

DrayTek

Firewall
Object Based



Firewall Cases

In deze handleiding gaan we een voorbeeld geven hoe u een bepaalde situatie kunt oplossen doormiddel van een aantal Firewall >> Filter Rules.

Situatie: Bedrijf

U heeft van de directeur een opdracht gekregen om voor zijn bedrijf enkele firewall regels aan te maken. Het bedrijf bestaat uit 2 afdelingen; een verkoop afdeling en een support afdeling. Tevens heeft elke afdeling een afdelingshoofd. Voor de volgende groepen moet u regels aanmaken:

- **Directeur:** 192.168.1.2
- **Hoofd afdeling Verkoop:** 192.168.1.20
- **Afdeling Verkoop:** 192.168.1.21 t/m 192.168.1.39
- **Hoofd afdeling Support:** 192.168.1.40
- **Afdeling Support:** 192.168.1.41 t/m 192.168.1.45

De directeur wil dat de afdeling verkoop en support alleen gebruik mogen maken van poort 80. Hij wil voor zijn afdelingshoofden en zichzelf volledig toegang.

U begint met het aanmaken van verschillende IP-Objecten voor de verschillende afdelingen, dit kunt u doen bij 'Objects Settings >> IP-Objects'. U maakt een nieuw object aan door op een bepaald nummer te klikken.

Als eerste maakt u een IP-Object aan voor de directeur, zoals u ziet op onderstaande afbeelding. Hiervoor maakt u gebruik van de LAN interface, en bij Address type selecteert u 'Single Address'.

Objects Setting >> IP Object

Profile Index : 1

Name:	Directeur
Interface:	LAN/DMZ/RT/VPN ▾
Address Type:	Single Address ▾
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.2 <input type="button" value="Select"/>
End IP Address:	0.0.0.0 <input type="button" value="Select"/>
Subnet Mask:	255.255.255.254 / 31 ▾
Invert Selection:	<input type="checkbox"/>

Next >>

Vervolgens gaat u een IP-Object aanmaken voor de verkoop afdeling, hierbij maakt u gebruik van een reeks IP-adressen. Bij Interface selecteert u wederom de LAN kant, aangezien de verkoop afdeling aangesloten is op het interne netwerk.

Objects Setting >> IP Object

Profile Index : 2

Name:	Afd. Verkoop
Interface:	LAN/RT/VPN ▾
Address Type:	Range Address ▾
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.21 <input type="button" value="Select"/>
End IP Address:	192.168.1.39 <input type="button" value="Select"/>
Subnet Mask:	255.255.255.254 / 31 ▾
Invert Selection:	<input type="checkbox"/>

<< Previous

Next >>

Hetzelfde doet u voor de support afdeling, hierbij gebruikt u ook de LAN interface.

Objects Setting >> IP Object

Profile Index : 3

Name:	Afd. Support
Interface:	LAN/RT/VPN ▾
Address Type:	Range Address ▾
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.41 <input type="button" value="Select"/>
End IP Address:	192.168.1.45 <input type="button" value="Select"/>
Subnet Mask:	255.255.255.254 / 31 ▾
Invert Selection:	<input type="checkbox"/>

<< [Previous](#) [Next](#) >>

U moet nu alleen nog twee IP-Objecten aanmaken voor de afdelingshoofden, zoals u ziet op onderstaande afbeeldingen. Hierbij maakt u gebruik van een Single Address.

Objects Setting >> IP Object

Profile Index : 4

Name:	Hoofd Verkoop
Interface:	LAN/RT/VPN ▾
Address Type:	Single Address ▾
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.20 <input type="button" value="Select"/>
End IP Address:	0.0.0.0 <input type="button" value="Select"/>
Subnet Mask:	255.255.255.254 / 31 ▾
Invert Selection:	<input type="checkbox"/>

<< [Previous](#) [Next](#) >>

Objects Setting >> IP Object

Profile Index : 5

Name:	Hoofd Support
Interface:	LAN/RT/VPN ▾
Address Type:	Single Address ▾
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.40 <input type="button" value="Select"/>
End IP Address:	0.0.0.0 <input type="button" value="Select"/>
Subnet Mask:	255.255.255.254 / 31 ▾
Invert Selection:	<input type="checkbox"/>

<< [Previous](#) [Next](#) >>

Op de onderstaande afbeelding ziet u de zojuist aangemaakte IP-Objecten:

Objects Setting >> IP Object

[Create from ARP Table](#)
[Create from Routing Table](#)

IP Object Profiles: [Set to Factory Default](#) |

View:

Index	Name	Address	Index	Name	Address
1.	Directeur	192.168.1.2	17.		
2.	Afd. Verkoop	192.168.1.21 ~ 192.168.1.39	18.		
3.	Afd. Support	192.168.1.41 ~ 192.168.1.45	19.		
4.	Hoofd Verkoop	192.168.1.20	20.		
5.	Hoofd Support	192.168.1.40	21.		
6.			22.		
7.			23.		
8.			24.		
9.			25.		
10.			26.		
11.			27.		
12.			28.		
13.			29.		
14.			30.		
15.			31.		
16.			32.		

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) >> [Next](#) >>

<p>Export IP Object</p> <p><input checked="" type="radio"/> Backup the current IP Objects with a CSV file</p> <p><input type="radio"/> Download the default CSV template to edit</p> <p><input type="button" value="Download"/></p>	<p>Restore IP Object</p> <p><input type="button" value="Bestand kiezen"/> Geen bestand gekozen</p> <p><input type="button" value="Restore"/></p>
--	---

Nu we alle IP-Objecten hebben aangemaakt moeten we deze nog verdelen in een tweetal IP-Groups. De afdeling verkoop en support moeten in 1 IP-Group komen, en de directeur en de 2 afdelingshoofden ook. Navigeer naar 'Object Setting >> IP Group' en klik op een Index nummer.

Objects Setting >> IP Group

Profile Index : 1

Name: Directeur&Hoofd

Interface: LAN

Available IP Objects

- 2-Afd. Verkoop
- 3-Afd. Support

Selected IP Objects

- 1-Directeur
- 4-Hoofd Verkoop
- 5-Hoofd Support

OK Clear Cancel

Wanneer u de IP-Objecten correct hebt aangemaakt krijgt u bij 'Available IP Objects' een 5 tal IP-objecten te zien. Deze 5 IP-objecten gaat u verdelen in 2 groepen, een voor de directeur en de twee afdelingshoofden en een voor de twee afdelingen. U vult bij 'Name' de bijbehorende naam in en geeft bij 'Interface' de LAN interface op. Vervolgens selecteert u de juiste IP-Objecten en klikt op onderstaande afbeelding om ze in een groep te plaatsen.



Zoals u in onderstaande afbeelding ziet hebben we 2 IP-Groups aangemaakt. Natuurlijk heeft u de mogelijkheid om meerdere IP-Objecten en/of IP-Groupen aan te maken.

Objects Setting >> IP Group

IP Group Table: | [Set to Factory Default](#) |

Index	Name	Index	Name
<u>1.</u>	Directeur&Hoofd	<u>17.</u>	
<u>2.</u>	Verkoop&Support	<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Bij 'Objects Settings' heeft u ook de keuze om een 'Service Type Object' en 'Service Type Group' aan te maken. U kiest voor een Service Type Object. Hierin gaat u een object aanmaken voor poort 80.

Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	<input type="text" value="HTTP Poort"/>		
Protocol	TCP	<input type="text" value="6"/>	
Source Port	=	<input type="text" value="1"/>	~ <input type="text" value="65535"/>
Destination Port	=	<input type="text" value="80"/>	~ <input type="text" value="80"/>

Next >>

Belangrijk: De Source port is een Pseudo poort, deze wordt door de DrayTek gebruikt voor inkomende en uitgaande sessie's. Advies is deze altijd op 1 t/m 65535 te laten staan.

We maken hierna nog een Service Type object aan voor DNS verkeer.

Objects Setting >> Service Type Object Setup

Profile Index : 2

Name	DNS		
Protocol	UDP	17	
Source Port	=	1	~ 65535
Destination Port	=	53	~ 53

<< Previous Next >>

Navigeer vervolgens naar 'Firewall >> Filter Setup' en klik op Filter Set 2 (Default Data Filter).

Firewall >> Filter Setup ?

Filter Setup | Set to Factory Default |

Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Vervolgens zet u rechts onderin de Next Filter Set op Set#3 en klikt u links onderin op Filter Set 3 om een hier een nieuwe firewall regel aan te maken.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2
 Comments : Default Data Filter

Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53	Block Immediately			Down
2	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

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

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

OK Clear Cancel

Geef de firewall regel een naam en zet een vinkje bij Enable. Klik vervolgens op Rule 1.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 3
 Comments : Verkoop&Support

Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately			Down
2	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12 Next Filter Set None ▼

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

OK Clear Cancel

We creëren een Block if No Further Match regel, hierin blokkeren we al het verkeer van binnen (LAN) naar buiten (WAN). Wanneer u dan op OK klikt zult u merken dat u geen toegang meer hebt tot het internet (WAN).

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 3 Rule 1

Enable

Comments: Block OUT

Schedule Profile: None, None, None, None
 Clear sessions when schedule is ON

Direction: LAN/RT/VPN -> WAN Advanced

Source IP: Any Edit

Destination IP: Any Edit

Service Type: Any Edit

Fragments: Don't Care

Application	Action/Profile	Syslog
Filter	Block If No Further Match	<input type="checkbox"/>
Branch to Other Filter Set	None	
Sessions Control	0 / 30000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	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

U maakt voor de directeur en zijn afdelingshoofden een nieuwe regel aan, waarin wordt vermeld dat ze een Pass Immediately krijgen op al het LAN => WAN verkeer.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 3 Rule 2

Enable

Comments

Schedule Profile , , ,

Clear sessions when schedule is ON

Direction

Source IP

Destination IP

Service Type

Fragments

Application	Action/Profile	Syslog
Filter	<input type="text" value="Pass Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set	<input type="text" value="None"/>	
Sessions Control	<input type="text" value="0 / 30000"/>	<input type="checkbox"/>
MAC Bind IP	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="None"/>	<input type="checkbox"/>
APP Enforcement	<input type="text" value="None"/>	<input type="checkbox"/>
URL Content Filter	<input type="text" value="None"/>	<input type="checkbox"/>
Web Content Filter	<input type="text" value="None"/>	<input type="checkbox"/>
DNS Filter	<input type="text" value="None"/>	<input type="checkbox"/>

Advance Setting

U maakt een nieuwe regel aan die u eerst activeert, vervolgens geeft u de juiste beschrijving op en verandert u de Direction in LAN/RT/VPN => WAN. Deze regel heeft betrekking op de directeur en zijn afdelingshoofden, zij hebben geen restricties op het LAN => WAN verkeer, dus wordt er hier gewerkt met een 'Pass Immediately'. Vervolgens klikt u bij Source IP op 'Edit', hier heeft u de mogelijkheid om bij Address Type voor 'Group and Objects' te kiezen.

IP Address Edit

Address Type	Group and Objects ▾
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	255.255.255.254 / 31 ▾
Invert Selection	<input type="checkbox"/>
IP Group	1-Directeur&Hoofd ▾, None ▾
IP Object	None ▾, None ▾
IPv6 Group	None ▾
IPv6 Object	None ▾, None ▾, None ▾

Nu hoeft u alleen nog maar een regel aan te maken voor de Verkoop & Support afdeling. Deze 2 afdelingen hebben alleen toegang tot poort 80. U geeft bij Source IP de IP Group op waarin u deze 2 afdelingen heeft geplaatst.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 3 Rule 3

<input checked="" type="checkbox"/> Enable	Comments: Pass Verk&Supp		
Schedule Profile	None ▾, None ▾, None ▾, None ▾	<input type="checkbox"/> Clear sessions when schedule is ON	
Direction	LAN/RT/VPN -> WAN ▾	<input type="button" value="Advanced"/>	
Source IP	Verkoop&..	<input type="button" value="Edit"/>	
Destination IP	Any	<input type="button" value="Edit"/>	
Service Type	HTTP Poort, DNS	<input type="button" value="Edit"/>	
Fragments	Don't Care ▾		
Application Filter	Action/Profile : Pass Immediately ▾	Syslog : <input type="checkbox"/>	
Branch to Other Filter Set	None ▾		
Sessions Control	0 / 30000	<input type="checkbox"/>	
MAC Bind IP	Non-Strict ▾	<input type="checkbox"/>	
Quality of Service	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	<input type="button" value="Edit"/>		

Bij Source IP geeft u de IP Group Verkoop & Support op.

IP Address Edit

Address Type	Group and Objects ▼		
Start IP Address	0.0.0.0		
End IP Address	0.0.0.0		
Subnet Mask	255.255.255.254 / 31 ▼		
Invert Selection	<input type="checkbox"/>		
IP Group	2-Verkoop&Support ▼	None ▼	
IP Object	None ▼	None ▼	
IPv6 Group	None ▼		
IPv6 Object	None ▼	None ▼	None ▼

OK Close

Vervolgens selecteert u bij Service Object de aangemaakte Service Type Objects. Aangezien de twee afdelingen alleen toegang tot HTTP en DNS mogen hebben.

Service Type Edit

Service Type	Group and Objects ▼		
Protocol	Any ▼		
Source Port	= ▼	1	~ 65535
Destination Port	= ▼	1	~ 65535
Service Group	None ▼		
Service Object	1-HTTP Poort ▼	2-DNS ▼	None ▼

OK Close

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.