AscenLink LinkOS V7.2.19 B7966

Release Notes

AscenLink Release Notes – LinkOS V7.2.19 B7966

February 21, 2017

Revision 1

Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

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	http://training.fortinet.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: ascenlink@fortinet.com

Table of Contents

Introduction

Summary

This LinkOS firmware V7.2.19 B7966 is the twentieth build for Fortinet AscenLink V7.2. From this release, the Generic Receive Offload (GRO) mechanism on each of AscenLink's network interfaces is disabled by default for better Tunnel Routing performance. Several issues about Tunnel Routing and Optimum Route were fixed in this release. BIND, TNP, OpenSSL and PHP were upgraded to fix security vulnerabilities. This document provides a list of resolved issues, upgrade procedures and support information for AscenLink LinkOS V7.2.19 B7966. Please review all sections of this document prior to upgrading your device.

Supported Models

LinkOS **V7.2.19 B7966** is the latest AscenLink firmware version released for AscenLink-700, AscenLink-5000 and AscenLink-6000.

Compatibility

LinkOS **V7.2.19 B7966** provides support and is compatible with all versions of LinkReport. AscenLink-6000 requires LinkOS V6.1, or higher.

Updated Features in V7.2.19 B7966

Mantis ID 397295

From this release, the Generic Receive Offload (GRO) mechanism on each of AscenLink's network interfaces is disabled by default for better Tunnel Routing transmission performance. The parameter `genericreceive-offload` of CLI command `sysctl` added in release 7.2.14 to enable/disable GRO is removed; now it is unable to enable GRO on AscenLink.

Resolved Issues in V7.2.19 B7966

Mantis ID 406516

The BIND package employed by AscenLink was upgraded to 9.10.4-P5 to fix security vulnerabilities CVE-2016-9444, CVE-2016-9147, and CVE-2016-9131.

Mantis ID 405964

The ARP detection of AscenLink HA mechanism would go wrong if the target LAN/DMZ port was configured with VLAN tags. The VLAN tags were missed in the ARP queries. It would fail to deliver the ARP packets and therefore cause an incorrect HA takeover.

Mantis ID 405127

The OpenSSL employed by AscenLink was upgraded to 1.0.2k to fix security vulnerabilities.

Mantis ID 405027

In a HA deployment, the master unit's heartbeats might be stuck if it was busy resending configurations to the slave unit (caused by failure in synchronization, such as checksum error). This might cause incorrect HA takeover (both units became master) if an ARP detection just happened at the same time.

Mantis ID 403376

Optimum Route's dynamic detection might fail to receive the detection responses on some WAN links if both the following statements were true:

- Optimum Route was applied to many WAN links (such as 25 WAN links) in an Auto Routing policy.
- The WAN links had very low latency (less than 1ms) between AscenLink and the detection target.

Optimum Route algorithm, therefore, might give an incorrect routing path due to the incomplete detection result.

Mantis ID 402505

When logging to an AscenLink's Web UI from a different time zone, the displayed traffic statics line charts of Bandwidth Management and Tunnel Routing (*Statistics* > *BM* and *Statistics* > *Tunnel Traffic*) had the x-axis scale in the time zone of the local host browsing the statistics. It is supposed to be in the time zone where the AscenLink is located.

Mantis ID 402438

The PHP package employed by AscenLink was upgraded to v5.6.30 to fix security vulnerabilities.

Mantis ID 401412

Configuration of a VLAN would disappear on the Web UI after the configuration was exported and imported if the VLAN was mapped to None.

Mantis ID 401316

It failed to enable OSPF on a LAN port that was mapped to an aggregated port.

Mantis ID 401042

In a Tunnel Routing network with Default Rule was enabled for a Tunnel Group between two AscenLink units, one would fail to receive the information (to establish the routing rules) if one of the following statements was true to the corresponding Tunnel Group on its opposite unit:

- had many IP addresses, ranges or subnets configured in Default Rule.
- had any Source field in Default Rule configured as LAN/DMZ, and there were many LAN/DMZ subnets (probably more than six subnets) deployed to the unit.

Mantis ID 399574

DNS Proxy replaces destinations of the matched DNS requires with the first-detected reachable DNS server configured to the selected WAN link. However, DNS Proxy would incorrectly replace the destinations with 0.0.0.0 if all the configured DNS servers of the WAN link were unreachable. It is supposed to try another WAN link according to the specified algorithm when it happens.

Mantis ID 399365

IP Conflict Test (*System* > *Diagnostic Tool*) did not work with redundant DMZ ports.

Mantis ID 397146

The NTP package employed by AscenLink was upgraded to 4.2.8p9 to fix the security vulnerabilities.

Mantis ID 396532

Optimum Route's dynamic algorithm had a mistake in calculating the costs (round trip time, traffic load and the weights) of WAN links, which results in unexpected routing path.

Mantis ID 395731

In a HA deployment with turning on its debug log, the following issues would occur if a SNMP client continued sending SNMPGET requests to the slave unit:

- The SNMP client would receive no responses from the slave unit.
- Web UI would fail to display the summary page (*System* > *Summary*) after closing and re-logging to the Web UI.
- Error message "Peer information is not available" would pop up after closing and re-logging to the Web UI several times

This happened on firmware version v7.2.3 and later running on platforms AL-700 and AL-5000.

Mantis ID 395015

AscenLink set no maximum limitation to DNS Proxy's Intranet Source and Proxy Domains rules, but always the first 26 (for AL-200) and 56 (for AL-5000 and AL-6000) rules worked, the rest of the rules were ineffective.

Mantis ID 393778

Miss-detection sometimes happened to Optimum Route detection algorithm. A few of the candidates (the participating WAN links) were missed and it might resulted in an unexpected routing path.

Mantis ID 393762

The Optimum Route detection algorithm would always decide a routing path among four of the WAN candidates if there were more than four WAN links participated in an Auto Routing policy with Optimum Route algorithm. The rest WAN links would never be chose even if they were in better condition.

Mantis ID 393755

Even if a target was unreachable through a WAN link, Optimum Route sometimes routed packets destined to the target to the WAN link. Optimum Route should choose a path from other WAN links that are serviceable for the target.

Mantis ID 393754

The dynamic evaluation results that cached in a specified aging period for Optimum Route to pick the optimum WAN link would never be cleared (even if they were really expired) if the results were generated in the first five minutes of AscenLink's uptime. These cached results would continue affecting Optimum Route's calculation and cause an unexpected routing path being given.

Mantis ID 393409

It failed to access the IPv6 addresses deployed in the DMZ of a dual-stack bridge-mode multiplestatic-IP WAN link from external networks.

Firmware Upgrade Procedures

Upgrading Information

- Note that only versions later than V6.5 B4175 (V6.5 B4175 is included) are supported for upgrade to V7.2.19 B7966. To upgrade to V7.2 from V6.5 or V7.0, it requires an upgrade of V7.1 first (See "AscenLink V7.1 Firmware Upgrade Quick Guide", which is available from FortiCare at https://support.fortinet.com). For V7.0 (B5338 and B5246), please update to V7.0 B5526 **first** before updating to V7.2.19 B7966.
- System with demonstration licenses cannot be upgraded to R7.1 and later. Please contact Fortinet at ascenlink@fortinet.com for information on updating these systems to NFR units.
- AscenLink's firmware image and upgrade license key are available from FortiCare at https://support.fortinet.com once customer's AscenLink Serial Number is registered. However, because of US Government export restrictions on Tunnel Routing technology, all registration to FortiCare for customers using V7.0 or V6.5 **MUST** be "ordered" via your distributor and Fortinet Order Management. Registrations for in-warranty systems will be at no charge, as usual, but Fortinet must have end-user visibility and update its databases in order to support AscenLink. The SKU for ordering a Registration is **AL-REGI-FC**. This is a one-time requirement. Future upgrades will be automatically available to in-warranty customers via the FortiCare website, without the need for additional ordering.

Upgrade procedure

Upgrade from V6.5, V7.0 B5526, V7.1 or V7.2.x

After registering to FortiCare, the License Key can be generated inside FortiCare (for in-warranty Serial Number).

Start the upgrade procedure as follow:

- Always back up your system configurations and store in a safe place before upgrading (and downgrade).
- Log on to AscenLink as Administrator and go to [System > Administrator] page.
- Click Update to start the upgrade procedure
  - Click Browse to select the path where the new firmware image is saved
  - Enter the Update Key you received from Fortinet
  - Select Upload.
- Be patient while firmware is being upgraded. During the upgrade, do not turn off the system, unplug the power or repeatedly click the Submit button.
- The message "Update succeeded" will appear after the upgrade is completed. Please reboot the system afterwards for the firmware to take effect.

Getting Help

For customer support of Fortinet's AscenLink products shipped, please contact your local Fortinet AscenLink channel partner or http://www.fortinet.com/support/contact_support.html. AscenLink system must be registered to FortiCare to receive support.

Patches and updates are regularly released for Fortinet's AscenLink products. For access, please register at https://support.fortinet.com/ or contact ascenlink@fortinet.com.