FortiBalancer™ 8.4.0.34

Release Notes

for 400, 1000, and 2000 models

FortiBalancer™ 8.4.0.34 Release Notes

March 5, 2014

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training Services	http://training.fortinet.com
FortiGuard	http://www.fortiguard.com
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiBalancer™ 8.4.0.34.

For additional documentation, please visit:

http://help.fortinet.com/fbl.html

What's new

Before upgrading, review the following changes for impact to your unique network.

For more information on features and commands, please refer to the FortiBalancer 8.4 User Guide and CLI Handbook.

Adding logs and friendly prompts for license expiration

When the license is going to expire in 15 days, the system notifies you of the remaining valid days of the license in the following four ways:

- Generate a warning-level log every day
- Generate an SNMP trap notification every day
- Display a warning message on the web UI
- Display a warning message when the administrator executes the command `show version`

After the license is expired, the system also uses the preceding four ways to instruct the customer to purchase a new license. Until a new valid license is loaded, the administrator cannot execute most commands in the "config" mode.

Individual session control

The FortiBalancer SLB module introduces a new, generally applied, and session ID-based method for achieving individual session persistence. The persistence method can either operate independently on Layer 4/7 SLB or work in collaboration with existing Layer 7 SLB persistence policies, including header, persistence cookie, persistence URL, and QoS body (newly added).

In the collaborative operation case, the policy extracts the session ID and the persistence method uses the session ID to implement session persistence.

As for the independent operating case, the persistence method maintains a mapping table to keep track of each session ID and its associated real server. The persistence method also dynamically processes the timeout information of each session ID to control each session independently.

New CLI commands

To support this new feature, the following commands have been added:

```
slb group method <group_name> persistence <session_id_type> [rr|sr|lc]
[threshold]
```

```
slb group persistence request header <group_name> <header_name>
[prefix] [delimiter] [flag]
```

```
slb group persistence request urlquery <group_name> <query_name>
```

```
slb group persistence request cookie <group_name> <cookie_name>
```

```
slb group persistence request body <group_name> <prefix> <delimiter>
[flag]

slb group persistence response header <group_name> <header_name>
[prefix] [delimiter] [flag]

slb group persistence response cookie <group_name> <cookie_name>

slb group persistence response body <group_name> <prefix> <delimiter>
[flag]

slb group persistence value <group_name> <offset> [session_id_length]

slb group persistence session static <group_name> <static_session_id>
<real_name> [port]

slb policy qos body <policy_name> {virtual_name|vlink_name}
{group_name|vlink_name} <prefix> <delimiter> <flag> <precedence>
```

Modified CLI commands

To support this new feature, the following command has been modified:

```
slb persistence timeout <timeout_minutes> [group_name] [idle|duration]
```

ePolicy

ePolicy is a Tools Command Language (TCL) and script-based function for extending the functions of the FortiBalancer appliance. It allows administrators to customize new features for the FortiBalancer appliance in addition to the existing functions to route, direct, rewrite, and block traffic.

The elements of ePolicy include the event, command, and command invocation rule. By functions, the scripts of ePolicy can be classified into the setting script and runtime script.

ePolicy does not support HTTP pipelining. It is only applicable to virtual services of the HTTP type.

New CLI commands

To support this new feature, the following commands have been added:

```
epolicy import setting <url> <script_name>

epolicy import script <url> <script_name>

epolicy attach setting <vs_name> <script_name>

epolicy attach script <vs_name> <script_name>

no epolicy attach setting <vs_name>

no epolicy attach script <vs_name> <script_name>

epolicy delete setting {script_name|all}

epolicy delete script {script_name|all}
```

Role-based administration control (RBAC)

To achieve the granular and flexible control over the administrators' privilege on the system, the FortiBalancer appliance has introduced the role based administration control function.

This function assigns administrators with privileges on the system by applying certain roles to them. A role defines a group of privileges on executing the system CLI commands.

If the operation privilege of a role is `permit`, the role permits the administrators to execute the CLI commands that match the `filter_string` of this role. Conversely, if the operation privilege of a role is "deny", the role disallows the administrators to execute the matched CLI commands.

One administrator can be assigned one or more roles, and the logic among the multiple roles is "OR". If any role assigned to an administrator permits the execution of a command, the administrator can execute this command; if all roles assigned to an administrator deny (or none of the roles permits) the execution of a command, the administrator cannot execute this command. If an administrator is not assigned any role, the administrator is allowed to execute all the commands of the access control level.

Monitoring the web UI requires the privilege for executing the `show` CLI commands. Please make sure the administrators who need to monitor a specific feature on the web UI are assigned the role with the correspondent `show` privileges.

New CLI commands

To support this new function, the following commands have been added:

```
role name <role_name>
role permit <role_name> <filter_string>
role deny <role_name> <filter_string>
role clone <old_role_name> <new_role_name>
role test cli <role_name> <cli_command>
role user <user_name> <role_name>
```

Advanced ACL (SLB QoS)

To prevent network resources from being consumed by unwanted client requests and to ensure the user experience of the trustworthy clients, the Advanced ACL feature is now available.

This function allows the administrators to define ACL rules to restrict the connections per second (CPS) and concurrent connections (CC) utilizable for the clients on a specified subnet. If clients on the specified subnet have used up the connections utilizable for them, their accesses will be denied.

This function can ensure the access of trustworthy clients in a static or dynamic way.

- The static way is to add the trustworthy clients into an ACL whitelist. Clients on whitelists are free from any restriction when accessing the FortiBalancer appliance.
- The dynamic way is to identify the clients that have carried cookies inserted by the FortiBalancer appliance. When accessing the HTTP or HTTPS virtual services for which the

insert cookie policy has been used, the clients that carry cookies inserted by the FortiBalancer appliance in the requests will be free from the restriction of any ACL rule.

ACL rules and ACL whitelists can take effect only after they are applied to SLB virtual services. They can be applied to TCP-based virtual services, such as TCP, TCPS, HTTP, and HTTPS virtual services.

New CLI commands

To support this new function, the following commands have been added:

```
acl rule <rule_name> <client_ip> {netmask|prefix} <acl_mode>
<acl_type> <max_limit>
```

```
acl whitelist <whitelist_name> <client_ip> {netmask|prefix}
```

```
acl apply rule virtual <rule_name> <vs_name>
```

```
acl apply whitelist virtual <whitelist_name> <vs_name>
```

Comprehensive IPv6 support

As of FortiBalancer 8.4.0.1, the appliance provides a more comprehensive support for the IPv6 stack. The following sections describe the IPv6 support in detail.

IPv6 support for SLB

As of FortiBalancer 8.4.0.1, the SLB module provides IPv6 support for all types of SLB protocols (except RDP and SIP), all SLB methods (except SNMP), all SLB policies, and all types of health check.

Table 1: IPv6 support for the SLB sub-modules

Sub-modules	IPv6 supported
Real Service & Virtual Service	IP L2IP RTSP DNS UDP Portrange RADIUS FTP/FTPS TCP/TCPS HTTP/HTTPS Packet-based UDP
Method	All SLB methods except SNMP
Policy	All SLB policies

Health Check	All health check

Furthermore, the following enhancements have been made:

- Besides the reverse mode and transparent mode, “IPv6 to IPv6” deployment method now can be used in the triangle mode.
- Besides the “IPv4 to IPv4” method, the DirectFWD function now can work with the “IPv6 to IPv6”, “IPv4 to IPv6”, and “IPv6 to IPv4” deployment methods. This function takes effect for the “IPv4 to IPv4” and “IPv6 to IPv6” NAT.

New CLI commands

To support this new function, the following commands have been added:

```
slb virtual l2ip <virtual_name> <vip> [gateway_ip]

slb real l2ip <real_name> <real_ip>

slb real ip <real_name> <ip> [max_conn] [icmp|none] [hc_up] [hc_down]
[udp_timeout]

slb real rtsp <real_name> <ip> [port] [max_conn] [rtsp-
tcp|tcp|icmp|script-tcp|script-udp|dns|none] [hc_up] [hc_down]
[timeout]

slb real dns <real_name> <ip> <port> [max_conn] [dns|icmp|script-
tcp|script-udp|sip-tcp|sip-udp|dns|none] [hc_up] [hc_down] [timeout]

slb real udp <real_name> <ip> <port> [max_conn] [hc_up] [hc_down]
[timeout] [icmp|script-tcp|script-udp|radius-auth|radius-acct|sip-
tcp|sip-udp|dns|none]

fwd tcp <local_ip> <local_port> <remote_ip> <remote_port> [timeout]

fwd udp <local_ip> <local_port> <remote_ip> <remote_port> [timeout]
```

IPv6 support for LLB

FortiBalancer 8.4.0.1 added comprehensive IPv6 support for the LLB module. The following table shows the IPv6 support for the LLB sub-modules.

Table 2: IPv6 support for the LLB sub-modules

Sub-modules	IPv6 supported
Route	Eroute LLB link route RTS route IPflow route IP region Link bandwidth limit
Method	RR WRR SR

	DD HI
DNS Host	IPv6 host Handling AAAA queries
Health Check	ICMPv6 DNS TCP

In the outbound direction, only route-based LLB support IPv6 configurations, while NAT-based LLB does not support IPv6 configurations.

IPv6 support for GSLB

As of FortiBalancer 8.4.0.1, the GSLB module can create the mapping between hostnames and IP addresses through the A and AAAA records. Therefore, the hostnames in DNS queries not only from IPv4 clients but also from IPv6 clients can be resolved to IPv4 or IPv6 addresses.

IPv6 support limitations for the GSLB module are as follows:

- For DNS AAAA queries, the GSLB module supports only the RR method and does not support health check.
- SDNS proximity rules do not support IPv6.
- The GSLB module cannot use the IPv6 region table.

The AAAA records on the GSLB module are configured by using the command `sdns ipv6` or `sdns pool ipv6` instead of the command `llb dns host`.

IPv6 support for NAT

As of FortiBalancer 8.4.0.1, the appliance provides complete IPv6 support for IPv4 to IPv4 NAT and IPv6 to IPv6 NAT.

Besides, NAT static, port forwarding, and NAT pool configurations all support IPv6.

Since NAT64 and NAT46 are now supported, the IPv6 NATPT function is obsolete and therefore is removed in this release.

IPv6 support for Webwall

Webwall now supports filtering the TCP, UDP and ICMP packets that are using the IPv4 or IPv6 addresses.

To support this enhancement, parameters in the following commands that are shown in **bold** now support both IPv4 and IPv6:

```
accesslist deny ah|esp <source_ip> <source_mask|source_prefix>
<destination_ip> <destination_mask|destination_prefix> <accesslist_id>

accesslist deny icmp echoreply|echorequest <source_ip>
<source_mask|source_prefix> <destination_ip>
<destination_mask|destination_prefix> <accesslist_id>

accesslist deny tcp |udp <source_ip> <source_mask|source_prefix>
<source_port> <destination_ip> <destination_mask|destination_prefix>
<destination_port> <accesslist_id>

accesslist permit ah|esp <source_ip> <source_mask|source_prefix>
<destination_ip> <destination_mask|destination_prefix> <accesslist_id>

accesslist permit icmp echoreply|echorequest <source_ip>
<source_mask|source_prefix> <destination_ip>
<destination_mask|destination_prefix> <accesslist_id>

accesslist permit tcp|udp <source_ip> <source_mask|source_prefix>
<source_port> <destination_ip> <destination_mask|destination_prefix>
<destination_port> <accesslist_id>
```

IPv6 support for clustering

VIPs of IPv6 type now can be switched between clustered units. Units can use the IPv6 links to send IPv6 VRRP advertisement packets to communicate the status information with each other.

To support this enhancement, the parameters in the following commands shown in bold now support both IPv4 and IPv6:

```
cluster virtual ifname <interface_name> <cluster_id>

synconfig peer <peer_name> <peer_ip>

synconfig sdns peer <peer_name> <peer_ip>
```

IPv6 support for HA

VIPs of IPv6 type now can be switched between units on which the corresponding floating IP group is enabled. Units can use the IPv6 links between each two units to directly communicate the health status, group status, and other information or synchronize configurations with each other. HA supports IPv6 gateways and health check on IPv6 gateways.

IPv6 support for general system & tools

As of FortiBalancer 8.4.0.1, the appliance provides IPv6 support for the following functions and tools:

- AAA server
- Log server
- NTP server
- SSH access control
- SNMP
- IPv6 statistics
- Synconfig via IPv6 link
- NDP management

- Static DNS cache entry
- NS lookup

Log Server

To set the remote log server, the `<host_ip>` parameter in the following command now supports both IPv4 and IPv6:

```
log host <host_ip> [port] [udp|tcp] [host_id]
```

NTP server

The `<ip>` parameter in the following command now supports both IPv4 and IPv6:

```
ntp server <ip> [version]
```

SSH access control

The `<ip_address>` and `<netmask|prefix>` parameters in the following command now support both IPv4 and IPv6:

```
support <ip_address> <netmask|prefix>
```

SNMP

The `<host_ip>`, `<source_ip>`, and `<netmask|prefix>` parameters in the following commands now support both IPv4 and IPv6:

```
snmp host <host_ip> [1|2|3] [user_name|community_name] [engine_id]
[auth_password] [authNopriv|authPriv] [priv_password]
```

```
snmp ippermit <source_ip> <netmask|prefix>
```

NDP

To support IPv6 NDP management, the following command has been added. It adds a static NDP entry to the system:

```
ipv6 ndp <ipv6_address> <mac_address>
```

Static DNS cache entry

The `<ip>` parameter in the following command now supports both IPv4 and IPv6:

```
dns cache host <host_name> <ip>
```

NS lookup

The `{ip|hostname}` parameter in the following command now supports both IPv4 and IPv6:

```
nslookup {ip|hostname}
```

To implement the IPv6 support for SNMP, some OIDs are also changed.

IPv6 support is not currently available for the QoS feature.

“IPv4 to IPv6” transition technologies

As IPv4 address space is becoming depleted, the “IPv4 to IPv6” transition is inevitable. However, the transition will take some time, and during this period, networks must support both IPv4 and IPv6 addressing. In this regards, Fortinet introduces the DNS64, NAT64, DNS46 and NAT46 transition technologies in addition to IPv4/IPv6 dual stack for traffic to flow between the IPv4 and IPv6 infrastructures smoothly.

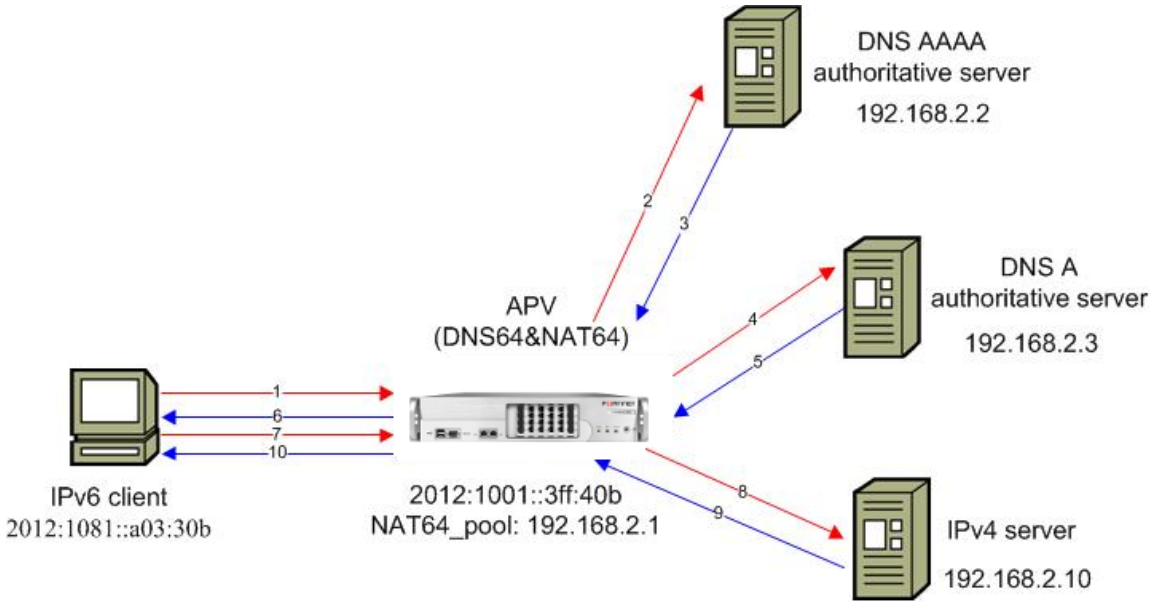
The DNS64 and NAT64 functions work together to allow emerging IPv6 clients to access existing IPv4 services. While, the DNS46 and NAT46 functions work together to allow existing IPv4 clients to access emerging IPv6 services.

The following sections describe these functions in detail.

DNS64 and NAT64

The DNS64 function converts the DNS AAAA queries sent from IPv6 clients to DNS A queries and then converts the DNS A responses to DNS AAAA responses. This ensures that IPv6 clients can access IPv4 servers. FortiBalancer returns the translated IPv6 addresses to IPv6 clients. When IPv6 clients use these IP addresses to access IPv6 servers, the NAT64 (Network Address Translation IPv6 to IPv4) function converts the IPv6 packets sent from these clients to IPv4 packets. When the FortiBalancer appliance receives IPv4 packets from IPv4 servers, the NAT64 function converts IPv4 packets to IPv6 packets. This ensures that IPv6 clients can communicate with IPv4 servers normally. The DNS64 and NAT64 functions can be deployed on two FortiBalancer appliances separately, or deployed on one FortiBalancer appliance.

The DNS64 and NAT64 functions are applicable to the “IPv6 to IPv4” scenario, as shown in the following figure.



Application notes

The DNS64 function can be enabled on only one DNS virtual service. This virtual service, acting as the DNS proxy, converts DNS AAAA queries to DNS A queries and then converts DNS A responses to DNS AAAA responses.

To make the DNS64 function work properly, you need to configure the “default” and “backup” policies for this virtual service. The FortiBalancer appliance forwards DNS AAAA queries based

on the “default” policy and forwards DNS A queries based on the “backup” policy. Therefore, the real servers associated with the “default” policy should be DNS servers that can answer AAAA records, and those associated with the “backup” policy should be DNS servers that can answer A records.

New CLI commands

To support the DNS64 and NAT64 functions, the following commands have been added:

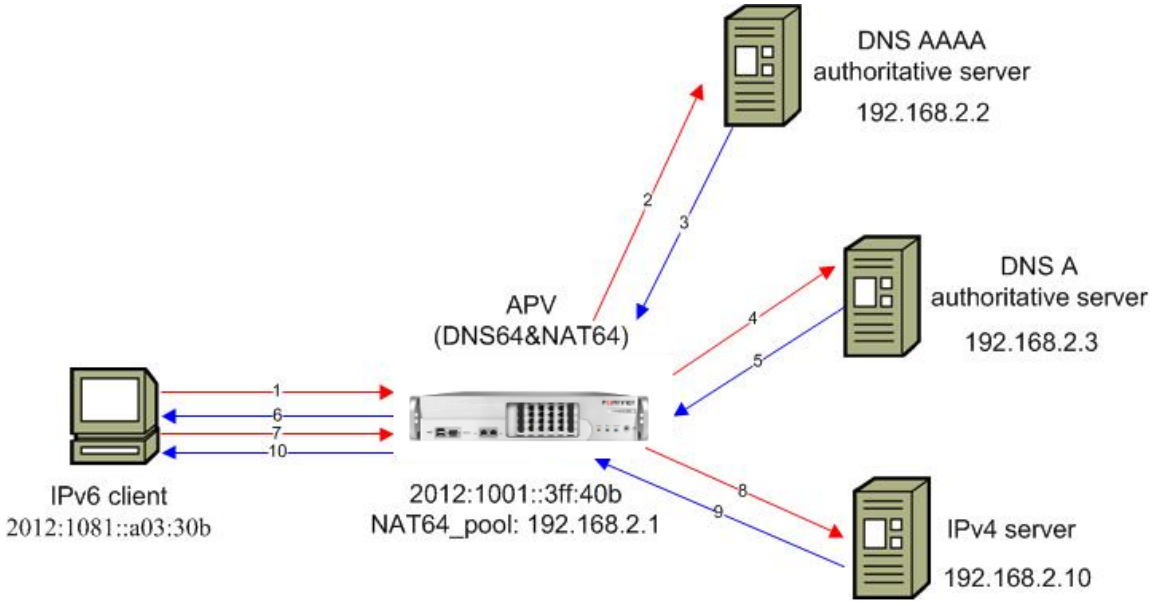
```
ipv6 dns64 on <dns_vs_name>
ipv6 dns64 prefix <dns64_prefix>
ipv6 nat64 on
ipv6 nat64 ippool <ipv4_pool_name>
ipv6 nat64 prefix <nat64_prefix>
ipv6 nat64 timeout <idle_timeout>
```

DNS46 and NAT46

To allow IPv4 clients to access IPv6 services smoothly, the DNS46 and NAT46 functions are introduced.

The DNS46 function converts the DNS A queries sent from IPv4 clients to DNS AAAA queries and then converts the DNS AAAA responses to DNS A responses. It also creates mapping records between the IPv6 addresses and IPv4 addresses. The FortiBalancer appliance returns the translated IPv4 addresses to IPv4 clients. When IPv4 clients use these IPv4 addresses to access IPv6 servers, the NAT46 function converts IPv4 packets sent from clients to IPv6 packets based the created mapping records. When the FortiBalancer appliance receives IPv6 packets from IPv6 servers, the NAT46 function converts IPv6 packets to IPv4 packets. This ensures that IPv4 clients can communicate with IPv6 servers normally. Because the DNS46 and NAT46 functions both use the mapping records, they must be deployed on one FortiBalancer appliance.

The DNS46 and NAT46 functions are applicable to the “IPv4 to IPv6” scenario, as shown in the following figure.



Application notes

The DNS46 and NAT46 functions can be enabled on only one DNS virtual service. This virtual service, acting as the DNS proxy, converts DNS A queries to DNS AAAA queries and then converts DNS AAAA responses to DNS A responses.

To make the DNS46 and NAT46 functions work properly, you need to configure the “default” and “backup” policies for this virtual service. The FortiBalancer appliance forwards DNS A queries based on the “default” policy and forwards DNS AAAA queries based on the “backup” policy. Therefore, the real servers associated with the “default” policy should be DNS servers that can answer A records, and those associated with the “backup” policy should be DNS servers that can answer AAAA records.

New CLI commands

To support the DNS46 and NAT46 functions, the following commands have been added:

```
ipv6 dnsnat46 on <dns_vs_name>
ipv6 dnsnat46 ipmap <ipv4_address> <netmask> [timeout]
ipv6 dnsnat46 ippool <ipv6_pool_name>
ipv6 dnsnat46 timeout <idle_timeout>
```

HA Phase II

In FortiBalancer 8.4.0.1, high availability (HA) changed fundamentally. After upgrading to this version, HA reconfiguration is strongly recommended.

FortiBalancer 8.4.0.1 introduced several important HA function enhancements, which are developed to make HA work more stable, allow wider deployment of HA, and further improve service reliability and continuity provided by the FortiBalancer appliance.

The following sections describe these enhancements in detail.

Fundamental architecture extension (N+1)

In HA phase I, HA only supports the 1+1 (Active/Standby and Active/Standby) deployment mode. In HA phase II, HA can be deployed on a maximum of 32 FortiBalancer appliances to ensure the reliability and continuity of application services. The typical deployment scenario “N+1” is now supported. To support this enhancement, the HA introduces the concept “unit” to identify each FortiBalancer appliance in the entire HA domain. Units in the HA domain exchange their running status including health status and group status with each other through reliable communication links.

Now, the primary link no longer needs to be configured. Instead, it is automatically established by using the unit’s communication IP address as the link’s IP address after the two units join the HA domain.

When HA is deployed on more than 2 FortiBalancer appliances, the SSF function and FFO link are not supported.

Enriched health check conditions

The failover of floating IP groups relies on the groups' health status. In HA phase II, the health check conditions supported by HA have been enriched. Besides the predefined condition "PORT_DOWN" and the gateway health check condition, HA also supports the following types of health check conditions:

Hardware

- CPU overheat health check condition
- SSL card health check condition

Software

- CPU utilization health check condition
- Zone memory utilization health check condition
- Memory pool utilization health check condition
- System memory health check condition
- Network packet memory health check condition
- Process health check condition

HA uses these health check conditions as the failover conditions of failover rules, which helps achieve flexible group failover.

Floating MAC

To avoid possible MAC table updates on the upstream routers and speed up the failover, HA introduces the floating MAC function.

With this function enabled, the floating MAC address (configured by using the command `ha floatmac mac`) is switched to the interface of the new appliance on which the group status is "Active" in case of group failover. In this way, the clients will not be aware that the appliance that provides the application services has been changed after the group failover, because the MAC addresses of the appliances that provide application services before and after group failover remain unchanged.

New CLI commands

To support the preceding enhancements, the following commands have been added:

```
ha unit <unit_name> <ip_address> [port]
ha log level <level>
ha floatmac {off|on}
ha floatmac mac <interface_name> <floating_mac> [interface_name]
ha hc cpu overheat <temperature> [interval] [up_check_times]
[down_check_times]
ha hc cpu utilization <fatal_percent> [interval] [up_check_times]
```

```
ha hc memory atcpzone <zone_name> <fatal_percent> <condition_name>
[up_check_times] [down_check_times]

ha hc memory mbuf <fatal_percent> [up_check_times] [down_check_times]

ha hc memory mpool <mpool_name> <fatal_percent> <condition_name>
[up_check_times] [down_check_times]

ha hc memory system [free_space_threshold] [used_swap_threshold]
[up_check_times] [down_check_times]

ha hc memory interval [interval]

ha hc process <process_name> <condition_name>

ha hc sslcard [interval] [up_check_times] [down_check_times]

ha hc vcondition name <vcondition_name> <condition_name> <logic>
```

Modified CLI commands

To support the preceding enhancements, the following commands have been modified:

Before:

```
ha link network secondary <peer_ip> <local_ip>

ha group priority local <group_id> <priority>

ha group priority peer <group_id> <priority>

ha group priority <unit_name> <group_id> <priority>

ha hc localgateway <gateway_ip> <condition_name> [interval]
[check_times]

ha hc peergateway <gateway_ip> <condition_name> [interval]
[check_times]
```

Now:

```
ha link network secondary <unit_name> <link_id> <ip_address> [port]

ha group priority <unit_name> <group_id> <priority>

ha hc gateway <unit_name> <gateway_ip> <condition_name> [interval]
[up_check_times] [down_check_times]
```

where <unit_name> is used to distinguish the local and peer units, which provides ease of configuration and management.

Deleted CLI command

To support the preceding enhancements, the following command has been deleted:

```
ha link network primary <peer_ip> <local_ip>
```

Non-Uniform Memory Access (NUMA)

Non-Uniform Memory Access (NUMA) is a memory design used in multiprocessing environment, where each processor can access its own local memory faster than a non-local memory, that is, memory local to another processor or memory shared between processors.

NUMA support is newly added to fully utilize FortiBalancer multi-processors. The key objective of FortiBalancer NUMA design is to enhance system performance by changing the memory allocation mechanism of the critical data structures.

To take advantage of NUMA's high performance, system configuration needs to be adjusted. The goal is to make all the domains in the system run independently to attain the best performance. For the SLB/LLB deployment with the NUMA feature, please refer to the NUMA deployment guide.

To support this new feature, the following commands have been added:

```
system tune dispatcher numa
system tune dispatcher default
no system tune dispatcher
```

IP address overlap support

When the NUMA SLB (single VIP, reverse mode) is deployed, the subnet of the interface to be added can overlap that of any existing interface.

To support this enhancement, the `overlap` parameter has been added to the following command:

```
ip address {system_ifname|mnet_ifname|vlan_ifname|bond_ifname}
<ip_address> {netmask|prefix} [overlap]
```

Performance enhancements

FortiBalancer performance is now significantly improved. Packet processing capability is greatly enhanced even when NUMA is off. Consequently, the performance of functions including the SLB and LLB is improved to a higher level. In addition, the SSL performance is also significantly enhanced.

Server Load Balance (SLB) enhancements

Connections removed when a real server is deleted

Previously, when a real server was deleted, the connections established with the real server still existed. Now, when a real server is deleted, connections to the real server are removed immediately.

To make this enhancement take effect, the administrator needs to execute the command `slb mode activeclose on` to enable the feature of actively closing Layer 4 TCP connections first.

Support for source or destination IP address-based persistence for Layer 2 SLB services

Previously, session persistence for Layer 2 SLB groups whose method was Hash IP (hi) or Consistent Hash IP (chi) had to be based on both source and destination IP addresses of the incoming packets. Now, the session persistence can be based on either the source IP address, the destination IP address, or both the source and destination IP addresses.

To support this enhancement, the following command is modified:

Before:

```
slb group method <group_name> {hi|rr|chi} [route|direct]
```

Now:

```
slb group method <group_name> {hi|rr|chi} [route|direct] [hash_mode]
```

This command defines a Layer2 SLB group. Layer 2 SLB supports three kinds of group methods: Round Robin (rr), Hash IP (hi) and Consistent Hash IP (chi).

hash_mode

The value can be `src`, `dst` or `default`.

If the value is `src`, the system performs session persistence by hashing the source IP address.

If the value is `dst`, the system performs session persistence by hashing the destination IP address.

If the value is `default`, the system performs session persistence by hashing both the source and destination IP addresses.

Support for UDP health check

The FortiBalancer appliance now supports UDP health check for real services of the UDP, DNS, SIPUDP, RADIUS Authentication, and RADIUS Accounting types.

To support this enhancement, the following commands have been modified:

Before:

```
slb real udp <real_name> <ip> <port> [max_conn] [hc_up] [hc_down]
[timeout] [icmp|script-tcp|script-udp|radius-auth|radius-acct|sip-
tcp|sip-udp|dns|none]
```

```
slb real dns <real_name> <ip> <port> [max_conn] [dns|icmp|script-
tcp|script-udp|sip-tcp|sip-udp|dns|none] [hc_up] [hc_down] [timeout]
```

```
slb real sipudp <real_name> <ip> [port] [max_conn] [icmp|script-
tcp|script-udp|radius-auth|radius-acct|sip-tcp|sip-udp|dns|none]
[hc_up] [hc_down] [timeout]
```

```
slb real radauth <real_name> <ip> [port] [max_conn] [icmp|script-
tcp|script-udp|radius-auth|radius-acct|dns|none] [hc_up] [hc_down]
[timeout]
```

```
slb real radacct <real_name> <ip> [port] [max_conn] [icmp|script-
tcp|script-udp|radius-auth|radius-acct|dns|none] [hc_up] [hc_down]
[timeout]
```

Now:

```
slb real udp <real_name> <ip> <port> [max_conn] [hc_up] [hc_down]
[timeout] [icmp|udp|script-tcp|script-udp|radius-auth|radius-acct|sip-
tcp|sip-udp|dns|none]
```

```
slb real dns <real_name> <ip> <port> [max_conn] [dns|udp|icmp|script-
tcp|script-udp|sip-tcp|sip-udp|dns|none] [hc_up] [hc_down] [timeout]
```

```
slb real sipudp <real_name> <ip> [port] [max_conn] [icmp|udp|script-
tcp|script-udp|radius-auth|radius-acct|sip-tcp|sip-udp|dns|none]
[hc_up] [hc_down] [timeout]
```

```
slb real radauth <real_name> <ip> [port] [max_conn] [icmp|udp|script-
tcp|script-udp|radius-auth|radius-acct|dns|none] [hc_up] [hc_down]
[timeout]
```

```
slb real radacct <real_name> <ip> [port] [max_conn] [icmp|udp|script-
tcp|script-udp|radius-auth|radius-acct|dns|none] [hc_up] [hc_down]
[timeout]
```

Optimized cache specifications

To provide diversified and enhanced cache performance, and facilitate the administrator to debug the system, the cache specifications are optimized as follows:

Table 3: Number of cache objects before and now

System memory	Number of cache objects	
	Before	Now
2G/4G Lite	64K	32K
4G		64K
8G		128K
16G		256K
24G		384K
32G		512K
64G		1M

The following items are added to the Advanced Statistics field in the output of the command `show statistics cache`:

Item	Description
Max cache objects	Maximum number of cache objects
Max cache frames	Maximum number of network buffers used by cache
Times of cache drain	Counts of cache exhaustion

The following notice-level logs have been added:

Log	Description
cache mbufs over limit	Generated when the number of network buffers used by cache exceeds the limit
cache objects	Generated when the number of

over limit	cache objects exceeds the limit

HTTP request content returned as text to avoid security risks

When an HTTP request parsing error occurs, the FortiBalancer appliance converts the request content into plain text and then returns the HTTP request to the client. In this way, even if the HTTP request contains executable content such as a script, the content is not executed on the client, which avoids security risks at the client.

HTTP error redirects

The HTTP error redirect function now enables the FortiBalancer appliance to redirect the clients' request for accessing a virtual service to a specified URL address when a specified error code is generated.

Furthermore, this function allows the FortiBalancer appliance to control whether to display the original URL in the new URL address, with a prefix separating the original URL address and the redirect URL address. For example, the new URL address can be in the format of "redirect_url?prefix=original_url". To ensure the security of the network resources, this function allows the FortiBalancer appliance to encode the original URL address by using the base64 algorithm.

Currently, the following error codes are supported:

- 901: The SSL virtual host requires the client certificate;
- 902: The SSL client certificate's key size is too small;
- 903: The SSL client certificate is not trusted;
- 904: The SSL client certificate is expired;
- 905: The SSL client certificate is invalid yet;
- 906: The SSL client certificate has been revoked.

The HTTP error redirect function only works with the HTTPS type of virtual service.

New CLI command

To support this new function, the following command has been added:

```
http redirect error <error_code> <vs_name> <redirect_url> [prefix]
[encoding_mode]
```

Added "notice" log for health check failure

A log of "notice" level is now added to record the failure of real service health check when the status of the real service is up. After the status of the real service changes to down, the system stops generating these logs.

Extended maximum timeout value of SLB virtual services

The maximum value of the parameter `timeout` in the `slb timeout <virtual_name> <timeout>` command has been extended to 199,999,999, in seconds.

Reserved words not permitted in SLB configurations

To avoid incorrect behaviors, the system disallows using the system-reserved words (regardless of its case sensitivity) as the SLB real service names, virtual service names, vlink names, and additional health check names.

Support for more additional health checks

The maximum number of additional health checks that can be configured on the FortiBalancer appliance has increased from 400 to 4000. This allows the FortiBalancer appliance to meet higher requirements on additional health checks.

New symbols for logging HTTP requests

Two new symbols have been added for logging HTTP requests:

Symbol	Meaning
%F	IP address using which the FortiBalancer appliance connects to the real sever
%O	Port using which the FortiBalancer appliance connects to the real sever

Support for viewing the name of the client certificate header

The new CLI command `show http xclientcert header` has been added to allow you to view the name of the client certificate header.

SLB Policy order for QoS Body

The `policy_type` parameter in the following command now supports the QoS body policy (`slb policy qos body <policy_name> {virtual_name|vlink_name} {group_name|vlink_name} <prefix> <delimiter> <flag> <precedence>`) in the following command:

`slb policy order <order_template_name> <policy_type> <precedence>`

Notification for abnormal status of SSL card

When the hardware status of the SSL card is abnormal, a CRITICAL level fastlog is recorded about every 20 seconds. In addition, a warning is added to the output of the command `show version`.

Support for additional content types for session ID retrieve

For application session persistence, to retrieve session from HTTP response, two more HTTP response content-types are supported: “application/vnd.wap.xhtml+xml” and “application/xhtml+xml”.

Session ID matching mechanism enhancement

The Session ID matching mechanism is enhanced. For a group configured with an SLB Session Persistence method and associated with an SLB policy:

When “persistence response” is not configured:

- If the Session ID defined by the Session Persistence method exists, the system uses the Session ID defined by the Session Persistence method to update the persistence table.
- If the Session ID defined by the Session Persistence method does not exist, the system uses the Session ID defined by the SLB policy to update the persistence table.

When both “persistence request” and “persistence response” are configured:

- If the Session ID defined by the Session Persistence method exists, the system uses the Session ID defined by the Session Persistence method to lookup the persistence table.
- If the Session ID defined by the method does not exist or it exists but does not match the persistence table, the system uses the Session ID defined by the SLB policy to lookup the persistence table.

Secure Socket Layer (SSL) enhancements

SSL CRL memory information added to the output of the “show memory” command

To facilitate debugging the system, the SSL CRL memory information is added to the output of the `show memory` command.

Command that displays the certificate status of a host

To facilitate debugging, the system provides a new command to display the certificate status (active or inactive) of a virtual or real host.

To support this enhancement, the following command has been added:

```
show ssl status certificate <host_name>
```

To support this enhancement, the following command is modified:

Before:

```
show ssl status
```

Now:

```
show ssl status host
```

Check on SSL key length added

The system now automatically checks the SSL key length. If the key length is 4096 bits and not supported by the hardware, a prompt is displayed.

Support for configuring minimum RSA key length required for client certificates

As of FortiBalancer 8.4.0.1, the system allows the administrator to configure the minimum RSA key length required for client certificates when used to access a specified SSL virtual host. When clients try to access a specified virtual service by using certificates with RSA keys shorter than the configured minimum key length, client access will be rejected and the error

code “902: The SSL client certificate’s key size is too small” will be displayed. The minimum RSA key length can be 512, 1024, 2048, or 4096 bits.

New CLI commands

To support the preceding enhancement, the following commands have been added:

```
ssl settings clientcert minkey <virtual_host_name> <key_length>
no ssl settings clientcert minkey <virtual_host_name>
```

Modified CLI commands

To support the preceding enhancement, the `error_code` parameter in the following commands supports the error code “902”:

```
ssl import error <error_code> <url> [virtual_host_name]
ssl load error <error_code> [virtual_host_name]
show ssl import error page <error_code> [virtual_host_name]
no ssl import error <error_code> [virtual_host_name]
show ssl load error page <error_code> [virtual_host_name]
no ssl load error <error_code> [virtual_host_name]
http redirect error <error_code> <vs_name> <redirect_url> [prefix]
[encoding_mode]
no http redirect error <error_code> <vs_name>
```

Customizable items for generating a CSR

When the administrator enters information to generate a CSR, the “State or province”, “Location or local city”, and “Email address of administrator” subject fields are optional, and a maximum of three values can be specified for the “Organizational unit” subject field.

Multi-filter based certificate verification support for virtual hosts

Previously, client authentication and filter-based certificate verification were supported and need be configured together for the SSL virtual host. However, only one filter is allowed and the filter must be the “subject” field based. If the certificate does not match the filter, the client access will be rejected.

Now, client authentication and filter-based certificate verification are configured separately. Multiple filters are allowed and filters can be either the “subject” field or the “issuer” field based.

To be specific, an SSL virtual host supports a maximum of three “certfilter” configurations, among which the logical relationship is “OR”. Each “certfilter” configuration can contain at most two filters, between which the logical relationship is “AND”. If the client certificate does not match any “certfilter” configuration, the client access will be rejected. If the client certificate does not match all filters in a “certfilter” configuration, it does not match the “certfilter” configuration.

To support this enhancement, the following commands are added:

```
ssl settings clientauth <host_name>
ssl settings certfilter <vhost_name> <filter1> [filter2]
```

To support this enhancement, the following command has been deleted:

```
ssl settings clientauth <host_name> [subject_filter]
```

Support for 4096-bit SSL certificate

As of FortiBalancer 8.4.0.1, the appliance supports 4096-bit keys, besides 1024-bit and 2048-bit keys. That is, the administrator can generate a 4096-bit self-signed SSL certificate or import an existing 4096-bit SSL certificate.

To support this enhancement, the following command has been modified:

```
ssl csr <host_name> [key_length]
```

Now, the “key_length” parameter can be set to the value 1024, 2048 or 4096.

TLS1.2/SHA2 Support

FortiBalancer now supports the TLS1.2 protocol and the SHA2 cipher suites. However, the TLS1.2 protocol is only supported on SSL virtual hosts currently.

This new feature improves the application delivery security for customers. The following table describes the current support matrix of cipher suites by protocols SSL3.0, TLS1.0 and TLS1.2 for SSL virtual hosts and real hosts respectively on APVx600 series appliances.

Table 4: Cipher suites support by protocol

Cipher Suites	Bits	Protocols – Virtual Hosts			Protocols – Real Hosts		
		SSL 3.0	TLS 1.0	TLS 1.2	SSL 3.0	TLS 1.0	TLS 1.2
RC4-MD5	128	√	√	√	√	√	X
RC4-SHA	128	√	√	√	√	√	X
DES-CBC-SHA	64	√	√	X	X	X	X
DES-CBC3-SHA	192	√	√	√	√	√	X
AES128-SHA	128	√	√	√	√	√	X
AES256-SHA	256	√	√	√	√	√	X
AES128-SHA256	128	X	X	√	X	X	X
AES256-SHA256	256	X	X	√	X	X	X
EXP-RC4-MD5	40	√	X	X	X	X	X
EXP-DES-CBC-SHA	40	√	X	X	X	X	X

"√" indicates that the cipher suite is supported; "X" indicates that the cipher suite is not supported.

To support this new feature, the following two CLI changes have been made:

- The `version` parameter of the command `ssl settings protocol <host_name> <version>` supports the TLS1.2 protocol, in addition to SSL3.0 and TLS1.0 protocols. The default `version` value for SSL virtual hosts has changed to SSLv3:TLSv1:TLSv12.
- The `cipher_string` parameter of the command `ssl settings ciphersuite <host_name> <cipher_string>` supports all cipher suites supported by the TLS1.2 protocol. The default `cipher_string` value for SSL virtual hosts has changed to RC4-MD5:RC4-SHA:DES-CBC3-SHA:DES-CBC-SHA:AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256:EXP-RC4-MD5:EXP-DES-CBC-SHA:!SSLv2. The `cipher_string` value for SSL real hosts has changed to RC4-MD5:RC4-SHA:DES-CBC3-SHA:AES128-SHA:AES256-SHA:!SSLv2.

In addition, the web UI also supports this enhancement. When you turn on the TLS1.2 protocol for SSL virtual hosts on FortiBalancer appliances, if the SSL hardware is incompatible, both CLI and web UI display the message "TLSv12 is not supported by hardware".

Link Load Balance (LLB) enhancements

Added check mechanism for new eroute configuration

FortiBalancer is now enhanced to check the new eroute configurations in order to avoid possible difficulties or confusions about management.

A new eroute will fail to be added if both the following two conditions are met at the same time:

- The new eroute has the same priority with an existing eroute.
- The 5-tuple array of the new eroute overlaps that of any existing eroute. That is to say, an invalid new eroute should meet all the following conditions:
  - Its source subnet overlaps that of the existing eroute.
  - Its destination subnet overlaps that of the existing eroute.
  - Its source port range overlaps that of the existing eroute.
  - Its destination port range overlaps that of the existing eroute.
  - Its protocol has common subset with that of the existing eroute.

Back up eroutes before you upgrade. Eroutes configured with overlapping networks will cause eroutes to be lost when upgrading to FortiBalancer 8.4.0.1.

NAT log enhancement

Previously, NAT logs were generated when the system received SYN packets. In case of SYN flood attacks, a large number of NAT logs would be generated, which affected the

performance of the NAT function. Now, NAT logs are generated only when TCP connections are established. This enhancement prevents the NAT performance from being affected by SYN flood attacks.

Multicore function for processing route traffic

When the multicore function is enabled, FortiBalancer will use multiple threads to process route traffic, which greatly improves the traffic forwarding performance. By default, this function is disabled.

To support this enhancement, the following command has been added:

```
system tune route multicore {on|off}
```

When the multi-core function is enabled, SLB, DNS, RTSP, and RDP do not work.

LLB link used for ping packets

A new parameter `gateway_ip` is added in the `ping` and `ping6` commands to specify the IP address of the gateway of an LLB link route. When this parameter is specified, ping packets are sent to the host through the LLB link determined by this parameter.

Fastlog recorded when no port is available for NAT

When no port is available for NAT, a fastlog is recorded to notify the user.

Support for more LLB link routes

The maximum number of IPv4 and IPv6 LLB link routes supported by the system is now increased from 32 to 128.

Supporting displaying the matched IPflow route

As of FortiBalancer 8.4.0.1, the administrator can execute the command `show route match <src_ip> <src_port> <dst_ip> <dst_port> <protocol> [interface_name] [action_table]` to view the IPflow route that matches the entered `src_ip`, `src_port`, `dst_ip`, `dst_port`, and `protocol`.

Port range support for eroute

As of FortiBalancer 8.4.0.1, port range is supported for the eroute configuration.

To support this enhancement, the parameter `srcport` and `dstport` in the following command can be specified as either a port number or a port range now:

```
ip eroute <name> <priority> <srcip> {srcmask|prefix} <srcport>
<dsthost> {dstmask|prefix} <dstport> <proto> <gatewayip> [weight]
```

Hash IP method for outbound LLB

FortiBalancer is now enhanced to support the Hash IP (hi) method for outbound LLB. Hash IP method distributes the outbound traffic among links in the way that the link with higher weight is routed with higher probability, by performing hash operations on the source IP. When the chosen link is down, the system will perform hash operations again on the links available.

When the HI method is deployed for outbound LLB, the IPflow function can be disabled.

To support this enhancement, the following new command has been added:

```
llb method outbound hi
```

Domain name support for outbound link selection

As of FortiBalancer 8.4.0.1, the domain name of the destination host can be specified when configuring Eroute for outbound LLB. Thus, the FortiBalancer appliance now is able to resolve the domain name to an IPv4 or IPv6 address and uses the IP address to select the outbound link.

To support this enhancement, the parameter “dsthost” in the following command can be specified as either the domain name or the IP address of a destination host now:

```
ip eroute <name> <priority> <srcip> {srcmask|prefix} <srcport>
<dsthost> {dstmask|prefix} <dstport> <proto> <gatewayip> [weight]
```

Supporting LLB DD-based health check

Previously, LLB Dynamic Detecting (LLB DD) was only used to select a link with the shortest response time from a route group with the same priority. That is, the system sent LLB DD packets to the traffic’s destination only if two or more LLB link routes were available, and if no Eroute had been configured or no less than two Eroutes with the same priority had been configured. Then, the system selected the link with the short response time based on the LLB DD results.

Now, the system supports the LLB DD-based health check function. When this function is enabled, if two or more LLB link routes are available, the system will send LLB DD packets to the traffic’s destination no matter whether Eroutes have been configured. If the destination is detected unavailable (response timeout) through a link, the system will switch the traffic to the link with the highest priority among all the currently available links.

To support this enhancement, the following commands have been added:

```
llb link health remote [enable|disable]
```

Overlapped network subnets are displayed while configuring “ipregion route”

If network subnets overlap when the administrator is executing the `ipregion route` command to add routes using an IP region table, the system displays information of all overlapped network subnets in the IP region table.

Global Server Load Balance (GSLB) enhancements

Removing SDNS bandwidth function for hostnames

As of FortiBalancer 8.4.0.1, the SDNS bandwidth function for hostnames is removed.

To support this function change, the following command has been modified as follows:

Before:

```
sdns bandwidth {region|site|member|vip|host}
{region|site|member|host_name|ip address} <mode> <maxbandwidth>
[region|site]
```

Now:

```
sdns bandwidth {region|site|member} {region|site|member|ip address}
<mode> <maxbandwidth>
```

Removing the SDNS alias function

The SDNS alias function is now obsolete. Therefore, it is removed as of FortiBalancer 8.4.0.1. To support this function change, the following commands have been deleted:

```
sdns alias <alias_name> <host_name>
```

```
no sdns alias <alias_name> <host_name>
```

```
clear sdns alias
```

```
show sdns alias [alias_name]
```

SDNS manual and batch switchover

Manual switchover

The manual switchover function allows you to manually switch the resolved IP address of a domain name from the currently used IP address to an IP address with the specified priority. This function ensures application availability and improves user experience.

The prerequisites for using the manual switchover function are:

- The “region” method is configured for domain names
- The “IP overflow (IPO)” pool method is configured for corresponding SDNS pools

The manual switchover function is available only when the automatic switchover function of the SDNS pool is disabled or when the automatic switchover function is enabled but the preemption mode is “non-preemptive”.

Batch switchover

To help manually switch the resolved IP addresses of domain names as a batch, the FortiBalancer appliance allows you to add specific domain names to a group for unified monitoring and management. The web UI provides a visible domain group monitoring and management function.

When the resolved IP addresses of multiple domain names become unavailable, you can use this function to switch the resolved IP addresses to desired IP addresses as a batch.

Benefits

Effectively ensures the service usability and improves the experience of end users.

Helps customer administrators to flexibly configure and manage SDNS pools and to improve the capabilities of disaster tolerance.

Save the management time in the case of relevant configuration changes.

Related CLI commands

To support this new feature, the following commands have been added:

```
sdns pool ipo autoswitch <host> {site|region} {on|off}
sdns pool ipo resetgroup <group_name> [desired_priority]
sdns host group name <group_name>
sdns host group member <group_name> <host_name>
```

In addition, the following commands have changed:

Before:

```
show sdns pool [host_name|rule_name] [pool_name]
show statistics sdns host [host_name]
```

Now:

```
show sdns pool [host_name|rule_name] [pool_name] [group_name]
show statistics sdns host [host_name] [group_name]
```

General system & tools enhancements

NAT64 and NAT46 logs added

FortiBalancer 8.4.0.34 provides NAT64 and NAT46 logs. Use the `log nat custom` command to configure the log format.

Specific fan information is logged when a fan failure occurs

To help the administrator to quickly locate a failed fan, the system logs the specific information of the failed fan.

CLI prompt for configuring log server is optimized

If a syslog server whose host ID is not 0 is specified to receive logs, at least one log filter should be configured. To remind the administrator that this configuration is needed, the prompt of the `log host <host_ip> [port] [udp|tcp] [host_id]` command has been modified:

Before:

```
id(optional,default = 0)
```

Now:

```
id(optional, 0 - 65535. Default is 0, all log will be sent to log
server. If id isn't 0, log filter MUST be configured, otherwise, no
log will be sent)
```

Enhanced log filters

Previously, logs matching the log filter string were sent to the log server. Now, the administrator can configure whether FortiBalancer appliance sends logs that match the log filter string or that belong to the specified module(s) to different log servers, which are specified by the `host_id` parameter.

To support this enhancement, the following command has been modified:

Before:

```
log filter <host_id> <filter_id> <filter_string>
```

Now:

```
log filter <host_id> <filter_id> <filter_string> [module_name]
[method]
```

module_name

This optional parameter specifies the module name used together with `filter_string` to filter syslogs. The module name is case insensitive. The maximum length of the module name is 40 characters.

For supported modules, please view the Log List file in the .txt or .html format on web UI by clicking the View button in the Log Documentation area of Admin Tools > Graph > Logging > General.

Multiple modules are supported in a format such as “SSL:SLB:LLB”. The default value is “all”, which specifies all modules of the system.

method

This optional parameter specifies the sending of syslogs.

- “0” indicates that the syslogs matching the log filter string but not belonging to the specified module(s) are sent to the syslog host.
- “1” indicates that the syslogs matching the log filter string and belonging to the specified module(s) are sent to the syslog host.

The default value is “1”.

Support for priority control on the local database and the external authentication server for external authentication

Previously, the local database was used first when external authentication was enabled. The external authentication server was used only when the user name did not exist in the local database.

Now, the administrator can configure whether the local database or the external authentication server is used first when external authentication is enabled. By default, the local database is used first.

To support this enhancement, the following command has been modified:

Before:

```
admin aaa {on|off}
```

Now:

```
admin aaa {on|off} [priority]
```

View “error” logs for wrong-format CLIs during the configuration loading process

In non-interactive mode, if the system encounters wrong-format CLIs during the configuration loading process, it generates error-level logs. The administrator can execute the command `show log buff backward` to view these wrong-format CLIs. This enhancement helps the administrator to debug the system.

Logging for administrators' logins and logouts via web UI

To facilitate auditing the administrators that have managed the FortiBalancer appliance, the system now supports recording logs for the administrators' logins and logouts via the web UI. These logs contain the IP addresses used by administrators to log in to or log out of the system.

For example:

100014006 user "array" from 192.168.2.1 login webui success

100014006 user "array" from 192.168.2.1 logout webui success

View SSL session cache usage

Now, the administrator can execute the command `show memory` to view the SSL session cache usage, including the size of a session cache, limit of session caches, used session caches, free session caches, and requested session caches.

User-friendly prompt added when changing the protocol used by XML-RPC

To change the protocol used by XML-RPC, the administrator needs to first disable XML-RPC for the currently used protocol (HTTP or HTTPS). To avoid misoperations, the following user-friendly prompt has been added for changing the protocol used by XML-RPC:

XMLRPC is runing, xmlrpc off is needed to change the configuration

Controls for generating NAT and FWD logs

Previously, the system did not generate NAT logs but generated FWD logs by default, and the administrator could not change these default settings. Now, the system does not generate either NAT or FWD logs by default. The administrator can execute the `no log message disable` command to enable the system to generate NAT logs and FWD logs. In addition, the log levels of NAT and FWD logs are changed to info.

RFC 5424 syslog

RFC 5424 defines the standard format of syslogs. To support syslogs compliant with the RFC 5424 format, the RFC 5424 syslog function is introduced. The format is "<PRI>VER TIMESTAMP HOSTNAME APPNAME PROCID MSGID STRUCTURED-DATA MSG-CONTENT". (The PROCID and STRUCTURED-DATA fields are not supported temporarily and are displayed as "-".)

By default, the RFC 5424 syslog function is disabled. It takes effect only when the system logging function has been enabled by using the `log on` command.

New CLI commands

To support this new function, the following commands have been added:

```
log rfc5424 {on|off}
log rfc5424 appname <app_name>
log rfc5424 msgid <system_log_id> <custom_log_id>
```

SLB address translation logs

As of FortiBalancer 8.4.0.1, the system is able to generate SLB address translation logs. In SLB reverse mode, when receiving a request from the client, the FortiBalancer appliance will translate the source and destination IP addresses to the VIP and a real service's IP address respectively.

To support this enhancement, the following command has been added:

```
log nat custom <format_string>
```

Added error logs for wrong-format CLIs during the configuration loading process

In non-interactive mode, if the system encounters wrong-format CLIs during the configuration loading process, it will generate error-level logs. The administrator can execute the command `show log buff backward` to view these wrong-format CLIs. This enhancement helps the administrator to debug the system.

Logging for administrators' logins and logouts via web UI

To facilitate auditing the administrators that have managed the FortiBalancer appliance, the system now supports recording logs for the administrators' logins and logouts via Web UI. Such logs contain the IP addresses used by administrators to log in to or log out of the system.

For example:

```
100014006 user "admin" from 192.168.2.1 login webui success
100014006 user "admin" from 192.168.2.1 logout webui success
```

Support for displaying CPU utilization of each core

To facilitate debugging the system, the system supports displaying the CPU utilization of each CPU core. To support this enhancement, the following command has been added:

```
show debug usage cpu
```

Supporting displaying of SSL session cache usage

Now, the administrator is able to execute the command `show memory` to view the SSL session cache usage, including the size of a session cache, limit of session caches, used session caches, free session caches, and requested session caches.

"admin" account recovery mechanism enhancement

The FortiBalancer appliance provides the default login account "admin/admin" to allow the administrator to log in to the device. Previously, if the administrator forgot the password of the "admin" account, the "admin" account recovery mechanism allowed the administrator to reset the password to "admin".

Now a further enhancement has been made to the account recovery mechanism. If the default login account "admin" is deleted by accident, the administrator can recover the account. The method of recovering the "admin" account is the same as that of resetting the account's password.

Log buffer extended to support 2000 logs

In earlier versions, the log buffer could store 500 logs. At present, the log buffer can store a maximum of 2000 logs.

Cacti support

FortiBalancer appliances now fully support Cacti, which is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality.

Support for disabling system logs by log ID

FortiBalancer 8.4.0.34 allows you to disable system logs by log ID. A maximum of 32 system logs can be disabled. Disabling system logs helps to reduce the space required for storing system logs and saves the bandwidth used for sending logs to the log server.

To support this enhancement, the following command has been added:

```
log message disable <log_id>
```

To view the IDs of generated system logs, execute `log option logid on` and then `show log buff`.

Alternatively, you can obtain the ID of every system log by performing the following steps:

1. In the web UI, go to *Admin Tools* > *Graph* > *Logging* > *General*.
2. In the Log Documentation area, click either of the *View* buttons.

Support for deferred system update

Administrators can now import a new update package without immediately rebooting the FortiBalancer appliance. With the update deferred, if any configurations are changed after the new update package is imported, the administrator can run the command `write all deferred` before rebooting the appliance to save the running configurations. After the appliance reboots, the new system takes effect and the configurations are automatically synchronized into the new system.

Even if the deferred update is not implemented, the administrator can also run the command `write all deferred` to save configurations, which has the same effect as the command `write memory`.

To support this enhancement, the following command has been modified:

Before:

```
system update <url>
```

Now:

```
system update <url> [immediate|deferred]
```

The default value of command `system update <url> [immediate|deferred]` is `immediate`.

To support this enhancement, the following commands have been added:

```
write all deferred
```

`show system update deferred`

If the FortiBalancer appliance is downgraded to a build that does not support deferred update, and then is fallen back, the output of the command `show system update deferred` is displayed as `incomplete upgrade` but, in fact, the fallback has already been successfully completed.

Debug enhancements

In FortiBalancer 8.4.0.34, the snapshot function is obsolete.

To support this function change, the following commands have been deleted:

```
debug snapshot all [level]
```

```
debug snapshot proxy [level]
```

To allow the debugging function to work well for SSL, the following changes have been made:

Now:

```
debug trace live ssl <interface_name> <host_name> [encrypt|plain]
[ssldump_argument]
```

- Parameter `host_name` supports both real and virtual host in FortiBalancer 8.4.0.34;
- For parameter `encrypt|plain`, plain mode is not supported for real host;
- Parameter `ssldump_argument` is added.

OID added for SSL connections established per second

A new OID ".1.3.6.1.4.1.7564.20.2.4.1.9." is added for querying the number of SSL connections established per second.

High availability enhancements

More flexible failover policy

To achieve more flexible failover based on port status, the administrator can add the port health check conditions (PORT_1~PORT_32) to vconditions and use vconditions as failover conditions. For example, if two port health check conditions are added to a vcondition and the relationship between the two conditions is "OR", group failover occurs only when both ports become down. If the relationship is "AND", group failover occurs when either port goes down. Please note that after a network port health check condition is added to a vcondition, the corresponding predefined failover rule will not take effect.

Web UI enhancements

Configuration for rules for sending log alert messages

In *Admin Tools* > *Graph* > *Logging*, the Email subtab is added for configuring the rules of sending log alert messages.

Support for enabling and disabling real services in batch

In the *SLB Real Services Configuration* area of *Server Load Balance* > *Real Services* > *Real Services*, the administrator can enable or disable the selected real services in batch by selecting multiple lines of real service entries in the table and clicking the *Enable* or *Disable* action link. This enhancement helps the administrator improve the efficiency in managing real services.

Optimizing web UI timeout log

The log for the web UI timeout, which can be viewed in the output of `show log buffer backward`, has been optimized to be easier to understand.

Optimizing the note for the Checker Flag parameter on the web UI

In the *Add Health Checker* area of *Server Load Balance* > *Check Lists* > *Health Checker*, the note for the Checker Flag parameter has been optimized to be more accurate. This enhancement may help avoid possible incorrect configurations of the *Checker Flag* parameter.

Display of current CPS count of a real service

In *Server Load Balance* > *Real Services* > *Real Services* > *Edit Real Service Entry*, a new statistics item *Current CPS Count* is added for the real service whose value of the *Max Connections Per Second* parameter is non-zero.

Support for NAT statistics

In *System Configuration* > *NAT* > *Statistics*, the NAT Statistics area is added to display inbound and outbound NAT statistics.

Start time added to predefined graphs

In the *View Graph* area of *Admin Tools* > *Graph* > *Graph Monitoring* > *Predefined Graphs*, a *Start Time* text box is added to specify the start time of a predefined graph.

Upgrade instructions

Hardware model support

FortiBalancer™ 8.4.0.34 supports:

- FortiBalancer-400
- FortiBalancer-1000
- FortiBalancer-2000

Upgrading from previous releases

The recommended update path is:

1. FortiBalancer 8.x
2. FortiBalancer 8.4.0.34

If you do not update the firmware in this order, your configuration may not be correctly converted to be compatible with the new firmware.

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 5: Resolved issues

Bug ID	Description
42579	The FTP downloading service failed because the FortiBalancer appliance did not send the ICMP “Destination Unreachable-Fragmentation Needed and DF Set” packet received from the router to the real server due to the multi-core TCP/IP stack design.
42434	The FortiBalancer appliance failed to use port 20 as the default port to transfer FTP data in FTP active mode.
42346	When the response line “HTTP/1.1 200 OK” from the real server was split in front of “200 OK” and transferred in multiple frames, an error occurred in response code parsing and the FortiBalancer appliance sent the error “502 Bad Gateway” to the client.
41934	When HTTP compression and the reuse of server connections for multiple transactions were both enabled on the FortiBalancer appliance, and packets from the client contained both the GET method and the POST method that contains the message body, the access through IE browser became extremely slow or even no response is returned.
41797	The VIP was inaccessible because memory leak occurred.
39959	In the Server Load Balance (SLB) health template displayed by the command `show health template`, two problems have been fixed: The configuration examples of the `health app` command were provided in the incorrect format `health app <real_name> <ip> <port> <list name> [frequency] [hc_localip] [hc_localport]`. The correct format should be `health app {real_name|add_hc_name} <list_name> [frequency] [hc_localip] [hc_localport]`. `telnet_check` is misspelled as `telnet_checker` in the command example of `health member telnet_list telnet_checker`.
39530	System reboot caused by a double-free memory error. If L7 SLB had been configured and the system was overloaded, a double-free memory error might occur when the system was closing TCP connections. As a result, system reboot might occur.
39616	URLs failed to hit the originally-hit SLB regex policy. When two or more SLB regex policies were configured, the regex string of one policy (policy1) was the prefix of another policy (policy2), and some URLs had hit policy1 but not policy2, these URLs would not hit policy1 after policy2 was deleted.

39060	FTP server access abnormality occurred due to the SLB FTP conflict with static NAT. After "**nat static**" has been configured, all ATCPs would listen to the specified VIP. In addition, SLB FTP data connections would go to L7 thread. This issue has now resolved.
38860	With the HTTP content rewrite function enabled, a client accessing an HTTP or HTTPS virtual service might send a RST packet if a line in the response was longer than 10KB. This issue has now resolved.
38747	In rare cases, if L4 TCP services were running on the system, system panic might occur when the system was processing RST packets.
38210 25173	The per-VS SLB timeout value set by using the command `slb timeout` should take precedence over the global TCP connection timeout value set by using the command `system tune tcpidle`. However, when both of the two timeout values had been specified for TCPS and HTTPS virtual services, the smaller timeout value would take effect for TCPS and HTTPS VSs. Now, once the per-VS SLB timeout value is specified for a TCPS or HTTPS VS, the per-VS SLB timeout value will always take effect.
37261	An IPv4 FTP client sent a request with the EPSV mode chosen, but the FortiBalancer appliance responded the client with the PSV mode. As a result, the IPv4 FTP client failed to establish data connection with the FTP server.
36557	Under rare circumstances, disabling the real services and then enabling them again might lead to a system reboot.
35541	When only one HTTPS connection in the system was used to download a large file from a real server, the state machine failed to start in time. As a result, the downloading speed on the HTTPS connection might be slower than expected.
34833	Adding VIPs to or deleting VIPs from a FortiBalancer appliance equipped with the 10G NIC would cause the 10G NIC to reboot.
44747 44807	If the health check type of a real service was specified as "none" and the real service was configured with additional health checks in the "OR" relation, the health check status of the real and virtual services were both displayed as UP when all additional health checks failed.
44195	Uploading a file to the real server through the FortiBalancer appliance failed when the file size was equal to or larger than 4 GB.
44053	When HTTPS SLB was configured and the server bandwidth was higher than the client bandwidth, downloading a large file through the VIP would fail.
44810	When `cache=yes` was specified in the `cache filter rule` command, the response with `cache-control no-cache` failed to be cached.
41516	If two real servers returned an identical session ID, client requests that should have matched the second real server returning the session ID

	would match the first real server. Now, if two real servers returned an identical session ID, the connection to the second real server will be reset.
43654	When HTTP cache was enabled and the client connection was lost, the FortiBalancer appliance would keep caching the responses from the real server, which led to temporary service suspension.
43330	Error “503 Service Unavailable”, which affected all virtual services, occurred when resources failed to be allocated for incomplete connections because the incomplete connection limit had been reached.
43208	Under the L7 SLB scenario, after the client sent a Get request and then a FIN packet, the downloading of a large file failed.
42659	When the DirectFWD function, the DirectFWD module’s syncache function, and hardware checksum function were all enabled, hardware checksums of certain packets sent from the client and forwarded by the FortiBalancer appliance were incorrect.
40585	The health request string of SMTP configured by the `health request` command according to the output of the `show health template` command was invalid. The output of the `show health template` command is updated to indicate that the health request string must end with `\r\n`.
42668	When receiving an SSL alert message of incorrect length, the FortiBalancer appliance would record log “SSL: Memory allocation failure. Error code: 54”, which was irrelevant to memory allocation. The system now records log “SSL: received a record with incorrect length” in such a circumstance.
41903	When no SSL host was configured, the system checked the certificate and generated a certificate check failure log “SSL: certm failed to check cert”. Now the system does not check the certificate if no SSL host is configured.
41856	FortiBalancer 8.4.0.34 has updated its SSL module to address the security vulnerability reported by CVE-2013-0166.
41745	The FortiBalancer appliance automatically rebooted because the certificate contained extremely only field strings.
39806	Previously, the testing SSL certificate and private key generated by executing the command `ssl csr` were saved without an index. When the administrator executed the command `ssl import certificate <host_name> [cert_index] [tftp_ip] [file_name]` to import an official certificate issued by CA to replace the testing certificate, the system might not find a matched private key with the same index as the imported certificate. As a result, certificate import failed. The testing certificate and private key generated by `ssl csr` are saved with index “1”. To replace the testing certificate, the administrator can import an official certificate with index “1”.
39153	The output of the command `ssl export key` displayed the last encrypted key after the administrator imported non-encrypted PEM-

	format key. If the key currently being used is not exportable, the system will prompt so instead of exporting the last encrypted key.
38474	With the SSL session reuse function enabled, when receiving new SSL requests after the session caches had been all occupied, the system would check for idle session caches on which no connection was running. Due to SSL connection leak, no idle session cache was available. As result, the system failed to assign session caches to new SSL requests and new SSL connections were abnormally reset.
37554	FortiBalancer rejected clients' valid certificates when both the following conditions were met: • The CRL memory function was disabled by executing the command `ssl globals fastcrl off`. • The only difference between the serial numbers of clients' valid certificates and the serial numbers in the CRL was 0s at the end of these numbers.
43111 22470	Some client certificates failed to be verified because the check on the KeyUsage field was mandatory. Now, the system does not check the KeyUsage field by default.
43067	Only the CA root certificate whose version extension was V1.0 could be imported to the FortiBalancer appliance. This issue has been resolved by removing the limit on the version extension of CA root certificate. Now, the CA root certificate whose version extension was not V1.0 can also be imported to the FortiBalancer appliance.
44444	When receiving an SSL packet of incorrect data length, the FortiBalancer appliance would record log "SSL: Memory allocation failure. Error code: 52". However, the issue was irrelevant to memory allocation. The system now records log "SSL: Host host_name received a record with incorrect length from client_IP" in such a circumstance.
44910 44937	For new SSL HW on a FortiBalancer 2000, with a large number of SSL virtual hosts configured, not all SSL virtual hosts could automatically start after the FortiBalancer appliance rebooted.
42828	Although the command `ssl activate certificate` had been successfully executed, the log message indicated that the command failed to be executed.
42586	Only the eroutes with subnet masks being multiples of eight were valid.
38179	Ping failure occurred when eroute connection being used with LLB failed. This issue has been resolved by clearing PCB when the eroute being used is changed.
38172	New "nat port" configuration failing to take effect If a new `nat port` was configured with a network segment (specified by `source_ip` and `netmask|prefix`) that overlaps that of an existing `nat port` configuration, the new configuration may fail to take effect.
37725	RTS working abnormally

34948	When the RTS function was enabled, if the gateways of any two LLB links had the same MAC address, the RTS function might work abnormally.
43888	The prompt for the command `llb link route`, which is `Add a new link and the basic health checker of the link`, was outdated because the LLB health check mechanism has been updated and the LLB health checker needs to be added manually. The prompt for the command `llb link route` is updated to `Add a new link route`.
43740	After "ipregion route" configurations were added when there had already been abundant "ip eroute" configurations, the configuration loading process was slow during the start of the FortiBalancer appliance. This issue has now been resolved by optimizing the "ipregion route" configuration storage mechanism.
43288	The system failed to forward response packets due to a route match error.
44500	When both the LLB proximity method and the Return To Sender (RTS) function were enabled, the FortiBalancer appliance frequently rebooted.
42880 39615 38169	In FortiBalancer 8.4.0.34, the BIND9 component is updated to address the security vulnerabilities reported by CVE-2013-2266, CVE-2012-3817, and CVE-2012-4244.
41716	When an IP pool was configured and the IP addresses of the IP pool were used as VIPs for clustering or HA, IP address conflict occurred during configuration synchronization. **Note:** After the system is updated to FortiBalancer 8.4.0.34, please run the `write memory` command to make sure that this issue will not occur.
41885	In discreet mode, after failover occurred for several times because a port of the master FortiBalancer appliance was repeatedly unplugged and then plugged, cluster status of ports with the same VCID became different on this FortiBalancer appliance.
34149	The output of the command `show route match <src_ip> <src_port> <dst_ip> <dst_port> <protocol> [interface_name] [action_table]` failed to show the IPflow entries that matched the parameter settings.
39615 38169	The BIND9 component in GSLB has been upgraded to version 9.8.4 to address the vulnerabilities reported by CVE-2012-3817 and CVE-2012-4244.
38610 37675	When SDNS statistics was enabled for the local DNS, if the case sensitivity of domain names in DNS queries changed frequently, memory leaks might occur due to defects of the SDNS statistics function. As a result, the GSLB module might fail to resolve domain names.
40203	The commands `ha ssf on` and `ha ssf off` are used to respectively enable and disable the SSF function on a specified virtual service or NAT.

	However, “NAT” is missing in the help strings of both commands.
41522	After the FortiBalancer appliance ran for a period of time, the HA module failed and log information “/ca/bin/decisiond startup” was generated.
41560	The HA function checked the complete release version number of a unit when the unit is trying to join the HA domain. This might lead to frequent network interruption. Now, the HA function checks the release version number to the second digit. For example, for FortiBalancer 8.4.0.x, the HA function checks only 8.4.
44440	When units in an HA domain are configured with IPv6 addresses and Webwall is enabled on the units, an ACL rule permitting bootup synconfig packets from the peer unit should be configured so that bootup synconfig can work properly.
44422	The bootup synconfig function fails if units in the HA domain use different FortiBalancer systems. To use the bootup synconfig function, units in the HA domain should use identical ArrayOS systems. For example, if one unit uses FortiBalancer 8.4.0.34, other units in the HA domain should also use FortiBalancer 8.4.0.34.
43903	When the Runtime Synconfig function was enabled, the configurations of the `ip eroute`, `no ip eroute`, and `clear ip eroute` commands could not be synchronized between units in real time. To provide better user experience, the `ip eroute`, `no ip eroute`, and `clear ip eroute` commands are added to the HA Runtime Synconfig Whitelist. As a result, the configurations of these commands can be synchronized between units in real time.
40113 33922	The clustering backup unit failed to synchronize configurations from the master unit when the `va` processes of the clustering module on the backup unit hang. When the `va` process of the clustering module hang, the system rebooted automatically.
39371	When a FortiBalancer with NIC bond configuration on 10Gb NICs ran the `synconfig to` command, the customer’s switch would report that the 10Gb NICs were removed from the bond and then re-joined the bond, although bond configuration was not changed at all on FortiBalancer. **Note:** As of FortiBalancer 8.4.0.1, `interface mtu` and `interface speed` configurations will not be synchronized by the command `synconfig to`.
39306	In a cluster in Active-Standby mode and with multiple cluster VIPs configured, if one VIP was deleted from the backup and the master units in sequence, the status of the other VIPs would become active on both units and this would last for a short time.
38354	When the interval at which the master unit broadcasts ARP packets was set to 0 seconds by using the command `cluster virtual arp interval 0`, the timeout value for reading VRRP packets on the master unit might be incorrectly changed to 0 seconds, which indicated no timeout. As a result, the master unit would stay in a loop waiting for the

	new VRRP packet to arrive, which caused a rise of CPU utilization on the master unit.
42439	The time zone of the FortiBalancer appliance could not be set to GMT+4. The time zone can now be set to “United Arab Emirates”, which indicates GMT+4.
40997	When the administrator logged into the FortiBalancer appliance through the serial port and executed the `monitor` command with default parameter values, the command could not be stopped after the administrator pressed Enter. This issue has now been resolved as follows: 1. To execute the `monitor` command, log into the FortiBalancer appliance through SSH or Web UI. 2. If the administrator logs into the FortiBalancer appliance through the serial port and execute the `monitor` command, the refreshing interval should be set to 10 seconds or longer.
44761	When Webwall was enabled, VRRP packets were blocked by Webwall. As a result, the master and backup statuses of the clustered nodes became incorrect.
40786	A software enhancement has been made to solve an exception where the XML-RPC function failed to be disabled by the command `xmlrpc off`.
40651	The FortiBalancer appliance incorrectly and repeatedly displayed the warning messages “One of the power supplies has failed” and “The failed power supply is restored”, when the power supply actually had not failed.
40130	Occasionally, the value of the SNMP OID “.1.3.6.1.4.1.12356.4.1.0” (current system total available memory) obtained by the SNMP client was 0.
40067	In the logMaxSeverity OBJECT-TYP area of the MIB file, the values of the error and debug logs were wrong: error(4) and debug(8).
39471	After the system of a unit had been running for 25 days, the internal TCP connection between the SNMP module and the cluster module might be disconnected because the system calculated the timeout value incorrectly. As a result, the SNMP module failed to obtain cluster status information from the cluster module.
38769	The prompt of the command `ssl activate certificate` was grammatically incorrect. The prompt has changed to “Do you want to activate 1st/2nd/3rd certificate [YES/(NO)]:”.
38664	The maximum length of the password for an administrator added by using the command `user` was 80 alphanumeric characters. However, the maximum length of the administrator’s password did not take effect and a password of more than 80 characters could be configured for an administrator.
37406	When the command `ip arp` had been executed to add a static ARP entry and then `write memory` executed to write the configuration to the memory, the `ip arp` configuration would be missing after system reboot. This issue has now been resolved, and a maximum of 128 static ARP

	entries are allowed to be configured.
37009	When only the bond interface was configured with an IP address, the system prompted the error message “traceroute: Can't find any network interfaces” after the `traceroute` command was executed.
36939	The hardware checksum error occurred when the FortiBalancer appliance received packets with the CWR or ECE flag, because it did not recalculate the checksum after removing the flag.
34916	System panic occurred due to obsolete logging and graphing tool.
34755	Vulnerabilities reported as CVE-2012-0021 and CVE-2012-0053.
32497	The maximum number of VLANs allowed on a FortiBalancer appliance is now expanded to 4096.
43521	The syslogTrap OID in the actual data packet (.1.3.6.1.4.1.7564.24.3) was incorrect. The correct OID should be the one in the MIB file (.1.3.6.1.4.1.7564.24.3.1).
42827	FortiBalancer 8.4.0.34 has reduced the attack risk reported by CVE-2010-5107. For CVE-2013-2566, the attack risk is determined by the RC4 cipher suite; therefore, not using the RC4 cipher suit will eliminate the attack risk.
42630 42852	The command line interface (CLI) was locked up because of the resource allocation failure.
36940	The output of the command show `statistics nat` was incomplete because the number of the inbound packets was not counted.
44643	In FortiBalancer 8.4.0.x, the SNMP sysDescr and sysObjectID values were incorrect.
44507 44303 44268	The SNMP OIDs of FortiBalancer 8.4.0.x are incompatible with those of FortiBalancer 8.3.x.x. Now, the SNMP OIDs of FortiBalancer 8.4.0.34 are updated to be identical with the OIDs of FortiBalancer 8.3.x.x.
44275	When you upgrade to FortiBalancer 8.4.x, the license key is upgraded automatically. This upgraded license key is not compatible with earlier systems. To avoid problems with incompatible license keys when you downgrade, before you upgrade to FortiBalancer 8.4.x, use the `show version` command to back up the existing license keys. You can re-enter these backed-up keys if you downgrade your system.
44456 45523	When the interface type is i82576 or i82580, and traffic was heavy, certain error messages were generated and the system might panic.
39310	The GSLB BIND9 feature allows the name server to give different responses based on the source IP address. However, Web UI did not support importing multiple zone files for the same zone. To perform BIND9 configuration, please select *Advanced Load Balance > Global*

	Load Balance > *Records* > *Others* in Config mode on Web UI.
38944	When the administrator tried to change the `first choice method` for an SLB group on the web UI, an error occurred.
38216	In the *Access Group Configuration* table of *Webwall* > *Access Control*, he administrator might fail to delete an access group configuration by selecting a row and clicking the *Delete* action link. Instead, another row of access group configuration was deleted.
43839	UDP traffic whose destination was the FortiBalancer appliance did not pass the Webwall check as configured. The current default behavior of Webwall is to check all traffic when Webwall is enabled.
44081	When Webwall was enabled, HA heartbeat packets from the peer unit would be discarded if no ACL rule was configured to permit HA heartbeat packets. As a result, the status of the peer unit could not be acknowledged. Now, Webwall will not restrict HA heartbeat packets.
45264	When Webwall was enabled, FTP data connection packets would be blocked by Webwall unless an ACL rule was configured to permit FTP packets. Now, Webwall will automatically permit FTP data connection packets.
44939	With Webwall enabled, Webwall permitted UDP packets that were destined for the virtual IP address of the configured static NAT and did not match any configured ACL permitting rule.
38143	Some language errors appeared when the web UI was being displayed in Japanese.
37765	After a virtual service was selected from the *Please Select a Virtual Service* drop-down list box in the *SLB Virtual Service Status area of Server Load Balance* > *Monitoring* > *Status*, the web UI failed to display the status of this virtual service. Meanwhile, the CPU utilization rose.
34360	Garbled characters occasionally appeared in the SDNS statistics report, dynamic proximity statistics report, or LLB link statistics report when these reports were viewed on or exported from the web UI in Chinese.
33811	The names of the real service types were all in lower-case letters, such as “tcp” and “tcps”. This issue has been resolved to by changing them to upper-case letters.
42849	After the administrator clicked a feature link from the side bar on an Internet Explorer 10 or Chrome browser, the feature link did not become bold and the feature links did not align with the left-hand margins.
44096	The long real service name could not be completely displayed on the web UI.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 6: Known issues

Bug ID	Description
39871	HA and cluster configurations cannot coexist for the same VIP. When both HA and cluster are configured for a VIP, HA configurations do not take effect.
39612	System interface on 10G NIC listening to at most 128 multicast MAC addresses. If the FortiBalancer appliance is equipped with the 10G NIC, each system interface on the NIC can listen to at most 128 multicast MAC addresses. When an IPv6 address (local IP address or VIP) is configured on a system interface, the system interface has to listen to one additional multicast MAC address. When more than 128 multicast MAC addresses need to be listened by the system interface, the system interface might not receive packets sent to some multicast MAC addresses. To avoid this issue, do not configure too many IPv6 VIPs on a system interface.
39348	CPU utilization increases abnormally due to ACL rule configuration. When the subnet of an ACL rule contains the subnets of many ACL rules, the system will consume many CPU resources when matching client IP addresses with these ACL rules. As a result, the CPU utilization rises abnormally. To avoid the abnormal rise of CPU utilization, do not configure too many ACL rules with their subnets directly belonging to the subnet of an ACL rule.
39200	Two system tune commands can conflict. When the commands `system tune accel mq` and `system tune dispatcher numa` are both configured, system performance deteriorates sharply. Therefore, only one of these commands should be configured.
39082	Client authentication changes after a downgrade from 8.4.0.1 to 8.3.0.x. In 8.3.x, client authentication was enabled by the command `ssl settings authmandatory`. Therefore, when the system is downgraded from FortiBalancer 8.4.0.1 to 8.3.0.x, client authentication might be enabled by the `ssl settings authmandatory` configuration. As a result, the SSL host status will change from “Active” to “Inactive” if there is no SSL Root CA. After the downgrade, please check whether the client authentication configuration in 8.3.x is the same as that in 8.4.0.1.
38963	High CPU utilization when graph monitoring was enabled. When 4000 SLB virtual services are configured and graph monitoring is enabled by executing the command `statmon on`, the CPU utilization will become high even if there is no traffic on these virtual services. To avoid high CPU utilization in this case, disable graph monitoring by executing the command `statmon off`.

37887	Link LED did not indicate the speed mode. The Link LEDs on add-on NICs of the FortiBalancer appliance have only the yellow color to indicate the 1 Gbps, 10 Mbps or 100 Mbps speed mode. As a result, administrators cannot determine the current speed mode from the Link LEDs.
45426	If more than one thousand SSL virtual hosts are configured and then started, certain SSL virtual hosts may fail to start and coredump may occur.
43885 44070	When the network traffic is heavy, using an SSH-based script to frequently access the FortiBalancer appliance in a short time of period may cause system suspension.