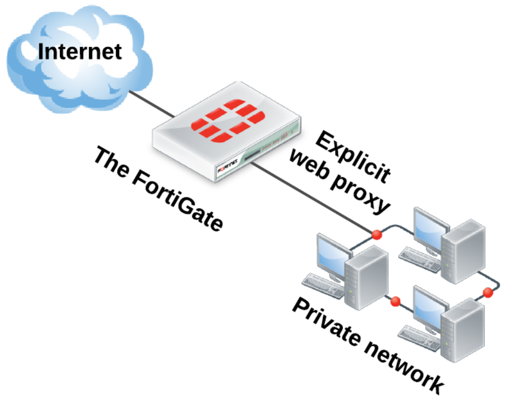
Explicit Web Proxy

FortiOS explicit web proxy provides HTTP and HTTPS proxying with the added benefits of UTM security, SOCKS, IPv6 support, and chaining to other proxy services.

The FortiGate explicit web proxy feature enables explicit HTTP and HTTPS, FTP over HTTP, or SOCKS proxying of IPv4 and IPV6 traffic on one or more FortiGate interfaces. To access web services, users on a network must configure their web browser to use the explicit proxy and set the proxy server address to the IP address of the FortiGate interface that has explicit proxy enabled.

The explicit web proxy receives web browser sessions to be proxied and forwards them through the FortiGate unit to a destination interface. Before a session leaves, the explicit web proxy changes the source address of the session packets to the IP address of the exiting interface. In Transparent mode, the explicit web proxy changes the source address to the management IP address.

You can use web proxy security policies to control access to the proxy and implement security features such as UTM, authentication, and web caching. UTM features include advanced threat protection, application control, and sandboxing. The explicit web proxy provides IPv6 support, with the ability to mask multiple IPv6 addresses as a single address.

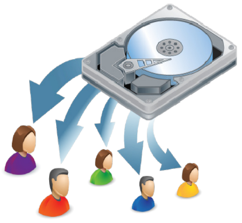


You can also configure a FortiGate as:
- an explicit FTP proxy server
- a reverse explicit FTP proxy server

Proxy Automatic Configuration (PAC)

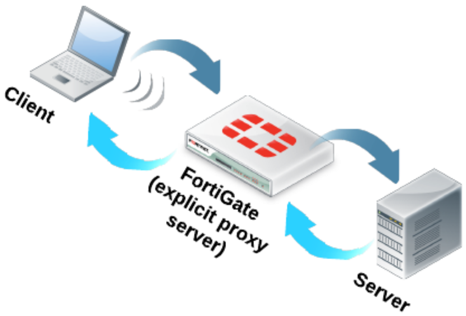
It's easy to add users to your explicit proxy network by deploying Proxy Automatic Configuration (PAC). The PAC file defines how the web browsers choose the appropriate proxy server for receiving a given URL, and includes specifications on how to use a particular proxy or to connect directly. Once the PAC file is stored on the FortiGate unit, you can automate the web proxy configuration by having users enter the PAC URL address provided by a Network Administrator into their web browser's proxy settings.

Web caching



Explicit web proxy users can accelerate web browsing performance with web caching. The explicit web proxy cache stores copies of all recently displayed web pages on a hard disk, and subsequent requests for the same content will be directed to the local copy. Web caching can be added to any security policy or any HTTP or HTTPS traffic accepted by that security policy. A typical topology—with web caching enabled on a FortiGate between users and web servers—will optimize performance on your wide area network.

SOCKS sessions



Socket Secure, or SOCKS, is an Internet protocol that allows an external server to communicate with an explicit proxy server as if it were the actual client. SOCKS is fully supported when enabled by the CLI. Explicit web proxy supports SOCKS sessions from a web browser, but only supports SOCKS versions 4 and 5.

Proxy chaining

Explicit web proxy performs proxy chaining by redirecting web proxy sessions to other proxy forwarding servers. You can use proxy chaining to integrate the explicit proxy seamlessly with other proxies already used by your organization.

You can deploy proxy chaining in an enterprise environment with small satellite offices and a main office. If each office has a web proxy server, users at each of the satellite offices can use their local server as an explicit web proxy server. Any type of proxy server at the satellite office can forward web proxy sessions and integrate with the FortiGate explicit web proxy server at the central office. The sessions can then easily connect to web servers on the Internet.

Load balancing and health checking

FortiGate units monitor web proxy forwarding servers by forwarding a connection to the remote server every 10 seconds. If the remote server does not respond, it is considered down until it does respond. When a server in a load balance group goes down, the server alerts administrators and can also send SNMP traps. Health checking also detects when the unresponsive server becomes healthy again. Health checking can be set up for each remote server, and you can also specify different websites to check for each server.

Explicit web proxy performs traffic load balancing with multiple forwarding servers in a forwarding server group. Server load balancing also checks HTTP redirects and allows you to set the maximum number of redirects.

Unified Threat Management (UTM)

With security policies it's easy to control explicit web proxy traffic and apply security features, such as Unified Threat Management (UTM), access authentication, and traffic logging.

You can apply the following UTM security features to your explicit web proxy traffic:

- Antivirus scanning
- Web filtering
- Intrusion Prevention (IPS)
- Application control
- Data Leak Prevention (DLP)

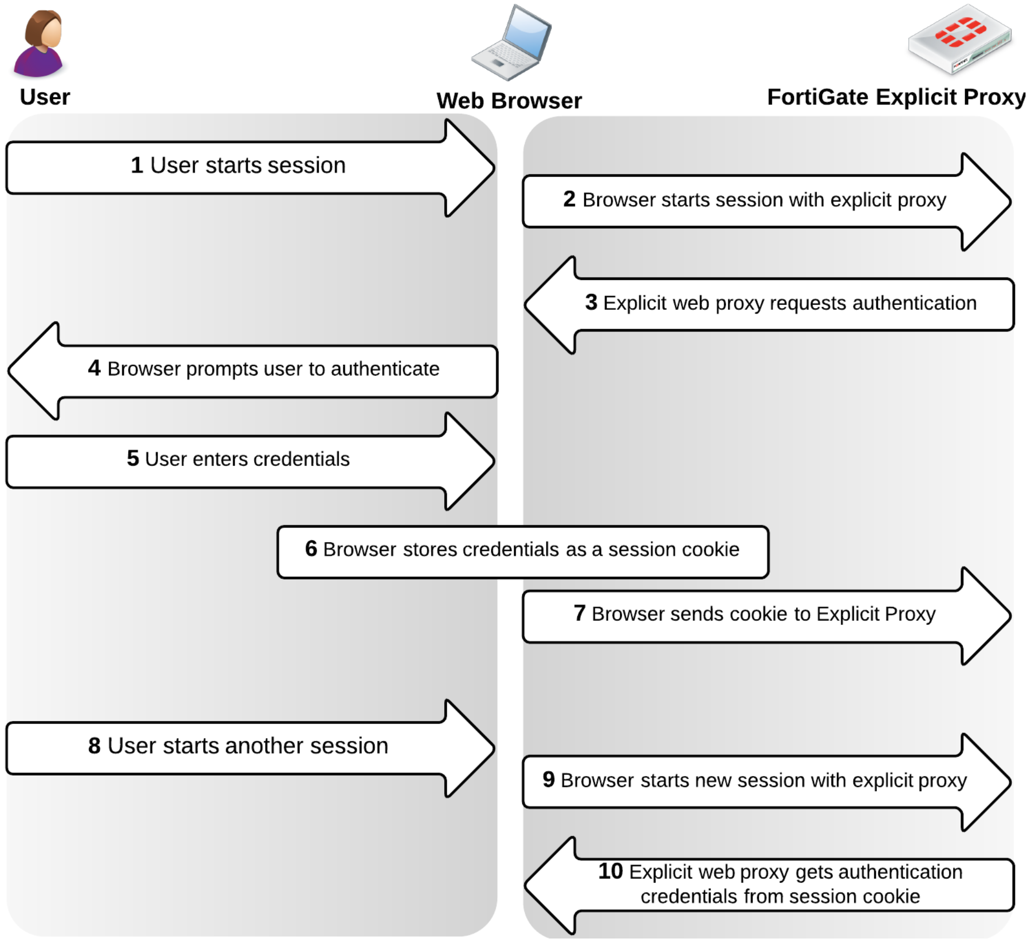
Integrating with FortiSandbox

FortiSandbox is an Advanced Threat Protection Appliance that identifies highly targeted and tailored attacks that increasingly bypass traditional defenses and lurk within networks. FortiGuard sandboxing can examine web proxy traffic activity and provide coverage. FortiSandbox also provides pre-filter to reduce load and latency, rich threat intelligence, and optional intelligence sharing.

User authentication

You can use authentication to control access to the explicit web proxy, to identify users, and to apply a variety of UTM features to different users. Two modes are available:

Session-based authentication of web proxy sessions uses HTTP basic and digest-based authentication. Digest-based authentication, as described in RFC 2617, prompts the user for credentials from the browser, allowing individual users to be identified by their web browser instead of IP address. HTTP authentication, as shown below, allows the FortiGate unit to identify multiple users accessing services from a shared IP address.


User
Web Browser
FortiGate Explicit Proxy
1 User starts session
2 Browser starts session with explicit proxy
3 Explicit web proxy requests authentication
4 Browser prompts user to authenticate
5 User enters credentials
6 Browser stores credentials as a session cookie
7 Browser sends cookie to Explicit Proxy
8 User starts another session
9 Browser starts new session with explicit proxy
10 Explicit web proxy gets authentication credentials from session cookie

IP-based authentication applies authentication by source IP address and is compatible with basic, digest, NTLM, form, or FSSO authentication methods. Once a user authenticates, all sessions to the explicit web proxy from that IP address are assumed to be from that user and are accepted until the authentication timeout ends or the session times out.

Summary of explicit web proxy features and benefits

- **Proxy Automatic Configuration (PAC)** allows you to easily configure user's proxy browser settings automatically.
- **Web Caching** accelerates your browsing speed and reduce your overall internet bandwidth usage.
- **SOCKS** uses an encrypted channel to facilitate communication between youweb server and web browser.
- **Proxy chaining** redirects web proxy sessions to other proxy forwarding servers in your infrastructure, and provides seamless integration with your existing proxy forwarding servers.
- **Load balancing and health checking** optimize responsive traffic distribution and application availability.
- **FortiSandbox** identifies targeted and tailored attacks, monitors web proxy traffic, and provides pre-filter.
- **Unified Threat Management (UTM)** applies advanced security features to your web traffic for safe browsing
- **User authentication** controls access, identifies users, and applies your choice of UTM features.