

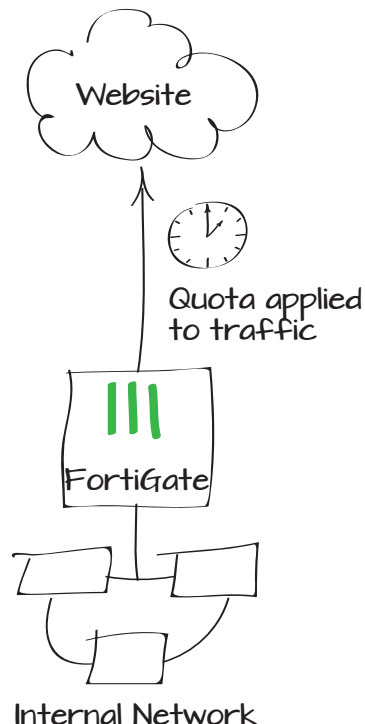
# Limiting access to personal interest websites using quotas

Many workplaces allow employees to access personal interest websites during their breaks. The most efficient method to do this is by using quotas, since they do not require set schedules. This example uses quotas to allow access at any point during the day but only for a total of 15 minutes for each user.



This example requires an active license for FortiGuard Web Filtering Services.

1. Creating a web filter profile that uses quotas
2. Adding the web filter profile to a security policy
3. Adding HTTPS scanning (optional)
4. Results



## Creating a web filter profile that uses quotas

Go to **Security Profiles > Web Filter > Profiles**.

Create a new profile and enable **FortiGuard Categories**. Right-click on the category **General Interest - Personal** and select **Monitor**. Do the same for the category **General Interest - Business**

These categories include a variety of sites that are commonly blocked in the workplace, such as games, instant messaging, and social media.

Expand **Quota on Categories with Monitor, Warning and Authenticate Actions** and select **Create New**. Select both **General Interest - Personal** and **General Interest - Business** and set the **Quota** amount to 15 Minutes.



You can also apply quotas to specific sub-categories within a FortiGuard Category, such as Shopping and Auction and Social Networking, both of which are found in the General Interest - Personal category). By doing this, you can target specific sites you wish to limit without affecting every site within the larger category.

Name: quotas

Comments: allows access to general interest with quotas 45/255

Inspection Mode:  Proxy  Flow-based  DNS

FortiGuard Categories

Show All

- 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

- General Interest - Personal
- General Interest - Business
- Unrated

Quota: 15 Minute(s)

## Adding the web filter profile to a security policy

Go to **Policy > Policy > Policy**.

Edit the policy controlling the traffic you wish to apply the quotas to. Under **Security Profiles**, enable **Web Filter** and set it to use the new profile.

Policy Type  Firewall  VPN

Policy Subtype  Address  User Identity  Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Use Destination Interface Address  Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

**Logging Options**

No Log

Log Security Events

Log all Sessions

**Security Profiles**

ON AntiVirus

ON Web Filter

## Adding HTTPS scanning (optional)

If you wish to apply the quotas to HTTPS traffic as well as HTTP, you must create an SSL inspection profile and add it to your security policy. For more information about blocking HTTPS traffic, see “[Blocking HTTPS traffic with web filtering](#)” on page 149.

## Results

Browse to [www.ebay.com](http://www.ebay.com), a website that is found within the General Interest - Personal category.

Access to the website is allowed for 15 minutes, after which a block message appears. The message will persist for all General Interest - Personal sites until the quota is reset, which occurs every day at midnight.

Go to **Log & Report > Traffic Log > Forward Traffic Log** to monitor allowed and blocked traffic to these categories that have quotas.

Select an entry for more information about a session.

### FortiGuard Web Filtering

**Web Page Blocked**

Your daily quota for this category of webpage has expired, in accordance with your internet usage policy.  
URL: [www.ebay.com/chp/collectibles-art](http://www.ebay.com/chp/collectibles-art)  
Category: Shopping and Auction  
To have the rating of this web page re-evaluated [please click here](#).

Dst	Security Acti...	Application Details	Threat
173.194.43.66 (www.google-analytics.com)	✘	safebrowsing.clients.google.com	Search Engines and Portals
108.160.162.43 (notify5.dropbox.com)	✘	notify5.dropbox.com	File Sharing and Storage
93.158.134.25 (mail.yandex.ru)	✘	mail.yandex.com	Web-based Email
108.160.162.43 (notify5.dropbox.com)	✘	notify5.dropbox.com	File Sharing and Storage
66.135.211.36 (srv.g.ebay.com)	✘	srx.main.ebayrtm.com	Shopping and Auction
66.211.181.181 (www.ebay.com)	✘	www.ebay.com (and another)	Shopping and Auction
174.37.236.19 (cacerts.digicert.com)	✔	cacerts.digicert.com	Information Technology
108.160.163.51 (notify5.dropbox.com)	✘	notify5.dropbox.com	File Sharing and Storage
132.246.2.7 (static.ak.facebook.com)			
66.211.181.181 (www.ebay.com)	✔	www.ebay.com (and another)	Shopping and Auction

<b>Application Details</b>	srx.main.ebayrtm.com	<b>Category Description</b>	Shopping and Auction
<b>Date/Time</b>	07:40:56 (1378280456)	<b>Destination Country</b>	United States
<b>Dst</b>	66.135.211.36 (srv.g.ebay.com)	<b>Dst Interface</b>	wan1
<b>Dst Port</b>	80	<b>Duration</b>	11
<b>Hostname</b>	srx.main.ebayrtm.com	<b>Level</b>	notice <span style="color: blue;">■■■■■</span>
<b>Log ID</b>	13	<b>Policy ID</b>	2
<b>Protocol</b>	6	<b>Received</b>	3473
<b>Received Packets</b>	6	<b>Security Action</b>	✘
<b>Security Event</b>	webfilter	<b>Security Sub Type</b>	ftgd-quota
<b>Sent</b>	701	<b>Sent / Received</b>	701 B / 3.39 KB
<b>Sent Packets</b>	4	<b>Sequence Number</b>	29326
<b>Service</b>	HTTP	<b>Source Country</b>	Reserved
<b>Src</b>	192.168.100.112	<b>Src Interface</b>	lan
<b>Src NAT IP</b>	172.20.120.236	<b>Src NAT Port</b>	57344
<b>Src Port</b>	57344	<b>Status</b>	close
<b>Sub Type</b>	forward	<b>Threat</b>	Shopping and Auction
<b>Timestamp</b>	Wed Sep 4 07:40:56 2013	<b>Tran Display</b>	snat
<b>URL Count</b>	1	<b>Virtual Domain</b>	root