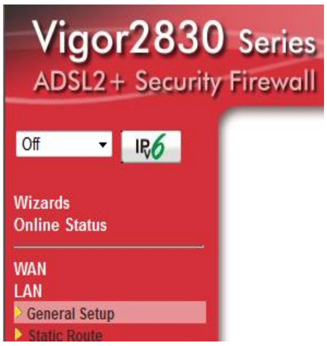
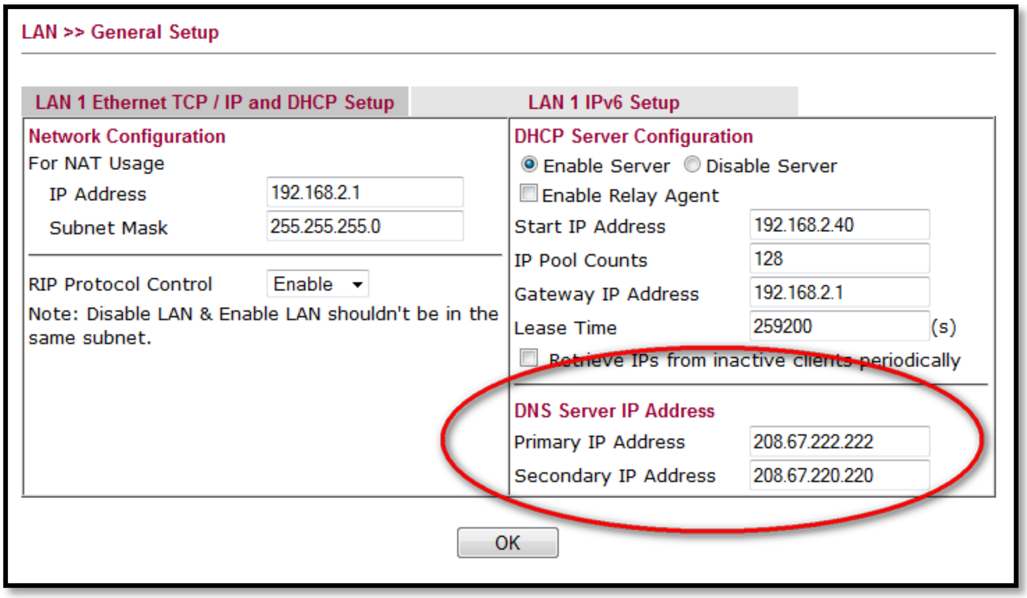
Configuring OpenDNS on a Draytek 2830

In The LAN, General Setup, click on the [Details Page] for your LAN and set the Primary and Secondary DNS server addresses to the OpenDNS servers as shown below.

- Primary IP address = 208.67.222.222
- Secondary IP address = 208.67.220.220





LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup | LAN 1 IPv6 Setup

Network Configuration

For NAT Usage

IP Address	192.168.2.1
Subnet Mask	255.255.255.0
RIP Protocol Control	Enable

Note: Disable LAN & Enable LAN shouldn't be in the same subnet.

DHCP Server Configuration

● Enable Server ○ Disable Server

□ Enable Relay Agent

Start IP Address	192.168.2.40
IP Pool Counts	128
Gateway IP Address	192.168.2.1
Lease Time	259200 (s)

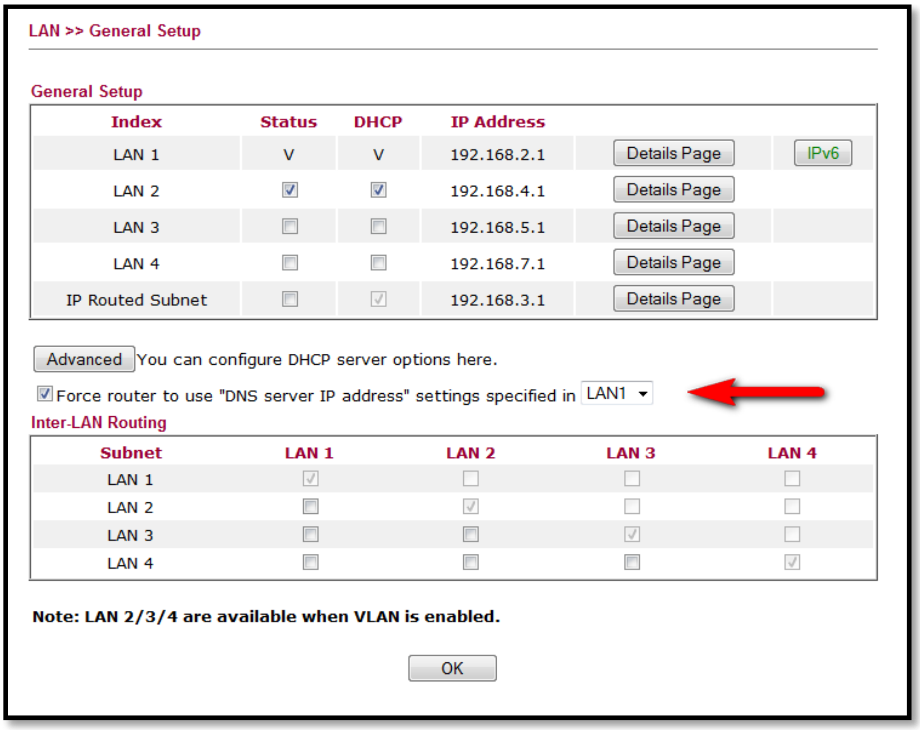
□ Retrieve IPs from inactive clients periodically

DNS Server IP Address

Primary IP Address	208.67.222.222
Secondary IP Address	208.67.220.220

OK

If you have more than one internal LAN then check the box marked “Force router to use "DNS server IP address" settings specified in” and select the LAN you configured for OpenDNS (usually LAN1).



LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.2.1	Details Page	IPv6
LAN 2	☑	☑	192.168.4.1	Details Page	
LAN 3	□	□	192.168.5.1	Details Page	
LAN 4	□	□	192.168.7.1	Details Page	
IP Routed Subnet	□	☑	192.168.3.1	Details Page	

Advanced You can configure DHCP server options here.

☑ Force router to use "DNS server IP address" settings specified in LAN1

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	☑	□	□	□
LAN 2	□	☑	□	□
LAN 3	□	□	☑	□
LAN 4	□	□	□	☑

Note: LAN 2/3/4 are available when VLAN is enabled.

OK

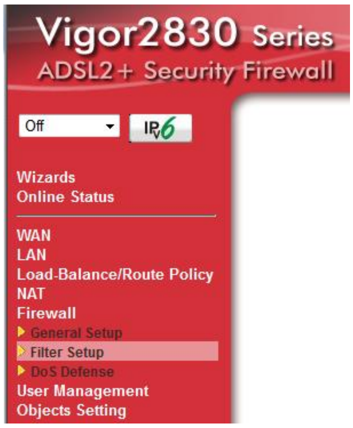
Setting up DNS to only go to OpenDNS (block all others)

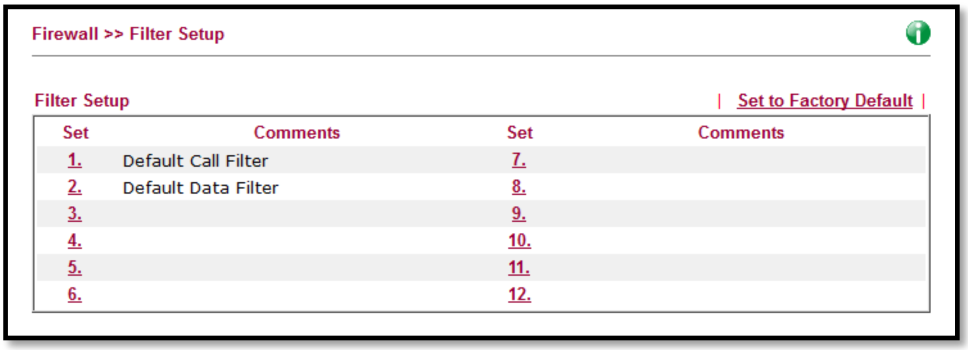
The problem is that if you manually type in DNS settings in your computer network settings it will bypass the Open DNS settings. So what we need to do now is to help your router not to allow any other DNS settings through. To do this go to the firewall settings on your router (not your computer) and block all outgoing TCP and UDP requests on port 53 that are not going to Open DNS.

Add three rules.

- allow DNS lookups that are going to open DNS 208.67.222.222
- allow DNS lookups that are going to open DNS 208.67.220.220
- block any other DNS lookups.

Here's where the rules are added:



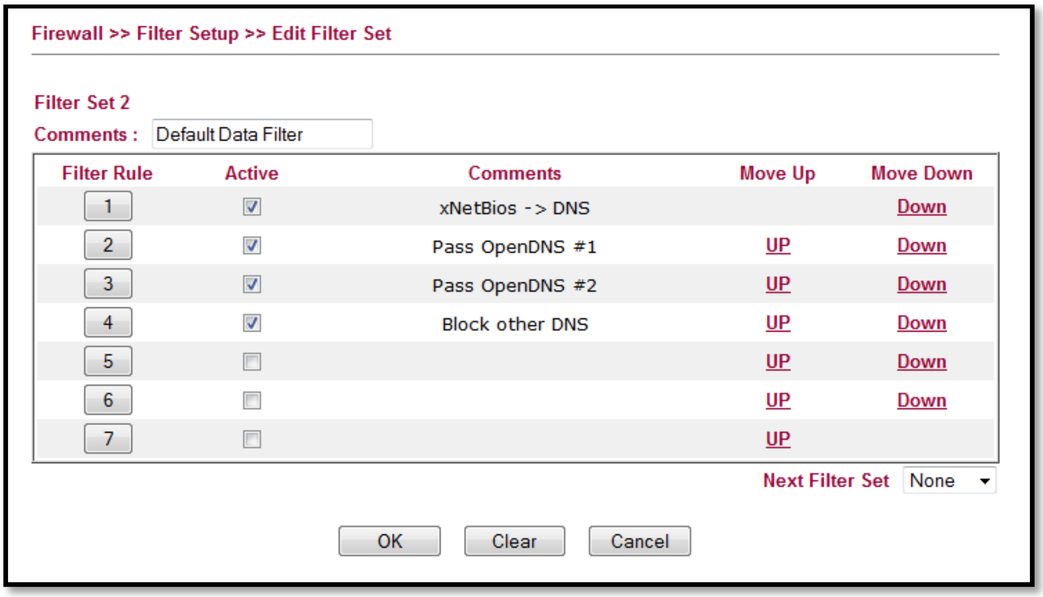

Firewall >> Filter Setup

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.	

On the Draytek modem the firewall settings are set up under **default data filter**

Here are the three rules to add:


Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

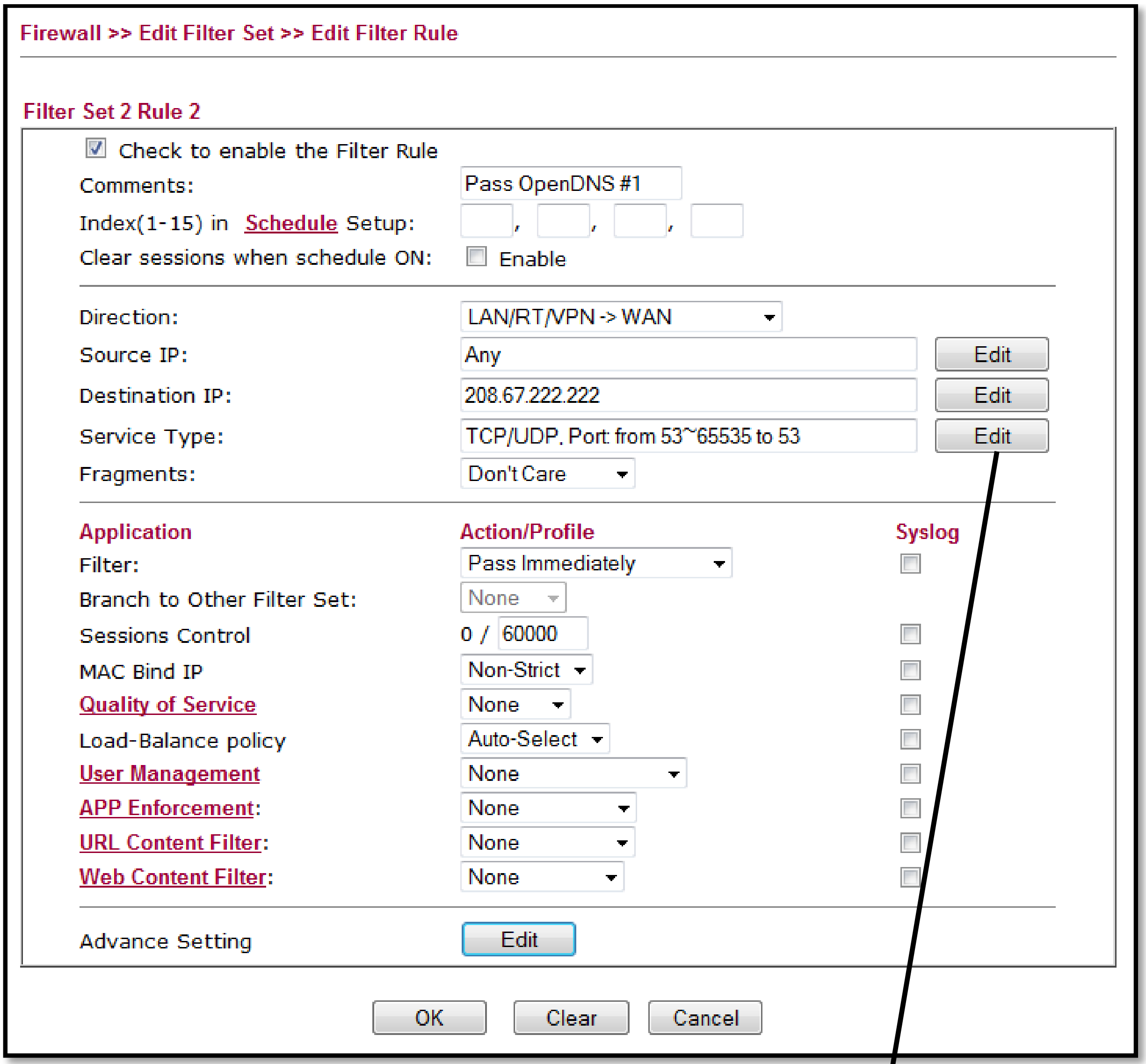
Comments : Default Data Filter

Filter Rule	Active	Comments	Move Up	Move Down
1	☑	xNetBios -> DNS		Down
2	☑	Pass OpenDNS #1	UP	Down
3	☑	Pass OpenDNS #2	UP	Down
4	☑	Block other DNS	UP	Down
5	□		UP	Down
6	□		UP	Down
7	□		UP	

Next Filter Set: None

In a default configuration; Rule 1 already exists, so we add rules 2, 3 & 4.

Adding Rule 2



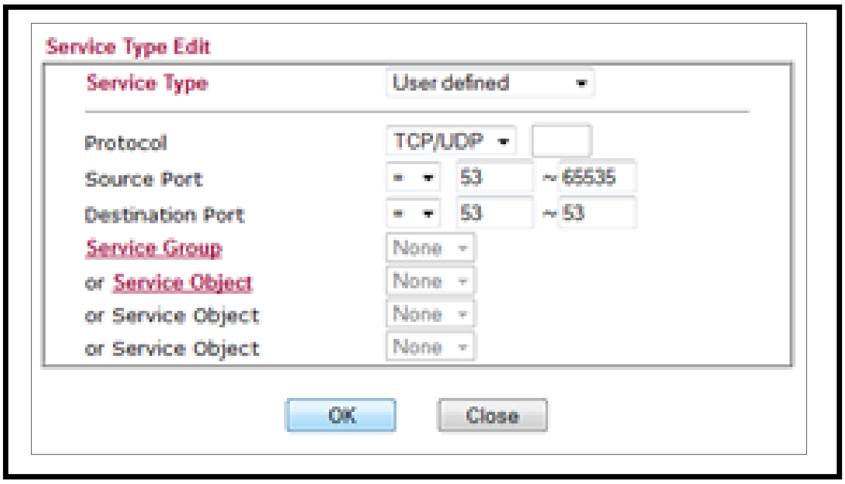
Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

☑ Check to enable the Filter Rule

Comments:	Pass OpenDNS #1
Index(1-15) in Schedule Setup:	, , ,
Clear sessions when schedule ON:	□ Enable
Direction:	LAN/RT/VPN -> WAN
Source IP:	Any
Destination IP:	208.67.222.222
Service Type:	TCP/UDP, Port from 53~65535 to 53
Fragments:	Don't Care

Application	Action/Profile	Syslog
Filter:	Pass Immediately	□
Branch to Other Filter Set:	None	
Sessions Control	0 / 60000	□
MAC Bind IP	Non-Strict	□
Quality of Service	None	□
Load-Balance policy	Auto-Select	□
User Management	None	□
APP Enforcement:	None	□
URL Content Filter:	None	□
Web Content Filter:	None	□



Service Type Edit

Service Type	User defined
Protocol	TCP/UDP
Source Port	= 53 ~ 65535
Destination Port	= 53 ~ 53
Service Group	None
or Service Object	None
or Service Object	None
or Service Object	None

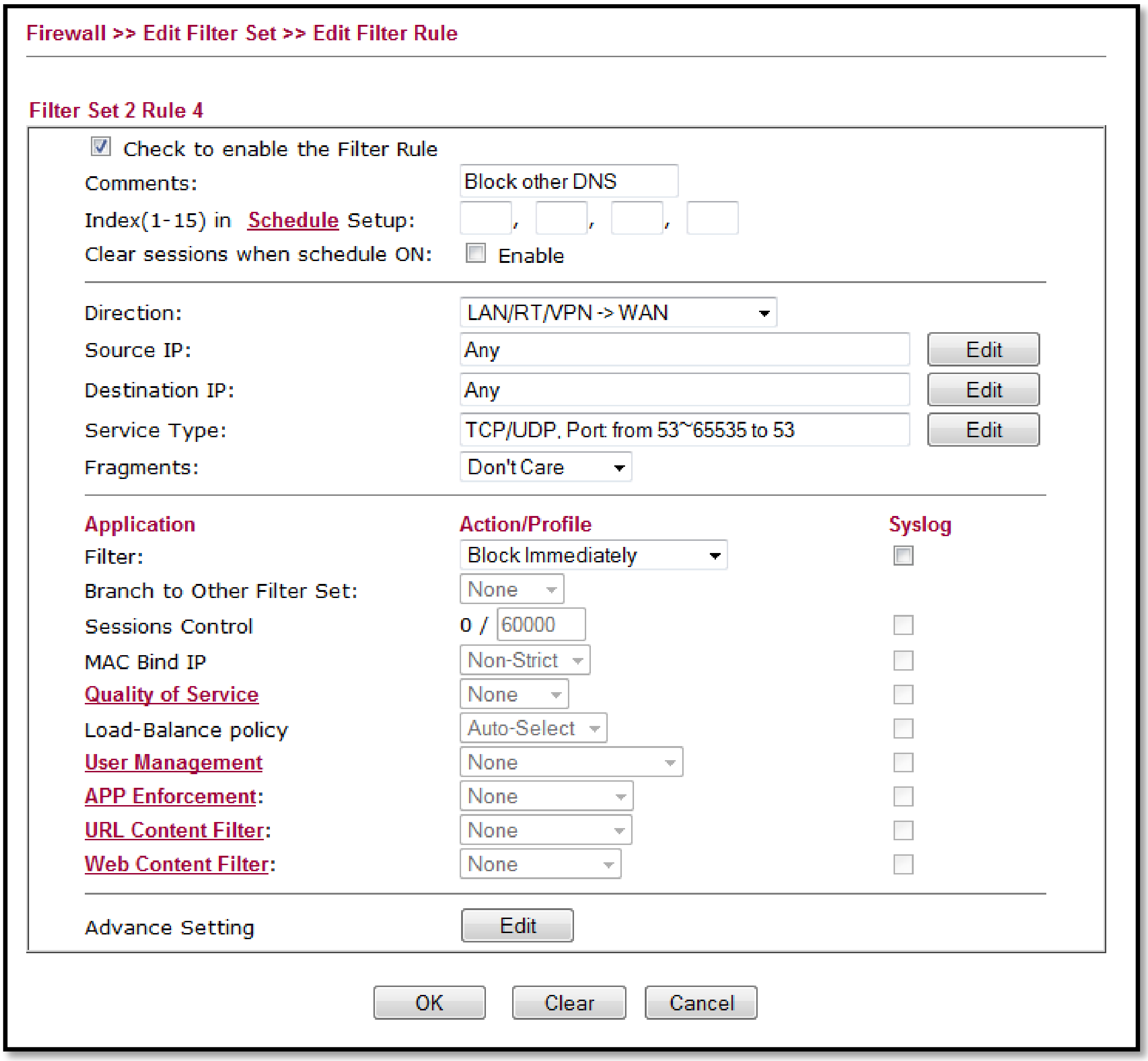
Rule 2 allows any traffic going to the first Open DNS server.

Adding Rule 3

Rule 3 was the same as rule except we use the second DNS number. 208.67.220.220 and we call it “Pass OpenDNS #2”

Adding Rule 4

Finally Rule 4 comes after Rule 2 & 3 and blocks all other DNS requests.



Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 4

☑ Check to enable the Filter Rule

Comments: Block other DNS

Index(1-15) in Schedule Setup: , , ,

Clear sessions when schedule ON: □ Enable

Direction: LAN/RT/VPN -> WAN

Source IP: Any [Edit]

Destination IP: Any [Edit]

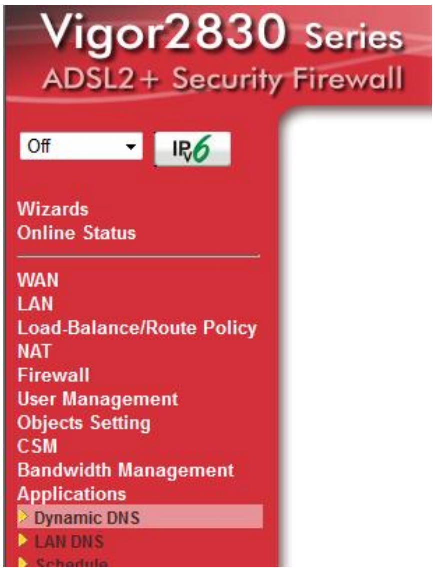
Service Type: TCP/UDP, Port from 53~65535 to 53 [Edit]

Fragments: Don't Care

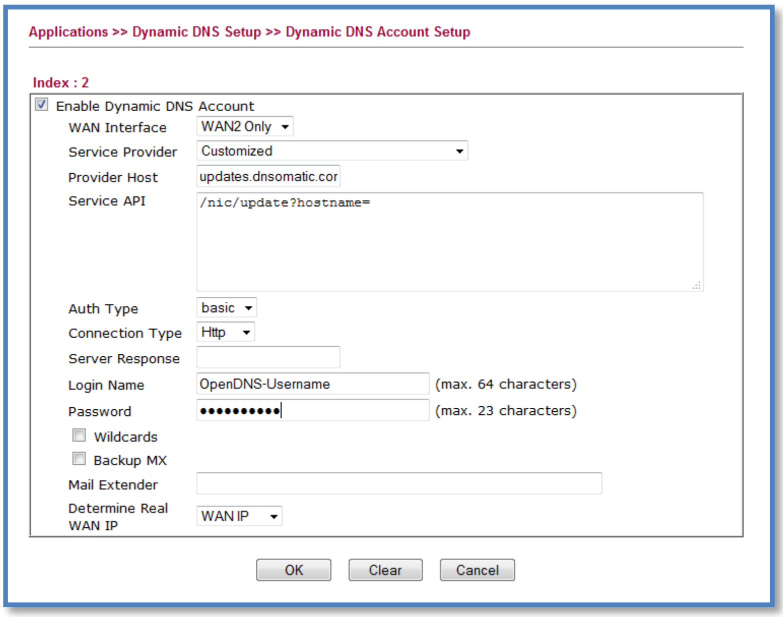
Application	Action/Profile	Syslog
Filter:	Block Immediately	□
Branch to Other Filter Set:	None	
Sessions Control	0 / 60000	□
MAC Bind IP	Non-Strict	□
Quality of Service	None	□
Load-Balance policy	Auto-Select	□
User Management	None	□
APP Enforcement:	None	□
URL Content Filter:	None	□
Web Content Filter:	None	□

Advance Setting [Edit]

Setting Dynamic DNS updates for OpenDNS



Set for the appropriate WAN interface (WAN2 = Fibre)



Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Index : 2

☑ Enable Dynamic DNS Account

WAN Interface	WAN2 Only
Service Provider	Customized
Provider Host	updates.dnsomatic.cor
Service API	/nic/update?hostname=
Auth Type	basic
Connection Type	Http
Server Response	
Login Name	OpenDNS-Username (max. 64 characters)
Password	•••••••••• (max. 23 characters)

□ Wildcards

□ Backup MX

Mail Extender	
Determine Real WAN IP	WAN IP

WAN interface = WAN2 only
Service Provider = Customised
Provider host = updates.dnsomatic.com
Service API = /nic/update?hostname=
Auth Type = basic
Connection type = http
Server response = <empty>
Login Name = OpenDNS Username
Password = OpenDNS Password
Wildcards = <unchecked>
Backup MX = <unchecked>
Mail Extender <empty>
Determine Real WAN IP = WAN IP