

How to configure DNS based FortiGuard web filtering with FortiOS v5.4

114 Les Carr Wed, Aug 2, 2017 [Fortigate UTM](#) 4592

Products

FortiGate v5.4

Description

This article provides a sample configuration for DNS based FortiGuard web filtering.

In FortiOS v5.2 the DNS web filtering is one option of 'Web Filter' profile. In FortiOS v5.4 this feature has moved to separate 'DNS Filter' security profile.

The use of this feature is straightforward:

- Create and configure 'DNS Filter' profile
- Create and configure firewall policy
- Assign the profile to the firewall policy

FortiOS intercepts DNS requests from clients to DNS servers and asks FortiGuard servers for rating.

It is recommended to filter client's DNS requests only and not the DNS requests from client internal DNS servers.

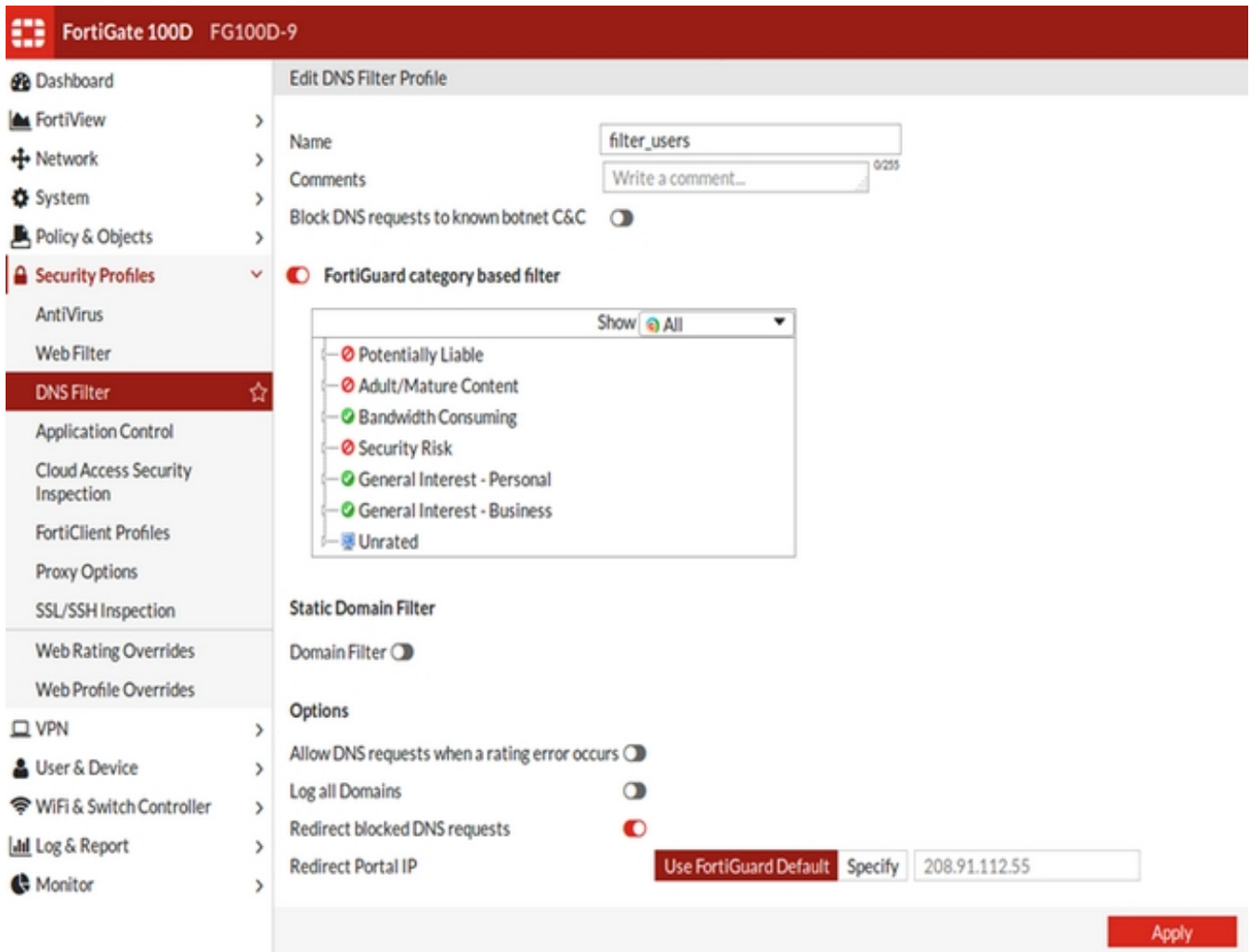
Technical Note: How to configure DNS based FortiGuard web filtering with FortiOS v5.4

//

[Network topology](#)

Internet w/ DNS servers === (wan1)[FG100D](lan) === PCs in LAN

[Configure DNS filter](#)



Technical Note: How to configure DNS based FortiGuard web filtering with FortiOS v5.4

//

CLI

```
config dnsfilter profile
edit "filter_users"
config ftgd-dns
```

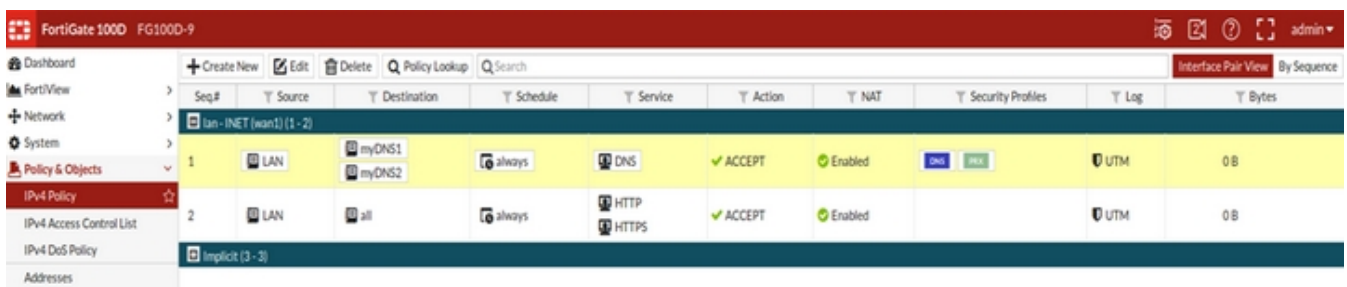
```
config filters
  edit 1
    set category 83
    set action block
  next
  edit 2
    set category 5
    set action block
  next
  edit 3
    set category 1
    set action block
  next
  edit 4
    set category 6
    set action block
  next

... truncated ...

  edit 29
  next
end
end
next
end
```

//

Configure firewall policies



Seq.#	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	LAN	myDNS1 myDNS2	always	DNS	ACCEPT	Enabled	DNS, UTM	UTM	0 B
2	LAN	all	always	HTTP HTTPS	ACCEPT	Enabled		UTM	0 B
Implicit (3 - 3)									

Technical Note: How to configure DNS based FortiGuard web filtering with FortiOS v5.4

//

```
config firewall policy
edit 1
set srcintf "lan"
set dstintf "wan1"
set srcaddr "LAN"
set dstaddr "myDNS1" "myDNS2"
set action accept
set schedule "always"
set service "DNS"
set utm-status enable
set dnsfilter-profile "filter_users"
set profile-protocol-options "default"
set nat enable
next
edit 2
set srcintf "lan"
set dstintf "wan1"
```

```
set srcaddr "LAN"  
set dstaddr "all"  
set action accept  
set schedule "always"  
set service "HTTP" "HTTPS"  
set nat enable  
  
next  
end
```

To troubleshoot use the following command:

```
diag debug enable  
diag debug application dnsproxy -1
```

When finished, disable debug with:

```
diag debug reset  
diag debug disable
```

Online URL: <https://kb2.ic.uk/article.php?id=114>