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.
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**.

---

**User Group List**

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Group Type</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSSO_Guest_Users (0 Members)</td>
<td>Fortinet Single Sign-On (FSSO)</td>
<td></td>
</tr>
<tr>
<td>employees (2 Members)</td>
<td>Firewall</td>
<td>bbennet, cforbes</td>
</tr>
</tbody>
</table>
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.
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.

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