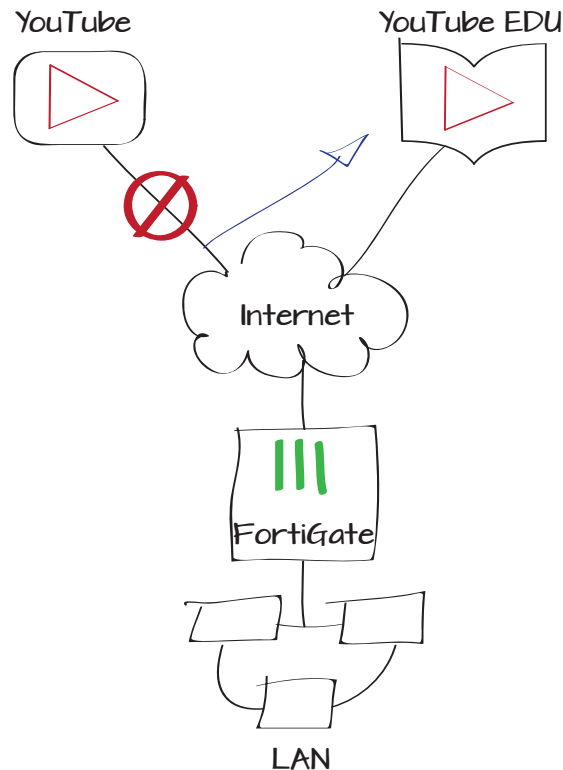


Setting up YouTube for Education

This recipe describes how to apply the YouTube For Education filter, preventing access to all videos that are not part of YouTube's Education portal. It also describes how to implement security policies to prevent two common workarounds that allow users to avoid the filter: using HTTPS access, and visiting a specific YouTube URL.

1. Adding an Application Control Sensor
2. Creating URL and Category web filters
3. Configuring SSL/SSH Inspection
4. Creating blocking and redirecting security policies
5. Results



Adding an Application Control Sensor

Go to **Security Profiles > Application Control > Application Sensors**.

Select the Plus icon in the upper right corner to create a new application sensor.

Select **Create New** to create the application filter, and set the **Sensor Type** to **Specify Applications**. Filter the results by searching for 'youtube', and highlight all the entries that contain it.

Set the **Action** to **Block**.

Sensor Type Filter Based Specify Applications
Filter Options Basic Advanced

Search: youtube

Application Name	Category	Technology
Free.YouTube.Download	Video/Audio	Client-Server
YouTube_Video.Embedded	Video/Audio	Browser-Based
YouTube	Video/Audio	Browser-Based
YouTube.Downloader.YTD	Video/Audio	Client-Server
YouTube_Comment.Posting	Video/Audio	Browser-Based
YouTube_HD.Streaming	Video/Audio	Browser-Based
YouTube_Play.Video	Video/Audio	Browser-Based
YouTube_Search.Safety.Mode.Off	Video/Audio	Browser-Based
YouTube_Search.Video	Video/Audio	Browser-Based
YouTube_Uploading	Video/Audio	Browser-Based

Action: Monitor Block Reset Traffic Shaping

Creating URL and Category web filters

Go to **Security Profiles > Web Filter > Profiles**. You'll need to create two filters; one to block access to the YouTube URL and one to enforce the YouTube Education Filter.

Create a new web filter profile, that will block HTTP and HTTPS access to YouTube.

Enable **Web Site Filter**, and create a new URL filter, entering "*.youtube.com" as the URL. Set the Type to **Wildcard**, and the **Action** to **Block**.

Name: Block_YouTube_HTTPS
Comments: Write a comment... 0/255
Inspection Mode: Proxy Flow-based DNS
 FortiGuard Categories
Show All X
+ Local Categories
+ Potentially Liabile
+ Adult/Mature Content
+ Bandwidth Consuming
+ Security Risk
+ General Interest - Personal
+ General Interest - Business
+ Unrated
Quota on Categories with Monitor, Warning and Authenticate Actions
 Enable Safe Search
 Scan Encrypted Connections (Exempted Categories: Banking Health Care Personal Privacy)
 Enable Web Site Filter
Create New Edit Delete

URL	Type	Action	Status
*.youtube.com	Wildcard	Block	Enable

Create a second web filter profile, that will enforce the YouTube for Education filter.

You can also enable FortiGuard Categories to block other unwanted content, but **Bandwidth Consuming > Streaming Media and Download** must be allowed or your users will not be able to access the Education portal.

Enable **Safe Search**, and enable the **Youtube Education Filter**. Enter the Education Filter registration code, provided to you by YouTube. To get a code, visit <http://www.youtube.com/t/education>.

Configuring SSL/SSH Inspection

Go to **Policy > Policy > SSL/SSH Inspection**.

Create a new **Deep Inspection Options** profile. Ensure that **SSH Deep Scan** is enabled.

Name

Comments

Inspection Mode Proxy Flow-based DNS

FortiGuard Categories

Show Allow

- Bandwidth Consuming
 - File Sharing and Storage
 - Freeware and Software Downloads
 - Internet Radio and TV
 - Internet Telephony
 - Peer-to-peer File Sharing
 - Streaming Media and Download

▶ Quota on Categories with Monitor, Warning and Authenticate Actions

Enable Safe Search

Search Engine Safe Search - Google, Yahoo!, Bing, Yandex

YouTube Education Filter

Name

Comments

SSL Inspection Options

CA Certificate

Inspect All Ports

Enable	Protocol	Inspection Port(s)
<input checked="" type="checkbox"/>	HTTPS	<input type="text" value="443"/>
<input checked="" type="checkbox"/>	SMTPS	<input type="text" value="465"/>
<input checked="" type="checkbox"/>	POP3S	<input type="text" value="995"/>
<input checked="" type="checkbox"/>	IMAPS	<input type="text" value="993"/>
<input checked="" type="checkbox"/>	FTPS	<input type="text" value="990"/>

SSH Inspection Options

Enable SSH Deep Scan

Creating blocking and redirecting security policies

Now, go to **Policy > Policy > Policy**. You will need to create two policies, to prevent the two filter workarounds.

Create the first policy, which will block HTTPS traffic to YouTube.

Set the internal-network-facing interface as **Incoming Interface**, your Internet-facing interface as **Outgoing Interface**, and select HTTPS for **Service**.

Enable NAT.

Under **Security Profiles**, enable **Web Filter**, using your HTTPS filter. Enable **Application Control**, using your App filter.

Lastly, enable **SSL/SSH Inspection**, using your Deep Inspection filter.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	port1 (Internal)
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTPS
Action	ACCEPT
<input checked="" type="checkbox"/> Enable NAT	

Security Profiles	
<input type="checkbox"/> AntiVirus	default
<input checked="" type="checkbox"/> Web Filter	Block_YouTube_HTTPS
<input checked="" type="checkbox"/> Application Control	Block_YouTube_App
<input type="checkbox"/> IPS	default
<input type="checkbox"/> Email Filter	default
<input type="checkbox"/> DLP Sensor	default
<input type="checkbox"/> VoIP	default
<input type="checkbox"/> ICAP	default
Proxy Options	default
<input checked="" type="checkbox"/> SSL/SSH Inspection	YT_Deep_Inspection

Create the second policy, which will force all remaining YouTube traffic to the Education portal.

Set the internal interface as **Incoming**, the internet-facing interface as **Outgoing**, and enable NAT.

Under **Security Profiles**, enable **Web Filter**, using your Education filter.

Enable **SSL/SSH Inspection**, using your Deep Inspection filter.

Return to the policy list and move your HTTPS blocking policy as close to the top as possible without affecting existing policies.

Move the education filter policy immediately below the HTTPS policy.

Policy Type Firewall VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Security Profiles

AntiVirus

Web Filter

Application Control

IPS

Email Filter

DLP Sensor

VoIP

ICAP

Proxy Options

SSL/SSH Inspection

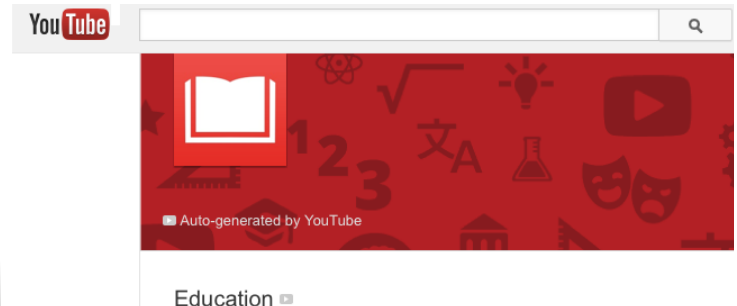
Seq.#	From	To	Service	Action	Web Filter
1	port1	wan1	HTTP HTTPS	Accept	Block_YouTube_HTTPS
2	port1	wan1	ALL	Accept	YT_Education_Filter

Results

Browse to www.youtube.com. You will arrive at the YouTube for Education homepage and only be able to access videos that have been approved as educational content.

If you attempt to avoid the filter by visiting <https://www.youtube.com>, the browser will attempt to reach the page but will eventually time out or present a message such as “The connection to the server was reset” or “Server not found”.

If you attempt to avoid the filter by visiting a specific YouTube URL, such as www.youtube.com/watch?v=H9UtpYOwlgk, the video will be replaced with an error message like the one shown.



Server not found

Firefox can't find the server at youtube.com.

- Check the address for typing errors such as ww.example.com instead of www.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

