Vervanging Remote Access voorziening KSE

Afstudeerscriptie

Farhaz Hofman
Studentnummer: 2165204

Bestand	:	Afstudeerscriptie - Vervanging Remote Access voorzieningen KSE - Farhaz Hofman.docx
Versie	:	4
Opgesteld door	:	Farhaz Hofman
Studentnummer Fontys:		2165204
Aantal pagina's	:	27

VOORWOORD

Dit document is het resultaat van mijn afstudeerproject bij KSE Process Technology B.V. Een project waarbij een hoop aspecten van mijn opleiding bij elkaar zijn gekomen.

Het project dat ik bij KSE mocht uitvoeren bestond uit het zoeken naar een alternatief voor de huidige remote access faciliteiten. Naast het onderzoek voor de pakketkeuze, ben ik ook nagegaan op wat voor manier de gebruikers tegen de huidige faciliteiten aankijken. De resultaten hiervan waren enigszins verrassend.

Graag zou ik mijn bedrijfsbegeleider Dirk Lubbers willen bedanken voor de ondersteuning en feedback tijdens het project. Ook mijn docentbegeleider Casper Schellekens wil ik bedanken voor de ondersteuning tijdens het project. Daarnaast wil ik mijn vaste projectgroep van de afgelopen jaren, John, Jeroen, Remy en Ransley, bedanken voor de tussentijdse controle en de mogelijkheid tot brainstormen over de gekste dingen. Verder wil ik mijn ouders, Bas en Hawan, en mijn vrienden bedanken voor het hebben van geduld de afgelopen jaren. Een speciaal bedankje voor Esther en Julia die geholpen hebben om mijn teksten enigszins leesbaar te houden.

Farhaz Hofman
Augustus 2015

SAMENVATTING

KSE Process Technology B.V. is een familiebedrijf gevestigd in Bladel dat productie-automatiseringssystemen en wegers produceert voor de diervoerindustrie. De klanten zijn steeds verder over de grens te vinden. Tevens gaan steeds meer klanten over op een 24/7-productieschema. Daarom is het nodig dat medewerkers van KSE te allen tijde verbinding kunnen maken met het bedrijfsnetwerk van KSE.
De huidige oplossing voor remote access is een IPsec oplossing van FortiNet. De IT afdeling constateerde echter toenemende problemen met deze client. Daarnaast worden de IPsec poorten steeds vaker geblokkeerd op hotspot locaties zoals vliegvelden en hotels. Vandaar dat er de vraag lag te zoeken naar een nieuwe oplossing op basis van SSL VPN.

Een onderzoek is gestart onder de gebruikers om in beeld te krijgen welke problemen de eindgebruikers ondervinden. Dit is gedaan met behulp van een enquête. Uit de organisatie kwamen geluiden dat de gebruikers veel problemen ondervonden met de FortiNet oplossing. Dit was terug te vinden in de enquêteresultaten.
Na de enquête volgde een interview met de manager van IT, waarin bepaald is wat de knelpunten zijn vanuit de ogen van IT en wat de wensenlijst is. Deze zijn vervolgens samengevoegd om tot een lijst van requirements te komen.

Aan de hand van de lijst met requirements is een shortlist van firewall leveranciers opgesteld. Er is bekeken wat de leveranciers te bieden hebben, en er zijn in samenwerking met de partners van de leveranciers keuzes gemaakt voor eventuele oplossingen. Hierna is per oplossing bekeken hoe goed deze scoorde ten opzichte van de lijst met requirements.

Uit het hele proces is naar voren gekomen dat zowel de FortiNet als de Pulse Secure oplossing goed aansluiten op de wensen van KSE. Echter het uitgebrachte advies is om verder te gaan met Pulse Secure, omdat deze qua functionaliteit toch het meeste heeft te bieden.

Voor de twee-staps-verificatie gaat mijn advies uit naar SecurAccess. Hoewel SecurAccess de meest prijzige oplossing is, is het wel een flexibele oplossing. Vooral de ondersteuning voor de vele platformen en de self-service website voor de eindgebruiker is zeer positief.

Op het moment van schrijven is het advies nog niet geaccepteerd. Hier zal in de loop van september 2015 uitsluitsel over komen. Tot de definitieve goedkeuring is gegeven, is er een voorstel implementatieplan gemaakt.

SUMMARY

KSE Process Technology B.V. is a family-run business located in Bladel, which produces weighers and production-automation systems for the feed industry. The customers are to be found increasingly further beyond the border. Additionally, more customers are switching to a 24/7-production schedule. These developments resulted in the need for KSE employees to be able to connect to KSE's company network at any given time.

The current remote access solution is an IPsec solution from FortiNet. The IT department noticed increasing problems with it, such as the instability of the client. Moreover, the ports used for IPsec are increasingly blocked at hotspot locations such as airports and hotels. Which resulted in the request to check out new solutions based on SSL VPN.

To start we needed to find out which problems the end-users are experiencing. This was done using a survey. Information from inside the organization suggested that many employees had problems with the FortiNet solutions. However, this information could not be found in the survey results. Following, an interview with the IT manager ensued, to specify what the problems are from an IT standpoint. The requirements from the IT department were collected as well. All this information was combined to create the list of requirements.

With the list of requirements established, a shortlist of firewall vendors was drafted. It was checked what solution the vendors had on offer and together with a few partners a solid choice was made for a possible solution from the vendors. Following, each solution was viewed to see how well it scored compared to our list of requirements.

The whole process has revealed that both FortiNet's and Pulse Secure's solution measure well against the wishes of KSE. However, the overall advice did go to the Pulse Secure solution as it has the most to offer in terms of functionality.

My advice for a two-factor authentication solution is SecurAccess. Although SecurAccess is the most expensive solution, it is quite flexible. Especially the wide support for different platforms and self-service website for the user is positive feature.

At the time of writing, the advice has not yet been accepted. During the course of September 2015, a definitive answer is expected. Until the final approval has been given, a proposal for an implementation plan has been created.

INHOUDSOPGAVE

1. INLEIDING

KSE Process Technology B.V. levert automatiseringssystemen en weegsystemen voor de diervoerindustrie. Door de toenemende 24/7-productie van diervoer en de toename van internationale klanten is er steeds meer behoefte buiten kantoortijden te werken.

De ICT afdeling van KSE heeft hiervoor een remote access oplossing in gebruik van FortiNet. De laatste jaren waren er steeds meer problemen met deze oplossing, voornamelijk met de clientsoftware. Vandaar dat er vanuit KSE de opdracht kwam te zoeken naar een nieuwe oplossing voor de remote access faciliteiten.

In hoofdstuk 5 is het resultaat terug te vinden van een onderzoek dat gehouden is onder de gebruikers om vast te stellen wat de problemen waren die de gebruikers ondervonden. In hoofdstuk 6 is te lezen wat het resultaat is van de gedane pakketselectie, het advies dat hieruit volgde. Tot slot bevat hoofdstuk 7 een conclusie en aanbevelingen.

2. Het Bedrijf

KSE Process Technology B.V. is een familiebedrijf dat zich bezig houdt met de productie van specialistische wegers voor de korrel- en poederverwerkende industrie. Ook houdt het zich bezig met de automatisering van fabrieken in de feed- en premixindustrie.

Enkele grote klanten van KSE zijn:

- De Heus
- Fransen Gerrits
- Nutreco
- Cargill
- Aveve
- Felleskjøpet

2.1. Geschiedenis

KSE is een familiebedrijf dat is opgericht in 1973 te Hapert. Het is begonnen als elektrotechnisch installatiebedrijf dat voornamelijk opereerde in de kas- en stalindustrie. In 1993 werd KSE marktleider op het gebied van automatisering in de diervoerderindustrie in Nederland en België. Alfra Doseer- en Weegsystemen B.V. werd in 1997 geacquireerd. Dit was ook de start van de internationalisering van KSE. In 1999 verhuisde KSE van Hapert naar een nieuw pand in Bladel dat gebouwd is naast de fabriek van ALFRA. In 2009 werd KSE failliet verklaard, maar heeft het een doorstart kunnen maken onder de naam KSE Process Technology B.V.

2.2. Locaties

Sinds 2015 heeft KSE nog maar één kantoorlocatie welke zich bevindt in Bladel. Vanuit Bladel vinden alle activiteiten van KSE plaats. Naast de werknemers in Bladel heeft KSE enkele werknemers die continu op afstand werken. Dit zijn er twee in de Verenigde Staten, twee in Polen en één in Hoorn.

2.3. Producten

KSE heeft 2 productlijnen.

- Automatiseringssoftware PROMAS
- Specialistische wegers voor de korrel en poeder verwerkende industrie welke onder de merknaam ALFRA vallen.

2.4. IT AFDELING

Het departement IT van KSE bestaat uit vier vaste medewerkers:

Dirk Lubbers	IT-Manager
Farhaz Hofman	IT-Specialist
Fons Dolmans	Applicatie Ontwikkelaar
Rob Verberne	Systeembeheerder

Daarnaast heeft KSE ICT regelmatig een stagiaire tot haar beschikking.

Binnen het departement is er een afdeling Informatiemanagement. Deze bestaat uit personen afkomstig van diverse andere departementen binnen de organisatie. De afdeling heeft een adviesgevende en besluitvormende rol met betrekking tot het informatiemanagement binnen KSE.

KSE ICT is verantwoordelijk voor de interne ICT omgeving en heeft een adviserende rol in ICT vraagstukken van de projecten- en servicedivisie.

3. OPDRACHTOMSCHRIJVING

KSE is naast een project- en product- ook een serviceverlenende organisatie. Dit houdt in dat een groot deel van het personeel buiten de reguliere kantooruren om resources van het kantoornetwerk van KSE nodig heeft. Ook kan het netwerk nodig zijn om service te verlenen aan klanten met een storing.

3.1. PROBLEEMSTELLING

Verkopers, projectengineers en service-engineers moeten te allen tijde verbinding kunnen maken met het netwerk van KSE. Verkopers moeten verbinding kunnen maken om mogelijke klanten altijd te kunnen voorzien van de meest recente productinformatie. Projectengineers moeten verbinding kunnen maken om tijdens de projectfase altijd de meest recente klantsituatie te kunnen raadplegen. Daarnaast moeten zij beschikbaar zijn voor nazorg na de inbedrijfstelling. De service engineers verlenen een 24/7-helpdeskdienst voor de klant en moeten daarom ook op elk moment bij de klant kunnen inloggen. Momenteel is hiervoor een op IPsec gebaseerde oplossing van FortiNet beschikbaar.

Op dit moment zijn er enkele knelpunten in de huidige oplossing aan te wijzen, zowel vanuit de beheerkant als de gebruikerskant. Deze worden hieronder toegelicht.

Het gebruik van IPsec heeft als voorwaarde dat poorten 500 en 4500 open staan. Over deze poorten loopt de communicatie voor het opzetten van de IPsec tunnel. De laatste tijd is steeds meer te merken dat op hotspots in hotels en vliegvelden deze poorten gesloten zijn. Dit geeft veel problemen voor verkopers op de baan. Vaak zijn deze ‘gratis’ hotspots alleen beschikbaar omdat ze het mogelijk maken verkeer te analyseren en gebruikers te traceren. Door het gebruik van een VPN wordt het onmogelijk gemaakt om het verkeer te analyseren en lopen de aanbieders inkomsten mis.

De client software van FortiNet, genaamd FortiClient, geeft vaak problemen. Het heeft met regelmaat stabiliteitsproblemen, en het herinstalleren van de client is te vaak nodig. Ook zijn veel systemen merkbaar instabieler geworden na de installatie van de client.
Helaas wil FortiNet per major versie van de client de functionaliteit aanpassen. Het kan per versie verschillen of er een firewall functie, anti-virusscanner of een webfilter aanwezig is. Wij hebben ook al eens meegemaakt dat in een nieuwe versie een component is verwijderd waar wij gebruik van maakten. Hierdoor was het niet mogelijk verbinding te maken met de nieuwe versie. Dit heeft drie minor versies gekost alvorens dit probleem opgelost was.

Door de toename van het gebruik van Apple producten, merkten wij ook dat de vraag naar ondersteuning voor het Apple platform steeg. Voor SSL is er van FortiNet al wel een client met OSX ondersteuning, voor IPsec is dit helaas niet het geval. Dit heeft als gevolg dat alle gebruikers die thuis een Apple computer hebben en verbinding willen maken met het KSE netwerk, dit moeten doen via een Windows virtual machine.

Verder mist KSE ICT de mogelijkheid om te onderzoeken of op de thuissystemen voldoende beschermd zijn tegen virussen en malware. Het is al enkele keren voorgekomen dat virusuitbraken op de productienetwerken van de klant KSE als bron hebben gehad. De interne systemen worden goed gecontroleerd. Dit is op dit moment niet mogelijk voor de systemen van de gebruikers thuis.

3.2. DOELSTELLINGEN

De doelstelling van het project is een advies geven voor een nieuwe oplossing voor de remote access omgeving van KSE. De nieuwe oplossing zal op basis zijn van SSL ten opzichte van de huidige IPsec oplossing. Voor een extra niveau van beveiliging dient de nieuwe oplossing gecombineerd te worden met een twee-staps-verificatiemethode. Tevens zal voor de nieuwe oplossing een implementatieplan opgesteld worden.

3.3. AANPAK VAN DE OPDRACHT

Het project is volgens de V2 methode uitgevoerd. Dit houdt in dat er bepaalde stappen ondernomen moeten worden, en dat de bijbehorende documenten opgesteld moeten worden.

- Opstellen van PID
- Naderonderzoek (Requirementsanalyse / IST-SOLL)
- Advies (Pakketselectie)
- Implementatieplan opstellen

3.4. GEBRUIKTE METHODEN

Voor het managen van het project is de V2 methode van Fontys aangehouden. Deze projectmethodiek is de afgelopen jaren als standaard gebruikt bij de uitgevoerde projecten tijdens de opleiding.
De V2 methode is door Fontys in het begin van de jaren 90 ontwikkeld. Het is het resultaat van een post-HBO cursus Kwaliteitskunde. Het is een methode die is toegespitst op verbetertrajecten. Geduurde de jaren is V2 methode bijgewerkt zodat het nog altijd mee kan in de voortduurde evolutie van de ICT.
(Vleugel, 2009)

De MoSCoW methode is gebruikt om de prioriteiten van de requirements te bepalen. Bij deze methode worden de requirements in vier verschillende prioriteitsgroepen verdeeld. De methode heeft geen banden met de stad in Rusland, maar de naam MoSCoW vormt een ezelsbruggetje voor de eerste letter van de prioriteitsgroepen:

- Must have
    - Requirements die verplicht aanwezig moeten zijn.
- Should have
    - Requirements die zeer gewenst zijn.
- Could have
    - Requirement die gewenst zijn.
- Won't have
    - Ook wel eens Would like. Requirements die gewenst zijn, maar die geen (speciale) aandacht zullen krijgen.

(Wikipedia, 2015)

4. Remote Access

Remote access is tegenwoordig niet meer weg te denken uit het bedrijfsleven. Ook is steeds meer te zien dat mensen het gebruiken voor hun privé-omgeving.
In het bedrijfsleven is het tegenwoordig eigenlijk onmisbaar. Vooral omdat steeds meer bedrijven naar 'het nieuwe werken' overgaan. Iets wat stimuleert niet volgens het 9-to-5 principe te werken, maar de werknemer hun eigen dag in te laten delen. En zelfs een groot deel te laten werken vanuit huis. Dit is alleen mogelijk als de werknemer de mogelijkheid heeft om vanuit een niet-kantoor omgeving verbinding te kunnen maken met het bedrijfsnetwerk.
Ook gaan productiebedrijven steeds meer naar een 24/7-productieschema, waardoor van de dienstverleners vaak ook verwacht worden om bij problemen 24/7-ondersteuning te leveren.

4.1. Manieren van Remote Access

De traditionele manier van remote access is het opzetten van een VPN verbinding. Dit houdt in dat vanaf een client systeem met behulp van een stukje software een beveiligde verbinding wordt opgezet naar een firewall die verbonden is met het privé-netwerk. Hierbij word vaak gebruik gemaakt van de PPTP en L2TP protocollen. Tegenwoordig wordt het gebruik van PPTP afgeraden omdat deze niet meer als veilig beschouwd word (Microsoft Security TechCenter, 2012). Toch worden ze nog veel gebruikt. Dit heeft als reden dat alle besturingssystemen standaard deze twee protocollen ondersteunen, waardoor het niet nodig is extra software te installeren om een verbinding te realiseren.
De huidige standaarden die als veilig beschouwd worden zijn IPsec en SSL VPN (Microsoft Technet, 2015). IPsec en SSL VPN zullen in de volgende paragraaf toegelicht worden.
Op dit moment is er een sterke opkomst van cloudbased remote access oplossingen, zoals Teamviewer en LogMeIn. Deze oplossingen zijn populair omdat het enige wat ze nodig hebben een verbinding naar het internet over poort 80 is. Dit betreft de standaard HTTP-poort. Daardoor kan de software door vrijwel alle firewalls heen die geen deep packet inspection doen. Dit werkt doordat de software een verbinding maakt naar een centrale server. De gebruiker maakt dan vervolgens ook verbinding met de centrale dienst. Deze dienst zorgt ervoor dat er een remote sessie opgezet wordt tussen het werkstation en de gebruiker.

4.2. IPsec VPN vs SSL VPN

In onderstaande sectie wordt belicht wat de meest kenmerkende verschillen zijn tussen IPsec en SSL VPN.

4.2.1. Verbinding maken

IPsec heeft vaak per leverancier eigen clientsoftware, er dient daarom altijd een extra stukje software te worden geïnstalleerd voordat er een beveiligde verbinding gemaakt kan worden.
SSL VPN werkt via een browser. Er is een web portal beschikbaar waarop ingelogd kan worden. Vanuit daar kunnen enkele applicaties beschikbaar gesteld worden.

4.2.2. Authenticatie

Bij het opzetten van de IPsec tunnel heb je naast de username en password ook de pre-shared key of een clientcertificaat nodig. Deze is vaak alleen intern bij het bedrijf te bemachtigen, waardoor het voor buitenstaanders moeilijker wordt om poging tot authenticatie te doen. Bij SSL VPN is dit niet aanwezig. Alleen een username en password kan voldoende zijn. Om deze reden wordt SSL VPN vaak gecombineerd met een one-time password twee-staps verificatie. Dit zorgt ervoor dat na het inloggen ook een code moet worden ingegeven die alleen ontvangen kan worden door de echte eigenaar van de username en password. Dit voorkomt dat iemand anders de credentials van een ander kan gebruiken.

4.2.3. Poorten

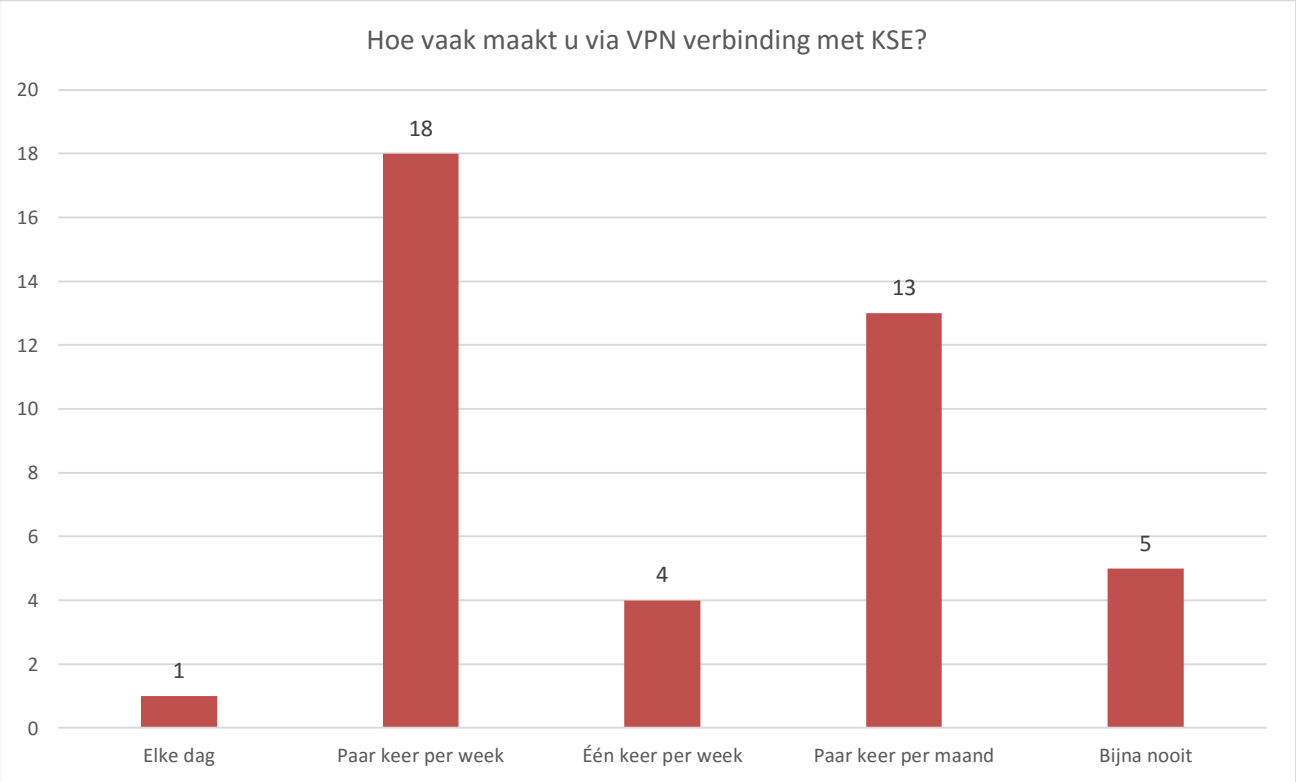
IPsec werkt standaard op poort 50, 51, 500 en 4500. SSL VPN werkt op poort 443; de HTTPS-poort. Steeds vaker worden op openbare hotspots of hotel wifi alleen de poorten voor web- en emailverkeer doorgelaten. Dit geeft gebruikers met een IPsec VPN veel hinder, omdat het dan niet mogelijk is om een beveiligde verbinding op te kunnen zetten met het bedrijfsnetwerk. Omdat SSL VPN over de standaard HTTPS poort werkt, is het bijna altijd mogelijk om via die openbare en hotel hotspots een veilige verbinding op te zetten.

5. VOORONDERZOEK

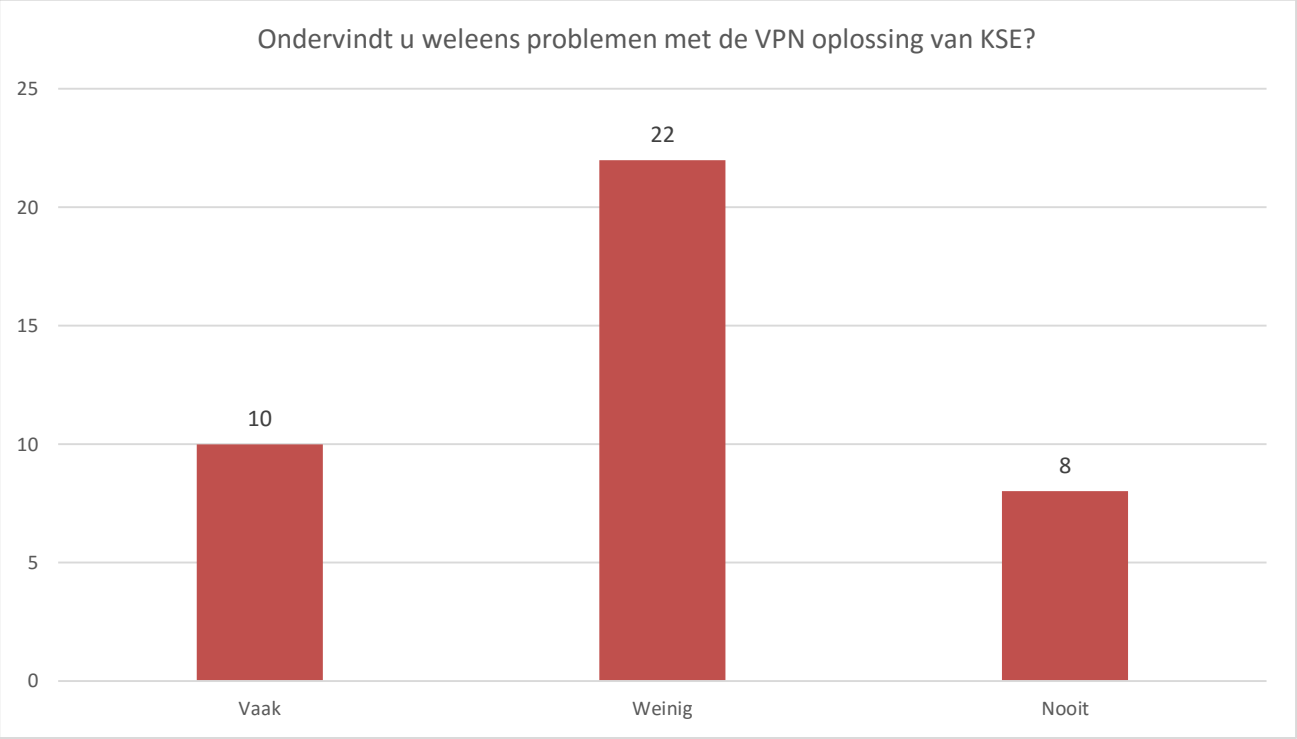
5.1. GEBRUIKERSENQUÊTE

Om duidelijk in beeld te krijgen wat de medewerkers van KSE denken over de huidige oplossing, is onder een selecte groep medewerkers van KSE een enquête gehouden om te achterhalen wat de mening is van de gebruikers over de huidige oplossing. De selectie is gedaan op basis van lidmaatschap van de rechtengroep die toestemming heeft via VPN verbinding te maken. Ook zijn er vragen gesteld om te achterhalen of er eventuele wensen of aandachtspunten zijn. Op de enquête hebben 45 mensen gereageerd.

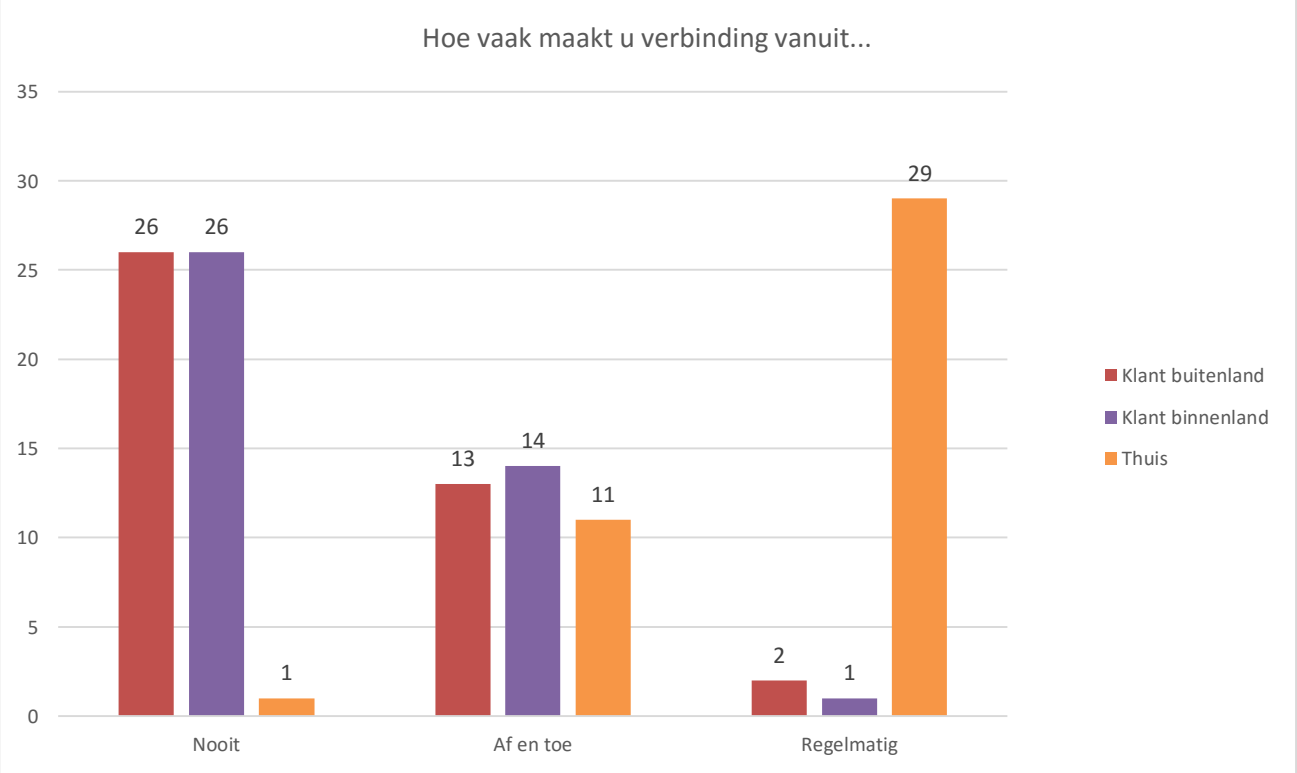
Hier volgen enkele grafische weergaves van de gegeven antwoorden met een korte toelichting.



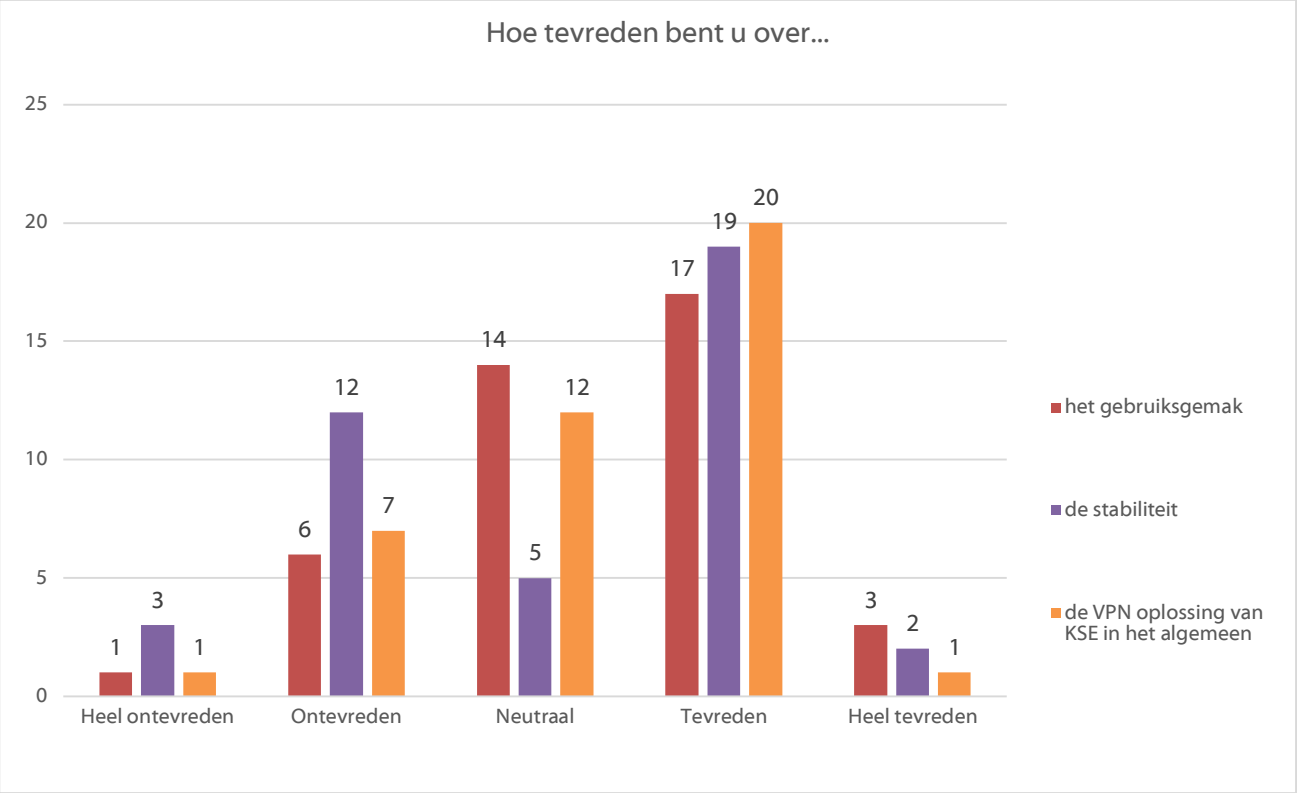
Van de medewerkers die over de rechten beschikken om een VPN verbinding te maken blijkt het grotendeel hier regelmatig gebruik van te maken.



In tegenstelling tot de verwachting van ICT, blijken de medewerkers minder problemen te ondervinden met de VPN oplossing van KSE.



Deze vraag is gesteld om de individuele antwoorden te kunnen valideren. Het kan bijvoorbeeld zo zijn dat een medewerker meldt dat hij of zij veel problemen ondervindt van de VPN verbinding, en tegelijkertijd veel verbinding maakt vanuit het buitenland. De problemen zullen in dit geval veroorzaakt worden door de hoge latency van de verbinding, in plaats van de software of de FortiGate oplossing in zijn geheel.



Een klein deel van de ondervraagden meldt problemen met de stabiliteit, maar over het geheel gekeken zijn de gebruikers tevreden.

Tot slot zijn er nog enkele open vragen gesteld waarbij de medewerkers hun mening konden geven over de huidige oplossing en eventuele wensen voor de nieuwe oplossing kenbaar konden maken. Daar zijn de volgende punten uitgekomen:

5.1.1. Wat zijn veel gemelde problemen?

- Geen verbinding op kunnen zetten.
- Verbinding valt vaak uit.
- Client geeft veel problemen; systeem instabiliteit, vervelende updater et cetera.

5.1.2. Wat zien de medewerkers graag verbeterd?

- Ondersteuning voor Apple OSX
- Split-tunneling (toegang tot KSE netwerk en gelijktijdig het thuisnetwerk)

5.1.3. Wat vinden de medewerkers het belangrijkst?

- Stabiliteit

De indruk vanuit de IT-afdeling was dat mensen erg ontevreden waren over de huidige oplossing. Uit de enquête blijkt echter dat dit niet het geval is. De problemen die het meest genoemd worden waren al bekend bij IT. De opmerkingen die uit de enquête zijn gekomen, zijn opgenomen in de requirements.

5.2. EERSTE VENDOR SELECTIE (SHORTLIST)

Voor de eerste vendor keuze moet een selectie gemaakt worden uit de tientallen leveranciers van VPN remote access oplossingen. Een exotische oplossing is uitgesloten volgens de requirements. Zodoende is uitgezocht wat de grootste of beste leveranciers van firewall producten zijn.
Op basis van de Gartner chart van 2015 (Adam Hils, 2015) is de volgende lijst van leveranciers opgesteld:

- CheckPoint
- Cisco
- FortiNet
- SonicWall
- Palo Alto
- Pulse Secure (voorheen Juniper Pulse)

De lijst opgesteld op basis van de hoogste scorende oplossingen. Omdat er ook de wens is voor een niet-exotische oplossing is door ICT bekeken wat voor hun bekende leveranciers zijn. Om deze reden is Intel/McAfee niet opgenomen in de shortlist. SonicWall/Dell is daarvoor in de plaats gekomen, mede omdat Dell de vaste leverancier is van laptops, desktop en servers bij KSE.

6. VENDOR- EN OPLOSSINGSELECTIE

6.1. REQUIREMENTS

Na overleg met Dirk Lubbers (Manager IT) is een lijst met requirements voor de nieuwe oplossing tot stand gekomen. Tevens is er onder de eindgebruikers een enquête gehouden om te onderzoeken wat de wensen zijn vanuit de organisatie.
Vanuit productmanagement is gevraagd te kijken welke mogelijkheden de client biedt tot gescript een VPN tot stand te brengen. Deze vraag is ontstaan door de wens om de machinebesturingen te voorzien van een dial home functie ten behoeve van remote troubleshooting.

Na het opstellen van deze lijst is volgens de MoSCoW methode bepaald welke waarde de eisen hebben. Daar is de volgende tabel uit voortgekomen.

Nr.	Requirement	Must	Should	Could	Won't
1	Functioneren op Windows	X			
2	Functioneren op OSX	X			
3	Functioneren op Linux				X
4	Ondersteuning voor 2FA	X			
5	Uitgebreide monitoring/rapportage	X			
6	Authenticatie op basis van AD	X			
7	Stabiele oplossing	X			
8	Low footprint client	X			
9	Client compliance[1]	X			
10	Goede stabiliteit bij hoge latency verbinding	X			
11	Niet gebaseerd op JAVA	X			
12	Self updating client	X			
13	Split tunneling[2]		X		
14	Webbased portal voor end-user	X			
15	Functioneren op Windows Phone		X		
16	Functioneren op Apple iOS		X		
17	Functioneren op Google Android		X		
18	Alerts bij limiet overschrijdingen		X		
19	Mogelijkheid tot aanpassen portal		X		
20	Geen exotische oplossing[3]		X		
21	Vanuit portal aanbieden van RDP			X	
22	Vanuit portal aanbieden van Fileshares			X	
23	Vanuit portal aanbieden van SharePoint			X	
24	Vanuit portal aanbieden van PING			X	
25	(Deels) geautomatiseerd account aanmaken voor leveranciers			X	
26	Client gescript kunnen starten en VPN tunnel starten[4]			X	

[1] De mogelijkheid om te kunnen controleren of een gebruikerssysteem die verbinding wil maken bijvoorbeeld bijgewerkte anti-virus software heeft.
[2] Split tunneling geeft de eindgebruiker de mogelijk gelijktijdig verbonden te zijn met het bedrijfsnetwerk en netwerk waar vanuit de gebruiker een verbinding probeert te maken. Bijvoorbeeld het thuisnetwerk.
[3] Het zou een oplossing moeten zijn die wereldwijd veel gebruikt word. Zodat je bij problemen niet meteen hoeft aan te kloppen bij de leverancier, maar ook de user communities kan raadplegen.
[4] Een wens gekomen van de afdeling productmanagement. Dit geeft de wegersystemen die aan klanten verkocht worden, zonder moeilijke hardware oplossingen, de mogelijkheid zelf een verbinding ten behoeve van serviceverlening op te zetten naar KSE.

De requirements zullen op aanwezigheid beoordeeld worden. Op het moment dat een oplossing over een requirement beschikt, zal het aantal punten toegekend worden.
De puntenbepaling is als volgt:

- Must have: 5 punten
- Should have: 3 punten
- Could have: 2 punten
- Won't have: 1 punt

Aan het einde van de vergelijking zullen de punten opgeteld worden en zal de hoeveelheid punten een goede indicatie geven van wat de best passende oplossing voor KSE is.

6.2. Bekeken VPN oplossingen

6.2.1. CheckPoint

Via een collega ben ik in contact gekomen met een technische consultant van Checkpoint. Deze heeft KSE bezocht om samen te onderzoeken wat de beste oplossing zou kunnen zijn. Tijdens dit bezoek is voorgesteld om te kijken naar de CheckPoint Security Gateway 2200. Van CheckPoint heb ik ook een trial versie van de applicatie gekregen om hands-on de software te kunnen testen.

6.2.2. Cisco

Voor Cisco heeft KSE geen directe partners, daarom heb ik direct contact gezocht met Cisco. Zij hebben mijn verhaal aangehoord en mij medegedeeld dat ze op korte termijn een partner contact op zouden laten nemen met mij. Dit is helaas niet gebeurd. Tijdens het globale vooronderzoek kwam naar voren dat Cisco geen oplossingen had die aansloten op de capaciteit eis van KSE. Oftewel te klein of te groot waardoor de prijs omhoog schoot. Het dochtermerk van Cisco, Meraki, heeft alleen IPsec remote access oplossingen. Dit alles in acht nemend is Cisco direct afvallen als mogelijk oplossing.

6.2.3. FortiNet

KSE heeft FortiNet al in huis als firewall en IPsec VPN oplossing. Ik heb contact gezocht met onze huidige leverancier (Secure Layers) om te onderzoeken wat de mogelijkheden zijn van de SSL-optie op de firewall. Omdat wij onze oude firewall nog in bezit hebben, heb ik zaken kunnen testen zonder de productieomgeving tot last te zijn.

6.2.4. Palo Alto

Voor Palo Alto ben ik in contact gekomen met de leverancier Lantech. Deze zijn ook langs geweest bij KSE voor een productpresentatie. Ik heb jammer genoeg geen technische demo en trial versie van de software mogen ontvangen. Ondanks dit is gekeken naar de PA-200 als mogelijke oplossing voor KSE, omdat deze voldoet aan de requirements gesteld door KSE.

6.2.5. Pulse Secure (voorheen Juniper Pulse)

Voordat ik in de vendor onderzoeksfase van mijn opdracht kwam, heeft Juniper al contact met mij gezocht. WeSecure, partner van Juniper, heeft KSE bezocht voor een uitgebreide technische demonstratie. Aan de hand van de requirements van KSE heeft WeSecure als advies de MAG-2600 gegeven. Ik heb een trial versie van de software ontvangen om hands-on te testen.

6.2.6. SonicWall

SonicWall biedt in hun remote access range van producten geen oplossingen aan op basis van SSL, enkel IPsec. Hierdoor valt SonicWall direct af als mogelijke oplossing.

6.3. Bekeken twee-staps-verificatie oplossingen

Bij FortiNet, Palo Alto en Pulse Secure zijn naast de SSL VPN-oplossing ook twee-staps-verificatie oplossingen aangeboden.

Op technisch vlak zijn de oplossingen op het gebied van de koppeling naar de VPN hetzelfde. De VPN oplossing praat via RADIUS naar de twee-staps-verificatiesoftware, die op zijn beurt een authenticatieverzoek verstuurt naar active directory en daar bovenop een tweede check doet.

De volgende drie oplossingen zijn aangeboden:

6.3.1. FortiAuthenticator van FortiNet

De twee-staps-verificatie oplossing van FortiNet. Deze biedt OTP's aan via een app, SMS of een hardware token. Deze oplossing is aangeboden door SecureLayers.

6.3.2. SecurAccess van SecurEnvoy

SecurAccess is aangeboden door Wesecure als twee-staps-verificatieoplossing. Ook deze biedt OTP's aan via SMS en een app. SecurAccess heeft een selfservice portal voor de eindgebruiker. Hierdoor kan een gebruiker zelf instellen hoe en op welk device hij de code wil ontvangen. Bovendien is er de mogelijkheid tot het uitdraaien van een lijst met codes voor mensen die geen device hebben waarop de code ontvangen kan worden. SecurAccess heeft voor bijna ieder platform een app beschikbaar.

6.3.3. Authasas Advanced Authentication van Authasas

Authasas is aangeboden door Lantech. Helaas heb ik hier geen demo van mogen ontvangen. Authasas onderscheidt zich van de twee andere oplossingen door ondersteuning die geboden wordt voor veel andere authenticatie protocollen. Hierdoor is het een erg breed product. Bovendien zijn er veel zaken te gebruiken als twee-staps-verificatie middel. Naast de gebruikelijke SMS of app zijn ook yubikeys, biometrische devices of USB sticks te gebruiken als verificatie middel. Een groot gemis voor Authasas is het ontbreken van een Windows Phone app. KSE is gestandaardiseerd op Windows Phone. Om deze reden valt Authasas af als mogelijke twee-staps-verificatie oplossing.

6.4. Conclusie

Checkpoint heeft het hoogst gescoord in de vergelijking. Checkpoint is een zeer complete oplossing met veel vooruitstrevende zaken; de manier hoe BYOD wordt benaderd vanuit Checkpoint is bijvoorbeeld vrij uniek. In plaats van bedrijfsresources direct op het device te benaderen, worden deze vanuit een afgesloten app aangeboden aan de eindgebruiker. Een nadeel is dat Checkpoint de duurste oplossing is.

KSE heeft FortiNet al in huis, waardoor de omschakeling naar SSL VPN vrijwel niets kost. Bovendien scoort FortiNet redelijk hoog in de vergelijking. De FortiNet oplossing is een vrij standaard oplossing. Een voordeel wat FortiNet biedt is het direct aanbieden van tunnel-mode in de browser. Dat het een standaard oplossing is, is ook terug te vinden in de lage mogelijkheid van configuratie en personalisatie van de portal en beheeropties.

Palo Alto heeft het laagst gescoord in de vergelijking. Het mist een webportal waarop een overzichtelijke wijze resources aangeboden kunnen worden. Dit is toch iets waar vanuit ICT naar gezocht wordt, om voor onze minder technische werknemers, klanten en leveranciers een positieve gebruikerservaring te garanderen.

Pulse Secure is de marktleider op het gebied van SSL VPN. De webportal is zeer uitgebreid en kan de eindgebruikers veel bieden. De webportal kan met de Meeting functie en filebrowsing ook een oplossing bieden voor het samenwerken met klanten en leveranciers tijdens projecten. Het nadeel van Pulse Secure is dat voor de volledige functionaliteit van de webclient JAVA geïnstalleerd moet worden. Bovendien beschikt het over uitgebreide monitoring. Aan de beheerkant is er een uitgebreide mogelijkheid tot configuratie.

FortiAuthenticator is een basis twee-staps-verificatie oplossing. Ondanks de naam, is FortiAuthenticator geen speciale FortiNet oplossing. FortiAuthenticator is tijdens het begin van het project afgevallen als oplossing, omdat er geen Windows Phone app beschikbaar was. Enkele maanden geleden is deze toch beschikbaar gemaakt.

SecurAccess is na verloop van tijd de duurste oplossing, maar wel de meeste flexibele. Een groot voordeel aan SecurAccess is dat de eindgebruiker zelf controle heeft over hoe de twee-staps-verificatie moet plaatsvinden.

6.4.1. FortiNet vs Pulse Secure

Uit het bovenstaande is te concluderen dat de twee oplossingen die overblijven FortiNet en Pulse Secure zijn. Er zal nu ingegaan worden op wat de doorslaggevende verschillen zijn tussen de twee oplossingen.

6.4.1.1. JAVA

Voor zowel FortiNet als Pulse Secure is JAVA nodig als er gebruikt gemaakt zal worden van de in-browser RDP, VNC of SSH/Telnet clients. Beiden bieden ook een filebrowser aan waarmee fileshares direct vanuit de browser benaderd kunnen worden. FortiNet heeft hiervoor JAVA nodig. Pulse Secure heeft hier geen JAVA voor nodig.

6.4.1.2. Tunnel-mode

Bij FortiNet is tunnel-mode direct beschikbaar vanuit de browser. Pulse Secure installeert een desktop applicatie genaamd Pulse Connect wat zorgt voor een tunnel-mode connectie.
Een tunnel-mode connectie houdt in dat een direct verbinding gemaakt word met het bedrijfsnetwerk. Er kan direct vanuit applicaties verbinding gemaakt worden met diverse diensten, zonder gebruik te maken van browserbased clients.

6.4.1.3. Functionaliteit

Zowel FortiNet als Pulse Secure beschikken over de standaard set functionaliteit. Aan de beheerderskant is FortiNet nogal beperkt in de opties in vergelijking met Pulse Secure.
Bij Pulse Secure kan op een veel dieper niveau geconfigureerd worden wat er voor welke gebruiker beschikbaar is. Hierdoor is betere gebruikerservaring te realiseren op basis van welke medewerker, leverancier of klant er inlogt.
Naast de remote access functionaliteiten biedt Pulse Secure ook een Meeting functie aan, Junos Pulse Collaboration. Dit is een tool om samenwerken met bijvoorbeeld leveranciers en klanten te vergemakkelijken. Op een makkelijke en veilige manier is zeer snel een scherm te delen met de rest van de deelnemers van de meeting. Deze tool kan ook toegepast worden voor remote supportverlening voor medewerkers of klanten.
Voor Exchange webmail biedt Pulse Secure een extra optie, waardoor het mogelijk is dat Pulse Secure de authenticatie afhandelt, inclusief twee-staps-verificatie. Hiermee is de webmail beter beveiligd.

7. Conclusie en Aanbevelingen

7.1. Conclusie

Dit project had als doelstelling het zoeken naar een alternatieve oplossing voor de remote access voorzieningen van KSE Process Technology B.V., welke gebaseerd is op SSL VPN. De te vervangen oplossing is een oplossing gebaseerd op IPsec van FortiNet. De hoofdredenen dat er de vraag ontstaan is om te zoeken naar een alternatieve oplossing waren de probleemgevende client, en dat de IPsec poorten steeds vaker geblokkeerd worden op openbare hotspots.
Door het ondervragen van de medewerkers over hun ervaringen met de FortiNet oplossing kwamen enkele duidelijk in beeld. De wensen waar de medewerkers het meest om vroegen zijn ondersteuning voor een Apple OSX besturingssysteem en betere ondersteuning voor split tunneling. Ondanks de geluiden uit de organisatie, bleken de hoeveelheid problemen die de medewerkers ondervonden mee te vallen.

Na het opstellen van een shortlist die grotendeels gebaseerd is op de "Gartner Magic Quadrant for Enterprise Firewalls" van 2015, is begonnen met het doorlichten van de verschillende oplossingen. Vervolgens is per requirement bekeken of de oplossingen eraan voldoet. Hier is een puntentelling aan gekoppeld.

Checkpoint kwam uit de meting met de hoogste punten, maar was helaas ook de duurste oplossing. De twee opvolgers waren FortiNet en Pulse Secure. FortiNet heeft vrijwel geen extra kosten, omdat KSE deze al in huis heeft. Toch in het advies naar Pulse Secure gegaan, omdat de feature set meer te bieden heeft. Ook buiten de scope van het project om.
Daarnaast is er gekeken naar mogelijke twee-staps-verificatie oplossingen. Hier kwam SecurAccess van SecurEnvoy het beste naar voren, door de goede mogelijkheid van selfservice voor de medewerker en de brede device ondersteuning voor het genereren van de tokens.

De doelstelling was het vinden van een bij KSE passende remote access oplossing, met een bijpassende twee-staps-verificatie methode. Omdat er een compleet advies afgegeven is, is te concluderen dat de doelstelling is bereikt.

7.2. Aanbevelingen

Voor SSL VPN gaat mijn advies uit naar Pulse Secure. De hoge functionaliteit die de webportal kan bieden is een groot pluspunt. Het feit dat het een dedicated remote access appliance is, is gunstig wat betreft de kosten. Hoewel de FortiNet oplossing ook hoog scoort, en vrijwel niets extra kost voor KSE, weegt deze optie mijns inziens niet op tegen de extra mogelijkheden die Pulse Secure biedt.

Pulse Secure biedt namelijk naast de standaard ook een Meeting functie, een filebrowser die geen JAVA nodig heeft, een uitgebreide mogelijkheid van configureren, en uitgebreide monitoring.

KSE ICT is momenteel ook aan het kijken naar het aanbieden van collaboration tools voor de organisatie, om beter samen te kunnen werken met klanten en leveranciers. Pulse Secure kan hier goede opties bieden zoals de Meeting functie en filebrowser. De uitgebreide configuratiemogelijkheden en monitoring aan de beheerkant zijn een pre.

Voor de twee-staps-verificatie gaat mijn advies uit naar SecurAccess. Hoewel SecurAccess de meest prijzige oplossing is, is het wel een flexibele oplossing. Vooral de ondersteuning voor de vele platformen en de self-service website voor de eindgebruiker is zeer positief.

Op het moment van schrijven is het advies nog niet geaccepteerd. Hier zal in de loop van september 2015 uitsluitsel over komen. Tot de definitieve goedkeuring is gegeven, is er een voorstel implementatieplan gemaakt. Deze is terug te vinden als bijlage 6.

8. EVALUATIE

Het is een lange rit geweest. Maar het resultaat is er eindelijk. De doorlooptijd van mijn project ligt ver boven het gemiddelde. De vraag is natuurlijk: heb ik ervan geleerd? Gelukkig is dat antwoord ja. Mijn eigen planning was in het begin veel te algemeen, waardoor de targets te groot waren. Dit had als gevolg dat de planning onoverzichtelijk was en ik niet goed vooruit kon. Na enkele grote targets opgedeeld te hebben in meerdere kleine, was het proces beter te overzien.
Een ander struikelpunt waar ik vaak tegen aangelopen ben, is het feit dat ik mijn project niet genoeg prioriteit gaf. In plaats van bij KSE te werken aan mijn project, ging ik te snel collega's met problemen helpen. Ondanks dat het goed was om deze mensen te hulp te schieten, was het schadelijk voor de progressie van mijn project. Ook de tussenkomst van enkele andere grote projecten hielp niet mee aan de voortgang. Op een gegeven moment ben ik vaker nee gaan zeggen tegen collega's, om zo mijn project niet in gevaar te laten komen. Gelukkig hadden mijn collega's hier begrip voor.

Ondanks bovengenoemde tegenslagen kijk ik met plezier terug naar deze periode. Wat mij veel deugd deed was hoeveel mijn project en studie leefden onder mijn collega's. Elke week waren er altijd een paar mensen die geïnteresseerd waren in de vooruitgang. Dit waren ook vooral de Apple gebruikers, die toch zitten te springen om afscheid te nemen van hun virtuele Windows machines.

De belangrijkste leerpunten die ik meeneem uit dit project:

- Niet bang zijn om gedetailleerd te plannen.
- Omgaan met verkopers is een vak. Hier heb ik weer genoeg oefening in gehad.
- Het is niet erg om af en toe de prioriteit bij jezelf te leggen.

9. BRONNEN

Adam Hils, G. Y. (2015, May 18). *Magic Quadrant for Enterprise Network Firewalls*. Opgehaald van Technology Research | Gartner Inc.: http://www.gartner.com/technology/reprints.do?id=1-2DVI0YW&ct=150422&st=sb&elqaid=1245&elqat=2&elqTrackId=3fde15b81c9b4061864 1ac7bb3b9641f

Microsoft Security TechCenter. (2012, August 20). *Microsoft Security Advisory 2743314 - Unencapsulated MS-CHAP v2 Authentication Could Allow Information Disclosure*. Opgehaald van Microsoft Security TechCenter: https://technet.microsoft.com/library/security/2743314

Microsoft Technet. (2015, July 28). *VPN Tunneling Protocols*. Opgehaald van Microsoft Technet: https://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx

Vleugel, K. (2009). *Het verbeteringsproces volgens de V2-methode* (3.1 ed.). Eindhoven: Fontys Hogescholen.

Wikipedia. (2015, July 24). *IPsec*. Opgehaald van Wikipedia: https://en.wikipedia.org/wiki/IPsec

Wikipedia. (2015, June 27). *Layer 2 Tunneling Protocol*. Opgehaald van Wikipedia: https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

Wikipedia. (2015, July 8). *MoSCoW method*. Opgehaald van Wikipedia: https://en.wikipedia.org/wiki/MoSCoW_method

Wikipedia. (2015, July 25). *Point-to-Point Tunneling Protocol*. Opgehaald van Wikipedia: https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

Wikipedia. (2015, July 16). *Transport Layer Security*. Opgehaald van Wikipedia: https://en.wikipedia.org/wiki/Transport_Layer_Security

10. VERKLARENDE WOORDENLIJST

Begrip	Verklaring
Active Directory	Gebruikers- en computersbeheer software van Microsoft.
Appliance	Een stuk software dat op eigen hardware of virtueel draait met een specifieke functie, zoals bijvoorbeeld een firewall.
Biometrische devices	Apparaten die kunnen scannen op basis van lichaamseigenschappen van de gebruiker. Bijvoorbeeld: irisscanner of vingerafdruklezer.
BYOD	Bring-Your-Own-Device. Een afkorting voor een trend in de IT, waarbij werknemers hun privéapparatuur gebruiken voor hun werk.
Deep packet inspection	Bij deep packet inspection wordt ook naar de inhoud van een IP-pakket gekeken om te achterhalen wat voor verkeer het is. Normaal gebeurt dit op basis van informatie in de header van het IP-pakket.
Dial home functie	Benaming voor de functie waarbij een apparaat zelf een verbinding naar bijvoorbeeld het hoofdkantoor kan leggen, zodra het over een internetverbinding beschikt.
DSL	Direct Subscriber Line. Een technology die het mogelijk maakt om over het koperen telefoonnet een internet verbinding te realiseren met hoge bandbreedte.
Fileshares	Gedeelde netwerkmappen op het bedrijfsnetwerk.
GPRS	General Packet Radio Service. Een techniek die het mogelijk maakt over het mobiele netwerk datapakketten te versturen en ontvangen.
IPsec	Een standaard voor het versleutelen van IP-netwerkverkeer.
JAVA	Een veel gebruikte programmeertaal.
L2TP	Layer 2 Tunneling Protocol. Een nieuwer VPN protocol ontwikkeld door Microsoft en Cisco. Waarbij de technieken van PPTP van Microsoft en L2F (Layer 2 Forwarding) van Cisco zijn gecombineerd. Resulterend is een makkelijke te gebruiker protocol (PPTP), maar wat beschikt over veilige encryptie methodes (L2F).
Latency	Latency is de tijd die zit tussen het moment dat een commando wordt gegeven voor een actie en het moment dat deze wordt uitgevoerd.
MoSCoW	Een methode om eisen in een eisenpakket onder te verdelen in de volgende prioriteiten: Must have, Should have, Could have en Won't have.
OTP	One-Time-Password. Een twee-staps-verificatiemethode waarbij de gebruiker bij het inloggen een tijdelijke code ontvangt die ingevuld moet worden. De code is vaak maar voor korte tijd geldig.
PING	Een netwerkcommando waarbij getest kan worden of de verbinding tussen twee computers actief is.
PPTP	Point to Point Tunneling Protocol. PPTP is een mede door Microsoft ontwikkelde VPN protocol. Word veel gebruikt door adoptie in bijna alle besturingssystemen. Maar tegenwoordig door gebruik van zwakke encryptie niet veilig meer.
RADIUS	Remote Authentication Dial In User Service. Een gestandaardiseerde, platform onafhankelijke methode om gebruikers te verifiëren.
RDP	Remote Desktop Protocol. Een softwarematige oplossing van Microsoft voor het op afstand overnemen van een computer.
Sharepoint	Document management systeem van Microsoft

SMS	Short Messaging Service. Een methode om via het mobiele netwerk korte berichten van maximaal 160 tekens te sturen.
SSL	Een encryptiemethode om internetverkeer te beveiligen.
Twee-staps-verificatie	Een methode die een gebruikersnaam en wachtwoord verifieert, en vervolgens door middel van een tweede verificatie methode checkt of de gebruiker is wie hij zegt dat hij is.
Yubikeys	Een OTP apparaat in de vorm van een USB stick.

11. BIJLAGEN

Bijlage 1 Plan van Aanpak
Bijlage 2 Enquêteverslag
Bijlage 3 Requirements
Bijlage 4 Naderonderzoek (IST-SOLL)
Bijlage 5 Adviesrapport
Bijlage 6 Implementatieplan

Vervanging Remote Access voorzieningen KSE

Bijlage 1: Plan van Aanpak

Bestand	:	0.2 PvA - Vervanging Remote Access voorzieningen KSE.docx
Versie	:	
Datum van uitgifte	:	12-8-2015
Opgesteld door	:	Farhaz Hofman
Aantal pagina's	:	13

KSE Proven Process Technology
ALFRA Dosing & Weighing Technology
PROMAS Future Proof Automation

INHOUDSOPGAVE

1. Het project bij KSE Process Technology B.V.

1.1. KSE Process Technology B.V.

KSE Process Technology B.V. is een familiebedrijf gevestigd in Bladel. Het heeft 1 klein filiaal in Hoorn. En verder nog enkele engineers werkzaam vanuit Polen en de Verenigde Staten.
KSE Process Technology B.V. heeft 2 hoofdbezigheden. Het verzorgd complete productielijn automatiseringen voor voornamelijk mengvoer- en premixfabrieken. Daarnaast heeft KSE Process Technology B.V. ook een productenlijn van wegers voor de korrel en poeder verwerkende industrie. Voor zowel de weger als de automatisering wordt door KSE Process Technology B.V. 24/7 service aangeboden.

De serviceverlening wordt tussen 17:00 - 08:00 en het weekend gedaan door geplande consignatie dienst. Deze werken 99% van de keren vanuit huis.

De service mensen, externe engineers en thuiswerkers maken verbinding via een FortiNet IPsec oplossing.

De VPN client software heeft in het verleden voor veel problemen gezorgd.
O.a.:

- Het heeft een onbeheerde anti-virus module, welke problemen gaf op de fileshares.
- Na updates wilde de VPN connecties niet meer werken.
- Clientsoftware was vaak ook oorzaak voor onstabiele systemen.

Vandaar dat er vanuit de ICT van KSE Process Technology B.V. de vraag is of er betere oplossingen zijn voor KSE Process Technology B.V.
Of dat wellicht de nieuwere versie minder problemen geeft.

1.2. Direct betrokkenen

Farhaz Hofman	ICT Specialist / Project Manager	KSE Process Technology B.V.
Dirk Lubbers	Manager ICT / Opdrachtgever	KSE Process Technology B.V.
Medewerkers KSE	Eindgebruikers	KSE Process Technology B.V.

2. PROBLEEM- EN DOELSTELLINGEN

2.1. PROBLEEMSTELLING

Verkopers, projectengineers en service-engineers moeten te allen tijde verbinding kunnen maken met het netwerk van KSE. Verkopers moeten verbinding kunnen maken om mogelijke klanten altijd te kunnen voorzien van de meest recente productinformatie. Projectengineers moeten verbinding kunnen maken om tijdens de projectfase altijd de meest recente klantsituatie te kunnen raadplegen. Daarnaast moeten zij beschikbaar zijn voor nazorg na de inbedrijfstelling. De service engineers verlenen een 24/7 helpdeskdienst voor de klant en moeten daarom ook op elk moment bij de klant kunnen inloggen. Op dit moment is hiervoor een op IPsec gebaseerde oplossing van FortiNet beschikbaar.

Op dit moment zijn er enkele knelpunten in de huidige oplossing aan te wijzen, zowel vanuit de beheerkant als de gebruikerskant. Deze worden hieronder toegelicht.

Het gebruik van IPsec heeft als voorwaarde dat poorten 500 en 4500 open staan. Over deze poorten loopt de communicatie voor het opzetten van de IPsec tunnel. De laatste tijd is steeds meer te merken dat op hotspots in hotels en vliegvelden deze poorten gesloten zijn. Dit geeft veel problemen voor verkopers op de baan. Vaak zijn deze 'gratis' hotspots alleen beschikbaar omdat ze het mogelijk maken verkeer te analyseren en gebruikers te traceren. Door het gebruik van een VPN wordt het onmogelijk gemaakt om het verkeer te analyseren en lopen de aanbieders inkomsten mis.

De client software van FortiNet, genaamd FortiClient, geeft vaak problemen. Het heeft met regelmaat stabiliteitsproblemen, en het her-installeren van de client is te vaak nodig. Ook zijn veel systemen merkbaar instabieler geworden na de installatie van de client.
Helaas wil FortiNet per major versie van de client de functionaliteit aanpassen. Of er een firewall functie aanwezig is kan per versie verschillen. Net als een anti-virusscanner of een webfilter. Wij hebben ook al eens meegemaakt dat in een nieuwe versie een component is verwijderd waar wij gebruik van maakten. Hierdoor was het niet mogelijk verbinding te maken met de nieuwe versie. Dit heeft drie minor versies gekost alvorens dit probleem opgelost was.

Door de toename van het gebruik van Apple producten, merkten wij ook dat de vraag naar ondersteuning voor het Apple platform steeg. Voor SSL is er van FortiNet al wel een client met OSX ondersteuning. Helaas voor IPsec niet. Dit heeft als gevolg dat alle gebruikers die thuis een Apple computer hebben en verbinding willen maken met het KSE netwerk, dit moeten doen via een Windows virtual machine.

Verder mist KSE IT de mogelijkheid om te onderzoeken of op de thuissystemen voldoende beschermd zijn tegen virussen en malware. Het is al enkele keren voorgekomen dat virusuitbraken op de productienetwerken van de klant KSE als bron hebben gehad. De interne systemen worden goed gecontroleerd. Dit is op dit moment niet mogelijk voor de systemen van de gebruikers thuis.

2.2. DOELSTELLING

De doelstelling van het project is een advies geven voor een nieuwe oplossing voor de remote access omgeving van KSE. De nieuwe oplossing zal op basis zijn van SSL ten opzichte van de huidige IPsec oplossing. Voor een extra niveau van beveiliging dient de nieuwe oplossing gecombineerd te worden met een twee-staps-authenticatie methode. Tevens zal voor de nieuwe oplossing een implementatieplan opgesteld worden.

3. De opdracht

3.1. Opdrachtomschrijving

Het vervangen van de huidige IPsec gebaseerde remote access faciliteiten van KSE Process Technology B.V. met een op SSL gebaseerde oplossing.

3.2. Producteisen

- Gebaseerd op SSL
- Moet te gebruiken zijn op de volgende OS'en: Microsoft Windows en Apple OSX.
- Moet op de volgende mobiele apparaat soorten te gebruiken zijn: Microsoft Windows Phone, Google Android en Apple iOS.
- Gebruik maken van ACL om toegang te bewaken. Dus administratief medewerkers geen toegang geven tot klant netwerken.
- Client software moet te managen zijn en geen negatieve invloed hebben op het clientsysteem.
- User authenticatie koppeling naar Active Directory.

3.3. Eindproduct

Een nieuwe op SSL gebaseerde remote access oplossing die aan bovenstaande eisen voldoet.

3.4. Betrokken partijen

Opdracht gevende organisatie:	KSE Process Technology B.V.
Opdrachtgever:	Dirk Lubbers
Opdracht nemende organisatie:	KSE Process Technology B.V.
Opdrachtnemer:	Farhaz Hofman

4. De projectactiviteiten

- Opstellen requirements lijst
    - Enquête houden onder gebruikers om wensen en punten van aandacht te achterhalen
    - Overleg met Dirk Lubbers voor de requirements vanuit ICT en KSE
- Requirements indelen middels MoSCoW methode
- Bestaande en gewenste situatie beschrijven
- Globaal vendor onderzoek doen.
- Specifiek vendor/oplossing onderzoek doen
- Implementatie plan maken

5. DE PROJECTGRENZEN EN RANDVOORWAARDEN

5.1. PROJECTGRENZEN

Het project zal zich richten op de faciliteiten voor de medewerkers van KSE Process Technology B.V.

Vanuit product management is er de wens om ook te kijken of de nieuwe software gebruikt kan worden in een dail-home opstelling voor de stand-alone computersystemen van de wegers. Het zal meegenomen worden in het onderzoek naar de oplossing, maar zal geen invloed hebben op het eindbesluit.

5.2. VOORWAARDEN VOOR GESLAAGD PROJECT

Het project kan als geslaagd beschouwd worden op het moment dat er een advies is voor een remote access oplossing is die voldoet aan de gestelde requirements.

6. De producten

- Plan van aanpak
- Gebruikers enquête rapport
- Naderonderzoek
- Adviesrapport
- Implementatie plan
- Gebruikers- en beheerdersdocumentatie

7. KWALITEIT

Toegepaste methodes:

- V2 methode voor project doorloop

Hulpmiddelen

- Projectnotities
  - Microsoft OneNote
- Documentatie / rapportage
  - Microsoft Word
- Enquête afname
  - Microsoft SharePoint
- Enquête analyse
  - Microsoft Excel
- Tijdsregistratie
  - N.t.b.

8. De projectorganisatie

8.1. Organisatie

Alle functies binnen de project groep zullen opgenomen worden door de projectleider; Farhaz Hofman.

8.2. Informatie

Communicatie
Door de korte fysieke afstand tussen de opdrachtgever en projectleider, zal overleg plaats vinden wanneer het nodig is. Planning hiervoor is niet direct nodig.

Tijdregistratie
Farhaz Hofman zal een gedetailleerde urenverantwoording bijhouden. En als dit gewenst is, kan dit overgeleverd worden aan de opdrachtgever.

Archivering
Het project zal i.v.m. flexibiliteit als primaire opslag plaats de dropbox van Farhaz Hofman hebben. Na afronding van het project zullen de definitieve versie van de eind- en deelproducten ook het in intranet van KSE Process Technology B.V. geplaatst worden.

9. DE PLANNING

10. KOSTEN/BATEN-OVERZICHT

Een uitgewerkt kosten/baten overzicht zal volgen in het Adviesrapport.

De meeste kosten van de project zullen komen uit:

- Eventueel aanschaf nieuw apparatuur
- Onderhoudscontracten
- Opleiding gebruikers/beheerders

De baten zullen vooral gehaald worden uit:

- Gebruikers zullen beter en vaker verbinding kunnen maken.

11. VERKLARENDE WOORDENLIJST

Begrip	Verklaring
ACL	Access Control List. Een lijst waarin bijgehouden wel gebruiker of gebruikersgroep toegang heeft tot bepaalde functies, folder of bestanden.
Apple iOS	Het mobiele OS van Apple
Apple OSX	Het desktop OS van Apple
Dail-home opstelling	Een software opstelling met als functie zodra het een verbinding heeft naar het internet, een VPN connectie kan opzetten naar het “home” netwerk
Dropbox	Een cloudbased file opslag dienst
Google Android	Het mobiele OS van Google
IPsec	Internet Protocol Security. Een encryptie standaard voor netwerk verkeer. IPsec encryptie vindt plaats op layer 3 van het OSI model
Microsoft Windows	Het desktop OS van Microsoft
Microsoft Windows Phone	Het mobiele OS van Microsoft
OS	Operating System. Besturingssysteem. Een programma dat zorgt voor de aansturing van de hardware, waardoor een gebruiker optimaal andere programma’s kan uitvoeren.
SSL	Secure Sockets Layer. Een encryptie standaard voor netwerk verkeer. SSL encryptie vindt plaats op layer 4 van het OSI model
VPN	Virtual Private Network. Een technologie om over een publiek netwerk een beveiligde verbinding op te zetten naar een privé- of bedrijfsnetwerk.

Vervanging Remote Access voorzieningen KSE

Bijlage 2: Enquêteverslag

Resultaten van enquête gehouden onder de werknemers van KSE.

Bestand	:	1.1 Enqueteverslag - Vervanging Remote Access voorzieningen KSE.docx
Versie	:	
Datum van uitgifte	:	12-8-2015
Opgesteld door	:	Farhaz Hofman
Aantal pagina's	:	13

INHOUDSOPGAVE

1. INLEIDING

Om duidelijk in beeld te krijgen wat de medewerkers van KSE Process Technology B.V. denken over de huidige oplossing, is er een enquête gehouden onder een selecte groep. Ook zijn er vragen gesteld om te achterhalen of er eventueel wensen of aandachtspunten zijn.

2. DE ENQUÊTE

De enquête is niet onder alle medewerkers van KSE Process Technology B.V. verspreid. Enkel de medewerkers die rechten hebben om via VPN verbinding te making met KSE hebben de enquête ontvangen.

De enquête bestond uit de volgende vragen:

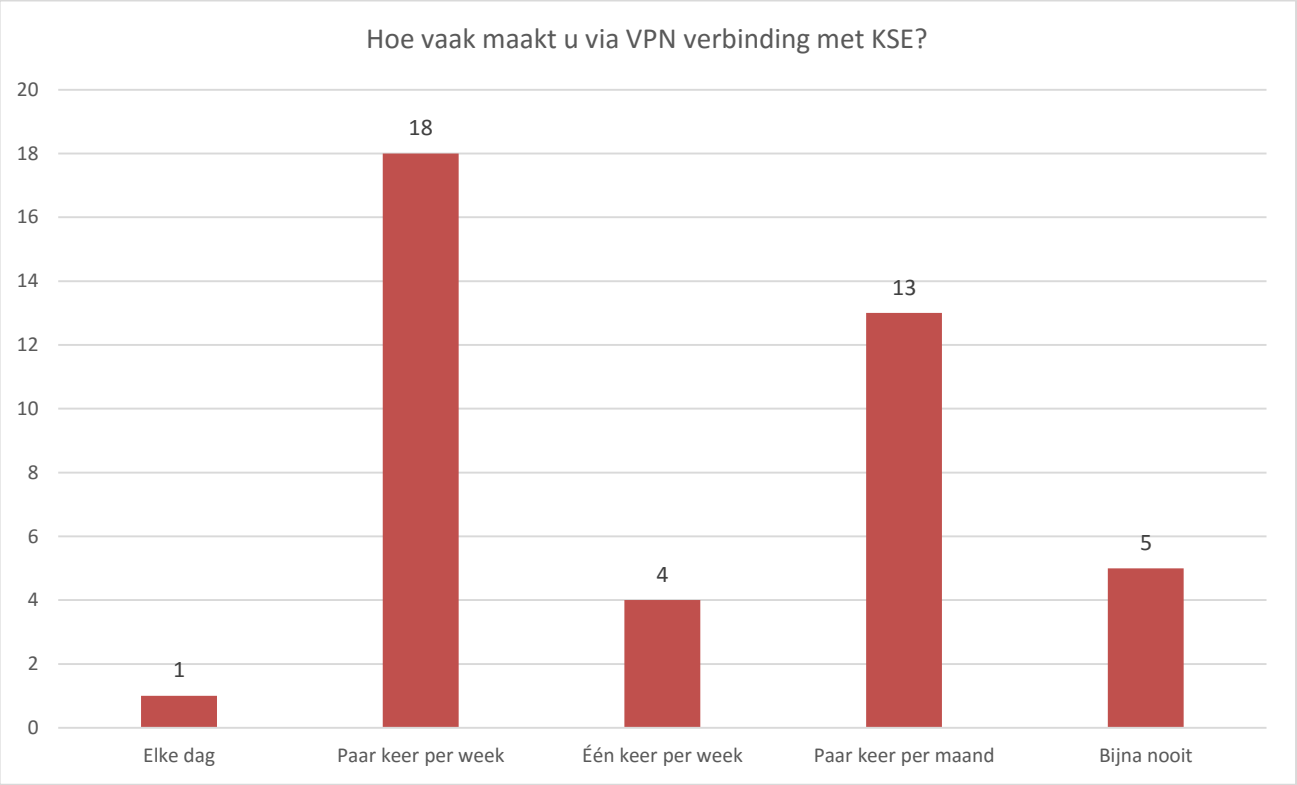
1. Hoe tevreden bent u over de VPN oplossing van KSE in het algemeen?
    a. Heel ontevreden
    b. Ontevreden
    c. Neutraal
    d. Tevreden
    e. Heel tevreden
2. Hoe tevreden bent u over de stabiliteit?
    a. Heel ontevreden
    b. Ontevreden
    c. Neutraal
    d. Tevreden
    e. Heel tevreden
3. Hoe tevreden bent u over het gebruiksgemak?
    a. Heel ontevreden
    b. Ontevreden
    c. Neutraal
    d. Tevreden
    e. Heel tevreden
4. Hoe vaak maakt u via VPN verbinding met KSE?
    a. Elke dag
    b. Paar keer per week
    c. Één keer per week
    d. Paar keer per maand
    e. Bijna nooit
    f. Nooit
5. Vanuit waar maakt u weleens verbinding?
    a. Thuis
        i. Nooit
        ii. Af en toe
        iii. Regelmatig
    b. Klant (Binnenland)
        i. Nooit
        ii. Af en toe
        iii. Regelmatig
    c. Klant (Buitenland)
        i. Nooit
        ii. Af en toe
        iii. Regelmatig
6. Ondervindt u weleens problemen met de VPN oplossing van KSE?
    a. Altijd
    b. Vaak
    c. Weinig
    d. Nooit
7. Indien u weleens problemen ondervindt, kan u deze dan beschrijven?
    a. [OPEN]
8. Wat vind u het belangrijkste voor een goede VPN verbinding?
    a. [OPEN]
9. Zijn er dingen die u verbeterd zou willen zien aan de huidige VPN oplossing van KSE?
    a. [OPEN]
10. Heeft u verder nog op- en/of aanmerkingen over de huidige VPN oplossing van KSE?
    a. [OPEN]

Antwoorden van medewerkers die bij vraag 6 “Nooit” hebben geantwoord zijn verwijderd uit de resultatenset. Dit was dan ook een controle vraag. Hiermee konden antwoorden eruit gehaald worden van mensen die toch geen ervaring hebben met de VPN en dus ook geen goede mening kunnen vormen erover. Twee medewerkers gaven dit antwoord.

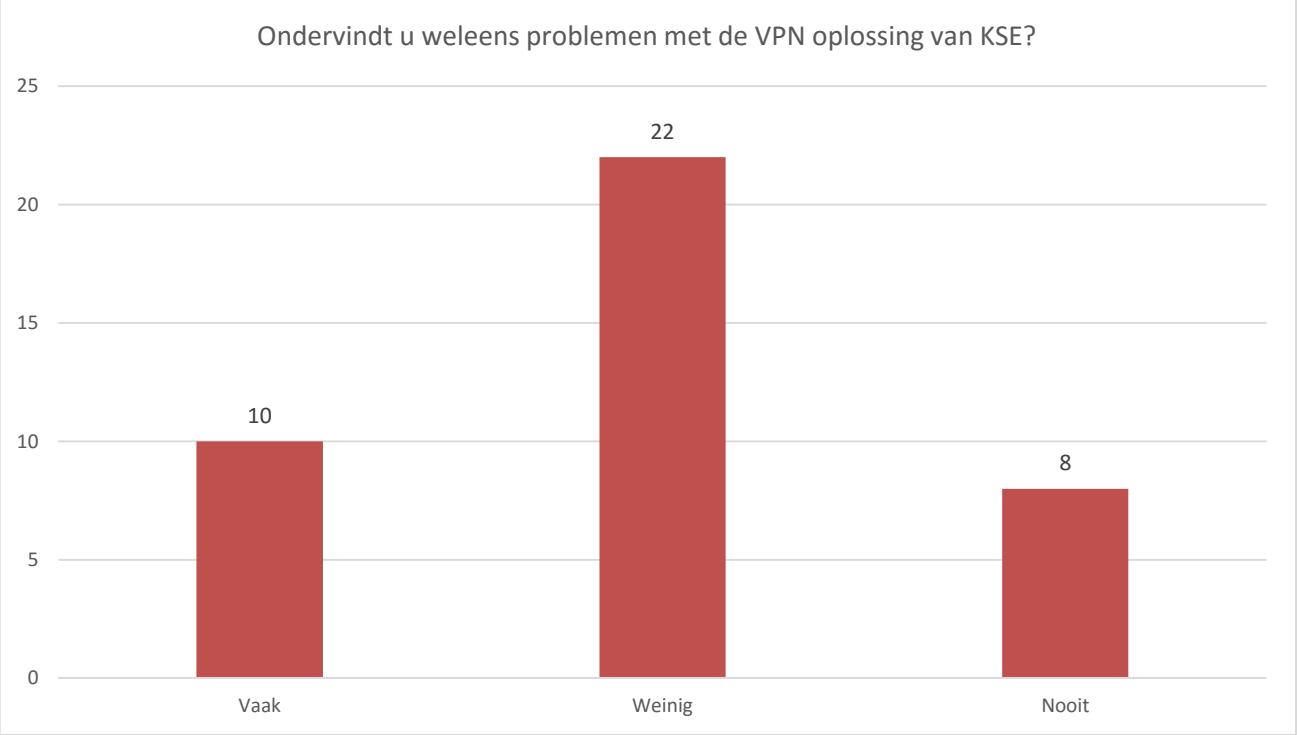
Één andere reactie is verwijderd omdat de medewerker in kwestie alles zeer negatief beoordeelde, en vervolgens bij vraag 10 meldde dat hij pas kort bij KSE werkt en daarom nooit verbinding maakt met VPN.

3. De resultaten

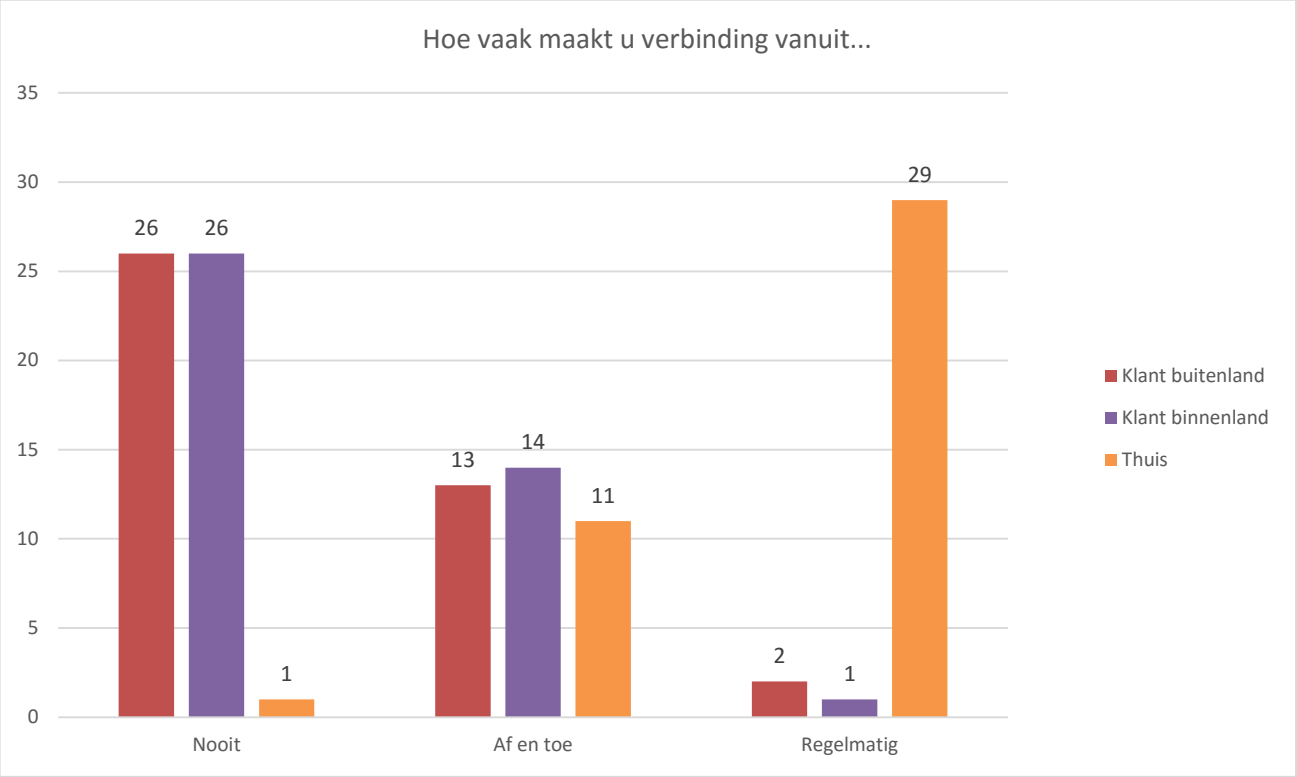
3.1. Multiple choice vragen grafisch weergegeven



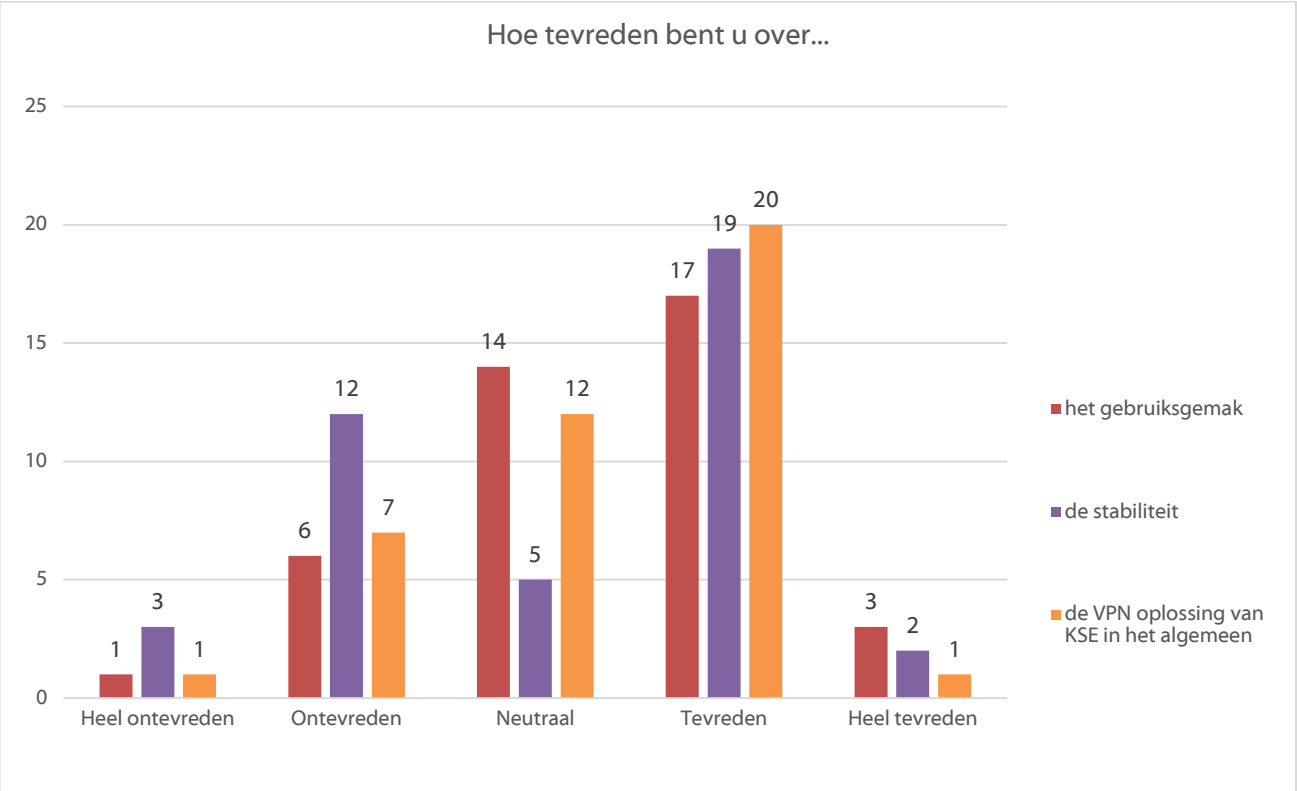
Van de medewerkers die over de rechten beschikken om een VPN verbinding te maken blijkt het grotendeel hier regelmatig gebruik van te maken.



In tegenstelling tot de verwachting van ICT, blijken de medewerkers minder problemen te ondervinden met de VPN oplossing van KSE.



Deze vraag is gesteld om de individuele antwoorden te kunnen valideren. Het kan bijvoorbeeld zo zijn dat een medewerker meldt dat hij of zij veel problemen ondervindt van de VPN verbinding, en tegelijkertijd veel verbinding maakt vanuit het buitenland. De problemen zullen in dit geval veroorzaakt worden door de hoge latency van de verbinding, in plaats van de software of de FortiGate oplossing in zijn geheel.



Een klein deel van de ondervraagden meldt problemen met de stabiliteit, maar over het geheel gekeken zijn de gebruikers tevreden.

3.2. DE ANTWOORDEN VAN DE OPEN VRAGEN OPGESOMD

3.2.1. Indien u weleens problemen ondervindt, kan u deze dan beschrijven?

- SERVER LAG ER EEN KEER UIT, TOEN VIA DE BACKUP INGELOGD NA ADVIES VRAGEN AAN MR FARHAZ
- VPN valt uit. E-mail werkt niet altijd. Soms geen VPN verbinding kunnen maken als je bij klanten bent.
- Na vanalles geprobeerd te hebben, kan ik nog steeds geen VPN verbinding maken van mijn PC thuis. Als ik weet dat ik een verbinding moet kunnen maken, neem ik een laptop mee.
- Continue popups met vraag voor update, hiervoor de service op hand moeten zetten. Duurt lang (30 seconde tot een minuut) voordat er een verbinding is. Verbinding valt af en toe weg.
- Onverwachte onderbreking
- Soms vergt het inloggen wat tijd. Snelheid internet?
- Soms valt de verbinding regelmatig weg.
- Elke keer als ik thuis mijn prive laptop opstart is er een update voor forti client. Dan kun je aangeven of je die wil of niet. Als je aangeeft dat je dit niet wil en nooit meer vragen, komt dit toch terug.
- Niet op kunnen zetten van een verbinding.
- Verbinding verbroken
- VPN komt niet tot stand, kan pc/server waarmee ik verbinding tracht te maken niet vinden, termijn pc/server wel 'aan' staat
- Heel af en toe dat ik niet kan inloggen. Als ik dan gebruik maak van het backup ip adres, werkt het wel.
- Verbinding verbreekt zonder duidelijke reden. kan vaak mijn pc op de zaak niet vinden snelheid is beroerd, speciaal als je pc's in Hoorn gebruikt.
- Soms moet ik meerdere keren proberen om een verbinding te maken met de Forticliënt voordat de verbinding daadwerkeijk wordt opgezet.
- Vaak werkt outlook (email) niet meer zoals voorheen, traag blijft hangen. Krijg dan ""Limmet acces"". Niet stabiel, maar dit kan dan ook aan de internet verbinding liggen.
- Overdag wordt je VPN verbinding soms weggedrukt, vanwege het drukke data verkeer is mij verteld. Werking forticlient hangt samen met Chipset firmware versie, onduidelijk, installatie op nieuwe computer ging hierdoor moeizaam.
- Het waren meestal firewall gerelateerde problemen... en het laatste probleem staat in het ticket systeem (jij weet het beste wat daar mee was.... SRAA).
- Meestal is het dan iets dat er de VPN helemaal uit ligt, dit komt gelukkig niet vaak voor.
- Als er wat veranderd is. Soms komt verbinding niet tot stand.
- Het gebeurd heel af en toe dat ik geen verbinding gemaakt kan krijgen
- Af en toe duurt het lang om verbinding te krijgen. Af en toe valt de verbinding weg (kan ook andere oorzaken hebben).
- Heel soms lukt het niet om in te loggen, maar na even wachten lukt het wel.
- Remote inloggen en daarna een virtuele machine opstarten. Op deze virtuele machine werkt de muis niet goed of traag.
- De applicatie wil graag een update installeren. Maar volgens Farhaz mag dat niet (mag dat nog steeds niet?). Ondanks dat ik zeg dat hij het antwoord onthouden moet blijft hij er om vragen.
- niet beschikbaar door netwerk problematiek, VPN zelf is in orde
- Met TellUs is remote niet (snel) te werken. Zeker bij veel handelingen achter elkaar is de vertraging soms zeker een seconde. Dat is lang als je heel veel van vensters wisselt, etc. Ik weet alleen niet of de VPN verbinding hiervoor verantwoordelijk is, of dat dit andere oorzaken heeft.
- De internetverbinding van mijn eigen computer valt weg zodra ik verbonden ben met het KSE netwerk via Forticlient.

- Verbinding valt regelmatig weg of er valt geen verbinding te maken

3.2.2. Zijn er dingen die u verbeterd zou willen zien aan de huidige VPN oplossing van KSE?

17 antwoorden uit lijst verwijderd omdat deze een vorm van "Nee" zijn.

- Als er een VPN verbinding is dan werkt de e-mail vaak niet.
- Ik wil vanuit mijn PC thuis verbinding kunnen maken met KSE.
- Stabieler, sneller verbinding maken, geen popups
- Lastig dat ik niet bij lokale netwerkschijf kan.
- Beschikbaarheid voor MAC OSX
- Client voor mobiele platforms. Of beter nog verbinding maken zonder specifieke client applicatie.
- Ook geschikt voor OSX maken.
- als het werkt is prima maar veel te vaak dat verbinding verbroken is
- Nu gebruik ik thuis een VM met daarop Windows en de Forti software. Nadat je verbinding had met KSE werd namelijk ook het webfilter op je thuis pc gegooid. Niet altijd even handig.
- Verbindingsmogelijkheid door middel van telefoon/iPad. Wanneer dat mogelijk is kan 'in the veld' via RDP verbinding worden gemaakt met het klantsysteem. Er zijn situaties tijdens storingen/IBS waarbij dat zeer wenselijk zou zijn.
- Dat mijn outlook goed blijft werken. en als de VPN okay is dat de verbinding met Tellus en klantfiles dan ook goed is.
- Dat forticlient je PC niet zo traag maakt!!!
- Makkelijker en sneller inloggen, bijvoorbeeld met een vingerafdruk.
- Op dit moment niet. Eventueel zou een autoreconnect na het verliezen van de verbinden handig zijn (weet niet of de huidige VPN hier al over beschikt omdat ik altijd met een stabiel internet inlog.
- Ik zou graag een met een portable app VPN verbinding willen kunnen maken. Met VPN-ware op een USB-stick vanaf elke computer in de wereld VPN verbinding maken zonder sporen na te laten op die PC.
- Eenvoudiger password strategie om vanuit KSE klanten te benaderen. Vooral voor service mensen die midden in de nacht gebeld worden is dit belangrijk
- Ja, Apple ondersteuning.
- Met zo weinig mogelijk muisklikken verbinding. Voorkeur 1 icoon.
- Als ik thuis met mijn laptop een VPN verbinding met KSE maak en darn weer stop gaat mijn Windows defender en firewall niet meer automatisch aan.
- Ja, dat mijn eigen internetverbinding niet wegvalt zodra verbonden is via Forticlient. Op dit moment dien ik de bestanden lokaal op te slaan, te bewerken en vervolgens weer te uploaden. Zou gemakkelijk zijn wanneer dit rechtstreeks.
- de stabiliteit
- Automatische verbinding maken of standaard bij internetverbinding een veilige verbinding met kantoor hebben. Maar het moet tenminste stabiler

3.2.3. Wat vind u het belangrijkste voor een goede VPN verbinding?

- stabiliteit
- DAT HIJ VERBINDT..... SPREEKT BEETJE VOOR ZICH
- Stabiliteit.
- De verbinding moet veilig en stabiel zijn.
- Stabiliteit. GEEN vervelende popups!!!
- Stabiliteit van de verbinding
- Stabiliteit en makkelijk activeren/deactiveren.

- Betrouwbaarheid in gebruik.
- betrouwbaar zijn
- Altijd beschikbaar.
- stabiel, snel
- Stabiel en snel
- Stabiliteit en snelheid
- Snelheid. Betrouwbaarheid
- 1) Stabiel 2) Snel
- stabiel snel
- Op afstand kunnen werken op een zelfde manier (en snelheid) als wanneer je fysiek op de machine aan het werken bent.
- Verbinding moet stabiel zijn. Verbinding moet snel zijn. Makkelijk op te zetten zijn.
- Makkelijk verbinding maken. Stabiele verbinding. Voldoende snelheid
- snelheid en een kwalitatieve goede verbinding
- Stabiliteit
- Stabiel is, en eenvoudig te starten. Mag geen andere software beinvloeden. Vaak is de VPN nog okay echter geeft Tellus en klantfiles problemen met benadering.
- Dat VPN software stabiliteit en performance computer niet beinvloed (forticlient VPN doet dat niet, forticlient firewall doet dat heel erg BSOD) En meteen daar achteraan staat de stabiliteit van de verbinding.
- Dat de verbinding stabile is en het downloading snel is.
- Ik wil VPN verbinding en tegelijk toegang tot mijn eigen NAS/systemen (laagdrempelige instelling of goed beschreven).
- Snelle verbinding.
- dat er niet teveel geinstalleerd hoeft te worden en vanaf elke pc met internet verbinding gebruikt kan worden.
- Veilg, stabile, snel.
- stabiliteit en snelheid
- Veiligheid en stabiliteit, aansluitend komt snelheid.
- Ik wil in principe de PC standby maken, daarna weer opstarten en verder gaan met VPN. Maar ook snel, eenvoudig tot stand brengen en nooit uitvallen.
- Toegangkelijkheid, stabiliteit, veiligheid en snelheid
- Snelheid
- Gebruiksgemak, stabiliteit.
- Snel, beveiligd en betrouwbaar
- Apple ondersteuning! Stabiele verbinding, snelheid.
- Snel en eenvoudig verbinding.
- Betrouwbaarheid
- Dat het werkt en dat het snel toegang biedt.
- de stabiliteit
- Heel belangrijk, zeker aangezien we alles centraal op het netwerk opslaan en zo minmogelijk lokaal

3.2.4. Heeft u verder nog op- en/of aanmerkingen over de huidige VPN oplossing van KSE?

29 antwoorden uit de lijst verwijderd omdat deze een vorm van “Nee” zijn.

- Is het mogelijk om meerdere alternatieven te bieden voor een verbinding van thuis naar KSE?
- Heb ik al gezegd dat ik een hekel heb aan die popups?
- lijkt laatste tijd veel stabieler sinds win 7. ook mijn privee computer (win 8) is nu goed. af en toe dat je er helemaal niet op komt ook de alternative ingang is dan onberijkbaar

- M.b.t. verbinding richting klanten vindt ik dat er een autorisatie op zou moeten zitten. Nu is het te gemakkelijk om bij een klant in te loggen (om even iets na te kijken) waar de klant geen weet van heeft. Inloggen bij klanten zou via een 'KSE-portal' moeten gebeuren waarbij eerst melding aan de klant moet worden gedaan of toestemming aan de klant moet worden vevraagd, alvorens we de verbinding mogen maken. Wie welke verbinding maakt zou ook gelogd moete worden.
- Op zich werkt het prima. Ik kan er goed mee werken.
- zie boven
- Bij sommige mensen lijkt het continue problematisch te zijn. Waar ligt het dan aan? Het OS/firewall/anti virus op het eigen systeem? Een nieuwe VPN oplossing zou daar minder gevoelig voor moeten zijn. Of moet duidelijk aangeven wat een probleem zou kunnen zijn met de huid geinstalleerde software.
- Te veel handelingen en te veel tijd voordat er verbinding is.
- Nee, de huidige oplossing is stabiel en betrouwbaar
- Had ik al aangegeven, Apple ondersteuning?
- de stabiliteit
- Zoals bij 5c aangegeven, voor mij zijn de belangrijkste plaatsen thuis en in het buitenland maar dan vaak in het hotel.

4. Wat nemen we mee

4.1. Wat zijn veel gemelde problemen?

- Geen verbinding op kunnen zetten.
- Verbinding valt vaak uit.
- Client geeft veel problemen; systeem instabiliteit, vervelende updater.

4.2. Wat zien de medewerkers graag verbeterd?

- Ondersteuning voor Apple OSX
- Split-tunneling (dus toegang tot KSE netwerk en gelijktijdig ook het thuisnetwerk)

4.3. Wat vinden de medewerkers het belangrijkst?

- Stabiliteit

5. CONCLUSIE

Over het geheel zijn de medewerkers veel minder ontevreden over de huidige VPN dan dat er bij ICT gedacht werd. De gevonden resultaten waren dus verrassend.
De veel genoemde problemen waren al bekend bij de ICT afdeling, en vormden de motivatie om het project op te starten.
De behoefte aan split-tunneling (het gelijktijdig gebruik maken van het KSE netwerk en thuisnetwerk) was bekend, maar dat de behoefte zo hoog is was onbekend.

De punten die genoemd zijn in hoofdstuk 4 zullen worden meegenomen in het requirements document.

Vervanging Remote Access voorzieningen KSE

Bijlage 3: Project requirements

Bestand	:	1.2 Requirements - Vervanging Remote Access voorzieningen KSE.docx
Versie	:	
Datum van uitgifte	:	12-8-2015
Opgesteld door	:	Farhaz Hofman
Aantal pagina's	:	6

KSE Proven Process Technology
ALFRA Dosing & Weighing Technology
PROMAS Future Proof Automation

INHOUDSOPGAVE

1. INLEIDING

1.1. KSE PROCESS TECHNOLOGY B.V.

KSE Process Technology B.V. is een familiebedrijf gevestigd in Bladel. Bovendien zijn er nog enkele engineers werkzaam vanuit Polen en de Verenigde Staten.
KSE Process Technology B.V. heeft twee hoofdbezigheden. Het verzorgt de complete productielijn automatiseringen voor voornamelijk mengvoer- en premixfabrieken. Daarnaast heeft KSE Process Technology B.V. een productenlijn van wegers voor de korrel- en poederverwerkende industrie.
Voor zowel wegers als voor automatisering wordt door KSE Process Technology B.V. 24/7 service aangeboden.
De serviceverlening wordt tussen 17:00 - 08:00 en het weekend verleend door geplande consignatiediensten. Deze werken vrijwel altijd vanuit huis.
De service medewerkers, externe engineers en thuiswerkers maken verbinding via een FortiNet IPsec oplossing.
De VPN client software heeft in het verleden voor veel problemen gezorgd. Dit zijn onder andere:
- Het heeft een onbeheerde anti-virus module, welke problemen gaf op de fileshares.
- Na updates wilde de VPN connecties niet meer werken.
- Clientsoftware was vaak de oorzaak van onstabiele systemen.

Deze problemen hebben er toe geleid dat er vanuit de ICT afdeling van KSE Process Technology B.V. het verzoek is gekomen naar betere oplossingen te zoeken met betrekking tot de VPN client, of een nieuwere versie met minder problemen.

1.2. DIRECT BETROKKENEN

Farhaz Hofman	ICT Specialist / Project Manager	KSE Process Technology B.V.
Dirk Lubbers	Manager ICT / Opdrachtgever	KSE Process Technology B.V.
Medewerkers KSE	Eindgebruikers	KSE Process Technology B.V.

2. PROJECTSCOPE EN –GRENZEN

2.1. PROJECTSCOPE

Het project zal zich primair richten op het faciliteren van een remote access omgeving voor de medewerkers van KSE Process Technology B.V.

2.2. PROJECTGRENZEN

Vanuit productmanagement is er de wens om te kijken of de nieuwe oplossing gebruikt kan worden in een dial-home opstelling voor de stand-alone computersystemen van de wegers. Hier zal naar gekeken worden, maar hierop zal geen afwijzing van een mogelijke oplossing plaatsvinden.

3. REQUIREMENTS

3.1. VANUIT GEBRUIKERS

Door middel van het houden van een enquête onder de gebruikers is geïnventariseerd wat verbeterpunten en wensen zijn met betrekking tot de nieuwe VPN oplossing.
De complete resultaten van de enquête zijn terug te vinden in het document "1.1 Enquêteverslag – Vervanging Remote Access voorzieningen KSE.(docx/pdf)"
Uit de enquête zijn de volgende resultaten gekomen:

3.1.1. Wat zijn veel gemelde problemen?

- Geen verbinding op kunnen zetten.
- Verbinding valt vaak uit.
- Client geeft veel problemen; systeem instabiliteit, vervelende updater.

3.1.2. Wat zien de medewerkers graag verbeterd?

- Ondersteuning voor Apple OSX
- Split-tunneling (gelijktijdig toegang tot het KSE netwerk en het thuisnetwerk)
- Ondersteuning voor Linux

3.1.3. Wat vinden de medewerkers het belangrijkste?

- Stabiliteit

Deze punten zullen meegenomen worden in het functioneel- en technisch ontwerp.

3.2. VANUIT KSE/ICT

In januari 2015 heeft er overleg plaats gevonden tussen Dirk Lubbers (Manager ICT) en Farhaz Hofman (IT Specialist / Projectmanager) om vast te stellen wat de wensen zijn vanuit KSE ICT.
De resultaten staan hier weergegeven en zijn gecategoriseerd volgens de MoSCoW methode.

3.2.1. Must have

- Moet op zijn minst werken op de volgende client besturingssystemen:
  - Microsoft Windows
  - Apple OSX
- Twee staps verificatie
  - Voorkeur SMS/Softtoken
- Goede monitoring/rapportage
- Koppeling met active directory voor user authenticatie
- Stabiele oplossing.
- Low footprint client
- Client compliance
  - Alleen verbinding maken wanneer het systeem dat verbinding maakt voldoet aan bepaalde eisen, zoals een up-to-date antivirus..
- Goede stabiliteit bij hoge latency (buitenland)
- Niet gebaseerd op Java.
- De client moet self updating zijn.
- Webbrowserbased portal voor eindgebruikers.

3.2.2. Should have

- Werken op de volgende client besturingssystemen:
  - Microsoft Windows Phone

    - Apple IOS
    - Google Android
- Melding bij overschrijding van een in te stellen datahoeveelheid.
- Customizability van portal
- Geen exotische oplossing

3.2.3. Could have

- Vanuit portal standaard aanbieden:
    - RDP
    - Enkele fileshares
    - SharePoint
    - PING
- Deels geautomatiseerd accounts aanmaken voor bijvoorbeeld leveranciers

Verder is er vanuit productmanagement het verzoek gekomen om te kijken naar de mogelijkheid van een dial-home functie, zodat de nieuwe oplossing eventueel ingezet kan worden voor een dial-home functie op de standalone weegmachines van KSE. Op deze manier kan remote service verlening aan die machines bewerkstelligd worden.

Qua licensering moet op dit moment rekening gehouden worden met minimaal 25 concurrent users en maximaal 150 mogelijke users die verbinding moeten kunnen maken. Er moet rekening gehouden worden met groei in de toekomst.

Vervanging Remote Access voorzieningen KSE

Bijlage 4: Naderonderzoek

Beschrijving van IST en SOLL situaties

Bestand	:	1.3 Naderonderzoek - Vervanging Remote Access voorzieningen KSE.docx
Versie	:	
Datum van uitgifte	:	12-8-2015
Opgesteld door	:	Farhaz Hofman
Aantal pagina's	:	8

Inhoudsopgave

1. INLEIDING

Dit document is opgesteld ter ondersteuning van het onderzoek naar een nieuwe remote access oplossing voor KSE Process Technology B.V.

Het document brengt duidelijk de IST situatie in beeld. Dit is de situatie waarin KSE zich momenteel in bevindt. Daarnaast wordt de gewenste situatie na afloop van het project, de SOLL situatie, belicht.

2. IST SITUATIE

De huidige remote access oplossing van KSE is gebouwd op producten van FortiNet. KSE heeft een firewall cluster bestaande uit twee FortiNet FortiGate 100D devices. Medewerkers die vanuit een externe locatie verbinding willen maken met het KSE netwerk, dienen gebruik te maken van een computer welke een versie van Microsoft Windows als besturingssysteem heeft. Hierop kan FortiClient geïnstalleerd worden. Dit is de VPN client software van FortiNet. Door de ICT afdeling is een installer gemaakt die de benodigde IPsec configuratie aan boord heeft. Als de client gestart wordt, kan er een keuze gemaakt worden uit twee profielen. Eén maakt verbinding via de hoofd internetlijn van KSE; een glasvezel verbinding van 50 Mbit. De tweede is een back-up profiel waarvan gebruikt gemaakt kan worden als de eerste niet werkt. De back-up internetlijn is een SDSL verbinding van 2 Mbit.

Nadat een medewerker een verbinding probeert te starten wordt er gevraagd om een username en password in te geven. Dit zijn de active directory credentials van de betreffende medewerker. De firewall checkt vervolgens of de credentials juist zijn en of de medewerker lid is van de active directory groep Global FortinetDailUp. Deze koppeling heeft als onderliggende techniek RADIUS. Als de checks positief zijn, zal het systeem een IP adres krijgen in het 172.21.11.0/24 subnet. Als er via de back-up lijn verbinding gemaakt wordt is het een IP in het 172.21.12.0/24 subnet.

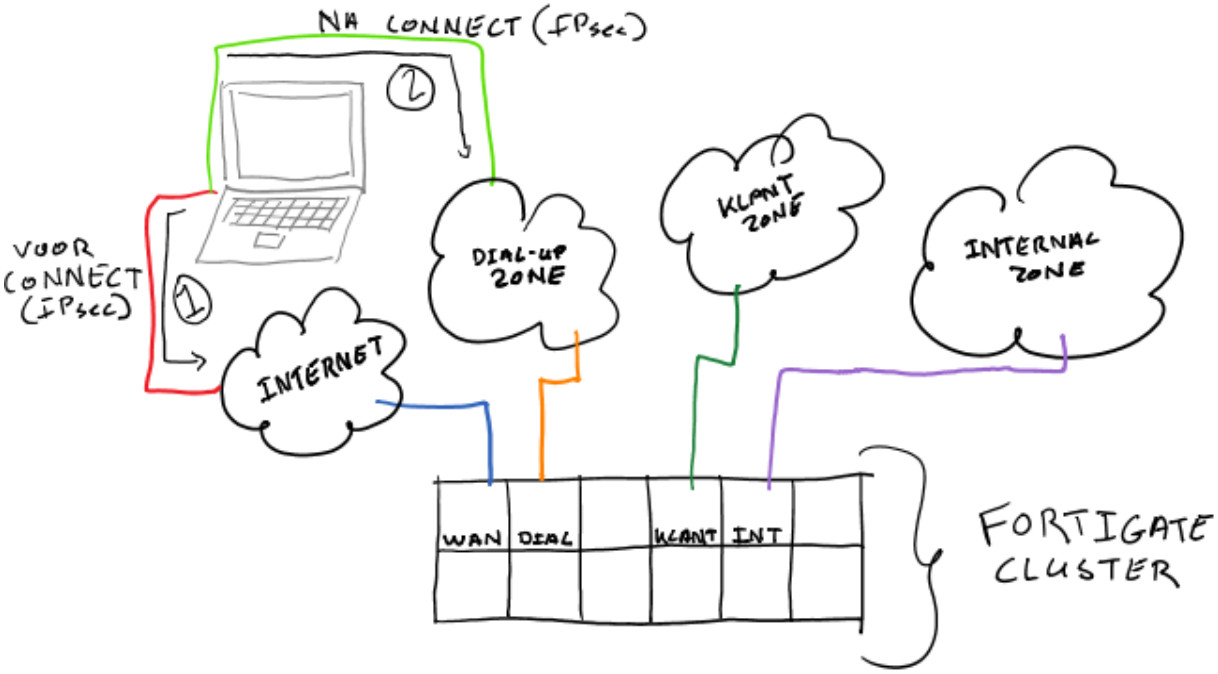
Het 172.21.11.0/24 en 172.21.12.0/24 subnet zijn lid van de “DialUp Zone”. Op deze zone worden de verschillende firewall policies gemaakt.

Op het moment dat de verbinding tot stand is gekomen heeft de medewerker vrij toegang tot het complete KSE netwerk en het verlengde van het netwerk.

172.21.0.0/16	KSE kantoor range. Hierin bevinden zich ook het server vlan en printer vlan.
172.22.0.0/16	Externe KSE locaties
172.24.0.0/16	Range waarin netwerken op klantlocaties zich bevinden
172.30.0.0/16	Range waarin ontwikkelsystemen voor klanten zich bevinden

De toegang wordt in de firewall geregeld op basis van zones. Er zijn verschillende zones gedefinieerd.

internal-zone	172.20.0.0/14	
external-zone	217.166.76.82/ 89.184.176.252/32	WAN1 hoofdlijn (glasvezel) WAN2 backuplijn (SDSL)
Dialup-zone	172.21.11.0/24 172.21.12.0/24	
Klant-Zone	172.24.*.0/24 (en nog veel meer)	



2.1. HUIDIGE KNEL PUNTEN

- Niet flexibel genoeg bij tijdelijk situaties (denk aan klanten en leveranciers)
- Vaak blokkade van IPsec poorten bij WiFi hotspots
- Instabiele client:
    - Fortinet slaat vaak een nieuw richting in met de client, en heeft geen duidelijk doel.

3. SOLL SITUATIE

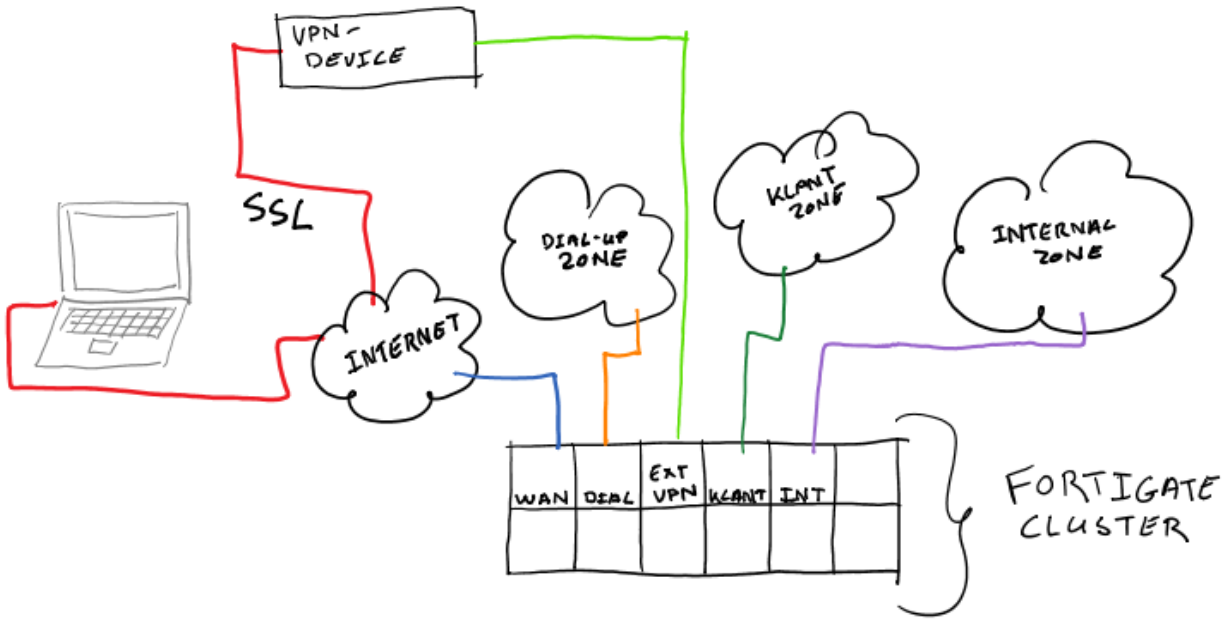
Het uitgangspunt voor de nieuwe oplossing moet een SSL VPN zijn. Hierin zijn meerdere eindsituaties te bedenken.

Voor alle situaties zullen de volgende zaken hetzelfde zijn:

- De medewerker kan via een SSL beveiligde webpagina of client-applicatie een VPN-verbinding opzetten om vervolgens verbinding te maken met interne systemen of klantsystemen.
- Authenticatie dient plaatst te vinden op basis van een koppeling met het Active Directory van KSE.
- Twee-staps-verificatie door middel van SMS, (soft)token of app verificatie.
- Er moet een webpagina (portal) beschikbaar gemaakt kunnen worden om op die manier voor klanten, leverancier of agenten links aan te bieden naar de verschillende bronnen van informatie, of test systemen waar toe ze toegang mogen hebben.

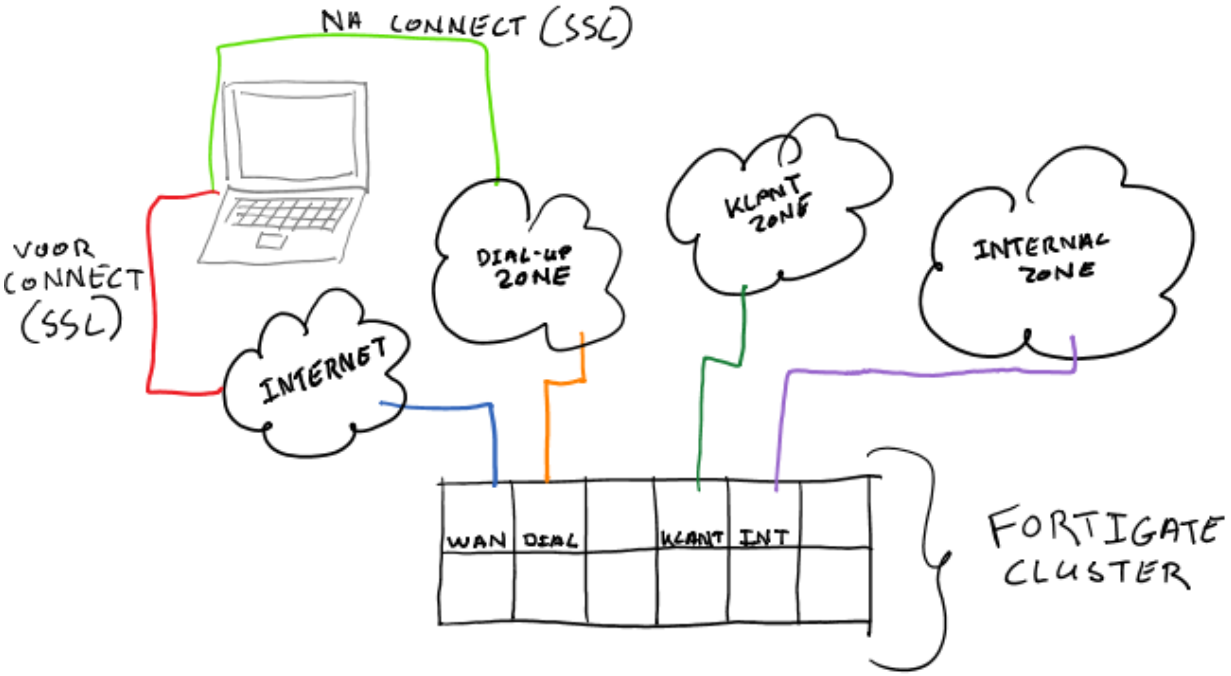
3.1. MOGELIJKE SITUATIES

3.1.1. Situatie 1: VPN Device direct aan internet



In deze situatie zal er een nieuw apparaat geïntroduceerd worden. Deze zal aan de voorkant langs de FortiGate's komen te staan, en een eigen publiek IP adres hebben.
De gebruiker zal via een webportal of client kunnen inloggen. Na het inloggen worden vanuit dit apparaat, afhankelijk van wat voor gebruiker het is, de juiste diensten aangeboden. Denk hier aan bookmarks naar sharepoint sites, of RDP links naar terminal servers. Klanten kunnen gebruik maken van RDP links naar test servers. Voor interne gebruikers is er ook de mogelijkheid om naar hun eigen werkstation te verbinden.
De achterkant van het apparaat, de interne kant, zal via de FortiGate het interne netwerk op mogen. In de ideale situatie zullen er per soort gebruiker, leverancier of klant aparte subnetten gedefinieerd worden. 'Op deze manier kunnen er in de FortiGates policies en specifieke anti-virusscans op het verkeer losgelaten worden, en dat op basis van bron IP adressen.

3.1.2. Situatie 3: FortiGate als VPN Concentrator



De FortiGates gaan in deze situatie zelf als SSL VPN host optreden. De gebruiker zal via een webportal of client kunnen inloggen. Na inloggen worden vanuit dit apparaat, afhankelijk van wat voor gebruiker het is, de juiste diensten aangeboden. Denk hier aan bookmarks naar sharepoint sites, RDP links naar terminal servers. Klanten kunnen gebruik maken van RDP links naar test servers. Voor interne gebruikers is er ook de mogelijkheid om naar hun eigen werkstation te verbinden.

Intern in de FortiGates zullen aparte IP subnets per soort gebruiker, leverancier of klant gedefinieerd worden. Op deze manier kunnen er in de FortiGates policies en specifieke anti-virusscans op het verkeer losgelaten worden, en dat op basis van bron IP adressen.

3.2. TWEE STAPS VERIFICATIE

Na het inloggen met de Active Directory gebruikersnaam en wachtwoord, dient er ten behoeve van de twee staps verificatie nog een code ingevoerd te worden. Deze code kan op meerdere manieren aangeleverd worden aan de eindgebruiker, namelijk; SMS, hardtoken (sleutelhanger) of softtoken (APP op telefoon).

3.2.1. SMS

Na inloggen met de Active Directory credentials op de portal zal er naar een opgegeven GSM nummer een code gestuurd worden, die dan ingevoerd moet worden.

3.2.2. Hardtoken

De gebruikers krijgen een sleutelhanger mee, die op basis van de tijd een code zal genereren. Deze dient dan na het inloggen met de Active Directory credentials ingevoerd te worden.

3.2.3. Softtoken

Hetzelfde principe dat geldt voor de hardtoken, geldt voor de softtoken. De code wordt echter niet gegenereerd door een sleutelhanger, maar door een app op een smartphone met Apple iOS, Google Android, of Windows Phone

Vervanging Remote Access voorzieningen KSE

Bijlage 5: Adviesrapport

Vendoronderzoek

Bestand	:	3.1 Adviesrapport - Vervanging Remote Access voorzieningen KSE - V1.0.docx
Versie	:	4
Datum van uitgifte	:	12-8-2015
Opgesteld door	:	Farhaz Hofman
Aantal pagina's	:	18

KSE Proven Process Technology
ALFRA Dosing & Weighing Technology
PROMAS Future Proof Automation

INHOUDSOPGAVE

1. ADVIESRAPPORT

1.1. VERSIEGESCHIEDENIS

Versie	Versiedatum	Veranderingen
0.1	10-07-2015	Eerste versie.
1.0	13-07-2015	Verbeteringen aangebracht na controles. Managementsamenvatting toegevoegd.
2.0	21-07-2015	Toevoeging uitwerking requirements punten 8 en 11.
3.0	07-08-2015	Verduidelijking conclusie en advies.
4.0	11-08-2015	Wijzigingen n.a.v. feedback Casper Schellekens.

1.2. GOEDKEURING

Dit document is geldig als het is goedgekeurd en ondertekend door:

Naam	Handtekening	Functie	Datum	Versie
Dirk Lubbers		Manager ICT		

1.3. VERSPREIDING

Naam	Functie	Datum	Versie
Dirk Lubbers	Manager ICT		

2. MANAGEMENTSAMENVATTING

Verkopers, project engineers en service engineers moeten te allen tijde verbinding kunnen maken met het netwerk van KSE. Verkopers moeten (mogelijke) klanten altijd kunnen voorzien van de meeste recente productinformatie. Projectengineers moeten tijdens de projectfase altijd de meest recente klantsituatie kunnen raadplegen en na de inbedrijfstelling de klant voorzien van nazorg. De service engineers verlenen een 24/7-helpdeskdienst voor de klant en moeten daarom elk moment bij de klant kunnen inloggen. Op dit moment is hiervoor een op IPsec gebaseerde oplossing van FortiNet beschikbaar.

In dit rapport is vooral gekeken naar de combinatie van de hoeveelheid requirements waarover de oplossingen beschiken, en hoe deze binnen de organisatie ingezet kunnen worden.

Voor SSL VPN gaat mijn advies uit naar Pulse Secure. De hoge functionaliteit die de webportal kan bieden is een groot pluspunt. Het feit dat het een dedicated remote access appliance is, is gunstig wat betreft de kosten. Hoewel de FortiNet oplossing ook hoog scoort, en vrijwel niets extra kost voor KSE, weegt deze optie mijns inziens niet op tegen de extra mogelijkheden die Pulse Secure biedt.

Pulse Secure biedt namelijk naast de standaard ook een Meeting functie, een filebrowser die geen JAVA nodig heeft, een uitgebreide mogelijkheid van configureren, en uitgebreide monitoring.

KSE ICT is momenteel ook aan het kijken naar het aanbieden van collaboration tools voor de organisatie, om beter samen te kunnen werken met klanten en leveranciers. Pulse Secure kan hier goede opties bieden zoals de Meeting functie en filebrowser. De uitgebreide configuratiemogelijkheden en monitoring aan de beheerkant zijn een pre.

Voor de twee-staps-verificatie gaat mijn advies uit naar SecurAccess. Hoewel SecurAccess de meest prijzige oplossing is, is het wel een flexibele oplossing. Vooral de ondersteuning voor de vele platformen en de self-service website voor de eindgebruiker is zeer positief.

3. AANLEIDING

3.1. PROBLEEMSTELLING

Verkopers, project engineers en service engineers moeten te allen tijde verbinding kunnen maken met het netwerk van KSE. Verkopers moeten (mogelijke) klanten altijd kunnen voorzien van de meeste recente productinformatie. Projectengineers moeten tijdens de projectfase altijd de meeste recente klantsituatie kunnen raadplegen en na de inbedrijfstelling de klant voorzien van nazorg. De service engineers verlenen een 24/7-helpdeskdienst voor de klant en moeten daarom elk moment bij de klant kunnen inloggen. Op dit moment is hiervoor een op IPsec gebaseerde oplossing van FortiNet beschikbaar.

3.2. DOELSTELLING

De doelstelling van het project is een advies vormen voor een nieuwe oplossing voor de remote access omgeving van KSE. De nieuwe oplossing zal op basis zijn van SSL ten opzichte van de huidige IPsec oplossing. Voor een extra niveau van beveiliging dient dit gecombineerd te worden met een twee-staps-verificatiemethode. Tevens zal er een implementatieplan opgesteld worden.

4. OPLOSSINGEN

4.1. REQUIREMENTS

Na overleg met Dirk Lubbers (Manager IT) is een lijst met requirements voor de nieuwe oplossing tot stand gekomen. Tevens is er onder de eindgebruikers een enquête gehouden om te onderzoeken wat de wensen zijn vanuit de organisatie.
Vanuit productmanagement is gevraagd te kijken welke mogelijkheden de client biedt tot gescript een VPN tot stand te brengen. Deze vraag is ontstaan door de wens om de machinebesturingen te voorzien van een dial home functie ten behoeve van remote troubleshooting.

Het overleg heeft uiteindelijk de volgende lijst van requirements opgeleverd:

1. Functioneren op Windows
2. Functioneren op OSX
3. Functioneren op Linux
4. Ondersteuning voor 2FA
5. Uitgebreide monitoring/rapportage
6. Authenticatie op basis van AD
7. Stabiele oplossing
8. Low footprint client
9. Client compliance[1]
10. Goede stabiliteit bij hoge latency verbinding
11. Niet gebaseerd op JAVA
12. Self updating client
13. Split tunneling[2]
14. Webbased portal voor end-user
15. Functioneren op Windows Phone
16. Functioneren op Apple iOS
17. Functioneren op Google Android
18. Alerts bij limiet overschrijdingen
19. Mogelijkheid tot aanpassen portal
20. Geen exotische oplossing[3]
21. Vanuit portal aanbieden van RDP
22. Vanuit portal aanbieden van Fileshares
23. Vanuit portal aanbieden van SharePoint
24. Vanuit portal aanbieden van PING
25. (Deels) geautomatiseerd account aanmaken voor leveranciers
26. Client gescript kunnen starten en VPN tunnel starten[4]

[1] De mogelijkheid om te kunnen controleren of een gebruikerssysteem dat verbinding wil maken, bijvoorbeeld bijgewerkte anti-virus software heeft.
[2] Split tunneling geeft de eindgebruiker de mogelijkheid gelijktijdig verbonden te zijn met het bedrijfsnetwerk, en het netwerk waar vanuit de gebruiker een verbinding probeert te maken. Dit is bijvoorbeeld het thuisnetwerk.
[3] Het zou een oplossing moeten zijn die wereldwijd veel gebruikt wordt, zodat je bij problemen niet meteen hoeft aan te kloppen bij de leverancier, maar ook de user communities kan raadplegen.
[4] Een wens van de afdeling productmanagement. Dit geeft de wegersystemen die aan klanten verkocht worden, de mogelijkheid zelf een verbinding ten behoeve van serviceverlening op te zetten naar KSE. Dit kan gebeuren zonder ingewikkelde hardware oplossingen,

Na het opstellen van deze lijst is volgens de MoSCoW methode bepaald welke waarde de eisen hebben. Daar is de volgende tabel uit voortgekomen.

Nr.	Requirement	Must	Should	Could	Won't
1	Functioneren op Windows	X			
2	Functioneren op OSX	X			
3	Functioneren op Linux				X
4	Ondersteuning voor 2FA	X			
5	Uitgebreide monitoring/rapportage	X			
6	Authenticatie op basis van AD	X			
7	Stabiele oplossing	X			
8	Low footprint client	X			
9	Client compliance	X			
10	Goede stabiliteit bij hoge latency verbinding	X			
11	Niet gebaseerd op JAVA	X			
12	Self updating client	X			
13	Split tunneling		X		
14	Webbased portal voor end-user	X			
15	Functioneren op Windows Phone		X		
16	Functioneren op Apple iOS		X		
17	Functioneren op Google Android		X		
18	Alerts bij limiet overschrijdingen		X		
19	Mogelijkheid tot aanpassen portal		X		
20	Geen exotische oplossing		X		
21	Vanuit portal aanbieden van RDP			X	
22	Vanuit portal aanbieden van Fileshares			X	
23	Vanuit portal aanbieden van SharePoint			X	
24	Vanuit portal aanbieden van PING			X	
25	(Deels) geautomatiseerd account aanmaken voor leveranciers			X	
26	Client gescript kunnen starten en VPN tunnel starten			X	

De requirements zullen op aanwezigheid beoordeeld worden. Op het moment dat een oplossing over een requirement beschikt, zal het aantal punten toegekend worden.
De puntenbepaling is als volgt:

- Must have: 5 punten
- Should have: 3 punten
- Could have: 2 punten
- Won't have: 1 punt

Aan het einde van de vergelijking zullen de punten opgeteld worden en zal de hoeveelheid punten een goede indicatie geven van wat de best passende oplossing voor KSE is.

4.2. SHORTLIST SELECTIE

Voor de eerste vendor keuze moet een selectie gemaakt worden uit de tientallen leveranciers van VPN remote access oplossingen. Een exotische oplossing is uitgesloten volgens de requirements. Zodoende is uitgezocht wat de grootste of beste leveranciers van firewall producten zijn.

Op basis van de Gartner chart van 2015 (Hils, Young, & D'Hoinne, 2015) is de volgende lijst van leveranciers opgesteld:

- CheckPoint
- Cisco
- FortiNet
- SonicWall
- Palo Alto
- Pulse Secure (voorheen Juniper Pulse)

De lijst is opgesteld op basis van de hoogste scorende oplossingen. Omdat er ook de wens is voor een niet-exotische oplossing is door ICT bekeken wat voor hun bekende leveranciers zijn. Om deze reden is Intel/McAfee niet opgenomen in de shortlist. SonicWall/Dell is daarvoor in de plaats gekomen, mede omdat Dell de vaste leverancier is van laptops, desktop en servers bij KSE.

4.3. BEKEKEN OPLOSSINGEN

Er zal nu wat verder ingegaan worden op de gekozen leveranciers en zal kort de aangeboden oplossing worden beschreven.

4.3.1. CheckPoint

Via een collega ben ik in contact gekomen met een technische consultant van Checkpoint. Deze heeft KSE bezocht om samen te onderzoeken wat de beste oplossing zou kunnen zijn. Tijdens dit bezoek is voorgesteld te kijken naar de CheckPoint Security Gateway 2200. Van CheckPoint heb ik ook een trial versie van de applicatie gekregen om hands-on de software te kunnen testen.

4.3.2. Cisco

Voor Cisco heeft KSE geen directe partners, daarom heb ik direct contact gezocht met Cisco. Zij hebben mijn verhaal aangehoord en mij medegedeeld dat ze op korte termijn een partner contact op zouden laten nemen met mij. Dit is helaas niet gebeurd. Tijdens het globale vooronderzoek kwam naar voren dat Cisco geen oplossingen had die aansloten op de capaciteit eis van KSE. Oftewel te klein of te groot waardoor de prijs omhoog schoot. Het dochtermerk van Cisco, Meraki, heeft ook alleen IPsec remote access oplossingen. Dit alles in acht nemend is Cisco direct afvallen als mogelijk oplossing.

4.3.3. FortiNet

KSE heeft FortiNet al in huis als firewall en IPsec VPN-oplossing. Ik heb contact gezocht met onze huidige leverancier (Secure Layers) om te onderzoeken wat de mogelijkheden zijn van de SSL-optie op de firewall. Omdat wij onze oude firewall nog in bezit hebben, heb ik zaken kunnen testen zonder de productieomgeving tot last te zijn.

4.3.4. Palo Alto

Voor Palo Alto ben ik in contact gekomen met de leverancier Lantech. Deze zijn ook langs geweest bij KSE voor een productpresentatie. Ik heb jammer genoeg geen technische demo en trial versie van de software mogen ontvangen. Ondanks dit is gekeken naar de PA-200 als mogelijke oplossing voor KSE, omdat deze voldoet aan de requirements gesteld door KSE.

4.3.5. Pulse Secure (voorheen Juniper Pulse)

Voordat ik in de vendor onderzoeksfase van mijn opdracht kwam, heeft Juniper al contact met mij gezocht. WeSecure, partner van Juniper, heeft KSE bezocht voor een uitgebreide technische demonstratie. Aan de hand van de requirements van KSE heeft WeSecure als advies de MAG-2600 gegeven. Ik heb een trial versie van de software ontvangen om hands-on te testen.

4.3.6. SonicWall

SonicWall biedt in hun remote access range van producten geen oplossingen aan op basis van SSL, enkel IPsec. Hierdoor valt SonicWall direct af als mogelijke oplossing.

4.4. VERGELIJKING OPLOSSINGEN

Nr.	Requirement	CheckPoint	FortiNet	Palo Alto	Pulse Secure
1	Functioneren op Windows	x	x	x	x
2	Functioneren op OSX	x	x	x	x
3	Functioneren op Linux	x	-	/	x
4	Ondersteuning voor 2FA	x	x	x	x
5	Uitgebreide monitoring/rapportage	x	/	-	x
6	Authenticatie op basis van AD	x	x	x	x
7	Stabiele oplossing	-	-	-	-
8	Low footprint client	x	/	x	x
9	Client compliance	x	x	x	x
10	Goede stabiliteit bij hoge latency verbinding	-	-	-	-
11	Niet gebaseerd op JAVA	x	/	x	/
12	Self updating client	x	x	x	x
13	Split tunneling	x	x	x	x
14	Webbased portal voor end-user	x	x	/	x
15	Functioneren op Windows Phone	x	x	-	x
16	Functioneren op Apple iOS	x	x	x	x
17	Functioneren op Google Android	x	x	x	x
18	Alerts bij limiet overschrijdingen	-	-	-	-
19	Mogelijkheid tot aanpassen portal	x	x	-	x
20	Geen exotische oplossing	x	x	x	x
21	Vanuit portal aanbieden van RDP	x	x	-	x
22	Vanuit portal aanbieden van Fileshares	x	x	-	x
23	Vanuit portal aanbieden van SharePoint	x	x	-	x
24	Vanuit portal aanbieden van PING	x	-	-	-
25	(Deels) geautomatiseerd account aanmaken voor leveranciers	-	-	-	-
26	Client gescript kunnen starten en VPN tunnel starten	x	x	x	x

(- = geen punten, / = gedeeltelijke punten, x = volledige punten)

4.4.1. Opmerkingen

4.4.1.1. Punt 3

Palo Alto heeft geen native client voor Linux OS'en. Er zijn wel third-party clients beschikbaar.

4.4.1.2. Punt 7

De stabiliteit is op dit moment niet goed te testen. Dit kan pas op het moment dat een dergelijke oplossing in bedrijf is, en het een load heeft van enkele gebruikers. Dit is de reden dat er voor deze requirement geen beoordeling gegeven is.

4.4.1.3. Punt 8

Alle oplossingen kunnen via de browser werken door middel van een browserplugin. Deze hebben een vrij lage impact op het systeem. Naast de browserplugins zijn er ook standalone applicaties beschikbaar om direct vanaf de desktop een verbinding te kunnen opzetten. Op die van FortiNet na

hebben ze allen een lage impact op het systeem. De client van FortiNet komt gebundeld met een webfilter en anti-virus. Iets wat als hinderlijk ervaren kan worden.

4.4.1.4. Punt 10

De betrouwbaarheid bij hoge latency is in de testomgeving niet goed te testen. FortiNet en Pulse Secure heb ik getest over een 2G GPRS verbinding. Hier ging het verbinding maken wel goed. Omdat het niet voor alle oplossingen goed te testen is, is er voor deze requirement geen beoordeling gegeven.

4.4.1.5. Punt 11

Pulse Secure krijgt hier een mindering op de punten. Om gebruik te kunnen maken van de volledige functionaliteit van de webportal zal JAVA geïnstalleerd moeten zijn op het clientsysteem.

4.4.1.6. Punt 14

De portal van Palo Alto is er alleen voor het downloaden van de client.

4.4.1.7. Punt 26

Checkpoint kan automatisch VPN starten op basis van verkeer naar een bepaald subnet. Alle vier de oplossingen hebben voor hun clients een commandline interface waardoor gescript een VPN opgezet kan worden.

4.5. UITKOMST VERGELIJKING

Nr.	Requirement	CheckPoint	FortiNet	Palo Alto	Pulse Secure
1	Functioneren op Windows	5	5	5	5
2	Functioneren op OSX	5	5	5	5
3	Functioneren op Linux	1	0	1	1
4	Ondersteuning voor 2FA	5	5	5	5
5	Uitgebreide monitoring/rapportage	5	2,5	0	5
6	Authenticatie op basis van AD	5	5	5	5
7	Stabiele oplossing	0	0	0	0
8	Low footprint client	5	2,5	5	5
9	Client compliance	5	5	5	5
10	Goede stabiliteit bij hoge latency verbinding	0	0	0	0
11	Niet gebaseerd op JAVA	5	3	5	3
12	Self updating client	5	5	5	5
13	Split tunneling	3	3	3	3
14	Webbased portal voor end-user	5	5	0	5
15	Functioneren op Windows Phone	3	3	0	3
16	Functioneren op Apple iOS	3	3	3	3
17	Functioneren op Google Android	3	3	3	3
18	Alerts bij limiet overschrijdingen	0	0	0	0
19	Mogelijkheid tot aanpassen portal	3	3	0	3
20	Geen exotische oplossing	3	3	3	3
21	Vanuit portal aanbieden van RDP	2	2	0	2
22	Vanuit portal aanbieden van Fileshares	2	2	0	2
23	Vanuit portal aanbieden van SharePoint	2	2	0	2
24	Vanuit portal aanbieden van PING	2	0	0	0
25	(Deels) geautomatiseerd account aanmaken voor leveranciers	0	0	0	0
26	Client gescript kunnen starten en VPN tunnel starten	2	2	2	2
	TOTAAL	**79**	**69**	**55**	**75**

4.6. KOSTEN VERGELIJKING

Er zijn bij de overgebleven vendoren prijsopgaves opgevraagd op basis van de volgende parameters:

- 20 gelijktijdige gebruikers
- 100 gebruikers die verbinding moeten kunnen maken
- Indien mogelijk dient de front-end redundant uitgevoerd te worden

	Checkpoint	FortiNet	Palo Alto	Pulse Secure
Hardware	$ 6.100,00	€ 0,00	€ 3.500,00	€ 1.092,00
Extra gebruikers licentie				€ 1.271,20
Support	$ 2.260,00	€ 0,00	$ 720,00	€ 319,00
Totaal investering	**€ 5.481,00**	**€ 0,00**	**€ 3.500,00**	**€ 2.363,20**
Totaal operationele kosten per jaar	**€ 2.031,00**	**€ 0,00**	**€ 647,00**	**€ 319**
Totaal na 1 jaar	**€ 8.512,00**	**€ 0,00**	**€ 4.147,00**	**€ 2.682,20**
Totaal na 3 jaar	**€ 11.574,00**	**€ 0,00**	**€ 5.441,00**	**€ 3.320,20**
Totaal na 5 jaar	**€ 15.636,00**	**€ 0,00**	**€ 6.735,00**	**€ 3.958,20**
Opmerkingen	Prijzen in dollars gekregen. Support is per 3 jaar.	Hardware al in bezit. Geen extra kosten voor SSL VPN.	Geen support prijzen ontvangen. Support prijzen verkregen via internet (PaloGuard.com, 2015)	Voor een redundant opstelling dienen de prijzen maal 2 gedaan te worden

(Dollars zijn op 10-07-2015 omgerekend naar euro's.)

4.7. TWEE-STAPS VERIFICATIEOPLOSSINGEN

Bij FortiNet, Palo Alto en Pulse Secure zijn naast de SSL VPN oplossing ook twee-staps-verificatieoplossingen aangeboden.
Op technisch vlak zijn de oplossingen op het gebied van de koppeling naar de VPN hetzelfde. De VPN-oplossing praat via RADIUS naar de twee-staps-verificatiesoftware, die op zijn beurt een authenticatieverzoek verstuurt naar active directory en daar bovenop een tweede check doet.

De volgende drie oplossingen zijn aangeboden:

4.7.1. FortiAuthenticator van FortiNet

De twee-staps-verificatieoplossing van FortiNet. Deze biedt OTP's aan via een app, SMS of een hardware token. Deze oplossing is aangeboden door SecureLayers.

4.7.2. SecurAccess van SecurEnvoy

SecurAccess is aangeboden door Wesecure als twee-staps-verificatieoplossing. Ook deze biedt OTP's aan via SMS en een app. SecurAccess heeft een selfservice portal voor de eindgebruiker. Hierdoor kan een gebruiker zelf instellen hoe en op welk device hij de code wil ontvangen. Bovendien is er de mogelijkheid tot het uitdraaien van een lijst met codes voor mensen die geen device hebben waarop de code ontvangen kan worden. SecurAccess heeft voor bijna ieder platform een app beschikbaar.

4.7.3. Authasas Advanced Authentication van Authasas

Authasas is aangeboden door Lantech. Helaas heb ik hier geen demo van mogen ontvangen. Authasas onderscheidt zich van de twee andere oplossingen door de ondersteuning die geboden wordt voor veel andere authenticatieprotocollen. Hierdoor is het een erg breed product. Bovendien zijn er veel zaken te gebruiken als twee-staps-verificatiemiddel. Naast de gebruikelijke SMS of app zijn ook yubikeys, biometrische devices of USB sticks te gebruiken als verificatiemiddel. Een groot gemis voor

Authasas is het ontbreken van een Windows Phone app. KSE is gestandaardiseerd op Windows Phone. Om deze reden valt Authasas af als mogelijke twee-staps-verificatie oplossing.

4.7.4. Kosten vergelijking

Voor iedere oplossing is een prijs opgevraagd voor 100 gebruikers.

	FortiAuthenticator	SecurAccess	Authasas
Appliance licentie	€ 1.950,00	€ 0,00	€ 0,00
100 gebruikers	€ 4.500,00	€2.806,40	€ 3.000,00
Support	€ 450,00	€ 0,00	€ 600,00
Totaal investering	**€ 6.450,00**	**€ 0,00**	**€ 3.000,00**
Totaal operationele kosten per jaar	**€ 450,00**	**€ 2.806,40**	**€ 600,00**
Totaal na 1 jaar	**€ 6.900,00**	**€ 2.806,40**	**€ 3.600,00**
Totaal na 3 jaar	**€ 7.800,00**	**€ 8.419,20**	**€ 4.800,00**
Totaal na 5 jaar	**€ 8.700,00**	**€ 14.032,00**	**€ 6.000,00**
Opmerkingen	Tokens voor gebruikers zijn een eenmalige aanschaf.	Kosten worden per gebruiker per jaar berekend. Appliance heeft geen extra kosten. Support inbegrepen.	

4.8. Overige kosten

Andere kosten die meegenomen moeten worden zijn:

- SSL-certificaat
- Installatie
- SMS verzenden

Een SSL-certificaat zal aangeschaft worden bij GoDaddy, waar KSE haar eerdere SSL-certificaten heeft aangeschaft. Bovendien bevallen de diensten van GoDaddy goed.

Voor iedere oplossing wordt uitgegaan van ongeveer twee dagen installatie. Ervaring wijst uit dat uurtarieven onder verschillende leveranciers niet veel verschillen.

Alle oplossingen hebben ondersteuning voor de grote SMS gateways op internet, waardoor de kosten hiervoor gelijk zullen zijn. Vanuit KSE zal echter aangedrongen worden op het gebruik van een app, aangezien de app in tegenstelling tot het versturen van een SMS geen kosten aan zich heeft verbonden bij het ontvangen van een code.

Gezien de bovenstaande kostenposten voor elke oplossing ongeveer gelijk zijn, is dit niet in detail meegenomen in dit adviesrapport.

5. CONCLUSIE

Checkpoint heeft het hoogst gescoord in de vergelijking. Checkpoint is een zeer complete oplossing met veel vooruitstrevende zaken; de manier hoe BYOD wordt benaderd vanuit Checkpoint is bijvoorbeeld vrij uniek. In plaats van bedrijfsresources direct op het device te benaderen, worden deze vanuit een afgesloten app aangeboden aan de eindgebruiker. Een nadeel is dat Checkpoint de duurste oplossing is.

KSE heeft FortiNet al in huis, waardoor de omschakeling naar SSL VPN vrijwel niets kost. Bovendien scoort FortiNet redelijk hoog in de vergelijking. De FortiNet oplossing is een vrij standaard oplossing. Een voordeel wat FortiNet biedt is het direct aanbieden van tunnel-mode in de browser. Dat het een standaard oplossing is, is ook terug te vinden in de lage mogelijkheid van configuratie en personalisatie van de portal en beheeropties.

Palo Alto heeft het laagst gescoord in de vergelijking. Het mist een webportal waarop een overzichtelijke wijze resources aangeboden kunnen worden. Dit is toch iets waar vanuit ICT naar gezocht wordt, om voor onze minder technische werknemers, klanten en leveranciers een positieve gebruikerservaring te garanderen.

Pulse Secure is de marktleider op het gebied van SSL VPN. De webportal is zeer uitgebreid en kan de eindgebruikers veel bieden. De webportal kan met de Meeting functie en filebrowsing ook een oplossing bieden voor het samenwerken met klanten en leveranciers tijdens projecten. Het nadeel van Pulse Secure is dat voor de volledige functionaliteit van de webclient JAVA geïnstalleerd moet worden. Bovendien beschikt het over uitgebreide monitoring. Aan de beheerkant is er een uitgebreide mogelijkheid tot configuratie.

FortiAuthenticator is een basis twee-staps-verificatieoplossing. Ondanks de naam, is FortiAuthenticator geen speciale FortiNet oplossing. FortiAuthenticator is tijdens het begin van het project afgevallen als oplossing, omdat er geen Windows Phone app beschikbaar was. Enkele maanden geleden is deze toch beschikbaar gemaakt.

SecurAccess is na verloop van tijd de duurste oplossing, maar wel de meeste flexibele. Een groot voordeel van SecurAccess is dat de eindgebruiker zelf controle heeft over hoe de twee-staps-verificatie moet plaatsvinden.

5.1. FORTINET VS PULSE SECURE

Uit het bovenstaande is te concluderen dat de twee oplossingen die overblijven FortiNet en Pulse Secure zijn. Er zal nu ingegaan worden op wat de doorslaggevende verschillen zijn tussen de twee oplossingen.

5.1.1. JAVA

Voor zowel FortiNet als Pulse Secure is JAVA nodig als er gebruikt gemaakt zal worden van de in-browser RDP, VNC of SSH/Telnet clients. Beiden bieden ook een filebrowser aan waarmee fileshares direct vanuit de browser benaderd kunnen worden. FortiNet heeft hiervoor JAVA nodig. Pulse Secure heeft hier geen JAVA voor nodig.

5.1.2. Tunnel-mode

Bij FortiNet is tunnel-mode direct beschikbaar vanuit de browser. Pulse Secure installeert een desktop applicatie genaamd Pulse Connect wat zorgt voor een tunnel-mode connectie.

Een tunnel-mode connectie houdt in dat een direct verbinding gemaakt word met het bedrijfsnetwerk. Er kan direct vanuit applicaties verbinding gemaakt worden met diverse diensten, zonder gebruik te maken van browserbased clients.

5.1.3. Functionaliteit

Zowel FortiNet als Pulse Secure beschikken over de standaard set functionaliteit. Aan de beheerderskant is FortiNet nogal beperkt in de opties in vergelijking met Pulse Secure.
Bij Pulse Secure kan op een veel dieper niveau geconfigureerd worden wat er voor welke gebruiker beschikbaar is. Hierdoor is betere gebruikerservaring te realiseren op basis van welke medewerker, leverancier of klant er inlogt.
Naast de remote access functionaliteiten biedt Pulse Secure ook een Meeting functie aan, Junos Pulse Collaboration. Dit is een tool om samenwerken met bijvoorbeeld leveranciers en klanten te vergemakkelijken. Op een makkelijke en veilige manier is zeer snel een scherm te delen met de rest van de deelnemers van de meeting. Deze tool kan ook toegepast worden voor remote supportverlening voor medewerkers of klanten.
Voor Exchange webmail biedt Pulse Secure een extra optie, waardoor het mogelijk is dat Pulse Secure de authenticatie afhandelt, inclusief twee-staps-verificatie. Hiermee is de webmail beter beveiligd.

6. ADVIES

In dit rapport is vooral gekeken naar de combinatie van de hoeveelheid requirements waarover de oplossingen beschikten, en hoe deze binnen de organisatie ingezet kunnen worden.

Voor SSL VPN gaat mijn advies uit naar Pulse Secure. De hoge functionaliteit die de webportal kan bieden is een groot pluspunt. Het feit dat het een dedicated remote access appliance is, is gunstig wat betreft de kosten. Hoewel de FortiNet oplossing ook hoog scoort, en vrijwel niets extra kost voor KSE, weegt deze optie mijns inziens niet op tegen de extra mogelijkheden die Pulse Secure biedt.

Pulse Secure biedt namelijk naast de standaard ook een Meeting functie, een filebrowser die geen JAVA nodig heeft, een uitgebreide mogelijkheid van configureren, en uitgebreide monitoring.

KSE ICT is momenteel ook aan het kijken naar het aanbieden van collaboration tools voor de organisatie, om beter samen te kunnen werken met klanten en leveranciers. Pulse Secure kan hier goede opties bieden zoals de Meeting functie en filebrowser. De uitgebreide configuratiemogelijkheden en monitoring aan de beheerkant zijn een pre.

Voor de twee-staps-verificatie gaat mijn advies uit naar SecurAccess. Hoewel SecurAccess de meest prijzige oplossing is, is het wel een flexibele oplossing. Vooral de ondersteuning voor de vele platformen en de self-service website voor de eindgebruiker is zeer positief.

7. OVERIGE

7.1. BEGRIPPENLIJST

Begrip	Verklaring
Active Directory	Gebruikers- en computersbeheer software van Microsoft.
Appliance	Een stuk software dat op eigen hardware of virtueel draait met een specifieke functie, zoals bijvoorbeeld een firewall.
Biometrische devices	Apparaten die kunnen scannen op basis van lichaamseigenschappen van de gebruiker. Bijvoorbeeld: irisscanner of vingerafdruklezer.
BYOD	Bring-Your-Own-Device. Een afkorting voor een trend in de IT, waarbij werknemers hun privéapparatuur gebruiken voor hun werk.
Dial home functie	Benaming voor de functie waarbij een apparaat zelf een verbinding naar bijvoorbeeld het hoofdkantoor kan leggen, zodra het over een internetverbinding beschikt.
Fileshares	Gedeelde netwerkmappen op het bedrijfsnetwerk.
GPRS	General Packet Radio Service. Een techniek die het mogelijk maakt over het mobiele netwerk datapakketten te versturen en ontvangen.
IPsec	Een standaard voor het versleutelen van IP-netwerkverkeer.
JAVA	Een veel gebruikte programmeertaal.
MoSCoW	Een methode om eisen in een eisenpakket onder te verdelen in de volgende prioriteiten: Must have, Should have, Could have en Won't have.
OTP	One-Time-Password. Een twee-staps-verificatiemethode waarbij de gebruiker bij het inloggen een tijdelijke code ontvangt die ingevuld moet worden. De code is vaak maar voor korte tijd geldig.
PING	Een netwerkcommando waarbij getest kan worden of de verbinding tussen twee computers actief is.
RADIUS	Remote Authentication Dial In User Service. Een gestandaardiseerde, platform onafhankelijke methode om gebruikers te verifiëren.
RDP	Remote Desktop Protocol. Een softwarematige oplossing van Microsoft voor het op afstand overnemen van een computer.
Sharepoint	Document management systeem van Microsoft
SMS	Short Messaging Service. Een methode om via het mobiele netwerk korte berichten van maximaal 160 tekens te sturen.
SSL	Een encryptiemethode om internetverkeer te beveiligen.
Twee-staps-verificatie	Een methode die een gebruikersnaam en wachtwoord verifieert, en vervolgens door middel van een tweede verificatie methode checkt of de gebruiker is wie hij zegt dat hij is.
Yubikeys	Een OTP apparaat in de vorm van een USB stick.

8. BRONNENLIJST

Adam Hils, G. Y. (2015, Mei 18). *Magic Quadrant for Enterprise Network Firewalls*. Opgehaald van Technology Research | Gartner Inc.: http://www.gartner.com/technology/reprints.do?id=1-2DVI0YW&ct=150422&st=sb&elqaid=1245&elqat=2&elqTrackId=3fde15b81c9b4061864 1ac7bb3b9641f

Paloguard.com. (2015, July 10). *Palo Alto Networks Enterprise Firewall PA-200*. Opgehaald van PaloGuard.com: http://www.paloguard.com/Firewall-PA-200.asp

Vervanging Remote Access voorzieningen KSE

Bijlage 6: Implementatieplan

Bestand	:	Implementatieplan - Vervanging Remote Access voorzieningen KSE.docx
Versie	:	
Datum van uitgifte	:	12-8-2015
Opgesteld door	:	Farhaz Hofman
Aantal pagina's	:	6

KSE Proven Process Technology
ALFRA Dosing & Weighing Technology
PROMAS Future Proof Automation

INHOUDSOPGAVE

1. INLEIDING

Dit voorstel voor een implementatieplan is het gevolg van het advies gegeven in het project "Vervanging Remote Access voorzieningen KSE". Het advies wat is afgegeven is het implementeren van een oplossing van Pulse Secure.

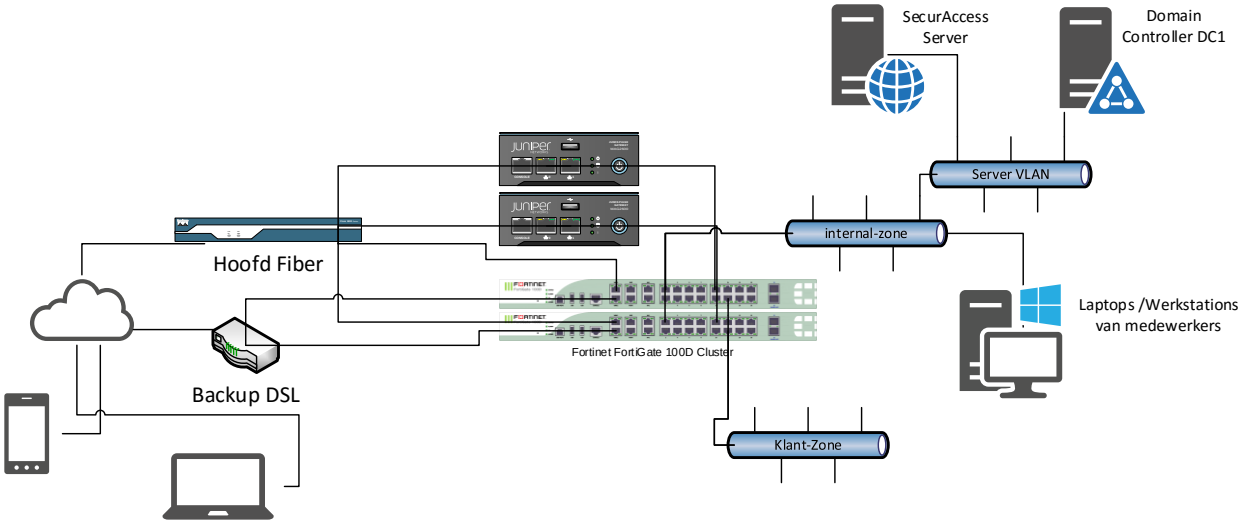
Op het moment van schrijven staat de implementatie bij acceptatie van het advies gepland voor september of oktober 2015.

2. VOORSTEL TECHNISCH ARCHITECTUUR

De twee MAG 2600's van Pulse Secure zullen in een active/passive[1] high availability (hoge beschikbaarheid) opstelling komen te functioneren. Ze zullen allebei op de hoofdglasvezellijn aangesloten worden en hier een publiek IP krijgen. Om geen single point of failure te hebben is gekozen voor deze opstelling. De interne kant van de MAG 2600's zullen aan de FortiNet aangesloten worden. Ook zullen zij in het VPN VLAN geconfigureerd gaan worden. Al het verkeer zal voordat het 't interne netwerk opgaat op virussen en malware gescand worden door de FortiGates.

In de toekomst wordt de back-up DSL lijn vervangen door een glasvezellijn. Mocht KSE op deze lijn meerdere IP adressen krijgen, dan zou er overgegaan kunnen worden op een active/active[2] opstelling. Iedere MAG 2600 zal dan op een aparte lijn aangesloten worden. Dit heeft als reden dat bij uitval van de hoofd glasvezellijn, medewerkers nog steeds verbinding kunnen maken met de het netwerk van KSE.

Voor de autorisatie zullen de MAG 2600's via een active directory koppeling verbonden worden aan de domain controller DC1. Voor de twee-staps-verificatie zullen de MAG 2600's via het RADIUS protocol verbonden worden met de SecurAccess machine. Voor de extra autorisatie zal de SecurAccess machine via een active directory koppeling verbonden zijn met de DC1.
De SecurAccess machine zal enkel toegankelijk zijn voor de medewerkers vanuit alleen het interne netwerk. Dit is voor de configuratie van de twee-staps-verificatie.



In het naderonderzoek in ook voorgesteld de nieuwe oplossing "achter" de FortiGate's te plaatsen. Daar is niet voor gekozen, omdat bij uitval van de FortiGate dan geen remote verbinding meer mogelijk is. Ook de IT afdeling kan dan op afstand geen verbinding meer maken en dus ook niet kijken wat er eventueel mis is. Een probleem oplossen gaat dan veel langer duren.

[1] Een active/passive opstelling houdt in dat er twee dezelfde devices aangesloten zijn, maar dat er maar één actief is. Als de eerste uitvalt, neemt de tweede de activiteiten van de eerste automatisch over.
[2] Bij active/active opstelling zijn beide devices actief. Dit kan zijn voor beschikbaarheid via verschillende internetlijnen. Of voor het verdelen van de werkbelasting over de twee devices.

3. VOORSTEL PLANNING

Voor de implementatie is de volgende planning voorgesteld.

		Week 1					Week 2					Week 3					Week 4					Week 5					Week 6				
Activiteit	**Door**	**M**	**D**	**W**	**D**	**V**	**M**	**D**	**W**	**D**	**V**	**M**	**D**	**W**	**D**	**V**	**M**	**D**	**W**	**D**	**V**	**M**	**D**	**W**	**D**	**V**	**M**	**D**	**W**	**D**	**V**
Voorbereidingen	KSE ICT																														
Installatie / Configuratie / Training	WeSecure																														
Customizen en finetuning voor gebruik bij KSE	KSE ICT																														
Testen met enkele medewerkers	KSE ICT																														
Opstellen documentatie gebruik	KSE ICT																														
Opstellen documentatie beheer	KSE ICT																														
Communicatie naar organisatie	KSE ICT																														
Inloopmomenten voor minder technische mensen	KSE ICT																														
Live gaan	KSE ICT																														
Pulse Secure naast FortiNet laten draaien	KSE ICT																														
Uitzetten Remote Access op FortiNet	KSE ICT																														

3.1. VOORBEREIDINGEN

Publieke IP adressen bepalen. Virtuele machine klaarmaken voor installatie van SecurAccess software.

3.2. INSTALLATIE / CONFIGURATIE / TRAINING

Installatie en configuratie van de Pulse Secure en SecurAccess software door de consultants van WeSecure. De training zal een hands-on training zijn, waarbij één medewerker van KSE IT dicht betrokken zal zijn de initiële configuratie.

3.3. CUSTOMIZEN EN FINETUNING VOOR GEBRUIK BIJ KSE

Het aanpassen van de portal ten behoeve van optimale gebruikers ervaring. Dus het alvast aanmaken van bookmarks naar veel gebruikte netwerk locaties en terminal servers.

3.4. TESTEN MET ENKELE MEDEWERKERS

Tijdens deze periode zullen er met enkele gebruikers de nieuwe oplossing getest worden. Dit zijn gebruikers die vaker applicaties testen voor de IT afdeling. Deze medewerkers zijn op een juiste manier kritisch en hebben ook het vermogen problemen goed te omschrijven.

3.5. OPSTELLEN DOCUMENTATIE GEBRUIK

Er zullen handleidingen voor het gebruik opgesteld worden en instructies voor de eventuele installatie van de client. Sommige acties zullen ook door middel van een filmpje toegelicht gaan worden. De documentatie zal verspreid worden via het intranet van KSE.

3.6. OPSTELLEN DOCUMENTATIE BEHEER

Voor de medewerkers van IT zal documentatie opgesteld gaan worden door de medewerker van de hands-on training heeft gekregen. De documentatie zal de configuratie beschrijven.

3.7. COMMUNICATIE NAAR ORGANISATIE

Door middel van een email naar alle medewerkers zal gecommuniceerd worden over de aanstaande wijzigingen in de remote access omgeving. Er zal minimaal één reminder gestuurd worden om de medewerkers te herinneren.

3.8. INLOOPMOMENTEN VOOR MINDER TECHNISCHE MEDEWERKERS

Zoals bij elk bedrijf zijn er bij KSE ook mensen in dienst die minder technisch onderlegd zijn. We zullen voor deze mensen ook inloopmoment gaan plannen zodat ze een hands-on uitleg krijgen van

de nieuwe remote access oplossing. Vaak als ze het een keer gezien en gedaan hebben is het duidelijk voor ze.

3.9. LIVE GAAN

Het moment dat we de Pulse Secure oplossing in bedrijf nemen en het gebruikt kan gaan worden door de organisatie

3.10. PULSE SECURE NAAST FORTINET LATEN DRAAIEN

Omdat niet iedereen gelijk over kan naar de nieuwe oplossing blijft voor twee weken FortiNet naast Pulse Secure draaien. Zeker voor de medewerkers die in het buitenland werken moet de tijd genomen worden om te zorgen dat zij stabiel via de nieuwe oplossing kunnen werken voordat de oude buiten bedrijf wordt gesteld.

3.11. UITZETTEN REMOTE ACCESS OP FORTINET

Na twee weken zal de remote access functionaliteit van FortiNet uitgeschakeld worden.