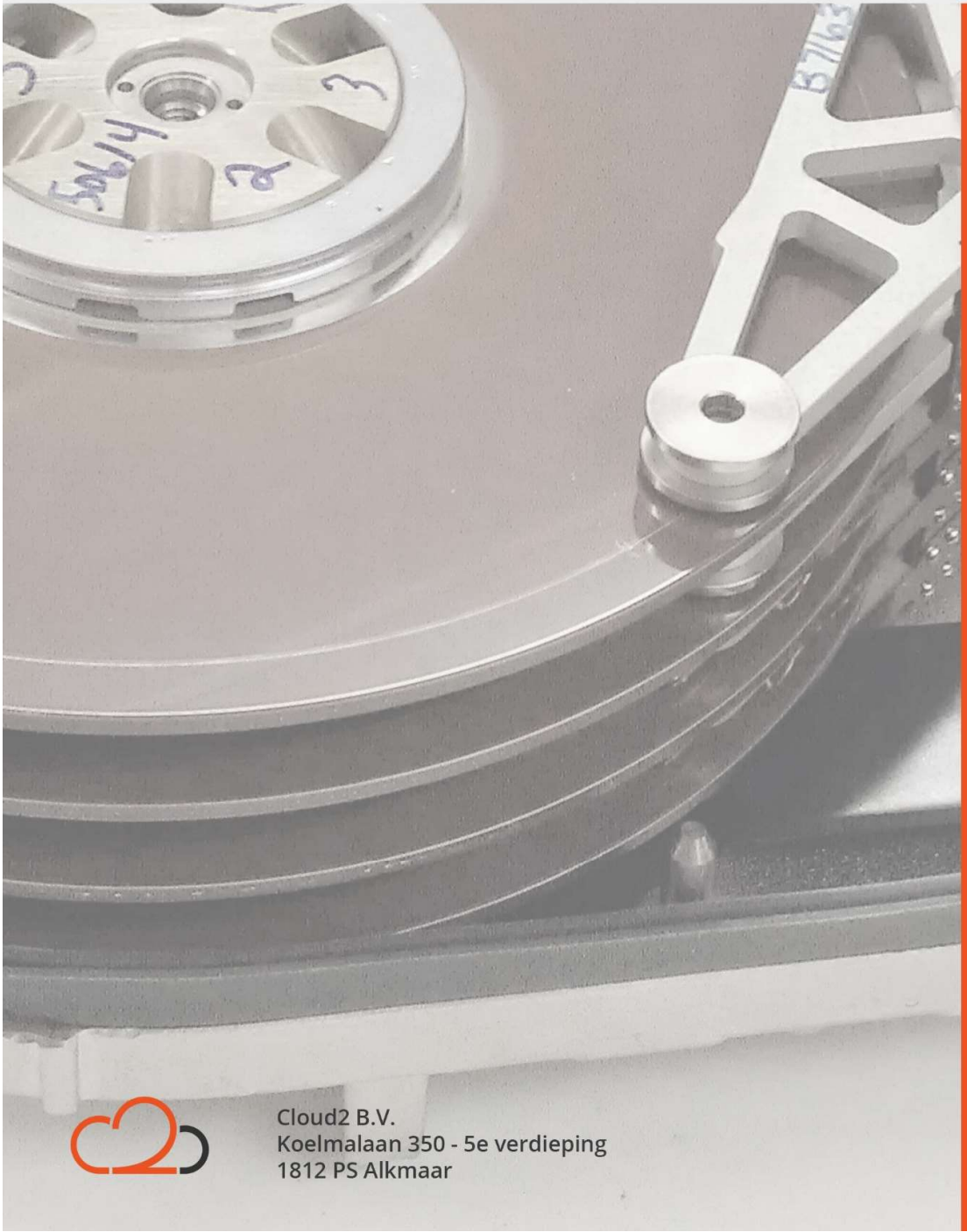
RDP Beschikbaar maken



Cloud2 B.V.
Koelmalaan 350 - 5e verdieping
1812 PS Alkmaar

Contents

RDP Beschikbaar maken

Deze manual beschrijft welke stappen ondernomen moeten worden om RDP beschikbaar te maken voor de IaaS omgeving.

STAPPEN

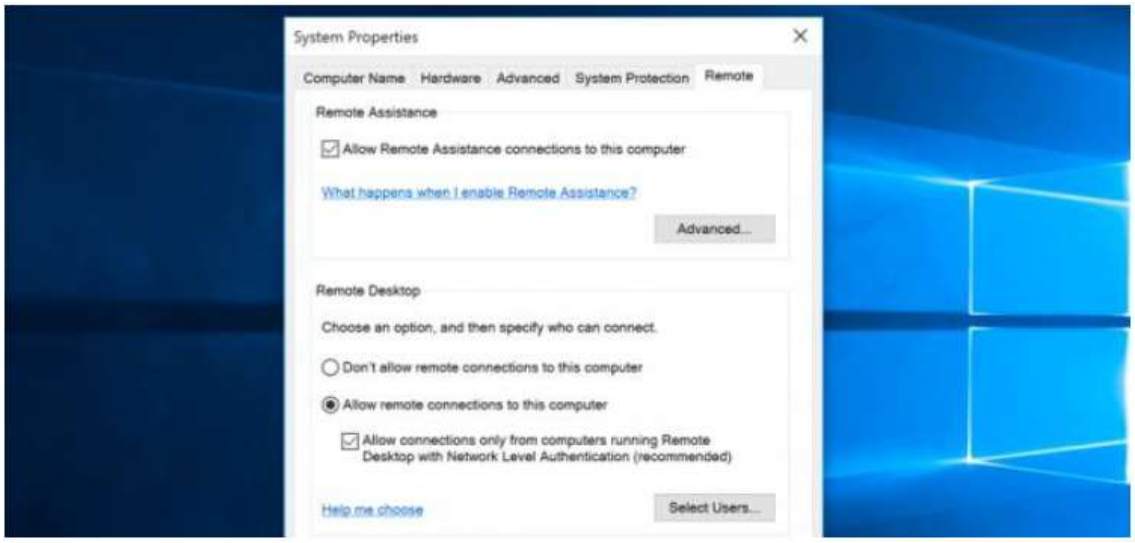
De volgende stappen zullen ondernomen worden:

- Verbindingen via RDP openzetten in Windows;
- Aanpassen van Windows Firewall;
- Sophos UTM Firewall configureren;
- Stappen om te verbinden;
- Troubleshooting.

VERBINDINGEN VIA RDP OPENZETTEN IN WINDOWS

Ga in Windows 10 naar start en tik hier in 'Allow remote access', kies vervolgens voor 'Allow remote access to your computer' zoals in onderstaand scherm naar voren komt:

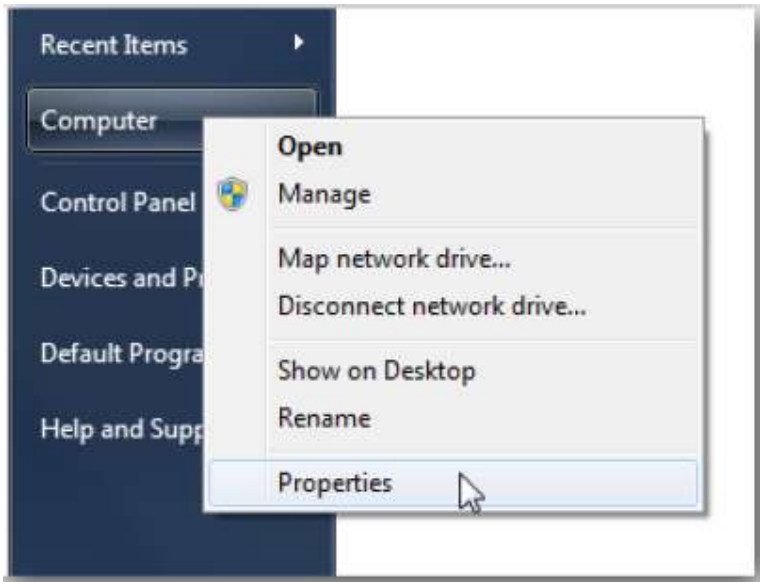
Daarna kan het vinkje aangezet worden bij 'Allow remote connections to this computer'.



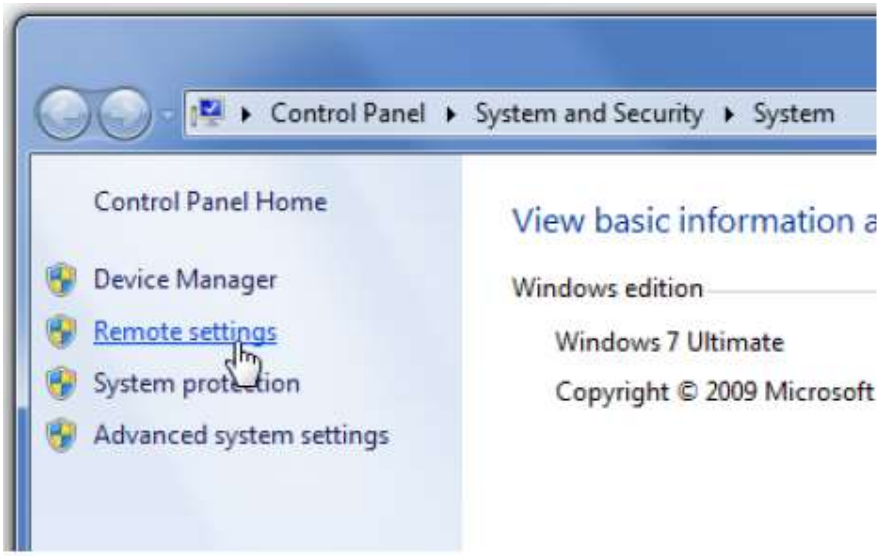
U kunt vervolgens nog aangeven welke users er connectie mogen maken of dat oudere Windows versies ook connectie kunnen maken.

Als u gebruikt maakt van Windows 7 of Vista kunt u het volgende doen om de bovenstaande configuratie in te stellen.

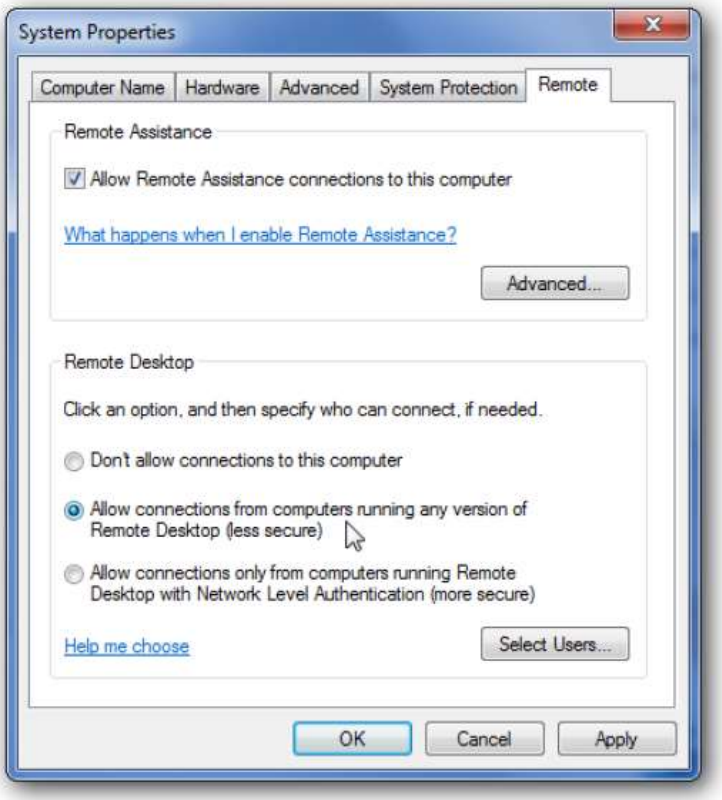
Om het Configuratiescherm naar voren te halen kunt u via Start het onderstaande scherm naar voren halen om daar vervolgens met de rechtermuisknop te klikken op Computer en dan te kiezen voor Properties:



Kies daarna aan de linkerkant voor ‘Remote setings’.



Hier kunt u dan vervolgens de instellingen aanpassen en dan de functie ‘Allow connections from computers running any version of Remote Desktop (les secure)’ aanzetten.



SECURITY SETTINGS

Een aantal basic security settings moeten handmatig aangezet worden om ervoor te zorgen dat de RDP server zoveel mogelijk beschermd wordt. Denk hierbij vooral aan het locken van accounts na meerdere inlogpogingen en het bijhouden van inlogpogingen. Hiermee kun je bijv. brute force aanvallen enorm vertraging.

Om een Account Lockout Policy in te stellen doe je het volgende:

1. Klik op de Start knop en kies voor Uitvoeren.
2. Type vervolgens secpol.msc in en druk op Enter.
3. Navigeer naar Account Policies → Account Lockout Policy.
4. Klik met de rechtermuisknop op 'Account lockout threshold' en kies Properties.
5. Geef het aantal toegestane inlogpogingen en kies voor OK.
6. Windows vult zelf de 'Account lockout duration' en 'Reset account lockout counter after' in met de standaard waarde van 30 minuten. Deze kunnen aangepast worden door op de policies te klikken en de te kiezen voor Properties. Na de aanpassen kies je voor OK.

Om de inlogpogingen op de machine bij te houden doe je het volgende:

1. Klik op de Start knop en kies voor Uitvoeren.
2. Type vervolgens secpol.msc en druk op Enter.
3. Navigeer naar Local Policy → Audit Policy.
4. Klik met de rechteruisknop op 'Audit account logon events' en kies voor Properties.
5. Check de Failure box aan en kies voor OK.
6. Klik vervolgens met de rechtermuisknop op 'Audit logon events policy' en kies voor Properties.
7. Check de Failure box aan en kies voor OK.

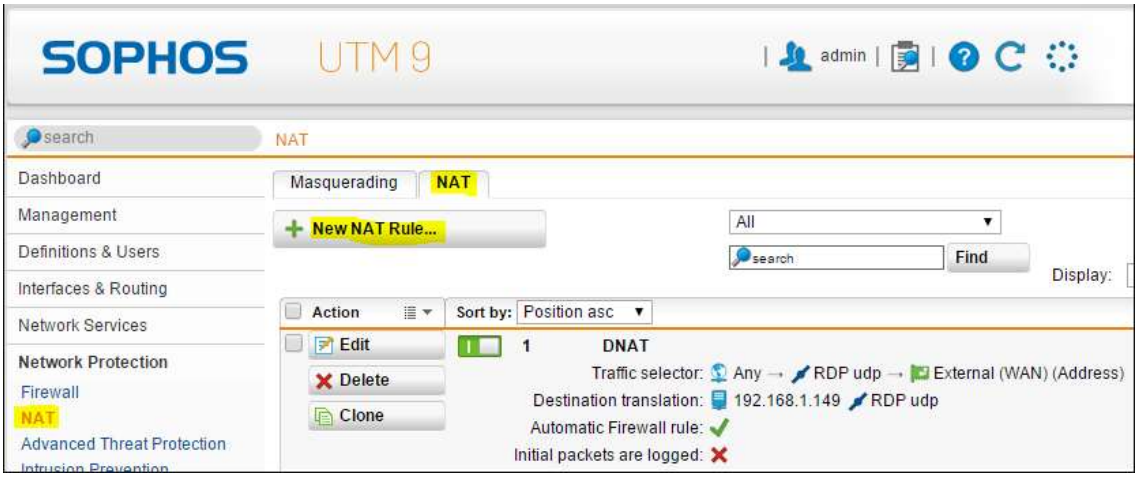
Hiermee is een basic laag van security toegevoegd aan de machine. De inlogpogingen kun je nu controleren in de logfiles welke te vinden zijn in de Event Viewer (eventvwr.msc).

AANPASSEN WINDOWS FIREWALL

1. Navigeer naar Control Panel → All Control Panel Items (small icons) → Windows Firewall.
2. Linksboven selecteert u 'Allow an app for feature through Windows Firewall'.
3. Navigeer naar Remote Desktop en vink aan: Public.

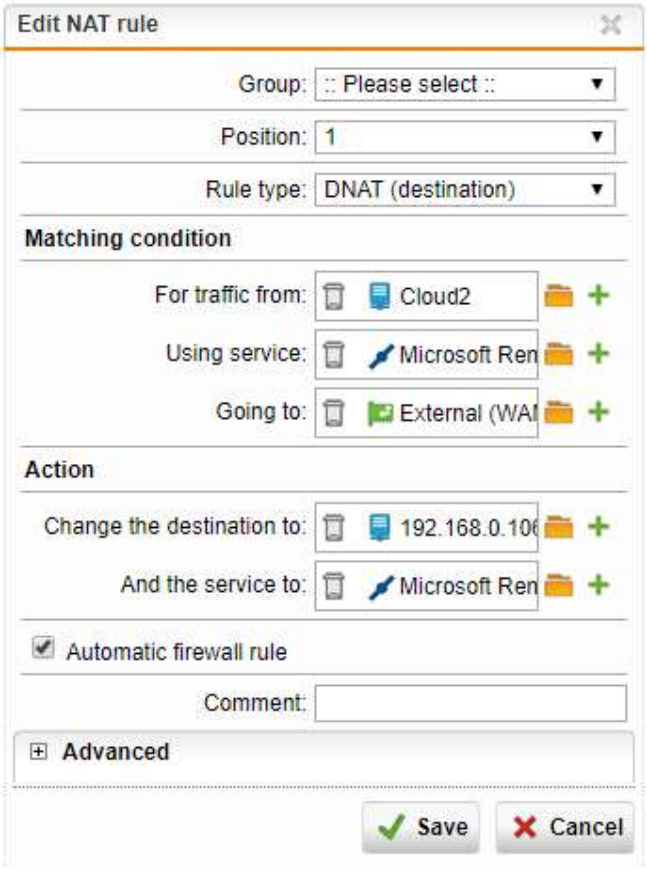
SOPHOS UTM FIREWALL CONFIGUREREN

In de Sophos UTM wereld wordt er niet gesproken over port forwards, er wordt gesproken over een destination NAT of DNAT. Dit wordt ingesteld via de webportal onder Network Protection → NAT → Tabblad NAT.



Hierboven ziet u een voorbeeld van een regel die gebruikt wordt om een RDP connectie te starten.

- Bij **rule type** kies voor DNAT;
- Bij Matching condition – For traffic from – Dit kunt u op **Any** zetten zodat elke host toegang krijgt of u kunt hier specifieke hosts opgeven zodat de toegang tot enkel die hosts gelimiteerd wordt.
- Bij **User Service** kiest u voor een nieuwe service door op de plus te klikken. Vervolgens kunt u kiezen voor de service Microsoft Remote Desktop.
- Het **Going to** veld wordt ingevuld met het **External (WAN)** netwerk omdat iedereen die connectie wilt maken gebruik gaat maken van het WAN IP adress.
- Bij **Action** en **Change the destination to** geeft u het specifieke interne IP adres van de host op waar connectie naar gemaakt moet worden.
- En bij het veld **And the service** to wordt dezelfde service opgegeven als eerder, **Microsoft Remote Desktop**.
- Verifieer of het vinkje aanstaat bij **Automatic firewall rule** zodat er automatisch een firewall rule wordt aangemaakt.



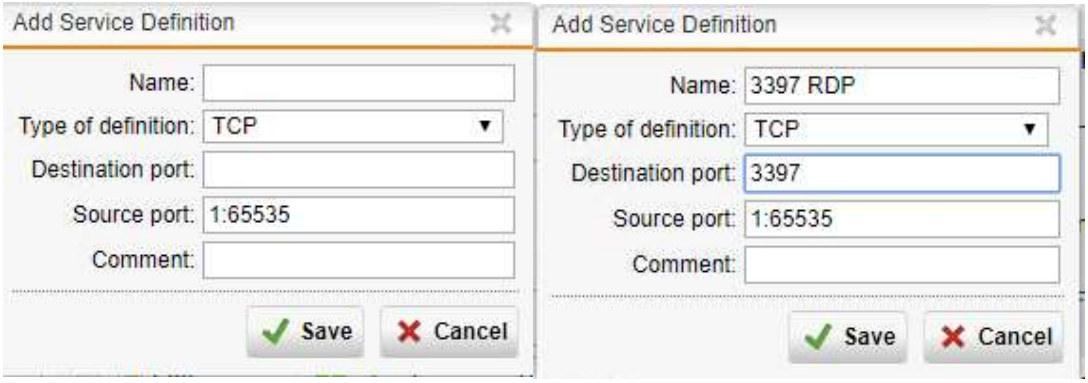
Na het instellen van de bovengenoemde gegevens, kies voor Save. Het kan ook handig zijn om het **Comment** veld te gebruiken voor een korte beschrijving van de NAT regel. Hiermee wordt het zoeken naar bepaalde regels makkelijker. Zodra de regel is opgeslagen, check of de **groene slider** naar rechts is geschoven zodat hij geactiveerd is.

Dit bovenstaande proces werkt in het algemeen voor alle services mochten die vanuit extern benaderd moeten worden. Let er echter op dat met de NAT/port forward een bepaalde host dus openbaar gesteld wordt naar buiten toe.

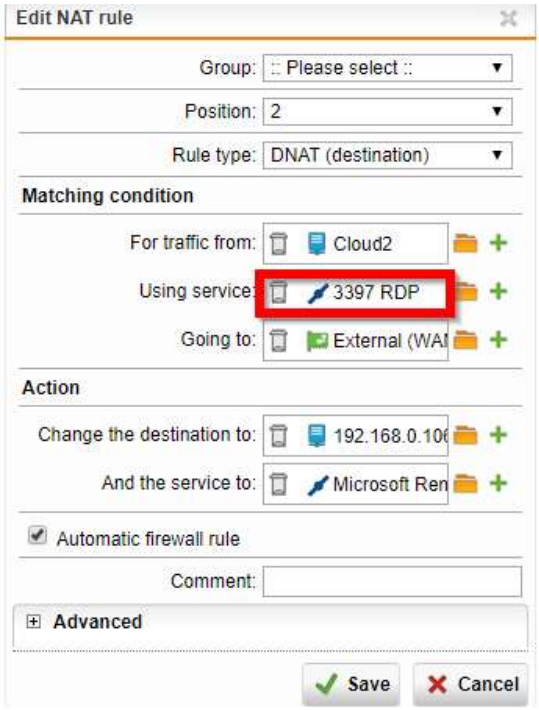
TOEVOEGEN TWEEDE RDP SERVER

Voor het toevoegen van meerdere RDP servers kunt u de stappen volgen onder het kopje Sophos UTM firewall configureren. Hieronder wordt beschreven hoe de RDP luisterpoort aangepast kan worden.

Eerst moet er een service aangemaakt worden onder matching conditions. K. Wanneer u daar op heeft geklikt komt het volgende scherm naar voren. Dit scherm vult u in met de condities waar deze service aan moet voldoen.



Wanneer dit ingevuld is klikt u op Save. Wanneer u op Save heeft geklikt ziet u het volgende scherm. De net aangemaakte service wordt geplaatst op de “lege” plek van Using Service.



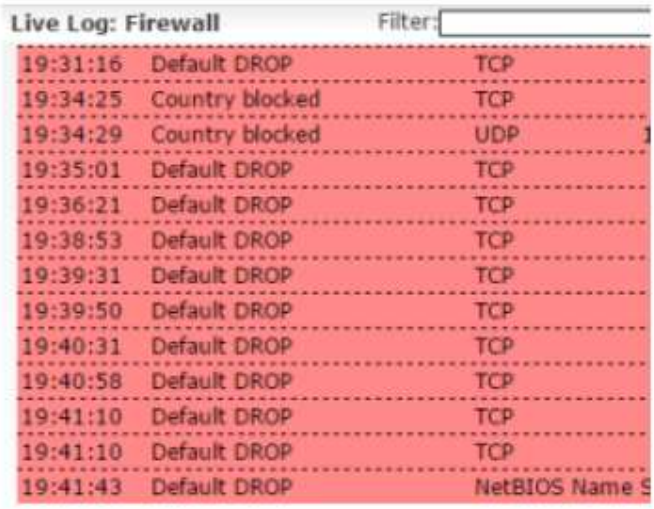
Na het instellen van de bovengenoemde gegevens, kies voor Save. Activeer hierna de nieuwe NAT rule, dit doet u door de slider naar rechts is verschoven, zodat deze groen kleurt.

STAPPEN OM TE VERBINDEN

1. Start Remote Desktop Connection en verbind met het externe IP adres inclusief het poortnummer.
2. Vul het domeinnaam\user in OF machinenaam\user;
3. Verbind met succes.

TROUBLESHOOTING

Zodra er een NAT regel of gewone firewall regel nagekeken moet worden, kan er gebruik gemaakt worden van de Live Firewall log. Hier wordt vrij snel duidelijk of een regel goed is ingesteld en of hij werkt of niet.



De Live Firewall log vindt u onder Network Protection → Firewall → Open Live Log. Hier worden de real time logs weergegeven.