Controlling which applications can access network resources and the Internet

In this example, you will learn how to use Application Control to monitor traffic and determine if there are any applications currently in use that should not have network access. If you discover any applications that you wish to block, application control will then be used to ensure that these applications cannot access the network.

1. Enabling Application Control and multiple security profiles
2. Using the default application profile to monitor network traffic
3. Adding the default profile to a security policy
4. Reviewing the FortiView dashboards
5. Creating an application profile to block applications
6. Adding the blocking sensor to a security policy
7. Results

---

```
Session begins

Application specific traffic

Application control enabled?

Traffic not affected

Application targeted?

Action applied

yes

no
```
1. Enabling Application Control and multiple security profiles

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.

Select **Show More** and enable **Multiple Security Profiles**. **Apply** the changes.

2. Using the default application profile to monitor network traffic

Go to **Security Profiles > Application Control** and view the **default** profile.

A list of application **Categories** is shown. By default, most categories are already set to **Monitor**. In order to monitor all applications, select **All Other Known Applications** and set it to **Monitor**. Do the same for **All Other Unknown Applications**.

The default profile also has **Deep Inspection of Cloud Applications** turned **ON**. This allows web-based applications, such as video streaming, to be monitored by your FortiGate.
3. Adding the default profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Enabling Application Control will automatically enable **SSL Inspection**. In order to inspect traffic from Cloud Applications, the **deep-inspection** profile must be used.

Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see “Preventing security certificate warnings when using SSL full inspection” on page 72.

4. Reviewing the FortiView dashboards

Go to **System > FortiView > Applications** and select the **now** view.

This dashboard shows the traffic that is currently flowing through your FortiGate, arranged by application (excluding Cloud Applications).
If you wish to know more about an application's traffic, double-click on its entry to view drilldown information, including traffic sources, traffic destinations, and information about individual sessions.

Similar information can be viewed for Cloud Applications by going to System > FortiView > Cloud Applications and selecting Applications that have been used in the last 5 Minutes.

Cloud Applications also have drilldown options, including the ability to see which videos have been viewed if streaming video traffic was detected.
5. Creating an application profile to block applications

In the above example, traffic from BitTorrent, a Peer-to-Peer (P2P) downloading application, was detected. Now, you will create an application control profile that will block P2P traffic.

The new profile will also block all applications associated with Youtube, without blocking other applications in the Video/Audio category.

Go to Security Profiles > Application Control and create a new profile.

Select the P2P category and set it to Block.

Under Application Overrides, select Add Signatures.

Search for Youtube and select all the signatures that are shown.

Select Use Selected Signatures.
The signatures have been added to the Application Overrides list and have automatically been set to Block.

Enable **Deep Inspection of Cloud Applications**.

<table>
<thead>
<tr>
<th>Application Signature</th>
<th>Category</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>YouTube</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube.App</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>Youtube.Downloader.YTD</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_Comment.Posting</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_HD.Streaming</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_Search.Safety.Mode.Off</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_Search.Video</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_Video.Access</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_Video.Embedded</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_Video.Play</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>YouTube_Video.Upload</td>
<td>Video/Audio</td>
<td>Block</td>
</tr>
<tr>
<td>Youtubeproxyfree</td>
<td>Proxy</td>
<td>Block</td>
</tr>
</tbody>
</table>

**Options**

- **ON** Deep Inspection of Cloud Applications

---

6. **Adding the blocking sensor to a security policy**

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **Application Control** to use the new profile.
7. Results

Attempt to browse to www.youtube.com. A warning message will appear, stating that the application was blocked.

Traffic from BitTorrent applications will also be blocked.

To see information about this blocked traffic, go to System > FortiView > All Sessions, select the 5 minutes view, and filter the traffic by application.