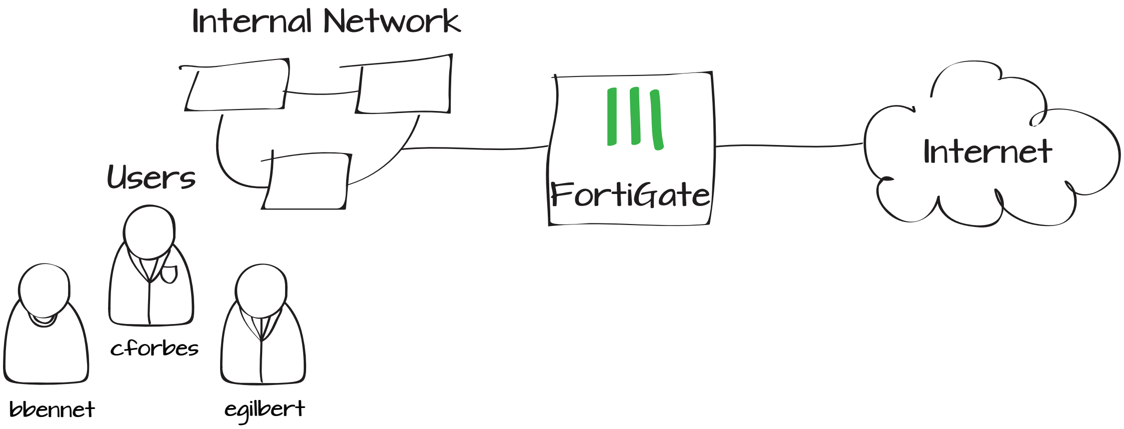
Identifying network users and applying web filters based on identity

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.

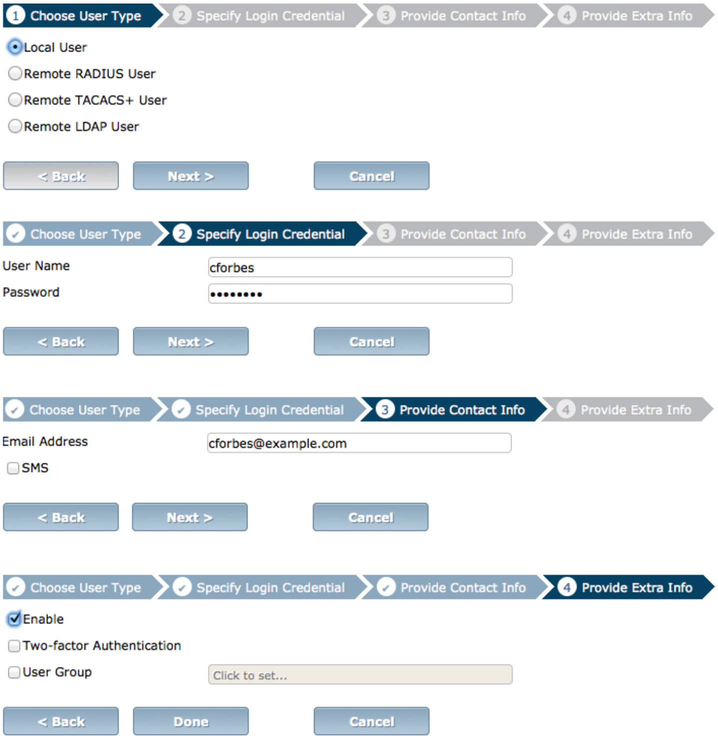
1. Creating users
2. Creating a user group
3. Creating a web filter profile
4. Configuring an identity-based security policy
5. Results



Creating users

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

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



● Local User
○ Remote RADIUS User
○ Remote TACACS+ User
○ Remote LDAP User

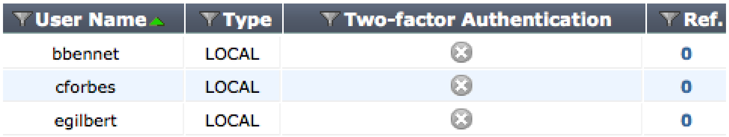
User Name	cforbes
Password	••••••••

Email Address	cforbes@example.com

□ SMS

☑ Enable
□ Two-factor Authentication
□ User Group Click to set...

All three users now appear in the user list.

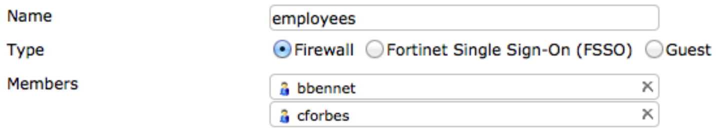


User Name	Type	Two-factor Authentication	Ref.
bbennet	LOCAL	⊗	0
cforbes	LOCAL	⊗	0
egilbert	LOCAL	⊗	0

Creating a user group

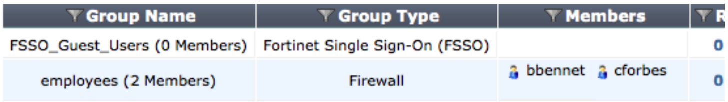
Go to **User & Device > User > User Groups**.

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



Name	employees
Type	● Firewall ○ Fortinet Single Sign-On (FSSO) ○ Guest
Members	bbennet × cforbes ×

The user group now appears in the user group list.

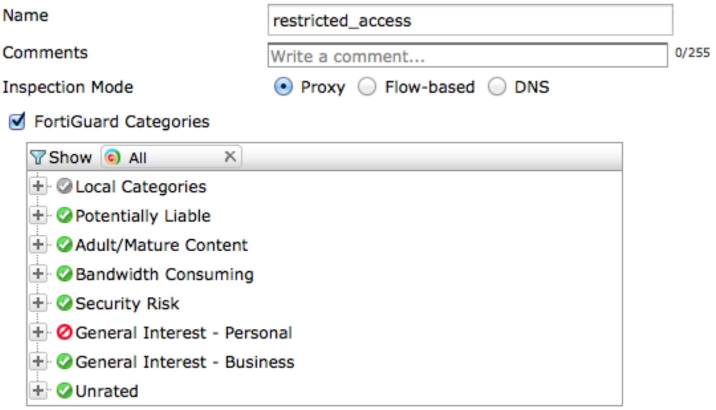


Group Name	Group Type	Members	R
FSSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)		0
employees (2 Members)	Firewall	bbennet cforbes	0

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	restricted_access
Comments	Write a comment... 0/255
Inspection Mode	● Proxy ○ Flow-based ○ DNS

☑ FortiGuard Categories

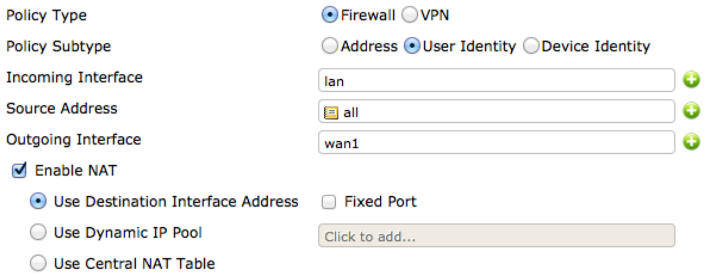
Show All ×

- + ✓ 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**.



Policy Type ● Firewall ○ VPN

Policy Subtype ○ Address ● User Identity ○ Device Identity

Incoming Interface: lan

Source Address: all

Outgoing Interface: wan1

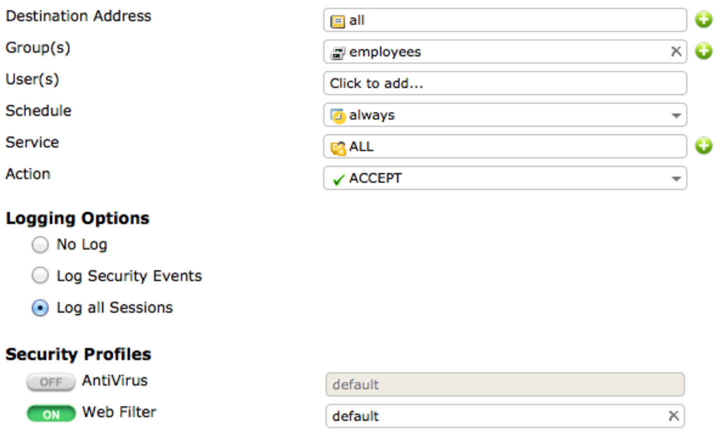
☑ Enable NAT

● Use Destination Interface Address ☐ Fixed Port

○ Use Dynamic IP Pool: Click to add...

○ Use Central NAT Table

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.



Destination Address: all

Group(s): employees

User(s): Click to add...

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Logging Options

○ No Log

○ Log Security Events

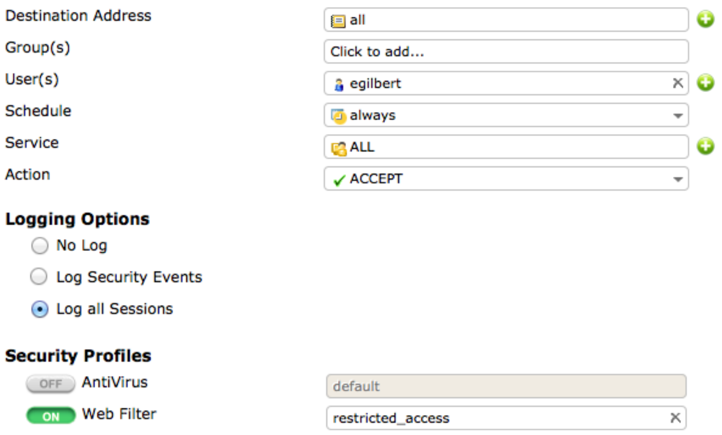
● Log all Sessions

Security Profiles

OFF AntiVirus: default

ON Web Filter: default

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



Destination Address: all

Group(s): Click to add...

User(s): egilbert

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Logging Options

○ No Log

○ Log Security Events

● Log all Sessions

Security Profiles

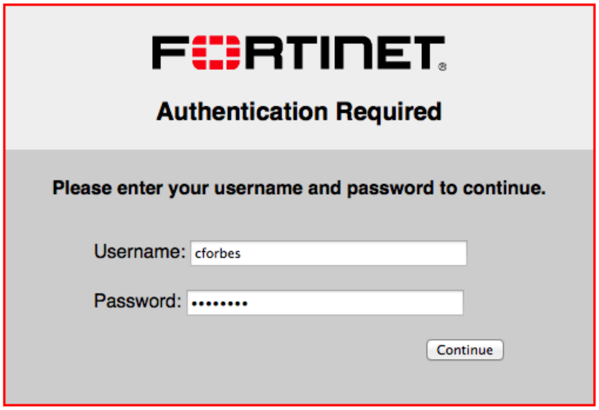
OFF AntiVirus: default

ON 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, a site that is in the **General Interest - Personal** category. Using this account, you can access the website.



FORTINET

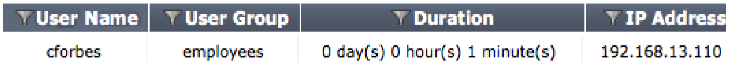
Authentication Required

Please enter your username and password to continue.

Username: cforbes

Password: ••••••••

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

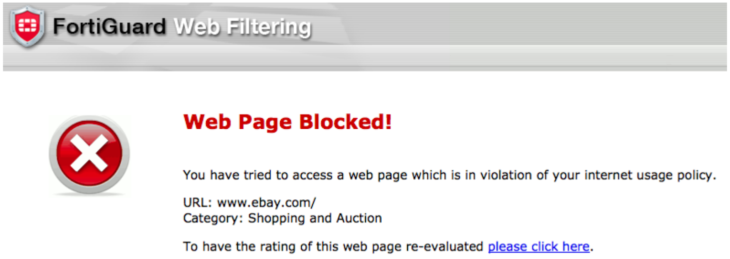


User Name	User Group	Duration	IP Address
cforbes	employees	0 day(s) 0 hour(s) 1 minute(s)	192.168.13.110

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. Now that you are using the egilbert account, the website will be blocked.



FortiGuard Web Filtering

Web Page Blocked!

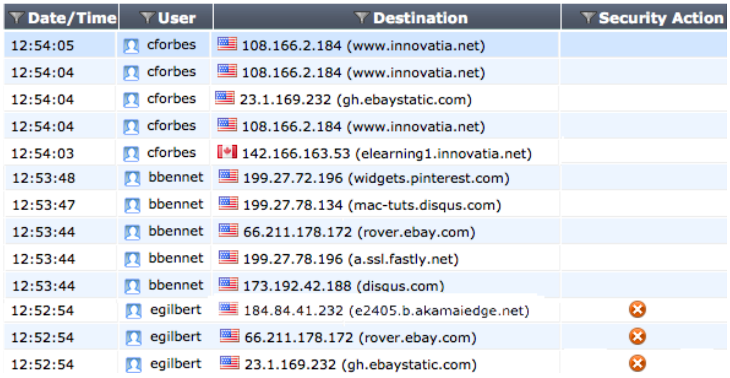
You have tried to access a web page which is in violation of your internet usage policy.

URL: www.ebay.com/
Category: Shopping and Auction

To have the rating of this web page re-evaluated please click here.

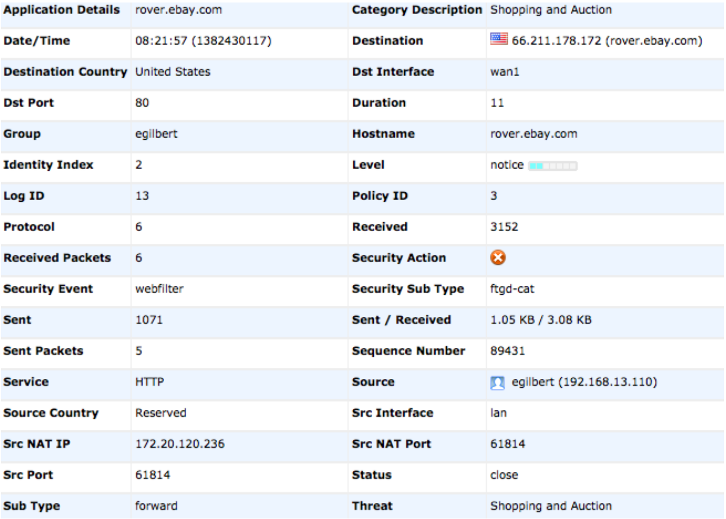
Go to **Log & Report > Traffic Log > Forward Traffic**. Right-click on the header row, enable the **User** column, and select **Apply** to view session information for each user.

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



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)	⊗

Select an entry for more information.



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