

DrayTek

Firewall
SMTP & FTP



Firewall Configuratie

In deze handleiding gaan we een aantal voorbeelden geven hoe u een bepaalde situatie kunt oplossen door middel van een aantal Filter Rules.

Situatie 1

U maakt gebruik van een e-mail server in uw interne netwerk, het is de bedoeling dat alleen deze e-mail server gebruik mag maken van TCP poort 25 uitgaand. Dit is eenvoudig te configureren in de Firewall configuratie van de DrayTek.

U gaat naar het Firewall >> Filter Setup menu, en maakt hier een nieuwe filter regel aan. In de eerste firewall regel maakt u een Blokkade aan voor al het uitgaande verkeer naar TCP poort 25. Wanneer deze regel actief is zal niemand gebruik kunnen maken van TCP poort 25 uitgaand.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Enable

Comments

Schedule Profile , , ,

Clear sessions when schedule is ON

Direction

Source IP/Country

Destination IP/Country

Service Type

Fragments

| Application | Action/Profile | Syslog |
|----------------------------|--|--------------------------|
| Filter | <input type="text" value="Block If No Further Match"/> | <input type="checkbox"/> |
| Branch to Other Filter Set | <input type="text" value="None"/> | |
| Sessions Control | <input type="text" value="0 / 50000"/> | <input type="checkbox"/> |
| MAC Bind IP | <input type="text" value="Non-Strict"/> | <input type="checkbox"/> |
| <u>Quality of Service</u> | <input type="text" value="None"/> | <input type="checkbox"/> |
| <u>User Management</u> | <input type="text" value="None"/> | <input type="checkbox"/> |
| <u>APP Enforcement</u> | <input type="text" value="None"/> | <input type="checkbox"/> |
| <u>URL Content Filter</u> | <input type="text" value="None"/> | <input type="checkbox"/> |
| <u>Web Content Filter</u> | <input type="text" value="None"/> | <input type="checkbox"/> |
| <u>DNS Filter</u> | <input type="text" value="None"/> | <input type="checkbox"/> |

Advance Setting

Bij het configureren van de Service Type is het belangrijk dat alleen Destination port wordt geconfigureerd, zoals op onderstaande afbeelding te zien is. De Source Port is een pseudo poort welke door de DrayTek wordt gebruikt voor inkomend & uitgaand verkeer.

De configuratie van de Service Type in deze Firewall regel zal er als volgt uitzien:

Service Type Edit

Service Type: User defined

Protocol: TCP 6

Source Port: = 1 ~65535

Destination Port: = 25 ~25

Service Group: None

Service Object: None, None, None

OK Close

De e-mail server heeft op dit moment nog geen toegang tot TCP poort 25 uitgaand, daarom zult u nog een Firewall regel aan moeten maken voor 1 bepaald Source IP-Address. Indien u onderstaande Firewall Regel overneemt zal alleen 192.168.1.254 gebruik kunnen maken van TCP poort 25 uitgaand.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Enable

Comments: SMTP Pass

Schedule Profile: None, None, None, None

Clear sessions when schedule is ON

Direction: LAN/DMZ/RT/VPN -> WAN [Advanced]

Source IP/Country: 192.168.1.254 [Edit]

Destination IP/Country: Any [Edit]

Service Type: TCP, Port: from any to 25 [Edit]

Fragments: Don't Care

| Application | Action/Profile | Syslog |
|----------------------------|------------------|--------------------------|
| Filter | Pass Immediately | <input type="checkbox"/> |
| Branch to Other Filter Set | None | <input type="checkbox"/> |
| Sessions Control | 0 / 50000 | <input type="checkbox"/> |
| MAC Bind IP | Non-Strict | <input type="checkbox"/> |
| Quality of Service | None | <input type="checkbox"/> |
| User Management | None | <input type="checkbox"/> |
| APP Enforcement | None | <input type="checkbox"/> |
| URL Content Filter | None | <input type="checkbox"/> |
| Web Content Filter | None | <input type="checkbox"/> |
| DNS Filter | None | <input type="checkbox"/> |

Advance Setting [Edit]

OK Clear Cancel

Situatie 2

U maakt gebruik van een FTP server in uw interne netwerk, deze FTP server zal wanneer u een port forwarding of open port regel aanmaakt bereikbaar zijn voor het hele internet. Nu kunt u de Firewall van de DrayTek zo configureren dat alleen bepaalde Public IP-adressen toegang krijgen tot de FTP server.

Het aanmaken van de firewall regels zal bijna hetzelfde zijn als situatie 1. Als eerste maakt u een blokkade aan voor al het inkomend verkeer naar poort 21. Deze regel zal er als volgt uitzien.

The screenshot shows the configuration for a firewall rule named 'Filter Set 2 Rule 2'. The rule is enabled and has the comment 'Block FTP'. The schedule profile is set to 'None'. The direction is 'WAN -> LAN/DMZ/RT/VPN'. The source IP is 'Any' and the destination IP is '192.168.1.253'. The service type is 'TCP, Port: from any to 21'. The action is 'Block If No Further Match'. The sessions control is set to '0 / 50000'. The MAC bind IP is 'Non-Strict'. The quality of service, user management, app enforcement, URL content filter, web content filter, and DNS filter are all set to 'None'. The syslog checkbox is unchecked. There are 'OK', 'Clear', and 'Cancel' buttons at the bottom.

| Application | Action/Profile | Syslog |
|----------------------------|---------------------------|--------------------------|
| Filter | Block If No Further Match | <input type="checkbox"/> |
| Branch to Other Filter Set | None | <input type="checkbox"/> |
| Sessions Control | 0 / 50000 | <input type="checkbox"/> |
| MAC Bind IP | Non-Strict | <input type="checkbox"/> |
| Quality of Service | None | <input type="checkbox"/> |
| User Management | None | <input type="checkbox"/> |
| APP Enforcement | None | <input type="checkbox"/> |
| URL Content Filter | None | <input type="checkbox"/> |
| Web Content Filter | None | <input type="checkbox"/> |
| DNS Filter | None | <input type="checkbox"/> |

De configuratie van de Service Type in deze Firewall regel zal er als volgt uitzien:

Service Type Edit

| | | | |
|--|----------------|--------|---------|
| Service Type | User defined ▼ | | |
| Protocol | TCP ▼ | 6 | |
| Source Port | = ▼ | 1 | ~ 65535 |
| Destination Port | = ▼ | 21 | ~ 21 |
| Service Group | None ▼ | | |
| Service Object | None ▼ | None ▼ | None ▼ |
| <input type="button" value="OK"/> <input type="button" value="Close"/> | | | |

Op dit moment wordt al het verkeer naar poort 21 door de DrayTek geblokkeerd. Nu hoeft u alleen nog maar een nieuwe filter regel aan te maken waarin u aangeeft dat een bepaald Public IP-adres wel toegang mag hebben tot de FTP server.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 2

| | | | |
|--|---|---|--------|
| <input checked="" type="checkbox"/> Enable | | | |
| Comments | Pass FTP | | |
| <u>Schedule Profile</u> | None ▼ | None ▼ | None ▼ |
| | <input type="checkbox"/> Clear sessions when schedule is ON | | |
| Direction | WAN -> LAN/DMZ/RT/VPN ▼ | <input type="button" value="Advanced"/> | |
| Source IP/Country | 11.22.33.44 | <input type="button" value="Edit"/> | |
| Destination IP/Country | 192.168.1.253 | <input type="button" value="Edit"/> | |
| Service Type | TCP, Port: from any to 21 | <input type="button" value="Edit"/> | |
| Fragments | Don't Care ▼ | | |
| Application | Action/Profile | Syslog | |
| Filter | Pass Immediately ▼ | <input type="checkbox"/> | |
| Branch to Other Filter Set | None ▼ | | |
| Sessions Control | 0 / 50000 | <input type="checkbox"/> | |
| MAC Bind IP | Non-Strict ▼ | <input type="checkbox"/> | |
| <u>Quality of Service</u> | None ▼ | <input type="checkbox"/> | |
| <u>User Management</u> | None ▼ | <input type="checkbox"/> | |
| <u>APP Enforcement</u> | None ▼ | <input type="checkbox"/> | |
| <u>URL Content Filter</u> | None ▼ | <input type="checkbox"/> | |
| <u>Web Content Filter</u> | None ▼ | <input type="checkbox"/> | |
| <u>DNS Filter</u> | None ▼ | <input type="checkbox"/> | |
| Advance Setting | <input type="button" value="Edit"/> | | |
| <input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/> | | | |

Belangrijk : Indien u een nieuwe Filter Set aanmaakt, bijvoorbeeld Filter Set 3 dan dient u bij Filter Set 2 aan te geven dat de Firewall tevens Filter Set 3 moet meenemen in de Firewall. Wanneer u dit niet doet zullen alle Firewall regels in Filter Set 3 niet actief zijn.

Zoals u ziet op onderstaande afbeelding kunt u de Next Filter Set aanpassen, hier geeft u vervolgens de Filter Set op welke de DrayTek moet activeren na Filter Set 2.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2
 Comments :

| Rule | Enable | Comments | Direction | Src IP | Dst IP | Service Type | Action | CSM | Move Up | Move Down |
|------|-------------------------------------|-----------------|-----------------------|-------------|---------------|-----------------------------------|---------------------------|-----|--------------------|----------------------|
| 1 | <input checked="" type="checkbox"/> | xNetBios -> DNS | LAN/DMZ/RT/VPN -> WAN | Any | Any | TCP/UDP, Port: from 137~139 to 53 | Block Immediately | | | Down |
| 2 | <input checked="" type="checkbox"/> | Block FTP | WAN -> LAN/DMZ/RT/VPN | Any | 192.168.1.253 | TCP, Port: from any to 21 | Block If No Further Match | | UP | Down |
| 3 | <input checked="" type="checkbox"/> | Pass FTP | WAN -> LAN/DMZ/RT/VPN | 11.22.33.44 | 192.168.1.253 | TCP, Port: from any to 21 | Pass Immediately | | UP | Down |
| 4 | <input type="checkbox"/> | | LAN/DMZ/RT/VPN -> WAN | Any | Any | Any | Pass Immediately | | UP | Down |
| 5 | <input type="checkbox"/> | | LAN/DMZ/RT/VPN -> WAN | Any | Any | Any | Pass Immediately | | UP | Down |
| 6 | <input type="checkbox"/> | | LAN/DMZ/RT/VPN -> WAN | Any | Any | Any | Pass Immediately | | UP | Down |
| 7 | <input type="checkbox"/> | | LAN/DMZ/RT/VPN -> WAN | Any | Any | Any | Pass Immediately | | UP | |

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12

Wizard Mode: most frequently used settings in three pages
 Advance Mode: all settings in one page

Next Filter Set



Voorbehoud

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

Copyright verklaring

© 2020 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

Trademarks

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.