# NetScaler configuratie guide (NS12)

Voor ShareFile met lokale StorageZone

## Omschrijving van de opzet

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



*De opstelling; “Citrix ShareFile met lokale storage zone door middel van NetScaler met AAA-functionaliteit”.*

## Vereisten en randvoorwaarden

* Werkende NetScaler VPX (NS10.5 of hoger is aangeraden) (2 indien high availability nodig is)
* Geldig publiek aanvaard certificaat
* Publiek IP-adres en DNS-naam (2 indien high availability nodig is)
* Active Directory (AD) en account met leesrechten
* Interne StorageZone Controller (2 indien nood aan load balancing en high availability)
* ShareFile Enterprise editie met sharefile.com subdomein

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

Sinds NS versie 10.5 is NetScaler is voorzien van een ingebouwde “NetScaler voor ShareFile setup”. Die standaard setup is geen verplichting, maar biedt een grote hulp indien een basissetup voldoet.



Ga naar het configuratie tabblad in de NetScaler VPX GUI interface.

Navigeer naar traffic management en klik op zet NetScaler op voor ShareFile.

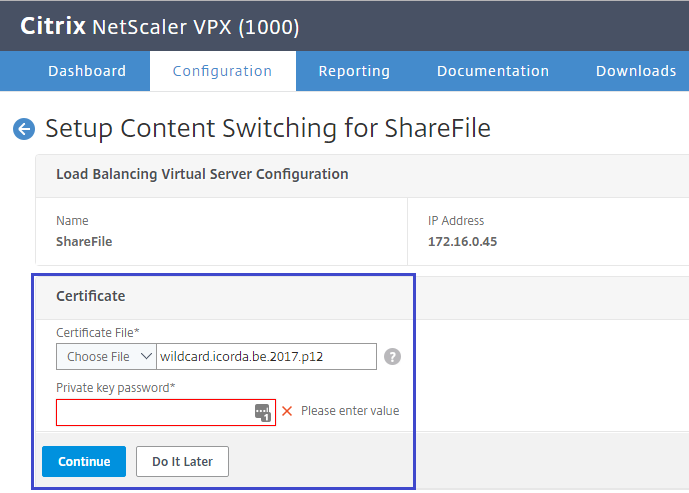
### Content switching virtuele server (CS-VS)

Vul het IP-adres in dat gebruikt zal worden om de NetScaler (en achterliggende StorageZone) van buitenaf te bereiken. Dit kan een DMZ IP-adres zijn indien ze correct voorzien wordt van een NAT regel naar een publiek IP-adres.

Geef de content switching virtuele server een naam. De gekozen naam maakt 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).

Vink de ShareFile Data en StorageZones Connector selectievakjes aan.

Klik op volgende.



Importeer een certificaat uit NetScaler, of uit de lokale serveropslag.

Indien het certificaat beveiligd is met een wachtwoord dient u dat vervolgens in te vullen.

Klik op volgende

### StorageZone (SZ) & load balancing virtuele server (LB-VS)

Kies voor het toevoegen van een nieuwe StorageZone Controller.

Voorzie het IP-adres van de StorageZone Controller server.

Volgens de beste praktijken wordt er gekozen voor HTTPS over poort 443. Hou er rekening mee dat in dit geval een certificaat moet voorzien worden op de StorageZone Controller server (in de IIS-Manager). Dat certificaat mag zelf gesigneerd zijn.

Klik op toevoegen

### AAA virtuele server (AAA-VS)

Configureer een nieuw LDAP policy onder de LDAP-authenticatie.

Geef een IP-adres op voor de AAA-VS.

Geef het IP-adres van de lokale AD-server op (dat mag een primaire of secundaire server zijn).

Geef de correcte poort op waarover het AD-verkeer intern verloopt (standaard is dat 389).

Geef het SSO-domein op, standaard zal dat hetzelfde zijn als het AD-domein.

Vul de Base-DN in (dat is de plaats in AD waar de users zich bevinden).

Geef een AD-account met leesrechten op als Administrator Bind DN. Voorzie bij voorkeur een serviceaccount waarvan het wachtwoord niet meer zal veranderen in plaats van een Administrator account. Hier kan gerust een nieuw account voor aangemaakt worden.

Als inlognaam wordt meestal gekozen voor het oudere “sAMAccountName” of het nieuwere “userPrincipalName”. De eerste wordt ook ondersteund door pre Windows 2000 machines.

Standaard zal de NetScaler voor ShareFile setup gebruik maken van basic policies. Aangezien die verouderd zijn en afgekeurd worden, raadt Citrix aan om ze om te zetten in advanced policies. Dit kan gemakkelijk gedaan worden door het volgende commando in te geven in de command line interface van NetScaler en achteraf de nieuwe configuratie in te laden.



Klik op volgende.

Klik op finish.

## Extra configuratie

Verder er nog wat geconfigureerd worden alvorens NetScaler correct zou functioneren. Daar bovenop zijn er opties die toegevoegd kunnen worden, maar niet verplicht voor de werking van de opstelling.

### Netwerkinstellingen

Navigeer naar systeem 🡪 netwerk onder het configuratie tabblad.

#### IP-adressenC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_IP.png

Onder het menu-item “IPs” bevinden zich de IP-adresse die reeds aangemaakt werden tijdens het doorlopen van de setup. Hier moet nog een subnet IP-adres aan toegevoegd worden dat de communicatie van de NetScaler met het internet regelt. Dit subnet IP-adres moet zich in hetzelfde subnet bevinden als het adres van de CS-VS. Voor elk subnet waarin de NetScaler actief is zal zo een subnet IP-adres voorzien moeten worden. Standaard vraagt NetScaler vanaf de eerste opstart al achter een intern subnet adres. Indien dat nog niet geconfigureerd werd, moet er één aangemaakt worden voor de interne communicatie tussen NetScaler en andere componenten van de setup.

#### InterfacesC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_Interfaces.PNG

Onder het menu-item “Interfaces” zouden reeds 3 interfaces voorzien moeten zijn.

1. De loopback interface
2. Een interface voor het interne netwerk
3. Een interface voor de DMZ

Het is mogelijk om ze van aliassen te voorzien indien gewenst.

#### Virtual local area network (VLANC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_VLAN.PNG)

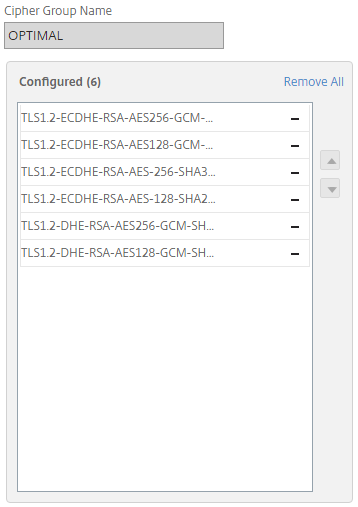
Onder het menu-item “VLANs” kunnen VLAN’s gecreëerd worden. Indien bepaalde interfaces die verbonden zijn met de AD DNS-server, StorageZone controller of gateway zich bevinden in een VLAN moet dit ook in NetScaler aangemaakt worden. Vergeet niet van de passende interfaces te binden aan het correcte VLAN-nummer tijdens de configuratie.

#### RoutesC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_Routes.PNG

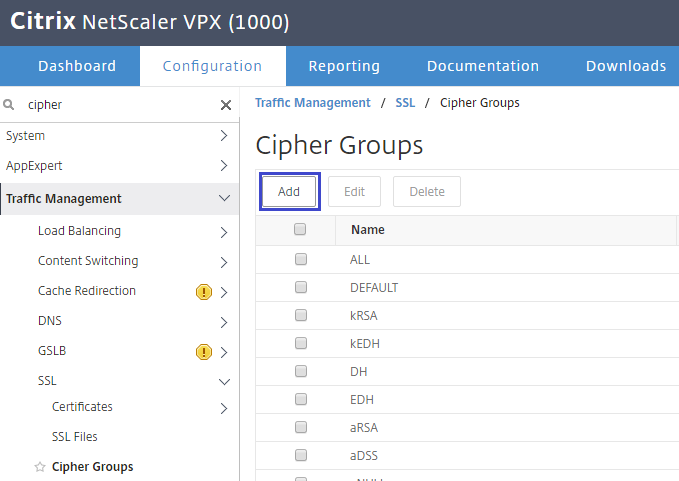
Onder het menu-item “Routes” kunnen routes aangemaakt worden zodat NetScaler weet waar hij IP-verkeer naartoe moet sturen. Standaard zal voor alle gekend IP-adressen (die tijdens de configuratie aan bod kwamen) reeds een route aangemaakt zijn. Er moet enkel nog een default route voorzien worden dat al het ongekende IP-verkeer naar het internet stuurt. De default route krijgt 0.0.0.0 als IP-adres en subnet masker en de default gateway van de DMZ als gateway adres.

### Cipher suites (optioneel)

Om de kans op succesvolle aanvallen op het netwerkverkeer te minimaliseren is het aangeraden om enkel de veiligste SSL-verbindingen toe te laten. Om enkel gebruik te maken van veilige algoritmes moet er een Cipher groep gecreëerd worden. Hier volgt een voorbeeld van een zelf gemaakte optimale Cipher groep.



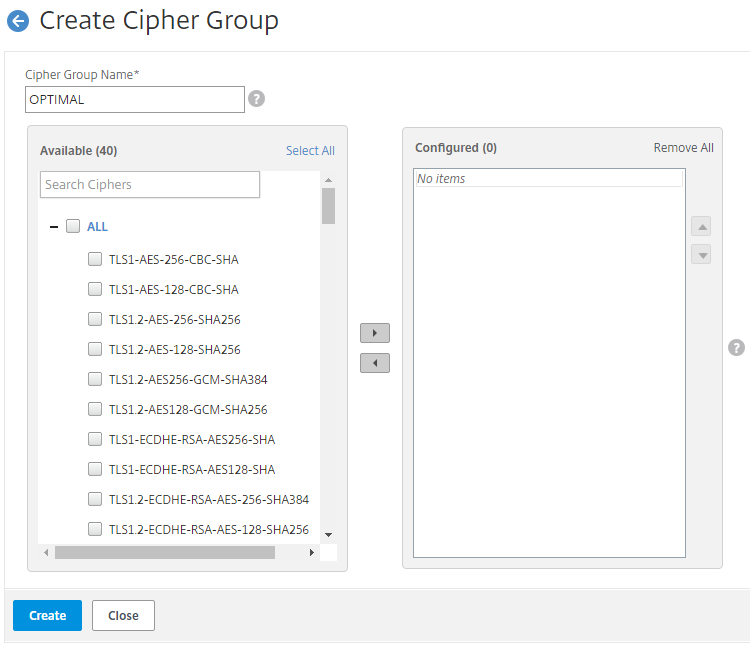
Navigeer naar traffic management, klik op SSL en dan ‘Cipher Groups’.

****

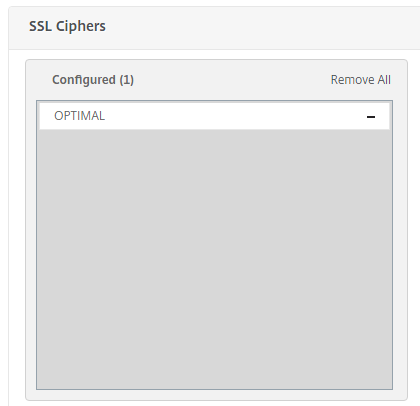
Voeg een nieuwe Cipher groep toe.

Geef de nieuwe Cipher groep een passende naam.

Begin met het toevoegen van Cipher suites.



Voeg de nodige Cipher suites toe door ze aan te vinken. (Onder de ‘ALL’ groep kunnen alle ondersteunde Cipher suites teruggevonden worden).



Link de Cipher suites aan de virtuele servers. Verwijder ook de default Cipher suite die er standaard aan toegewezen was.

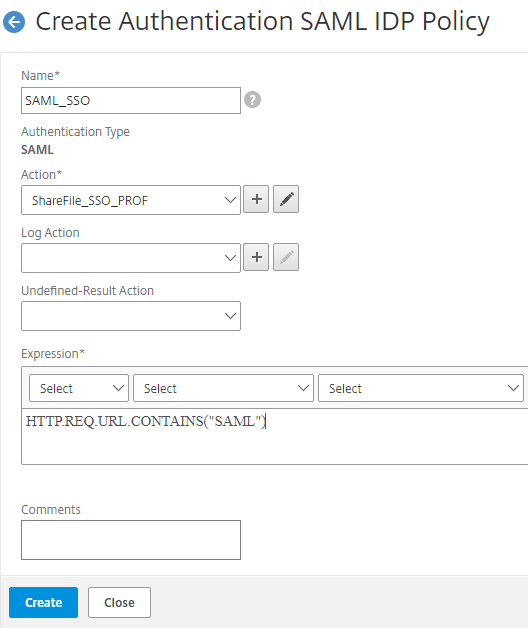
### Single sign-on (SSO) (optioneel)

In deze opstelling wordt er reeds geconnecteerd met de StorageZone door middel van de AD-gegevens, SSO is dus al aanwezig. Het kan toch handig zijn om te weten hoe SAML 2.0 en OAuth 2.0 geconfigureerd worden in NetScaler. SAML kan namelijk ook gebruikt worden om aan te melden op ShareFile met diezelfde AD-gegevens. OAuth kan dan weer gebruikt worden voor SSO in externe applicaties die aan ShareFile gekoppeld worden.

#### SAML 2.0

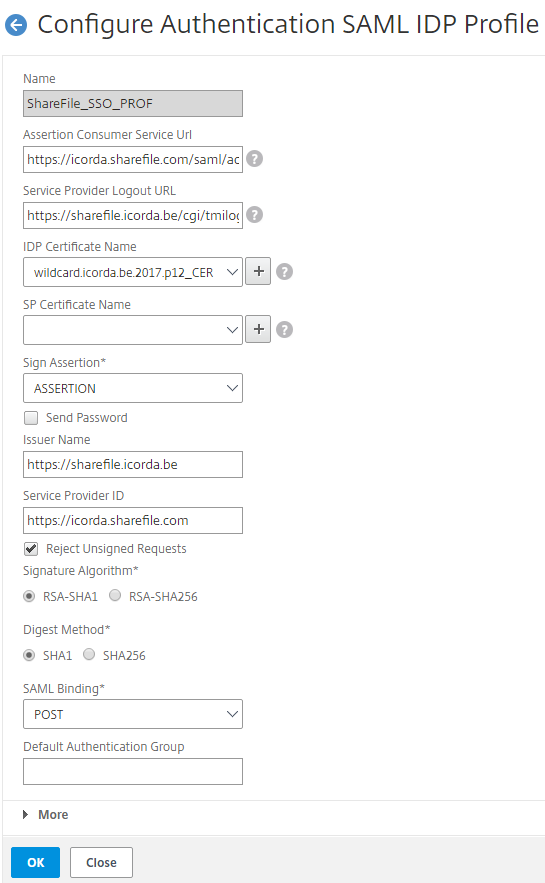
Navigeer naar security 🡪 AAA – Application traffic 🡪 policies 🡪 authenticatie 🡪 geavanceerde policies 🡪 SAML IDP.

Ga naar het policies tabblad en druk op toevoegen om een SAML IDP policy aan te maken.



Geef een expressie op in de vorm van “HTTP.REQ.URL.CONTAINS(“SAML”)”.

Druk op het plus icoon om een actie (SAML IDP Profile) toe te voegen aan de policy.



Geef het ShareFile subdomein gevolgd door “/saml/acs” op als Assertion Consumer Service URL.

Als logout URL kan het publieke adres van de NetScaler gebruikt worden gevolgd door “cgi/tmilogout”.

Gebruik het certificaat van de CS-VS als IDP certificaat voor SAML.

Het certificaat dat ShareFile aanmaakt na de SSO configuratie is het SP certificaat dat hier thuishoort. Zie de ShareFile configuratie guide hiervoor.

### NetScaler Gateway (indien van toepassing)

Indien NetScaler als gateway gebruikt wordt in de opstelling, moet een NetScaler Unified Gateway (UG) aangemaakt worden.

Deze Gateway zal automatisch beschikbaar zijn als een CS-VS, de content switching policies kunnen dus evengoed aan deze UG gebonden worden om dezelfde setup werkend te krijgen.