

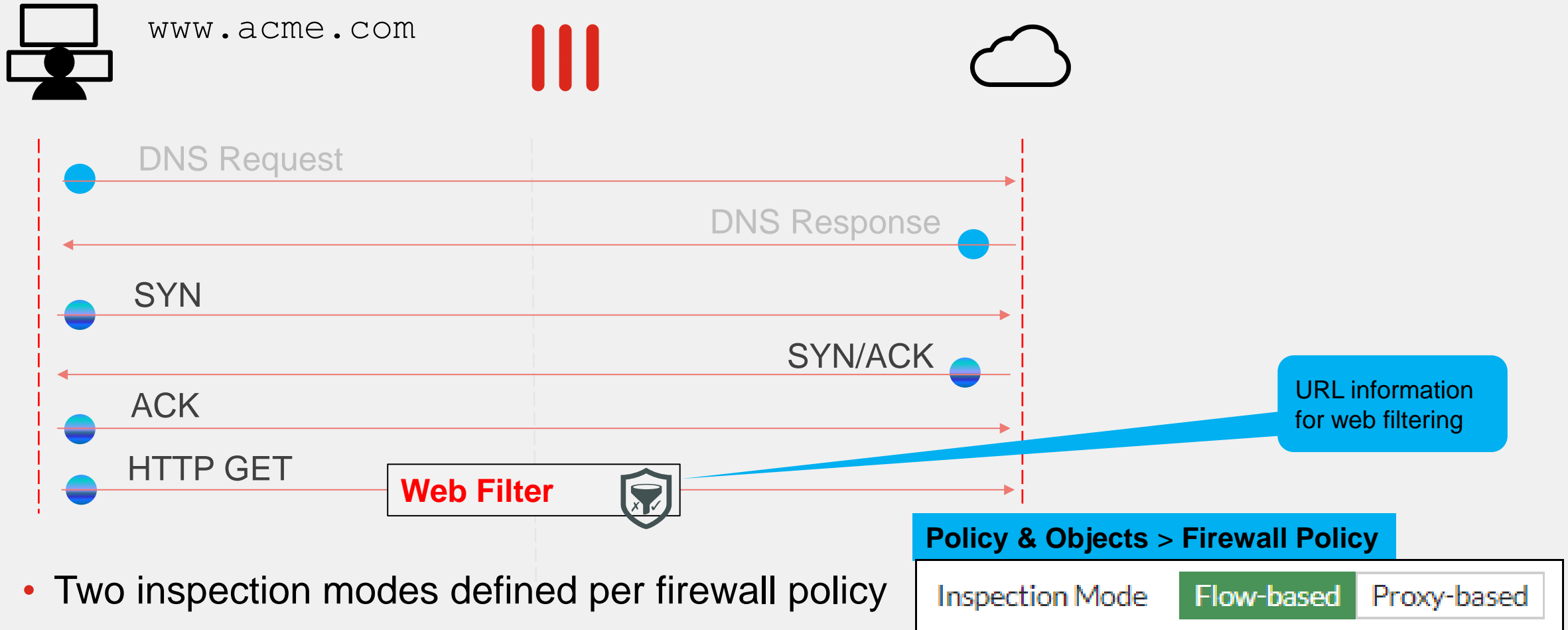
FortiGate Administrator

Web Filtering

Objectives

- Select the correct inspection mode (flow or proxy) based on security needs
- Configure certificate inspection for web filtering
- Configure a web filter profile in flow-based inspection mode
- Configure a web filter profile in proxy-based inspection mode
- Configure FortiGuard categories
- Configure a URL filter
- Troubleshoot web filtering issues

When Does Web Filtering Activate?

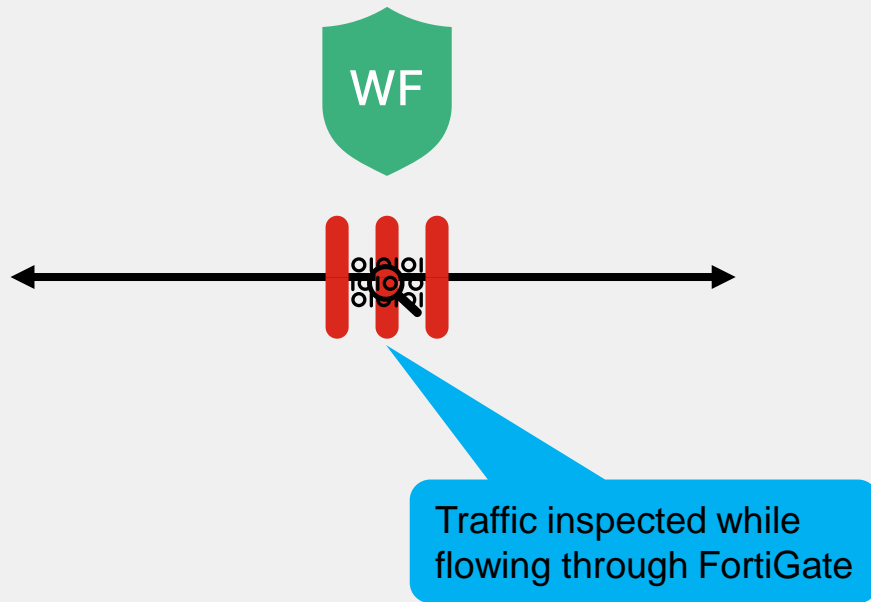


- Two inspection modes defined per firewall policy

Web Filtering Inspection Modes

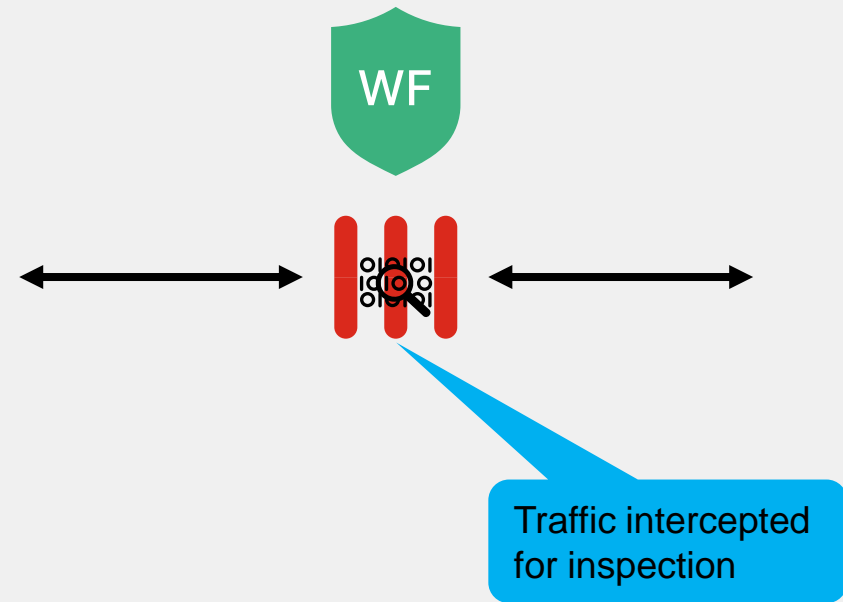
- Flow-based inspection

- Default inspection mode
- Requires fewer processing resources
- Faster scanning



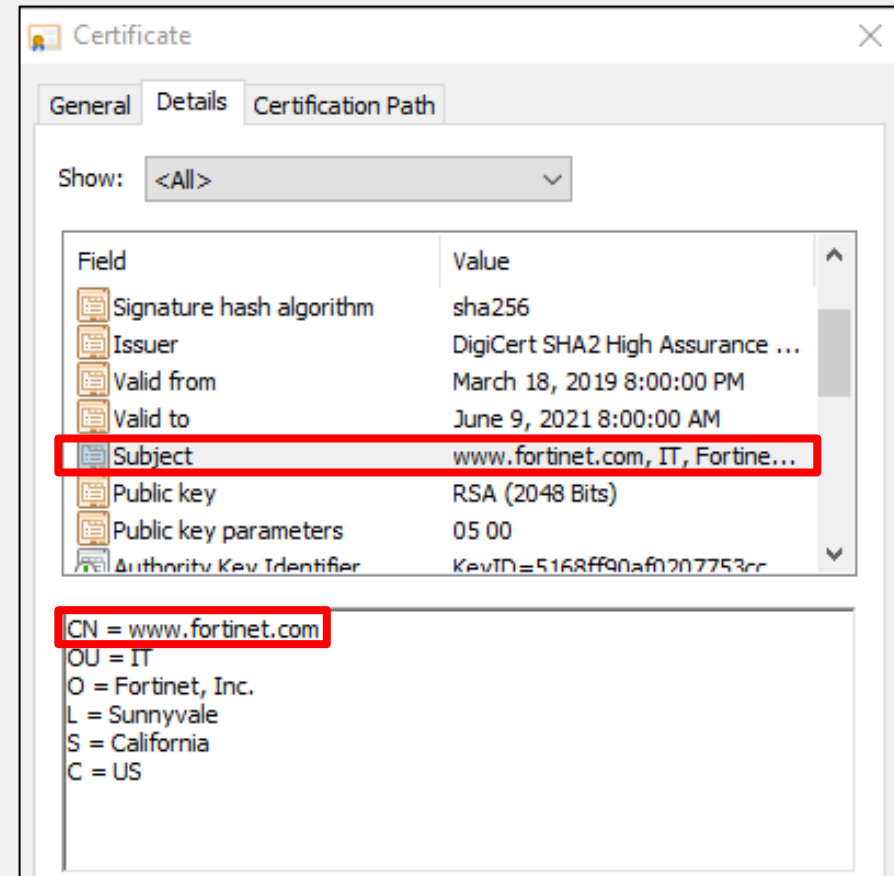
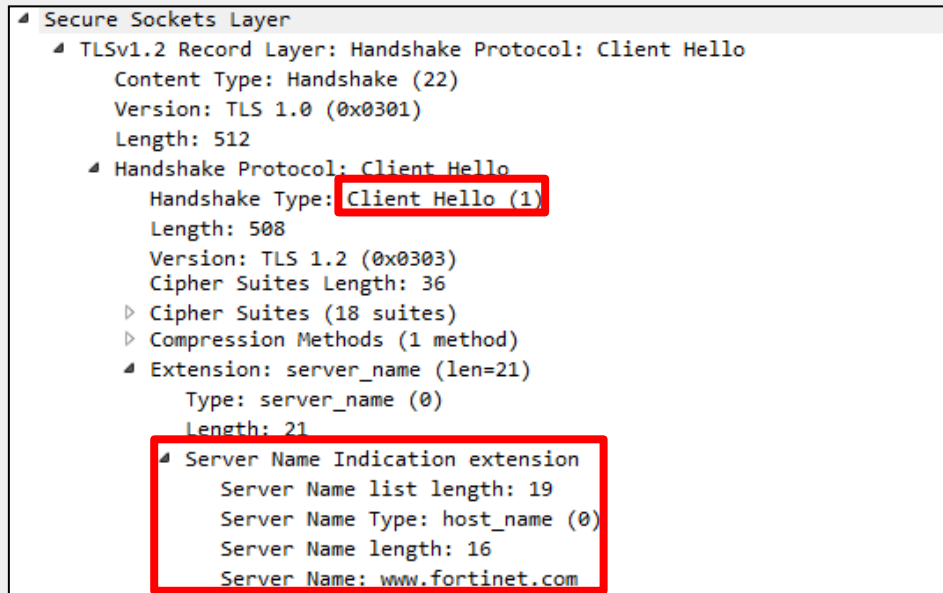
- Proxy-based inspection

- More thorough inspection
- Provides additional options
- More resource intensive



SSL Certificate Inspection

- Uses the SNI extension from the Client Hello of the SSL handshake to obtain the FQDN
- If server name identification (SNI) is not present, FortiGate uses the CN field in the server certificate to obtain the FQDN



Configure SSL Certificate Inspection

Security Profiles > SSL/SSH Inspection

Edit SSL/SSH Inspection Profile

Name

Comments 0/255

SSL Inspection Options

Enable SSL inspection of **Multiple Clients Connecting to Multiple Servers**
Protecting SSL Server

Inspection method **SSL Certificate Inspection** Full SSL Inspection

CA certificate Download

Blocked certificates **Allow** **Block** View Blocked Certificates

Untrusted SSL certificates **Allow** **Block** View Trusted CAs List

Server certificate SNI check **Enable** **Strict** **Disable**

Protocol Port Mapping

Inspect all ports ☐

HTTPS ☒

Select **Multiple Clients**
Connecting to Multiple Servers

Select **SSL Certificate Inspection**

Action if the SNI does not match
the CN or SAN fields
(only in proxy-based inspection)

You can specify more than one port
number (separated by comma)

Configure Web Filter Profiles—Flow Based

- Apply web filter profile to a flow-based firewall policy

Select **Flow-based**

Enable **FortiGuard Category Based Filter** and configure each category

Enable and configure **Static URL Filter** if needed

Enable and configure **Rating Options** if needed

Security Profiles > Web Filter

New Web Filter Profile

Name WebFilter

Comments Write a comment... 0/255

Feature set **Flow-based** Proxy-based

☐ FortiGuard Category Based Filter

☒ Static URL Filter

Block invalid URLs ☐

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☐

☒ Rating Options

Allow websites when a rating error occurs ☐

Rate URLs by domain and IP Address ☐

Configure Web Filter Profiles—Proxy Based

- Apply a web filter profile to a flow-based firewall policy

Select **Proxy-based**

Feature available only in proxy-based

Security Profiles > Web Filter

New Web Filter Profile

Name

Comments 0/255

Feature set ☐ Flow-based ☒ **Proxy-based**

☐ FortiGuard Category Based Filter

☐ Allow users to override blocked categories

☒ Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☒ **P**

Restrict YouTube Access ☒ **P**

Log all search keywords ☒ **P**

☒ Static URL Filter

☒ Rating Options

☒ Proxy Options

Restrict Google account usage to specific domains ☒ **P**

HTTP POST Action ☒ **Allow** ☐ **Block**

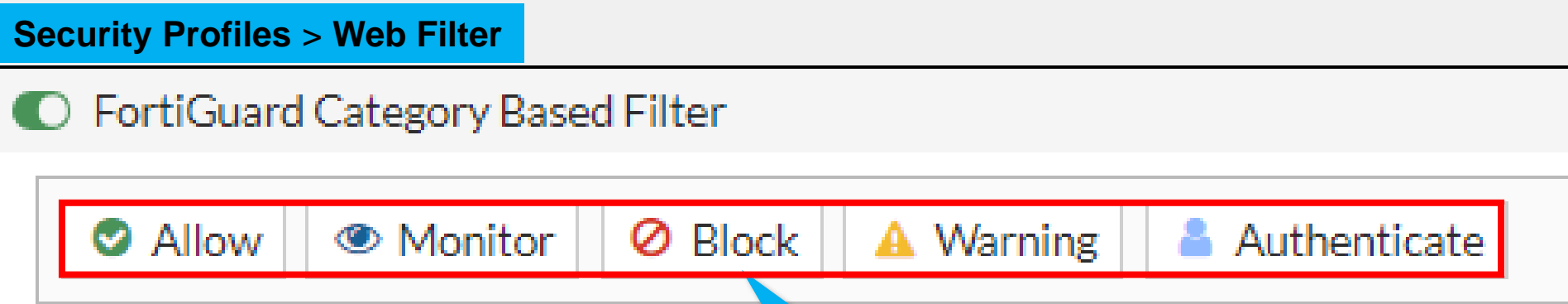
Remove Java Applets ☒ **P**

Remove ActiveX ☒ **P**

Remove Cookies ☐

FortiGuard Category Filter

- Websites split into multiple categories
- Live connection to FortiGuard with active contract required
- Can use FortiManager instead of FortiGuard



Available actions per category

Web Filter FortiGuard Category Action—Monitor

- Monitor action allows and logs web sites accesses

Security Profiles > Web Filter

Edit Web Filter Profile

Name: Monitor

Comments: Monitor and log all visited URLs. 33/255

Feature set: Flow-based Proxy-based

☒ FortiGuard Category Based Filter

☒ Allow ☒ Monitor ☐ Block ☐ Warning ☐ Authenticate

Name	Action
Education	Monitor

27% 95

Category Usage Quota

+ Create New Edit Delete

Category	Total quota
Education	1024 MB

1

Set action to monitor

Quota configuration available in proxy-based mode

Web Filter FortiGuard Category Action—Quotas

- Applies to **Monitor**, and also **Warning** and **Authenticate** actions
- Quotas available only in proxy-based mode

Security Profiles > Web Filter

Edit Web Filter Profile

Category Usage Quota P i

Category	Total quota
Education	1024 MB

+ Create New Edit Delete

1

New/Edit Quota

Category Education x

Quota Type Time Traffic

Total quota 0 hour(s) 5 minute(s) 0 second(s)

Daily quotas based on time or traffic amount

New/Edit Quota

Category Education x

Quota Type Time Traffic

Total quota 1024 MB

Web Filter FortiGuard Category Action—Warning

- Informs the user before proceeding

Security Profiles > Web Filter

New Web Filter Profile

Name: Warning

Comments: Write a comment... 0/255

Feature set: Flow-based Proxy-based

☒ FortiGuard Category Based Filter

☒ Allow ☐ Monitor ☐ Block ☒ Warning ☐ Authenticate

Name	Action
Internet Telephony	Warning

Set action to warning

Customizable warning interval

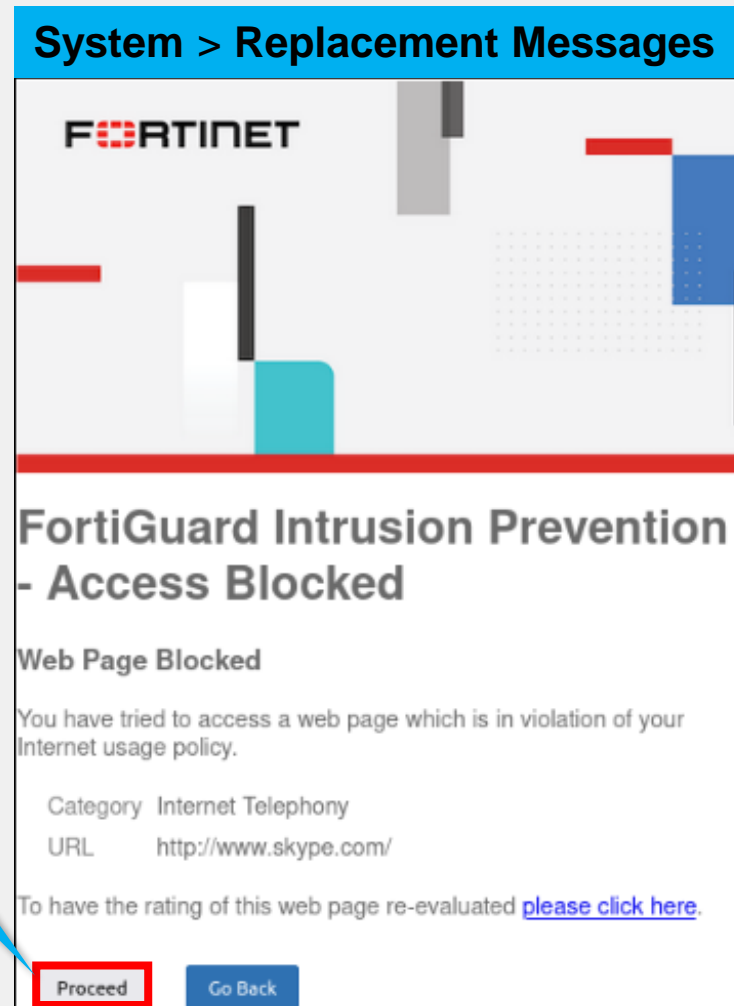
Edit Filter

Warning Interval: 0 hour(s) 5 minute(s) 0 second(s)

Web Filter FortiGuard Category Action—Warning (Contd)

- Displays a customizable warning message

Click to view
the website



Web Filter FortiGuard Category Action—Authenticate

- To configure the **Authenticate** action:
 - Define **Users** and **Group**
 - Set action to **Authenticate**
 - Select **User Group**

Security Profiles > Web Filter

☒ FortiGuard Category Based Filter

☒ Allow ☐ Monitor ☐ Block ☐ Warning ☒ Authenticate

Name	Action
Streaming Media and Download	<input checked="" type="checkbox"/> Authenticate

Edit Filter

Warning Interval hour(s) minute(s) second(s)

Selected User Groups

Set action to authenticate

Customizable authenticate interval

User groups allowed to authenticate

Web Filter FortiGuard Category Action—Authenticate (Contd)

- User credentials requested in message

System > Replacement Messages

FORTINET

**FortiGuard Intrusion Prevention
- Access Blocked**

Web Filter Block Override

Please contact your administrator to gain access to the web page.

Username:

Password:

Continue

User credentials to
access the website
category action set to
authenticate

Web Rating Override

- Changes a website category, not the category action

Security Profiles > Web Rating Overrides

Edit Web Rating Override

URL

www.bing.com

Lookup rating

Category

General Interest - Business

Sub-Category

Search Engines and Portals

Comments

Write a comment...

0/255

Override to

Category

Security Risk

Sub-Category

Malicious Websites

Information on the original category

Configuration of the override category

Adds information and the column **Original Category**

Configure a URL Filter

- Check against configured URLs in URL filter from top to bottom

Enable **URL Filter**

Three pattern types

Four available actions

Security Profiles > Web Filter

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

[+ Create New](#) [Edit](#) [Delete](#)

URL	Type	Action	Status
.*\something\{org biz}	Regular Express...	<input type="radio"/> Exempt	<input checked="" type="checkbox"/> Enable
somewhere.*	Wildcard	<input checked="" type="radio"/> Monitor	<input checked="" type="checkbox"/> Enable
www.somesite.com/s...	Simple	<input checked="" type="radio"/> Block	<input checked="" type="checkbox"/> Enable

New URL Filter

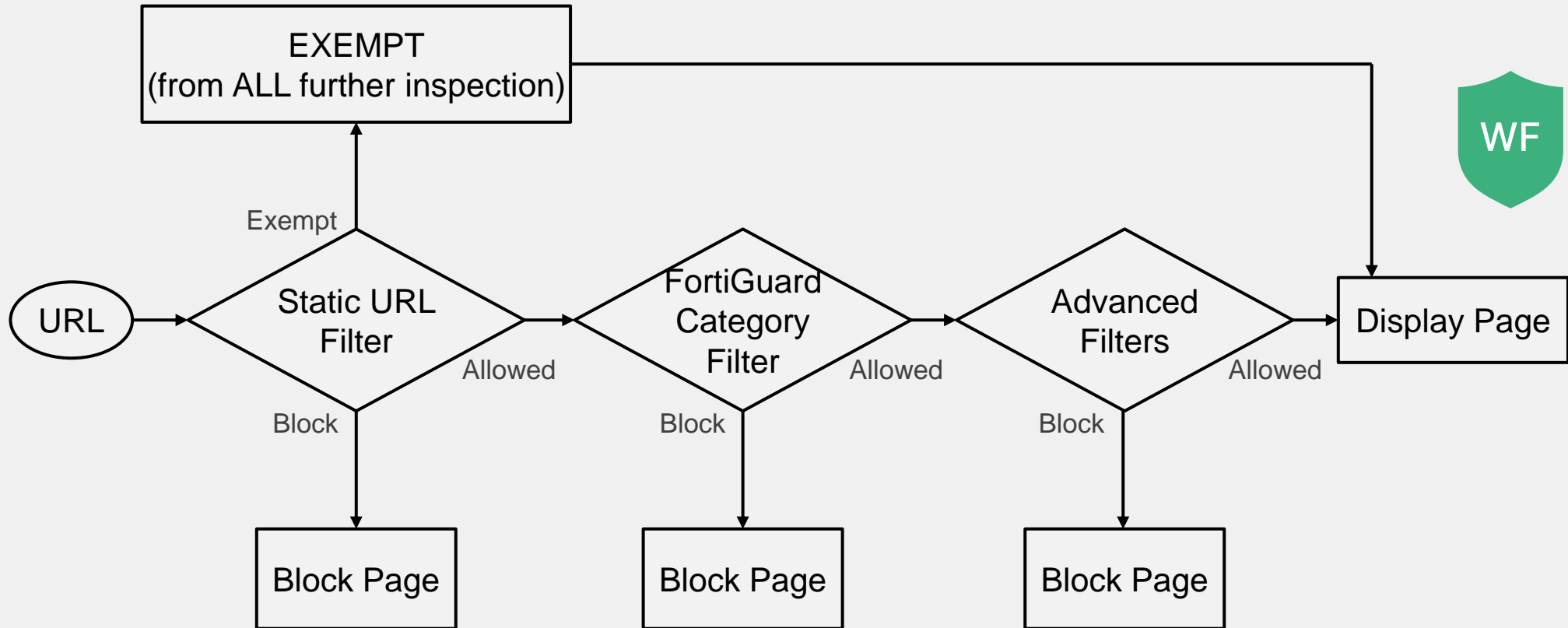
URL

Type ☒ Simple ☐ Regular Expression ☐ Wildcard

Action ☒ Exempt ☐ Block ☐ Allow ☐ Monitor

Status ☒ Enable ☐ Disable

HTTP Inspection Order



Troubleshooting the FortiGuard Connection

- FortiGuard category filtering requires a live connection

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract
\
Num. of servers : 1
Protocol     : https
Port        : 8888
Anycast     : Disable
Default servers : Not included

-- Server List (Wed Sep 20 09:22:42 2023) --
```

IP	Weight	RTT	Flags	TZ	FortiGuard-requests	Curr Lost	Total Lost	Updated Time
10.0.1.241	-244	2	I	0	122	0	0	Wed Sep 20 09:21:55 2023

Weight decreases with successful packets


Troubleshooting the FortiGuard Connection (Contd)

- Change default FortiGuard or FortiManager communications from HTTPS port 443:
 - Disable FortiGuard anycast setting on CLI to use UDP ports 443, 53, or 8888

```
config system fortiguard
    set fortiguard-anycast {enable|disable}
    set protocol {udp|https}
    set port {8888|53|443}
end
```


- Enable **Web Filter cache** to reduce requests to FortiGuard

System > FortiGuard



 Filtering

Web Filter cache	<input checked="" type="checkbox"/>	Clear cache after	60	Minutes
Email Filter cache	<input checked="" type="checkbox"/>	Clear cache after	30	Minutes

FortiGuard filtering services HTTPS 8888

 Test Connectivity

Filtering services availability

Web Filtering	
Anti-Spam	

[Request re-evaluation of a URL's category](#)

Default TTL is 60 minutes

Troubleshooting Web Filtering Issues

- Web filtering not working even with a valid FortiGuard live connection?

Compare **inspection mode** setting with **feature set** in web filter profile

Verify the web filter profile applied

For encrypted protocols, certificate-inspection must be at least selected

Policy & Objects > Firewall Policy

Inspection Mode | Flow-based | **Proxy-based**

Security Profiles


AntiVirus	<input type="checkbox"/>		
Web Filter	<input checked="" type="checkbox"/>	WEB	default
Video Filter	<input type="checkbox"/>		
DNS Filter	<input type="checkbox"/>		
Application Control	<input type="checkbox"/>		
IPS	<input type="checkbox"/>		
File Filter	<input type="checkbox"/>		
SSL Inspection	<input checked="" type="checkbox"/>	SSL	certificate-inspection


Web Filter Log


- Record HTTP traffic activity including action, profile used, category, URL, quota info


Log & Report > Security Events > Web Filter


Summary Logs








 Search




 Web Filter

 Disk

 24 hours

 Details


Date/Time	User	Source	Action	URL	Category	Initiator	Sent / Received
2023/09/20 07:43:02		10.0.1.10	 Blocked	https://www.google.com/	Search Engines and Portals		517 B / 0 B

Click to download the raw log data

Information on action and policy ID

Name of web filter profile

Name of web filter profile and replacement message used

Log Details		
Action		
Action		 Blocked
Policy ID		1 (Full_Access)
Web Filter		
Profile		default
Request Type		direct
Direction		outgoing
Category ID		41
Category		Search Engines and Portals
Message		URL belongs to a category with warnings enabled

Knowledge Check

1. Which action in URL filtering bypasses all security profiles?

- ✓ A. Exempt
- B. Allow

2. Which statement about proxy-based web filtering is true?

- A. It requires fewer resources than flow-based.
- ✓ B. It transparently analyzes the TCP flow of the traffic.

Review

- ✓ Describe FortiOS inspection modes
- ✓ Implement a web filter profile in flow-based and proxy-based inspection modes
- ✓ Work with web filter categories
- ✓ Configure a URL filter for further granularity
- ✓ Troubleshoot common web filtering issues
- ✓ Monitor logs for web filtering events