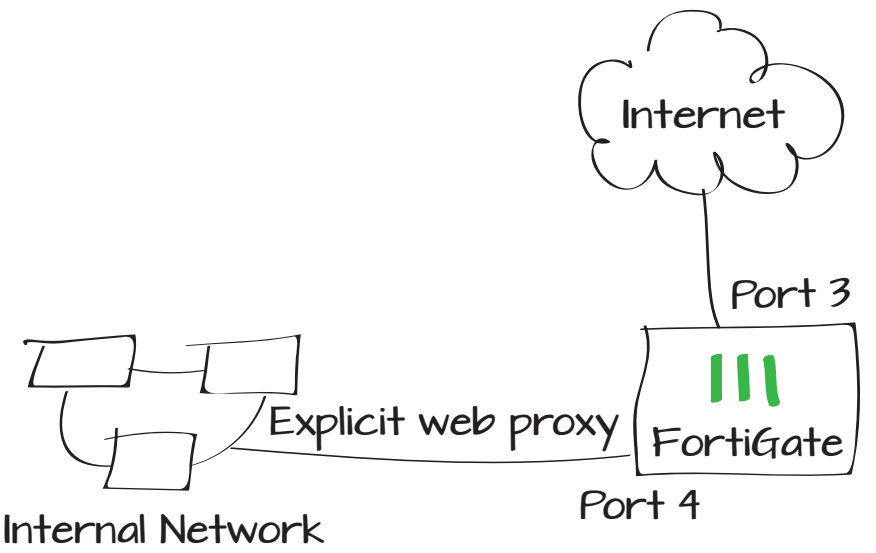
Setting up an explicit proxy for users on a private network

In this example, an explicit web proxy is set to accommodate faster web browsing. This allows internal users to connect using port 8080 rather than port 80.

1. Enabling explicit web proxy on the internal interface
2. Configuring the explicit web proxy for HTTP/HTTPS traffic
3. Adding a security policy for proxy traffic
4. Results



Enabling explicit web proxy on the internal interface

Go to **System > Network > Interfaces**.

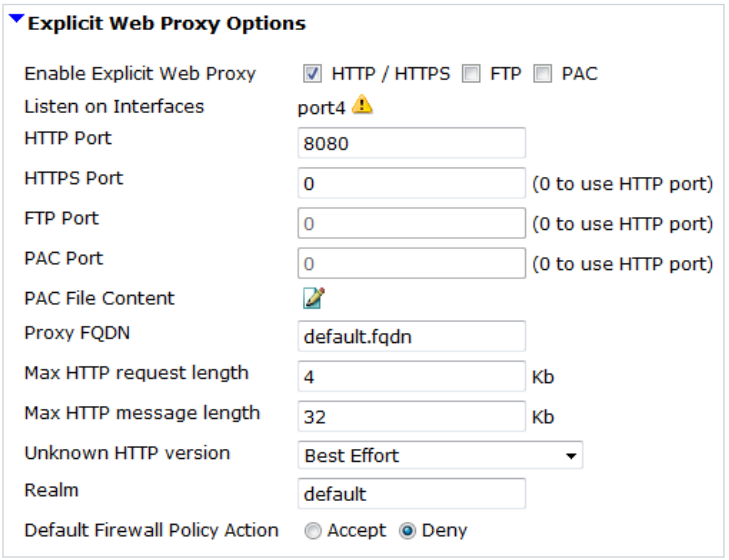
Edit an internal port (port 4 in the example). **Enable** both **DHCP Server** and **Explicit Web Proxy**.

Go to **System > Config > Features**. Ensure that **WAN Opt. & Cache** is enabled.

Configuring the explicit web proxy for HTTP/HTTPS traffic

Go to **System > Network > Explicit Proxy** and enable the HTTP/HTTPS explicit web proxy.

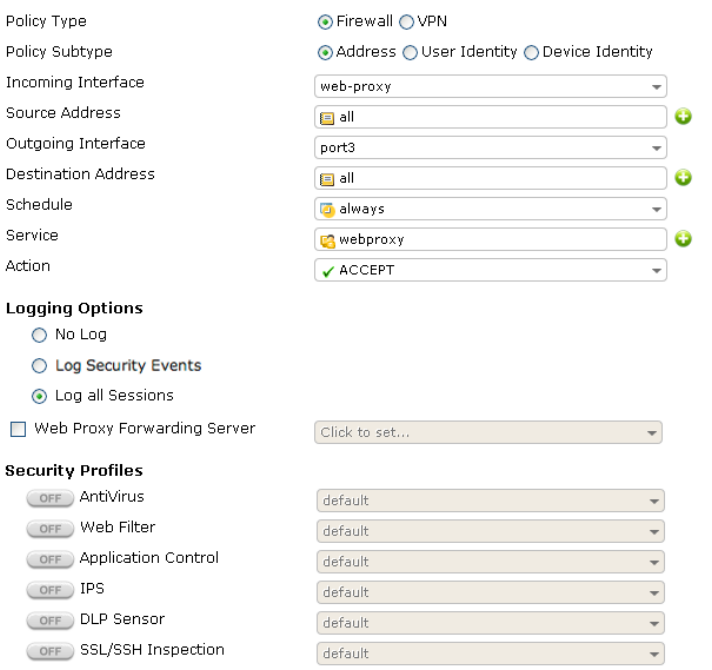
Ensure that the **Default Firewall Policy Action** is set to **Deny**.



Adding a security policy for proxy traffic

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

Create a new policy and set the **Incoming Interface** to **web-proxy**, the **Outgoing Interface** to an internal port (in the example, port 3), and the **Service** to **webproxy**.



Results

Configure web browsers on the private network to connect using a proxy server. The IP address of the HTTP proxy server is 10.10.1.99 (the IP address of the FortiGate internal interface) and the port is 8080 (the default explicit web proxy port). Web browsers configured to use the proxy server are able to connect to the Internet.

Go to **Policy > Policy > Policy** to see the ID of the policy allowing webproxy traffic.

Web proxy traffic is not counted by security policy.