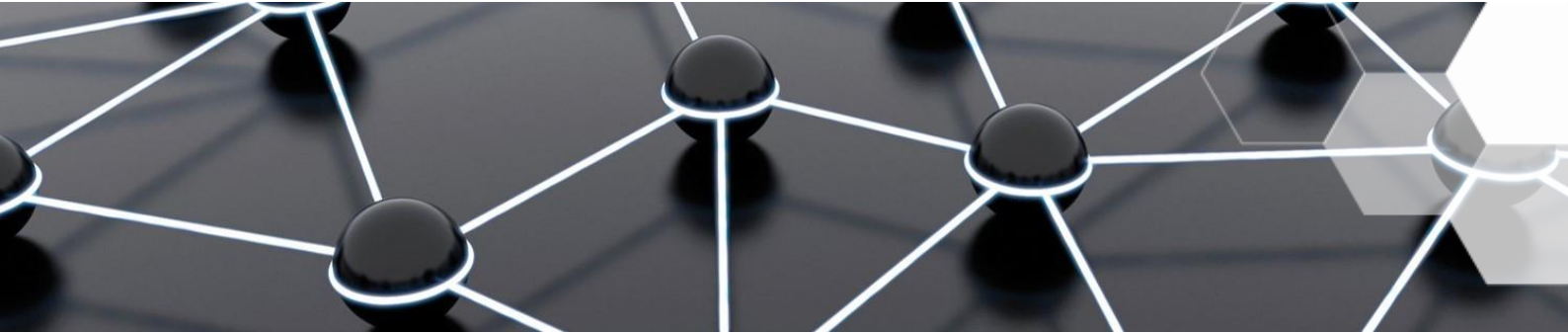




Panteia

Research to Progress

Research voor Beleid | EIM | NEA | IOO | Stratus | IPM



Eindgebruikersonderzoek zakelijke netwerkdiensten

Paul van der Zeijden; René Vogels; Marianne van Marwijk

Zoetermeer, 16 november 2017

De verantwoordelijkheid voor de inhoud berust bij Panteia. Het gebruik van cijfers en/of teksten als toelichting of ondersteuning in artikelen, scripties en boeken is toegestaan mits de bron duidelijk wordt vermeld. Vermenigvuldigen en/of openbaarmaking in welke vorm ook, alsmede opslag in een retrieval system, is uitsluitend toegestaan na schriftelijke toestemming van Panteia. Panteia aanvaardt geen aansprakelijkheid voor drukfouten en/of andere onvolkomenheden.

The responsibility for the contents of this report lies with Panteia. Quoting numbers or text in papers, essays and books is permitted only when the source is clearly mentioned. No part of this publication may be copied and/or published in any form or by any means, or stored in a retrieval system, without the prior written permission of Panteia. Panteia does not accept responsibility for printing errors and/or other imperfections.

Inhoudsopgave

1	Inleiding	4
1.1	Aanleiding	4
1.2	Gesloten VPN versus open VPN	4
1.3	Aanpak en verloop onderzoek	5
2	Resultaten	8
2.1	Toepassingen gesloten VPN	8
2.2	Redenen toepassen gesloten VPN	8
2.3	Wat voor de huidige gesloten VPN?	9
2.4	Gebruik open VPN	10
2.5	Open VPN als alternatief voor gesloten VPN	10
2.6	Overwegingen om over te stappen	11
2.7	Kosten	14
3	Conclusies	15



1 Inleiding

1.1 Aanleiding

De Autoriteit Consumenten en Markt (ACM) voert regelmatig marktanalyses uit in de telecommarkt, waarbij markten worden afgebakend en geanalyseerd en wordt bepaald of er sprake is van aanbieders met een aanmerkelijke marktmacht (AMM). Hiervoor heeft de ACM behoefte aan onderzoek naar de vraagsubstitutie onder zakelijke afnemers van **gesloten VPN's naar open VPN's**. De ACM heeft Panteia gevraagd een enquête uit te voeren onder zakelijke afnemers **van Gesloten VPN's**. In deze rapportage worden de resultaten van het onderzoek uitgewerkt.

De resultaten van de enquête moeten de opdrachtgever helpen antwoord te geven op de vraag in hoeverre **Open VPN's voor zakelijke afnemers een alternatief zijn voor Gesloten VPN's**. Het gaat hierbij om het oordeel van zakelijke afnemers van Gesloten VPN's.

1.2 Gesloten VPN versus open VPN

De volgende zakelijke netwerkdiensten worden onderscheiden: klassieke huurlijnen, **gesloten VPN's (Ethernet-VPN's en IP-VPN's)**, dark fiber en lichtpaden, en open VPN's. VPN staat voor virtual private network.

Gesloten VPN

Gesloten VPN's worden door zakelijke eindgebruikers gebruikt voor het koppelen van bedrijfslocaties. Dit gaat via een pakket geschakeld netwerk waarvoor verschillende technieken worden gebruikt, met name Ethernet (Ethernet-VPN, ofwel E-VPN) en Internet Protocol (IP-VPN). **Gesloten VPN's kunnen worden geleverd met beschikbaarheids- en capaciteitsgaranties.**

Open VPN

Open VPN's zijn bedrijfsnetwerken gebouwd op een openbare internetverbinding. Dit verschilt van een gesloten VPN waarbij er een aparte vaste VPN-aansluiting wordt gerealiseerd. Een open VPN bestaat uit een combinatie van een internetaansluiting en een open VPN-verbinding tussen bedrijfslocaties, waarbij beide diensten afzonderlijk ingekocht kunnen worden bij verschillende operators.

Open VPN's omvatten geen remote access, een toepassing die ervoor zorgt dat een enkele gebruiker (bijvoorbeeld een thuiswerker of mobiele werker) tijdelijk en locatieonafhankelijk met een bedrijfsnetwerk verbonden kan worden door middel van een verbinding met software (VPN-cliënt). De reden hiervoor is dat het bij zakelijke netwerkdiensten gaat om het verbinden van bedrijfslocaties.

1.3 Aanpak en verloop onderzoek

Telefonische enquête en beoogde netto-respons

Het onderzoek is uitgevoerd door middel van een telefonische enquête onder zakelijke gebruikers van gesloten VPN's. De beoogde netto-respons was 250 geslaagde gesprekken met zakelijke gebruikers van gesloten VPN's. Dit is voldoende om betrouwbare uitspraken te doen over de populatie van zakelijke gebruikers van gesloten VPN's.

Doelgroep

Beoogde respondenten waren bedrijven die gebruik maken van een gesloten VPN. Deze worden gebruikt voor het verbinden van verschillende vestigingen, voor het verbinden met IT-dienstverleners, etc. Volgens de Telecommonitor van de ACM gaat het om circa 100.000 aansluitingen. VPN's bestaan per definitie uit meerdere aansluitingen. Het aantal aansluitingen per VPN verschilt enorm. Er zijn daardoor geen aantallen beschikbaar over het aantal bedrijven dat gesloten VPN's gebruikt, en voor welke doeleinden.

Het was van belang om zakelijke gebruikers van gesloten VPN's te benaderen. Het gebruik van een algemeen bedrijvenbestand, zoals het KvK-bestand, was hiervoor niet geschikt omdat de trefkans (een zakelijke gebruiker van een gesloten VPN) te klein was. Daarom is ervoor gekozen een adressenbestand te gebruiken waarbij de trefkans groter zou zijn. Dit bestand is aangeleverd door de ACM. Het gaat om een lijst bedrijven met adresgegevens dat is gebaseerd op een bedrijvenbestand dat de ACM in 2015 heeft gekocht van SIZO. De lijst bevat alle bedrijven (vestigingen) met meer dan 5 werknemers. Selectie van geschikte respondenten heeft vervolgens plaatsgevonden op basis van een aantal gerichte vragen om na te gaan of bedrijven gebruik maken van een gesloten VPN.

Onzekerheden/risico's

Vooraf was reeds duidelijk dat sprake was van een aantal onzekerheden en risico's bij het uitvoeren van de telefonische enquête. Deze laten zich als volgt samenvatten:

- Onvoldoende IT-kennis bij de respondenten, waardoor respondenten mogelijk geen goed zicht hebben of sprake is van gesloten of open VPN en/of vragen hierover onvoldoende konden beantwoorden. Daarbij komt dat de terminologie niet altijd eenduidig wordt gehanteerd. Het kan bijvoorbeeld zijn dat open VPN's voor respondenten met onvoldoende kennis gesloten VPN's lijken;
- Veel bedrijven hebben hun ICT-activiteiten uitbesteed waardoor onvoldoende kennis over VPN in het bedrijf zelf aanwezig is;
- Vertrouwelijkheid waardoor potentiële respondenten geen informatie willen geven over hun IT-netwerken en daarom niet mee willen werken of de naam van de provider niet willen noemen.

Deze aspecten hebben zich gedurende het onderzoek allemaal in meer of mindere mate voorgedaan. Dit leidt ertoe dat niet altijd met zekerheid kan worden gesteld dat daadwerkelijk sprake is van een gesloten VPN en er sprake is van enige onzekerheid ten aanzien van de resultaten en conclusies.



Werkwijze selectie

Voor de selectie van geschikte respondenten is bij potentiële respondenten eerst gevraagd naar de IT-verantwoordelijke binnen het bedrijf. Aan de IT-verantwoordelijke is vervolgens gevraagd of het bedrijf gebruikmaakt van een gesloten VPN. Indien zij hebben aangegeven gebruik te maken van een gesloten VPN zijn enkele checkvragen gesteld, waaronder de naam van de provider van de gesloten VPN en vragen over de aard van de internetverbinding (rechtstreeks of via een centrale beveiligde internetkoppeling).

In een volgende stap is de consistentie van de beantwoording gecontroleerd. In de gevallen dat het onwaarschijnlijk is dat het gaat om een gesloten VPN, zijn de respondenten niet in de onderzoeksresultaten opgenomen en zijn aanvullende telefonische interviews gehouden.

Redenen waarom het onwaarschijnlijk was dat gebruik wordt gemaakt van een gesloten VPN waren:

- **de provider die is genoemd bij 'anders' biedt geen gesloten VPN aan** (bijvoorbeeld Xs4all). Diverse respondenten hebben een ICT-bedrijf genoemd die voor hen de ICT en de VPN verbinding regelt. Ook daarbij is een inschatting gemaakt of het waarschijnlijk is dat het betreffende ICT-**bedrijf voor gesloten VPN's kan zorgen (door de website van de ICT-bedrijven te bekijken)**;
- respondenten gaven bij de toepassingen alleen aan dat de VPN wordt gebruikt voor remote access;
- respondenten die geen toepassingen voor hun gesloten VPN konden noemen.

Responsverantwoording

Zoals in het voorgaande is aangegeven is door de ACM een adressenbestand aangeleverd van bedrijven die door hen als kansrijk werden ingeschat (grotere kans dat het bedrijf over een gesloten VPN beschikt). Dit adressenbestand bevatte 153.356 adressen. Omdat in overleg met de ACM werd ingeschat dat de trefkans nog groter is bij bedrijven die meerdere vestigingen hebben, zijn bedrijven die hieraan niet voldeden uit het adressenbestand gehaald¹.

In het aangeleverde adressenbestand waren geen telefoonnummers opgenomen. Panteia heeft de overgebleven adressen zoveel mogelijk verrijkt met een telefoonnummer met behulp van het Kamer van Koophandel bestand en vervolgens ontdebeld (op basis van telefoonnummer). In totaal bleven 43.636 adressen beschikbaar. Hieruit is een aselechte steekproef getrokken van 4.805 adressen, waarvan een deel is gebruikt. In tabel 1 is het responsverloop weergegeven. Daaruit blijkt het grote aantal weigeringen, het grote aantal bedrijven dat de ICT heeft uitbesteed waarbij er onvoldoende kennis in het bedrijf is om

¹ Gedurende het veldwerk bleek dat een deel van de bedrijven maar één vestiging had. In de enquête is gevraagd naar het aantal vestigingen. 60 bedrijven die in het aangeleverde bestand geregistreerd staan als bedrijf met meerdere locaties gaven als antwoord dat de organisatie niet uit meerdere vestigingen bestaat. Dit kan te maken hebben met onjuistheden in het basisbestand of onjuiste interpretatie van de vraag door de respondent, bijvoorbeeld als het bedrijf onderdeel is van een concern maar de respondent de vraag heeft geïnterpreteerd voor de eigen vestiging.

de vragen te kunnen beantwoorden en het grote aantal selectiegesprekken om bedrijven met een gesloten VPN te vinden.

tabel 1 Responsverloop

	<i>Aantal</i>	<i>%</i>
Contacten met bedrijven	2.577	100%
Weigering	1.228	47,7%
ICT wordt uitbesteed, niemand in bedrijf weet er iets van	224	8,7%
Geen gesloten VPN (inclusief volledige gesprekken, die zijn verwijderd omdat het onwaarschijnlijk was dat sprake was van een gesloten VPN)	874	33,9%
<i>Volledig gesprek gevoerd</i>	<i>251</i>	<i>9,7%</i>

Representativiteit

Aangezien er geen bestanden zijn van bedrijven **die gesloten VPN's** gebruiken is voor het onderzoek gebruik gemaakt van een door de ACM aangeleverd adressenbestand waarvan is aangenomen dat de kans bedrijven te treffen met een gesloten VPN zo groot mogelijk is. Om deze kans nog te vergroten zijn binnen dit bestand alleen bedrijven gebruikt voor het onderzoek waarvan was aangegeven dat zij meerdere locaties **hebben (aangezien werd aangenomen dat gesloten VPN's veelal gebruikt worden door bedrijven met meerdere locaties)**. Hieruit is vervolgens een aselechte steekproef getrokken. Deze werkwijze is gekozen om een zo goed mogelijke afspiegeling te realiseren van bedrijven die gebruik **maken van gesloten VPN's**. Aangezien er geen bestand is van gebruikers **van gesloten VPN's met verschillende kenmerken is het niet mogelijk om exact na te gaan of de respondenten een goede afspiegeling zijn van de gebruikers van gesloten VPN.**

Kenmerken respondenten

Het veldwerk heeft geresulteerd in 251 bruikbare interviews. Enkele kenmerken van deze respondenten zijn:

- 191 van de 251 respondenten hebben meerdere vestigingen
- 10 van de 251 respondenten hebben naast gesloten VPN ook open VPN
- 27 van de 251 respondenten hebben ook een huurlijn
- 22 van de 251 respondenten hebben ook een Dark Fiber of Lichtpad.



2 Resultaten

In dit hoofdstuk worden de resultaten van de telefonische enquête onder **gebruikers van gesloten VPN's weergegeven. Achtereenvolgens komen aan de orde de toepassingen waarvoor gesloten VPN's worden gebruikt, redenen om gebruik te maken van gesloten VPN, wat men had voor het huidige contract voor de gesloten VPN, de mate waarin open VPN gezien wordt als alternatief voor gesloten VPN en de overwegingen om van gesloten VPN over te stappen naar open VPN.**

2.1 Toepassingen gesloten VPN

VPN vooral voor dataverkeer, e-mail en beveiliging

In tabel 2 is aangegeven voor welke toepassingen de respondent de gesloten VPN gebruiken. De meest voorkomende toepassing betreft het dataverkeer, gevolgd door e-mail en beveiliging. Bij andere toepassingen worden onder andere genoemd: bedrijfsapplicaties en ERP boekhouding.

tabel 2 Toepassingen waarvoor de gesloten VPN wordt gebruikt, aantal respondenten in procenten (n=251)

<i>Toepassing</i>	<i>%</i>
Beveiliging	69%
Data	96%
E-mail	77%
Interne telefonie	46%
Video conferencing	15%
PIN	25%
Andere toepassingen	13%

Bron: Panteia, 2017.

2.2 Redenen toepassen gesloten VPN

62% noemt als reden veiligheid

In tabel 3 worden de redenen genoemd om te kiezen voor het gebruik van gesloten VPN in plaats van open VPN. De belangrijkste reden is duidelijk veiligheid. Bij andere redenen is genoemd: advies van ict-aanbieder of systeembeheerder, verplichting vanuit moederbedrijf of leverancier, capaciteit/betrouwbaarheid, beheer en gemak.

tabel 3 Redenen voor het gebruik van gesloten VPN in plaats van een open VPN, aantal respondenten in procenten (n=251)

<i>Toepassing</i>	<i>%</i>
Kwaliteitsgaranties	7%
Snelheid	5%
Veiligheid	62%
Andere redenen	20%
weet niet/wil niet zeggen	19%

Bron: Panteia, 2017.

2.3 Wat voor de huidige gesloten VPN?

33% had hiervoor
niets

Aan de respondenten is gevraagd wat zij hadden voor de ingang van het huidige gesloten VPN contract. Een derde van de respondenten geeft aan hiervoor niets te hebben gehad. Ruim een kwart van de respondenten weet het niet of wil het niet zeggen. Bijna een kwart had voor het huidige contract ook een gesloten VPN. Een klein deel van de respondenten is overgestapt van een huurlijn of van een open VPN naar een gesloten VPN (beide 7%).

tabel 4 Wat hadden de respondenten voor ingang van het huidige contract voor de gesloten VPN, aantal respondenten in procenten (n=251)

<i>Netwerkdienst voor de huidige gesloten VPN</i>	<i>%</i>
Ook gesloten	24%
Huurlijn	7%
Open VPN	7%
Niks	33%
Weet niet/wil niet zeggen	29%
Total	100%

Bron: Panteia, 2017.

Overgestapt
vanwege veiligheid

Aan de respondenten die hebben aangegeven van huurlijn of van open VPN naar gesloten VPN te zijn gestapt, is gevraagd wat hiervan de redenen waren. Bij de overstap van huurlijn naar gesloten VPN worden redenen genoemd als veiligheid, snelheid/capaciteit en kosten. Bij de overstap van open VPN naar gesloten VPN wordt vooral veiligheid als reden genoemd. Daarnaast worden snelheid en betrouwbaarheid een enkele keer genoemd.



2.4 Gebruik open VPN

Tien respondenten hebben aangegeven naast de gesloten VPN een open VPN te gebruiken. Geen van deze tien respondenten maakt voor beveiliging gebruik van de open VPN, terwijl zes van deze respondenten wel een gesloten VPN gebruiken voor beveiliging. **De open VPN's worden gebruikt voor:**

- E-mail (5)
- Data (4)
- Remote desktop (4)
- Interne telefonie (3)
- Video conferencing (1)

2.5 Open VPN als alternatief voor gesloten VPN

Meerderheid ziet open VPN niet als alternatief...

...vooral niet voor beveiliging

Voor een aantal toepassingen kan een open VPN een alternatief zijn voor een gesloten VPN volgens de deelnemers aan het onderzoek. In tabel 5 zijn de resultaten weergegeven. De laatste kolom laat zien hoeveel respondenten gesloten VPN voor die toepassing gebruiken. Voor alle toepassingen geldt dat de meeste respondenten open VPN niet zien als alternatief voor gesloten VPN. Het sterkst geldt dat voor beveiliging en voor data.

tabel 5 Mate waarin open VPN wordt gezien als alternatief voor gesloten VPN, per toepassing, aantal respondenten in procenten van het aantal respondenten dat de gesloten VPN voor de betreffende toepassing gebruikt

Toepassing	Wel	Niet	Weet niet/ wil niet zeggen	n
Beveiliging	8%	71%	21%	174
Data	14%	64%	22%	242
E-mail	23%	55%	22%	193
Interne telefonie	26%	50%	24%	116
Video conferencing	26%	58%	16%	38
PIN	22%	54%	24%	63
Andere toepassingen	22%	56%	22%	32

Bron: Panteia, 2017.

Veiligheid belangrijkste reden

In tabel 6 zijn per toepassing de redenen weergegeven waarom voor de respondenten open VPN geen alternatief is voor gesloten VPN. Daaruit blijkt dat veiligheid veruit de belangrijkste reden is voor alle toepassingen, met uitzondering van video conferencing. Voor video conferencing is de up- en download capaciteit de belangrijkste reden.

tabel 6 Redenen waarom open VPN niet wordt gezien als alternatief voor gesloten VPN, per toepassing, aantal respondenten in procenten van het aantal respondenten dat open VPN niet ziet als alternatief voor de gesloten VPN voor de betreffende toepassing

<i>Reden</i>	<i>beveiliging</i>	<i>data</i>	<i>e-mail</i>	<i>interne telefonie</i>	<i>video confe- rencing</i>	<i>PIN</i>	<i>Andere toepas- singen</i>
Up- en download Capaciteit	3%	2%	3%	3%	86%	3%	0%
Beschikbaarheidsgarantie	4%	5%	4%	5%	0%	0%	0%
Capaciteitsgarantie	4%	1%	2%	7%	0%	9%	11%
Veiligheid	67%	78%	79%	59%	0%	65%	61%
Andere redenen	9%	10%	8%	14%	5%	15%	28%
Weet niet/wil niet zeggen	21%	10%	10%	19%	9%	18%	11%
(n)	(123)	(154)	(106)	(58)	(22)	(34)	(18)

Bron: Panteia, 2017.

Als open VPN wel een alternatief is, dan wordt daarvoor een aantal redenen genoemd. Een klein aantal respondenten ziet open VPN als alternatief voor gesloten VPN en niet alle respondenten kunnen of willen een reden noemen. Per toepassing gaat het om de volgende redenen:

- Beveiliging: veiligheid zou bij open VPN ook voldoende mogelijk zijn en daarnaast de prijs,
- Data: open VPN is geschikt als het om minder gevoelige data gaat of als de veiligheid voldoende is te beheren en daarnaast de prijs,
- E-mail: open VPN is geschikt als deze voldoende is te beveiligen; daarnaast wordt aangegeven dat e-mail veelal via open verbindingen loopt; daarnaast de prijs,
- Interne telefonie: omdat er geen vertrouwelijke gegevens over de telefoon gaan; als de veiligheid voldoende is te beheren,
- Video conferencing: het gaat om weinig vertrouwelijke informatie,
- PIN: open VPN is hiervoor voldoende beveiligd en daarnaast de kosten.

2.6 Overwegingen om over te stappen

Overweging om met de hele organisatie over te stappen naar open VPN

Overstappen naar open VPN geen optie voor 76%

Aan de respondenten is gevraagd of zij zouden overwegen met de gehele organisatie over te stappen naar open VPN. Voor driekwart is dat geen optie en 14% weet het niet of wil het niet zeggen. 10% zou het overwegen.



tabel 7 Mate waarin de respondenten met de gehele organisatie zouden overstappen van gesloten VPN naar open VPN, aantal respondenten in procenten (n=251)

<i>Overstappen overwegen</i>	<i>%</i>
Ja	10%
Nee	76%
Weet niet/wil niet zeggen	14%
Totaal	100%

Bron: Panteia, 2017.

De antwoorden op de vraag waarom respondenten een overstap naar open VPN voor de gehele organisatie zouden overwegen kunnen als volgt worden gecategoriseerd:

- Afhankelijk van de mogelijkheden en de voor- en nadelen (9 x genoemd),
- Als het goedkoper is (8 x genoemd),
- Als het voldoende beveiligd is (4 x genoemd),
- Als het wordt geadviseerd door externen (2 x genoemd).

De gegeven antwoorden zijn over het algemeen weinig concreet. De respondenten lijken er daarom weinig zicht op te hebben, waarbij het twijfelachtig is of men daadwerkelijk zou overwegen om over te stappen naar open VPN.

De redenen waarom respondenten **niet** overwegen een overstap naar open VPN voor de gehele organisatie te maken kunnen als volgt worden gecategoriseerd (aspecten die tenminste 5 keer zijn genoemd):

- Open VPN is niet veilig genoeg (107 x genoemd)
- Bestaande contracten laten dit niet toe/men is tevreden met de huidige situatie (22 x genoemd)
- De capaciteit/snelheid/betrouwbaarheid/ kwaliteit zijn bij open VPN minder (11 x genoemd)
- Open VPN is minder beheersbaar en minder controleerbaar (8 x genoemd)
- Het is geadviseerd door een externe partij (7 x genoemd)
- Het is een eis van de leverancier of het moederbedrijf om gesloten VPN te gebruiken (5 x genoemd)
- Kosten om over te stappen naar open VPN c.q. de kosten van open VPN zijn te hoog (5 x genoemd)

De onvoldoende veiligheid van een open VPN is de belangrijkste reden om een overstap naar open VPN niet te overwegen. Een van de respondenten voor wie veiligheid onvoldoende is merkt op dat er te veel gevoelige informatie over de VPN verbinding gaat om een overstap te overwegen. Anderen noemen de gegarandeerde veiligheid bij gesloten VPN en de vertrouwelijkheid van data als reden om de overstap niet te overwegen.

Overweging om met een deel van de organisatie over te stappen naar open VPN

Aan de respondenten die niet overwegen om met de gehele organisatie over te stappen op open VPN of dat niet weten of niet willen zeggen, is gevraagd of zij overwegen om met een deel van de organisatie over te stappen naar open VPN. Van deze groep gaf 90% aan dat niet te overwegen. 8% zou dat wel overwegen.

90% stapt ook niet met een deel over

tabel 8 Mate waarin de respondenten met een deel van de organisatie zouden overstappen van gesloten VPN naar open VPN, aantal respondenten in procenten van het aantal respondenten dat niet voor de gehele organisatie overweegt over te stappen (n=190)

<i>Overstappen overwogen</i>	<i>%</i>
Ja	8%
Nee	90%
Weet niet/wil niet zeggen	2%
Totaal	100%

Bron: Panteia, 2017.

Als een overstap naar open VPN voor een deel van de organisatie wordt overwogen wordt genoemd dat dat voor een deel van de toepassingen zou kunnen of nu al gebeurt. Voorbeelden zijn telefonie en e-mail. Niet alles hoeft in dezelfde mate beveiligd te worden. Een van de respondenten noemt dat hij een mix maakt op basis van kosten en veiligheid. Verder noemt een respondent dat een gedeeltelijke overstap overwogen afhangt van hoe belangrijk het verkeer is voor het operationele proces.

De antwoorden op de vraag waarom respondenten een overstap naar open VPN voor een deel van de organisatie **niet** overwegen kunnen als volgt worden gecategoriseerd (aspecten die tenminste 5 keer zijn genoemd):

- Open VPN is niet veilig genoeg (86 x genoemd)
- Bestaande contracten laten dit niet toe/men is tevreden met de huidige situatie (12 x genoemd)
- Het is geadviseerd door een externe partij (7 x genoemd)
- Open VPN is minder beheersbaar en minder controleerbaar (6 x genoemd)
- Het is een eis van de leverancier of het moederbedrijf om gesloten VPN te gebruiken (6 x genoemd)

Overweging om in de komende drie jaar een mogelijke overstap naar open VPN te kijken

Respondenten die niet overwegen om met de gehele organisatie over te stappen op open VPN of dat niet weten of niet willen zeggen is gevraagd of zij verwachten hier in de komende 3 jaar naar te kijken. Van deze groep gaf 82% aan dit niet te gaan doen. 11% verwacht hier wel in de komende drie jaar naar te kijken. Factoren die hierbij een rol gaan spelen zijn (in vrijwel gelijke mate) veiligheid, capaciteit en kosten.

82% gaat ook de komende 3 jaar niet naar een open VPN overstap kijken



tabel 9 Mate waarin de respondenten verwachten in de toekomst (tussen nu en 3 jaar) wel naar een mogelijke overstap van gesloten VPN naar open VPN te kijken, aantal respondenten in procenten van het aantal respondenten dat niet voor de gehele organisatie overweegt over te stappen (n=190)

<i>Overstappen overwegen</i>	<i>%</i>
Ja	11%
Nee	82%
Weet niet/wil niet zeggen	7%
Totaal	100%

Bron: Panteia, 2017.

2.7 Kosten

Inzicht in de kosten
is beperkt

Huidige kosten per maand voor de gesloten VPN

Aan de respondenten is gevraagd wat zij per maand betalen voor hun gesloten VPN. 77% van de respondenten wist dit niet of wilde dit niet zeggen. Bij de overige 23% van de respondenten liep het bedrag aanzienlijk uiteen, namelijk van nul euro tot 25.000 euro. Dit kan te maken hebben met bedrijfsgrootte, aantal vestigingen en aard en gebruik van de gesloten VPN-verbinding. De mediaan was 200 euro.

Besparing bij overstap naar open VPN

Vervolgens is de respondenten gevraagd wat zij denken per maand te besparen wanneer zij met hun gesloten VPN volledig zouden overstappen naar open VPN. In het voorgaande is reeds aangegeven dat weinig respondenten overwegen om over te stappen naar open VPN. Het is dan ook niet verrassend dat 88% van de respondenten geen antwoord kon of wilde geven op de vraag naar een mogelijke besparing. Bij degenen die wel een antwoord gaven gaf 55% aan geen besparing te verwachten en bij de andere antwoorden varieerde het bedrag van 50 tot 7.000 euro.

3 Conclusies

Met de resultaten van de telefonische enquête onder zakelijke gebruikers van gesloten VPN kan een oordeel worden gegeven over de mate waarin open VPN een alternatief is voor gesloten VPN. Uit de resultaten kunnen de volgende conclusies worden getrokken:

- **Gesloten VPN's worden** vooral gebruikt voor data (96%), e-mail (77%) en beveiliging (69%).
- De veruit belangrijkste reden voor het gebruik van een gesloten VPN in plaats van een open VPN is veiligheid.
- Een beperkt deel van de respondenten had voor de gesloten VPN een huurlijn (7%) of een open VPN (7%). De belangrijkste reden om over te stappen van een open VPN naar een gesloten VPN was veiligheid.
- Voor de verschillende toepassingen wordt open VPN slechts in beperkte mate gezien als een alternatief voor gesloten VPN, vooral voor beveiliging (8%) en voor data (14%).
- De belangrijkste reden om open VPN niet te zien als alternatief voor gesloten VPN is voor vrijwel alle toepassingen de veiligheid. Alleen bij video conferencing is de belangrijkste reden de up- en download capaciteit.
- Respondenten overwegen slechts in beperkte mate om met een gesloten VPN over te stappen naar een open VPN. De belangrijkste reden om dit niet te overwegen is wederom veiligheid.
- Respondenten hebben weinig zicht op de kosten van de gesloten VPN en eventuele besparingen bij een overstap naar open VPN. Kosten zijn kennelijk niet het belangrijkste issue bij de keuze tussen gesloten en open VPN.
- Overall kan worden geconcludeerd dat het veiligheidsaspect de reden is dat open VPN over het algemeen niet gezien wordt als substituuat voor gesloten VPN.

