6.13 UPS gebruiken voor stroomuitval op te vangen

Het zijn niet altijd aanvallen van buitenaf die een bedreiging vormen voor de data op uw NAS. Uit eigen ervaring kan ik u vertellen dat een stroomuitval funest is voor een NAS. Nadat ik een kortsluiting had gehad, kreeg ik de NAS met geen mogelijkheid meer aan de praat. Een deel van de data kon ik door het optuigen van een LINUX-machine nog redden, maar ik had mijn lesje geleerd.

Door gebruik te maken van een Uninterruptible Power Supply (UPS) kan dataverlies en het kapot gaan van de NAS worden voorkomen. Als de stroom uitvalt, neemt de UPS het over. Hoelang de NAS dan nog kan blijven functioneren is afhankelijk van de kracht van de UPS. Mijn APC Back-UPS RS 900G zou in theorie een uur stroom moeten leveren als er twee 8-bay nassen op aangesloten zijn.

Direct of naar een aantal seconden, minuten of uren schakelt uw NAS over naar veilig modus. Concreet betekent dit dat de services worden beëindigd, de schijven worden unmount en het systeem wordt uitgeschakeld. Desgewenst kunt u instellen dat de NAS weer moet starten nadat de stroomuitval is verholpen.

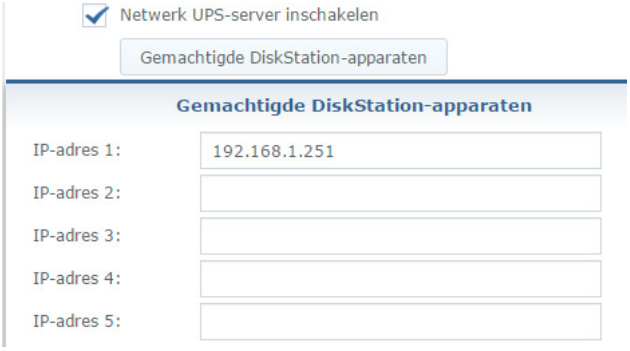
1. Sluit de UPS aan op uw NAS met de bijgeleverde UTP-naar USB-kabel. De USB-kabel kunt u aan de achterkant aansluiten op een USB-poort.
2. Sluit de UPS aan op uw netwerk met de bijgeleverde UTP-kabel.
3. Zorg dat u uw NAS met de stroomkabel is aangesloten op de master back-up van uw UPS.
4. Voorzie de UPS van stroom. Het kost de nodig tijd om de accu van de UPS volledig op te laden.
5. Log in op uw NAS en ga naar Configuratiescherm > Hardware en stroom.
6. U komt binnen op het tabblad Algemeen.
7. Plaats een vinkje bij Automatisch opnieuw starten na een stroomuitval.

8. Klik op het tabblad UPS.
9. Plaats een vinkje voor UPS-ondersteuning inschakelen.
10. Klik op de knop Apparaatgegevens en kijk of uw UPS wordt herkend.

11. Als uw UPS niet wordt herkend, start dan uw NAS opnieuw. Dit werkte bij mij in elk geval.
12. Plaats een vinkje voor Tijd voordat DiskStation naar veilige modus overschakelt en geef daar de tijd aan in seconden, minuten of uren. Schakelt u deze functie niet in dan gaat uw DiskStation pas in Veilige modus als de accu bijna leeg is.
13. Als u alleen maar uw NAS hebt aangesloten op uw UPS, dan is het geen probleem dat de UPS wordt uitgeschakeld als de NAS in veilige modus is gezet en dus uit staat. Zodra de stroomvoorziening is hersteld, zal zowel de UPS als uw NAS weer automatisch aan worden gezet. Houd er rekening mee, dat u uw router ook

voorziet van noodstroom als u uw NAS extern wil benaderen.

14. U kunt, afhankelijk van uw UPS, vijf andere nassen aansluiten op de noodstroomvoorziening. Plaats daarvoor een vinkje bij Netwerk UPS-server inschakelen en klik daarna op de knop Gemachtigde DiskStation-apparaten.



15. Geef hier het lokale IP-adres van uw andere nassen op in uw netwerk.
16. Op uw andere NAS gaat u ook naar Configuratiescherm > Hardware en stroom > UPS en plaatst u een vinkje bij UPS-ondersteuning inschakelen.

17. Geef bij Netwerk UPS-server IP het lokale IP-adres op van uw eerste NAS.
18. U kunt zelf nog bepalen of deze NAS direct met de server in veilige modus moet gaan of dat u daar een afwijkende tijd voor kiest.
19. Als u nu de stroomkabel van de UPS-server uit het stopcontact trekt, zal de UPS in werking treden.
20. U krijgt direct een melding van uw Synology NAS op uw desktop, via e-mail of DS Finder.

6.14 Firewall configureren

Uw Synology NAS beschikt over een eigen firewall. Door de firewallregels aan te passen kunt u alle IP-adressen, specifieke IP-adressen en complete regio's weigeren of toestaan van bepaalde poorten of applicaties gebruik te maken.

Het instellen van de firewallregels is niet moeilijk, maar het luistert wel nauw. Een verkeerde regel zorgt ervoor dat u of uw gebruikers op bepaalde momenten niet meer kunnen inloggen. Als u een regel probeert te maken die uzelf buitensluit, dan krijgt u daarvan direct een melding.

Bij het instellen van de firewallregels is het altijd handig om een tablet of telefoon bij de hand te hebben die gebruik kan maken van een extern IP-adres om de regels te testen. Het is verstandig eerst regels aan te maken die uzelf altijd toegang verlenen.

Firewallregels kunnen worden opgeslagen in een firewallprofiel. U kunt zelf profielen aanmaken na gelang uw eigen wensen. Na het kiezen van een profiel gaat u regels aanmaken. Zo'n regel geldt in eerste instantie voor alle interfaces (netwerkaansluitingen, PPPoE en VPN) op uw NAS. Het is handig om vooraf te weten, dat wanneer u de optie op alle interfaces laat staan u wel door een regel een bepaalde poort kunt beveiligen, maar dat alle andere gebruikte poorten op uw NAS open blijven staan.

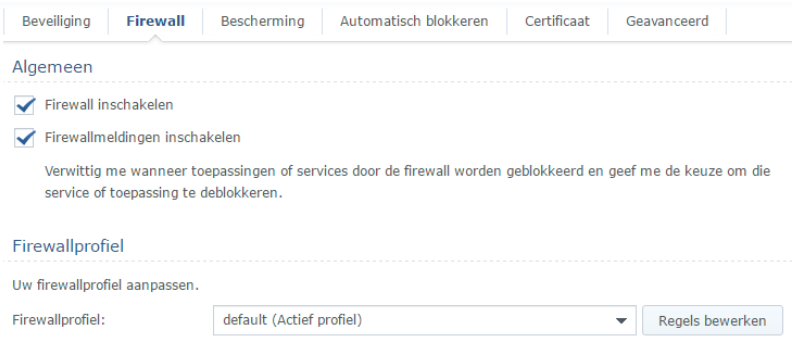
Kiest u als interface een specifieke netwerkverbinding van uw NAS, dan krijgt u de vraag wat er moet gebeuren als er niet voldaan wordt aan de regels. Gaat u de toegang dan weigeren of staat u de toegang toe.

Als u hier kiest voor Toegang weigeren, dan betekent dit dat u voor alle applicaties op uw NAS regels zult moeten aanmaken als die er nog niet zijn. Een voorbeeld. Stel u wilt dat alle IP-adressen toegang mogen krijgen tot uw DSM-poorten. Dat is handig, want dan kunt u vrijelijk uw mobiele telefoon gebruiken in de hele wereld om toegang te krijgen tot uw NAS. U maakt daarvoor een regel aan en kiest voor de optie Toegang weigeren als niet aan de regels wordt voldaan.

De consequentie is nu, dat u nu geen gebruik meer kunt maken van VPN of apart File Station of Audio Station kunt benaderen via hun directe poorten. U zult dus voor alle andere applicaties op die op uw NAS draaien regels moeten aanmaken om toegang te verlenen. Kiest u voor de optie Toegang toestaan als er niet aan de regels wordt voldaan, dan kunt u wel bij die overige applicaties, mits u daarvoor de rechten heeft en de poorten zijn geforward op uw router.

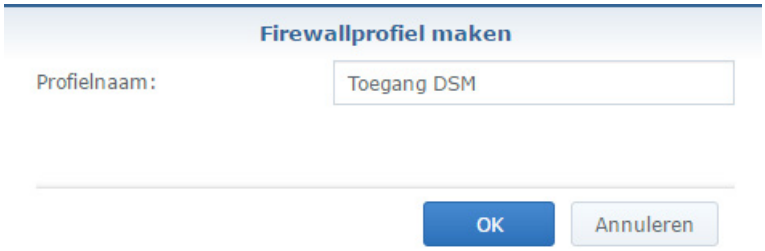
6.14.1 Firewallregels om alleen uzelf toegang te verlenen

Er zijn tientallen voorbeelden te geven om een regel aan te maken voor de firewall. Ik kies als voorbeeld voor een aantal regels die u toegang geven tot de loginpagina van uw DSM en de rest van de wereld buitensluiten. U kunt daarna op uw DSM inloggen als u werkt binnen uw lokale netwerk, gebruik maakt van het externe IP-adres van uw NAS en als u via VPN inlogt.



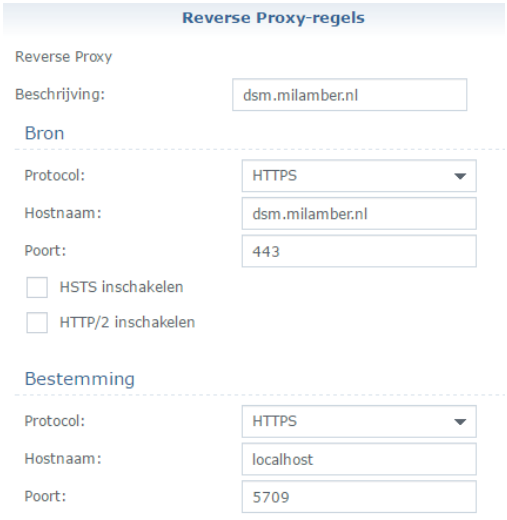
1. Ga naar Configuratiescherm > Beveiliging.
2. Klik op het tweede tabblad Firewall.
3. Plaats een vinkje bij Firewall inschakelen en bij Firewallmeldingen inschakelen.
4. Klik op het pijltje bij Firewallprofiel en klik op het plusteken om een nieuw

profiel te maken.



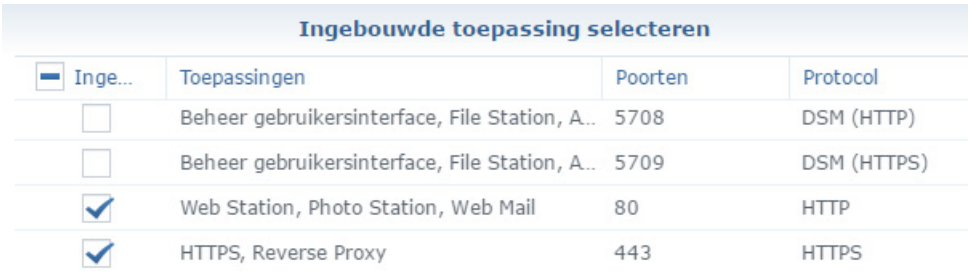
5. Selecteer het profiel en klik op Regels bewerken. In het venster dat nu verschijnt, komen straks de regels te staan voor dit profiel. Deze regels kunnen worden toegepast op alle interfaces of op een interface naar keuze.

6. Selecteer als interface de LAN waarop uw NAS is aangesloten en klik op Maken.
7. Eerder heb ik aandacht besteed aan Reverse Proxy. Toen heb ik laten zien, dat u al het verkeer over poort 80 of 443 kunt laten lopen om te kunnen inloggen op de NAS. De Reverse Proxy zorgt ervoor dat het verkeer afkomstig van poort 80 of 443 door wordt gestuurd naar het poortnummer van DSM.
8. Door het instellen van de firewallregels kunt u nu bepalen wie er toegang krijgt tot die poorten. De eerste twee regels die u wilt aanmaken zijn de regels die u toegang verlenen; zowel intern (uw lokale netwerk) als extern (het externe IP-adres van uw NAS).

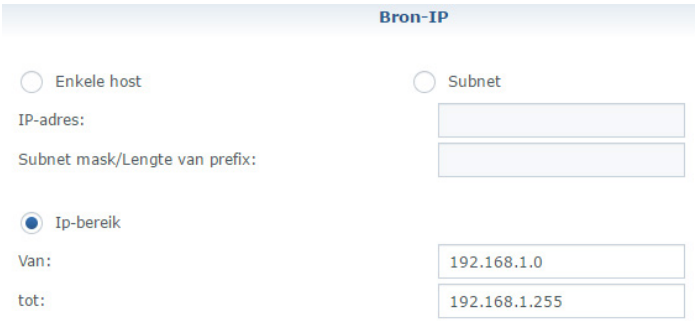


9. De eerste stap bij het maken van een regel is, dat u de poort(en) selecteert die moeten worden beveiligd. U kunt in één keer alle poorten selecteren door de optie Alles te kiezen, u kunt uit de lijst met toepassingen een

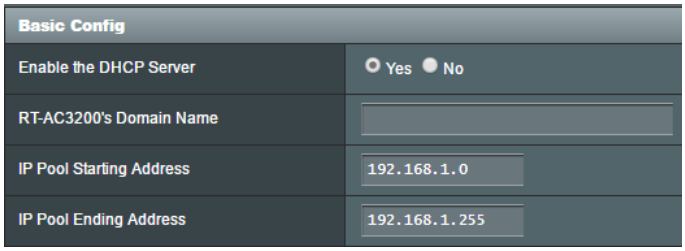
toepassing selecteren met bijbehorende poorten of u kunt de optie Aangepast kiezen om zelf een poort op te geven. Selecteer de optie Selecteer uit een lijst met ingebouwde toepassingen en klik op de knop Selecteren.



10. Maakt u gebruik van Reverse Proxy, selecteer dan de poorten 80 en 443. Maakt u geen gebruik van Reverse Proxy maar van de reguliere DSM-poorten, kies dan de twee DSM-poorten die u gebruikt. Klik op OK.
11. Vervolgens geeft u aan welke IP-adressen gebruik mogen maken van deze poorten. Klik onder Bron IP op Specifiek IP en klik op de knop Selecteren.



12. U kunt een enkel IP-adres opgeven of een reeks IP-adressen. Als u wilt dat u binnen uw netwerk met alle pc's kunt inloggen, dan selecteert u IP-bereik en geeft u de range op van uw lokale netwerk. U kunt deze reeks achterhalen bij uw DHCP-instellingen van uw router.



13. Klik op OK en zorg dat onder Actie de optie Toestaan is aangevinkt. Klik op OK.

14. De regel staat nu in de lijst. Selecteer onderin dit scherm de optie Toegang weigeren als er niet wordt voldaan