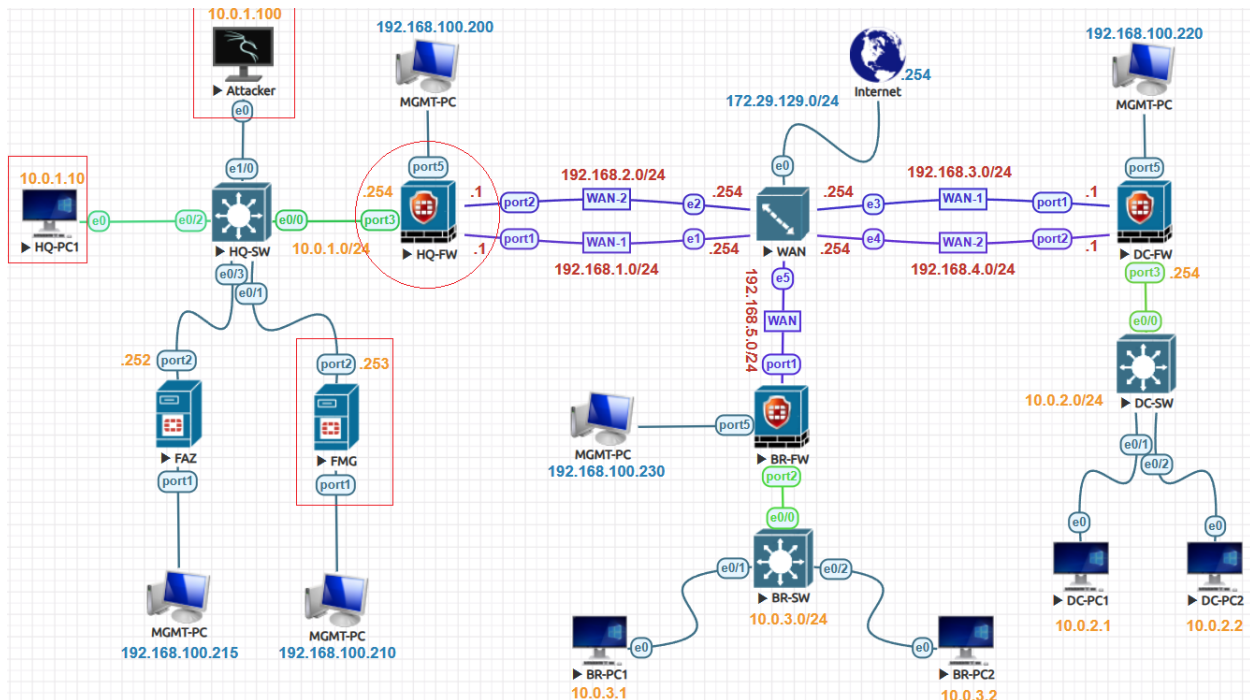


## Web Filter Profile FortiGuard Filter Lab:



Go to **Policy & Objects > Object Configurations > Security Profiles > Web Filter** there are preloaded four predefined web filters.

Policy & Objects			
Policy Package			
Install			
ADOM Revisions			
Tools			
Create New Edit Delete More Column Settings			
Name	Comments	Feature Set	
default	Default web filtering.	Flow-based	
sniffer-profile	Monitor web traffic.	Flow-based	
wifi-default	Default configuration for offloading WiFi	Flow-based	
monitor-all	Monitor and log all visited URLs, flow-ba	Flow-based	

## FortiGuard Filter:

To block category, go to **Policy & Objects > Object Configurations > Security Profiles > Web Filter** and go to the FortiGuard category based filter section.

### ☒ FortiGuard Category Based Filter

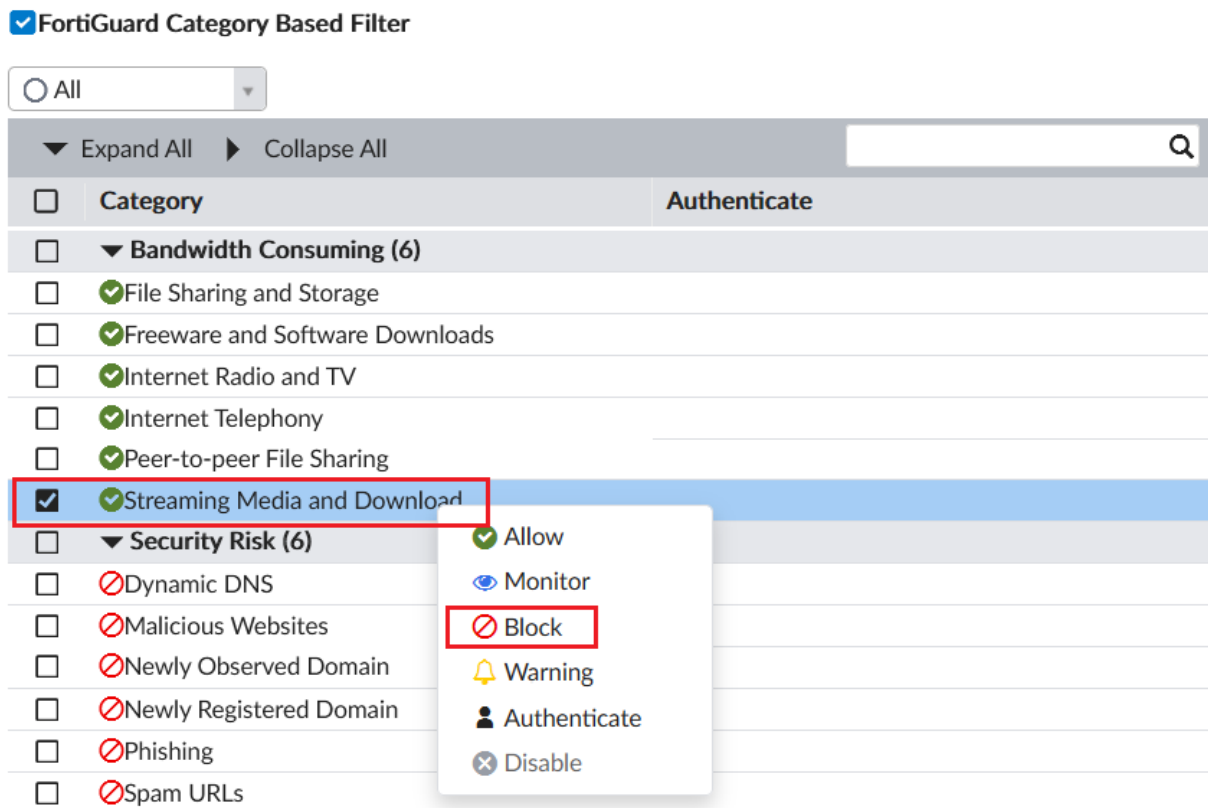
☐ All

▼ Expand All ▶ Collapse All

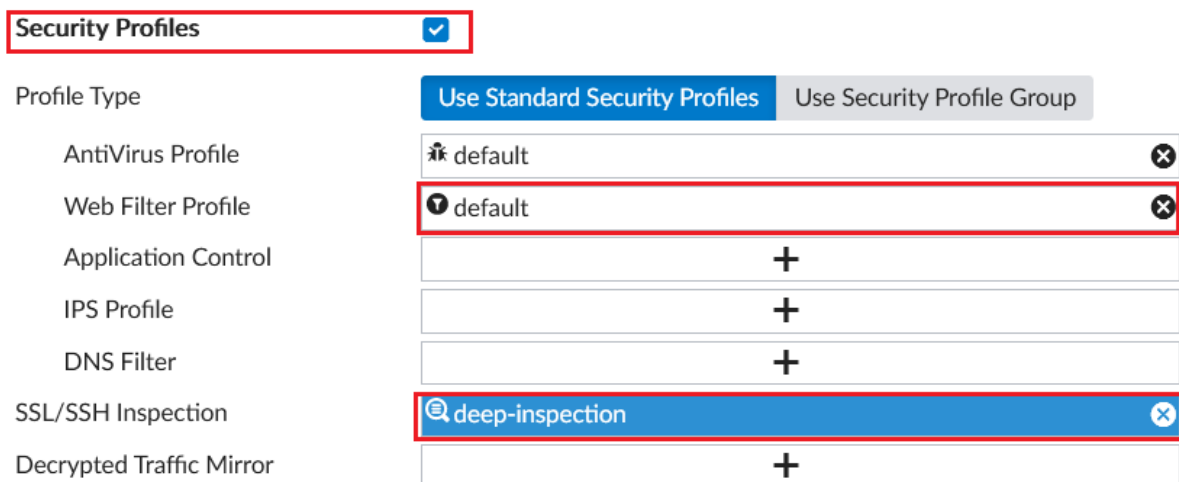
<input type="checkbox"/> Category	Authenticate
<input type="checkbox"/> ▼ Bandwidth Consuming (6)	
<input type="checkbox"/> <input checked="" type="checkbox"/> File Sharing and Storage	
<input type="checkbox"/> <input checked="" type="checkbox"/> Freeware and Software Downloads	
<input type="checkbox"/> <input checked="" type="checkbox"/> Internet Radio and TV	
<input type="checkbox"/> <input checked="" type="checkbox"/> Internet Telephony	
<input type="checkbox"/> <input checked="" type="checkbox"/> Peer-to-peer File Sharing	
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> Streaming Media and Download	
<input type="checkbox"/> ▼ Security Risk (6)	
<input type="checkbox"/> <input checked="" type="checkbox"/> Dynamic DNS	
<input type="checkbox"/> <input checked="" type="checkbox"/> Malicious Websites	
<input type="checkbox"/> <input checked="" type="checkbox"/> Newly Observed Domain	
<input type="checkbox"/> <input checked="" type="checkbox"/> Newly Registered Domain	
<input type="checkbox"/> <input checked="" type="checkbox"/> Phishing	
<input type="checkbox"/> <input checked="" type="checkbox"/> Spam URLs	

Action	Description
Allow	Permit access to the sites in the category.
Block	Prevent access to the sites in the category. Users trying to access a blocked site sees a replacement message indicating the site is blocked.
Monitor	Permits and logs access to sites in the category.
Warning	Displays a message to the user allowing them to continue if they choose.
Authenticate	Requires the user to authenticate with the FortiGate before allowing access.

Open the **Bandwidth Consuming**- section by clicking the + icon beside it. Select **Streaming Media and Download** and then select **Block**.

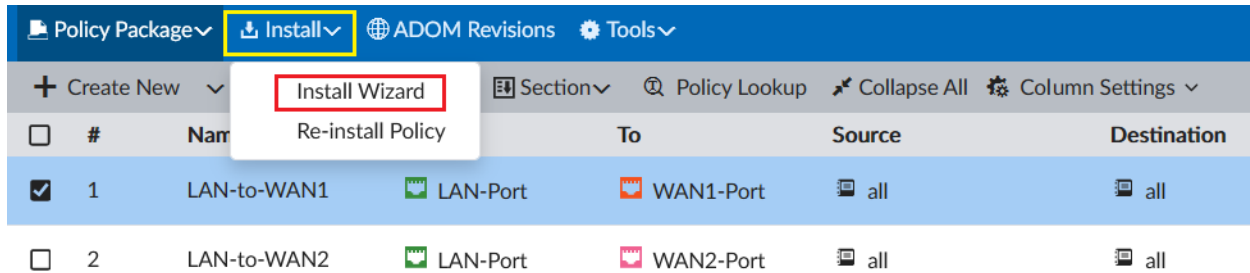


Continue on the FortiManager GUI, click **Policy Packages**, Click **HQ-FW>Firewall Policy**. Select the first policy at the top of the list, and then click **Edit**. Click the Security Profiles check box. Configure AntiVirus Profile and SSL/SSH Inspection and click **OK**.



## Install the Policy:

Continue on the FortiManager GUI, click **Install>Install Wizard**.



#	Name	To	Source	Destination
1	LAN-to-WAN1	LAN-Port	WAN1-Port	all
2	LAN-to-WAN2	LAN-Port	WAN2-Port	all

Select Install Policy Package & Device Settings. Conform that the HQ-FW policy package is selected. And then click **Next**.

### Install Wizard

☒ **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: **HQ-FW**

Comment:

☐ Create ADOM Revision

☐ Schedule Install

☐ Install Device Settings (only)

**Next >** **Cancel**

Confirm that the **HQ-FW** device is selected, and then click **Next**.

### Install Wizard - Policy Package and Device Setting (HQ-FW)

Please select one or more devices to install ( Use checkbox or Ctrl or Shift key for multiple selections)

☐ Device Name      IP Address      Platform




☒ HQ-FW      192.168.100.200      FortiGate-VM64-KVM




**< Back**      **Next >**      **Cancel**

Click Install Preview to see changes that will be applied to FortiGate. Click Close on the Install Preview page. Click **Install**.

## Install Wizard - Policy Package (HQ-FW)

Installation Preparation Total: 3/3,  Success: 3,  Warning: 0,  Error: 0 

-  Interface Validation
-  Policy and Object Validation
-  Ready to Install.

 Install Preview  Policy Package Diff			
<input type="checkbox"/>	Device Name	Status	Action
<input checked="" type="checkbox"/>	HQ-FW[root]	 Connection Up	

Install






Cancel

Once done click **Finish**.

## Install Wizard - Policy Package (HQ-FW)

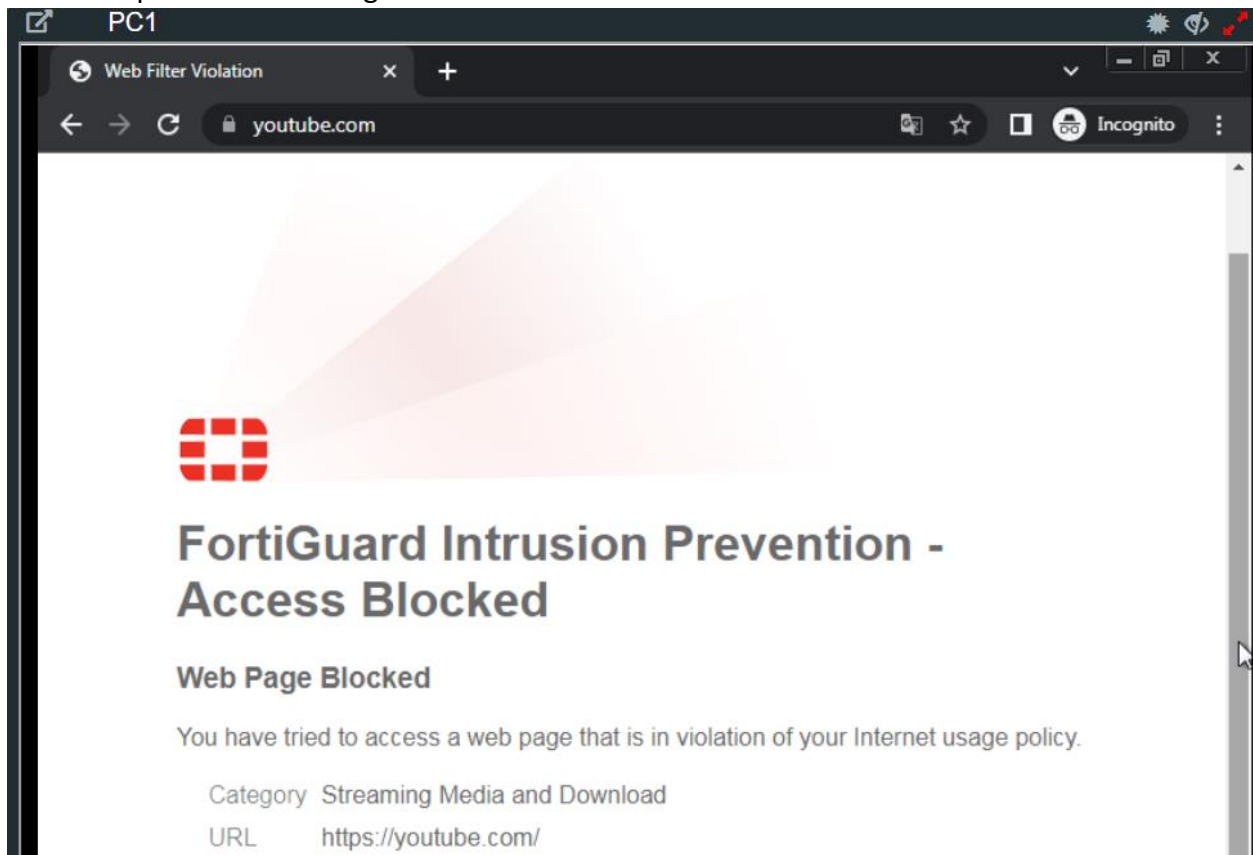
22%

Total: 0/1,  Pending: 0,  In Progress: 1,  Completed: 0 

 View Installation Log  View Progress Report  Column Settings 			
#	Name	Time Used	Status
1	HQ-FW	N/A	 15%

### Verification & Testing:

Validate the URL filter results by going to a blocked website. Go to the **YouTube** website, you see the replacement message.



To check web filter logs in the GUI, Go to **Log & Report > Web Filter**.

Date/Time	User	Source	Action	URL	Category Description
32 seconds ago		10.0.1.10	blocked	https://youtube.com/favicon.ico	Streaming Media and Download
32 seconds ago		10.0.1.10	blocked	https://youtube.com/	Streaming Media and Download
43 seconds ago		10.0.1.10	blocked	https://rr3---sn-q4fl6nde.googlevide...	Streaming Media and Download
43 seconds ago		10.0.1.10	blocked	https://rr3---sn-q4fl6nde.googlevide...	Streaming Media and Download

### Warning Message:

To configure a warning, go to **Policy & Objects > Object Configurations > Security Profiles > Web Filter** and go to the FortiGuard category based filter section. Open the General Interest - Business section by clicking the + icon beside it. Select **Web Hosting** and then select Warning.

☒ **FortiGuard Category Based Filter**

☐ All

▼ Expand All ▶ Collapse All

Category

Authenticate

<input type="checkbox"/>	✓ Armed Forces	
<input type="checkbox"/>	✓ Business	
<input type="checkbox"/>	✓ Charitable Organizations	
<input type="checkbox"/>	✓ Finance and Banking	
<input type="checkbox"/>	✓ General Organizations	
<input type="checkbox"/>	✓ Government and Legal Organizations	
<input type="checkbox"/>	✓ Information Technology	
<input type="checkbox"/>	✓ Information and Computer Security	
<input type="checkbox"/>	✓ Online N	✓ Allow
<input type="checkbox"/>	✓ Remote.	👁 Monitor
<input type="checkbox"/>	✓ Search E	🚫 Block
<input type="checkbox"/>	✓ Secure V	🔔 Warning
<input type="checkbox"/>	✓ URL Sho	👤 Authenticate
<input type="checkbox"/>	✓ Web An	⛔ Disable
<input checked="" type="checkbox"/>	✓ Web Hosting	

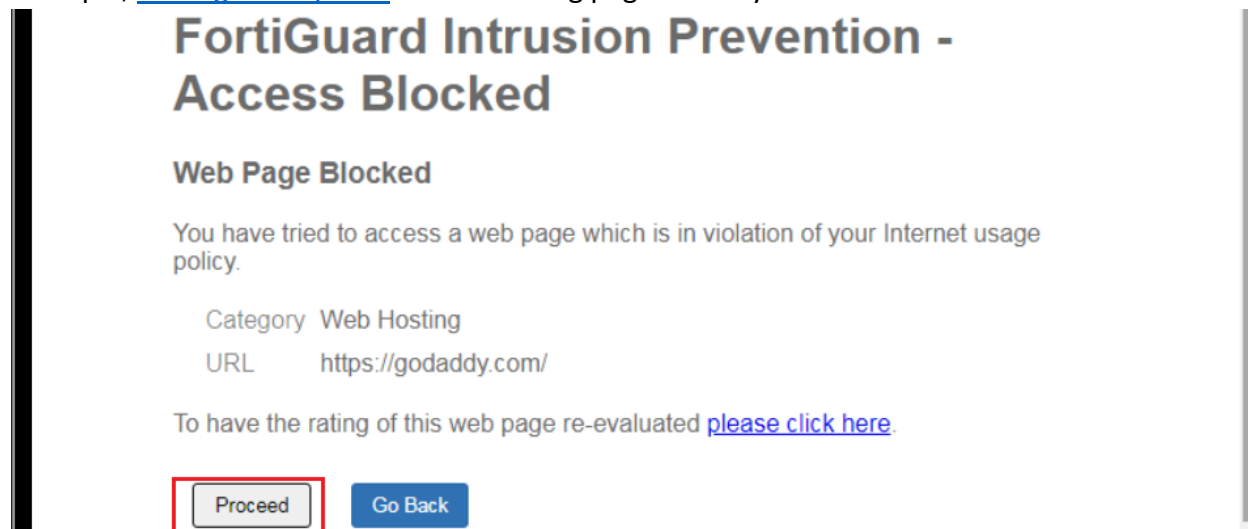
Set the **Warning Interval** which is the interval when the warning page appears again after the user chooses to **continue**.

Warning Interval

OK

Cancel

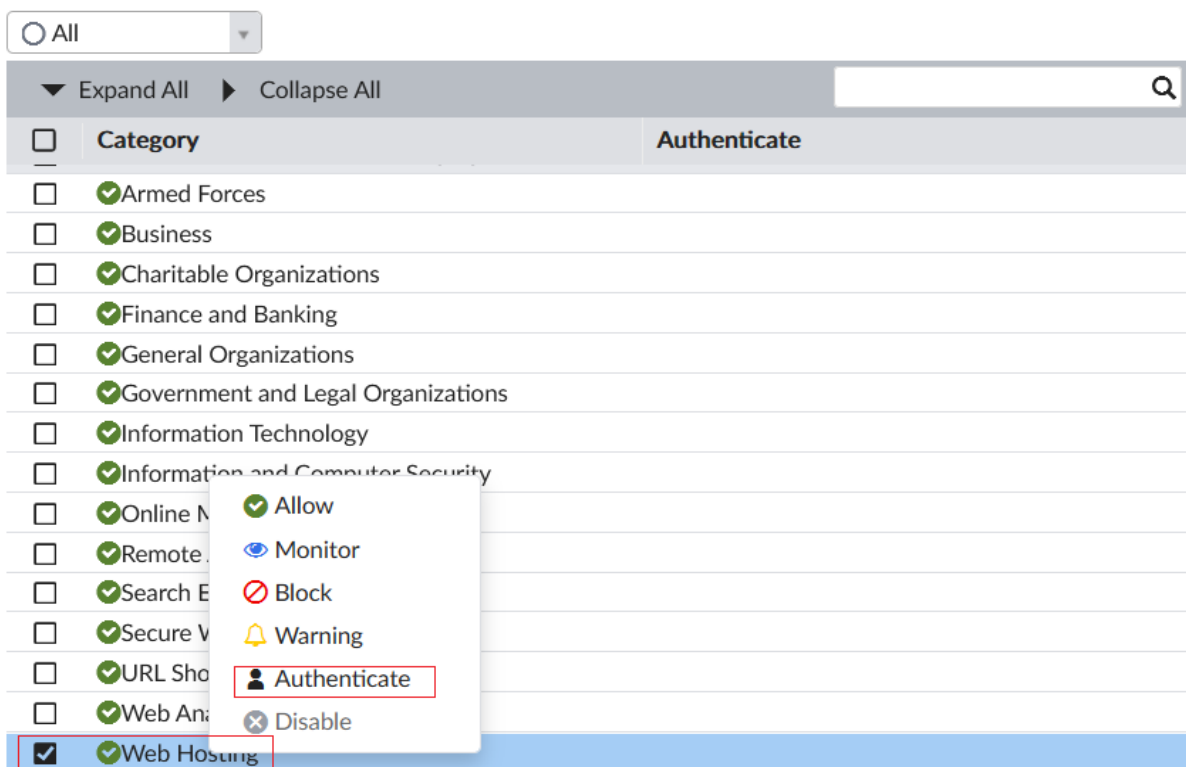
To validate that configured the warning, Go to a website belonging to the selected category, for example, [www.godaddy.com](http://www.godaddy.com) & see warning page where you can choose to Proceed or Go Back.



#### Authenticate Message:

To configure an authentication, go to **Policy & Objects > Object Configurations > Security Profiles > Web Filter** and go to the FortiGuard category based filter section. Open the General Interest - Business section by clicking the + icon beside it. Select **Web Hosting** and then select **Authenticate**.

☒ FortiGuard Category Based Filter






Set the Warning Interval which is the interval when the authentication page appears again after authentication. Click the + icon beside Selected User Group and select a user group. You must have a valid user group to use this feature.

### filters-authenticate

Warning Interval

Minute(s)

Available User Groups

 Guest-group

guest

✕

1 Entry Selected

OK

Cancel

To validate that configured the warning, Go to a website belonging to the selected category, for example, [www.godaddy.com](http://www.godaddy.com) & see warning page where you can choose to **Proceed** or **Go Back**.



## FortiGuard Intrusion Prevention - Access Blocked

### Web Page Blocked

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

Category Web Hosting

URL <http://godaddy.com/>

To have the rating of this web page re-evaluated [please click here](#).

Proceed

Go Back

Click Proceed to check that the authentication page appears. Enter the username and password of the user group you selected and click Continue. If the credentials are correct, the traffic is allowed through.



## FortiGuard Intrusion Prevention - Access Blocked

### Web Filter Block Override

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

Username:

Password: