# 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 Systeml

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

## Omschrijving van de opzet

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



:::::::::::::::::::::::::::::::::::::::::

Gebruikers zullen aanmelden op de ShareFile en indien nodig bestanden opslaan op of ophalen van de lokale StorageZone. De ShareFile stuurt hiervoor de query’s van de gebruiker naar de content switching virtuele server (CS-VS) van de NetScaler. Vooraleer een gebruiker toegang krijgt tot de lokale StorageZone zal de CS-VS verbinding maken met de AAA virtual server (AAA-VS). Die bezit de nodige policies om te oordelen of de gebruiker recht heeft op de content binnen de StorageZone. Indien dit het geval is worden de gegevens doorgestuurd naar de load balancing virtual server (LB-VS) die het evenredig verdeeld over de beschikbare StorageZone Controllers (SZ-C). Door middel van de informatie opgegeven in de gebonden load balancing services weet die LB-VS waar hij met dit verkeer naartoe kan.

Op netwerkniveau adverteert de interne StorageZone de publieke FQDN waaronder hij bereikbaar is aan de publieke ShareFile Cloud. Wanneer die ShareFile connectie probeert te maken zal hij een DNS-query uitvoeren en het publieke IP-adres dat hieraan gekoppeld is achterhalen. Dit IP-adres is voorzien van een network address translation (NAT) regel in ICORDA’s border router (en firewall) die naar het DMZ IP-adres van de NetScaler zijn CS-VS wijst. En zoals hierboven vermeld werd eindigt het verkeer op basis van enkele geconfigureerde policies en services uiteindelijk bij de lokale StorageZone.

## Vereisten en randvoorwaarden

* Werkende NetScaler VPX (NS10.5 of hoger is aangeraden) (twee indien high availability nodig is)
* Geldig publiek aanvaard certificaat
* Publiek IP-adres en DNS-naam (twee indien high availability nodig is)
* Active Directory (AD) en toegang tot AD-account met leesrechten
* Interne StorageZone Controller (twee indien nood aan load balancing en/of high availability)
* ShareFile Enterprise editie met sharefile.com subdomein

## NetScaler configuratie

Hier volgt de NetScaler configuratie die nodig is om de ShareFile Cloud te connecteren met de lokale StorageZone. Authenticatie voor de gebruikers met de lokale opslag gebeurt op NetScaler a.d.h.v. de AD-credentials. Ook SSO kan geconfigureerd worden op ShareFile en NetScaler, de configuratie die hier vermeld wordt maakt SSO mogelijk, door middel van het SAML 2.0 framework.

### Standaard NetScaler voor ShareFile setup (NS10.5 of hoger)

NetScaler is voorzien van een ingebouwde “NetScaler voor ShareFile setup” vanaf versie 10.5. Die standaard setup is geen verplichting, maar het kan de configuratie veel sneller en gemakkelijker maken. Om een volledig functionele opstelling met optimale beveiligingsmaatregelen en gebruikerservaring te bekomen is het aangeraden om dieper in te gaan op elke component en uit te zoeken welke extra configuratie deze nodig acht.

#### Content switching server

De eerste server dat geconfigureerd wordt tijdens de NetScaler voor ShareFile setup is de content switching virtuele server.

Eerst en vooral zal deze server voorzien moeten worden van een publiek IP-adres. Publiek betekent dat het gebruikt zal worden voor communicatie met het publieke internet. Om goed te functioneren zal men dus nood hebben aan een publiek herkend IP-adres dat in jouw bezit is of een DMZ IP-adres dat verbonden is met een publiek via een NAT-regel.

Buiten dat heeft de server ook nood aan een naam. De gekozen naam maakt eigenlijk niet zo veel uit, maar hou er rekening mee dat ze voorafgegaan zal worden door de string “\_SF\_CS\_” (die staat voor ShareFile Content Switching server).

Omdat de communicatie tussen de NetScaler en het internet waardevolle en gevoelige informatie kan bevatten, is het aangeraden om hem van een certificaat te voorzien zodat het verkeer over HTTPS kan lopen. In de volgende stap zal men dus een publiek aanvaard certificaat moeten voorzien. Dat certificaat kan een wildcard certificaat of een speciaal toegewijd certificaat zijn voor de NetScaler, zolang het maar gesigneerd is door een herkende certification authority (CA).

#### Load balancing Server

In de volgende stap worden de load balancing servers toegevoegd, voor elke SZ-C die toegevoegd wordt aan de opstelling zal de NetScaler automatisch een load balancing service configureren. Ook wanneer slechts één SZ-C opgezet wordt zal de content switching server standaard zijn verkeer doorsturen naar een LB-VS.

Eerst en vooral moet het interne IP-adres van de lokale SZ-C (of indien deze ontdubbelt zijn Controllers) voorzien worden.

Dan krijgt men de keuze om de communicatie met die Controller over HTTP of HTTPS te laten verlopen. Indien de beste werkmethode gevolgd wordt, gebruikt men hier ook een certificaat om HTTPS-verbindingen mogelijk te maken. *Het gebruik van HTTPS is hier echter minder belangrijk omdat dit verkeer volledig intern verloopt.* In deze opstelling wordt gebruikt gemaakt van een wildcard certificaat. Dit certificaat zal op de Controller geïnstalleerd moeten worden, aangezien de NetScaler een beveiligde verbinding zal aanvragen bij de Controller en niet omgekeerd. Meer info hierover kan teruggevonden worden in de hoofdstuk x over de StorageZone. Aangezien dit certificaat enkel nodig is om intern verkeer te beveiligen kan hier ook een zelf gesigneerd certificaat gebruikt worden.

#### Load balancing Service

Een load balancing server is voorzien van minstens één load balancing service. De “NetScaler voor ShareFile setup” koppelt zo een service automatisch. De service wordt voorzien van een IP-adres zodat de load balancing server weet naar waar hij het verkeer dat hij ontvangt moet sturen. In een NetScaler voor ShareFile setup zal elke load balancing service het IP-adres van een lokale StorageZone Controller toegewezen krijgen.

#### AAA-Server en LDAP-service

In de laatste stap van de setup wordt de authenticatie geconfigureerd. Standaard zal hier gevraagd worden achter de AD-gegevens van de opstelling. Eerst en vooral wordt er gevraagd achter een IP-adres voor het opzetten van de AAA-VS, dit is de server die (zoals de naam reeds meedeelt) de authenticatie, autorisatie en accounting regelt, in hoofdstuk x werd er reeds meer verteld over AAA. In principe is het voldoende om een vrij IP-adres te geven dat binnen de netwerk range van het interne domein valt.

De NetScaler met zijn AAA-server zal dus instaan voor alle authenticatie van de gebruikers met de lokale StorageZone. Hij vervangt hier het werk dat meestal toegewezen wordt aan lokale servers en hij gebruikt de reeds bestaande AD-gegevens of tokens.

De AD-gegevens die de NetScaler nodig heeft voor de authenticatie goed te laten verlopen zijn als volgt.

* Het IP-adres van de AD-server en de poort waarover die server zijn AD DNS-verkeer stuurt.
* Een vrij intern IP-adres voor de AAA-VS die meteen aangemaakt wordt.
* Het SSO-domein waar de AD-gegevens terug te vinden zijn.
* De Base DN (dit is de locatie in de AD waar de usergegevens terug te vinden zijn).
* Een AD-account met leesrechten (***best practice service account ww verandert niet)***

### Extra configuratie

Zoals eerder vermeld is er extra configuratie op de NetScaler nodig om de opstelling optimaal te configureren en beveiligen. Omdat er voornamelijk extra beveiligingsconfiguratie nodig is, zal het grootste deel hiervan doorgaan onder het “AAA-Application Traffic” menu-item.

De extra configuratie op de NetScaler gebeurt voornamelijk in policies en actions. Actions zeggen welke acties effectief uitgevoerd moeten worden. Deze worden gebonden aan policies die vertellen wanneer er actie genomen moet worden (dat gebeurt wanneer er aan de opgestelde expressie(s) voldaan wordt). Deze worden dan weer gebonden aan virtuele servers of services. De bijhorende servers moeten het passerend verkeer goed monitoren zodat ze gepast kunnen reageren wanneer aan de juiste voorwaarden voldaan wordt.

#### Netwerkinstellingen

Uiteraard moet de NetScaler voorzien worden van de correcte netwerkinstellingen. NetScaler werkt anders dan de meeste netwerktoestellen, Het maakt gebruikt van virtuele IP-adressen, subnet-adressen en interfaces. Elk IP-adres dat moet kunnen communiceren met de buitenwereld heeft nood aan een subnet-adres dat gebruikt wordt voor die communicatie. Zo wordt er per subnet (dat van buitenaf bereikbaar moet zijn) één subnet-adres voorzien. Alle IP-adressen in dat subnet zullen dat subnet-adres gebruiken voor communicatie naar buiten toe.

Op NetScaler kunnen ook interfaces aangemaakt worden. Zo kan men een Interne- en een DMZ-interface voorzien. De fysieke server in deze opstelling is voorzien van 3 netwerkkabels. Eén om netwerktoegang tot de IMM te voorzien. Eén om verbinding te leggen naar het interne netwerk (voor te connecteren met de Active Directory server en de StorageZone Connector). En één om toegang te voorzien naar het publieke internet, deze netwerkkabel legt een verbinding naar het interne DMZ-netwerk.

Verder is het nodig om de nodige netwerk routes te configureren. NetScaler moet weten waar het verschillend IP-verkeer naartoe moet sturen. Als hij niet opgesteld wordt als een default gateway, wordt hij best voorzien van een default route voor elke subnet waarin hij verkeer zal routen. In dit geval werd een route voorzien naar de default gateways van het intern- en DMZ-netwerk van ICORDA. Daarboven is er een default route met IP-adres 0.0.0.0 en subnet 0.0.0.0 opgesteld naar de default gateway van het DMZ-netwerk voor al het ongekende verkeer. Dergelijk ongekend verkeer komt namelijk van het publieke internet. Indien NetScaler toch als een default gateway opgesteld wordt, kunnen er dynamische routing protocollen geconfigureerd worden. Door communicatie met andere routers kan NetScaler routing informatie overnemen en de gepaste routes berekenen voor de nodige IP-adressen.

Aangezien DMZ-verkeer zich hier in een VLAN bevindt, moet NetScaler hiervan op de hoogte gebracht worden. Dat kan door een VLAN te creëren in de netwerkconfiguratie. Bij het creëren van zo een VLAN in NetScaler moet het juiste VLAN-nummer voorzien worden en moet ze gelinkt worden aan de juiste interface(s). Hier wordt het VLAN in kwestie gekoppeld aan de DMZ-interface.

#### Cipher suites

Voor een toename aan veiligheid van het netwerkverkeer is het aangeraden van een goede cipher suite aan te maken. Een cipher suite is een set van gebruikte algoritmes, het bevat meestal een sleutel uitwisselingsalgoritme, een versleuteld gegevensuitwisselingsalgoritme en een bericht authenticatie algoritme. Een cipher suite kan nog meer gegevens bevatten indien extra algoritmes gebruikt worden voor de sleutel uitwisseling, of gegevensuitwisseling. Er zijn honderden mogelijke cipher suite combinaties. Het is de bedoeling dat meerdere cipher suites ondersteund worden door beide partijen in een gegevensuitwisselingsproces. Op die manier is de kans groter dat beide partijen een gemeenschappelijke cipher suite ondersteunen, als dit niet het geval is kunnen ze geen versleutelde netwerverbinding opzetten. Het is ook aangeraden van de ondersteunde cipher suites zorgvuldig uit te kiezen zodat geen zwakke, gebroken algoritmes beschikbaar zijn. Indien beide partijen daarop terugvallen, is hun netwerkverkeer niet veiliger dan een gewone niet versleutelde verbinding. Bovendien bestaan er aanvallen die de handdruk tussen beiden partijen manipuleren zodat beiden akkoord gaan met de minst veilige ondersteunde cipher suite. In Client – Server verbindingen is het vooral aan de server om zijn ondersteunde cipher suites correct op te stellen. De client is vaak gelimiteerd door het besturingssysteem, dit is één van de redenen waarom Windows XP geen veilige omgeving meer is om te browsen op het internet.

#### Content switching policies en actions

De content switching virtual server (CS-VS) heeft als hoofdtaak het ontvangen en correct doorsturen van al het netwerkverkeer dat stroomt tussen de AD DNS-server, SZ-C, ShareFile en NetScaler. Hij maakt beslissingen op basis van de policies en actions die eraan toegewezen zijn. Hij zal op basis van die informatie de nodige bestemming van het verkeer bepalen en de gegevens daar naartoe sturen. In deze opstelling is de CS-VS ook het aanspreekpunt van de NetScaler. Wanneer de ShareFile Cloud contact op neemt met de NetScaler voor de nodige StorageZone te bereiken, zal hij een aanvraag sturen naar het publieke IP-adres van ICORDA dat op zich geNAT wordt naar het DMZ-adres van de CS-VS.

De content switching server moet het netwerkverkeer dat hij ontvangt van de ShareFile Cloud analyseren. Indien die user nog niet geauthentiseerd geweest is zal hij de AD-gegevens doorsturen naar de AAA-VS voor de nodige authenticatie. Indien het authentiseren reeds gebeurd is zal hij de ontvangen gegevens doorgeven naar de LB-VS.

Indien de “NetScaler voor ShareFile setup” correct gevolg geweest is zou dit deel van de opstelling reeds perfect werken. \*\*\* SSO?

#### AAA virtual server policies en actions

##### LDAP

##### SSO

(session policy, SAML, OAuth)

In deze opstelling is het gewenst om SSO te voorzien om een vlotter aanmeldproces te bekomen bij de authenticatie met ShareFile. De NetScaler zal hier het meeste werk doen, hij speelt de rol van de identity provider.

Aangezien ShareFile geen OAuth API voorziet voor SSO, blijkt het niet mogelijk om gebruik te maken van het nieuwere OAuth framework in deze opstelling.

ShareFile voorziet echter wel een OAuth API, maar enkel voor een application provider en niet voor een identity provider. De Oauth API zou dus nuttig zijn voor 3th party applications die OAuth ondersteunen en bruikbaar zijn binnen ShareFile, maar niet voor de authenticatie met Citrix ShareFile zelf.

Voorlopig is SAML 2.0 een mooie oplossing. Indien de compatibiliteit van dit verouderde framework te laag wordt, zal Citrix uiteraard een andere oplossing moeten voorzien. Een extra OAuth API voor een identification provider, die gebruikt kan worden voor SSO op ShareFile, is een mogelijke oplossing.

**SAML 2.0 korte werking**

De gebruiker wilt zich authentiseren met een service. De service vraagt een aantal gegevens op

**SAML 2.0 details**

Om SSO op de ShareFile mogelijk te maken moet de NetScaler voorzien worden van een SAML-policy. Daarin kan een expressie geconfigureerd worden in de vorm van “HTTP.REQ.URL.CONTAINS("saml")” dat duidelijk maakt aan de NetScaler dat de bijhorende action van toepassing is op al het passerend verkeer met “saml” in de request URL. In de action (voor SAML noemen ze dat een SAML profile) kan men dan de verdere gegevens aanvullen die van toepassing zullen zijn op het SSO verkeer tussen ShareFile en NetScaler. Er wordt gevraagd achter de assertion consumer service url, dat de url waar NetScaler zijn SAML-response naartoe stuurt.

### Extra mogelijkheden van NetScaler

Indien NetScaler als een border gateway opgesteld wordt kan hij ook instaan voor de NAT van het passerend IP-verkeer. In deze opstelling is dat niet het geval, de NetScaler hier zal enkel verkeer tussen de ShareFile en StorageZone en het DNS-verkeer van de DNS-server ontvangen. Hij zal niet als gateway dienen, en hij zal NAT overlaten aan de border gateway.

NetScaler kan ook geconfigureerd worden als een application firewall. Op die manier voldoet NetScaler als een standalone border router en firewall. Hier wordt dit werk ook overgelaten aan de reeds bestaande border router, die ook als firewall dient.

Indien NetScaler in een andere opstelling als default gateway gebruikt wordt zal de configuratie niet helemaal hetzelfde verlopen. In dat geval moet er een gateway server aangemaakt worden die voorzien wordt van het publieke of DMZ IP-adres waarom de NetScaler van buitenaf bereikbaar moet zijn. Deze default gateway kan dan dienen als de CS-VS door de content switching policies eraan te koppelen.

**NetScaler**

Publiek IP-adres

**CS-VS**

**LB-VS**

**AAA-VS**

**SZ-C**

**SZ-C**

**StorageZone**

FQDN

Sharefile.icorda.be

**ShareFile Cloud**

icorda.sharefile.com