Connect service geeft een veilige verbinding met één of meer publieke en/of private Cloud providers. Denk hierbij aan SaaS-oplossingen als Microsoft 365, Salesforce en Exact-online maar ook IaaS oplossingen als Microsoft Azure, Google Cloud, Oracle Cloud en AWS.

3.4 IP- en E-VPN

IP-VPN en E-VPN kunnen volledig geïntegreerd worden binnen een SD-WAN-oplossing, waarbij ze functioneren als onderliggende transportlagen. In deze hybride architectuur biedt SD-WAN de intelligentie en het beleid gedreven beheer, terwijl IP-VPN en E-VPN zorgen voor robuuste, betrouwbare connectiviteit met gegarandeerde Service Level Agreements (SLA's).

Met de SDN-gebaseerde netwerkinfrastructuur biedt DELTA Zakelijk IP-VPN en E-VPN aan als schaalbare, veilige en flexibel te beheren netwerkdiensten. IP-VPN garandeert betrouwbare point-to-point en any-to-any connectiviteit, terwijl EVPN een moderne, efficiënte benadering biedt voor Ethernet-multipoint diensten. Dankzij software-defined networking is provisioning sneller en volledig geautomatiseerd, met realtime netwerkinzichten en centraal beheer. Klanten profiteren van lagere operationele kosten, verhoogde netwerkzichtbaarheid en flexibeler beheer. E-VPN ondersteunt bovendien segmentatie en multitenancy, dit is ideaal voor complexe klantomgevingen.

3.5 Remote Access

Thuiswerken valt of staat met een stabiele verbinding met het kantoor netwerk. Als u vanuit huis werkt, is toegang nodig tot o.a. bestanden om werkzaamheden uit te voeren. Een VPN-verbinding zorgt niet alleen dat u uw computer thuis verbinding maakt met het bedrijfsnetwerk, maar ook dat uw computer gezien wordt als onderdeel van dat netwerk. Hierdoor heeft u via uw eigen computer toegang tot bedrijfsbestanden, -printers en -applicaties. Deze verbinding moet bovendien versleuteld worden zodat gevoelige data niet gemakkelijk kan worden onderschept. Met de Remote Access dienst kunt u een veilige VPN- verbinding opzetten naar uw bedrijfsnetwerk. Daarbij is het

verplicht gebruik te maken van two-factor-authenticatie (2FA) op basis van een app. Ook is het optioneel tegen meerprijs mogelijk gebruik te maken van een SAML/LDAP/AD koppeling.

3.6 High Availability Cluster

Als u zich zorgen maakt over uw bedrijfscontinuïteit, dan kunt u kiezen voor het inrichten van een active/passive-cluster. Dit is een configuratie waarbij er 2 identieke SD-WAN gateways worden ingezet op uw locatie. Eén van deze SD-WAN gateways is daarbij geconfigureerd als actief (active) en de andere als passief (passive).

In een active/passive cluster is er altijd een passieve gateway stand-by om onmiddellijk de actieve gateway over te nemen in geval van storing. Dit minimaliseert downtime en verhoogt de beschikbaarheid van het netwerk. Door de redundantie van de passieve node wordt de betrouwbaarheid van het netwerk aanzienlijk verbeterd, aangezien er altijd een back-up beschikbaar is.

In een normale situatie neemt de actieve gateway al het netwerkverkeer voor zijn rekening. Valt de actieve gateway uit, dan neemt de passieve gateway deze taak bijna naadloos over. U kunt zelfs de actieve en passieve gateway laten installeren met 2 internetverbindingen en de verbindingen koppelen aan verschillende netwerkpaden voor maximale beschikbaarheid.

3.7 Periodiek veiligheidsgesprek

Het security landschap is continu in beweging. Daarom is het wenselijk om periodiek te beoordelen of de huidige beveiligingsmaatregelen nog wel afdoende bescherming bieden en of er aanpassingen nodig zijn. Dit kan door historische informatie uit uw SD-WAN Gateway(s) te combineren met uw gewijzigde organisatie- en of securitybeleid.

Hiervoor biedt DELTA Zakelijk de betaalde optie om een periodiek veiligheidsgesprek te voeren met één van onze experts. Dit biedt periodiek advies en ondersteuning met betrekking tot waargenomen trends en bedreigingen. Deze worden u gemeld in de vorm van rapportages, inclusief aanbevelingen voor het treffen van reactieve maatregelen op basis van een gedocumenteerd voorstel voor verfijning en verbetering van uw standaardinstellingen en beschermingselementen.

U kunt tegen additionele kosten er voor kiezen om periodiek (om de 3 maanden) een veiligheidsgesprek te voeren.

3.8 Advanced Analytics

Sommige bedrijven willen meer gedetailleerd inzicht hebben in hun netwerk en de cyberdreigingen. Daarvoor biedt DELTA Zakelijk, als onderdeel van de SDN- dienstverlening, de Advanced Analytics dienst aan.

De Advanced Analytics dienst integreert netwerk logging, analyses en rapportage in één systeem, waardoor u meer inzicht krijgt in de staat van beveiliging binnen uw bedrijfsnetwerk.

De standaard pdf-rapportage die inbegrepen is bij de SD-WAN dienst biedt een maandelijks pdf-rapport en een maximale retentietijd van uw logfiles van 1 maand. Met de Advanced Analytics dienst kunt u zelf de retentietijd van uw logfiles bepalen en op die wijze analyses uitvoeren over langere periodes.

Advanced Analytics is een managed service die volledig ingericht is en beheerd wordt door DELTA Zakelijk. DELTA Zakelijk biedt ook de mogelijkheid om een training te volgen om het maximale uit deze service te halen.

3.9 SDN LAN en WLAN

Met Software Defined LAN (SD-LAN) van DELTA Zakelijk krijgt u de beschikking over een bedrijfsnetwerk voor uw locaties dat veilig, flexibel en inzichtelijk is. SD-LAN van DELTA Zakelijk bevat de Switches (Local Area Network/LAN) en Accesspoints (Wireless Local Area Network/WLAN) op een locatie van uw organisatie.

Investeren in kennis van complexe netwerktechnologie is verleden tijd, omdat u kunt bouwen op de kennis en kunde van de experts van DELTA Zakelijk.

Aan de hand van uw specifieke wensen en eisen bepalen we samen de beste configuratie voor uw locatie(s). Op basis daarvan implementeren we het SD-(W)LAN-netwerk bij u. Dit netwerk is en blijft technisch up-to-date en (ver)storingen proberen we, waar mogelijk, vooraf te voorkomen.

SD-(W)LAN is onderdeel van DELTA Zakelijk SDN. Op de SD-(W)LAN-dienstverlening zijn dezelfde servicelevel afspraken van toepassing als op DELTA Zakelijk SDN, tenzij anders aangegeven in deze dienstbeschrijving.

3.9.1 Onderdelen

De SD-(W)LAN-dienst bestaat uit verschillende onderdelen waarmee bijna alle mogelijke oplossingen gebouwd kunnen worden. Sommige van deze onderdelen zijn standaard. Dat wil zeggen dat het vaste onderdelen van de dienst zijn, die u altijd afneemt, of u deze nu gebruikt of niet. Andere onderdelen kunt u optioneel afnemen. De verschillende onderdelen en opties en hun afhankelijkheid (standaard of niet) vindt u terug in de tabel hieronder.

3.9.2 Bedraad netwerk (LAN Switches)

Netwerkbeheer is erg complex en kent verschillende disciplines die nauw met elkaar verbonden zijn. DELTA neemt graag het LAN-beheer uit handen.

LAN Switches ⁽¹⁾	Standaard
Wireless Access Points (AP) ^(2, 3)	Standaard
Rapportage	Standaard
Verbindingsmodules	Optioneel
Radioplan	Optioneel
Captive portal	Optioneel

¹ Niet beschikbaar zonder SD-WAN gateway op locatie

² Niet beschikbaar zonder SD-LAN switch(es)

³ Met uitzondering van 1 AP, deze wordt op de gateway aangesloten via een PoE adapter

Onze secure access switches worden eenvoudig beheerd in ons SDN-platform dat fungeert als één centraal punt voor beheer en configuratie. Op deze manier kunnen we uw netwerk optimaal beheren en onderhouden.

SD-LAN is software defined. Hierbij is de intelligente besturing vanuit een centrale omgeving vormgegeven. Deze kan de intelligente apparatuur op locatie effectief aansturen en controleren.

SD-LAN leveren we altijd inclusief standaard universele apparatuur (met licenties), welke bedrade aansluitsnelheden van 10 Mbit/s tot en met 1.000 Mbit/s ondersteunt voor eindgebruiker-apparaten.

Ook voorziet de apparatuur bijvoorbeeld IP voice toestellen, camera's of Access Points van stroom via Power over Ethernet (POE).

De beschikbare switches waaruit gekozen kan worden zijn:

- Switch 8-poorts, met PoE 130W
- Switch 24-poorts, met PoE 370W
- Switch 48-poorts, met PoE 740W

Bij de meest uitgebreide netwerken is het mogelijk om aggregatieapparatuur in te zetten en verkeer te bundelen. Zo kunnen snelheden gehaald worden van meer dan 40 Gbit/s.

Uw keuze zal afhankelijk zijn van bijvoorbeeld het verwachte bandbreedteverbruik, de hoeveelheid Wireless Access Points, het type bekabeling en het aantal apparaten en de wijze waarop deze gebruikmaken van power-over-ethernet (PoE).

Om veel tijd te besparen aan het uitzoeken en uitkiezen van de beste configuratie hebben we vanuit onze kennis en ervaring standaard SD-LAN-profielen ontwikkeld:

- Klein (8-192 poorten en 1 technische ruimte)
- Middel (193-768 poorten per locatie of 2-4 technische ruimtes)
- Groot (meer dan 768 poorten of meerdere gebouwen/ complexe omgeving)

Bij de bedraadde profielen “Middel” en “Groot” moet altijd een vooropname op uw locatie worden gemaakt. De precies benodigde aantallen, typen netwerkbouwblokken, opties en bijbehorende kosten zullen vastgesteld worden na deze vooropname (site survey). Bij het bedraadde profiel “Klein” is er geen vooropname nodig en zullen de beste configuratie en de benodigde aantallen door DELTA Zakelijk bepaald worden.

Er is altijd een DELTA Zakelijk SD-WAN gateway op de locatie nodig om SD-LAN bedraad te kunnen inrichten. Daarnaast is het beleid van DELTA Zakelijk dat de Contractant zorg moet dragen voor alle interne bekabeling, patchkasten, stroomvoorziening, koeling en eventuele andere zaken die op de locatie noodzakelijk zijn om de dienstverlening te kunnen verrichten en te kunnen garanderen.

3.9.3 Draadloos Netwerk (SD-WLAN)

SD-WLAN is een goede oplossing voor het bouwen van een Wi-Fi-netwerk met één of meerdere hoogwaardige Wireless Access Points. Zowel voor binnen en buiten kan eenvoudig een betrouwbaar draadloos netwerk gemaakt worden, inclusief een scheiding in het netwerk voor medewerkers en bezoekers.

De SD-WLAN apparatuur biedt u een intelligent netwerk waarmee u verkeersstromen op diverse niveaus kunt filteren, reguleren en rechten kunt geven. Bijvoorbeeld op applicatieniveau, gebruikersniveau, groepsniveau, (soort) apparaat, locatie, maar ook op tijdgebonden filters. De mogelijkheden tot filtering, regulering en rechtenbeheer werkt rol-gebaseerd.

Voor de draadloze omgeving leveren we altijd apparatuur (met licenties), die de gestandaardiseerde en relevante Wi-Fi-standaarden ondersteunt (Wi-Fi 6).

Ook voorziet de apparatuur in oplossingen voor specifieke omgevingen. Hierdoor is het mogelijk om voor bijna elk draadloze omgeving een passende oplossing te bouwen. De beschikbare Wireless Access Points waaruit gekozen kan worden zijn:

- Indoor
- Outdoor
- Hospitality

Draadloze signalen kunnen ook door derden worden ontvangen. Om privacy te waarborgen is versleuteling van data daarom gewenst. Dataverkeer op het Wi-Fi-netwerk met zakelijke toepassing wordt versleuteld volgens de WPA2 of WPA3 standaard. WPA2 is de industriestandaard binnen Wi-Fi-beveiliging. Met WPA2-beveiliging neemt DELTA Zakelijk maatregelen om het netwerk van de Contractant te beschermen.

De SD-WLAN dienst biedt standaard ook een gastennetwerk. Een gastennetwerk is een paswoord beveiligd Wi-Fi-netwerk en biedt gebruikers alleen toegang tot het internet. Via “client-isolation” wordt voorkomen dat apparaten op het gastennetwerk elkaar kunnen zien.

DELTA adviseert de Contractant bij het inrichten van de beveiliging, echter blijft de eindverantwoordelijkheid bij de Contractant. Ook waar het gaat over de verwerking van persoonsgegevens blijft de Contractant zelf verantwoordelijk.

DELTA Zakelijk is uitdrukkelijk niet aansprakelijk voor eventuele schade als gevolg van een inbraak op het Wi-Fi-netwerk. Het is van belang om maatregelen te nemen, zodat wachtwoorden niet bekend wordt bij onbevoegden. Daarnaast is het verstandig om gevoelige informatie binnen een eigen netwerk aanvullend te beschermen en te versleutelen.

Het inrichten van een draadloos netwerk is een complexe aangelegenheid. De noodzakelijke inrichting is afhankelijk van allerlei omgevingsfactoren en het gebruik zelf. Voor SD-WLAN hebben we daarom 2 standaardprofielen gedefinieerd voor draadloze toepassingen:

- Klein (tot ongeveer 1.500 m² en tot en met 6 AP's)
- Groot (meer dan 1.500 m², en meer dan 6 AP's, dekking voor buiten of speciale omgevingen)

Bij draadloos profiel "Klein" is er veelal geen vooropname nodig en zullen de beste passende elementen en de benodigde aantallen door DELTA Zakelijk bepaald worden. Hierdoor zijn de implementatiekosten lager. U kunt deze dan zelf eenvoudig (laten) installeren.

Voor draadloos profiel "Groot" zal vooraf een ontwerp gemaakt worden, inclusief site survey en eventueel radioplan. De benodigde poorten, typen netwerkbouwblokken, opties en bijbehorende kosten zullen vastgesteld worden na deze vooropname.

Er is altijd een DELTA Zakelijk SD-WAN gateway op de locatie nodig om SD-WLAN te kunnen inrichten. Bij meer dan 1 Accesspoint is zijn ook 1 of meerdere Power over Ethernet switches van de SDN-familie nodig.

3.9.4 Optionele Verbindingsmodules

Om SD-LAN Switches op hoge snelheid met elkaar te kunnen verbinden, kunt u de SD-LAN Switches uitbreiden met een SFP-module. SFP staat voor Small Form-factor Pluggable. De SFP is een kleine zender/ontvanger die past in een standaard insteekslot van de SD-LAN Switch.

Er zijn veel verschillende SFP-modules mogelijk. Dit komt doordat er verschillende koppelvlakken (zoals koper en glas) bestaan en er verschillende afstanden overbrugd kunnen worden.

De maximale transportsnelheid per module:

- SFP maximaal 1 Gbit/s
- SFP+ maximaal 10 Gbit/s
- QSFP maximaal 40 Gbit/s

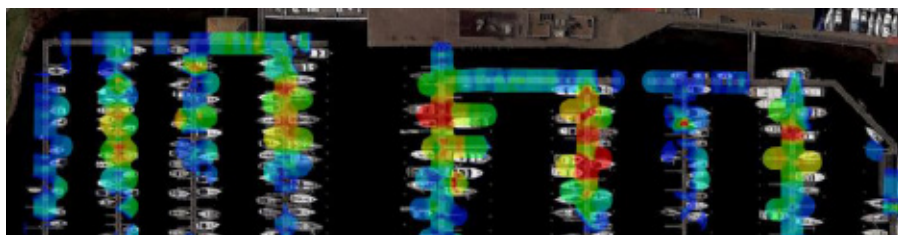
Voor deze opties kunnen aditionele kosten gelden.

3.9.5 Radioplan

Een draadloos netwerk is voor een gebruiker een beleving. Om aan het verwachtingspatroon te voldoen is een radioplan een middel om vooraf te onderzoeken hoe een optimale dekking/ performance tot stand moet komen. Optioneel biedt DELTA Zakelijk aan om tegen meerprijs een radioplan op te stellen.

De plaats van de Wireless Access Points (AP) en het aantal hiervan wordt zodanig gekozen dat de signalen van de verschillende AP's elkaar deels overlappen en zodoende zorgen voor een goede dekking. Het resultaat is een plattegrond waarin het bereik van de diverse Wireless Access Points is getekend. Dit radioplan kan voor 2.4 GHz en 5 GHz geoptimaliseerd worden.

Voor een gedegen radioplan zal de scope helder moeten zijn. Hierop wordt besloten of een heatmap noodzakelijk is. Een heatmap kan door simulatie tot stand komen (softwareprogramma) of worden ingemeten op locatie. Echter een heatmap is een momentopname en beïnvloedbaar door bebouwing, bezetting, elektrische apparatuur en overige radiosignalen (ruis). Bij omvangrijke trajecten kan ook een nameting worden gedaan ter controle op het originele plan. Een heatmap kan aditionele kosten met zich meebrengen. Hieronder een voorbeeld van een heatmap.



Een radioplan behelst de volgende onderdelen of een deel van de volgende onderdelen:

- Scope bepaling
- Aantal en type apparaten en de netwerksegmenten (SSID's)
- Type data stromen en informatie over gebruik van spraak en/of video over Wi-Fi
- Informatie over het gebouw: af te dekken ruimtes/ gebieden en eventuele geplande verbouwingen
- Gegevens over Internettoegang en capaciteit, LAN, toegang, IP Plan, VLANS en capaciteit. Kortom de eigenschappen van het vaste netwerk inclusief patchkasten, switches, gateway
- Plattegronden (bouwkundige en/of netwerktekeningen met maatvoering)
- Heatmap
- Voormeting en Nameting

3.9.6 Captive portal

DELTA Zakelijk biedt optioneel de mogelijkheid tot het activeren van een captive portal op het draadloze gastnetwerk. Captive portals kunnen worden gebruikt in openbare Wi-Fi-gastnetwerken, zoals die in hotels, luchthavens, cafés, scholen en bedrijven.

De captive portal voor SD-WLAN is een webpagina die gastgebruikers van het Wi-Fi-netwerk kan dwingen om bepaalde informatie in te vullen, akkoord te gaan met gebruiksvoorwaarden, of bepaalde verificatieprocessen te doorlopen voordat ze volledige toegang krijgen.

Kenmerken van het captive portal:

- Authenticatie en verificatie: Gebruikers moeten zich registreren of inloggen via de captive portal voordat ze toegang krijgen tot het netwerk.
- Gebruiksvoorwaarden: Gebruikers worden gevraagd om akkoord te gaan met de gebruiksvoorwaarden en het privacy beleid van het netwerk.
- Gebruikersbeheer: U kunt de netwerktoegang beperken op basis van tijd (bijv. sessies van een uur) of hoeveelheid data (bijv. 1 GB per sessie).
- Wettelijke naleving: In sommige gevallen bent u wettelijk verplicht om gebruikers te laten instemmen met gebruiksvoorwaarden of privacy verklaringen voordat ze toegang krijgen tot uw netwerk.
- Toegang voor geregistreerde gebruikers: In omgevingen zoals bedrijven of onderwijsinstellingen kan het captive portal worden gebruikt om alleen geregistreerde of geautoriseerde gebruikers toegang te geven tot het netwerk.

Samengevat biedt een captive portal een gecontroleerde en gestructureerde manier om toegang tot een Wi-Fi-gastnetwerk te beheren.

3.10 SD-Cloud

SD-Cloud van DELTA Zakelijk geeft u een veiligere centrale verbinding tussen uw bedrijfsnetwerk en het internet voor zowel inkomend als uitgaand netwerkverkeer door middel van de inzet van een redundante Cloud Gateway. Een Cloud Gateway geeft u de mogelijkheid om uw VPN-verbindingen in te richten via het hub-and-spoke model. Dit stelt u in staat het onderhoud van uw VPN's en beveiligingsinfrastructuur te ontlasten, diepgaand inzicht te krijgen, robuuste controles toe te passen en de uitgaven voor VPN en beveiliging te optimaliseren.

Een Cloud gateway biedt flexibiliteit doordat het kan worden geïmplementeerd, geconfigureerd en geschaald op basis

van de behoeften van uw organisatie. De hub elimineert soms de noodzaak om te investeren in dure hardware en licenties op elke locatie.

De hub kan fungeren als een centraal punt voor het implementeren van beveiligingsmaatregelen zoals firewalls, intrusion detection/prevention systemen (IDS/IPS), en andere beveiligingspolitiecs. Beheer en monitoring van het netwerk kunnen vanuit een centrale hub gebeuren, wat het beheer vereenvoudigt en de operationele kosten verlaagt. Problemen kunnen sneller worden geïdentificeerd en opgelost vanuit de centrale hub, wat de tijd die nodig is voor troubleshooting vermindert.

Bestaande verbindingen op basis van Ethernet of IP-VPN kunnen worden ingekoppeld op de Cloud gateway en indien gewenst daarna stap-voor-stap worden gemigreerd naar een SD-WAN VPN.

De SD-Cloud dienst is een managed service die volledig ingericht en beheerd wordt door DELTA Zakelijk. U krijgt een maandelijkse rapportage over de performance van uw SD-Cloud dienst.

3.10.1 Aanvullende Diensten SD-Cloud

De SD-Cloud dienst bestaat uit verschillende onderdelen waarmee alle oplossingen gebouwd kunnen worden. Sommige van deze onderdelen zijn standaard. Dat wil zeggen dat het vaste onderdelen van de dienst zijn, die u altijd afneemt, of u deze nu gebruikt of niet. Andere onderdelen kunt u optioneel afnemen.

De verschillende onderdelen en opties en hun afhankelijkheid (standaard of niet) vindt u terug in de onderstaande tabel. Sommige van deze hebben zijn al eerder in het document benoemd

3.10.2 Hub-and-Spoke VPN

Hub-and-Spoke VPN	Standaard
High availability apparatuur	Standaard ⁽¹⁾
Internet toegang	Standaard
Advanced Firewall	Standaard ⁽¹⁾
Rapportage	Standaard ⁽¹⁾
SDN Cloud Connect	Optioneel ⁽¹⁾
Remote Access	Optioneel ⁽¹⁾
MPLS-migratie	Optioneel

¹Reeds eerder beschreven.

Het hub-and-spoke model is een netwerkarchitectuur waarbij alle spoke locaties (filialen, kantoren, of externe locaties) verbonden zijn met een centrale hub locatie (in het datacenter van DELTA Zakelijk). Dit model wordt gebruikt om netwerkverkeer efficiënt te beheren en te centraliseren.

De belangrijkste eigenschappen van het hub-and-spoke model zijn:

- De centrale hub fungeert als een knooppunt waar alle spoke locaties mee verbonden zijn.
- De hub beheert en controleert het netwerkverkeer tussen de spoke locaties en naar externe bronnen zoals de Cloud, het internet of andere datacenters.
- Spoke-locaties zijn de uiteinden van het netwerk die verbonden zijn met de centrale hub.
- Deze locaties kunnen kantoren, filialen of andere remote sites zijn.

Het hub-and-spoke model is een veelgebruikte en effectieve architectuur voor SD-WAN-implementaties, vooral voor organisaties die centrale controle en eenvoudig beheer van hun netwerk willen.

3.10.3 Internet Toegang Cloud Gateway

De Cloud Gateway wordt geleverd in verschillende schaalbare verwerkingscapaciteiten, waarbij het internetverkeer en de verbindingen naar uw DELTA Zakelijk VPN-omgeving al in de dienst zijn opgenomen. U hoeft dus geen aparte, centrale internet- of extra DELTA Zakelijk VPN-verbinding meer aan te schaffen.

Het verwachte verkeer dat door de Cloud Gateway zal lopen, bepaalt de benodigde verwerkingscapaciteit.

Over het algemeen is dit de optelsom van de snelheden van de verbindingen op uw locaties. De af te nemen verwerkingscapaciteit die u nodig hebt, kiest u op basis van de benodigde verwerkingsnelheid.

U kunt kiezen uit de volgende varianten:

- Cloud Gateway 500 Mbit/s internet access
- Cloud Gateway 1 Gbit/s internet access
- Cloud Gateway 2 Gbit/s internet access
- Hogere snelheden op aanvraag.

3.10.4 MPLS-migratie

Het integreren van MPLS met een Cloud gateway kan helpen bij de migratie van MPLS. Uw verbindingen op basis van Ethernet of IP-VPN kunnen worden ingekoppeld op de Cloud gateway en indien gewenst daarna stap-voor-stap worden gemigreerd naar een SD-WAN VPN.

Door SD-WAN te implementeren naast bestaande MPLS- netwerken, kunnen bedrijven geleidelijk verkeer migreren zonder grote verstoringen. Dit maakt een geleidelijke overgang mogelijk waarbij MPLS en SD-WAN parallel kunnen werken. U kunt beginnen met het migreren van niet-kritieke applicaties naar SD-WAN, terwijl kritieke applicaties voorlopig op MPLS blijven. Hierdoor wordt het risico van migratie verminderd.

Naarmate het gebruik van MPLS afneemt, kunt u afzien van dure MPLS-circuits, wat aanzienlijke kostenbesparingen oplevert. U kunt eenvoudig nieuwe locaties toevoegen aan hun netwerk met SD-WAN zonder de complexiteit en beheerskosten van het uitbreiden van MPLS-infrastructuur.

Praktische migratiestappen:

- a. Planning: DELTA Zakelijk beoordeelt de huidige MPLS-omgeving en plant de migratie.
- b. Pilot: We voeren een pilot implementatie uit op een paar locaties om de SD-WAN te testen en eventuele problemen vroegtijdig te identificeren.
- c. Uitrol: We rollen SD-WAN geleidelijk uit naar meer locaties en migreren stap voor stap MPLS-verkeer naar SD-WAN.
- d. Afsluiten van MPLS: Zodra het verkeer met succes is gemigreerd en de SD-WAN prestaties voldoen aan de verwachtingen, kunnen MPLS-circuits worden afgesloten.

Aanvullende diensten

Aanvullende diensten zijn diensten welke op zichzelf staan, hebben een eigen dienstbeschrijving, maar werken optimaal samen met SDN.

4.1 Internet

DELTA Zakelijk levert een tal van Internetverbindingen met elk haar eigen specificaties. Voor het juiste advies kunt u rekenen op de deskundigheid van onze accountmanager.

4.2 Managed Voice

Managed Voice kent een zeer rijke feature set, draagt bij aan effectieve communicatie en is zeer eenvoudig te bedienen. Gespreksoptname, uitgebreide rapportage en Callcenter faciliteiten zijn allemaal ondervangen in één voordelige licentie per gebruiker.

4.3 TV

Voor B&B's, Hotels, Bungalowparken maar ook voor televisie kijken op kantoor of in sportkantines heeft DELTA Zakelijk diverse Zakelijke oplossingen voor optimaal kijkplezier.

Installatie

5.1 Implementatie

De implementatie van SDN wordt volledig door DELTA Zakelijk uitgevoerd. Om een tot een juiste implementatie te kunnen komen, maken we gebruik van een gestandaardiseerde aanpak. Hiermee zorgen we ervoor dat de SDN-oplossing goed aansluit bij het beoogde gebruik. Onze aanpak bestaat uit een aantal stappen, hieronder beschreven in het stappenplan.

5.1.1 Stappenplan

Voorstel: Onze verkoopmedewerkers brengen een voorstel uit op basis van met u besproken aannames. U hebt daarmee een indicatie van de maandelijkse exploitatiekosten voor de SDN-oplossing. Bent u akkoord dan gaan we door naar de ontwerpfase.

Ontwerp: Samen met u bespreken we de functionele eisen en wensen en de situationele omstandigheden van uw bedrijfslocaties. Op basis daarvan maken we een SDN-ontwerp. DELTA Zakelijk controleert de externe lijnverbindingen op geschiktheid of adviseert over nieuwe verbindingen.

Offerte: Op basis van alle verkregen informatie brengt DELTA Zakelijk een offerte uit waarin indicatieve aantallen zijn opgenomen en een inschatting is gemaakt van de overgangseisen en -kosten. Deze offerte tekent u indien akkoord. Site survey (optie): na ondertekening gaan wij indien nodig (of gewenst) de locaties af om de lokale omstandigheden vast te stellen. Hierbij kijken we naar randvoorwaarden voor de installatie, werkelijke benodigde aantallen en eventuele belemmerende (bouw)omstandigheden. Hierbij kan ook het maken van een radioplan en een heatmap nodig zijn.

Offerte Aanpassing: Op basis van de verkregen informatie, wordt een locatieontwerp gemaakt waar de werkelijke aantallen bepaald worden. Deze aantallen kunnen leiden tot het aanpassen van de offerte. Indien blijkt dat randvoorwaarden nog niet (voldoende) zijn ingevuld, kunnen die worden vormgegeven op basis van meerwerk. Deze offerte tekent u indien akkoord.

Locatievoorbereiding (optie): Het draaiboek voor de implementatie wordt opgesteld. Hierin vindt u ook het (technisch) ontwerp, een stappenplan van elke locatie en, indien van toepassing, overgangs- en terugvalscenario.

Installatie: Op een overeengekomen moment wordt de SDN-apparatuur geplaatst en ingeregeld. Deze werkzaamheden voeren we per locatie uit. Bij eenvoudige installaties kunt u deze werkzaamheden ook zelf uitvoeren.

Oplevering: Na de opstelling te hebben getest, wordt het SDN per locatie vrijgegeven door DELTA Zakelijk. U krijgt instructies voor het gebruik. De oplevering wordt vastgelegd in een opleveringsdocument, wat door beide partijen ondertekend dient te worden. Na de vrijgave door DELTA Zakelijk starten we met de facturatie en serviceverlening voor de bewuste locatie.

Training: Indien overeengekomen zullen we een training verzorgen voor uw medewerkers.

5.2 Levering

De levertijd van de Managed SDN dienst bedraagt tien (10) tot twaalf (12) weken na opdracht, of zoveel eerder als mogelijk is, vanaf het moment dat de Contractant de opdracht verstrekt. Een exacte datum van oplevering wordt in onderling overleg met de Contractant bepaald. De levering vindt over het algemeen plaats onder verantwoordelijkheid van een projectcoördinator van DELTA Zakelijk.

De levertijd start nadat DELTA Zakelijk de ondertekende overeenkomst van de Contractant heeft ontvangen. Voor het plannen van de werkzaamheden wordt er eventueel een locatiecontrole uitgevoerd. In overleg met de Contractant worden de werkzaamheden ingepland.

De levering van de dienst start op de dag dat de dienst is opgeleverd aan de Contractant. Vanaf dat moment wordt de dienst volgens de serviceafspraken gemonitord en kan de Contractant, indien van toepassing, storingen voor de dienst melden.

Wanneer de geplande opleverdatum niet gehaald wordt, zal dit tijdig aan de Contractant gemeld worden. In 95% van de gevallen wordt de opgegeven levertijd gehaald, maar dit kan door DELTA Zakelijk niet gegarandeerd worden. Specifiek voor outdoor werkzaamheden is de oplevertijd onder voorbehoud van vergunningverlening, graafwerkzaamheden, vorst en andere beperkingen van het stormseizoen.

5.3 Beheer

De SDN-dienst wordt geleverd als “managed service”. Hierbij inbegrepen zijn aanschaf, onderhoud, configuratie, beheer en vervanging (in geval van defect zonder opzet) van de voor deze dienst geïnstalleerde apparatuur op de klantlocatie. Het beheer van de klantapparatuur, de internetverbinding en/of netwerkbekabelingsaspecten vallen niet onder de dienst SDN.

5.4 Wijzigingen

Het is mogelijk om wijzigingen op de SDN-dienst aan te vragen. In overleg met de Contractant worden de werkzaamheden naar aanleiding van een wijziging bepaald, zodat DELTA Zakelijk tijdsbesteding en de kosten kan inschatten. Per locatie is door DELTA Zakelijk 15 minuten per maand gereserveerd voor het doen van kosteloze wijzigingen. Daarboven is DELTA Zakelijk gerechtigd om de tijd in rekening te brengen aan de Contractant. Het moment waarop de wijziging kan worden uitgevoerd, wordt in overleg met de Contractant bepaald en de doorlooptijd wordt gerekend vanaf het moment dat de opdracht in behandeling wordt genomen.

Aan wijzigingen buiten kantooruren kunnen extra kosten verbonden zijn.

Voor werkzaamheden zijn indicatieve prijzen en doorlooptijden opvraagbaar via uw Accountmanager.

Service

6.1 Algemeen

Op iedere dienst van DELTA Zakelijk is een Service Level Agreement, hierna SLA genoemd van toepassing. Bij DELTA Zakelijk Managed SDN Internet is Prioriteit inbegrepen. Raadpleeg de Dienstbeschrijving Service DELTA Zakelijk voor de details van het geboden Service Level.

Wijziging	Module/ Voorwaarde	(Mogelijk) invloed op
Gateway:		
Upgrade naar hoger model Gateway	Per locatie, t/m type 3	Hoger model dan type 3 kan maatwerk meebrengen
Portforwarding toevoegen/ verwijderen	5 stuks per Gateway	Subnetten, Firewall rules en/of routeringen
Extra VLAN toevoegen/ verwijderen	3 stuks per Gateway	Firewall rules
Locatie in-/ uitkoppelen via virtuele tunnel	Per tunnel	Firewall rules
Toevoegen van een mobiele ontsluiting t.b.v. 4G Back-up (secundair)	Per 4G Extender (1 per Gateway, aangesloten op de 2de WAN poort)	Firewall rules
Toevoegen van een extra Underlay ontsluiting (secundair)	Per Underlay (1 per Gateway, aangesloten op de 2de WAN poort)	Firewall rules
Verhuizen Hoofdlocatie/ Main HUB	Per Gateway van locatie A naar locatie B	Alle nevenlocaties
Wijzigen omschakelregels naar secundaire verbinding	Per gateway	
Routerfuncties		
Aanpassen DHCP en of NAT instellingen (Subnet, Fixed IP etc.)	Per VLAN	Firewall rules en/of Port Forwarding
Toevoegen/ wijzigen Fixed Public IP Subnet routeringen naar LAN-apparatuur	Per Fixed Public IP address	Firewall rules en/of Port Forwarding
Firewall		
Upgrade Basis Firewall naar Advanced	Per Gateway	
Whitelisten- of Blacklisten IP Adressen en/ of Domeinnamen	Per Item	
Whitelisten of Blacklisten IP Applicaties	Per Applicatie	
Toevoegen/ Wijzigen Firewall Rules	Per Regel	Gateways
Remote Access		
Gebruiker toevoegen/ verwijderen	Per 5 gebruikers	
Cloud		
Extra SDN Cloud Connect dienst toevoegen/ verwijderen	Per connectie	Firewall rules, Port Forwarding en/of routeringen
SD LAN		
Upgrade Switch model i.v.m. port te kort	Per switch	
Extra Switch	Per switch	
SD WAN		
Extra Wi-Fi Accesspoint (zelf installatie)	Per Accesspoint	
SSID Toevoegen/ verwijderen	Per SSID	VLAN, DHCP, NAT, Subnet
SSID naam wijzigen	Per SSID	
Wi-Fi wachtwoord wijzigen	Per SSID	
Wi-Fi authenticatie methode wijzigen	Per SSID	

Reports		
Wijziging in Monthly Report	Per report	
Advanced Analytics	Per klantomgeving	
Specials		
Extra locatie		Maatwerk
Spare Gateway (Cold Stand-by)	Per locatie	Maatwerk
Spare Gateway (Hot Stand-by)	Per locatie	Maatwerk

In het geval van inhuur van een verbinding van derden, kan een afwijkende SLA van toepassing zijn.

6.2 Zakelijke Helpdesk

DELTA Zakelijk Managed SDN Internet geeft 24/7 toegang tot de Zakelijke Klantenservice van DELTA Zakelijk voor het melden van eventuele storingen, raadpleeg de Dienstbeschrijving Service DELTA Zakelijk voor de contractmatrix.

Product voorwaardelijk

DELTA Zakelijk wil graag dat uw implementatie van SDN makkelijk verloopt. Het is goed om op voorhand naar alle omgevingscondities te kijken en te inventariseren of de omgeving klaar is voor de implementatie.

DELTA Zakelijk neemt hoogwaardige apparatuur van leveranciers af die op uw locatie(s) wordt geplaatst door professionals of u zelf. Deze apparatuur moet in de juiste omgeving worden geïnstalleerd en moet, gedurende de afgesproken contracttermijn, bereikbaar, storingsvrij en veilig staan.

Deze voorwaarden geven u een overzicht van de verantwoordelijkheden die u hebt en die DELTA Zakelijk heeft op de aan te sluiten locaties. Deze verantwoordelijkheden laten (ook) de voorwaarden zien voor een juiste en adequate implementatie en hoe u een veilige en storingsvrije omgeving kunt creëren voor het gebruiken van onze diensten. De vermelde verantwoordelijkheden zijn verplicht en dienen strikt opgevolgd te worden. Wij verwachten van u dat u bij de start van de implementatie aan deze verantwoordelijkheden voldoet.

7.1 SDN

Op SDN zijn onderstaande dienst specifieke afspraken en kaders van toepassing:

- a. Uw primaire netwerk (Access) moet grotendeels uit zakelijke DELTA Zakelijk-verbindingen bestaan.
- b. Deze Access wordt door DELTA Zakelijk verzorgd.
- c. Voor een locatie zonder Access/Internet van DELTA is een internetverbinding voor managementinformatie naar de DELTA Cloud is verplicht.
- d. De interne bekabeling is beschikbaar en functioneert (UTP min Cat6, 220/240V met 16 A).
- e. Energiekosten aangaande de Klantapparatuur en de Eindapparatuur van DELTA zijn voor rekening van de Contractant.
- f. De apparatuur staat in een afgesloten ruimte, alleen toegankelijk is voor geautoriseerde personen.
- g. Bij voorkeur wordt gebruik gemaakt van beschikbare ruimte in een 19" netwerkkast van de Contractant.
- h. Voor het vervangen van apparatuur op locatie zal u, de Contractant, zorg moeten dragen voor onbelemmerde en directe toegang tot de apparatuur. Dit is inclusief begeleiding en invulling van de randvoorwaarden naar de ruimte waar de apparatuur is geplaatst.
- i. Voor niet-standaard installaties van SD-WAN-apparatuur zal DELTA Zakelijk meerkosten op basis van tijd en materiaal in rekening brengen.
- j. Niet binnen de dienst vallende oorzaken van incidenten, liggen buiten verantwoording van DELTA Zakelijk. Voor het

- oplossen van deze incidenten, zullen kosten in rekening gebracht worden.
- k. Voor situaties waarbij volgens de wetgeving aanvullende maatregelen nodig zijn, zal u, de Contractant, hieraan invulling geven. Bijvoorbeeld: bij plaatsing hoger dan 3 meter, zal de Contractant zorgdragen voor een hoogwerker inclusief bediening en eventuele andere veiligheidsmaatregelen. DELTA Zakelijk draagt zorg voor een VCA-gecertificeerde medewerker die binnen deze omgeving mag werken.
 - l. Als door u, de Contractant, een specifieke certificering of instructie vereist wordt, kunnen de kosten daarvoor in rekening gebracht worden. Eventuele extra benodigde tijd zal volgens de overeengekomen SLA-tijden worden opgeschort.
 - m. Geschikte gebouwbekebeling is aanwezig en beschikbaar voor het aansluiten van benodigde dienstelementen.
 - n. Aansluiten van (rand)apparatuur verzorgt u zelf, hieronder valt bijvoorbeeld ook het patchen en configureren.

7.2 SD-WAN

Op SD-WAN zijn onderstaande aanvullende dienst specifieke afspraken en kaders van toepassing:

- a. **High availability active/passive cluster:** Op extra te plaatsen apparatuur zijn dezelfde voorwaarden van toepassing als op regulier te leveren apparatuur ongeacht de functionele werking.
- b. **Mobile WAN Redundancy:** De levering en installatie van de mobiele voorziening wordt gerealiseerd met additionele SD-WAN-apparatuur. Deze is gekoppeld aan de SD-WAN gateway en plaatsing is mogelijk in een andere ruimte. Als op locatie waar de SD-WAN gateway staat onvoldoende dekking is, kan worden gekozen voor een installatiepunt met betere dekking. Dit is altijd een in pandige locatie.

7.3 SD-(W)LAN

Op SD-LAN zijn onderstaande dienst specifieke afspraken en kaders van toepassing:

- a. Voor een SD-LAN-netwerk is een DHCP-service noodzakelijk om het netwerk te kunnen configureren en in dienst te zetten. Dit is de DHCP-service in de SD- WAN Gateways op uw locatie (klantlocatie).
- b. De SD-LAN-dienstverlening biedt geen functionaliteiten voor bouwkundige zaken.
- c. DELTA Zakelijk is niet aansprakelijk voor onvoldoende voeding (stroom) voor apparatuur die via power-over-ethernet (PoE) worden gevoed, als er apparaten worden aangesloten die niet zijn meegenomen in het LAN- ontwerp.

Op SD-WLAN zijn onderstaande dienst specifieke afspraken en kaders van toepassing:

- d. SD-WLAN wordt op alle locaties geleverd in combinatie met SD-LAN switches, met uitzondering van één Accesspoint.
- e. DELTA Zakelijk kan geen garantie geven op de beschikbare bandbreedte en/of dekking van het draadloze netwerk, omdat het radiodomein buiten invloedsfeer van de dienst valt.
- f. DELTA Zakelijk voorziet niet in speciale voorzieningen voor de montage van apparatuur, bijvoorbeeld als u, de Contractant, een design-plafond hebt, of Wireless Access Points op buitenmasten wilt (laten) plaatsen.
- g. Bekabeling naar de Access points dient door de Contractant zelf verzorgd te worden.
- h. De Contractant dient zorg te dragen voor de juiste conditionering van ruimte waar de apparatuur geplaatst wordt:
Indoor: temperatuur: min. 10°C, max. 30°C/ Vochtigheid: min. 15% max. 90% (niet condenserend).
Outdoor: Temperatuur: outdoor min. -20°C, max 65°C.

7.4 SD-Cloud

De Cloud Gateway dienstverlening levert verbindingen naar het internet, waarop onderstaande aanvullende voorwaarden van toepassing zijn:

- a. Als (het) internet of het verkeer over internet hinder ondervindt van uw internetgebruik via de internetaansluiting, bent u verplicht om aan de, in dit verband door DELTA Zakelijk gegeven, voorschriften en aanwijzingen (voor eigen rekening) gehoor te geven. Indien dit naar het oordeel van DELTA Zakelijk noodzakelijk is, kan DELTA Zakelijk de internetaansluiting, zo nodig onverwijld, tijdelijk buiten gebruik stellen.
- b. Het is niet toegestaan via uw internetaansluiting informatie of diensten aan te bieden of te gebruiken, indien dit

strafbaar of jegens derden onrechtmatig is. Instructies voor het opvolgen van de operationele procedures zoals aangegeven door DELTA Zakelijk zullen worden opgevolgd. DELTA Zakelijk heeft het recht de toegang tot informatie of diensten te blokkeren of maatregelen te treffen ter voorkoming van (verdere) verspreiding van informatie of ter voorkoming van toegankelijkheid of het gebruik van diensten via internet, als DELTA Zakelijk een ernstig vermoeden heeft dat de inhoud, openbaarmaking en/ of verspreiding van de desbetreffende informatie of het aanbod of het gebruik van de desbetreffende dienst strafbaar dan wel jegens derden onrechtmatig kan zijn.

- c. Voor de levering is een formele autorisatie door u noodzakelijk voor de verantwoording voor het gebruik van de IP-adressen die door DELTA Zakelijk aan u in bruikleen worden gegeven. Hiervoor krijgt u het verzoek van DELTA Zakelijk om een verantwoording te geven. Daarnaast ontvangt u formulieren voor de registratie of verhuizing van domeinnamen. Als er gebruik wordt gemaakt van diensten van derden voor DNS/IP-registraties, dan zal de Contractant zorgdragen voor verantwoording en waar nodig ondersteuning naar DELTA Zakelijk.