FortiWAN Release Notes

Version v5.2.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

May 17, 2019
FortiWAN v5.2.1 Release Notes
00-400-000000-20181031

TABLE OF CONTENTS

Change log

Date	Change Description
5/17/2019	FortiWAN 5.2.1 Initial Release
4/1/2019	FortiWan 5.2.0 Initial Release
1/22/2018	FortiWAN 5.1.2 Initial Release

Introduction

This document covers the main features, installation instructions, and known issues for the v5.2.1 release.

FortiWAN is a Link Load Balancing, Multi-Homing, and Tunnel Routing system that distributes outbound and inbound internet traffic across multiple WAN links of differing technologies as well as builds multi-link VPNs between sites.

The FortiWAN E-series features a new design and operating system (OS) which offers a faster and more configurable product that works in conjunction with the FortiWAN Controller to meet your SD-WAN needs.

Build number 0370.

Main Features

This section highlights the main features of the FortiWan v5.2.1 release.

Supports new hardware model 1000E

FortiWAN v5.2.0 supports a new hardware model, 1000E, which has 4x 1G Copper, 4x 1G SFP and 2x 2 10G SFP+.

For guidance on the FortiWAN 1000E installation process, refer to the 1000E Quick Start Guide (QSG) on https://docs.fortinet.com/product/fortiwan/ > Search Hardware > (drop down) 1000E QSG.

Supports KVM/Xen/Hyper-V

Besides VMWare ESXi, FortiWAN v5.2.0 also supports deploying VM instances to more hypervisors, including KVM, OpenXen and Hyper-V.

For guidance on the FortiWAN-VM installation process, refer to the FortiWAN-VM Installation Guide.

Supports 4G LTE modem as WAN link

FortiWAN v5.2.0 supports a single USB 4G modem as WAN link.

Typical QMI and cdc_ether driven USB modems are supported, including several popular products: D-Link DWM-222, Huawei E3372h-607, Huawei EB372h-155.

For more detail information please contact Fortinet support team.

Supports packet-based tunnel load balancing

Traditional link-load-balance algorithms are based on sessions, meaning, once a session is established, the subsequent packets will be forwarded by the fixed egress link that was selected for the first packet, thereby not using other links.

With the per-packet based load balancing, v5.2.0 will select an egress link for each packet, thus better utilizing the bandwidth of all tunnel links in a specific link-group thus to improve the effectivity.

Supports Fast & Quality route algorithm

Supports new algorithms for link selection, based on the lowest latency or lowest retransmit ratio.

Supports benchmark test on IPsec links and link groups

Adds CLI commands and GUI to run performance test on a single IPsec tunnel or links in a specific link group. System will generate traffic and calculate the round-trip time, packet loss rate and bandwidth to let users better know the current situation of the link or link-group.

Supports manually clear session

Adds command to show and clear filtered or all current sessions.

Supports more diagnose tools

Adds diagnose command to advertise ARP and detect IP conflict.

Upgrade notes

FortiWAN & Controller compatibility

If FortiWAN 5.2.1 is deployed, Controller 1.5.0 (or above) is required.

Supported hardware models & VM

The FortiWAN 5.2.1 release supports the following platforms:

- FortiWAN 30E
- FortiWAN 200E
- FortiWAN 1000E
- FortiWAN HyperV
- FortiWAN KVM
- FortiWAN VM
- FortiWAN OPENXEN
- FortiWAN XENSERVER
- These virtual platforms share the same range of VM licenses that determine the allotted bandwidth (10Mbps, 20Mbps, 50Mbps, 100Mbps, 200Mbps, 500Mbps, 1000Mbps, 2000Mbps)

Installation instructions

For guidance on the FortiWAN 30E, FortiWAN 200E, or FortiWAN 1000E installation process, refer to the Quick Start Guide (QSG).

For guidance on the FortiWAN-VM installation process, refer to the FortiWAN-VM Installation Guide.

Resolved Issues

Bug ID	Description
552570	When the vpn changes ip address, the routing algorithm for least-rtt underlay will fail
547327	After changing the ip range of the dhcp server in Fortiwan, the client gets a 0 subnet mask.
551602	In special situations, boxes may fail to connect to the Controller due to route searching failure
547699	In special situations, boxes may fail to connect to the Controller due to route searching failure
551676	The packet loss rate is always 100% on some overlay links
552283	Occasionally the box fails to register to Controller
556808	When restoring configuration, IPsec tunnels may fail to be established
557111	Unknown operation causes no reply from peer VTI interface and link quality detect failure
553992	In special cases the reverse traffic fails to match per-packet scheduling tunnel
550111	For some tunnels, the probe packet did not reach the peer after tunnel was sent.

Known issues

The following issues have been identified in this release. For inquiries about a particular bug or to report a bug, contact Fortinet Customer Service & Support.

Bug ID	Description
484109	The FortiWAN boot-up process may slow down if you have more than 1024 firewall rules configured. **Workaround:** To prevent a slowdown, do not add more than 1024 firewall rules.
484657	When updating the number of connection limits in a connection-limit policy, the new policy will not apply to older existing connections. The updated connection-limit policy will only apply to new connections. **Workaround:** Once the old connections expire or disconnect, the connection number will be accurately limited by the policy.
499016	If you use IKEv1, FortiWAN cannot establish multiple VPN tunnels with the same remote IP while using different local IP addresses. **Workaround**: If multiple IPsec tunnels are needed, use IKEv2 instead.
502556	Data connections will not be established if the Virtual Server is configured with non-21 ports for FTP. This is currently a limitation as FortiWAN only supports standard port 21 for FTP application in Server Load Balance.
502848	The GLB function will not work when a FTP virtual server with port 21 is configured. **Workaround:** Do not configure FTP Server Load Balance if you need to use the GLB function.
505926	The GLB function may not respond if more than 96 members are configured in one virtual-server pool. **Workaround:** To prevent this issue from occurring, do not add more than 96 members per virtual-server pool.
514604	The FortiWAN boot-up process may slow down if you have more than 1024 VLAN interfaces configured. **Workaround**: To prevent a slowdown, do not add more than 1024

Bug ID	Description
	VLAN interfaces.
537151	Indicators of FWN-1000E's fiber ports still light up when cables are connected but status is set to down via CLI **Workaround**: NIC driver behavior
538642	FWN-1000E can't detect fiber SPF if system boots up with copper SFP plugging in port5-8 **Workaround:** NIC driver behavior; rebooting the box will resolve the issue
555336	30E does not display logs on CLI **Workaround**: Use GUI to check logs
555031	SNAT does not work when using the secondary IP on a soft-switch interface **Workaround**: Don't use SNAT in such a scenario
540986	In vip rules if extport is non 443 port and mappedport is 443, the rule does not take effect **Workaround**: N/A