FortiBalancer 8.5.0.5

Release Notes

for 400, 1000, 2000 AND 3000 models

FortiBalancer 8.5.0.5 Release Notes

April 24, 2015

Revision 1

Technical Documentation	http://docs.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://forum.fortinet.com
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 paths, resolved issues, and known issues for FortiBalancer 8.5.0.5.

For additional documentation, please visit:

http://docs.fortinet.com/fortibalancer

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 8.5 User Guide and CLI and User Handbooks.

ReArchitected SDNS

In FBLOS 8.5 release, the Global Server Load Balancing (GSLB) feature is re-architected to make the Smart DNS (SDNS) architecture clearer and the configuration easier and more flexible, and provide comprehensive IPv6 support.

Clear SDNS architecture

After GSLB re-architecting, SDNS's architecture is similar to the FortiBalancer SLB feature,which is comprised of the following concepts:

- SDNS host name: is the domain name that can be resolved by SDNS.
- SDNS policy: determines the SDNS service pool for the host name.
- SDNS service pool: is a group of host IP addresses for the host name.
- SDNS service pool method: determines which host IP address or addresses in the hit service pool are returned in the DNS response.
- SDNS service IP: is a host IP address for the host name.

The workflow of re-architected SDNS is as follows:

1. Based on the domain name in the DNS query, SDNS finds the hit SDNS policy.
2. Based on the SDNS policy, SDNS finds the hit SDNS service pool.
3. Based on the method of the hit SDNS service pool, SDNS picks up service IPs.
4. SDNS returns the picked service IPs to the local DNS.

Easy and flexible way of SDNS configuration

GSLB re-architecting makes SDNS configuration easier and more flexible.

- Previously, SDNS has to use SLB Health Check function to perform health check on the service IP. Re-architected SDNS provides independent health check to monitor the health status of the service IPs in the SDNS service pool in real time.
- The structure of SDNS DPS is simplified. The DPS master and slave now are combined together as the DPS server. The DPS server provides the same functions as both the DPS master and slave previously provided. The simplified SDNS DPS structure makes the understanding and configuration of SDNS DPS easier
- Previously, complete A, AAAA and Canonical Name (CNAME) resource records needed to be configured by using the commands **"llb dns host", "sdns ipv6",** and **"sdns cname"** respectively. Now, the host name and IP address/CNAME part of

resource records are configured separately. SDNS will dynamically construct the complete resource records with the host names and the resolved IP addresses (service IPs) or CNAME to respond to DNS queries, which makes the configuration more flexible.

Comprehensive IPv6 support

After GSLB re-architecting, SDNS provides comprehensive IPv6 support:

- SDNS service IP: The service IP can be an IPv4 or IPv6 address.
- SDNS service pool: The service IPs in a service pool can be either all IPv4 addresses or IPv6 addresses. Note that a service pool cannot contain both IPv4 and IPv6 addresses.
- SDNS proximity rule: Proximity rules support IPv6.
- SDPS DPS: SDNS supports IPv6 DPS detectors and supporting detecting IPv6 local DNSs.
- SDNS health check: SDNS supports performing health checks on IPv4 and IPv6 service IPs.

The SDNS CLI commands in FortiBalancer 8.5 release are very different from those in FortiBalancer 8.4 release. For the SDNS CLI commands in FortiBalancer 8.5 release, please refer to the FortiBalancer 8.5 CLI Handbook. For more information about the GSLB feature, please refer to the FortiBalancer 8.5 User Guide

Note:

The GSLB feature in FortiBalancer 8.4 and 8.4.1 releases is incompatible with the re-architected GSLB feature in FortiBalancer 8.5 release. After the the system upgrade from FortiBalancer 8.4 or 8.4.1 to FortiBalancer 8.5, all the GSLB configurations will be missing and GSLB reconfiguration is required. Therefore, please read the FortiBalancer 8.5 Documentation carefully before the system upgrade.

SOAP API Support

Simple Object Access Protocol (SOAP) API provides a mechanism for operating the FortiBalancer appliance by using the SOAP interface. Administrators can use their client applications to send SOAP requests in XML form to the FortiBalancer appliance (as the SOAP server) and the FortiBalancer appliance returns the result data in XML form to the client applications via HTTP or HTTPS. This provides another management way for the FortiBalancer appliance.

Besides, SOAP API provides the following advantages:

- Customers' management platforms can manage the FortiBalancer appliance after integrating FortiBalancer SOAP APIs.
- SOAP APIs can be integrated with Cloud environments easily. For example, SOAP APIs currently can be integrated with OpenStack to provide the Load Balancing as a Service (LBaaS).

The SOAP Web service is disabled on the FortiBalancer appliance by default. This service must be enabled before administrators access the SOAP service. To ensure the security, the SOAP Web service requires authentication that only allows administrators with the SOAP API access privilege to access the SOAP service.

To help administrators base the interactions between SOAP API and client applications, Array Networks provides a SOAP API SDK that includes SOAP APIs used to implement the Link Load Balancing (LLB), Server Load Balancing (SLB), Secure Sockets Layer (SSL), Access Control, and System Management functions on the FortiBalancer appliance. This SDK file can be downloaded from WebUI of the FortiBalancer.

To use SOAP APIs, administrators must have a good knowledge in the following areas:

- High-level programming language such as C++, Java and Perl
- SOAP
- HTTP/HTTPS protocol
- XML
- TCP/IP protocol

To support this new feature, the following commands are added:

`soapapi on [http|https] [port]`

This command is used to enable the SOAP-based Web service. By default, this function is disabled.

Note:

The port sepcified in this command should be different from the port used in other functions such as XML RPC.

`soapapi off`

This command is used to disable the SOAP-based Web service.

`show soapapi`

This command is used to display the configuration of the SOAP-based Web service.

To support this new feature, the parameter in red is added to the following command:

`user` *`<user_name> <password> [enable|config|`* ***`soapapi`*** *`]`*

soapapi	Users with this access privilege are allowed to run the SOAP API service, but not any CLI command. Besides, users with this access privilege can only login via SOAP API.

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between Autonomous Systems (ASs) on the Internet. The BGP function in FortiBalancer 8.5.0.5 is enhanced to include more BGP features such as BGP capability advertisement and route redistribution, and to support more configuration methods such as resetting theconnection between BGP neighbors.

To support this enhancement, the following commands are added:

show ip bgp route [ip_address/mask|prefix]

This command is used to display the detailed information of the specified BGP route.

bgp capability <ip_address> <option>

This command is used to advertise specified BGP capabilities to the specified BGP neighbor.

no bgp capability <ip_address> <option>

This command is used to cancel the advertisement of the specified BGP capability previously to the specified BGP neighbor.

bgp passive <ip_address>

This command is used to configure the BGP neighbor to which the local BGP router does not actively send the Open packet.

bgp nexthopself <ip_address>

This command is used to set the next hop IP address of the advertised route to the IP address of the local BGP router.

bgp def_orig <ip_address>

This command is used to advertise the default route destined for the local BGP router to the BGP neighbor.

bgp local_as <ip_address> <as_number>

This command is used to set the substitute ASN used by the local BGP router to communicate with the specified EBGP neighbor.

no bgp local_as <ip_address> <as_number>

This command is used to delete the substitute ASN used by the local BGP router to communicate with the specified EBGP neighbor.

bgp shutdown <ip_address>

This command is used to terminate the communication with the specified BGP neighbor.

no bgp shutdown <ip_address>

This command is used to restore the communication with the specified BGP neighbor.

bgp redistribute <option>

This command is used to dynamically redistribute the routes of the specified type into BGP.

no bgp redistribute <option>

This command is used to cancel the dynamical redistribution of the routes of the specified type into BGP.

clear bgp ip [ip_address]

This command is used to reset the connection between the local BGP router and the specified BGP neighbor.

clear bgp asn <as_number>

This command is used to reset the connections between the local BGP router and all BGP neighbors in the specified AS.

To support this enhancement, the following commands are modified:

Before:

bgp router <as_number> <router_id>

This command is used to specify the autonomous system number (ASN) and the router ID.

show ip bgp neighbors

This command is used to display detailed information about BGP neighbors.

Now:

bgp asn <as_number>

This command is used to set the Autonomous System Number (ASN) of the local BGP router. Also, the value range of the "as_number" parameter is changed from 1~65,535 to 1~4,294,967,295.

bgp router <router_id>

This command is used to set the ID of the local BGP router

show ip bgp neighbors [ip_address]

This command is used to display detailed information of the specified BGP neighbor. If the parameter "ip_address" is not specified, the detailed information of all BGP neighbors will be displayed.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Route Health Injection (RHI) Support

Route Health Injection (RHI) is supported in FortiBalancer 8.5.0.5. After the RHI function is enabled, the system will insert or remove the route to a virtual service into or from the routing table based on the health status of real services related to this virtual service and advertise the route bound for the active virtual service to other routers on the network using Open Shortest Path First (OSPF).

After the RHI function is enabled:

- When the health check results of all real services related to a virtual IP address are DOWN, the virtual IP address will be set as INACT (inactive). The system will remove the routing information of the INACT virtual IP address from the routing table and therefore the routing information will not be advertised to other devices on the network.
- When the health check result of any real service related to the inactive virtual IP address is UP, the virtual IP address will be set as ACT (active). The system will inject the routing information of the ACT virtual IP address to the routing table and advertise the routing information to other devices on the network by using OSPF.

To support this new feature, the following commands are added:

ospf rhi {on|off}

This command is used to enable or disable the Route Health Injection (RHI) function. By default, the RHI function is disabled.

show ospf rhi status

This command is used to display the ACT and INACT statuses of virtual IP addresses.

show statistics rhi

This command is used to display the statistics of activated and deactivated virtual IP addresses.

clear statistics rhi

This command is used to clear the statistics of ACT and INACT virtual IP addresses.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook

Layer 7 Performance Enhancement

In FortiBalancer 8.5.0.5, the performance of the appliance is significantly improved. Packet processing capabilities including throughput, requests per second (RPS), and concurrent connections are greatly enhanced.

Enhancements

Server Load Balance (SLB)

Displaying the dynamic persistence session table for groups using persistence methods

In FortiBalancer 8.5.0.5, the administrator can view the details of a group that uses a persistence method by executing the “show slb persistence session” command. To support this enhancement, the following commands are added:

`show slb persistence session` `[group_name]`

This command is used to display the dynamic persistence session table for groups using persistence methods.

Real service connection not restricted by maximum number of open connections when using SLB cookie-based methods

Previously, all connections of a real service are restricted by the maximum number of open connections of the real service. In FortiBalancer 8.5.0.5, the connections of a real service are no longer restricted by the maximum number of open connections when the real service is selected by any of the following SLB cookie methods:

- Persistent Cookie (pc)
- Insert Cookie (ic)
- Rewrite Cookie (rc)
- Embed Cookie (ec)

To support this enhancement, the following commands are added:

`slb overload persistence` *`{on|off}`*

This command is used to enable or disable the function that protects connections related to SLB cookie-based methods from being restricted by the maximum number of open connections of the real service. By default, this function is disabled.

`show slb overload persistence`

This command is used to display the status of the function that protects connections related to SLB cookie-based methods from being restricted by the maximum number of open connections of the real server

Displaying SLB connections

FortiBalancer 8.5.0.5 supports the display of SLB connections on the FortiBalancer appliance

To support this enhancement, the following commands are added:

`show slb connection current <connection_number>` *`[filter]`*

This command is used to display the established Layer 4 connections from the client to the virtual service then to the real service in all the ATCP zones.

`show slb connection live` *`[filter]`*

This command is used to display the newly established connections from the client to the virtual service then to the real service after this command is executed.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Supporting group health check

Besides the basic health check, additional health check, and script health check, FortiBalancer 8.5.0.5 supports the SLB group health check. Administrators can configure the SLB group health check to obtain the status of each real service without configuring health check for real services individually, which simplifies the health check configurations. The supported types of SLB group health check include ICMP, TCP, TCPS, HTTP and HTTPS.

To support this enhancement, the following commands are added:

slb health <health_name> [type] [interval] [timeout] [hc_up] [hc_down] [http_method][url_path] [expected_codes]

This command is used to define a SLB group health check condition.

no slb health *<health_name>*

This command is used to remove the specified SLB group health check condition.

show slb health *[health_name]*

This command is used to display the specified SLB group health check condition.

clear slb health

This command is used to delete all the SLB group health check conditions.

slb group health *<group_name> <health_name>*

This command is used to associate the SLB group health check condition with the specified group.

no slb group health *<group_name> <health_name>*

This command is used to remove the association of the group health check condition with the specified group.

show slb group health *[group_name]*

This command is used to display the association of the group health check conditions with the specified group.

clear slb group health *[group_name]*

This command is used to delete all the group health check conditions of the specified group.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook

Supporting redirecting requests to specified URLs when error codes generated by either the FortiBalancer appliance or real server

IIn FortiBalancer 8.5.0.5 will redirect the requests to the specified URL when the specified error code is generated by either the FortiBalancer appliance or the real server.

Furthermore, besides error codes 901, 902, 903, 904, 905, and 906, the error codes for redirecting the requests now can be the 4xx and 5xx error codes specified in the HTTP RFCs such as RFC 2616.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Secure Socket Layer (SSL)

Changing the length limit of the SSL host name

In FortiBalancer 8.5.0.5, the maximum length of an SSL host name is changed from 255 to 240, in bytes.

Changing the default length of the SSL key pair

Industry standards set by the Certification Authority/Browser (CA/B) Forum require that certificates issued after January 1, 2014 MUST use at least 2048-bit key length. To meet the new requirement, the default length of the SSL key pair is changed from 1024 to 2048 bits. That is, the default value of the "key_length" parameter in the **"ssl csr"** command is changed from 1024 to 2048.

Supporting paged search for downloading CRL files from an LDAP server

In FortiBalancer 8.5.0.5, paged search is supported for downloading CRL files from an LDAP server. With this enhancement, regardless of the importing of the CRL filter file, the FortiBalancer appliance will successfully download CRL files from an LDAP server that supports paged search and has a limit on the number of CRL files.

Link Load Balance (LLB)

Enlarging maximum number of Eroute entries (ID: 43281)

In FortiBalancer 8.5.0.5, the maximum numbers of Eroute entries are enlarged as follows:

System Memory	Maximum Eroute entries
8GB	5,000
16GB	10,000
24GB	20,000
32GB	40,000
64GB	40,000
96GB	80,000
128GB	80,000

Changing the weight range of the wrr and hi methods for LLB links

The weight range of the weighted round robin (wrr) and hash ip (hi) methods for LLB links is changed in FortiBalancer 8.5.0.5. That is, the maximum value of the "weight" parameter in the "**llb link route"** and **"ip eroute"** commands has been changed from 4,294,967,295 to 1,048,576.

Displaying hit NAT entries for matched routes

In FortiBalancer 8.5.0.5, if a route matching the conditions specified in the **"show route match"** command hits a NAT entry, the NAT entry and NAT virtual IP address will also be displayed in the output of the **"show route match"** command. With this enhancement, the administrator will trace packets in a more efficient way

Filtering out NAT entries from the NAT entry table

FortiBalancer 8.5.0.5 allows the administrator to filter specific NAT entries out of the NAT entry table that contains massive NAT entries by using a related IP address.

To support this enhancement, the “ip_address” parameter is added to the following command:

```
show nat table [ip_address]
```

ip_address	Specify the IP address of a NAT entry. The IP address can be the source IP address, destination IP address, or NAT virtual IP address of the NAT entry.

Generating a log when the LLB bandwidth is overloaded

For an LLB link whose bandwidth threshold is specified by the **“llb link route”** command, the system will record a warning-level log when the LLB link is overloaded to help the administrator better monitor the system.

High Availability (HA)

All HA configuration deleted by the “clear config secondary” command

Previously, after the **“clear config secondary”** command is executed, HA configurations except for the unit and link configurations would be deleted. In FortiBalancer 8.5.0.5, all HA configurations will be deleted and restored to default settings after the **“clear config secondary”** command is executed.

Deleting the LCD process

The LCD process is deleted from FortiBalancer 8.5.0.5. Subsequently, the “process_name” parameter in the **“ha hc process”** command cannot be configured as “lcd”.

Supporting HA SSF when DirectFWD is enabled

Previously, after the DirectFWD function was enabled, the configured and enabled HA Stateful Session Failover (SSF) function would become invalid. Now, the SSF function will work properly after the DirectFWD function is enabled.

Note:

When the syncache function is enabled by the “slb directfwd syncache on” command, the SSF function will work properly only when the client side connection is completely established.

Clustering

Fast Failover supporting IPv6 addresses

In FortiBalancer 8.5.0.5, the Fast Failover (FFO) function can be applied to cluster nodes all of which use IPv6 addresses.

Reverse Proxy Cache

Changing the limit of the host name length in a cache filter rule

In FortiBalancer 8.5.0.5, the maximum length of the host name specified in a cache filter rule is changed to 79, in bytes. Previously, the host name length is not restricted.

Removing the function of changing the HTTP version in response from 1.1 to 1.0

The function of changing the HTTP version in response from 1.1 to 1.0 is obsoleted. Therefore, it is removed from FortiBalancer 8.5.0.5.

To support this function change, the following commands are deleted:

http modifyheader http10 {on|off}

show http modifyheader http10

Supporting the rewriting or inserting of the cache-control header in the HTTP response

The administrator can now configure the system to rewrite or insert the value of the cache-control header in the HTTP response from the virtual IP address to the client with a specified directive. The client will take actions indicated by the cache-control directive as caching a copy in the hard disk for future access. With this enhancement, client access, especially the access through a mobile device, will be highly accelerated.

The directive can be a standard cache-control directive defined in RFC 2616 or a cache-control directive agreed by the client and FortiBalancer appliance.

To support this enhancement, the following commands are added:

http rewrite response cachecontrol {on|off} [vs_name]

This command is used to enable or disable the function of rewriting the cache-control header in the HTTP response.

show http rewrite response cachecontrol status

This command is used to display the status of the function of rewriting the cache-control header in the HTTP response.

http rewrite response cachecontrol rule <vs_name> <regex> <cache_directives> <priority>

This command is used to define a rule for rewriting the cache-control header in the HTTP response for the specified virtual service. The rule indicates the operation to be performed by the client according to the specified directives when the URL is matched with the HTTP response.

no http rewrite response cachecontrol rule <vs_name> <regex**>**

This command is used to delete the rewrite rule for rewriting the cache-control header in the HTTP response for the specified virtual service.

show http rewrite response cachecontrol rule [vs_name]

This command is used to display the rewrite rules for rewriting the cache-control header in the HTTP response for the specified virtual service.

clear http rewrite response cachecontrol rule [vs_name]

This command is used to clear the rewrite rules for rewriting the cache-control header in the HTTP response for the specified virtual service.

Supporting the deletion of specific cached objects

Previously, the administrator could use the “clear cache content” command to only delete all cached objects at a time. In FortiBalancer 8.5.0.5, the administrator can delete specific cached objects matching the related host name and URL regular expression.

To support this enhancement, the following command is added:

cache evict <host_name> <url_regex>

This command is used to delete the cache objects that match the specified host name and URL regex.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Supporting importing a customized HTTP error page for all virtual services at a time

Before, the administrator can import a customized HTTP error page of an HTTP error code for a specified virtual service.

Now, the administrator can import a customized HTTP error page of an HTTP error code as the default HTTP error page. The system default HTTP error page will be used for a virtual service only when no customized default HTTP error page is enabled.

To support this enhancement, in addition to a virtual service name, the value of the “virtual_service” parameter in following commands can also be “default”:

http import error <error_code> <virtual_service> <url>

virtual_service	The value of this parameter can be a virtual service name or “default”. If a virtual service name is specified, a customized HTTP error page will be imported for the virtual service. If “default” is specified, a customized HTTP error page will be imported for all virtual services.

http error <error_code> <virtual_service>

virtual_service	The value of this parameter can be a virtual service name or “default”. If a virtual service name is specified, the customized HTTP error page of the specified HTTP error code will be enabled for the virtual service. If “default” is specified, the customized HTTP error page of the specified HTTP error code will be enabled for all virtual services.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

HTTP Content Rewrite

Changing the length of the URL regex to be added into the URL list

The maximum length of the “url_regex” parameter in the **“http rewrite body url list**” command has been changed from 1024 to 512 characters.

General System/Tools

Multicore traffic processing enabled by default

In FortiBalancer 8.5.0.5, the multicore traffic processing function is set to be enabled by default with the support of SLB functions including SLB Domain Name System (DNS), Real Time Streaming Protocol (RTSP), and Remote Desktop Protocol (RDP).

To support this enhancement, the following command is deleted:

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

Changes in SSH IP configuration clearing and synchronization

Previously, the configuration of the SSH IP address would be deleted after the **"clear config secondary"** command was executed. Now, this configuration will be deleted only after the **"clear config primary"** is executed. In addition, before, the configuration of the SSH IP address would be synchronized to or from the peer by the **"synconfig to"** or **"synconfig from"** command. Now, this configuration will not be synchronized after the administrator executes either of the commands.

Removing the function of one-arm L4 SLB acceleration (ID: 47076)

The function of Layer 4 SLB acceleration for the one-arm deployment is obsoleted. Therefore, it is removed from FortiBalancer 8.5.0.5.

To support this function change, the following commands are deleted:

```
system tune accel oa
no system tune accel oa
```

Changing current time value of the "show statistics ip" command

To help the administrator better manage the system, the time zone of the "current time" item in the output of the "**show statistics ip"** command is changed from a GMT value to the system time determined by the **"system timezone"** command.

Supporting tracing SSL activities with TLS 1.2 enabled

Previously, SSL activities could not be traced when Transport Layer Security (TLS) 1.2 was used for communication. Now, when TLS 1.2 is enabled, the FortiBalancer appliance supports the tracing of SSL activities by **the "debug trace ssl"** command.

Removing the function of setting the policy of the NIC package dispatcher

The function of setting the policy of the NIC package dispatcher is obsoleted. Therefore, it is removed from FortiBalancer 8.5.0.5.

To support this function change, the following commands are deleted:

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

Note:

After the system is upgrade to the FortiBalancer 8.5.0.5, an error log "User "fortinet" failed to execute cmd "system tune dispatcher default", code -12(invalid format)" will be generated. To avoid this log after the future reboot, execute the "write memory" command.

Adding SNMP OIDs for getting the number of broadcast and multicast packets

The following SNMP OIDs are now added for getting the number of broadcast and multicast packets in the inbound and outbound directions:

- .1.3.6.1.4.1.12356.23.4.1.22
- .1.3.6.1.4.1. 12356.23.4.1.23
- .1.3.6.1.4.1. 12356.23.4.1.24

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Adding SNMP OIDs for getting inbound and outbound interface throughput

The following SNMP OIDs are now added for getting the inbound and outbound throughput (bits/second) of the interfaces on the FortiBalancer appliance in the last five minutes:

- .1.3.6.1.4.1. 12356.23.4.1.19
- .1.3.6.1.4.1. 12356.23.4.1.20

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Supporting releasing system memory manually

In FortiBalancer 8.5.0.5, the administrator can quickly release occupied system memory by executing the following new command:

```
clear system resource
```

This command is used to release the occupied system memory.

Note:

This command can be used only when network traffic is null or low; otherwise, it may lead to unpredicted errors.

DirectFWD applicable to overlapped interfaces

In FortiBalancer 8.5.0.5, the DirectFWD function is applicable to interfaces configured with the overlap option (used in NUMA) by the **"ip address"** command. interface_name

Supporting binding IP pool to overlapped interfaces

In FortiBalancer 8.5.0.5, when the NUMA SLB (single VIP, reverse mode) is deployed, an IP pool can be bound to an interface configured with the overlap option. To support this enhancement, the parameter "interface_name" is added to the following command:

```
ip pool <pool_name> <start_ip> [end_ip] [interface_name]
```

interface_name	Optional. Specify the name of interface, which should be configured with the overlap option, such as a system, MNET, or bond interface. This parameter is used only when the NUMA SLB (single VIP, reverse mode) is deployed. The default value is null and the pool is bound to the original interface by default.

Supporting RIP, OSPF, and BGP-4 SNMP MIBs

FortiBalancer 8.5.0.5 supports SNMP MIB files of Routing Information Protocol version 2 (RIPv2), Open Shortest Path First (OSPF), and Border Gateway Protocol 4 (BGP-4). The administrator can download standard MIB files (RIPv2-MIB.txt, BGP4-MIB.txt, and OSPF-MIB.txt) from Internet and import the MIB files through the MIB browser to request information about RIPv2, OSPF, and BGP-4.

Supporting link aggregation health check

Link Aggregation Health Check is added to check the health status of a bond interface by sending the ICMP echo request to the destination IP address through each system interface of the bond interface, checking for the corresponding ICMP echo reply, and marking the system interface as “up” or “down”. Consequently, the administrator can use the system interface marked as “up” to transmit traffic. By default, Link Aggregation Health Check is disabled.

To support this enhancement, the following commands are added:

bond health <bond_name> <destination_ip> [interval] [timeout] [up_check_times][down_check_times] [gateway_ip]

This command is used to configure and enable the health check for the specified bond interface.

no bond health <bond_name>

This command is used to delete the health check for the specified bond interface. For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Supporting displaying remaining expiration time of a connection

To help the administrator better trace connections, the remaining expiration time (in seconds) of a connection is added to the output of the “show connection” command.

The following is an output example:

```
FBL(config)#show connection
Proto Local Address Foreign Address state expire Interface
-------------------------------------------------------------------
TCP 10.8.1.193:50345 10.3.1.195:50345 ESTABLISHED 59 su
ICMP 10.3.0.2:* *:* CLOSED 0 unknown
TCP 10.3.0.2:* *:* LISTEN 0 unknown
UDP 10.3.0.2:* *:* CLOSED 0 unknown
AN(config)#show connection
"ip=172.16.77.86,port=80,state=ESTABLISHED,format=count"
Host: FBL
 Current time: Thu Dec 27 15:31:33 GMT (+0000) 2013
TCP Total: 0
 ESTABLISHED: 0
UDP Total: 0
```

Also, when “format=count” is specified, the time zone of the “current time” item in the command output is changed from a Greenwich Mean Time (GMT) value to the time value determined by the “system timezone” command.

Supporting processing the packet whose destination MAC address is not local

Before, the FortiBalancer appliance would process only the packet whose destination MAC address is that of an interface on the FortiBalancer appliance. In FortiBalancer 8.5.0.5, the FortiBalancer appliance will process a packet regardless of its destination MAC address.

To support this enhancement, the following commands are added:

interface promisc <interface_name> {enable|disable}

This command is used to enable or disable the promiscuous mode of the specified system interface. When the promiscuous mode is enabled, the specified system interface will process the packets whose destination MAC address is not local.

clear interface promisc

This command is used to disable the promiscuous mode of all system interfaces.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Enhancing the XML RPC function

The XML RPC function allows the administrator to gain access and configure the system from remote locations. By default, the XML RPC function is disabled. In FortiBalancer 8.5.0.5, the XML RPC function is enhanced in the following ways:

- Supporting all CLI commands

  Previously, the XML RPC function did not support interactive commands that require the administrator's further confirmation. For example, the XML RPC function did not support the "clear health import response" command, after executing which the administrator needs to input "YES" to confirm the deleting. Now, the XML RPC function supports all such commands as the administrator has already input "YES".

- Returning error messages for failed CLIs to the client

  Previously, when a CLI was failed to be executed through XML RPC, the returned message might be "xmlrpc command successful", which would mislead the administrator. Now, the actual execution result will be returned to the client to help the administrator accurately configure the system.

In addition, in FortiBalancer 8.5.0.5, the configuration of the XML RPC function is simplified to provide more user-friendly experience. The detailed changes are as follows:

- Default XML RPC port

  Before, the default XML RPC port for HTTPS is 9999 and for HTTP is 9980. Now, port 9999 is used as the default port for both HTTPS and HTTP.

- Function of the "xmlrpc port" command

  Before, the "xmlrpc port" command is used to change the XML RPC port of the protocol (HTTP or HTTPS) used for the last time. Now, the "xmlrpc port" command is used to change the XML RPC port of both HTTP and HTTPS.

SSL log enhancement

In FortiBalancer 8.5.0.5, SSL logs are enhanced to provide the client IP address and suggested actions when an error occurs.

Real-time tracing of the SSL activities supporting IPv6 addresses

In FortiBalancer 8.5.0.5, the administrator can use the "debug trace live ssl" command to trace SSL activities with both IPv4 and IPv6 address in real time.

The parameter in red in the following command supports both IPv4 and IPv6:

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

Supporting the setting of the wait time for data transmission

To help the administrator better configure the FortiBalancer appliance to meet differentiated application requirements, the administrator can set the wait time of the FortiBalancer appliance for data transmission in FortiBalancer 8.5.0.5.
To support this enhancement, the following commands are added:

`system tune tcp timewait [timeout_value]`

This command is used to set the wait time for data transmission. It is recommended that you contact Fortinet Customer Support before changing the default settings.

`no system tune tcp timewait`

This command is used to reset the wait time for data transmission to the default value, which is 50 seconds.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Enhancement in the RFC 5424 syslog function (ID: 36525)

In FortiBalancer 8.5.0.5, the RFC 5424 syslog function is enhanced to allow the administrator to clear the settings of the MSGID field in the headers of all RFC 5424-compliant system logs using the following new command:

`clear log rfc5424 msgid`

This command is used to clear the settings of the MSGID field in the headers of all RFC 5424-compliant system logs.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Debugging monitor supporting specified modules (ID: 36027)

In addition to tracing system debugging information, the debugging monitor function now allows the administrator to trace the status of the specified modules on the FortiBalancer appliance.

To support this enhancement, the following command is modified:

Before:

`debug monitor on`

Now:

`debug monitor on [module_name]`

module_name	Optional. Specify the module name. The value can be SSL, SLB, LLB, GSLB and uProxy. The value is case insensitive. Multiple modules can be specified by repeatedly executing this command.

To support this enhancement, the following command is added:

`no debug monitor <module name>`

This command is used to delete the debugging monitor function for the specified module.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

Supporting specifying an LLB link to trace packets sent to the specified IP address or host

The route tracing function is enhanced to allow the administrator to trace the route of a packet sent to the specified IP address or host by sending the packet through a specific LLB link.

To support this enhancement, the following commands are modified:

Before:

```
traceroute {ip|hostname}
traceroute6 {ipv6|hostname}
```

Now:

```
traceroute {ip|hostname} [gateway_ip]traceroute6 {ipv6|hostname}
[gateway_ip]
```

gateway_ip	Optional. This parameter specifies the IPv4 or IPv6 address of the gateway of an LLB link route. When this parameter is specified, the packet is sent to the specified IPv4 or IPv6 address or host through the LLB link determined by this parameter.

For details, please refer to the FortiBalancer 8.5 User Guide and CLI Handbook.

WebUI

Supporting statistics of certain SLB policies

In **Admin Tools > Graph > Graph Monitoring > Predefined Graphs** and **Admin Tools > Graph > Graph Monitoring > User Defined Graphs**, the administrator can view the statistics of the redirect, qos body, header, hash url, radsid, raduname policies in the displayed graph.

In **Server Load Balance > Monitoring > Report**, after the administrator clicks the Preview action list, the statistics of the configured hash url, file type, and redirect policies are displayed in the graph.

Providing suggested actions in logs

In **Admin Tools > Graph > Logging > Disabled Log > Log ID List**, the suggested

action is added to each log to help the administrator troubleshoot the fault.

Supporting exporting a saved configuration file to the local PC through WebUI

In **Admin Tools > Config Management > Backup**, the administrator can export a saved configuration file to the local PC by clicking the **Saved File** radio button in the Running Configuration Backup area, selecting a saved file in **the Configuration on Saved File** table, and clicking the Export action link.

Upgrade paths

Hardware model support

FortiBalancer 8.5.0.5 supports:

- FortiBalancer-400
- FortiBalancer-1000
- FortiBalancer-2000
- FortiBalancer-3000

Upgrading from previous releases

Ensure the box is running release 8.0.x or higher.

- Ensure there is a network connection between the FortiBalancer and the HTTP/FTP server that contains the software file.
    - Ensure that the HTTP/FTP server is either on the same subnet or that a default gateway set up.
    - Ensure FortiBalancer has read access to the file on the server.

If you do not update the firmware in this order, your configuration might 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.

Server Load Balance (SLB)

Failing to upload an 8GB or larger file through the HTTPS virtual service

Uploading a file to the real server through the HTTPs virtual service on the FortiBalancer appliance failed when the file size was equal to or larger than 8GB. This issue has now been resolved.

Attachment of a health check to a HC checker list lost after system reboot

After a health check had been attached to a HC checker list by the **"health app"** command, the configuration of the attachment was lost after system reboot. This issue has now been resolved

Secure Socket Layer (SSL)

Virtual service down when DES-CBC-SHA was used and plain hello message from client not multiple times of the block

When the cipher suite DES-CBC-SHA was used and the SSL handshake was completed, virtual services would become down if the plain hello message sent from the client was not multiple times of the block. This issue has now been resolved.

WebUI

Displaying duplicated information for a virtual service

In ***Server Load Balance > Monitoring > Summary***, the information of a virtual service whose port range was specified would be displayed twice in the table. This issue has now been resolved.

Failing to delete a cache filter rule

In ***Proxy > Caching Proxy > Cache Settings > Cache Filter***, an existing cache filter rule with a regular expression could not be deleted after the administrator selected the rule and click the Delete action link. This issue has now been resolved.

Known issues

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

Server Load Balance (SLB)

FTPS SLB failing to reply the ACK packet to the client (ID: 47876)

When the FTPS SLB function is configured, the virtual IP address of the FTPS SLB fails to reply the ACK packet to the client. As a result, the client resets the connection. This issue will be resolved in the next patch release.

Failing to access a virtual service whose associated real service is another virtual service when DirectFWD enabled

When the DirectFWD function is enabled, the access to a virtual service whose associated real service is another virtual service on the FortiBalancer will fail.

Content length of the HTTP request should be less than 4096 bytes

If the content in the HTTP request header is larger than 4096 bytes, the connection between the client and the virtual IP address will be reset.

Not supporting HTTP request with the option method being asterisk (*)

The HTTP request whose Option method is the asterisk (*) is not supported by the FortiBalancer appliance.

High Availability (HA)

Displaying incorrect prompt when restoring the configuration from the last “write memory” operation

When the configuration from the last “write memory” operation, in which no HA local unit is defined, is being restored by the “config memory” command, the system will display the “Please define local unit firstly” prompt but the following default configurations actually configured:

- `ha hc cpu overheat 0`
- `ha hc cpu utilization 0`
- `ha hc memory mbuf 0`
- `ha hc sslcard 0`

Reverse Proxy Cache

Not completely hiding backend server from client if HTTP response header fields extended over multiple lines

If the header fields of the response from the backend server are extended over multiple lines, the server header cannot be completely hidden by the **“http mask server on”** command. Only the first line will be hidden.

Not supporting HTTP requests with header fields extended over multiple lines

The HTTP requests whose header fields are extended over multiple lines are not supported by the FortiBalancer appliance.

WebUI

Allowing login through WebUI with external authentication when local database has higher priority

When the local database is configured to be preferentially used by the "**admin aaa**" command, and the username exists in both local database and external authentication server with different passwords, the administrator can still log into the FortiBalancer appliance through WebUI with external authentication.

WebUI will hang until traceroute times out

In ***Admin Tools > Troubleshooting > Tools***, after the administrator configures the traceroute function with a specified timeout value, the WebUI will hang until the running time of traceroute reaches the timeout value.