Opzetten van een Citrix ShareFile met een lokale storage zone door middel van NetScaler met AAA-functionaliteit

# Samenvatting

# Woord vooraf

# Inhoudstafel

[Samenvatting 3](#_Toc511313458)

[Woord vooraf 4](#_Toc511313459)

[Inhoudstafel 5](#_Toc511313460)

[Lijst met gebruikte symbolen en afkortingen 7](#_Toc511313461)

[1 Voorstelling van het bedrijf 9](#_Toc511313462)

[1.1 ISO 9001 9](#_Toc511313463)

[1.2 Bedrijfsstructuur 11](#_Toc511313464)

[1.2.1 CEO 11](#_Toc511313465)

[1.2.2 Finance & Administration 11](#_Toc511313466)

[1.2.3 Human Resources 11](#_Toc511313467)

[1.2.4 Customer Care 12](#_Toc511313468)

[1.2.5 Development 12](#_Toc511313469)

[1.2.6 Operations 12](#_Toc511313470)

[1.3 Werking 12](#_Toc511313471)

[1.3.1 Missie 13](#_Toc511313472)

[1.3.2 ICT Infrastructure foundation 13](#_Toc511313473)

[1.3.3 Advanced ICT Infrastructure 13](#_Toc511313474)

[1.3.4 Applications 13](#_Toc511313475)

[1.3.5 Partners 14](#_Toc511313476)

[1.4 Contactgegevens 14](#_Toc511313477)

[2 Omschrijving van de bachelorproef 15](#_Toc511313478)

[2.1 Kort overzicht 15](#_Toc511313479)

[3 Actieplan 16](#_Toc511313480)

[4 Voorstudie 17](#_Toc511313481)

[4.1 Kiezen voor de Cloud 17](#_Toc511313482)

[4.1.1 Vergelijking met VPN 17](#_Toc511313483)

[4.1.2 Keuze aan Cloud-opstellingen 19](#_Toc511313484)

[4.1.3 Keuze aan Cloud-oplossingen 20](#_Toc511313485)

[4.1.4 ShareFile 21](#_Toc511313486)

[4.2 Netwerkvoorzieningen 22](#_Toc511313487)

[4.2.1 Citrix ShareFile 23](#_Toc511313488)

[4.2.2 Citrix NetScaler 23](#_Toc511313489)

[4.2.3 Citrix StorageZone Controller 24](#_Toc511313490)

[4.2.4 Domain Name System 24](#_Toc511313491)

[4.2.5 Active Directory 25](#_Toc511313492)

[4.2.6 NetScaler Traffic management 25](#_Toc511313493)

[4.2.6.1 Content switching 25](#_Toc511313494)

[4.2.6.2 Load balancing 26](#_Toc511313495)

[4.2.6.3 AAA 26](#_Toc511313496)

[4.2.6.4 Policies 27](#_Toc511313497)

[4.2.7 High availability 27](#_Toc511313498)

[4.3 Authenticatie 28](#_Toc511313499)

[4.3.1 AD-integratie 28](#_Toc511313500)

[4.3.2 SSO 29](#_Toc511313501)

[4.3.2.1 OAuth 29](#_Toc511313502)

[4.4 Extra beveiligingsimplementaties 31](#_Toc511313503)

[5 Praktische uitwerking 32](#_Toc511313504)

[Algemeen besluit 33](#_Toc511313505)

[Figuurlijst 34](#_Toc511313506)

[Bibliography 35](#_Toc511313507)

[Bijlagen 38](#_Toc511313508)

# Lijst met gebruikte symbolen en afkortingen

2FA two-factor authentication

AAA Authentication, Authorization and Accounting

AD Active Directory

CA certificate authority

CIFS Common Internet File System

DaaS Directory as a Service

DMZ demilitarized zone

DNS Domain Name System

ERP Enterprise resource planning

HA high availability

HTTPS HyperText Transfer Protocol Secure

IaaS Infrastructure as a Service

ICT Informatie en Communicatie Technologie

IDP identity provider

IP internetprotocol

ISO International Organization for Standardization

LDAP Lightweight Directory Access Protocol

OAuth Open Authorization

OpenID OpenID Connect

PaaS Platform as a Service

PFS perfect forward secrecy

QMP Quality Management Principles

RADIUS Remote Authentication Dial-In User Service

SaaS Software as a Service

SAML Security Assertion Markup Language

SAP Systeme, Anwendungen und Produkte in der Datenverarbeitung (bedrijf)

SLA service-level agreement

SP service provider

SSO single sign-on

URL Uniform Resource Locator

VPN virtual private network

# Voorstelling van het bedrijf

ICORDA is een professioneel ICT-bedrijf dat opgericht werd door CEO Joris Van Maldeghem in 1992. Het bedrijf is een solide partner voor kwalitatief hoogstaande informatica oplossingen en diensten. Buiten de implementatie van informatica oplossingen, voorzien ze ook de bijhorende support, advies en consultancy.

Deze oplossingen kunnen van allerlei aard zijn. De oplossingen variëren van softwaretoepassingen tot hardware-implementaties en netwerk opstellingen. SAP, ERP, IP-telefonie, back-up voorzieningen en Cloud integratie behoren tot de voornaamste services die ICORDA levert voor zijn klanten.

ICORDA richt zich tot organisaties die het beheer van hun netwerk-infrastructuur en softwaretoepassingen geheel of gedeeltelijk toevertrouwen aan een externe partner. Het bedrijf biedt zijn services aan binnen alle sectoren, op voorwaarde dat de klant werkt met een ICT-infrastructuur van *degelijke omvang*. [1]

## ISO 9001

ICORDA is ISO 9001:2015 gecertificeerd en toont daarmee aan dat ze gestructureerd en kwalitatief tewerk gaan. In 2005 behaalde het bedrijf dit certificaat door te voldoen aan de nodige voorwaarden. Sindsdien heeft het bedrijf zijn medewerkers goed opgeleid om te werken met een oog voor de normen en waarden van de ISO.

ISO 9001 streeft voornamelijk naar een goede werkstructuur en het bekomen van kwalitatieve eindproducten en diensten voor een maximale klanttevredenheid. Het is een internationale standaard met lokale herkenning, dat haalbaar is voor elk bedrijf ongeacht de grootte of omzet ervan.



Figuur 1‑1: De voordelen van ISO 9001 gecertificeerde bedrijven. [2]

Voor het behalen van het ISO 9001 certificaat wordt de aandacht voornamelijk gericht op het volgende:

* Customer focus
* Leadership
* Engagement of people
* Process approach
* Improvement
* Evidence-based decission making
* Relationship management

Deze vormen de zeven Quality Management Principles (QMP) van de ISO 9001 norm.

Het “Quality management systems – Requirements” document bevat alle informatie waarmee het bedrijf rekening moet houden om kwalitatief werk te kunnen leveren, en het ISO 9001:2015 certificaat te kunnen behalen. [3]

Ieder jaar wordt er vanuit de ISO een opvolgingsnazicht (follow-up audit) gepland. Het certificaat heeft een geldigheidsduur van 3 jaar. Om de 3 jaar is er dus nood aan een hercertificering. [4]

## Bedrijfsstructuur

CEO

Finance & Administration

Human Resources

Customer Care

Operations

Development

Figuur 1‑2: De bedrijfsstructuur van ICORDA NV

### CEO

ICORDA valt onder het beheer van CEO Joris Van Maldeghem. Joris is niet alleen een intelligente zakenman en oprichter van ICORDA, hij zit ook in de raad van bestuur van de Odisee hogeschool. In 1992 richtte hij het bedrijf op dat toen een oplossing voor automatische temperatuursregistratie in de voedingssector ontwikkeld had.

### Finance & Administration

De afdeling “Finance en Administration” is verantwoordelijk voor het financieel en administratief bedrijfsbeheer. Dit takenpakket betreft voornamelijk de boekhouding en facturatie. De werknemers in deze afdeling voorzien het bedrijf ook van de nodige aankopen.

### Human Resources

Aangezien ICORDA –met 30 werknemers- geen heel groot bedrijf is, is er geen aparte afdeling voor HR. Maar ICORDA is wel voorzien van een HR-medewerker, namelijk Karel Van Maldeghem. Hij werkt ook in de afdeling “Customer Care”.

### Customer Care

“Customer Care” is meestal de go-to voor klanten. Het eerste contact van de klanten vindt meestal plaats met de afdeling “Customer Care”, zij nemen dikwijls de telefoon op en beantwoorden de meeste mails. Ze stellen ook offertes op en brengen de garantie in orde. Op belangrijke afspraken met klanten is er een medewerker van Customer Care aanwezig.

### Development

“Development” staat in voor de ontwikkeling, installatie en implementatie van software. Voornamelijk houden zij hun bezig met het programmeren van “dedicated applications” voor de klanten. Ook de installatie van software van derden zoals SAP wordt door deze afdeling gedaan. Dit gaat meestal gepaard met Operations die dan de nodige infrastructuur (bv. Suse server voor SAP) installeert. Indien nodig zullen zij bestaande softwarepakketten bijwerken naar de behoeften van de klant. Een groot deel van hun tijd zal uitgaan naar debuggen en troubleshooting wanneer problemen opduiken.

### Operations

“Operations” werkt op het netwerkniveau. Voornamelijk houden zij hun bezig met het opzetten, onderhouden en beveiligen van netwerken, het installeren en configureren van servers en randapparatuur en het oplossen van netwerk- server- en computerproblemen. Ook zij zullen veel aan troubleshooting doen indien er netwerkproblemen optreden. Het grote verschil t.o.v. “Development” is dat ze voornamelijk binnen de eerste 4 lagen van het OSI-model werken.

ICORDA voorziet een toegewijde netwerkverbinding met zijn klanten. “Operations” wordt ook voorzien van een administratoraccount op het domein van de klant (met eventueel de nodige VPN-gegevens), zodat de situatie gemakkelijk opgevolgd kan worden vanop afstand, zonder noodzakelijk klantenbezoek. Dit maakt het ook mogelijk om de netwerkinfrastructuur van de klant voortdurend te kunnen auditen (ook voor de klanten die zich in het buitenland bevinden).

## Werking

Buiten de onderverdeling van het bedrijf over de verschillende afdelingen en het werken volgens de ISO-normen zijn er nog een aantal zaken waar rekening mee gehouden wordt op ICORDA.

ICT Infrastructure foundation

Network

Nodes

Security

Connectitvity

Management

Applications

Advanced ICT Infrastructure

IP Telephony

Access Infrastructure

Portals & websites

Applications

C-Logic Venice

SAP Business One

Custom Development

Figuur 1‑3: De verschillende niveaus waaruit een netwerkopstelling en oplossingen bestaan. [5]

### Missie

“ICORDA wil een solide leverancier zijn van kwalitatief hoogstaande informatica oplossingen: projecten, diensten, producten en advies voor de professionele organisatie” –Quote uit de bedrijfsvoorstelling PowerPoint van ICORDA. [5]

### ICT Infrastructure foundation

De “ICT Infrastructure foundation” ligt aan de basis van alle oplossingen en producten. Dit niveau draait vooral rond het fysieke netwerk. Dat zijn de nodes, de beveiliging ervan, de connectiviteit ertussen en het management van dit geheel.

### Advanced ICT Infrastructure

Daarop volgt de “Advanced ICT Infrastructure”. Dit niveau zegt meer over het doel van de netwerk infrastructuur. Voorbeelden in deze laag zijn IP-telefonie, toegangsinfrastructuur (access infrastructure), portals en websites.

### Applications

Dan volgen de softwarepakketten die thuishoren in “Applications”. Hier horen softwarematige oplossingen thuis zoals SAP Business One, C-Logic Venice…

### Partners

ICORDA heeft veel partners binnen de ICT-wereld. Hieronder vallen enkele belangrijke bedrijven zoals Citrix en Microsoft. ICORDA maakt (zowel intern als voor de klanten) optimaal gebruik van bijna alle producten en oplossingen dat Citrix te bieden heeft. Met de opkomst van mailfunctionaliteit en Cloud technologieën maken ze nu volop gebruik van de Microsoft zijn Office 365 softwareoplossing.

Buiten Citrix en Microsoft zijn er nog enkele belangrijke partners van ICORDA zoals Proximus, Lenovo, Cisco, SAP… Meer info kan je terugvinden op [de website van ICORDA](https://www.icorda.be).

[5]

## Contactgegevens

ICORDA NV

Adres: Brugsevaart 32, 9030 MARIAKERKE (GENT) België

Tel: +32 (0)9 227 66 76

Fax: +32 (0)9 227 97 45

E-mail: [info@icorda.be](mailto:info@icorda.be)

Ondernemingsnummer: BTW BE 0448.146.631 RPR GENT

Openingsuren: ma - vr: 8u30-12u30 | 13u30-17u30

# Omschrijving van de bachelorproef

Als bedrijf is het niet altijd slim of zelfs legaal om de volledige lokale opslag zomaar op een publieke Cloud te dumpen. Er zijn een aantal zaken waarmee het bedrijf rekening moet houden indien het gaat over de opslag van gevoelige data (zowel eigen data als die van klanten).

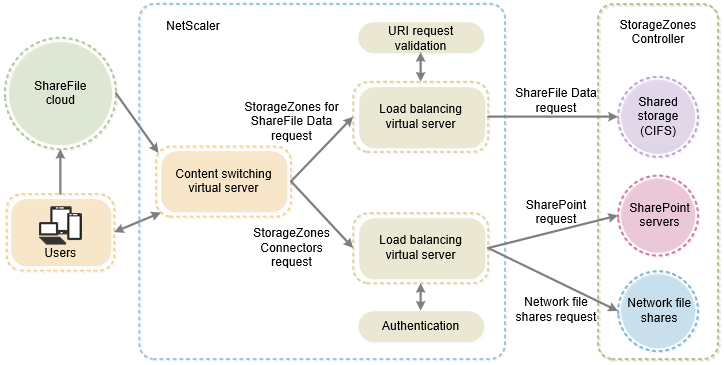
Ook op ICORDA probeert men hier rekening mee te houden. Toch wordt er steeds meer gestreefd naar een Cloud oplossing om extra beschikbaarheid en functionaliteit te bekomen. ICORDA overweegt dan ook een Cloud gerichte oplossing voor klanten die hier nood aan hebben.

Voor deze bachelorproef zal gebruik gemaakt worden van de Citrix ShareFile Cloud oplossing. ShareFile is een multifunctionele Cloud omgeving, die publiek, privaat of hybride kan opgesteld worden. In deze proef zal de ShareFile gekoppeld worden aan een lokale StorageZone met een StorageZone Controller server, zodat de troeven van lokale storage niet verloren gaan. De Cytrix NetScaler met zijn content switching, load balancing en secure authentication capaciteiten zal gebruikt worden als interne gateway en firewall. Er wordt dus gekozen voor een private opstelling, maar deze kan zonder veel moeite ook hybride gemaakt worden.

In dit boek zullen verschillende mogelijke oplossingen vergeleken worden. Aan elke keuze zal een grondige redenering voorafgaan. De keuzes die gemaakt worden zijn dan ook toepasselijk voor bepaalde klanten, maar niet noodzakelijk de juiste oplossing voor andere bedrijven in andere situaties. Ook de keuze voor de NetScaler en de verdere keuzes voor authenticatie worden verantwoord en vergeleken met de alternatieven. Vooral aan de NetScaler en de authenticatie zal veel tijd besteed worden in deze bachelorproef.

## Kort overzicht

**Titel en Opdracht:** “Opzetten van een Citrix ShareFile met een lokale storage zone door middel van NetScaler met AAA-functionaliteit”



Figuur 2‑1: Het diagram van de bachelorproef opstelling, ShareFile met NetScaler en StorageZones. [6]

* **Belangrijke componenten:** content switching server, load balancing server(s), AAA-server, StorageZone Controller, ShareFile Cloud, Active Directory, beveiligingsmaatregelen…

# Actieplan

|  |  |  |
| --- | --- | --- |
| Home | **Odisee**  **Studiegebied IWT**  **Opleiding Electronica-ICT**  2017-2018 | **Technologiecampus Gent**  Gebr. Desmetstraat 1  9000 GENT  Tel.: (09) 265 86 10  Fax: (09) 225 62 69 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ACTIEPLAN** (vereisten op pg. 2) | | | | |
| Student(e): Maxim Delaet Groep: 3ICT | | | | |
| Stageplaats: ICORDA NV | | | | |
| Stageleid(st)er (interne promotor): Evert-Jan Jacobs | | | | |
| Stagementor (externe promotor): Jochen Steenbrugge | | | | |
| **Stap** | **Inhoud** | **Streef- datum** | **Werkelijke**  **datum** | **Opvolging** |
| 1  2  3  4  5  6  7  8 | **Opzetten Windows omgeving, AD, fileserver**  **Opzetten van storagezone**  **Opzetten van ShareFile cloud**  **Opzetten en configuratie Netscaler**  **Certificaten, veiligheidsvoorzieningen en authenticatie (SSO)**  **2x StorageZone Controller en load balancing**  **Ontdubbelen Netscaler met DMZ**  **Uittesten performance en availability m.b.t. SLA** | 02/03/18  09/03/18  16/03/18  23/03/18  30/03/18  06/04/18  20/04/18  27/04/18 | 01/03/18  xx/03/18\*  xx/03/18\*  12/03/18  14/03/18 |  |

\* Vertraging opgelopen bij het opzetten van de StorageZone Controller voor de ShareFile Cloud vanwege beperkingen in de trial versie, adminaccount logingegevens ontvangen op 21/03

# Voorstudie

Hier volgt de voorstudie van de bachelorproef. In de voorstudie komt alle belangrijke informatie aan bod die op voorhand gekend moet zijn om aan de opdracht te kunnen beginnen. Hierin worden de verschillende mogelijkheden reeds vergeleken en de redeneringen uitgeschreven. De voorstudie zal ook de nodige details bevatten, met welke men rekening moet houden tijdens de feitelijke opstelling.

## Kiezen voor de Cloud

Kort gezegd kan men stellen dat de volgende punten doorslaggevend zijn bij de keuzes voor de toegang tot en opslag van gevoelige data.

* De data moet steeds (gemakkelijk) toegankelijk zijn, ongeacht de locatie van de gebruiker. (**availability**)
* De data kan alleen toegankelijk zijn voor de gebruikers die er recht op hebben. (**authentication**)
* De data moet goed afgeschermd zijn van ongewenste toegang en manipulatie (bv. Door hackers). (**security** en **integrity**)
* De dataopslag moet aan alle regels en wetten voldoen. (l**egality**)
* Gevoelige data wordt liefst in eigen handen gehouden, d.w.z. dat een eigen opslagruimte gebezigd wordt. Indien dat niet mogelijk is, houdt men liefst de private key in eigen handen. (**privacy**)

ICORDA probeert hier ook rekening mee te houden wanneer er naar de ideale oplossing voor een klant gezocht wordt.

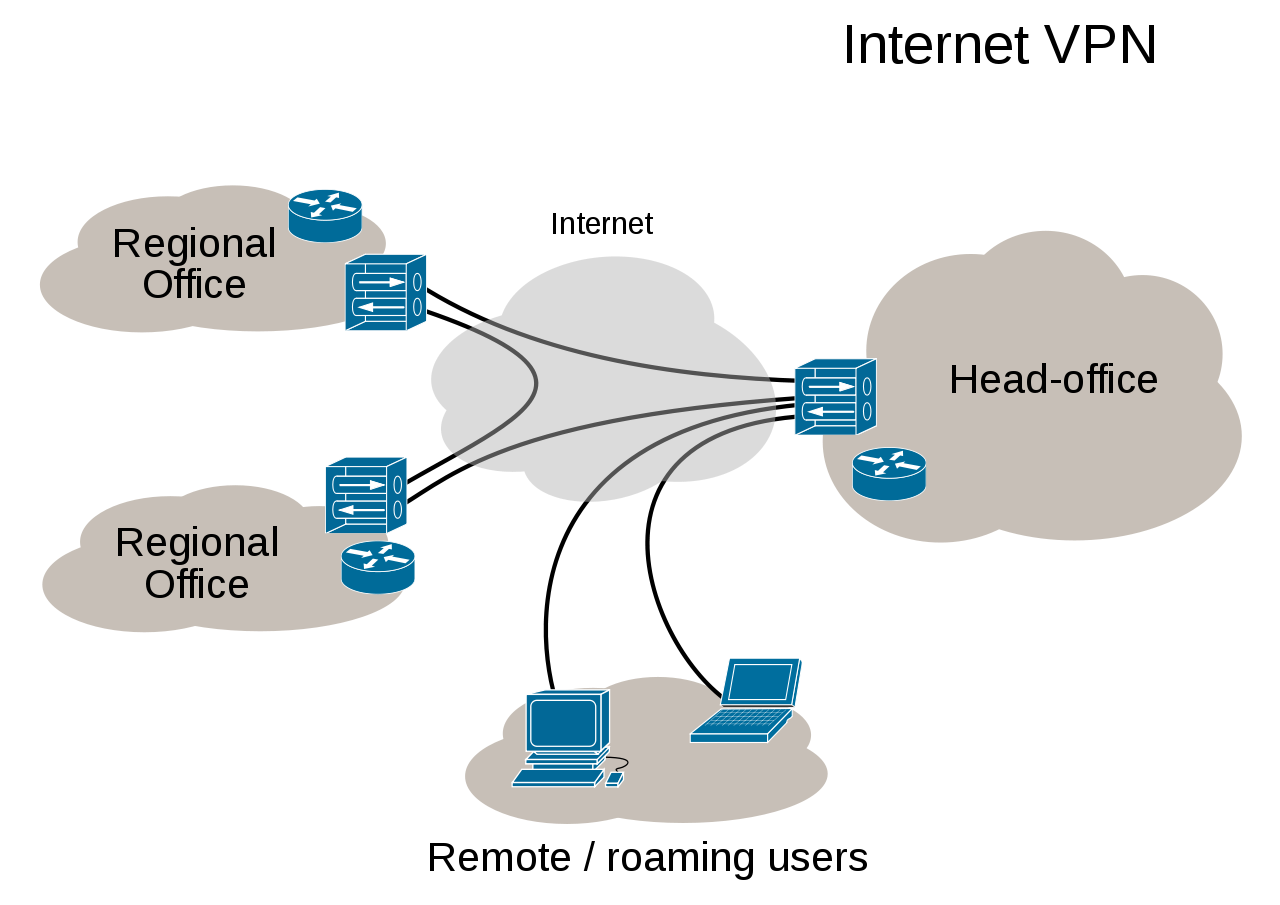
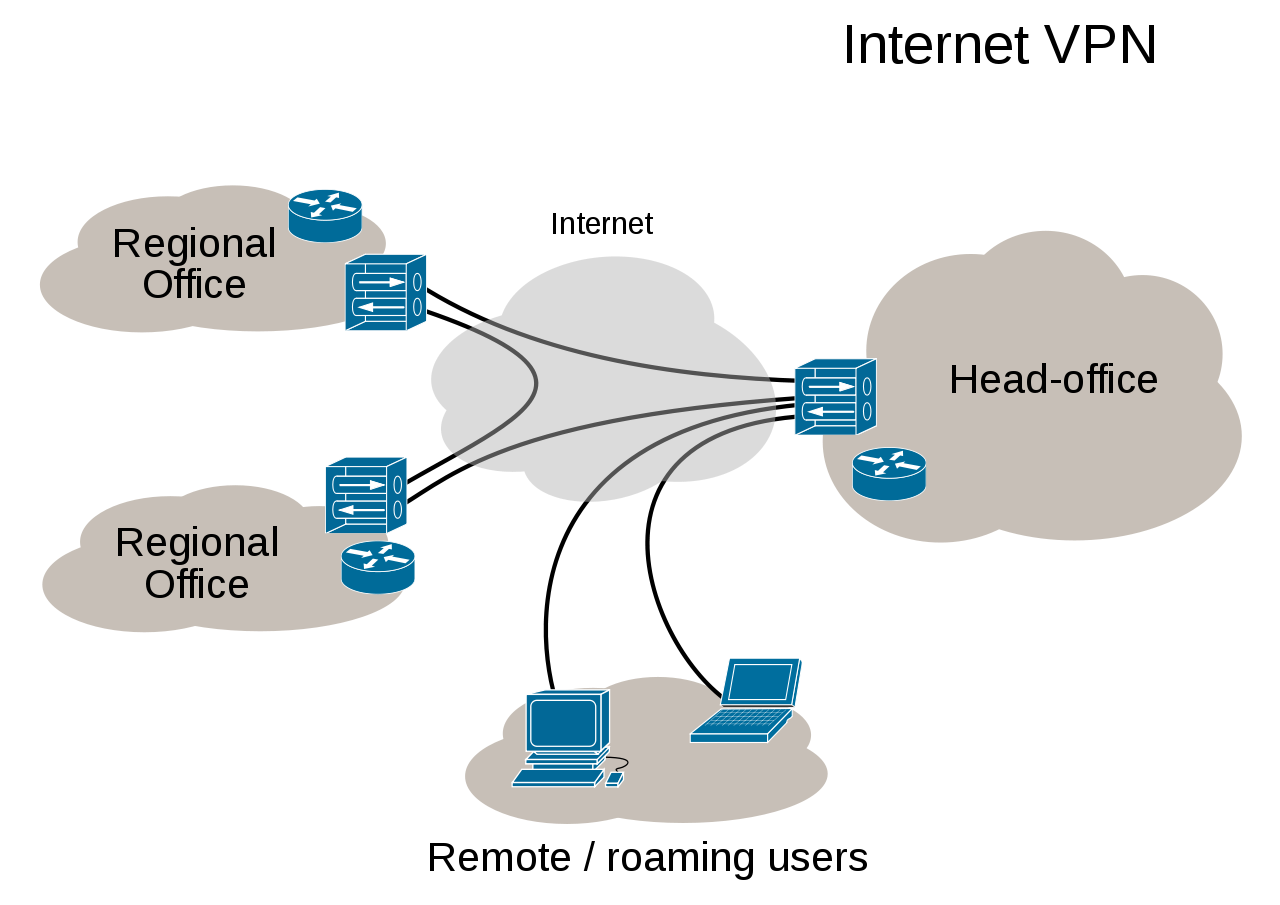
Bij sommige klanten kunnen bepaalde punten van heel groot belang zijn. Denk bijvoorbeeld aan een advocatenkantoor, zij willen een oplossing dat gemakkelijk toegankelijk is, **goed beveiligd** is en aan de nodige **wetten** voldoet.

Aangezien grote bedrijven vaak geografisch verspreid zijn over meerdere locaties en VPN-services niet altijd de favoriete oplossing zijn, is het aan te raden om onderzoek te doen naar de mogelijkheden die de Cloud te bieden heeft. Dergelijke goede functionaliteit gaat dan meestal gepaard met extra mogelijkheden zoals (verder)werken van thuis uit.

### Vergelijking met VPN

De Cloud is uiteraard niet de enige optie voor het wereldwijd toegankelijk maken van data. De VPN-technologie is een andere optie, die reeds door veel bedrijven geïmplementeerd wordt voor tal van redenen. Hoewel deze technologie een must is om bepaalde netwerkmogelijkheden te kunnen voorzien, is het geen ideale vervanger van de Cloud voor data access. Daar is het namelijk te omslachtig voor, en in principe is het er ook niet voor gemaakt.

Bij het opzetten een VPN-verbinding met een bedrijf, zal de gebruiker toegang krijgen tot het bedrijfsnetwerk alsof het zijn eigen thuisnetwerk is. De naam VPN (virtual private network) zegt dan ook veel over de werking van de betreffende technologie. De gebruiker zit niet fysiek in het netwerk, maar heeft wel toegang tot het netwerk, en bij deze dezelfde mogelijkheden als de interne gebruikers.



Figuur 4‑1: Een simpel overzicht van de werking van virtual private networks. [7]

Het grootte voordeel hiervan is meteen ook een nadeel voor het verlenen van data access op deze manier. Tijdens een actieve VPN-verbinding is de gebruiker namelijk virtueel verbonden met *en* *aanwezig in* het interne bedrijfsnetwerk. Dit is dikwijls niet de bedoeling als een gebruiker enkel nood heeft aan wat data uit het bedrijf waar hij of zij de rechten voor heeft. Het is niet nodig om toegang te krijgen tot het interne netwerk voor het ophalen van data. De extra functionaliteit die een VPN-verbinding voorziet, kan een groot beveiligingsrisico inhouden. Indien de beveiliging van de verbinding en de rechten niet strikt genoeg opgesteld zijn, kan de gebruiker via VPN-verbinding toegang krijgen tot extra functionaliteit. Dit brengt extra risico’s naar voren. Het is bovendien moeilijker om gebruikers vanop afstand te beperken en monitoren.

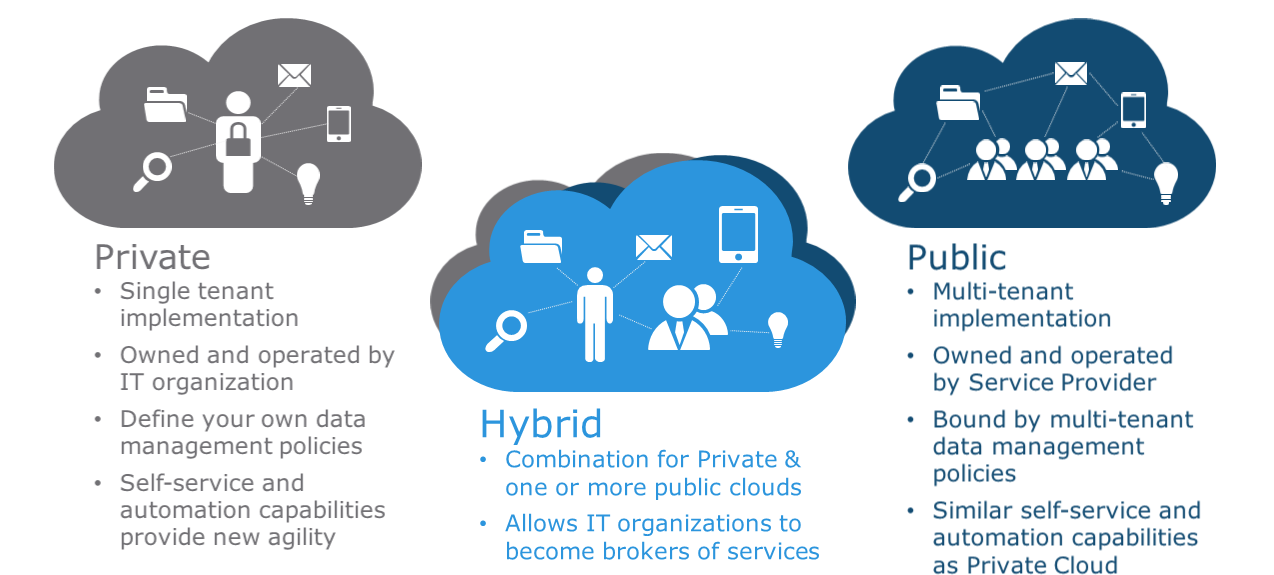
Cloud toegang is dan ook ontwikkeld met de bedoeling van enkel de nodige functionaliteit te voorzien en niet meer. *De verschillende types aan Cloud-oplossingen kan je terugvinden in 4.1.3 hieronder*. Een Cloud opstelling die voorzien is van gemakkelijke toegang tot data, zal alles binnen het netwerk dat geen data inhoudt zo goed mogelijk proberen afschermen van de publieke gebruiker.

**Conclusie:** De meest ideale oplossing tussen VPN en Cloud hangt volledig af van het doel dat men wil bereiken en de personen die er gebruik van zullen maken. Aangezien er in deze situatie enkel nood is aan gemakkelijke toegang tot data en het tevens mogelijk is dat onervaren mensen er gebruik van moeten maken, is een Cloud-oplossing het meest voor de hand liggend. Bovendien zal de Cloud toegang bij veel bedrijven gebruikt worden om klanten toegang te geven tot bepaalde data waar zij leesrecht op moeten hebben (denk opnieuw aan het advocatenkantoor), een VPN-verbinding voorzien voor die klanten zou hier weer een zee van beveiligingsproblemen introduceren.

### Keuze aan Cloud-opstellingen

Men kan een Cloud-opstelling steeds categoriseren onder één van de volgende types:

* Publieke Cloud
* Private Cloud
* Hybride Cloud



Figuur 4‑2: Verschillen tussen private, hybride en publieke Cloud. [8]

[9]

De publieke Cloud wordt tegenwoordig het meest gebruikt. Hierbij zal het bedrijf alle data voor de Cloud opslagen op een publieke server. Deze servers (vooral de “Enterprise”) zijn goed beveiligd en voorzien van veel functionaliteit. De functionaliteit ervan hangt af van de provider van de gekozen Cloud en het type Cloud oplossing, dat men wenst. *(In 4.1.3 kan je de verschillende types aan Cloud oplossingen terugvinden).*

Als men kiest voor een private Cloud zal die Cloud binnen het bedrijf opgesteld worden (on-premises). Bij deze opstelling blijven de gegevens opgeslagen op media dat in de handen van het bedrijf blijft. De controle is hier groter en het bedrijf hoeft de stap niet te zetten om een derde partij te vertrouwen met hun data. Tevens is het gemakkelijker om op deze manier te werken indien het bedrijf rekening moet houden met bepaalde regels en wetgevingen. Uiteraard wilt dit niet zeggen dat een private Cloud omgeving veiliger is dan de publieke, dit hangt volledig af van de mate waarin het bedrijf zijn Cloud omgeving kan beveiligen t.o.v. de publieke Cloud providers. Welk type opstelling globaal gezien het veiligste is, kan moeilijk gezegd worden, al gaat men ervan uit dat publieke Cloud-opstelling van het Enterprise niveau meestal zeer veilig is (enorm weinig geslaagde hackerspogingen hebben zich voorgedaan op Enterprise Cloud omgevingen, ondanks dat er enorm veel crimineel geld te verdienen valt met een geslaagde side-channel attack).

Aangezien de publieke Cloud in sommige gevallen niet aan te raden is (vanwege legale redenen of het gebrek aan vertrouwen van data in andermans handen) zullen de meeste bedrijven opteren voor het gebruik van een private of hybride Cloud omgeving. Indien het bedrijf echter de expertise of het budget ontbreekt voor een on-premises private Cloud zal het wel moeten opteren voor een publieke Cloud-opstelling. Bovendien kruipt er veel meer werk in de opzet van dergelijke Private Cloud-opstellingen. Voor het ophalen en doorsturen van grote bestanden zal dan ook een snelle internetverbinding en hoge bandbreedte met de site nodig zijn, wat weer extra geld kan kosten.

Verder is het nog mogelijk om een gulden middenweg te nemen, er bestaat namelijk ook een hybride Cloud-opstelling. Dit is letterlijk een mengeling van de publieke en private opstelling, en zal dus evenveel (of net iets meer) werk vereisen dan de private opstelling. Dergelijke hybride opstelling opent een wereld aan mogelijkheden voor bedrijven. Enerzijds kan het bedrijf bij gebruik van zo een opstelling alle overgevoelige data (of data met wettelijke verplichtingen) on-premises houden, terwijl het de andere bulk aan minder gevoelige data op publieke servers zet. Deze kunnen dan ook seamlessly integrated zijn in één platform onder éénzelfde web portal met dezelfde authenticatie en autorisatie. Het is ook mogelijk om zonder enige moeite bepaalde data te verplaatsen van de lokale naar de publieke servers of omgekeerd. Deze opstelling wordt dus ook dikwijls gebruikt door bedrijven indien zij stap voor stap willen overschakelen van een publieke naar een private Cloud-opstelling of omgekeerd.

Voor ICORDA is het soms aangeraden of zelfs wettelijk verplicht om een private of hybride opstelling te voorzien voor bepaalde klanten. Deze proef zal een private Cloud-opstelling bevatten, die zal weliswaar aangeboden worden vanuit een Citrix ShareFile omgeving dat zowel publiek, privaat als hybride opgesteld kan worden. Meer over de Citrix ShareFile kan je vinden in 4.2.1.

### Keuze aan Cloud-oplossingen

Zoals in 4.1.2 reeds aangegeven werd, zijn Cloud-voorzieningen vaak ontwikkeld met een specifieke doelstelling in het hoofd. In deze bachelorproef is er nood aan een **Cloud-storage**, dat hoort dan voornamelijk thuis onder het “**Software as a Service**” principe. Maar aangezien deze opstelling gebruik maakt van **ShareFile** om extra functionaliteit te bekomen (bv eigen routerings- en beveiligingsimplementaties d.m.v. de NetScaler, linken van private dataopslag d.m.v. de StorageZone) valt de opstelling in deze bachelorproef **eerder** onder het “**Infrastructure as a Service**” principe. Binnen de Cloud-voorzieningen kan men volgende principes terugvinden:

* Software as a Service (**SaaS**)
* Platform as a Service (**PaaS**)
* Infrastructure as a Service (**IaaS**)

[10]

Alle Cloud gerichte bedrijven bieden oplossingen aan die 1 (of in sommige gevallen meerdere) van de bovenstaande services bieden.

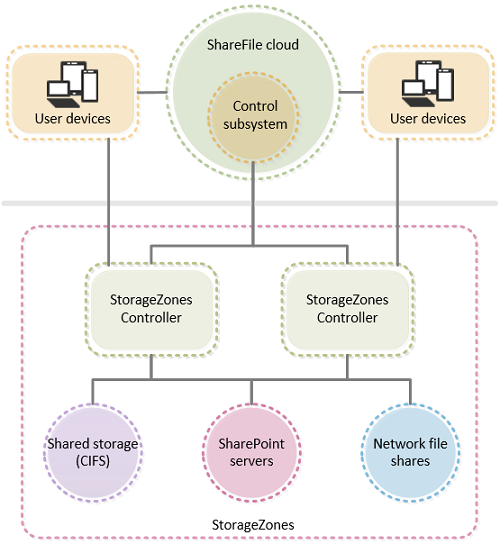
Een SaaS Cloud is in staat om de gebruiker een welbepaald softwarematige oplossing aan te bieden over het internet. Die is dan beschikbaar voor de gebruiker onder de vorm van een applicatie. Deze “*webapplicaties*” kunnen eender wat voorstellen, in dit geval gaat het om een storage oplossing, maar SaaS wordt eveneens aangeboden in de welgekende en veel gebruikte e-mail in de Cloud oplossingen. Zo bestaan er ook volledige Cloud-based softwarepakket zoals Office 365 van Microsoft.

In PaaS oplossingen ligt de functionaliteit aanzienlijk hoger dan in de net besproken SaaS oplossingen. PaaS wordt voornamelijk gebruikt door ontwikkelaars die nood hebben aan een Cloud-oplossing waarin zij mogelijks enige vorm van web-services/webapplicaties kunnen aanbieden aan hun klanten. Door de extra functionaliteit kunnen ontwikkelaars namelijk programmeren en configureren binnenin de Cloud omgeving. De functionaliteit binnen de gekozen PaaS oplossing zal zich dan ook sterk vertalen in de prijs die eraan vasthangt. Volledige functionaliteit (zoals dat lokaal het geval is) is dan ook nooit goedkoop in dergelijke Cloud-oplossingen.

IaaS sluit min of meer aan op het PaaS principe maar biedt meer mogelijkheden op het netwerkniveau. Binnen een IaaS oplossing is het effectief mogelijk om de netwerkinfrastructuur te beheren. Denk bijvoorbeeld aan het integreren van welbepaalde servers, firewalls en andere netwerktoestellen. Het aanmaken van users en beheren van authenticatie horen hier ook dikwijls thuis. In het geval van de ShareFile betekent dat meestal wel dat de functionaliteit beperkt blijft tot het implementeren en configureren van andere Citrix producten en oplossingen. Bij het gebruik van IaaS oplossingen met meer functionaliteit en minder gebondenheid hoort dan ook weer een extra dure kost. Toch zijn de mogelijkheden binnen het aanbod van Citrix producten en oplossingen groot.

### ShareFile

[De Citrix ShareFile slogan](https://www.sharefile.com/enterprise?aid=236117574128&src=google&kw=sharefile&gclid=EAIaIQobChMIusqkqqP92QIVpbvtCh1WQAxaEAAYASABEgLy_fD_BwE) stelt: “Flexible enough to meet enterprise needs. Secure enough to satisfy corporate policies. Easy enough for everyone to use.”



Figuur 4‑3: Diagram van ShareFile met StorageZones opstelling. [11]

Zoals reeds besproken, wordt in de opstelling voor deze bachelorproef een Citrix ShareFile (in combinatie met een Citrix NetScaler en StorageZone) gebruikt. Hier zal verder uitgelegd worden waarvoor ShareFile gebruikt kan worden, waarvoor het specifiek gebruikt wordt in deze toepassing, waarom het een goede oplossing is en wat de alternatieven zijn (inclusief hun voor- en nadelen).

Zoals [de ShareFile website](https://www.sharefile.com/enterprise?aid=236117574128&src=google&kw=sharefile&gclid=EAIaIQobChMIusqkqqP92QIVpbvtCh1WQAxaEAAYASABEgLy_fD_BwE) reeds aangeeft, wordt ShareFile voornamelijk gebruikt als Cloud-Storage. Daarbij is het wel voorzien van extra functionaliteit en security. Zo is die storage heel flexibel (denk aan de hybride mogelijkheden met lokale StorageZones), het geeft mogelijkheden zoals “easy web access” en “single sign-on” (SSO) kan hier gebruikt worden voor al uw webapps in combinatie met ShareFile), het voorziet opties voor het aanmaken van gebruikers en groepen en voor het beheer van de rechten.

In deze opstelling zal de ShareFile Cloud gebruikt worden als private Cloud in combinatie met een StorageZone, hij zal dus in verbinding staan met een StorageZone Controller (installatie en configuratie op een lokale fileserver) en een NetScaler die alle routering en authenticatie regelt. Bovendien zal de NetScaler ook zorgen voor load balancing en high availability *(meer over de NetScaler kom je te weten in 4.2.2)*.

Uiteraard is de Citrix ShareFile *volgens ICORDA* een favoriet voor de job aangezien het bedrijf reeds vele Citrixproducten gebruikt en dusdanig comptabiliteit garandeert. Maar, ook in vergelijking met andere Enterprise Cloud-storage producten springt ShareFile er dikwijls bovenuit. Ondanks talrijke prachtige Cloud-storage oplossingen voor bedrijven zoals “OneDrive for Business”, “Dropbox for Business”… Zijn er slechts enkelen die een gelijkaardige functionaliteit en feature set bieden als ShareFile. Twee alternatieven die er bovenuit komen zijn [ownCloud](https://owncloud.com/enterprise-edition/) en [Syncplicity](https://www.syncplicity.com/features/) Enterprise Edition.

OwnCloud is een private Cloud oplossing die voorzien is van een enorm aanbod aan features die gaan van volledige een samenstelbare encryptie (waar de user alle instellingen zelf kan kiezen) tot verhoogde Cloud monitoring capaciteiten, file firewall en antivirus implementatie. Op vlak van customizability reiken de mogelijkheden bij ownCloud nog verder dan bij ShareFile, langs de andere kant is ShareFile voorzien van een aantal Enterprise features die ownCloud niet biedt op dit moment (zoals 2FA en nieuwere authenticatie protocollen), voor bedrijven die daar nood aan hebben is ShareFile dan ook nog steeds (naar mijn mening) de beste oplossing. [12]

Nr. 2 in de lijst aan waardevolle concurrenten voor ShareFile is Syncplicity. Syncplicity is een heel goed alternatief voor ShareFile maar mankeert 2 belangrijke zaken om te voldoen aan alle Enterprise eisen. De support blijkt heel zwak te zijn. De hoeveelheid applicaties die implementeerbaar zijn in de minder gekende Cloud is heel beperkt (geen Office, Google Docs… integratie). [13]

Men kan besluiten dat ShareFile voor ICORDA en klanten, alsook andere bedrijven, één van de beste Enterprise Cloud-storage oplossingen is.

## Netwerkvoorzieningen

Voor de opstelling van de bachelorproef maak ik gebruik van speciale virtuele servers en Active Directory integratie. Hier volgt een lijstje van alle netwerkcomponenten en –voorzieningen die nodig zijn bij het maken van de opstelling:

**Componenten**

* Citrix ShareFile
* Citrix NetScaler
* Citrix StorageZone Controller
* Active Directory server

**Voorzieningen**

* Active Directory en Domain Name System
* content switching services
* load balancing services
* AAA-services
* high availability
* data met bijhorende rechten
* gebruikers met bijhorende credentials
* certificaten
* extra beveiligingsmaatregelen

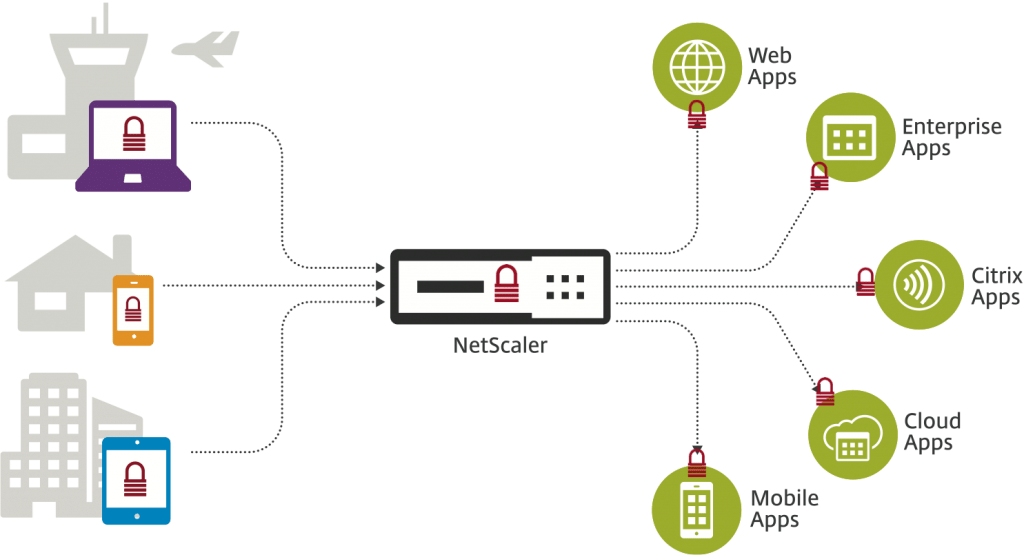
[Link naar een soortgelijke opstelling inclusief enkele netwerkvoorzieningen en componenten.](https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/single-sign-on-for-sharefile-with-netscaler.pdf)

[14], [6]

### Citrix ShareFile

Dit is de hybride Cloud die gebruikt wordt in verbinding met een lokale StorageZone en de Citrix NetScaler, deze werd reeds besproken doorheen deze voorstudie. *Lees 4.1.4 voor meer informatie over de Citrix ShareFile.*

### Citrix NetScaler



Figuur 4‑4: Algemene werking van een Citrix NetScaler. [15]

Dit is een ruim voorziene virtuele server die in staat is van verkeer te routen en het netwerk te beveiligen. De features van dit Citrix product zijn immens, in deze opdracht zal hij voornamelijk gebruikt worden als authenticatie en load balancing server voor de ShareFile en StorageZone. Er zijn verschillende NetScaler producten op de markt, voor deze opdracht wordt gebruik gemaakt van de NetScaler VPX die ontwikkeld is voor gebruik op virtuele servers. De hoofdfuncties zijn voornamelijk remote access infrastruture, content switching, load balancing, high availability, VPN-access, network firewall en policy management. [16]

De enige echte concurrent van de Citrix NetScaler is de F5 van F5 networks. Beiden bieden een bijna identiek product. De meningen over welke de betere is zijn divers, maar voor beiden zijn de pro en contra argumenten beperkt. Enerzijds wordt de NetScaler het meest aangeraden voor bedrijven die andere Citrix producten gebruiken, dit is dan ook bij velen het geval (ook het gekende StoreFront is een product van Citrix). Anderzijds werkt de F5 ook perfect samen met Citrix producten zoals StoreFront en de support ervoor is van een veel hoger Niveau, maar ook daar zit weer een tegenargument aan verbonden, Citrix support is inbegrepen in de prijs voor Enterprise producten, terwijl daar bij F5 een gigantisch prijskaartje aan vasthangt. De leercurve voor F5 zou iets lager liggen maar er zijn dan weer iets meer diepgaande details in de configuratie van een NetScaler. Uiteraard moet in deze opdracht met veel minder rekening gehouden worden, er zijn wel enkele basic Citrix producten die gebruikt zullen worden, maar een zeer gelijkaardige opstelling was ook mogelijk met de F5, alleen zou men daar met 2 grote problemen zitten. Ten eerste de F5 heeft geen software-only variant zoals de VPX bij NetScaler en ten tweede, de F5 is dan ook een veel duurdere aankoop als hardwarecomponent (dit is uiteraard ook het geval voor een Citrix hardware NetScaler zoals de MPX). [17], [18], [19]

### Citrix StorageZone Controller

De controller is de server die de verbinding legt tussen de ShareFile Cloud en de lokale storage, om private data beschikbaar te maken in de Cloud. In deze opstelling is de lokale date storage server ook opgezet als de StorageZone Controller. Om de server om te vormen tot een Citrix StorageZone Controller gebruikt men de StorageZones Controller executable van Citrix. Enkele voordelen die terug te vinden zijn op [de StorageZones Controller website](https://docs.citrix.com/en-us/storagezones-controller/5-0/about.html) luiden als volgt:

* Naleven van wettelijke eisen
* Optimale locaties gebruiken voor de opslag (vlak bij gebruikers voor performantie bijvoorbeeld)
* Maakt van de publieke ShareFile Cloud een hybride
* Flexibiliteit van de StorageZone, deze kan ook in een andere Cloud van derden geplaatst worden
* Veilige toegang tot lokale data van buitenaf
* Centraal beheer en weergave van verschillende opslagruimtes verspreid over de hele wereld
* Snel uploaden, downloaden, online bekijken en bewerken van data vanop elk type toestel

[11]

### Domain Name System

Het Domain Name System (DNS) wordt gebruikt om namen naar IP-adressen om te zetten (of omgekeerd). Het is een veel voorkomend systeem dat overal gebruikt wordt en door alle systemen ondersteund wordt. Het houdt een simpele mapping bij tussen de namen en de bijhorende IP-adressen die gekend zijn door de DNS-server.

Omdat deze opstelling een realistische bedrijfssituatie weerspiegelt, wordt er hier ook gebruik gemaakt van een DNS-server. De interne DNS-server bezit gegevens van de Fileserver, NetScaler en de Users (lokale computers). Telkens wanneer een computersysteem gegevens moet verzenden naar een ander systeem met een bepaalde naam, zal het de nodige informatie (het IP-adres van dat systeem) opvragen bij de DNS-server.

### Active Directory

Active Directory (AD) is een gigantische mappenstructuur die volledig gevuld is met objecten die “value-string pairs” bevatten. Er kan enorm veel informatie opgeslagen worden in een AD. Maar voornamelijk wordt het gebruikt om basisgegevens over groepen, gebruikers en computersystemen in het domein bij te houden. Zo zal een domein minstens 1 AD-server bevatten voor het bijhouden van die gegevens, van zodra het domein te groot of onderverdeeld wordt zullen er extra AD-servers toegevoegd worden aan dat domein of aan de subdomein(en). Ook wanneer een single point of failure vermeden wordt zal de AD-domeincontroller ontdubbeld worden, op deze manier kan men binnen het domein high availability proberen te bereiken.

Deze opstelling maakt gebruik van een Microsoft AD-server. De voornaamste gegevens die van belang zijn in deze opstelling zijn de gebruikersgegevens, voornamelijk de logingegevens. De NetScaler zal deze gegevens nodig hebben om een login poging op de ShareFile al dan niet door te laten.

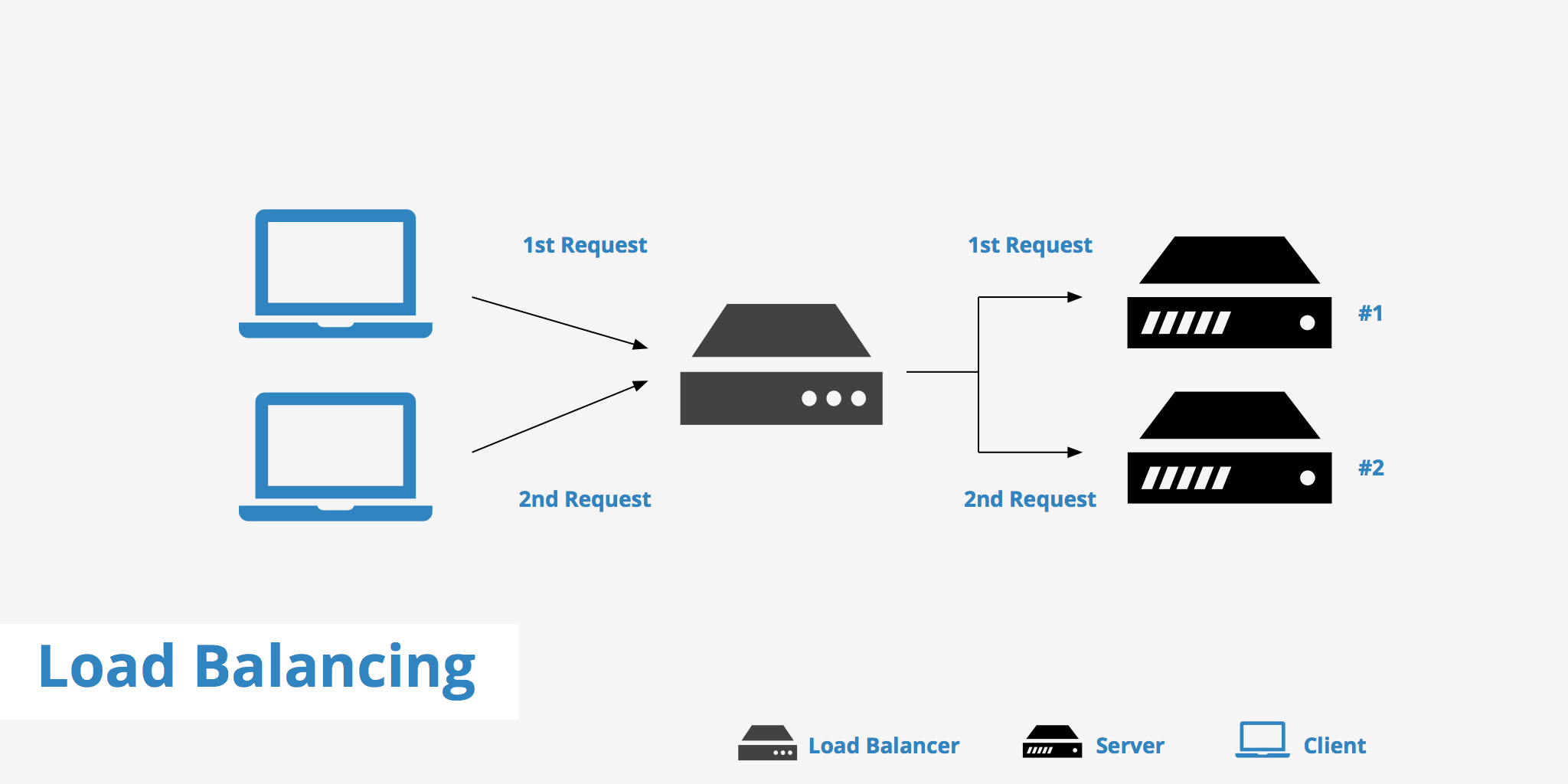
### NetScaler Traffic management

Eén van de voornaamste functies van de NetScaler in deze opstelling is zijn Traffic management. In tegenstelling tot de typische hedendaagse routers kan de NetScaler verkeer regelen op een hoger niveau. Dat wil zeggen dat de NetScaler bijvoorbeeld verkeer kan routen op basis van informatie in de get en post velden van een URL, of op basis van het type verkeer dat verstuurd wordt. Dergelijke functionaliteit zal heel nuttig zijn tijdens de opstelling. [20]

#### Content switching

Eén van de traffic managing services in de NetScaler is de content switching service. Deze zal, afhankelijk van de gekozen instellingen en policies, het verkeer routeren naar de correcte server. Zoals meestal het geval is, wordt ook in deze opstelling het verkeer naar een load balancing server gerouteerd. In grotere opstellingen kan het zijn dat er nog load balancing servers toegevoegd worden voor verkeer naar andere zaken zoals SoreFront of SharePoint servers. In dat geval zal de content switching server verder geconfigureerd worden en meer policies bevatten om het verkeer naar de correcte server te kunnen routeren. [20]

#### Load balancing



Figuur 4‑5: De werking van een Load Balancer. [21]

Zoals je in figuur 4-5 ziet, zal de Load Balancer het verkeer verdelen over de servers waarvoor het bestemd is. In deze opstelling staan er fileservers achter de Load Balancer waarop de private Cloud data zich bevindt. Deze functie is uiteraard enkel effectief wanneer de betreffende server ook ontdubbeld aanwezig is. Bij het plaatsen van een tweede server als kopie van de oorspronkelijke, biedt een load balancer de mogelijkheden om het huidige verkeer naar server 1 te halveren en andere helft van dat verkeer naar server 2 te sturen. De load balancing server (of kortweg load balancer) wordt ook geconfigureerd a.d.h.v. instellingen en policies.

In deze opstelling zal de load balancer nuttig worden van zodra enkele virtuele servers ontdubbeld worden voor het bekomen van high availability en in dit geval dus ook extra performantie. [20]

#### AAA

AAA staat voor Authentication, Authorization en Accounting.

**Authenticatie** gebeurt tijdens de login. Wanneer een gebruiker inlogt gaat hij door het authenticatieproces. Meestal geeft die gebruiker dan zijn gebruikersnaam en wachtwoord in (in het geval van SSO kan dit geautomatiseerd worden zodat de ShareFile login gebeurt a.d.h.v. de gebruikers hun AD-gegevens). Indien de logingegevens niet kloppen zal de gebruiker niet ingelogd geraken, indien de gegevens wel overeenkomen met een gebruikersnaam-passwoord entry in de database zal de gebruiker inloggen en bepaalde rechten toegewezen krijgen. Als de gebruiker bepaalde acties onderneemt na het inloggen dan moet hij voor die commando’s geautoriseerd zijn, dit autorisatieproces is meestal afhankelijk van het gebruikersprofiel. De **autorisatie** wordt dus meestal al bepaald tijdens de authenticatie, soms is het echter mogelijk dat voor bepaalde acties/commando’s extra autorisatie of een andere vorm van autorisatie vereist wordt (bv 2FA verificatie of een wachtwoord of beveiligingsvraag ingeven voor het aanpassen van gevoelige zaken). **Accounting** is een vorm van loggen waarbij gegevens over het systeem en de gebruiker continu berekend en opgeslagen worden. *(In de NetScaler worden de resultaten van de accounting standaard weergegeven op het Dashboard, extra accounting kan bereikt worden met de AAA-service.)* [22]*,* [23]*,* [24]

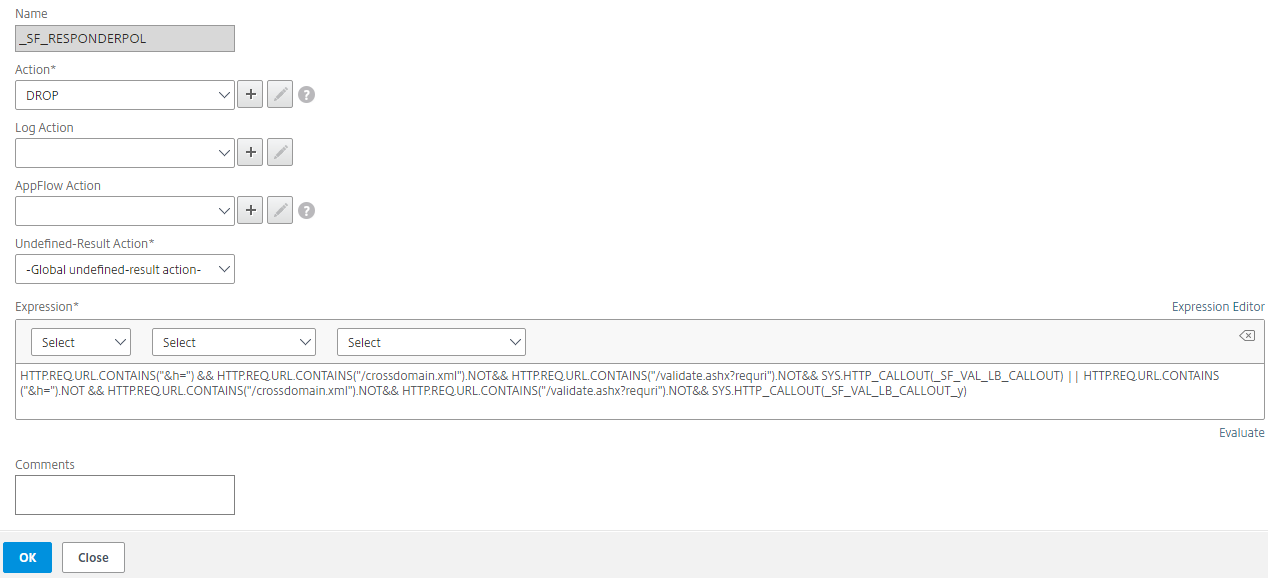
Net zoals dat bij de content switching en load balancing services het geval was, zal de functionaliteit van de AAA-service ook afhangen van de instellingen en policies die gebruikt worden tijdens het configureren van de server. [20]

Authenticatie is de meest gebruikte functie van de NetScaler zijn AAA-service in deze opstelling, meer informatie over Authenticatie volgt in 4.3.

#### Policies

Zoals reeds vermeld werd, zijn policies van groot belang bij het configureren van de services in de NetScaler. De NetScaler functioneert voornamelijk door de policies die de administrator heeft opgesteld en gekoppeld aan de verschillende servers en services.

Elk type policy in de NetScaler heeft gelijkaardige attributen, ze verschillen slechts in een paar kleinigheden en ze worden uiteraard ook anders ingevuld. Men kan dus zeggen dat een policy in de NetScaler een algemene structuur volgt, en die ziet er als volgt uit.



Figuur 4‑6: Opstellen van een policy in NetScaler.

* Policy name: De naam die gegeven wordt aan de policy, policies worden gelinkt aan servers/services op basis van hun naam.
* Action: **Wat** er gedaan moet worden indien het de policy matcht. Dit is de echte actieve inhoudt van de policy, de actie die ondernomen wordt.
* Extra (speciale) Actions.
* Expression: Dit toont aan **wanneer** de policy matcht met het verkeer en de actie mag uitgevoerd worden.

### High availability

High availability (HA) is een begrip dat steeds meer gebruikt wordt en waar steeds meer naar gestreefd wordt. Wanneer over HA gesproken wordt, bedoelt men dat een opstelling actief en online moet blijven wat er ook gebeurd. M.a.w. is het de bedoeling dat de opstelling, alsook alle gevoelige componenten binnen de opstelling, ontdubbeld worden zodat het uitvallen van eender welke component geen impact heeft op prestaties van de volledige opstelling. Natuurlijk heeft elke opstelling zo zijn beperkingen, men kan nooit 100% zeker zijn dat een opstelling blijft werken ongeacht de rampen die zich voordoen. Het is wel zo dat er tegenwoordig enorm veel moeite gedaan wordt en geld besteed wordt aan het creëren van een redundante HA-opstelling. Zo zullen grote bedrijven zelfs hun volledige ICT-infrastructuur ontdubbelen over verschillende locaties op aarde, zodat natuurrampen geen desastreuze gevolgen zouden hebben voor de uptime.

Mijn opstelling zal ook zo redundant mogelijk gemaakt worden, rekening houdend met de beperkingen in tijd en geld, maar dat is een extra doelstelling voor op het einde eens de proef af is. Daarbij zou het de moeite waard zijn om StorageZone Controller, NetScaler en AD-server te ontdubbelen.

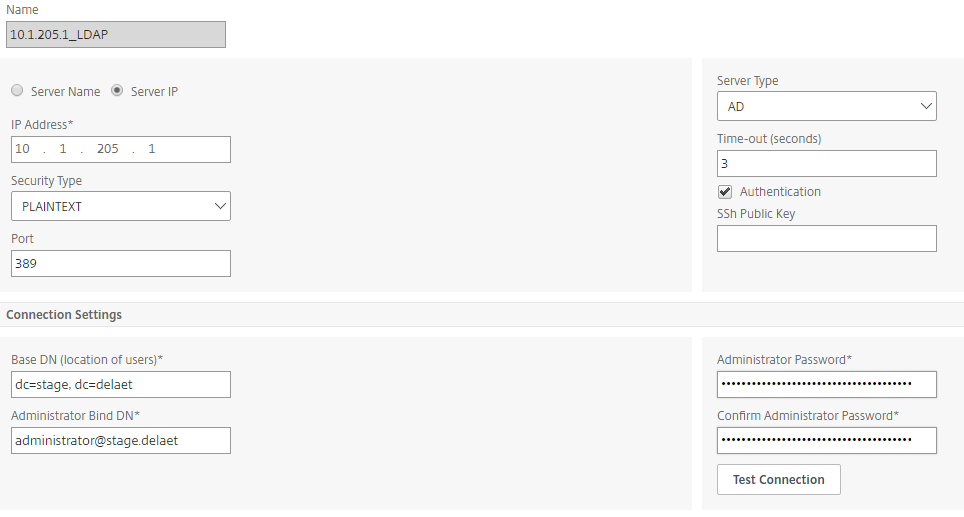
## Authenticatie

Zoals eerder vernoemd in 4.2.6.3 is authenticatie een belangrijke functie van de AAA-server in deze opstelling. Veel tijd zal dan ook gespendeerd worden aan het implementeren van een goede authenticatie. Daarom was het goed om hier extra vooronderzoek naar te doen. Uiteraard hoort dit onderwerp bij de beveiliging van de opstelling en dat is in een bedrijfsomgeving dan ook een superbelangrijke factor die steeds op punt moet staan. In de authenticatie voor deze opstelling worden 2 belangrijke zaken verwerkt, enerzijds de AD-gegevens en anderzijds het SSO-framework.

In een bedrijfsomgeving is het zeker aangeraden om de werknemers zo weinig mogelijk accounts te laten creëren zodat ze zo weinig mogelijk wachtwoorden moeten onthouden. Op die manier zullen ze ook een moeilijker wachtwoord kiezen. Bovendien zijn er veel accountspolicies in een AD-domein dat de gebruikers daartoe verplichten. Het zou dus ideaal zijn moesten deze AD-accounts gebruikt kunnen worden om aan te melden wanneer een gebruiker data opvraagt uit de StorageZone. Dit zou de situatie voor hun veel efficiënter en gemakkelijker maken.

### AD-integratie

NetScaler geeft de mogelijkheid voor het aanmaken van LDAP policies dat, indien goed geïmplementeerd, de mogelijkheid geeft om aan te melden met AD-credentials bij het opvragen van data uit de StorageZone. Het is dus mogelijk om AD te integreren in een setup zoals deze dat gebruik maakt van een NetScaler. [14]



Figuur 4‑7: Opstellen van de LDAP server en service in NetScaler.

### SSO

Door middel van single sign-on kunnen die AD-credentials gebruikt worden in web-portals die verbonden zijn met de NetScaler. Er zijn verschillende implementaties van SSO met SAML, OAuth, OpenID en RADIUS als bekendste. Elk van de net genoemde frameworks werkt op een andere manier, maar allen bereiken ze hetzelfde resultaat en met een heel gelijkaardig verloop. Wanneer SSO gebruikt wordt kan een gebruiker zich aanmelden (of authentiseren) voor verschillende services met slechts 1 combinatie aan logingegevens. De gebruiker vraagt eerst de loginpagina op voor de web-service die hij wenst te raadplegen, de service provider (hier de NetScaler) verwijst hem door naar de correcte identity provider, die antwoordt met de gegevens die nodig zijn voor de authenticatie. Indien de gebruiker correct authentiseert ontvangt hij beveiligingsgegevens van service provider waarmee hij de web-service nogmaals kan opvragen, met deze gegevens krijgt hij meteen toegang en kan de gebruiker inloggen.

Merk op, SSO wordt ook wel DaaS Directory as a Service genoemd, omdat het AD-functionaliteit als een service voor andere applicaties aanbiedt.

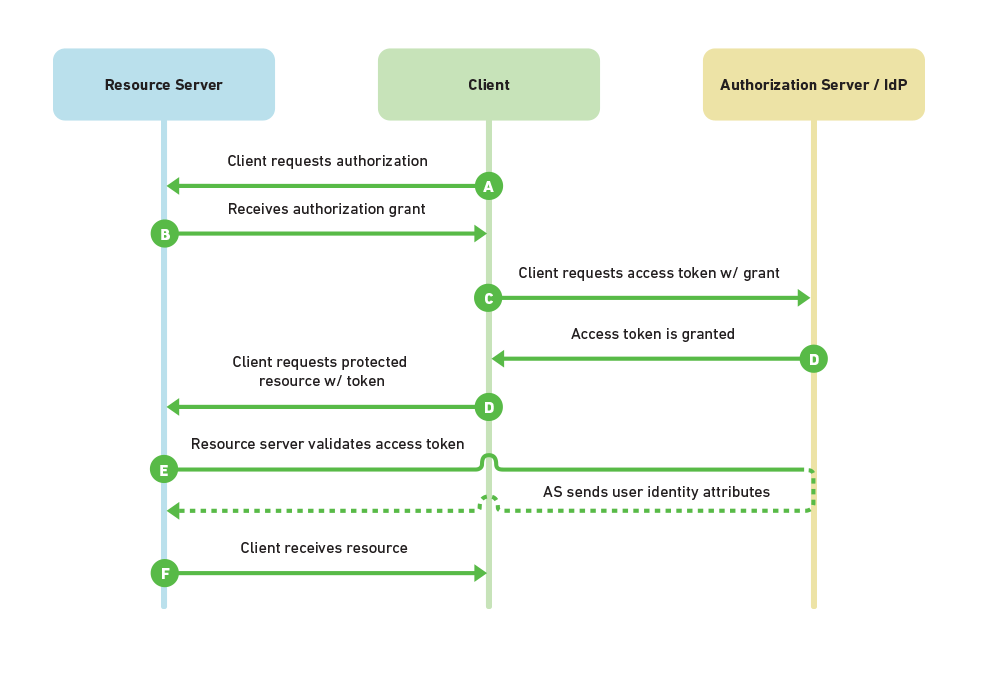
[14], [25] [26] [27]

#### OAuth

SSO is een principe dat de laatste jaren steeds meer gebruikt wordt, zowel door alledaagse gebruikers als bedrijven. Het is een prachtig principe dat de user experience bij het aanmelden voor applicaties sterk kan verbeteren. Ondanks dat de technologie reeds meer dan 15 jaar bestaat, heeft het zijn ruime adoptie pas bereikt in de laatste jaren. Uiteraard verandert er heel veel in 15 jaar tijd op vlak van de ICT en dus ook op vlak van de beveiliging en principes voor het inloggen op (web)applicaties. Het is daarom belangrijk dat de protocollen die het SSO-principe implementeren zo goed mogelijk up to date blijven.

De meest gekende en 1 van de oudste protocollen dat het SSO-principe ondersteunt is Microsofts SAML (Security Assertion Markup Language). Het SAML framework werd door de OASIS SSTC gedefinieerd in januari 2001. Sindsdien is het enkele keren aangepast, met versie 2.0 (2005) als laatste versie. SAML 2.0 is dus sterk verouderd, dit zorgt vooral voor een groot gebrek aan functionaliteit maar ook voor overhead en een minder sterke beveiliging. Om die reden is het beter om gebruik te maken van een recenter framework, of een framework dat doorheen de tijd onderhouden bleef. [28]

De meest recente OAuth standaard zou het gunstigste alternatief zijn. OAuth staat voor OAuth (Open Authorization) en voorziet dus voornamelijk de autorisatie van de user voor de gegevens die hij probeert op te vragen en te commando’s die hij probeert uit te voeren *(zie 4.2.6.3 voor extra uitleg over autorisatie)*. Ondanks dat OAuth als autorisatie standaard niet speciaal ontwikkeld is voor authenticatie, kan het SSO-principe toch perfect geïmplementeerd worden door de OAuth standaard te gebruiken. In deze opstelling zal dan ook het nieuwere OAuth autorisatie principe geïmplementeerd worden.



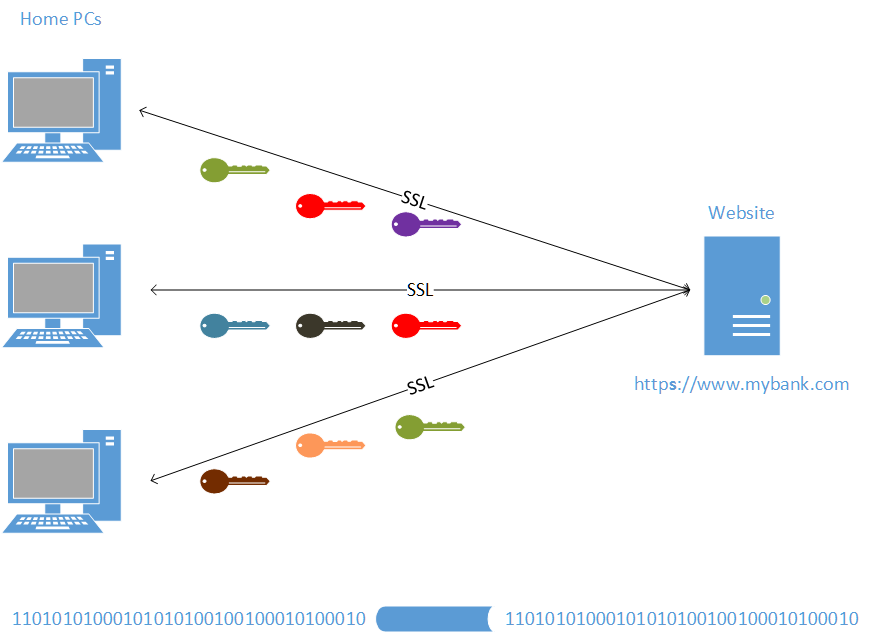
Figuur 4‑8: Schema van het OAuth autorisatieproces [29]

Zoals je op figuur 4-2 kan zien, zal het OAuth SSO-proces starten vanuit de cliënt (meestal een webbrowser) die wilt autoriseren met een “resource server”. Indien de cliënt kan bewijzen aan de “Resource Server” dat hij beschikt over de juiste rechten om te autoriseren met de “Authorization Server” zal hij een “authorization grant” ontvangen. Die grant kan hij dan gebruiken om een requests access token aan te vragen bij de “authorization server”. Met dat token kan hij aan de bijhorende gegevens indien hij dat nodig acht. [30], [31]

Aangezien OAuth een standaard is, en dus eerder een set van richtlijnen i.p.v. een set vaste regels, is het mogelijk om frameworks te schrijven die gebruik maken van de OAuth standaard en zaken toevoegen waar nodig. Zo is OpenID een heel gekend framework dat gebaseerd is op de OAuth standaard. Gebruik makend van dit framework kan het SSO-principe ook geïmplementeerd worden. De voordelen van OpenID zijn voornamelijk gericht naar Mobiele applicaties waarvan in deze optelling geen gebruik gemaakt wordt. [32], [33]

## Extra beveiligingsimplementaties

Buiten de authenticatie voor het inloggen op de ShareFile zijn er nog enkele beveiligingsimplementaties die van pas komen in de opstelling. Aangezien deze opstelling veel gebruikt zal worden om van buitenaf (op het publieke internet) verbinding te maken met de ShareFile Cloud, moet die verbinding uiteraard goed beveiligd zijn. Om de verbinding van een goede beveiliging te voorzien zal al het verkeer tussen de cliënt en de IDP (identity provider) en SP (service provider) steeds geëncrypteerd worden. De encryptie zal tot stand gebracht worden door gebruik te maken van het https-protocol. Daarom zullen het ICORDA wildcard certificaat en de root certificaten van ICORDA’s CAs (certificate authorities) geïmporteerd moeten worden waar nodig. Bovendien zulle zeer beveiligde cipher groups voorzien worden zodat elke https-verbinding enkel sterk geëncrypteerd kan verlopen met een hoge beveiliging en PFS perfect forward secrecy. PFS maakt het mogelijk voor de verbinding om -indien ze gehackt wordt- enkel dat verkeer van die sessie dat gehackt werd bloot te geven en geen andere sessies of gevoelige informatie van die gebruiker. Moest op die manier een hacker toch ooit door de https-beveiliging geraken en het verkeer kunnen uitlezen, dan is de kans groot dat hij daarmee enkel het oude wachtwoord van de gebruiker te weten komt. Indien de bedrijfspolicy werknemers verplicht om hun wachtwoord op regelmatige basis aan te passen, kan dit grote problemen vermijden moest een hack ooit plaatsvinden.



Figuur 4‑9: De werking van perfect forward secrecy door gebruik van verschillende session keys. [34]

# Praktische uitwerking

# Algemeen besluit

# Figuurlijst

[Figuur 1‑1: De voordelen van ISO 9001 gecertificeerde bedrijven. [2] 10](#_Toc509850452)

[Figuur 1‑2: De bedrijfsstructuur van ICORDA NV 11](#_Toc509850453)

[Figuur 1‑3: De verschillende niveaus waaruit een netwerkopstelling en oplossingen bestaan. [5] 13](#_Toc509850454)

[Figuur 2‑1: Het diagram van de bachelorproef opstelling, ShareFile met NetScaler en StorageZones. [6] 15](#_Toc509850455)

[Figuur 4‑1: Een simpel overzicht van de werking van virtual private networks. [7] 18](#_Toc509850456)

[Figuur 4‑2: Verschillen tussen private, hybride en publieke Cloud. [9] 19](#_Toc509850457)

[Figuur 4‑3: Diagram van ShareFile met StorageZones opstelling. [11] 21](#_Toc509850458)

[Figuur 4‑4: Algemene werking van een Citrix NetScaler. [15] 23](#_Toc509850459)

[Figuur 4‑5: De werking van een Load Balancer. [20] 26](#_Toc509850460)

[Figuur 4‑6: Opstellen van een policy in NetScaler. 27](#_Toc509850461)

[Figuur 4‑7: Opstellen van de LDAP server en service in NetScaler. 29](#_Toc509850462)

[Figuur 4‑8: Schema van het OAuth autorisatieproces [27] 30](#_Toc509850463)

[Figuur 4‑9: De werking van perfect forward secrecy door gebruik van verschillende session keys. [34] 31](#_Toc509850464)

# Bibliography

|  |  |
| --- | --- |
| [1] | ICORDA, „over-icorda,” ICORDA NV, 2016. [Online]. Available: https://www.icorda.be/icorda/over-icorda/. [Geopend 19 Maart 2018]. |
| [2] | K. Sutaria, „Benefits of ISO Certification for Startups & Small Businesses,” startupguys, 08 Maart 2016. [Online]. Available: https://www.startupguys.net/benefits-of-iso-certification-for-startups-small-businesses/. [Geopend 19 Maart 2018]. |
| [3] | „ISO\_9000,” Wikipedia, 18 Maart 2018. [Online]. Available: https://en.wikipedia.org/wiki/ISO\_9000. [Geopend 19 Maart 2018]. |
| [4] | J. V. Maldeghem, „ISO 9001 essentials,” Gent, 2017. |
| [5] | P. Tack, „Bedrijfsvoorstelling voor typografics,” Gent. |
| [6] | „Configure NetScaler for StorageZones Controller,” Citrix, 12 Maart 2018. [Online]. Available: https://docs.citrix.com/en-us/storagezones-controller/5-0/install/configure-netscaler.html. [Geopend 28 Februari 2018]. |
| [7] | „Virtual private network,” Wikipedia, 22 Maart 2018. [Online]. Available: https://en.wikipedia.org/wiki/Virtual\_private\_network. [Geopend 22 Maart 2018]. |
| [8] | „Private vs. Public vs. Hybrid Cloud: Which One to Choose?,” impressico business solutions, 2018. [Online]. Available: http://www.impressico.com/2015/11/05/private-vs-public-vs-hybrid-cloud-which-one-to-choose/. [Geopend 26 Maart 2018]. |
| [9] | S. Morris, „Cloud Types: Private, Public and Hybrid,” asigra, 8 September 2011. [Online]. Available: http://www.asigra.com/blog/cloud-types-private-public-and-hybrid. [Geopend 16 Februari 2018]. |
| [10] | Apprenda, „IaaS, PaaS, SaaS (Explained and Compared),” apprenda, 2018. [Online]. Available: https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/. [Geopend 17 Februari 2018]. |
| [11] | „About ShareFile StorageZones Controller,” Citrix, 05 April 2017. [Online]. Available: https://docs.citrix.com/en-us/storagezones-controller/5-0/about.html. [Geopend 12 Februari 2018]. |
| [12] | ownCloud, „enterprise-editioin,” ownCloud, 2018. [Online]. Available: https://owncloud.com/enterprise-edition/. [Geopend 20 Maart 2018]. |
| [13] | J. Gildred, „syncplicity-review,” cloudwards, 20 September 2017. [Online]. Available: https://www.cloudwards.net/syncplicity-review/. [Geopend 21 Maart 2018]. |
| [14] | Citrix, „Single sign-on for ShareFile with NetScaler,” 2015. [Online]. Available: https://www.citrix.com/content/dam/citrix/en\_us/documents/products-solutions/single-sign-on-for-sharefile-with-netscaler.pdf. [Geopend 28 Februari 2018]. |
| [15] | msandbu, „Setting up Unified Gateway on Netscaler 11,” Wordpress, 23 Juni 2015. [Online]. Available: https://msandbu.wordpress.com/2015/06/23/setting-up-unified-gateway-on-netscaler-11/. [Geopend 14 Februari 2018]. |
| [16] | Citrix, „netscaler-vpx,” 2016. [Online]. Available: https://www.citrix.com/products/netscaler-adc/resources/netscaler-vpx.html. [Geopend 21 Maart 2018]. |
| [17] | Citrix, „why choose NetScaler over F5,” 2014. [Online]. Available: https://www.citrix.fi/products/netscaler-adc/resources/netscaler-vs-f5.html. [Geopend 22 Maart 2018]. |
| [18] | „Compare Citrix vs F5 Networks in Application Delivery Controllers,” gartner, 2018. [Online]. Available: https://www.gartner.com/reviews/market/application-delivery-controllers/compare/citrix-vs-f5-networks. [Geopend 22 Maart 2018]. |
| [19] | Citrix, Regisseur, *NetScaler vs. F5 - 4 key technical differentiators.* [Film]. Citrix, 2015. |
| [20] | Citrix, „NetScaler 12.0,” Citrix, 28 April 2017. [Online]. Available: https://docs.citrix.com/en-us/netscaler/12.html. [Geopend 12 Februari 2018]. |
| [21] | KeyCDN, „Load Balancing,” proinity LLC, 29 Juni 2017. [Online]. Available: https://www.keycdn.com/support/load-balancing/. [Geopend 23 Maart 2018]. |
| [22] | „AAA Overview,” etutorials, 2018. [Online]. Available: http://etutorials.org/Networking/Router+firewall+security/Part+II+Managing+Access+to+Routers/Chapter+5.+Authentication+Authorization+and+Accounting/AAA+Overview/. [Geopend 01 Maart 2018]. |
| [23] | „AAA & NAS,” tutorialspoint, 2018. [Online]. Available: https://www.tutorialspoint.com/radius/aaa\_and\_nas.htm. [Geopend 01 Maart 2018]. |
| [24] | „Authentication Authorization and Accounting (AAA),” techopedia, 2018. [Online]. Available: https://www.techopedia.com/definition/24130/authentication-authorization-and-accounting-aaa. [Geopend 01 Maart 2018]. |
| [25] | G. Keller, „Implications of Web Application Single Sign-On,” jumpcloud, 28 May 2017. [Online]. Available: https://jumpcloud.com/blog/web-application-single-sign-on/. [Geopend 14 Februari 2018]. |
| [26] | S. Peyrott, „What is and how does Single Sign On Authentication work?,” auth0, 23 September 2015. [Online]. Available: https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/. [Geopend 14 Februari 2018]. |
| [27] | M. S, „how does saml work,” gluu, 19 December 2012. [Online]. Available: https://www.gluu.org/blog/how-does-saml-work-idps-sps/. [Geopend 14 Februari 2018]. |
| [28] | J. Kurtto, „The Difference Between SAML 2.0 and OAuth 2.0,” ubisecure, 03 Juli 2017. [Online]. Available: https://www.ubisecure.com/uncategorized/difference-between-saml-and-oauth/. [Geopend 15 Februari 2018]. |
| [29] | „Federated SSO, A Primer (SAML, OAuth 2.0, OpenID Connect),” M&S Consulting, 28 Januari 2018. [Online]. Available: https://www.mandsconsulting.com/federated-sso-a-primer-saml-oauth-2-0-openid-connect/. [Geopend 15 Februari 2018]. |
| [30] | M. Anicas, „An Introduction to OAuth 2,” digitalocean, 21 Juli 2014. [Online]. Available: https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2. [Geopend 15 Februari 2018]. |
| [31] | R. A. Grimes, „What is OAuth? How the open authorization framework works,” csoonine, 16 Augustus 2017. [Online]. Available: https://www.csoonline.com/article/3216404/authentication/what-is-oauth-how-the-open-authorization-framework-works.html. [Geopend 15 Februari 2018]. |
| [32] | „OpenID Connect explained,” connect2id, 2018. [Online]. Available: https://connect2id.com/learn/openid-connect. [Geopend 15 Februari 2018]. |
| [33] | C. Zhang, „OpenID Connect / oAuth 2.0: Integration with XenApp through Unified Gateway,” Citrix, 11 September 2015. [Online]. Available: https://www.citrix.com/blogs/2015/09/11/openid-connectoauth-2-0-integration-with-xenapp-through-unified-gateway/. [Geopend 15 Februari 2018]. |
| [34] | M. Matchen, „HTTPS, SSL, and [Perfect] Forward Secrecy,” blogspot, 2016. [Online]. Available: http://packetinspection.blogspot.be/2014/01/https-ssl-and-perfect-forward-secrecy.html. [Geopend 13 Februari 2018]. |

# Bijlagen