|  |
| --- |
|  |

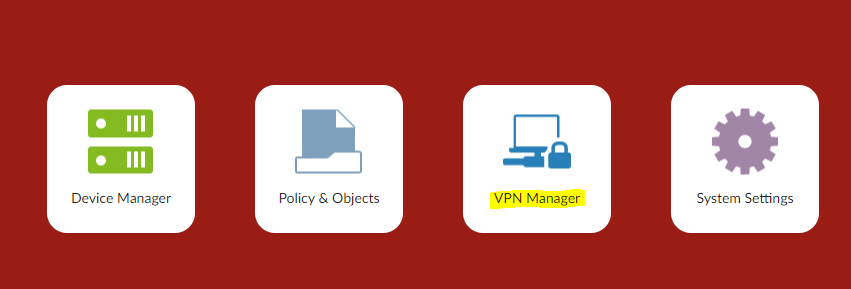


|  |
| --- |
| ***Fortinet – SSL VPN - Jan De Nul*** |
|  |

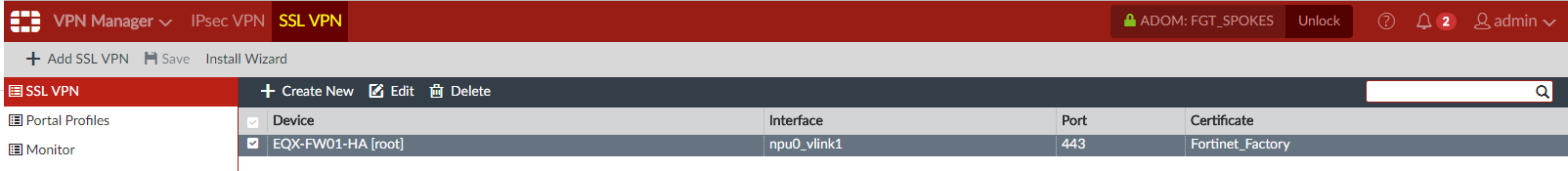
Inhoud

[1 FortiManager SSL VPN Configuratie 2](#_Toc511993825)

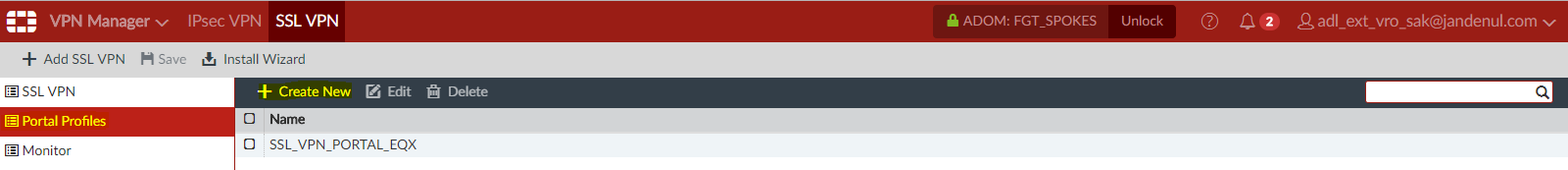
# FortiManager SSL VPN Configuratie

Prerequisite: PUBLIC IP nodig op de ISP1 interface!  
Login op de Fortimanager op de “FGT\_SPOKES” ADOM en kies voor VPN Manager.  
  


Kies voor “SSL VPN” boven aan in de rode balk.

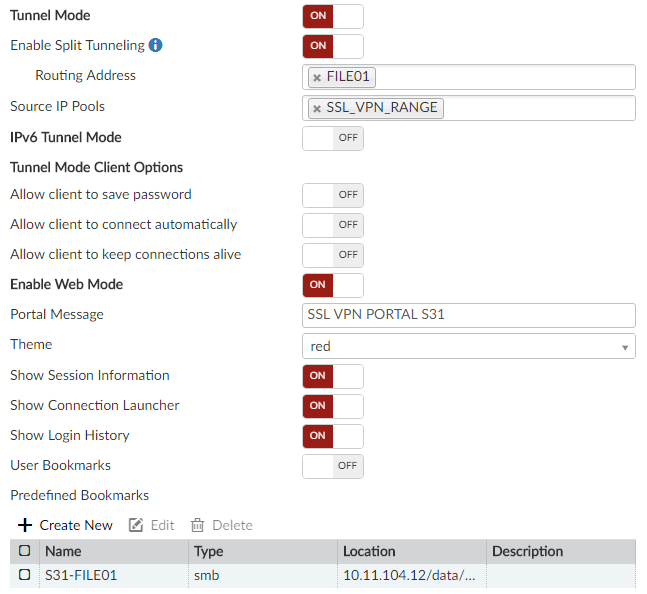


Klik aan de linker kant op “Portal Profiles” en kies voor create new.



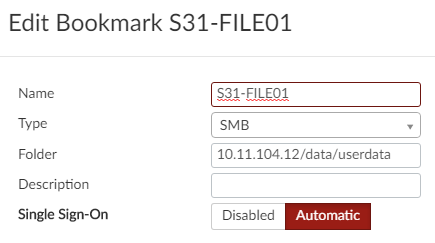
Vul de velden gelijkaardig aan onderstaand screenshot in en druk op OK. (Voorbeeld EQX)

Name -> SSL\_VPN\_PORTAL\_XXX (XXX – Site Abbreviation)  
Tunnel mode -> ON  
Enable Split Tunneling -> ON  
Routing Address ->FILE01(Kies voor de correcte adres objecten waartoe je toegang wil geven)  
Source IP Pool -> SSL\_VPN\_RANGE (Deze IP Range/object is op elke site hetzelfde)  
Enable Web Mode -> ON  
Portal Message -> SSL VPN PORTAL XXX (XXX – Site Abbreviation)  
Theme -> Red  
User Bookmarks -> OFF  
Predefined Bookmarks -> create new (Maak de gewenste bookmarks aan)

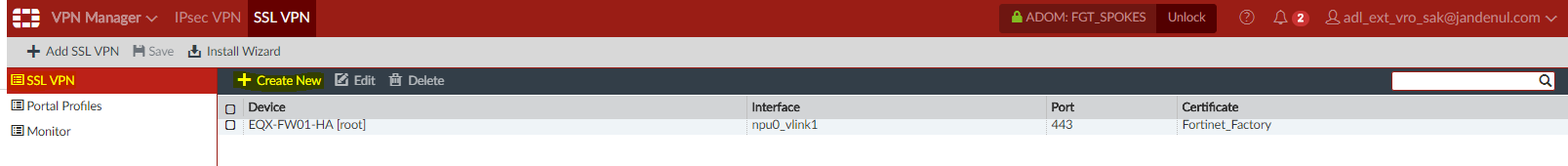


Voorbeelden Bookmark (S31)

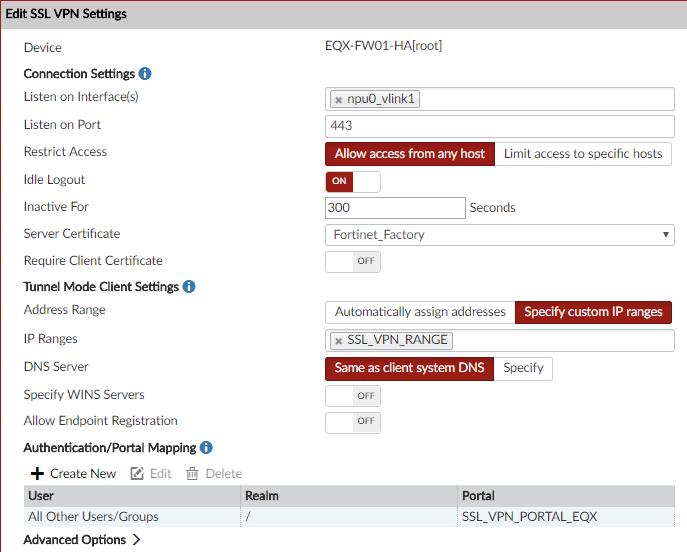
Voor de fileserver (smb) bookmark dienen de backslash(es) een gewone slash te zijn. ( \ -> / )  
Je dient de eerste 2 slashes niet mee te geven je kan meteen beginnen met IP adres.  
Single Sing-On is mogelijk als de system dns correct is ingevuld (dns suffix).

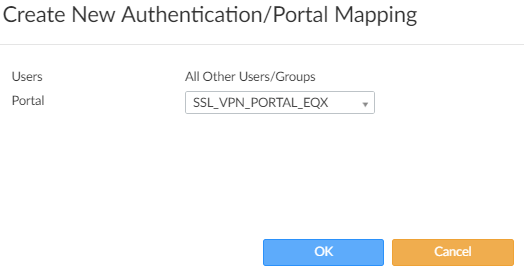


Klik in de linker kant terug op “SSL VPN” en kies voor create new.

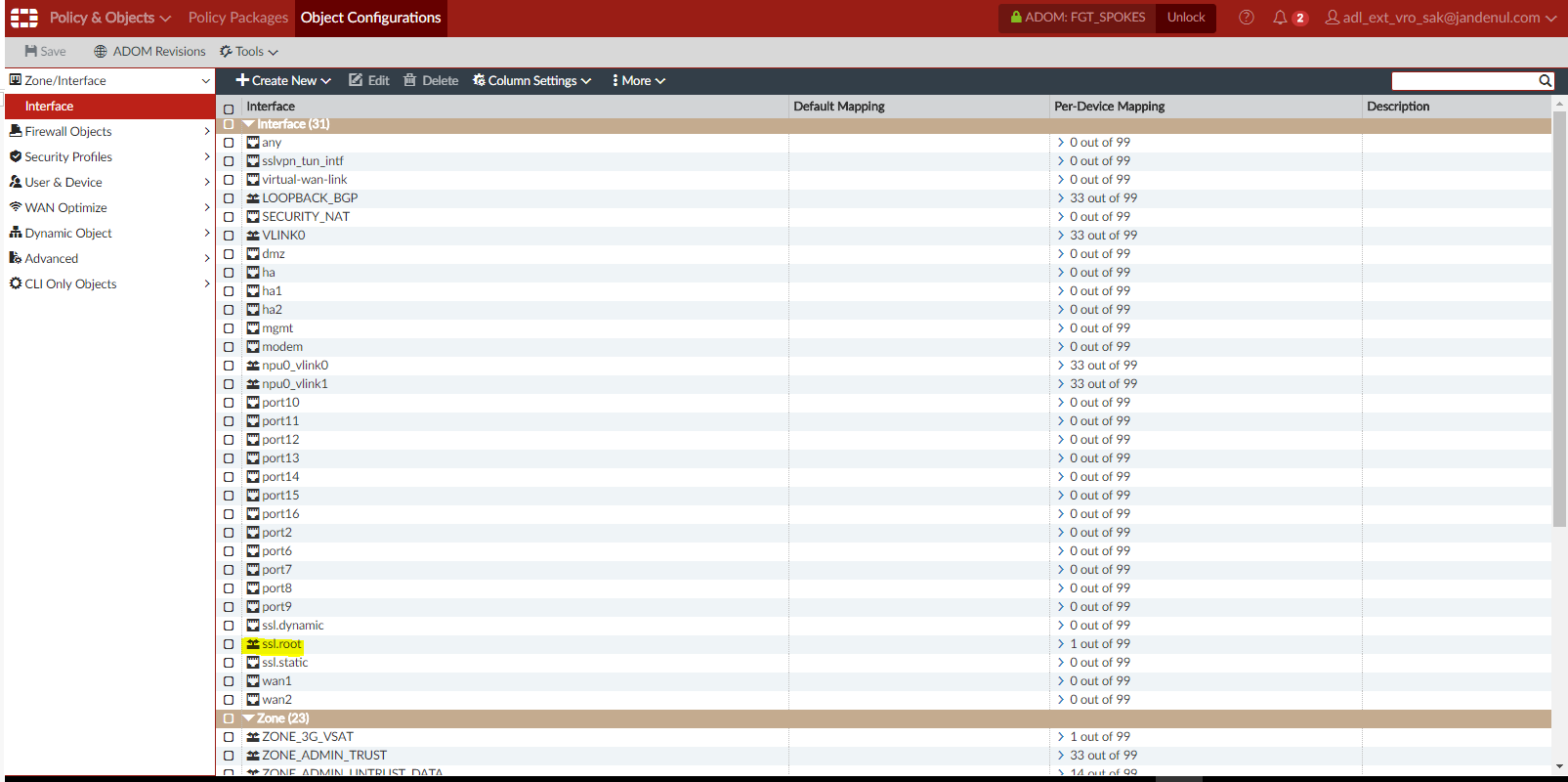


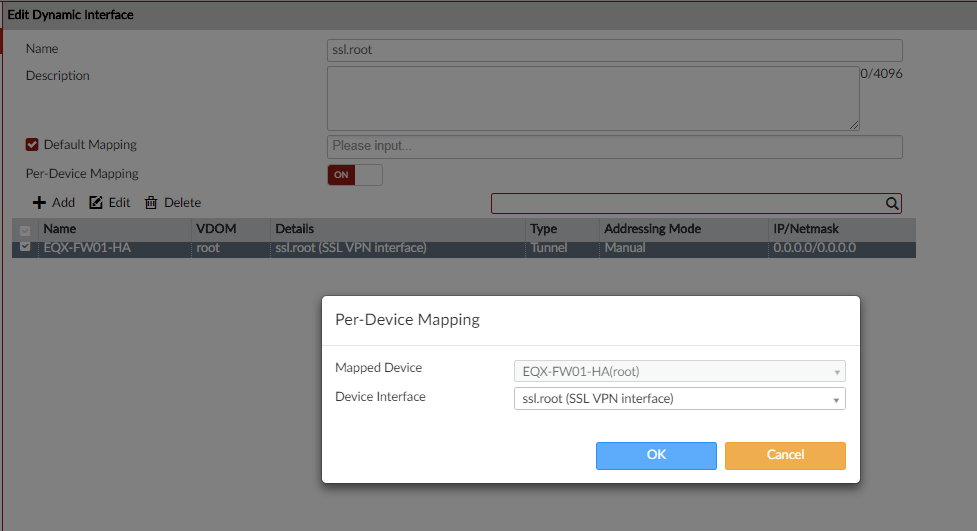
Vul de velden gelijkaardig aan onderstaand screenshot in en druk op OK. (Voorbeeld EQX)  
  
Device -> XXX-FW01-HA (of NODE0) [root] (Kies voor de gewenste firewall en de root VDOM hiervan)  
Listen on Interface(s) -> npu0\_vlink1  
Listen on Port -> 443  
Restrict Access -> Allow access from any host  
IP Ranges -> SSL\_VPN\_RANGE  
All Other Users/Groups -> SSL\_VPN\_PORTAL\_XXX (edit de default authentication/portal mapping)



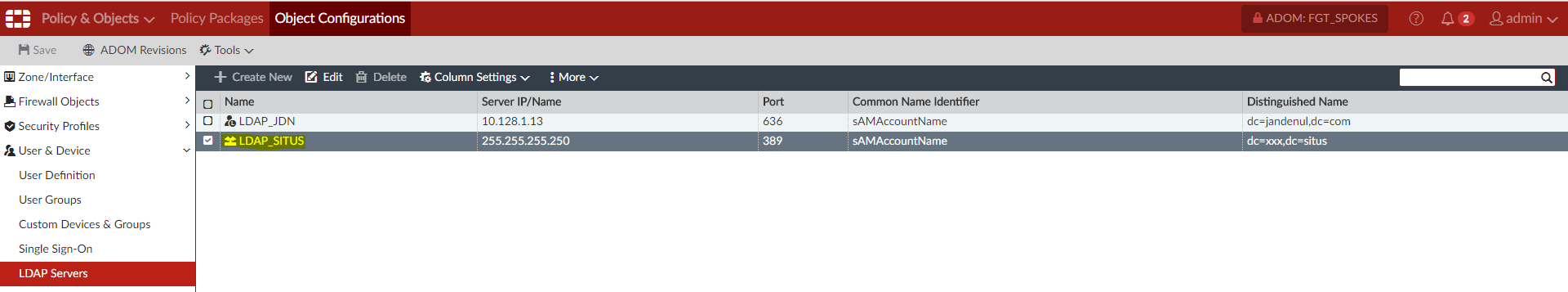


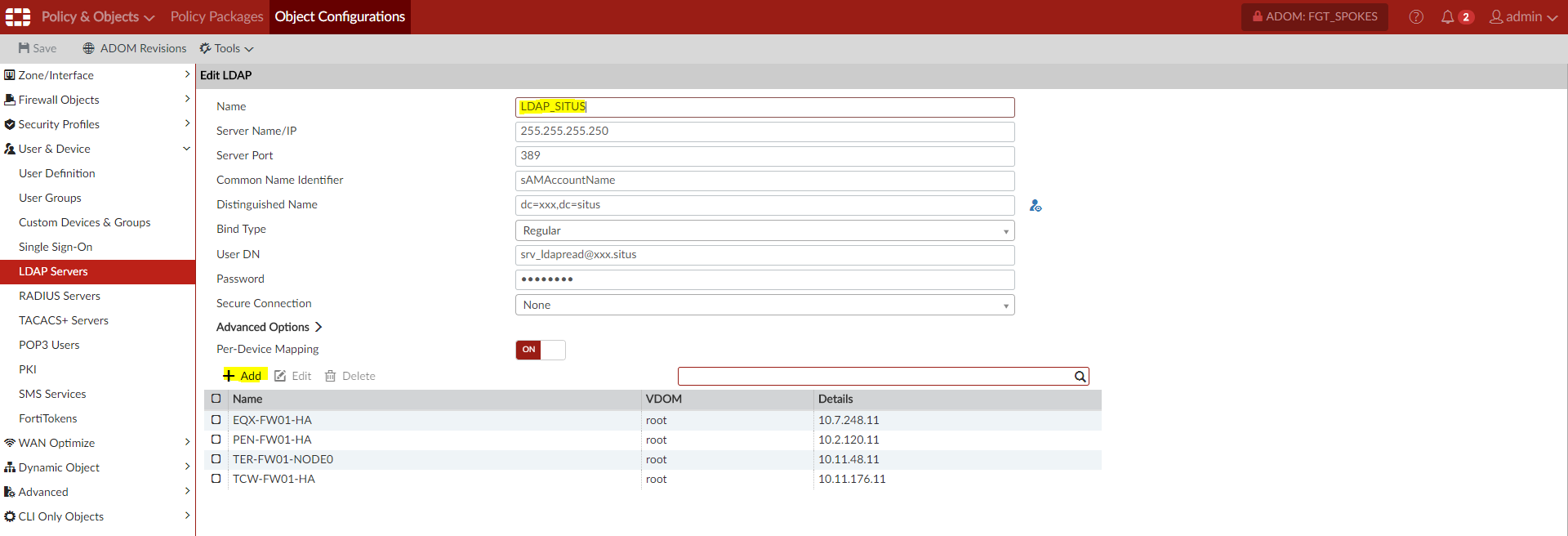
Ga naar Policy & Objects en kies voor Object Configurations.  
Controleer of de ssl.root interface de juiste “per-device mapping” heeft voor de firewall in kwestie.  
Zo niet voer de nieuwe versie van het “FortiManager script - Spokes offices” terug uit dat je gebruikt bij het uitrollen van de firewalls.





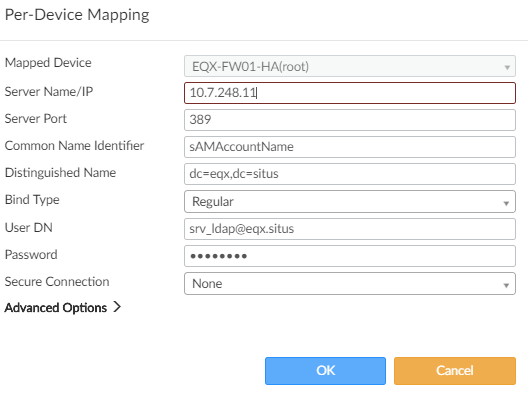
Klik in de linker kant op User & Device en kies voor LDAP Servers.  
Edit het bestaande object “LDAP\_SITUS” en maak een nieuwe “per-device mapping” aan.



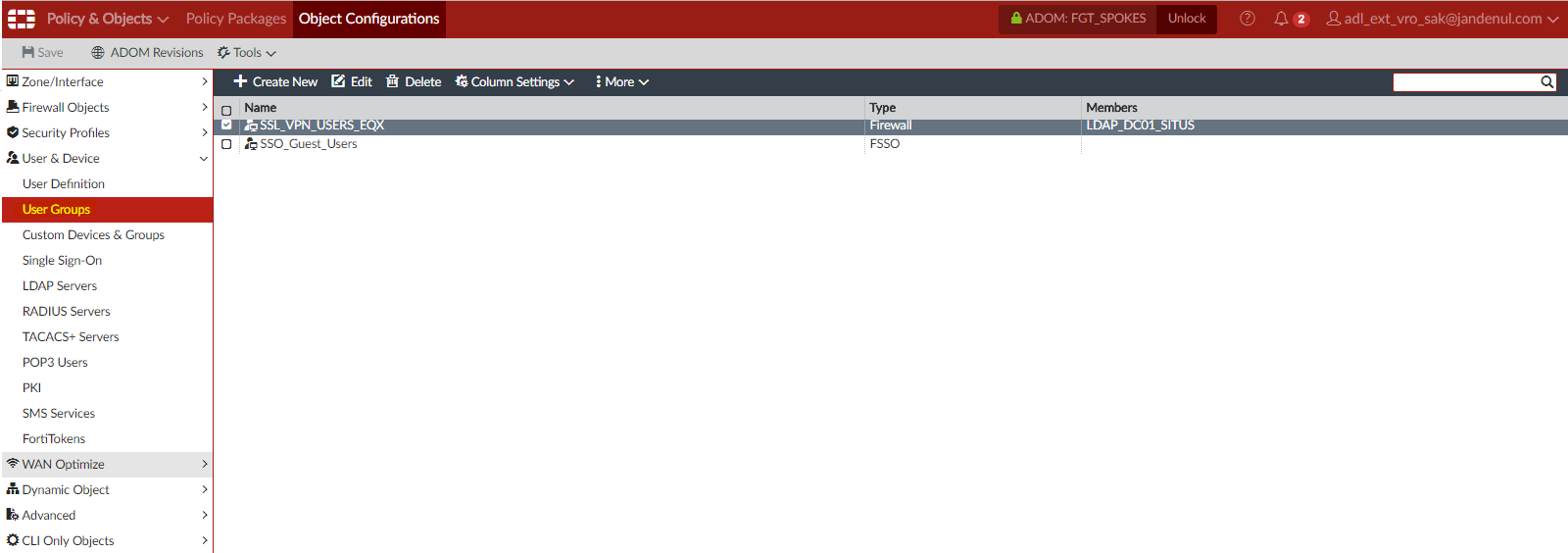


Vul de velden gelijkaardig aan onderstaand screenshot in en druk op OK. (Voorbeeld EQX)

Mapped Device -> XXX-FW01-HA (of NODE0) [root] (Kies voor de gewenste firewall en de root VDOM hiervan)  
Server Name/IP -> X.X.X.X (vul het IP adres van DC01 in ADMIN TRUST)  
Server Port -> 389  
Common Name Identifier -> sAMAccountName  
Distinguished Name -> dc=xxx,dc=situs (vul het domein van jou site in)  
Bind Type -> Regular  
User DN -> [srv\_ldap@xxx.situs](mailto:srv_ldap@xxx.situs) (vul de user in waarmee je ldap query kan uitvoeren)  
Password -> \*\*\*\*\*\* (vul het bijhorden wachtwoord van deze user in)  
Secure Connection -> None

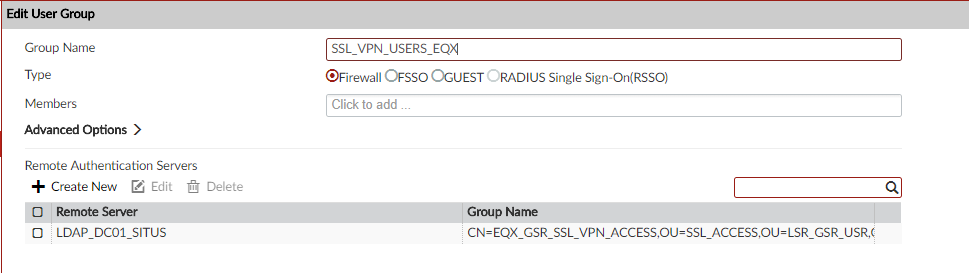


Klik in de linker kant op “User Groups” onder User & Device en kies voor create new.

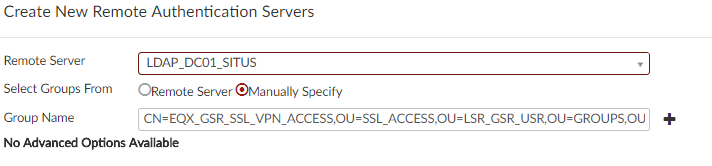


Vul de velden gelijkaardig aan onderstaand screenshot in en druk op OK. (Voorbeeld EQX)

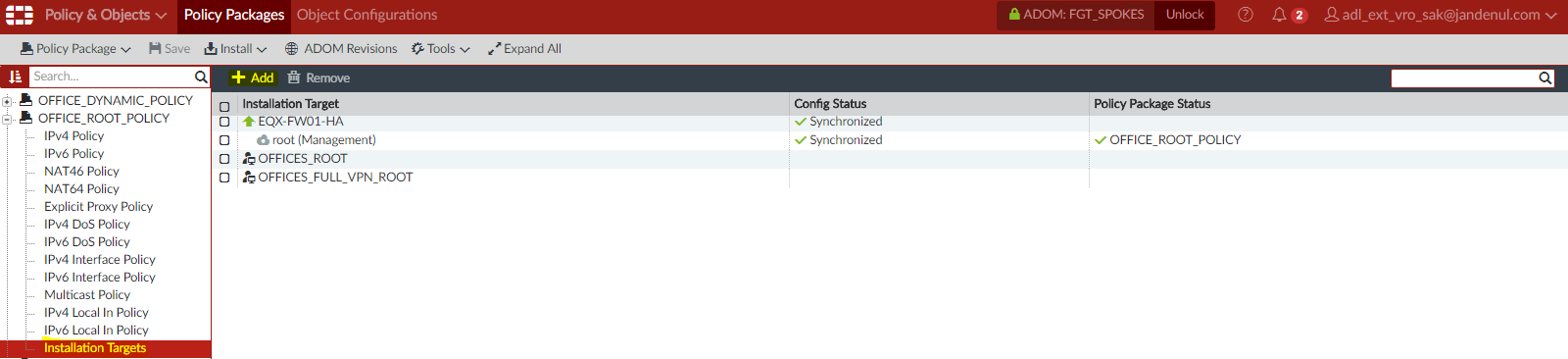
Group Name -> SSL\_VPN\_USERS\_XX (XXX – Site Abbreviation)  
Remote Authentication Servers -> create new

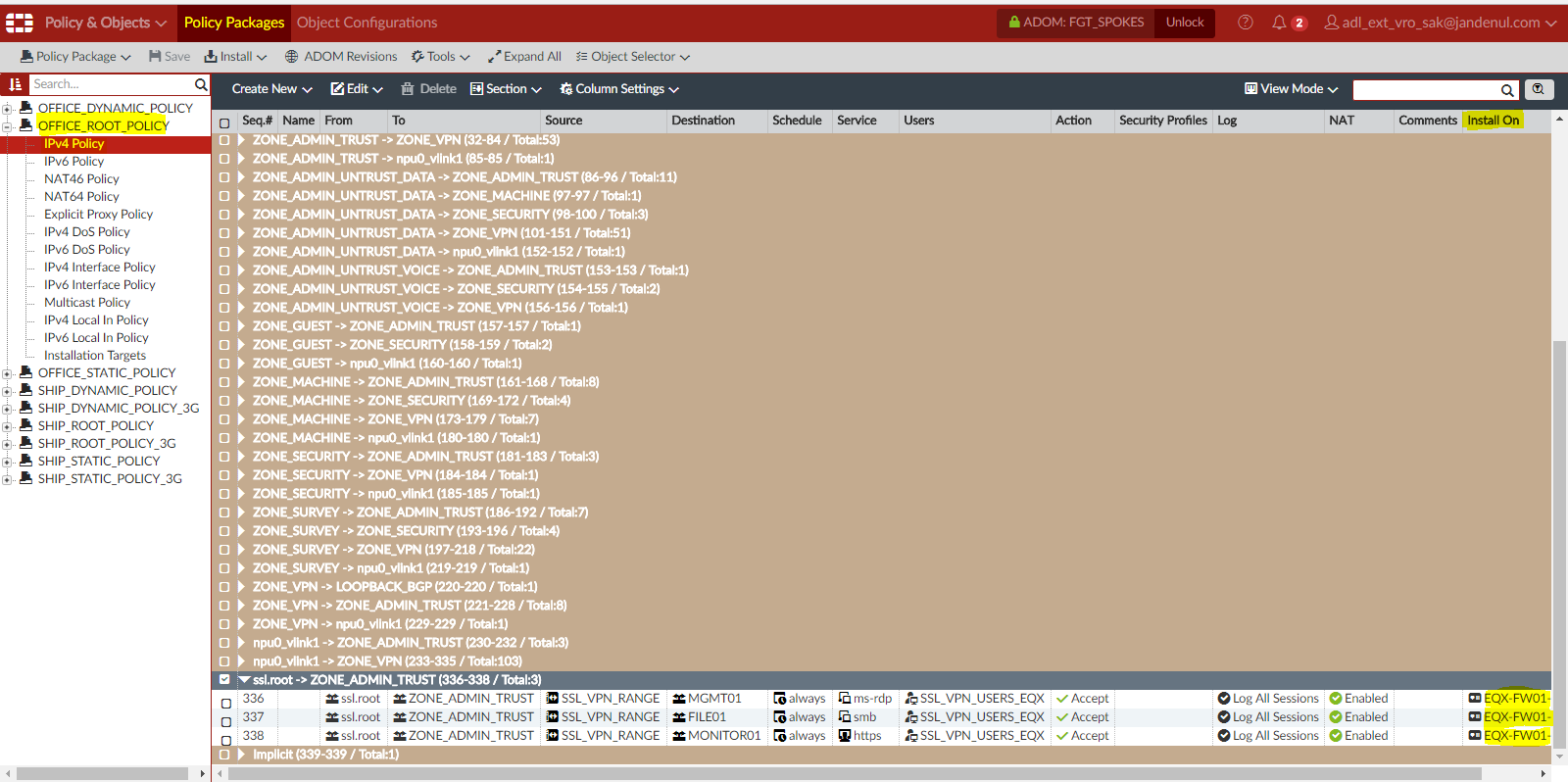


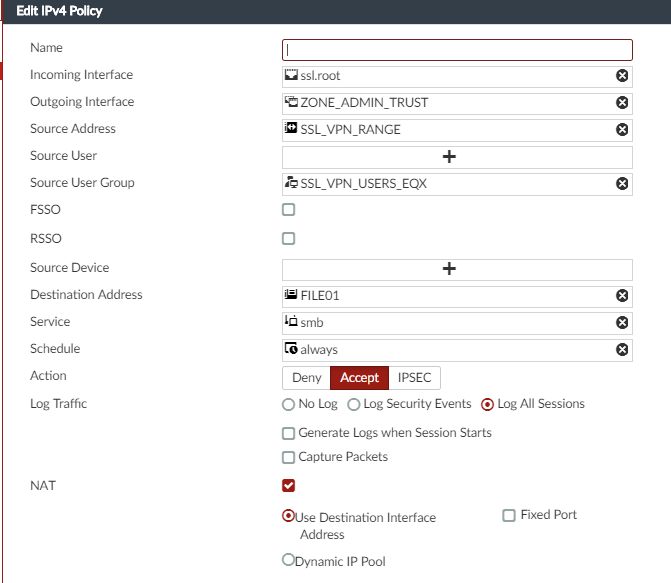
Kies hierbij de remote server “LDAP\_SITUS” en select groups from “Manually Specify”.  
Vul de gewenste Group Name in zoals onderstaand voorbeeld van EQX.  
  
“CN=EQX\_GSR\_SSL\_VPN\_ACCESS,OU=SSL\_ACCESS,OU=LSR\_GSR\_USR,OU=GROUPS,OU=\_CORP,DC=EQX,DC=SITUS”



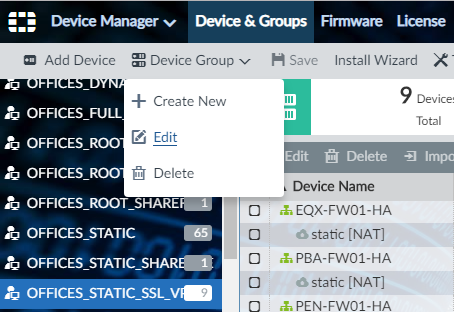
Ga naar Policy Packages en kies voor “OFFICE\_ROOT\_POLICY” package.  
Voeg als eerste de gewenste firewall toe aan de installation targets.



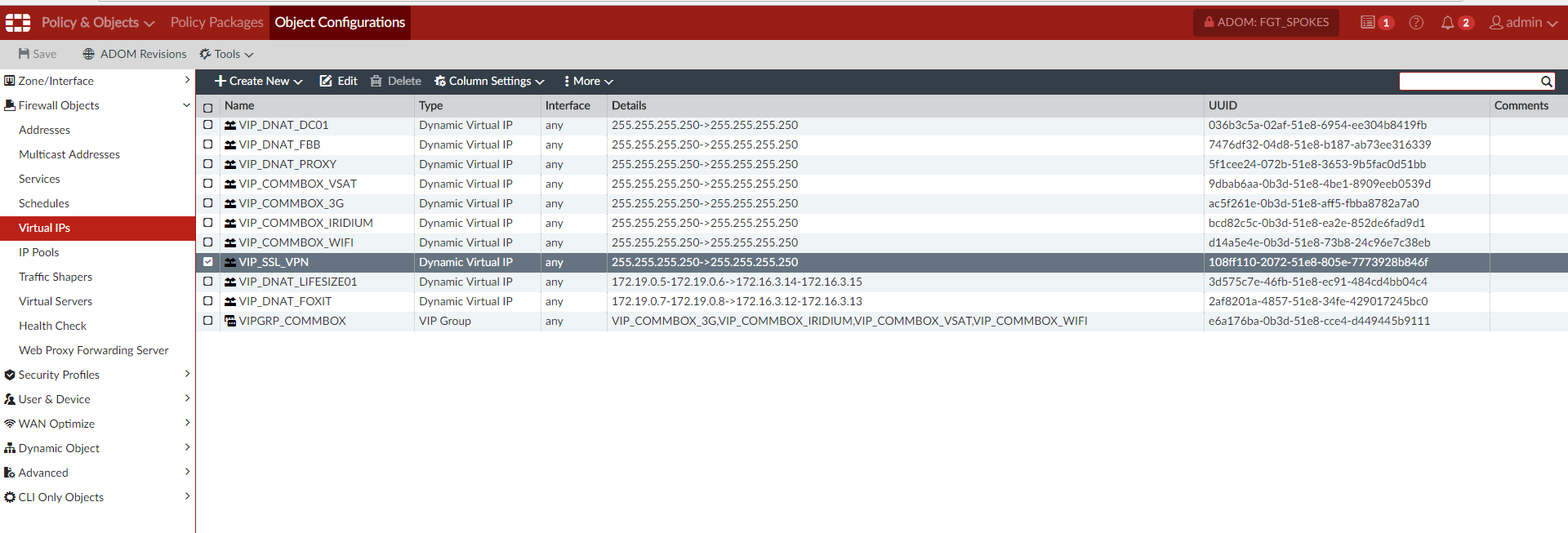
Maak de gewenste nieuwe policies aan voor het toelaten van het SSL VPN verkeer.  
Je kan hiervoor de policies van EQX gebruiken als voorbeeld (clone).  
Zorg dat je de column “install on” toevoegt via de column settings en jou site selecteert.  
Het is de bedoeling dat deze policies device specifiek zijn.  
  


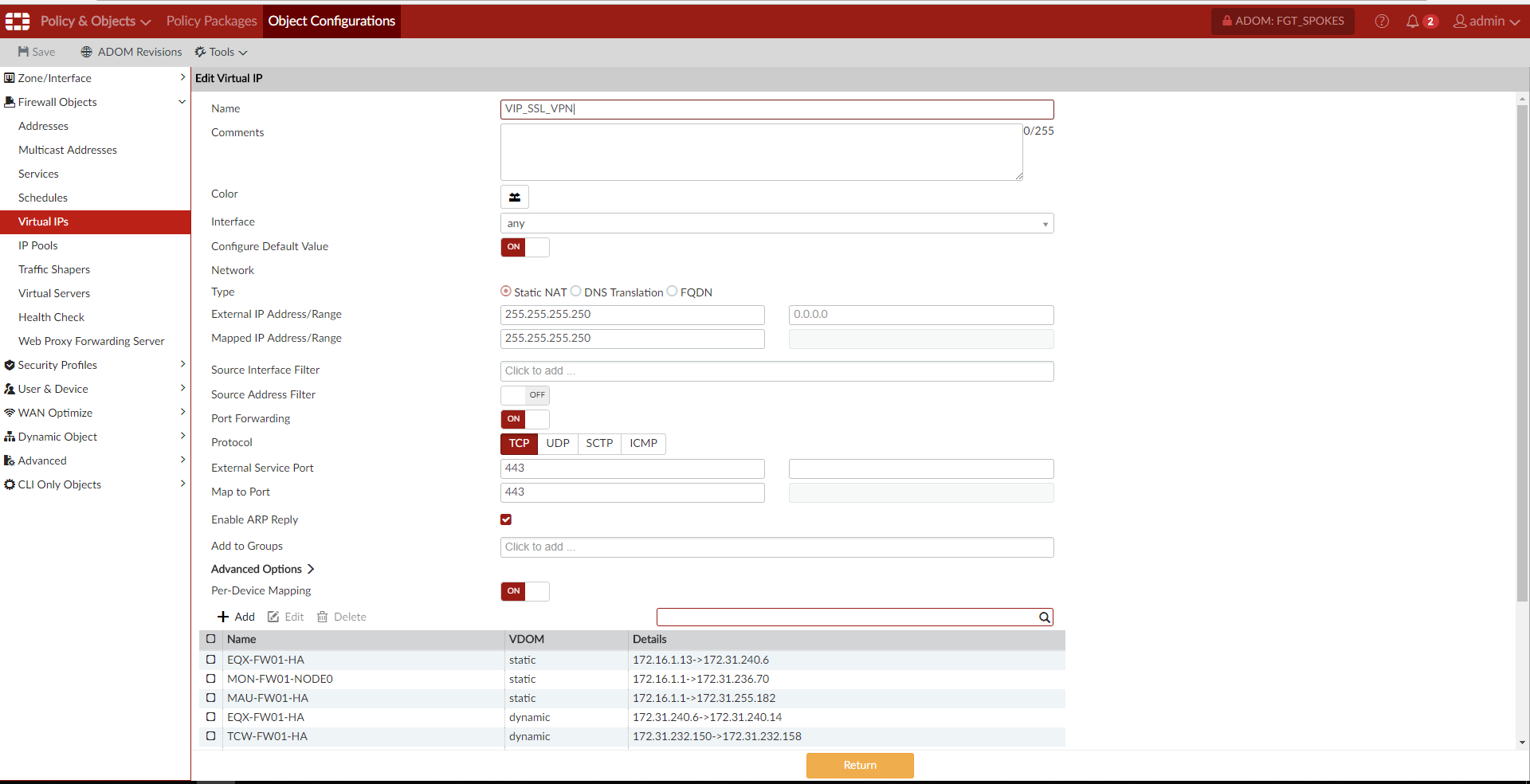


Voeg de Static VDOM ook toe aan de groep OFFICE\_STATIC\_SSL\_VPN.



Controleer ook even de per device mapping van het Virtual IP object “VIP\_SSL\_VPN”.  
Dit gebeurt normaal gezien door het install script voor nieuwe rollouts, maar sites uitgerold met oude versie van het script bevatten deze config niet. Sowieso zal je bij elke rollout van een office met SSL VPN de source in static vdom manueel moeten aanpassen naar het publieke IP adres van de ISP1 (WAN) interface (port6 VLAN 200). By default staat dit ingesteld op 172.16.1.1. Dit betekent ook dat bij het wijzigen van ISP of publiek IP dit manueel zal aangepast moeten worden.  
  
Static:                   WAN(ISP1) -> VLINK1  
Dynamic:             VLINK1 -> npu0\_vlink1





De policy packages dienen opnieuw gedeployed te worden na deze aanpassingen.  
Hierna zou het mogelijk moeten zijn om op het publieke IP adres te connecteren via HTTPS en onderstaand scherm te krijgen.

