SIVON

Samen
Inkopen
Voor
Onderwijs
Nederland

DIENSTBESCHRIJVING

VEILIG INTERNET

Maart 2022

Inhoud

Inleiding

Dit is de dienstbeschrijving van de dienst Veilig Internet. Veilig Internet maakt een snelle, veilige en betrouwbare internetverbinding beschikbaar voor scholen in het primair en voortgezet onderwijs (po en vo). Veilig Internet komt voort uit de samenwerking tussen SIVON en Kennisnet.

De coöperatie SIVON is een samenstelling van de leden van SIVON en de SIVON-organisatie. Door samen te werken binnen SIVON versterken de leden de slagvaardigheid en invloed in de ict- en leermiddelenmarkt, mét behoud van eigen regie. Met krachtenbundeling en een gezamenlijke aanpak worden grote stappen gemaakt. Het SIVON-aanbod van gebruiksvriendelijke, geavanceerde en geïntegreerde ict-voorzieningen stelt leraren en medewerkers in staat te werken aan toekomstgericht, persoonlijk en veilig onderwijs.

Kennisnet ondersteunt scholen bij een professionele inzet van ict. Kennisnet is voor scholen en instellingen in het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo) de gids en bouwer van het ict-fundament.

Deze dienstbeschrijving is bedoeld voor bestuurders, inkopers en ict-coördinatoren. Er wordt op hoofdlijnen beschreven wat de dienst Veilig Internet inhoudt, in welke varianten de dienst beschikbaar is en hoe op de dienst kan worden aangesloten.

Deze dienstbeschrijving kan te allen tijde eenzijdig door SIVON of Kennisnet worden aangepast. Bij wijzigingen zal SIVON zo mogelijk rekening houden met de (zakelijke) belangen van de afnemers van de dienst. Eventuele wijzigingen zullen tijdig worden gecommuniceerd.

1. Wat is Veilig Internet

Waarom Veilig Internet?

Het onderwijs is in toenemende mate afhankelijk van de aansluiting op het internet. Steeds meer scholen werken met digitale leermiddelen en leraren gebruiken digitale toepassingen ter ondersteuning van hun lessen. Een kwalitatief hoogwaardige ict-infrastructuur is daarom essentieel voor

een veilige en betrouwbare onderwijsomgeving. Preventieve beveiligings-maatregelen zijn in deze tijd onmisbaar om schadelijke bedreigingen te voorkomen. Hiermee voorkomen we de uitval van de ict-infrastructuur en waarborgen we de continuïteit van het onderwijs. Veilig Internet biedt een centraal ingerichte, beveiligde en betrouwbare internettoegang voor alle schoollocaties, bestuursgebouwen en datacenters die onder een school- bestuur vallen.

Wat biedt Veilig Internet?

De dienst Veilig Internet biedt twee belangrijke functionaliteiten in één dienst:

1. **Connectiviteit**

   Veilig Internet zorgt voor een aansluiting van alle locaties op het centrale datacenter: het Nationaal Dienstencentrum (NDC) van Veilig Internet. Via het NDC worden schoollocaties, het bestuursgebouw en datacenter van het schoolbestuur met elkaar en met het internet verbonden. Het schoolbestuur bepaalt per schoollocatie de gewenste bandbreedte en kwaliteit. SIVON ontzorgt het schoolbestuur met het aanbestedingstraject voor deze connectiviteit.

2. **Veiligheid**

   Veilig Internet zorgt ervoor dat schoollocaties en datacenters van het schoolbestuur op een veilige manier met elkaar en met het internet verbonden zijn. Via een *state of the art* firewall op het NDC worden passende beveiligingsmaatregelen toegepast op al het verkeer, zodat indringers en bedreigingen zoals DDoS-aanvallen worden tegengehouden. Zonder dat scholen daar iets van merken. Elk schoolbestuur krijgt zijn eigen (virtuele) firewall met een generieke set beveiligingsmaatregelen. Een schoolbestuur kan extra beveiligings- maatregelen toe laten voegen afhankelijk van de specifieke wensen binnen het bestuur.

De voordelen op een rij

Veilig dankzij de adequate preventieve maatregelen in het NDC om een veilige toegang tot het internet te garanderen en onder meer DDoS-aanvallen tegen te gaan.

Betrouwbaar omdat we op voorhand zorgvuldig geselecteerd hebben op de kwaliteit en betrouwbaarheid van de leveranciers van de firewall en de verbindingen.

Eenvoudig omdat SIVON de dienst op voorhand al Europees heeft aanbesteed. Schoolbesturen hoeven zelf geen aanbesteding meer te doen. SIVON onderhoudt alle contacten en contracten met de marktpartijen.

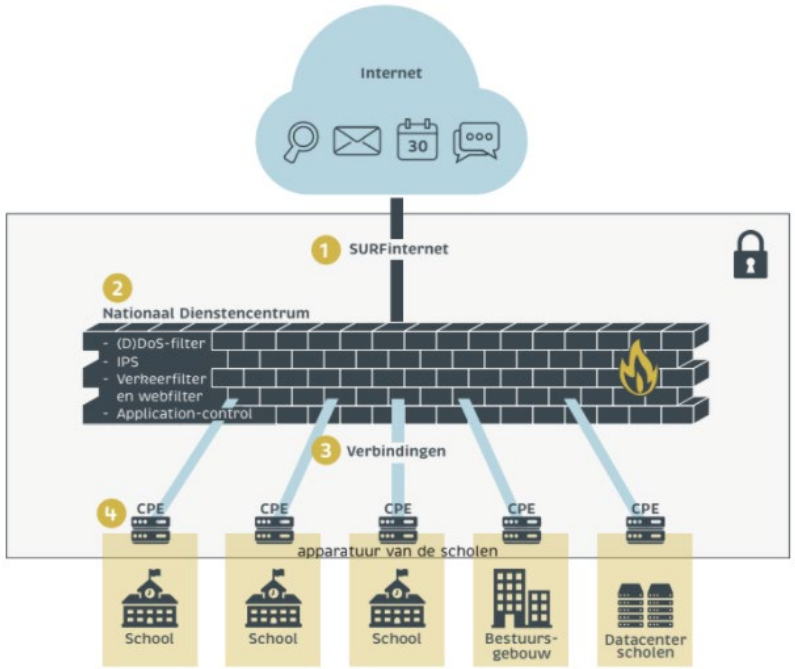
Voordelig dankzij de gezamenlijke inkoop vanuit de coöperatie en de subsidie voor de opstart. SIVON kan bij meerdere partijen inkopen en per locatie de beste aanbieder vinden.

Passend doordat de dienst voor en door het po en vo tot stand is gekomen en aansluit bij de specifieke behoeften van het onderwijs. Veilig Internet kent vier categorieën voor de fysieke verbindingen van en naar locaties, die verschillen in beschikbaarheid en kwaliteit. De gewenste categorie kan door het schoolbestuur per locatie gekozen worden. Per categorie kan het schoolbestuur ook nog kiezen tussen verschillende bandbreedtes.

2. Hoe werkt Veilig Internet

2.1. Overzicht van de dienst

Voor het bieden van **connectiviteit** en **veiligheid** is Veilig Internet opgebouwd uit verschillende onderdelen om alle schoollocaties onder één schoolbestuur uniform aan te sluiten. Deze onderdelen zijn vereenvoudigd weergegeven in onderstaande figuur.



De onderdelen in het kader maken deel uit van de dienst Veilig Internet. In het kort betekent dat het volgende:

1. De toegang tot het internet wordt gefaciliteerd via SURFinternet.
2. In het Nationaal Dienstencentrum (NDC) van Kennisnet zijn de beveiligingsmaatregelen ingericht op de centrale firewall.
3. De access provider zorgt op basis van de gewenste kwaliteit en bandbreedte voor de verbindingen tussen de schoollocaties en het NDC.
4. Op de schoollocatie wordt naast de apparatuur van de access provider, hardware van SIVON geplaatst, zodat het Local Area Network (LAN) kan worden aangesloten op Veilig Internet. De apparatuur op de schoollocatie (de Customer Premises Equipment, CPE's) is het aan- sluitpunt op de dienst Veilig internet en vormt het demarcatiepunt.

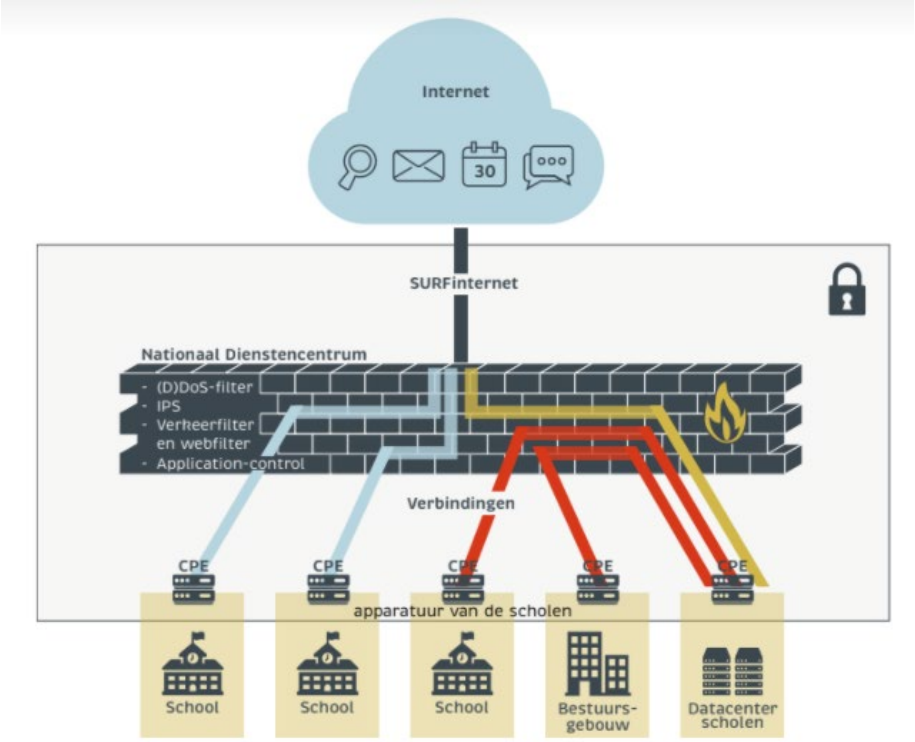
2.1.1. SURFinternet

De verbinding van en naar het internet van het NDC wordt verzorgd door SURF. SURFinternet zorgt voor een hoogwaardige en stabiele op het onderwijs gerichte internettoegang.

2.1.2. Nationaal Dienstencentrum

De (virtuele) firewalls van het NDC bewaken het verkeer van en naar internet en andere schoollocaties. Onderling verkeer tussen schoollocaties, indien door u gewenst, verloopt via de beveiligingsmaatregelen die zijn ingericht op de virtuele firewall van het schoolbestuur. Dit geldt eveneens voor het verkeer van een intern datacenter binnen het schoolbestuur.

De volgende afbeelding is een weergave van de mogelijke datastromen.



In het NDC bevinden zich de firewalls en de DNS-server. De beveiligingsmaatregelen, die onderdeel zijn van de dienst, zorgen voor een veilige toegang tot het internet en beschermen het dataverkeer tussen schoollocaties onderling en een eventueel datacenter. Het NDC is redundant uitgevoerd, waardoor een optimale beschikbaarheid gegarandeerd is.

In het NDC krijgt elk schoolbestuur een eigen virtuele firewall: de schoolbestuur-firewall. De firewalls van het NDC zijn *state of the art* en bevatten een vastgestelde set beveiligingsmaatregelen. De beveiligingsmaatregelen in de schoolbestuur-firewall gelden voor alle schoollocaties, aangesloten op de dienst Veilig Internet, die onder het schoolbestuur vallen.

De veiligheidsmaatregelen in de schoolbestuur-firewall vinden realtime plaats en zijn onderverdeeld in vijf categorieën en daarnaast biedt DNS de zesde categorie.

	CATEGORIE	CLASSIFICATIE
1	(D)DoS-filter	Algemeen
2	IPS	Algemeen
3	Verkeerfilter *(firewall policy)*	Specifiek
4	Webfilter	Specifiek
5	Application-control	Specifiek

De categorie met classificatie Algemeen geldt voor alle aangesloten schoolbesturen op Veilig Internet. De classificatie Specifiek betekent dat de instellingen per schoolbestuur kunnen afwijken op basis van specifieke wensen en behoeften. Alle functionaliteiten kunnen worden ingericht voor zowel IPv4 als IPv6.

Categorie 1: (D)DoS-filter

Een DDoS-aanval is een gecoördineerde poging van buitenaf om een computer, netwerk of dienst onbruikbaar te maken voor de normale gebruikers. Dit gebeurt door ontzettend veel verkeer te sturen naar servers of andere apparaten op de schoollocaties. Het gevolg is trage netwerk performance, onbereikbare of onbeschikbare netwerken, systemen of applicaties. Veilig Internet maakt gebruik van de DDoS-maatregelen van de firewall in het NDC om afwijkingen in het verkeer tijdig te herkennen. Komt het verkeer boven de ingestelde waarden, dan zal het verkeer vanaf de veroorzakende bron geblokkeerd worden. De firewall grijpt tijdig in waardoor het effect van een (D)DoS over het algemeen zeer beperkt zal zijn en de lessen gewoon door kunnen gaan.

De (D)DoS-controle bij Veilig Internet staat altijd aan voor alle schoolbesturen. Er hoeft niet handmatig ingegrepen te worden om de DDoS-aanval te stoppen, dit gebeurt volledig automatisch.

Categorie 2: IPS

Intrusion Prevention Service (IPS) is een vorm van netwerkbeveiliging die bescherming biedt tegen kwaadaardig verkeer richting uw netwerk. Het herkent verdacht netwerkverkeer en houdt het tegen. De techniek onderzoekt continu alle verkeersstromen met als doel exploits (malafide tools die gebruik maken van bugs of fouten) te detecteren en te blokkeren.

De instellingen voor de (D)DoS-filter en IPS worden door SIVON verzorgd en worden bijgesteld zodra dat nodig is.

Categorie 3: Verkeerfilter

Een verkeerfilter (firewall policy) is een geordende lijst verkeersstromen die toegestaan zijn van en naar het internet. Veilig Internet gaat uit van een standaard set aan verkeerfilters. Op basis van de wensen en behoefte van een schoolbestuur wordt dit aangepast.

In overleg kunnen maatwerk verkeerfilters toegepast worden voor een schoollocatie of segmenten (gebruikersgroepen). Door op IP-blokken (ranges) onderscheid te maken kunnen verkeersstromen wel of niet worden toegestaan. Het segmenteren binnen het LAN en het aanleveren van gesegmenteerde LAN IP-blokken dient te worden gedaan door de schoollocatie. Veilig Internet filtert niet het verkeer tussen de segmenten binnen het LAN van een schoollocatie.

Categorie 4: Webfilter

Het webfilter beperkt en blokkeert het bezoek aan ongewenste of ongeschikte websites die via het netwerk bezocht kunnen worden door medewerkers en leerlingen. Het webfilter beperkt daarmee ook ongewenst bezoek aan specifieke websites om malware te voorkomen. Malware is software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.

Het webfilter werkt met een standaard indeling met hoofdcategorieën en subcategorieën. De volgende subcategorieën zijn standaard voor iedereen geblokkeerd:

- Botnets: Block DNS requests to known botnet C&C
- Potentieel aansprakelijk: Child Abuse, Hacking, Illegal or Unethical
- Beveiligingsrisico: Malicious Websites, Phishing, SPAM URLs

Het schoolbestuur kan kiezen om aanvullende hoofd- en subcategorieën te blokkeren. In bijlage 2: technische specificaties is aanvullende informatie te vinden over de categorieën.

Categorie 5: Application-control

Met application-control kan de toegang beperkt worden tot specifieke groepen toepassingen (bijvoorbeeld VoiP, Remote Access en e-mail) op internet, anders dan gewone websites waarvoor het webfilter dient. De application-control werkt met een indeling in categorieën voor het blokkeren van toepassingen. De categorieën die zich lenen voor misbruik door leerlingen of niet vereist zijn voor het onderwijs, zijn standaard geblokkeerd. Het school- bestuur bepaalt welke categorieën geblokkeerd worden en kiest daarmee welke applicaties worden uitgesloten voor gebruik. Aanvullende informatie over deze categorieën zijn te vinden in bijlage 2: technische specificaties.

Categorie 6: DNS-server

Naast de schoolbestuur-firewall biedt het NDC een DNS-server. De DNS-server maakt onderdeel uit van de dienst Veilig Internet, het gebruik ervan is optioneel. DNS staat voor Domain Name System. Voor schoollocaties die zelf geen DNS-servers hebben, de DNS-server van de huidige access provider gebruiken of de dienst afnemen bij een derde partij, biedt Veilig Internet de mogelijkheid gebruik te maken van zijn DNS-servers. Een DNS-server zorgt ervoor dat de computer bij het intypen van een naam in een browser weet op welke server de website draait, zodat de computer daar de inhoud van de website kan ophalen.

De DNS-servers zijn voorzien van beveiligingsmaatregelen die het moeilijk maken om risicovolle domeinnamen te benaderen. De DNS-servers worden binnen het NDC gehost, wat bijdraagt aan een snelle reactietijd van websites en applicaties.

2.1.3. Verbindingen

Als onderdeel van de dienst Veilig Internet kan er per schoollocatie worden gekozen voor een verbinding uit vier categorieën in oplopende kwaliteit en tarief. Dat zijn:

○ Brons	Coax, koper- of glasvezelverbinding
○ Zilver	Glasvezelverbinding
○ Goud	Glasvezelverbinding
○ Redundant	Glasvezelverbinding dubbel uitgevoerd

Wanneer de bestaande ict-infrastructuur van een schoolbestuur zelf een SURFinternet aansluiting heeft via een SURF regiopop, dan maakt Veilig Internet in overleg hier gebruik van als alternatief voor de hier boven-genoemde categorieën. Veilig Internet verbindt de schoollocaties via het SURF netwerk met het NDC om van de beveiligingsmaatregelen van Veilig Internet te profiteren.

Om tot een gunstigste offerte te komen, besteedt SIVON verbindingen per schoollocatie aan bij de gecontracteerde marktpartijen. Het schoolbestuur kiest per locatie de gewenste categorie en contractstermijn voor de aansluiting met het NDC. SIVON zoekt vervolgens per locatie de beste aanbieder. Lees in hoofdstuk 3 meer over wat het betekent om op Veilig Internet aan te sluiten.

Het schoolbestuur heeft per schoollocatie de keuze uit verschillende contractstermijnen (1, 2 of 3 jaar) en verschillende bandbreedtes binnen een categorie. Per categorie staan beschikbaarheid en kwaliteit vast. Door de keuzevrijheid voor een categorie en binnen de categorie de bandbreedte, heeft u grip op de kosten van Veilig Internet. De opties in categorieën en bandbreedtes vindt u in de tabel op de volgende pagina.

Opties in categorieën en bandbreedtes

	MINIMALE BANDBREEDTE (Download en upload)	RT	JI	PL	BB
Brons	90/15 Mbps	Best effort	Best effort	Best effort	Best effort
	180/30 Mbps				
	500/40 Mbps				
Zilver	100 Mbps	20 ms	Best effort	0,30%	20%[1]
	200 Mbps				
	500 Mbps				
	1 Gbps				
Goud	500 Mbps	15 ms	10 ms	0,30%	99,50%
	1 Gbps				
	10 Gbps				
Redundant	500 Mbps	15 ms	10 ms	0,30%	99,50%
	1 Gbps				
	10 Gbps				

Toelichting

RT Round-trip-time is de maximale tijd (Latency) die het kost om een klein datapakket te zenden naar het NDC en terug te krijgen.

Ji Maximale Jitter heeft betrekking op de maximale variatie in tijdsvertraging in milliseconden (ms) tussen datapakketten over een netwerk.

PL Maximale Packet Loss betekent het verlies van verzonden of ontvangen pakketten over het internet.

BB Het Bandbreedte garantie percentage geeft de zekerheid weer, waarmee de beschikbaarheid van de bandbreedte kan worden gegarandeerd.

1. Bij Zilver wordt de bandbreedte in het netwerk van de access providers gedeeld met andere gebruikers, waardoor de aangegeven bandbreedte niet kan worden gegarandeerd. Aangezien veelal de gebruikers niet tegelijk actief zijn, is de gepercipieerde kwaliteit hoger dan formeel is afgegeven.

Voor schoolbesturen met schoollocaties met een lagere bandbreedte en kwaliteitsbehoefte wordt vanuit SIVON gekeken naar een extra categorie om de kosten te minimaliseren. Uw relatiemanager kan hier meer informatie over verstrekken.

2.2. Aanbestedingen

SIVON is een coöperatie en leden (schoolbesturen) kunnen middels de inbestedingsvariant van artikel 2.24b van de aanbestedingswet de dienst Veilig Internet afnemen van SIVON. Zoals aangegeven bestaat de dienst Veilig Internet uit twee onderdelen: connectiviteit en veiligheid.

Connectiviteit

SIVON heeft voor de totstandkoming van de connectiviteit tussen de schoollocaties en het NDC een Europese aanbesteding opgezet en uitgevoerd. Hierbij zijn meerdere access providers geselecteerd waarmee SIVON een raamovereenkomst heeft afgesloten voor het leveren van de verbindingen.

Hierbij wordt de volgende werkwijze toegepast:

- De uitgevraagde verbindingen per schoolbestuur worden uitgezet via een minicompetitie bij de door SIVON gecontracteerde access providers.
- De schoolbesturen sluiten de overeenkomsten voor afname van de verbinding met SIVON via een dienstverleningsovereenkomst waarin deze dienst is opgenomen.

Veiligheid

Naast de connectiviteit wordt door Kennisnet via SIVON ook veiligheid aangeboden. Hiervoor is via een Europese aanbesteding een leverancier gekozen voor de inrichting van de centrale geregelde beveiligingsmaatregelen in het NDC.

Zodra beide partijen het eens zijn dat de technische en functionele aansluiting van een groep schoollocaties van het schoolbestuur kan worden aangesloten op de dienst Veilig Internet, starten we met een minicompetitie voor de verbindingen.

2.3 Apparatuur op schoollocatie

Voor het gebruik van Veilig Internet plaatsen we apparatuur op schoollocaties. De apparatuur is het demarcatiepunt van Veilig Internet.

Router/CPE

Op de schoollocaties wordt apparatuur geplaatst van de access provider en van SIVON. De router van de access provider wordt aangesloten op de CPE van SIVON. De LAN-interface op de CPE van SIVON vormt het scheidingspunt van Veilig Internet met het lokale netwerk (LAN) van de schoollocatie. De koppeling van Veilig Internet met het lokale netwerk van de schoollocatie is IP gebaseerd. De CPE van SIVON zet de verbinding op tussen uw schoollocatie en het NDC over de verbinding van de access provider.

Aanvullende informatie over Network Address Translation (NAT) en Dynamic Host Configuration Protocol (DHCP) is te vinden in **bijlage 2: technische specificaties**.

IP-adressen

Elke schoollocatie krijgt eigen publieke IPv4-adressen. Per schoollocatie wordt een blok van maximaal 8 IPv4-adressen beschikbaar gesteld. Per datacenterlocatie wordt een blok van maximaal 16 IPv4-adressen beschikbaar gesteld. Indien er meer IPv4-adressen nodig zijn, geef dit dan tijdig aan.

Als er IPv6-adressen gewenst zijn, dan kan het schoolbestuur dit bij de aanvraag aangeven. Indien het schoolbestuur eigen IP-adressen heeft, kunt u deze – in overleg – blijven gebruiken.

Serverruimte

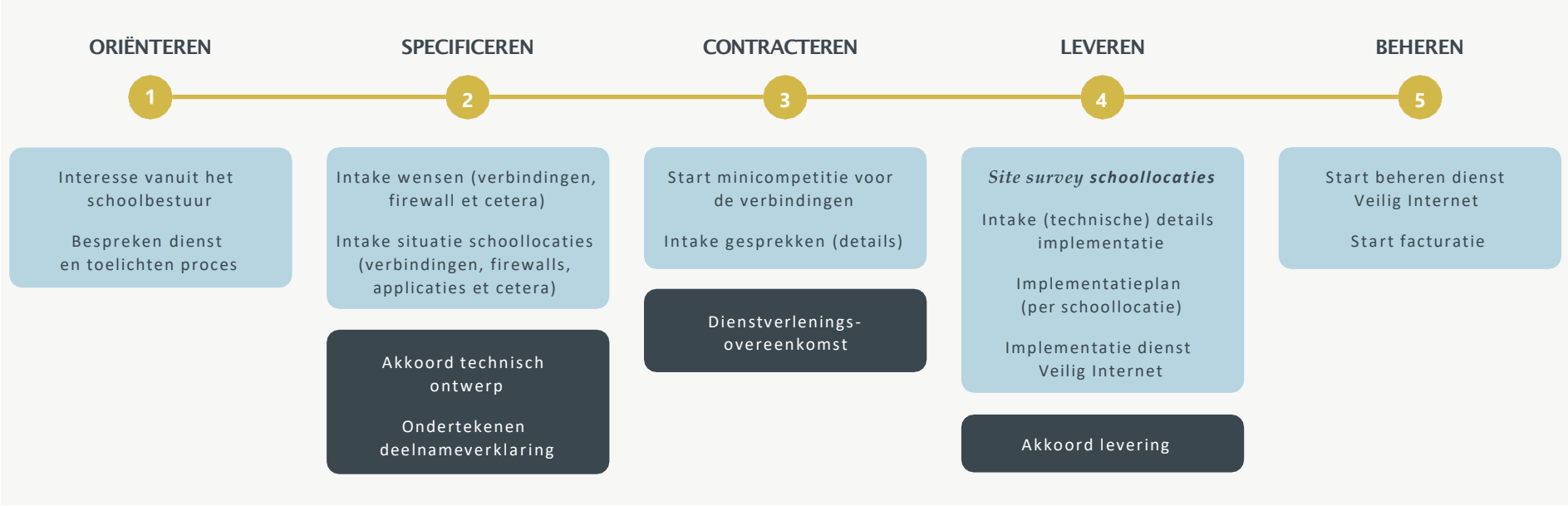
De apparatuur wordt geplaatst in de daarvoor bestemde serverruimte van een schoollocatie. Deze moet voldoende toegerust zijn om de apparatuur voor Veilig Internet te plaatsen. Daarbij gaat het om voor de hand liggende voorzieningen als geaarde stopcontacten, voldoende ruimte in het serverrack voor de CPE’s, stroom, koeling en de juiste stekkers.

3. Aansluiten op Veilig Internet

Bij interesse in Veilig Internet kunt u contact opnemen met de relatiemanager. De inrichting van Veilig Internet kan per schoolbestuur verschillen. Daarom doorlopen we samen met u de stappen van bestelling tot levering. Dit proces wordt zorgvuldig voorbereid en de invulling en uitvoering zijn afhankelijk van het aantal schoollocaties, de omstandigheden ter plaatse en de specifieke wensen en opties bepaald vanuit schoolbestuur.

Het proces dat SIVON met het schoolbestuur doorloopt is in grote lijnen als volgt in te delen:

In de voorbereiding wordt uitgebreid stilgestaan bij elke stap. Een aantal belangrijke stappen worden in de komende paragrafen toegelicht om meer inzicht te geven in de inhoud van de gesprekken die zullen plaatsvinden.



3.1 Het technisch ontwerp

SIVON stemt in de fases Specificeren en Leveren het technisch ontwerp af met het schoolbestuur. Dit technisch ontwerp wordt gezamenlijk samengesteld en in verschillende technische sessies gecompleteerd. In deze sessies wordt informatie verzameld zoals:

- Wat zijn de wensen rondom de bandbreedte per locatie?
- Is de locatie geschikt voor de gewenste bandbreedte?
- Hebben de schoollocaties eigen firewalls en wat zijn de functies van die firewalls?
- Is er onderlinge communicatie tussen de schoollocaties?
- Is er een datacenter aanwezig en wat is de functie ervan?
- Welke beveiligingsmaatregelen worden centraal ingericht?

Zodra op hoofdlijnen duidelijk is dat het schoolbestuur qua techniek in staat is aan te sluiten op de dienst Veilig Internet, wordt het technisch ontwerp vastgesteld. Dit is het teken dat ook de minicompetitie kan worden gestart.

Tijdens de minicompetitie, in de fase Contracteren, wordt gezamenlijk verder inhoud gegeven aan het technisch ontwerp. Het gaat dan vooral

om de lokale details en hoe deze passen in het geheel. Op basis van deze informatie worden in de fase Leveren de details voor de implementatie uitgewerkt.

3.2 De minicompetitie

Het schoolbestuur hoeft zelf geen aanbesteding te doen voor de verbindingen. SIVON besteedt de verbindingen tussen de schoollocaties en NDC aan namens het schoolbestuur, bij de gecontracteerde partijen via een minicompetitie.

SIVON stelt samen met het schoolbestuur een verbindingenoverzicht op.

In dit overzicht worden de schoollocaties opgenomen met adresgegevens, de gevraagde bandbreedte en de gewenste contractduur. Daarnaast wordt in dit overzicht ook een directiebegroting aangegeven per locatie. Dit bedrag geeft het maximale bedrag weer dat het schoolbestuur bereid is uit te geven voor de verbindingen per locatie gedurende de contractduur. Dit overzicht wordt als bijlage bij de deelnameverklaring (DV) gevoegd en via mijnSIVON.nl ter ondertekening aangeboden aan de tekenbevoegde van het schoolbestuur.

In de minicompetitie worden vervolgens de verbindingen uitgevraagd per locatie en ook gegund per locatie. Er wordt alleen gegund bij een bod onder de directiebegroting. De uitslag van de minicompetitie is bindend. Dat betekent dat de gegunde locaties met de uitgevraagde verbinding zullen worden aangesloten op het NDC.

Wanneer het aanbod van alle access providers boven de directiebegroting uit komt, ontstaat er een no bid. Indien er sprake is van een no bid door alle acces providers zal SIVON individueel contact opnemen met de partijen om af te stemmen wat de redenen zijn om een no bid af te geven en welke mogelijkheden er zijn voor de desbetreffende schoollocaties. SIVON helpt uiteraard graag mee om een realistische directiebegroting op te stellen. De definitieve keuze is aan u.

Zodra de locaties zijn gegund, gaat SIVON de contracten aan met de access providers en zal SIVON met het schoolbestuur het contract voor de dienst Veilig Internet ondertekenen.

3.3 De samenwerking

Het belangrijkste aspect van de aansluiting op Veilig Internet, in de fase Leveren, is de samenwerking tussen SIVON en het schoolbestuur. De daadwerkelijke aansluiting van de dienst is afhankelijk van een juiste samenkomst van verschillende activiteiten, die voornamelijk om aandacht van de schoollocaties vragen:

- De tijdige aanlevering van gegevens voor het technisch ontwerp
- De site surveys van de aannemers van de access providers
- Eventuele lokale werkzaamheden die moeten worden verricht voor de aansluiting van de verbinding
- De installatie van de CPE van de access provider
- De installatie van de CPE van SIVON
- Het testen van de afgestemde configuratie

Bovengenoemde activiteiten vragen om vroegtijdige en regelmatige afstemming. Vanuit SIVON zal er een vast aanspreekpunt zijn en het gehele traject begeleiden. Zodra de technische overleggen starten schuift een implementatiemanager aan om kennis te maken met het schoolbestuur en om de technische aspecten mee te krijgen. Na het doorlopen van de minicompetitie en nadat de gunning heeft plaatsgevonden, neemt de implementatiemanager de regie van de implementatie op zich.

Idealiter is er vanuit het schoolbestuur minimaal één vooruitgeschoven contactpersoon als aanspreekpunt voor SIVON, ook wel Single Point of Contact (SPOC) genoemd. De SPOC van het schoolbestuur krijgt toegang tot mijnSIVON.nl voor het goedkeuren van documenten die onderling worden uitgewisseld ten behoeve van de dienst Veilig Internet.

Tijdens de implementatie verlopen de contacten met de schoollocaties via de SPOC. In de samenwerking met de verschillende aannemers voor de access providers is het belangrijk dat data, tijden en lokale contactpersonen goed worden afgestemd en gedeeld met alle betrokkenen. Lokale ict-verantwoordelijken hebben het vaak druk en moeten rekening houden met allerlei dagelijkse geplande evenementen. Een wijziging aan de ict-infrastructuur komt zelden uit. SIVON vindt het dan ook belangrijk dat zij goed geïnformeerd zijn. Hun medewerking is cruciaal voor een succesvolle implementatie. Hierdoor kunnen verrassingen worden geminimaliseerd.

3.4 mijnSIVON.nl

Bij het aangaan van het lidmaatschap van SIVON heeft het schoolbestuur kennis gemaakt met mijnSIVON.nl. Voor de dienst Veilig Internet wordt de omgeving uitgebreid met de volgende functionaliteiten:

- Aanmelden van incidenten en verstoringen
- Indienen van technische wijzigingsverzoeken
- Inzage van voortgang en status van meldingen
- Communicatie via chat over deze meldingen met de Servicedesk
- Inzage in bandbreedtegebruik en connecties per verbinding
- Afhandeling formele documenten met de SPOC of tekenbevoegde
- Documenten ter ondertekening voor de tekenbevoegde

4. Serviceafspraken

Bij de aansluiting van een schoolbestuur op de dienst Veilig Internet wordt gedurende de implementatieperiode goed gekeken naar de eigenschappen van een schoolbestuur en de daarbij behorende wijze van aansluiten. Dit resulteert in een passende oplevering en nazorg.

Zodra een schoollocatie van een schoolbestuur volgens de afgestemde scope en planning is opgeleverd, gaat deze schoollocatie over van levering naar beheer. In dit hoofdstuk wordt op hoofdlijnen ingegaan op de serviceafspraken rondom de dienst Veilig Internet. Bij oplevering van de dienst wordt de meer specifieke informatie overhandigd.

Beschikbaarheid

De beschikbaarheid van de dienst Veilig Internet wordt uitgedrukt in het percentage van de tijd dat de dienst gedurende een jaar daadwerkelijk beschikbaar is. Zowel de beschikbaarheid van het NDC als de toegang tot het internet is hetzelfde voor alle schoolbesturen en bedraagt minimaal 99,94%.

De beschikbaarheid van de verbindingen van een schoollocatie naar het NDC is afhankelijk van de verbindingscategorie die het schoolbestuur per schoollocatie bepaalt. De verbindingen kennen per categorie de volgende minimale beschikbaarheid op jaarbasis:

CATEGORIE	BRONS	ZILVER	GOUD	REDUNDANT
Beschikbaarheids-percentage	Best effort	99,8%	99,95%	99,98%

Kennisnet support

Kennisnet support gaat u helpen bij storingen en incidenten. Geregistreerde SPOC's of vooraf opgegeven contactpersonen door het schoolbestuur kunnen contact opnemen met Kennisnet support. De support is tijdens werkdagen beschikbaar van maandag tot en met vrijdag van 07:30 – 17:00 uur. Het NDC en de verbindingen worden uiteraard 24/7 gemonitord om storingen snel te detecteren. Telefonisch aangemelde storingen worden direct in behandeling genomen, meldingen per mail binnen 30 minuten.

Wijzigingen

Voor wijzigingen en vragen over wijzigingen kan het schoolbestuur terecht bij Kennisnet support. Aanvragen voor wijzigingen in de beveiligingsmaatregelen kunnen direct gericht worden aan wijziging.veiliginternet@kennisnet.nl

SIVON kent categorieën voor wijzigingen, waarbij de doorlooptijd varieert:

	WIJZIGING	DOORLOOPTIJD
1	Beveiligingsmaatregelen: web- of applicatiefilter	Binnen 1 werkdag
2	Beveiligingsmaatregelen: verkeersfilter	In overleg
3	Wijzigen (NAT) routering	In overleg
4	Toevoegen/verhuizen schoollocatie	In overleg
5	Wijzigen bandbreedte	In overleg
6	Opheffen schoollocatie/schoolbestuur	In overleg
7	Overige wijzigingen	In overleg

Wijzigingen in de schoolbestuur-firewall worden niet in rekening gebracht en zijn onderdeel van de dienst.

De bandbreedte mag verhoogd of verlaagd worden tijdens de contracttermijn van de verbinding, mits de leverancier de gewenste bandbreedte kan leveren. De wijzigingen worden in rekening gebracht als onderdeel van de dienst en kunnen leiden tot eenmalige kosten en wijziging van de maandelijkse kosten. Indien door de wijziging de apparatuur op de schoollocatie vervangen moet worden, zijn de kosten voor SIVON gedurende de looptijd van de subsidie (2019-2023).

In geval van verhuizing kan een bestaande aansluiting op Veilig Internet meegenomen worden naar de nieuwe locatie, mits de nieuwe locatie zich bevindt in het verzorgingsgebied van de access provider. Eventuele eenmalige kosten voor verhuizen komen voor rekening van het schoolbestuur.

Indien het verhuizen van de bestaande aansluiting op de dienst Veilig Internet niet mogelijk is, wordt in overleg gekeken naar een oplossing.

Bekijk de volledige en actuele serviceafspraken van Veilig Internet op de website van SIVON.

5. Contractuele samenwerking

Het schoolbestuur sluit een contract af met SIVON voor Veilig Internet. Dat wil zeggen dat de onderliggende contracten voor de aansluiting op de schoollocaties die vallen binnen het schoolbestuur, worden afgesloten en beheerd door SIVON.

5.1 Documenten

De deelnameverklaring (DV)

SIVON gaat de minicompetitie aan namens het schoolbestuur. Door middel van de deelnameverklaring machtigt het schoolbestuur SIVON om de minicompetitie te starten. De deelnameverklaring is een eenzijdig ondertekende verklaring door het schoolbestuur. Daarin staat dat u akkoord bent met het indienen van de minicompetitie voor de aanvraag van verbindingen bij de access providers en dat u zich bewust bent van het feit dat uit deze minicompetitie een gunning komt waar u zich contractueel aan verbindt.

De dienstverleningsovereenkomst (DVO)

Voor Veilig internet gaat het schoolbestuur een overeenkomst aan met SIVON, waarin de overkoepelende bepalingen zijn beschreven voor de aansluiting van de verschillende schoollocaties op de dienst. Er gelden verschillende regels voor het opzeggen van de dienst Veilig Internet en

een opzegging van de internetverbinding naar een van de locaties. De DVO geeft duidelijkheid over deze onderwerpen.

5.2 Kosten

Als lid van SIVON betaalt u lidmaatschap en profiteert u van gunstige voorwaarden. Veilig Internet kent eenmalige en maandelijkse kosten.

Per schoollocatie betaalt u maandelijkse en eenmalige kosten. De kosten van de access providers worden doorbelast. Daarnaast wordt er ieder jaar door de ledenraad van SIVON een internettarief vastgesteld per categorie access en bandbreedte. Dit internettarief is er om de verwachte kosten van SIVON voor het komend jaar voor Veilig Internet te dekken.

Deze kosten zijn de optelsom van de kosten voor de verbindingen en de kosten voor de centraal ingerichte beveiligingsmaatregelen. De kosten voor de gesubsidieerde delen (vooral de beveiligingsmaatregelen) worden niet doorberekend gedurende de looptijd van de subsidie (2019-2023). Meer informatie vindt u hierover in de DVO.

5.3 Facturatie

Na levering aan de eerste schoollocatie ontvangt u de eerste factuur met de eenmalige kosten voor de installatie en uw maandelijkse kosten. Daarna ontvangt u per mail maandelijks een factuur voor alle schoollocaties aangesloten op Veilig Internet met de volgende informatie:

- kosten van de fysieke verbindingen voor de komende maand, opgesplitst per schoollocatie
- kosten van het internettarief voor de komende maand, opgesplitst per schoollocatie
- eenmalige kosten van wijzigingen op uw verzoek.

Als u vragen heeft over de facturatie, kunt u contact opnemen met Kennisnet support via 0800 – 321 22 33 of per mail via support@kennisnet.nl

6. Bijlagen

Bijlage 1: Begrippenlijst algemeen, terminologie

TERM	BETEKENIS
Access Provider	Marktpartij gecontracteerd door SIVON voor de levering van verbindingen van de schoollocaties naar het NDC.
CPE	Apparatuur zoals routers, bekabeling en overige benodigde voorzieningen, die door SIVON op een schoollocatie worden geplaatst om toegang tot de dienst Veilig Internet mogelijk te maken. Op de CPE mag de schoolinstelling het LAN aansluiten. Na het beëindigen van het contract dient de CPE teruggegeven te worden aan SIVON.
Nationaal Dienstencentrum (NDC)	De locatie(s), ondergebracht in datacentra van Veilig Internet, waar de veilige toegang naar en van het internet centraal geregeld wordt.
Schoolbestuur	Het orgaan van het bevoegd gezag dat op basis van statuten of een andere regeling belast is met de verantwoordelijkheid voor de uitoefening van de taken en bevoegdheden namens het bevoegd gezag.
Schoolbestuur-firewall	In het NDC wordt per schoolbestuur een virtuele firewall ingericht. Het schoolbestuur heeft de mogelijkheid hier specifieke beveiligingsmaatregelen in te stellen die gelden voor alle schoollocaties binnen het schoolbestuur.
Schoollocatie	Fysieke locatie(s)/gebouw(en) binnen een schoolbestuur, waaronder wordt verstaan de scholen, bestuursgebouwen en datacentra die onderdeel zijn van het interne schoolnetwerk.
Single Point of Contact (SPOC)	SPOC is één aanspreekpunt voor klanten bij een service, activiteit of programma voor de communicatie met persoon en organisaties geassocieerd met de bron.
Storing	Een niet-geplande onderbreking van signaal- of dataoverdracht over een ethernetverbinding. Een storing is een gebrek.
Verbinding	Verbinding tussen een schoollocatie en het NDC die door access provider wordt beheerd.
Werkdagen	Kalenderdagen, behalve zaterdagen, zondagen en algemeen erkende feestdagen in Nederland. Tevens valt de jaarlijkse collectieve sluiting van Kennisnet tussen kerst en oud en nieuw ook buiten de werkdagen. Uiteraard zal de monitoring en acties op het centrale gedeelte NDC gedurende deze momenten worden voortgezet.

Bijlage 2: Technische specificaties

Application control

De firewall kent een indeling in 19 categorieën voor het blokkeren van applicaties. De categorieën die zich lenen voor misbruik of niet vereist zijn voor het onderwijs zijn standaard geblokkeerd, zie onderstaande tabel.

HOOFDCATEGORIE		UITLEG
Business	Allow	Business related applications such as office suites
Cloud.IT	Allow	Cloud based applications
Collaboration	Allow	Applications used for desktop sharing, remote meetings and other connected collaboration
Email	Allow	Applications for sending/receiving and processing email
Game	Allow	Game applications
General.Interest	Allow	General interest tools, applications
Industrial	Allow	Industrial applications
Mobile	Allow	Mobile application communications
Network.Service	Allow	Applications used for network related services and communications
P2P	Block	Peer-to-Peer applications used for sharing files
Proxy	Block	Proxy and VPN applications
Remote.Access	Allow	Remote access applications for file transfer or remote control
Social.Media	Allow	Online social media applications
Storage.Backup	Allow	Online storage applications for storage of files and photos
Update	Allow	Communications to update servers for various applications
Video	Allow	Video sharing, streaming and broadcasting applications
VoIP	Allow	Voice over IP applications
Web.Client	Allow	HTTP based client applications
Unknown Applications	Allow	All traffic that was not detected by any of the other application categories

Een up-to-date overzicht van de applicaties is te vinden op de Fortinet website.

Webfilter

De leverancier van de firewalls in het NDC, Fortinet, hanteert een standaard indeling voor de websites in zeven hoofdcategorieën en 87 subcategorieën. Het schoolbestuur kan kiezen om aanvullende hoofd- en subcategorieën te blokkeren. Een up-to-date overzicht van de categorieën is te vinden op de Fortinet website.

Voorbeelden van te overwegen categorieën om te blokkeren zitten in de Adult content: Pornography, Nudity and Risque en Other Adult Materials.

Netwerk Address Translation

Network Address Translation (NAT) maakt onderdeel uit van de dienst Veilig Internet en gebeurt bij voorkeur op de CPE geplaatst op de schoollocatie.

In overleg en als het kan zijn er alternatieven mogelijk.

Dynamic Host Configuration Protocol

Het toepassen van Dynamic Host Configuration Protocol (DHCP), om automatisch IP-adressen toe te wijzen aan de verschillende computers in een netwerk, is alleen mogelijk wanneer er geen gebruik wordt gemaakt van segmentering in het LAN (VLANs). Als er meerdere VLAN’s zijn is DHCP de verantwoordelijkheid van de schoollocatie.

SIVON

COÖPERATIE SIVON

WWW.SIVON.NL
INFO@SIVON.NL