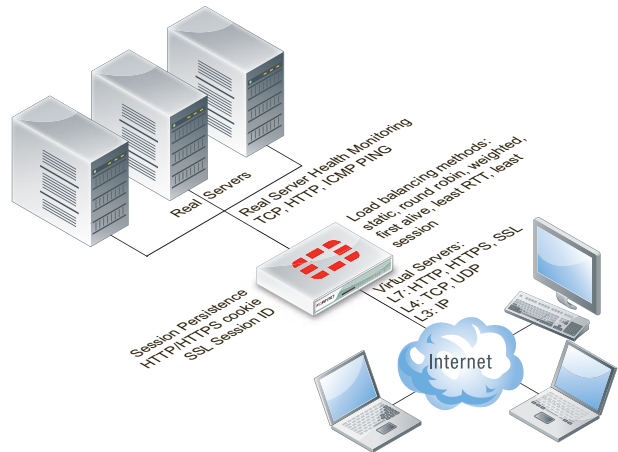


# Load Balancing

FortiOS combines sophisticated load balancing and session persistence capabilities together with SSL Offload to create a high performance and feature-rich load balancing solution

## Load Balancing combined with Unified Threat Management

By introducing comprehensive load balancing functionality to our UTM solution Fortinet have taken UTM protection to a whole new level (and place in the network). Fortinet are the industry pioneers of security consolidation; combining multiple security functions such as firewall, flow-based and proxy-based application control, antivirus, intrusion prevention, web filtering and DLP into a single appliance. By introducing comprehensive load balancing functionality, Fortinet have taken consolidation to a whole new level. Rather than go to the expense of deploying multiple, point solutions to protect your server farm such as firewall, IPS, load balancing etc which all sit in the same place in the network, a FortiGate unit can consolidate all these functions onto a single appliance or cluster. Although a major factor, the benefit of consolidation is not only limited to cost. Consolidating multiple security functions onto a single appliance can result in:



- Increased Resilience** A consolidated solution results in significantly simplified network architecture. High availability can be provided for all technologies with just a pair of devices rather than several.
- Reduced Operational Overheads** A unified GUI, logging and reporting will significantly reduce the resources required to manage the multiple technology areas. A consolidated solution provides a single point of contact for support and renewals rather than having to deal with multiple vendors.

## Load balancing feature set

The FortiOS load balancing feature set contains all of the features you would expect of a server load balancing solution. Traffic can be balanced across multiple backend servers based on multiple methods including static (failover), round robin, weighted to account for different sized servers, or based on the health and performance of the server including round trip time and number of connections. The load balancer supports HTTP/S, SSL or generic TCP/UDP or IP protocols. Session persistence is supported based on the SSL session ID, based on an injected HTTP cookie, or based on the HTTP host. Load balancing is supported on FortiGate devices from the FG50B upwards and supports 10,000 virtual servers on the high end systems.

Extensions	<b>SSL Offload</b>	<b>Network Security</b> (Firewall, flow and proxy-based AV, IPS, DLP, App Control)
Virtual Server	<b>Persistence</b> (cookie, SSL session id, host)	<b>Service Type</b> (L7 HTTP, L7 HTTPS, L7 SSL, L4 TCP, L4 UDP, L3 IP)
	<b>Load Balancing Methods</b> (static, round robin, weighted, first alive, least RTT, least session, HTTP host)	
Real Server	<b>Monitors</b> (TCP, HTTP, ICMP PING)	

## SSL offload

With more and more critical business applications being made available online, the demand for secure remote web based access has increased. Whilst securing web applications with SSL is essential, it does bring with it significant performance overheads. An SSL protected application running on a standard server will perform all the costly encryption/decryption and key exchange routines in software which uses vital CPU resources which could be used for running the application. The consequence of this is that many more or more powerful servers are required to deliver the application. The FortiGate technology however was designed with the explosion of SSL applications in mind. The key exchange and encryption/decryption tasks can be offloaded to the FortiGate which processes them in custom ASIC providing significantly more performance than a standard server could handle. This frees up valuable resources on the server farm which can be used to run a more responsive business.

## SSL content inspection

Traditionally, SSL encrypted application data would be invisible any border gateway filtering solution. This is because the encryption process prevents the payload of any connection from being seen other than by the communicating systems. The FortiGate SSL Offload feature allows the application payload to be inspected before it reaches your servers; preventing intrusion attempts, blocking viruses and preventing data leakage.

## Health Check

Health checking can be enabled to prevent load balancing traffic to a non-functioning real server. This can be based on a basic ICMP ping (is the server responding, tests OS functionality), TCP test (is the application listening on the specified port). The most comprehensive test is HTTP which tests the HTTP application is responding and that it is returning the correct content. This can be used to remove servers from the load balancing cluster which are returning invalid content. The removal of real servers from the clusters is based on the Interval, Timeout and Retry Settings:

<b>Interval</b>	How often to test the server.
<b>Timeout</b>	What maximum response time is permissible before a server is treated as non-functional.
<b>Retry</b>	How many failures before the server is considered "dead" and removed from the cluster.

## Server Monitoring and Management

The health and performance of the real servers can be monitored from the GUI. Virtual servers and their assigned real servers can be monitored for health status (are they active in the load balancing cluster), if there have been any monitor events (has the device exceeded the bounds of the health check), number of active sessions, round trip time and number of bytes processed. Should a server become problematic and require administration, it can be gracefully removed from the Virtual Server pool to enable disruption free maintenance. When a removed real server is able to operate it can gracefully be added back to the virtual server.

## HTTP Multiplexing

A performance saving feature of HTTP/1.1 compliant web servers is the ability to pipeline requests on the same connection. This allows a single HTTPD process on the server to interleave and server multiple requests. HTTP multiplexing reduces the number idle sessions, too many of which can exhaust the resources on a server. The Fortinet solution has the ability to take multiple separate inbound sessions and multiplex them over the same internal session. This reduces the load on the backend server and increases the overall performance.