**SDWAN – zWAN**

zWAN 1.2 - Release Notes

Version No: 1.2.-01.1023



*Published by Software Engineering*

AMZETTA-CONFIDENTIAL

Copyright AmZetta Technologies

5555 Oakbrook Pkwy Suite 280, Norcross, Georgia 30093, U.S.A.

All Rights Reserved

Confidential, Unpublished Document

Property of AmZetta Technologies

Logo

Description automatically generated

Table of Contents

Contents

[1. Component Information 3](#_Toc152595596)

[2. Release Candidates 3](#_Toc152595597)

[3. Supported Devices 4](#_Toc152595598)

[4. vCPE System Requirements 4](#_Toc152595599)

[5. FTP PATH 4](#_Toc152595600)

[6. GIT PATH 5](#_Toc152595601)

[7. Product Features 6](#_Toc152595602)

[8. SALIENT FEATURES 7](#_Toc152595603)

[9. New Features / Enhancements 16](#_Toc152595604)

[10. Bug Fixes 16](#_Toc152595605)

[11. Known Issues/ Limitations 16](#_Toc152595606)

[12. Notes & Recommendations 16](#_Toc152595607)

# **Component Information**

|  |  |
| --- | --- |
| **Project Tag Name** | **sdwan** |
| **Firmware Revision** | **1.2-01.1023** |
| **Firmware Build Date** | **November 29, 2023** |
| **Git Commit** | **75485e5bf1069211a7536bba6ae51e8d0aa74f0** |
| **X86 image (vCPE, Kettop & Lanner)** | **cpe-base-1.2-01.1023-5166.qcow2.xz, 1.36 GB (Md5 checksum)** |
| **X86 Patch** | **cpe-fw-package-1.2-01.1023-5166-Nov29-2023-153901.bin, 749 MB** |
| **BPI R64 Image** | **image-bpir64-1.2-01.1023-Nov29-2023-142414.img, 7.28 GB** |
| **BPI R64 PATCH** | patch-bpir64-1.2-01.1023-Nov29-2023-150359.bin, 398 MB |
| **BPI R3 Image** | **image-bpi-r3-1.2-01.1023-Nov29-2023-143200.img, 7.28 GB** |
| **BPI R3 Patch** | **patch-bpi-r3-1.2-01.1023-Nov29-2023-150548.bin, 431 MB** |
| **cWAN801 Image** | **image-cwan801-1.2-01.1023-Nov29-2023-142414.img, 14.5 GB** |
| **cWAN801 Patch** | **patch-cwan801-1.2-01.1023-Nov29-2023-150453.bin, 398 MB** |
| **AMZ z25 Image** | **Not available for 1.2-01.1023 build** |
| **AMZ z25 Patch** | **Not available for 1.2-01.1023 build** |

# **Release Candidates**

1. X86 - Base Image and Patch image
2. BPI R64 - Base Image and Patch image
3. BPI R3 - Base Image and Patch image
4. cWAN 801 - Base Image and Patch image
5. Templates
6. vCPE deployment script

# Supported Devices

* X86 Kettop (Celeron for Branch, i7 for Concentrator)
* X86 Lanner NCA-4010 (As Concentrator)
* X86 vCPE’s
* BPI R64
* BPI R3

# vCPE System Requirements

* **HOST HARDWARE for VCPE**
* Must support Linux kernel 4.19 or greater.
* A minimum of 3 N/W adapters are recommended.
* Must have minimum 8G RAM and 8 core CPU.
* To run as vCPE (host system should support VT-x and VT-d)

# FTP PATH

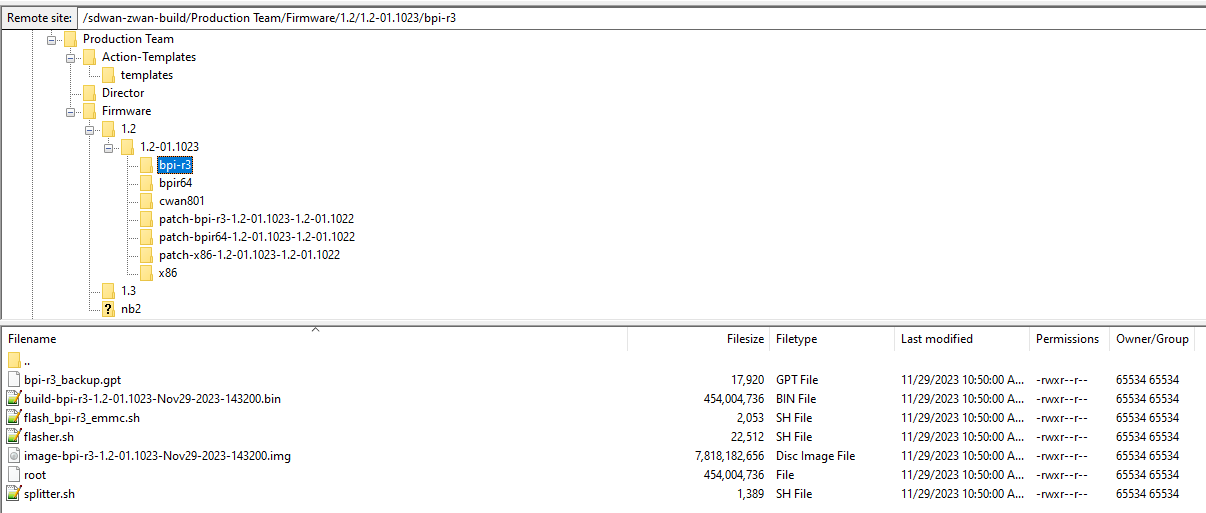
CPE Firmware Images, Templates and vCPE deployment scripts can be found in the below location

FTP: USSFTP.AMZETTA.COM

Username: zWAN

Password: 0WGtbTrg

PATH : \sdwan-zwan-build\Production Team



# GIT PATH

HW\_Test matrix report, Build Release notes and Installation documents can be found in the below location.

|  |  |
| --- | --- |
| HW Test report | <https://gitlab.amzetta.com/sdwan/zwan-doc/-/blob/master/Production%20Team/1.2/1.2-01.1023/FW_HW_Matrix.xlsx> |
| ARM Installation, x86, vCPE | <https://gitlab.amzetta.com/sdwan/zwan-doc/-/blob/master/Installation/zWAN_CPE_Firmware_Installation_on_different_platforms.docx> |
| Build release notes | <https://gitlab.amzetta.com/sdwan/zwan-doc/-/blob/master/Production%20Team/1.2/1.2-01.1023/zWAN_1.2__-_ReleaseNotes.docx> |
|  |  |

# Product Features

* INTRODUCTION

zWAN is Amzetta’s implementation of SDWAN solution. zWAN is targeted towards small to midsize enterprises that are looking to incorporate SDWAN into their networking infrastructure.

Amzetta’s zWAN is composed of two major parts

* A centralized management/orchestration server (or cluster of servers) responsible for the management plane and certain control plane activities.
* A distributed edge controller(s) that is responsible for data-plane activities.
* HIGH LEVEL ARCHITECTURE



# SALIENT FEATURES

* Topology support – Hub and spoke, hybrid topologies.
* Centralized Management and multi-tenancy.
  + Centralized Policy and Auto Policy
  + Active directory, open ID
  + Multi-factor authentication
  + Role based authorization
* Clustered Management and Orchestration Servers
  + Failover, load balancing.
  + Scale out as more edge controllers are added.
* Data plane separate from Management and control planes
  + Data traffic does not flow through the management servers. Customer’s data is not passed to management servers.
  + Enables SDWAN as a service.
* Monitoring and Reporting
* Edge controller supports heterogeneous hardware
  + ARM, x86/64 CPE, VM
* Value Added Functions
  + Multi-path WAN connectivity
    - IPSEC/SSLVPN one-to-many tunnel
    - Multiple tunnels
    - Asymmetric WAN links
  + Inbound/outbound load balancing across multiple WANs
  + Fault tolerance, automatic outage detection and recovery
  + QoS Tagging, Flow classification and prioritization.
  + TWAMP, flow optimizer, IPFIX
  + Dynamic routing, BGP, OSPF

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Feature | | | Description | | Status | |
| Deployment | VM | | The zWAN EC can be installed as a VM on any x86/64 based uCPE | |  | |
| Cloud Deployment | | The zWAN EC can be installed in the clients cloud. | |  | |
| ARM | | Banana PI R64 (MT7622), BPI-R3 | |  | |
| X86/64 | | Lanner NCA 4010 | |  | |
| Topology Support | Hub and spoke | |  | |  | |
| Branch to Branch | |  | |  | |
| Zero touch provisioning | | |  | |  | |
| Multiple WAN Interfaces | | |  | |  | |
| MPLS/ILL/Broadband | | |  | |  | |
| PPPoE | | |  | |  | |
| Multiple 3G-4G/5G LTE | SIM Slot | | Banana PI R64 (MT7622), BPI-R3, CWAN801 | |  | |
| Port | | MiniPCI or M.2 (refer HW model) | |  | |
| 10/100/1000 Mbps RJ-45 WAN Ethernet | | | Number of ports based on HW | |  | |
| Interface Alias | | | 2 WAN and 3 LANS ( refer hw model) | |  | |
| IPv6 | | | Basic IPv6 support at WAN interface | |  | |
| IPS/IDS | | | Minimum 2GB RAM and 4 Core CPU ( refer hw model) | |  | |
| Compression | | |  | |  | |
| Multiple 1000 Mbps RJ-45 LAN Ethernet | | | Number of ports based on HW | |  | |
| **Security** | | | | | |
| Stateful Inspection Firewall | | Stateful firewall services with ACL and/or Time based ACL to provide supervision and control | |  | |
| App aware firewall | | With Custom Application definition | |  | |
| Web/URL Filtering | | Allow or deny access to certain class of websites according to predefined set of policies. | |  | |
| Block infected/malicious domains | | * FQDN based Category and FQDN (flow classification, global block) | |  | |
| DDOS mitigation | | DNS (QA should not have any WAN ip’s connected to a 10.x network. For DDOS, 10.0.0.0/8 ip’s are considered as spoof) | |  | |
| IPD/IDS | |  | |  | |
| Device Authentication | | Certificate based authentication of devices | |  | |
| **Load Balancing and Failover** | | | | | |
| Load balance across WAN links | | Load balance across multiple broadband paths based on load balancing algorithms efficiently using all available WAN bandwidth. For example during congestion due to high amount of traffic, high bandwidth applications like Video Conferencing will be provisioned with maximum bandwidth required for optimal performance. | |  | |
| Recovery after a failure | | If a link carrying application traffic fails, the application traffic will be moved from failed link to a functioning link in seconds without any application timeouts and disconnects | |  | |
| Parallel Transfer | | Aggregates multiple links to provide more bandwidth for intensive applications like video/multimedia streaming, video conferencing and backup. | |  | |
| Link monitoring | | Monitor link flaps, link quality. If the link is not stable, the link is set to a monitor state. Once the link is back to stable state, then traffic sent through that link. | |  | |
| **Flow Optimization and control** | | | | | |
| The flow classification applies various filters over the network packets and takes specific actions based on the match. | | The following actions are covered.   * Load balancing * QoS * Firewall   The following filters can be applied on the input and output interfaces.   * Source IP (range) * Destination IP (range) * Packet size * DSCP Mark * Application * IP protocol type * Port (range) * TCP Flag * Connection State * Deep packet inspection (L3, L4) * Time, connection limit, bandwidth usage etc. | |  | |
| Dynamic WAN Link Selection and Load Balancing based on criteria such as reachability, delay, packet loss, jitter, LTE Signal Quality | | Net Balancer | |  | |
| **Traffic Steering** | | | | | |
| Traffic steering is used when the router is configured with multiple internet connections or tunnels for reasons such as balancing outgoing traffic, maintaining network redundancy and faults for one or multiple lines. The LAN traffic is distributed by using various policies over multiple internet gateways or tunnels (connection based load balancing and steering). Traffic can also be steered through a single interface. The detection of traffic is done by the flow classifier module and then steered based on the configured policy | | | | | |
| Branch Mode | | Gateways can be grouped based on the LAN network to form a separate load-balancing group. | |  | |
| Internet Breakout | | Any traffic that does belong to the branches are forwarded to the internet gateways. | |  | |
| Bridge remote LAN subnet | | Bridge over Tunnel | |  | |
| **Routing** | | | | | |
| OSPF | |  | |  | |
| BGP | |  | |  | |
| PIM Multicast | |  | |  | |
| **Flow Optimization** | | | | | |
| Dynamic WAN Link Selection and load balancing | | Based on criteria such as reachability, delay, packet loss, jitter, LTE Signal Strength | |  | |
| **Application Awareness** | | | | | |
| Application based routing | | Flow classification based on deep packet inspection. Application traffic is steered, and policies enforced based on these filters. | |  | |
| Application visibility | | Application traffic is categorized and IPFIX data transmitted. | |  | |
|  | | Encrypted packet support | | - | |
| **QoS** | | | | | |
| QoS marking | | Bidirectional support of QoS marking, classification, policy and shaping. | |  | |
| Priority Queuing | | Prioritize packet flows based on traffic class | |  | |
| Apply QoS policy to packets | |  | |  | |
| QoS adjustment | | Failure of one or more networks links results in readjustment of QoS policies of other sessions to conform to QoS policies | |  | |
| **Reporting** | | | | | |
| Traffic visibility | | Traffic statistics like tunnel bandwidth consumption, application usage, etc. exported using IPFIX | |  | |
| Application visibility | | Traffic statistics for custom Application (defined using 5 tuples) | |  | |
| IPFIX export | | Netflow | |  | |
| Syslog | |  | |  | |
| **Tunnel Support** | | | | | |
| IPSEC | | * Null encryption * 168 bit 3DES-EDE-CBC * 128 bit Blowfish-CBC * 192 bit Blowfish-CBC * 256 bit Blowfish-CBC * 128 bit AES-CBC * 192 bit AES-CBC * 256 bit AES-CBC * 128 bit AES-COUNTER * 192 bit AES-COUNTER * 256 bit AES-COUNTER * 128 bit AES-CCM;64 bit ICV * 192 bit AES-CCM;64 bit ICV * 256 bit AES-CCM ; 64 bit ICV * 128 bit AES-CCM ; 96 bit ICV * 192 bit AES-CCM ; 96 bit ICV * 256 bit AES-CCM ; 96 bit ICV * 128 bit AES-CCM ; 128 bit ICV * 192 bit AES-CCM ; 128 bit ICV * 256 bit AES-CCM ; 128 bit ICV * 128 bit AES-GCM ; 64 bit ICV * 192 bit AES-GCM ; 64 bit ICV * 256 bit AES-GCM ; 64 bit ICV * 128 bit AES-GCM ; 96 bit ICV * 192 bit AES-GCM ; 96 bit ICV * 256 bit AES-GCM ; 96 bit ICV * 128 bit AES-GCM ; 128 bit ICV * 192 bit AES-GCM ;128 bit ICV * 256 bit AES-GCM ;128 bit ICV * Null encryption ; 128 bit AES-GMAC * Null encryption ; 192 bit AES-GMAC * Null encryption ; 256 bit AES-GMAC * 128 bit Camellia-CBC * 192 bit Camellia-CBC * 256 bit Camellia-CBC * 128 bit Serpent-CBC * 192 bit Serpent-CBC * 256 bit Serpent-CBC * 128 bit Twofish-CBC * 192 bit Twofish-CBC * 256 bit Twofish-CBC * 128 bit CAST-CBC * 128 bit Camellia-COUNTER * 192 bit Camellia-COUNTER * 256 bit Camellia-COUNTER * 128 bit Camellia-CCM ; 64 bit ICV * 192 bit Camellia-CCM ; 64 bit ICV * 256 bit Camellia-CCM ; 64 bit ICV * 128 bit Camellia-CCM ; 96 bit ICV * 192 bit Camellia-CCM ; 96 bit ICV * 256 bit Camellia-CCM ; 96 bit ICV * 128 bit Camellia-CCM ; 128 bit ICV * 192 bit Camellia-CCM ; 128 bit ICV * 256 bit Camellia-CCM ; 128 bit ICV * 256 bit ChaCha20/Poly1305 ; 128 bit ICV | |  | |
| Rekey support | |  | |  | |
| SSL Tunnel | | SSL VPN is mutual authentication. Server authenticates Client and vice versa.  Server can accept any Client connection as long the both use same CA certificate and the Host certificate are generated and signed by the same CA certificate. Additionally, peer connection can be filtered based on Certificate Common Name (CN). | |  | |
| Tunnel Concentrator (server mode) | | CPE used in DC (Hub) | |  | |
| **Utilities** | | | | | |
| NTP | | Time synchronization | |  | |
| X509 certificate management | |  | |  | |
| Multihome DHCP | |  | |  | |
| DNS | |  | |  | |
| SSH | |  | |  | |
| NAT/PAT | |  | |  | |
| 802.1Q VLAN Tagging | |  | |  | |
| Bandwidth measurement | | Measure bandwidth between Tunnel endpoint | |  | |
| SpeedTest | | Interner Speedtest | |  | |
| **Additional Features** | | | | | |
| OS on eMMC | | Supported hardware’s | |  | |
| Firmware Management | | Firmware Update , Factory Reset, Restore Last Image | |  | |
| Verified Boot | | Signed booting process with 5.10 kernel | |  | |
| Local Web UI | | To perform Initial configuration | |  | |
| MAC allow/block | |  | |  | |
| Geofencing | | based on Trusted MAC | |  | |
| Branch subnet with IPSET | | To configure multiple subnet list with ease on NB and Flow Classifier | |  | |
| Saas Flow control and path affinity | |  | |  | |
| WIFI AP and Station mode ( supported hardware’s ) | | 2.4 GHz and 5GHz band AP and Station mode – based on supported hardware models | |  | |
| SNMP(v2 & v3) | | Basic SNMP service and SNMP TRAP alert for critical events | |  | |
| CPE configuration backup and restore | | Configuration backup and recovery | |  | |

# New Features / Enhancements

**None**

# Bug Fixes

**Resolved Bugs list:**

<http://usredmine.amzetta.com:8080/redmine/projects/ux_usabilium/issues?query_id=540>

# Known Issues/ Limitations

* **Patch Update:** Patch update will fail if the unit is taken for debugging and developer change the binary or script manually in the unit for the purpose of debugging.
* **5G support:** CPE 1.2 does not support 5G.
* **Director :** Use Tag 1.1.1-t20 or above

# Notes & Recommendations

1. Refer [Installation document.](https://gitlab.amzetta.com/sdwan/zwan-doc/-/tree/master/Installation)