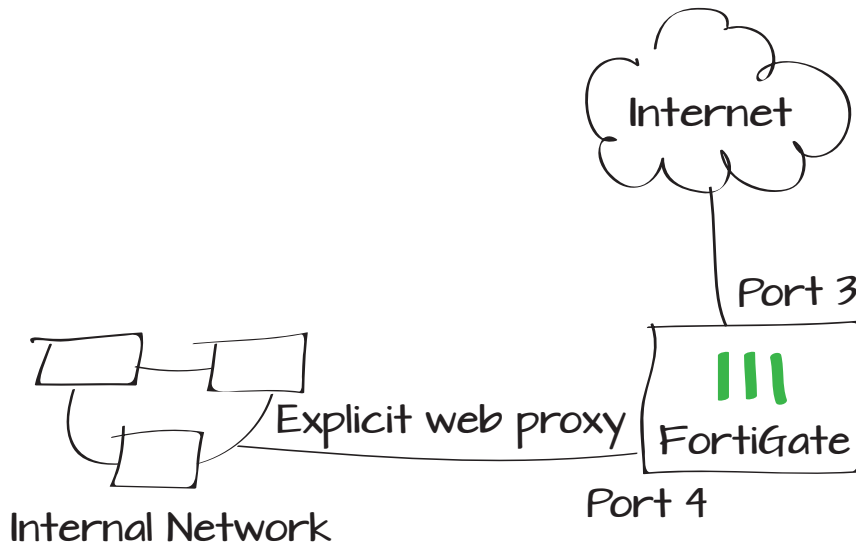


Setting up an explicit proxy for users on a private network

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**.

Name port4 (00:09:0F:4E:0E:C2)
Alias Internal Interface
Link Status Down
Type Physical Interface

Addressing mode Manual DHCP PPPoE One-Arm Sniffer Dedicate to
IP/Network Mask 10.10.1.99/255.255.255.0

Administrative Access HTTPS PING HTTP FMG-Access
 SSH SNMP TELNET FCT-Access

DHCP Server Enable

Address Range

Starting IP	End IP
10.10.1.100	10.10.1.200

Netmask 255.255.255.0

Default Gateway Same as Interface IP Specify

DNS Server Same as System DNS Specify

▶ Advanced...

Security Mode None

Device Management

Detect and Identify Devices

Enable Explicit Web Proxy

Listen for RADIUS Accounting Messages

Secondary IP Address

Comments Write a comment... 0/255

Administrative Status Up Down

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

Basic Features



Advanced Routing ? ON		IPv6 ? ON	
WAN Opt. & Cache ? ON		WiFi Controller ? ON	

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**.

Explicit Web Proxy Options

Enable Explicit Web Proxy	<input checked="" type="checkbox"/> HTTP / HTTPS	<input type="checkbox"/> FTP	<input type="checkbox"/> PAC
Listen on Interfaces	port4 		
HTTP Port	<input type="text" value="8080"/>		
HTTPS Port	<input type="text" value="0"/>	(0 to use HTTP port)	
FTP Port	<input type="text" value="0"/>	(0 to use HTTP port)	
PAC Port	<input type="text" value="0"/>	(0 to use HTTP port)	
PAC File Content			
Proxy FQDN	<input type="text" value="default.fqdn"/>		
Max HTTP request length	<input type="text" value="4"/>		Kb
Max HTTP message length	<input type="text" value="32"/>		Kb
Unknown HTTP version	<input type="text" value="Best Effort"/> ▼		
Realm	<input type="text" value="default"/>		
Default Firewall Policy Action	<input type="radio"/> Accept <input checked="" type="radio"/> 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.

Policy Type Firewall VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Logging Options

No Log

Log Security Events

Log all Sessions

Web Proxy Forwarding Server

Security Profiles

AntiVirus

Web Filter

Application Control

IPS

DLP Sensor

SSL/SSH Inspection

Create New Edit Delete Section View Global View

Seq.#	ID	Source	Destination	Service	Action	Log	Count
▶ port4 (Internal Interface) - port3 (External Interface) (1 - 2)							
▼ web-proxy - port3 (External Interface) (3 - 3)							
3	3	LAN	all	webproxy	ACCEPT		0 Packets / 0 B
▶ Implicit (4 - 4)							