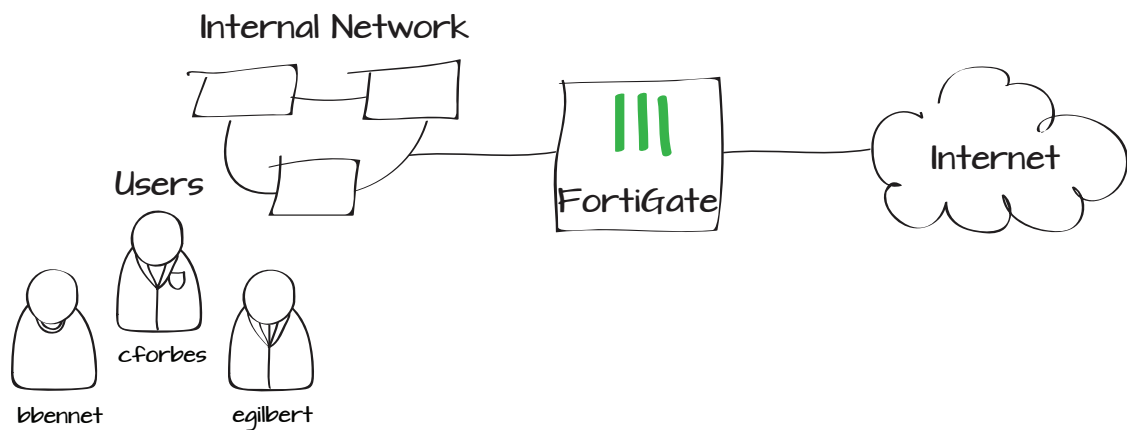


# Identifying network users and applying web filters based on identity

This example uses an identity-based security policy to identify and monitor all users accessing the Internet through your FortiGate unit by requiring them to authenticate in order to connect. Different web filtering profiles will also be applied to traffic based on the user's credentials.

1. Creating users
2. Creating a user group
3. Creating a web filter profile
4. Configuring an identity-based security policy
5. Results



## Creating users

Go to **User & Device > User > User Definition**.

Using the **User Creation Wizard**, create three local users: *bbennet*, *cforbes*, and *egilbert*.

All three users now appear in the user list.

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

Local User  
 Remote RADIUS User  
 Remote TACACS+ User  
 Remote LDAP User

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

User Name   
Password

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

Email Address   
 SMS

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

Enable  
 Two-factor Authentication  
 User Group

< Back Done Cancel

User Name	Type	Two-factor Authentication	Ref.
bbennet	LOCAL	<input checked="" type="checkbox"/>	0
cforbes	LOCAL	<input checked="" type="checkbox"/>	0
egilbert	LOCAL	<input checked="" type="checkbox"/>	0

## Creating a user group

Go to **User & Device > User > User Groups**.

Create a new user group and add users bbennet and cforbes.

The user group now appears in the user group list.

## Creating a web filter profile

Go to **Security Profiles > Web Filter > Profiles**. The default web filter profile is shown, which will be later applied to traffic for members of the user group.

Create a new profile. Enable **FortiGuard Categories** and set the category **General Interest - Personal** to **Block**.

Name

Type  Firewall  Fortinet Single Sign-On (FSSO)  Guest

Members

- X
- X

Group Name	Group Type	Members	R
FSSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)		0
employees (2 Members)	Firewall	bbennet cforbes	0

Name

Comments  0/255

Inspection Mode  Proxy  Flow-based  DNS

FortiGuard Categories

Show All X

- Local Categories
- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
- Security Risk
- General Interest - Personal
- General Interest - Business
- Unrated

## Configuring an identity-based security policy

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

Edit the policy controlling your outgoing traffic and set **Policy Subtype** to **User Identity**.

Create two **Authentication Rules** that allow Internet access. For the first rule, set **Group(s)** to the user group. Enable **Web Filter** and set it to use the default profile.

For the second rule, set **User(s)** to egilbert. Enable **Web Filter** and set it to use the new profile.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input type="radio"/> Address <input checked="" type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	lan
Source Address	all
Outgoing Interface	wan1
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
<input type="radio"/> Use Central NAT Table	
Destination Address	all
Group(s)	employees
User(s)	Click to add...
Schedule	always
Service	ALL
Action	ACCEPT
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
<b>Security Profiles</b>	
<input type="checkbox"/> AntiVirus	default
<input checked="" type="checkbox"/> Web Filter	default
Destination Address	all
Group(s)	Click to add...
User(s)	egilbert
Schedule	always
Service	ALL
Action	ACCEPT
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
<b>Security Profiles</b>	
<input type="checkbox"/> AntiVirus	default
<input checked="" type="checkbox"/> Web Filter	restricted_access

## Results

When a user attempts to connect to the Internet, the authentication screen will appear. In order to get full Internet access, log in as user cforbes.

Browse to [www.ebay.com](http://www.ebay.com), a site that is in the **General Interest - Personal** category. Using this account, you can access the website.

Go to **User & Device > Monitor > Firewall**. The cforbes account appears on the firewall monitor list.

Select the account on the list and select **De-authenticate**. This will require you to enter the credentials again in order to continue browsing the Internet.

Log in again, this time using the egilbert account.

Browse to [www.ebay.com](http://www.ebay.com). Now that you are using the egilbert account, the website will be blocked.



The image shows a Fortinet authentication screen. At the top, the Fortinet logo is displayed in a bold, black, sans-serif font. Below the logo, the text "Authentication Required" is centered. Underneath, a message reads "Please enter your username and password to continue." There are two input fields: "Username:" with the text "cforbes" entered, and "Password:" with a series of dots. A "Continue" button is located at the bottom right of the form area.

User Name	User Group	Duration	IP Address
cforbes	employees	0 day(s) 0 hour(s) 1 minute(s)	192.168.13.110

### FortiGuard Web Filtering



#### Web Page Blocked!

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

URL: [www.ebay.com/](http://www.ebay.com/)  
Category: Shopping and Auction

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

Go to **Log & Report > Traffic Log > Forward Traffic**. Right-click on the header row, enable the **User** column, and select **Apply** to view session information for each user.



You may be required to scroll down the menu in order to select **Apply**.

Select an entry for more information.

Date/Time	User	Destination	Security Action
12:54:05	cforbes	108.166.2.184 (www.innovatia.net)	
12:54:04	cforbes	108.166.2.184 (www.innovatia.net)	
12:54:04	cforbes	23.1.169.232 (gh.ebaystatic.com)	
12:54:04	cforbes	108.166.2.184 (www.innovatia.net)	
12:54:03	cforbes	142.166.163.53 (elearning1.innovatia.net)	
12:53:48	bbennet	199.27.72.196 (widgets.pinterest.com)	
12:53:47	bbennet	199.27.78.134 (mac-tuts.disqus.com)	
12:53:44	bbennet	66.211.178.172 (rover.ebay.com)	
12:53:44	bbennet	199.27.78.196 (a.ssl.fastly.net)	
12:53:44	bbennet	173.192.42.188 (disqus.com)	
12:52:54	egilbert	184.84.41.232 (e2405.b.akamaiedge.net)	✘
12:52:54	egilbert	66.211.178.172 (rover.ebay.com)	✘
12:52:54	egilbert	23.1.169.232 (gh.ebaystatic.com)	✘

<b>Application Details</b>	rover.ebay.com	<b>Category Description</b>	Shopping and Auction
<b>Date/Time</b>	08:21:57 (1382430117)	<b>Destination</b>	66.211.178.172 (rover.ebay.com)
<b>Destination Country</b>	United States	<b>Dst Interface</b>	wan1
<b>Dst Port</b>	80	<b>Duration</b>	11
<b>Group</b>	egilbert	<b>Hostname</b>	rover.ebay.com
<b>Identity Index</b>	2	<b>Level</b>	notice
<b>Log ID</b>	13	<b>Policy ID</b>	3
<b>Protocol</b>	6	<b>Received</b>	3152
<b>Received Packets</b>	6	<b>Security Action</b>	✘
<b>Security Event</b>	webfilter	<b>Security Sub Type</b>	ftgd-cat
<b>Sent</b>	1071	<b>Sent / Received</b>	1.05 KB / 3.08 KB
<b>Sent Packets</b>	5	<b>Sequence Number</b>	89431
<b>Service</b>	HTTP	<b>Source</b>	egilbert (192.168.13.110)
<b>Source Country</b>	Reserved	<b>Src Interface</b>	lan
<b>Src NAT IP</b>	172.20.120.236	<b>Src NAT Port</b>	61814
<b>Src Port</b>	61814	<b>Status</b>	close
<b>Sub Type</b>	forward	<b>Threat</b>	Shopping and Auction