## 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 virtuele 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 virtuele 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 LDAP-gegevens volgens 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 virtuele server (CS-VS)

De eerste server dat geconfigureerd wordt tijdens de NetScaler voor ShareFile setup is de CS-VS.

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 acties 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 IP-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.

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).

#### StorageZone (SZ) en Load balancing virtuele server (LB-VS)

In de volgende stap wordt de LB-VS aangemaakt, 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 tussenliggende 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 de NetScaler voor ShareFile setup zal elke load balancing service het IP-adres van een lokale StorageZone Controller toegewezen krijgen.

#### AAA virtuele server (AAA-VS) 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 (een service-account is het meest gewenst, dat wachtwoord 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 acties. Acties 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

De NetScaler moet nog 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 drie 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 SSL-netwerkverkeer is het aangeraden van een goede Cipher groep aan te maken. Zo een veilige Cipher groep bestaat uit een reeks Cipher suites waarvan geweten is dat ze niet kwetsbaar zijn voor de nieuwste netwerkaanvallen. 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 gebruiker 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.

De zelfgemaakte Cipher groep kan dan gelinkt worden aan alle virtuele servers op NetScaler ter vervanging van de standaard Cipher groep. Op deze manier zullen alle SSL-verbindingen verplicht gebruik maken van de zelf gekozen veilige algoritmes.

#### Single sign-on (SSO)

Alhoewel het in deze opstelling niet nodig is om extra configuratie uit te voeren voor het bekomen van SSO, kan het toch handig zijn om te weten hoe SAML 2.0 en OAuth 2.0 geconfigureerd worden in NetScaler. SAML en OAuth kunnen namelijk gebruikt worden voor SSO in applicaties die aan ShareFile gekoppeld worden (bijvoorbeeld mobiele applicaties of andere applicaties van derden zoals Google Docs).

Momenteel is er reeds SSO aanwezig in de opstelling. Om te connecteren met de StorageZone zal ShareFile (service provider) op de achtergrond de AD-gegevens van de user doorsturen naar NetScaler (identity provider). NetScaler vergelijkt de ontvangen gegevens met de gegevens uit de reeds geconfigureerde AD-server. Indien ze overeen komen zal de gebruiker zonder problemen verder kunnen werken op de lokale StorageZone.

##### Lightweight Directory Access Protocol (LDAP)

Na het doorlopen van de NetScaler voor ShareFile setup is NetScaler al voorzien van de nodige AD-gegevens om SSO mogelijk te maken voor het connecteren van de gebruikers met de lokale StorageZone.

In hoofdstuk xxx kan men zien welke gegevens NetScaler juist nodig heeft om een correcte LDAP-configuratie te bekomen.

NetScaler zal regelmatig contact maken met de AD-server en alle user en groep gegevens uit de AD bijhouden. Bij het authentiseren zal de AAA-VS de inkomende AD-gegevens hiermee vergelijken.

Deze LDAP-authenticatie verloopt volgens SAML 2.0 normen, aangezien de NetScaler ook hier IDP zal spelen voor de lokale StorageZone die hier de SP is. Het verschil is dat de gebruiker meteen verbindt met de IDP die bepaalt of hij de aanvraag doorstuurt naar een lokale StorageZone Connector. De gebruiker kan onmogelijk een directe verbinding aangaan met de lokale StorageZone Connector, de IDP zal hier steeds tussen zitten en zijn goedkeuring moeten geven.

##### Security Assertion Markup Language (SAML)

Om SAML SSO met externe applicaties op 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")”. Dergelijke expressie maakt duidelijk aan NetScaler dat de bijhorende actie van toepassing is op al het toekomende verkeer met “SAML” in de request URL. Indien ShareFile een SAML-authenticatie aanvraag naar NetScaler stuurt zal deze policy geactiveerd worden.

In de actie (voor SAML noemt dit een SAML-profile) kan men de verdere gegevens aanvullen die van toepassing zijn op het SSO-verkeer tussen ShareFile en NetScaler. Er wordt gevraagd achter een aantal gegevens om SAML mogelijk te maken. De ‘assertion consumer service URL’ is de URL waar NetScaler zijn SAML-response naartoe stuurt indien de SAML-authenticatie om de gebruiker de authentiseren met die service. De ‘issuer name’ is de publieke naam van de entiteit die de nodige tokens voorziet indien de SAML-authenticatie correct verloopt. De ‘service provider ID’ is de publieke naam van de entiteit die de nodige services verleent en de SAML-authenticatie request verstuurt. De ‘SAML binding’ is de manier waarop de SAML berichten verstuurt worden, dit kan via een POST of REDIRECT gebeuren. Verder is het ook nog mogelijk en aangeraden om een IDP en SP certificaat te voorzien bij de configuratie van SAML.

Er wordt al SAML gebruikt voor het authentiseren met de lokale StorageZone. Het is echt ook mogelijk om SAML te gebruiken voor het authentiseren met ShareFile zelf of het authentiseren met externe applicaties die aan ShareFile gelinkt kunnen worden.

Meer informatie over de werking van SAML kan je terugvinden in hoofdstuk xxx.

##### Open Authorization (OAuth)

In NetScaler is er geen aparte sectie voor de configuratie van een geavanceerd OAuth policy. Om een geavanceerd OAuth policy te creëren moet men een standaard geavanceerd authenticatie policy aanmaken en deze voorzien van een OAuth actie.

De policy kan men voorzien van een gelijkaardige expressie “HTTP.REQ.URL.CONTAINS("OAuth")”. Hier zal de OAuth actie uitgevoerd worden indien NetScaler een request ontvangt met de term OAuth in verwerkt.

In de OAuth action wordt er eerst gevraagd achter de ‘client ID’ en ‘client secret’. Beiden moeten op voorhand aangevraagd worden bij de IDP. De client ID is uniek en wordt gelinkt aan de SP waarvoor de gegevens werden aangevraagd. De client secret is geheim en wordt enkel gedeeld tussen de IDP en SP.

OAuth kan niet gebruikt worden om door middel van SSO aan te melden op ShareFile. ShareFile ondersteunt namelijk geen OAuth als servide provider, maar het ondersteunt wel OAuth als identity provider. ShareFile kan net zoals NetScaler gebruikt worden als een OAuth identity provider en bepaalde resources delen met services die dat nodig achten. Of de nodige login tokens voorzien voor services die anders telkens nieuwe logingegevens zouden vereisen.

Meer informatie over de werking van OAuth kan je terugvinden in hoofdstuk xxx.

### Andere 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 reeds bestaande border gateway.

NetScaler kan geconfigureerd worden als een applicatie firewall. Op die manier voldoet NetScaler als een standalone border router en firewall. In deze opstelling wordt dit werk overgelaten aan de reeds bestaande firewall.

Indien NetScaler wel als default gateway gebruikt wordt zal de configuratie niet helemaal hetzelfde verlopen. In dat geval moet er een gateway virtuele server aangemaakt worden die voorzien wordt van het publieke of DMZ IP-adres waarop de NetScaler van buitenaf bereikbaar moet zijn. Deze default gateway zal dan dienen als de CS-VS in dergelijke opstellingen.