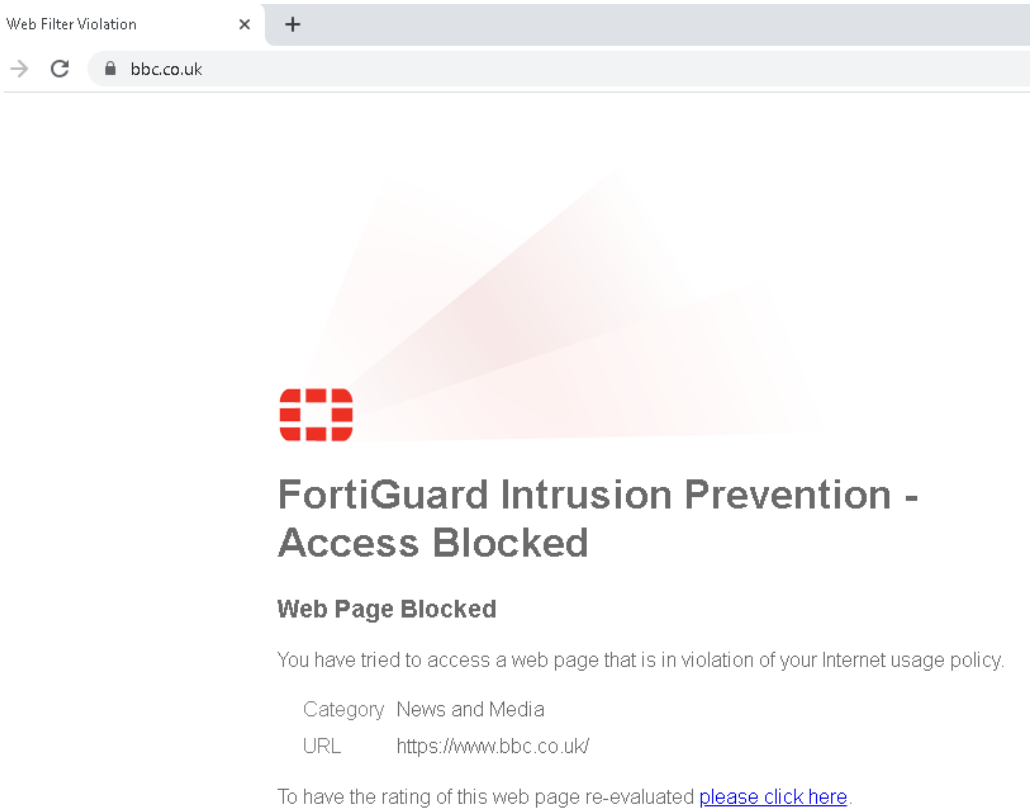
Webfilter (Flow mode) Tshoot

The below describes several use cases where the action of a Static URL is shown in the output for various debug commands:-

#diag ips debug enable urlfilter
#diag ips debug enable ssl
#diag debug enable

1. URL added to 'Static URL Filter' with action of 'Allow', and respective category of respective URL within 'FortiGuard Category Based Filter' action is 'Block'. End result URL blocked.

firewall # [13836@-1]eng_debug_log: Connecting to 212.58.236.129:443 (www.bbc.co.uk)
[13836@-1]eng_debug_log: Probe info:
[13836@-1]eng_debug_log: Server: 212.58.236.129:443
[13836@-1]eng_debug_log: Server name: www.bbc.co.uk
[13836@-1]eng_debug_log: STARTTLS: no
[13836@-1]eng_debug_log: Suport TLS 1.3: yes
[13836@-1]eng_debug_log: SNI verified: yes
[13836@-1]eng_debug_log: Certificate common name: www.bbc.co.uk
[13836@-1]eng_debug_log: Certificate SHA1 hash: 9AADDE656ACC23292E9000C76037AFF7F446E07B
[13836@-1]eng_debug_log: Certificate is self-signed: no
[13836@-1]eng_debug_log: parallel probes: 2
[13836@-1]eng_debug_log: Memory usage: 312 KiB, errors: 0
[13836@-1]probe_finish: probe is finished. id: 191, sess: 14169
[13836@-1]ssl_resume_sess: sess 14169: ssl resume
[13836@-1]ips_ssl_run_urlfilter: urlfilter matched:action=0 entryid=1 <---------- 'Allow' Static URL entry 1
[13836@-1]urlf_query_fgd: id:21210 sess:14169 action:0 error:0 src:2 host:www.bbc.co.uk url:/ rate_ip:0 ssl_exemption_query:0
[13836@-1]handle_fgd_answer: sess:14169, id:0, action:1, resume:0, error:0, ftgd_category:36, url_category:36, local_category:0, byip:0, log:1, time:0s <---------- Deny URL due to Category 'Block'
[13836@-1]on_rating_done: sess 14169, rate 36, action 1
[13836@-1]ips_eng_log_webfilter: sess:717760 type:10 action:1 host:www.bbc.co.uk source:2 url:/
[13836@-1]probe_finish: probe is finished. id: 192, sess: 14168
[13836@-1]ssl_resume_sess: sess 14168: ssl resume
[13836@-1]ips_ssl_run_urlfilter: urlfilter matched:action=0 entryid=1
[13836@-1]urlf_query_fgd: id:21211 sess:14168 action:0 error:0 src:2 host:www.bbc.co.uk url:/ rate_ip:0 ssl_exemption_query:0
[13836@-1]handle_fgd_answer: sess:14168, id:0, action:1, resume:0, error:0, ftgd_category:36, url_category:36, local_category:0, byip:0, log:1, time:0s
[13836@-1]on_rating_done: sess 14168, rate 36, action 1
[13836@-1]ips_eng_log_webfilter: sess:717759 type:10 action:1 host:www.bbc.co.uk source:2 url:/

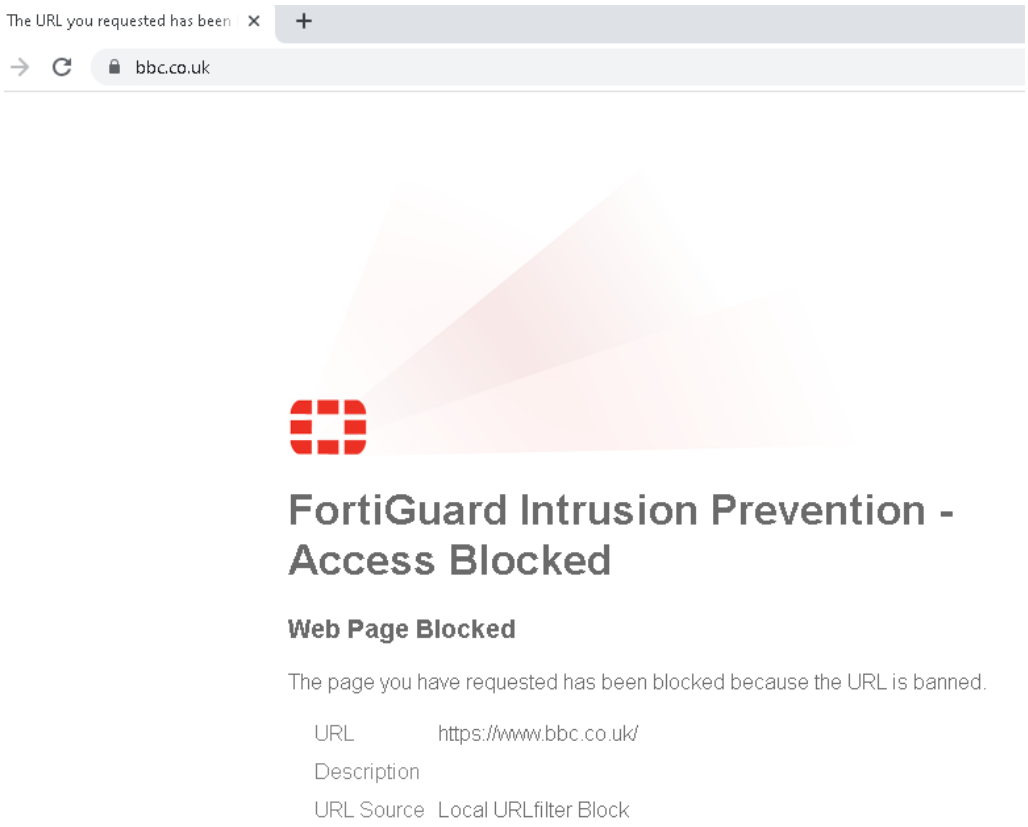


2. URL added to 'Static URL Filter' with action of 'Exempt', and respective category of respective URL within 'FortiGuard Category Based Filter' action is 'Block'. End result URL allowed.

```
firewall # [13836@-1]eng_debug_log: Connecting to 212.58.237.1:443 (www.bbc.co.uk)
[13836@-1]eng_debug_log: Probe info:
[13836@-1]eng_debug_log:   Server: 212.58.237.1:443
[13836@-1]eng_debug_log:   Server name: www.bbc.co.uk
[13836@-1]eng_debug_log:   STARTTLS: no
[13836@-1]eng_debug_log:   Suport TLS 1.3: yes
[13836@-1]eng_debug_log:   SNI verified: yes
[13836@-1]eng_debug_log:   Certificate common name: www.bbc.co.uk
[13836@-1]eng_debug_log:   Certificate SHA1 hash: 9AADDE656ACC23292E9000C76037AFF7F446E07B
[13836@-1]eng_debug_log:   Certificate is self-signed: no
[13836@-1]eng_debug_log: parallel probes: 2
[13836@-1]eng_debug_log: Memory usage: 315 KiB, errors: 0
[13836@-1]probe_finish: probe is finished. id: 194, sess: 14345
[13836@-1]ssl_resume_sess: sess 14345: ssl resume
[13836@-1]ips_ssl_run_urlfilter: urlfilter matched:action=8 entryid=1 <---------- 'Exempt' Static URL entry 1
[13836@-1]ips_exempt_features: [14345-0]:exempt activex_java_cookie
[13836@-1]ips_exempt_features: [14345-0]:exempt ftgd
[13836@-1]ips_exempt_features: [14345-0]:exempt local urlf
[13836@-1]ips_exempt_features: [14345-0]:exempt range
[13836@-1]ips_eng_log_webfilter: sess:718425 type:7 action:3 host:www.bbc.co.uk source:2 url:/
[13836@-1]probe_finish: probe is finished. id: 195, sess: 14344
[13836@-1]ssl_resume_sess: sess 14344: ssl resume
[13836@-1]ips_ssl_run_urlfilter: urlfilter matched:action=8 entryid=1
[13836@-1]ips_exempt_features: [14344-0]:exempt activex_java_cookie
[13836@-1]ips_exempt_features: [14344-0]:exempt ftgd
[13836@-1]ips_exempt_features: [14344-0]:exempt local urlf
[13836@-1]ips_exempt_features: [14344-0]:exempt range
[13836@-1]ips_eng_log_webfilter: sess:718424 type:7 action:3 host:www.bbc.co.uk source:2 url:/
```

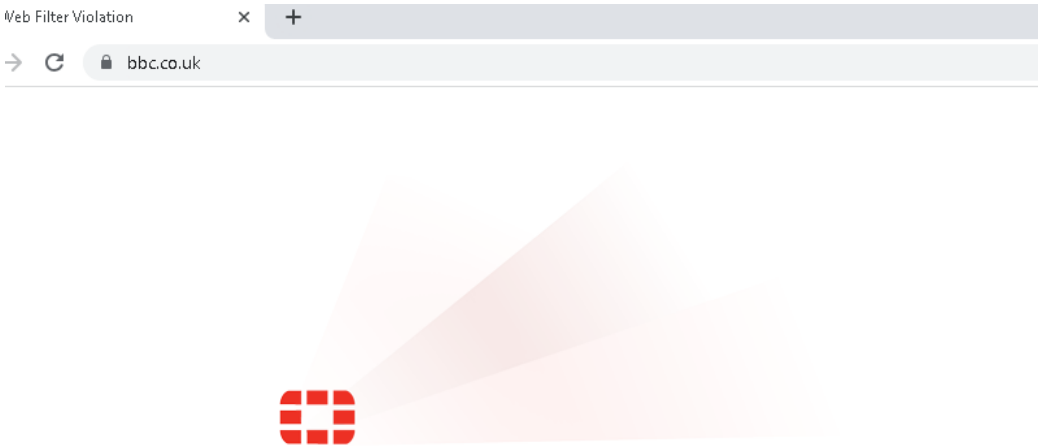
3. URL added to 'Static URL Filter' with action of 'Block', and respective category of respective URL within 'FortiGuard Category Based Filter' action is 'Block'. End result URL blocked.

firewall # [243@163]create_run_mode: SSL CA name: Fortinet_CA_SSL, untrust CA name: Fortinet_CA_Untrusted, VDOM: 0, enable: 0, mode: 0,
verifyca: 1, cert action: untrusted: 0, expired: 1, revoked: 1,
timeout: 0, failure: 1, whitelist: 0
[243@163]confirm_ssl: confirm SSL.
[243@163]on_cb: SSL client fingerprint: 0xD85F5EEBDFBBD7F4
[243@-1]eng_debug_log: Connecting to 212.58.235.129:443 (www.bbc.co.uk)
[243@-1]eng_debug_log: Probe info:
[243@-1]eng_debug_log: Server: 212.58.235.129:443
[243@-1]eng_debug_log: Server name: www.bbc.co.uk
[243@-1]eng_debug_log: STARTTLS: no
[243@-1]eng_debug_log: Suport TLS 1.3: yes
[243@-1]eng_debug_log: SNI verified: yes
[243@-1]eng_debug_log: Certificate common name: www.bbc.co.uk
[243@-1]eng_debug_log: Certificate SHA1 hash: 9AADDE656ACC23292E9000C76037AFF7F446E07B
[243@-1]eng_debug_log: Certificate is self-signed: no
[243@-1]eng_debug_log: parallel probes: 1
[243@-1]eng_debug_log: Memory usage: 231 KiB, errors: 0
[243@-1]probe_finish: probe is finished. id: 18, sess: 163
[243@-1]ssl_resume_sess: sess 163: ssl resume
[243@-1]ips_ssl_run_urlfilter: urlfilter matched:action=1 entryid=1 <---------- 'Block' Static URL entry 1
[243@-1]ips_eng_log_webfilter: sess:680 type:7 action:1 host:www.bbc.co.uk source:2 url:/
[243@165]create_run_mode: SSL CA name: Fortinet_CA_SSL, untrust CA name: Fortinet_CA_Untrusted, VDOM: 0, enable: 0, mode: 0,
verifyca: 1, cert action: untrusted: 0, expired: 1, revoked: 1,
timeout: 0, failure: 1, whitelist: 0
[243@165]confirm_ssl: confirm SSL.
[243@165]on_cb: SSL client fingerprint: 0x35E9B88331486F16
[243@165]ips_ssl_run_urlfilter: urlfilter matched:action=1 entryid=1
[243@165]ips_eng_log_webfilter: sess:683 type:7 action:1 host:www.bbc.co.uk source:2 url:/
[243@165]ssl_resume_sess: sess 165: ssl resume



4. URL added to ‘Static URL Filter’ with action of ‘Monitor’, and respective category of respective URL within ‘FortiGuard Category Based Filter’ action is ‘Block’. End result URL blocked, but entry logged.

```
firewall # [243@30]create_run_mode: SSL CA name: Fortinet_CA_SSL, untrust CA name: Fortinet_CA_Untrusted, VDOM: 0,
enable: 0, mode: 0,
verifyca: 1, cert action: untrusted: 0, expired: 1, revoked: 1,
timeout: 0, failure: 1, whitelist: 0
[243@30]confirm_ssl: confirm SSL.
[243@30]on_cb: SSL client fingerprint: 0x81B2C3A60CA3C6E3
[243@-1]eng_debug_log: Connecting to 212.58.237.129:443 (www.bbc.co.uk)
[243@-1]eng_debug_log: Probe info:
[243@-1]eng_debug_log:   Server: 212.58.237.129:443
[243@-1]eng_debug_log:   Server name: www.bbc.co.uk
[243@-1]eng_debug_log:   STARTTLS: no
[243@-1]eng_debug_log:   Suport TLS 1.3: yes
[243@-1]eng_debug_log:   SNI verified: yes
[243@-1]eng_debug_log:   Certificate common name: www.bbc.co.uk
[243@-1]eng_debug_log:   Certificate SHA1 hash: 9AADDE656ACC23292E9000C76037AFF7F446E07B
[243@-1]eng_debug_log:   Certificate is self-signed: no
[243@-1]eng_debug_log: parallel probes: 1
[243@-1]eng_debug_log: Memory usage: 264 KiB, errors: 0
[243@-1]probe_finish: probe is finished. id: 12, sess: 30
[243@-1]ssl_resume_sess: sess 30: ssl resume
[243@-1]ips_ssl_run_urlfilter: urlfilter matched:action=0 entryid=1 <---------- 'Allow' Static URL entry 1
[243@-1]ips_eng_log_webfilter: sess:207 type:7 action:0 host:www.bbc.co.uk source:2 url:/
[243@-1]urlf_query_fgd: id:12 sess:30 action:2 error:0 src:2 host:www.bbc.co.uk url:/ rate_ip:0 ssl_exemption_query:0
[243@-1]ips_urlf_add_query: id:12, queue:1, ssl_exemption: 0
[243@-1]urlf_query_fgd: session:30 suspended, query id:12
[243@-1]handle_fgd_answer: sess:30, id:12, action:1, resume:1, error:0, ftgd_category:36, url_category:36,
local_category:0, byip:0, log:1, time:0s <---------- Deny URL due to Category 'Block'
[243@-1]on_rating_done: sess 30, rate 36, action 1
[243@-1]ssl_resume_sess: sess 30: ssl resume
[243@-1]ips_eng_log_webfilter: sess:207 type:10 action:1 host:www.bbc.co.uk source:2 url:/
[243@-1]ips_urlf_del_query: id:12, queue:0
```



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category	News and Media
URL	https://www.bbc.co.uk/

To have the rating of this web page re-evaluated please click here.