zWAN Director


# PRODUCT OVERVIEW

## SD-WAN Centralized Management

An SD-WAN (Software-Defined Wide Area Networking) solution is a digital transformation of your network connectivity providing for enhanced security, optimized performance, lower costs, and ease of management for users and IT staff. The implementation of an SD-WAN solution will enhance application performance, user performance, reduce network expenses, unify network connectivity, and enable orchestration of application delivery across your network while increasing network security.

The AmZetta zWAN solution provides organizations with a comprehensive SD-WAN fabric complete with centralized management and enterprise security measures with the flexibility to extend into any environment, whether it be another physical location (home office, branch office, or datacenter) or multiple cloud vendors, on the fly with ease. The software can be run on a multitude of hardware, virtual appliances, and cloud directors to meet any organizational requirement. At the heart of AmZetta's zWAN solution lies the Director. The Director is the centralized management interface where control over the underlying networks, devices, sessions, edge controllers and data analytics are managed. The director can be installed on physical or virtual servers and resides either in the datacenter or in the cloud.

Take a detailed look into the features that AmZetta provides within the zWAN solution below.

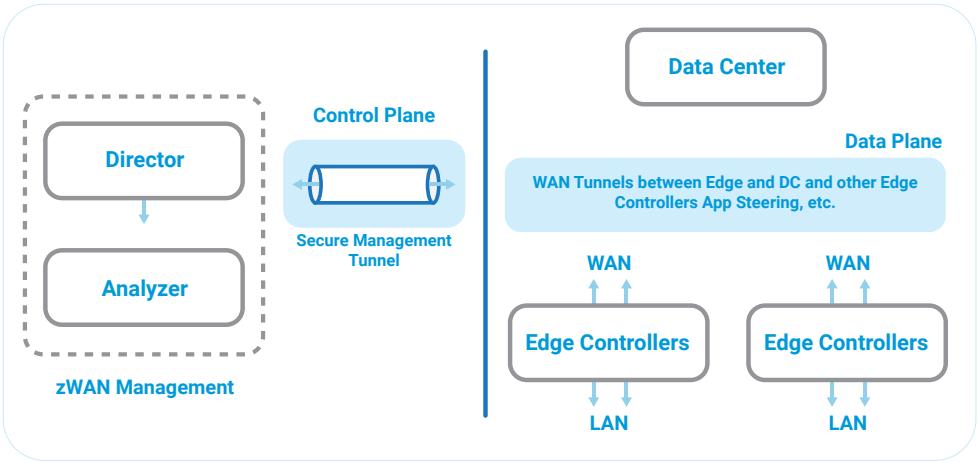


**Figure 1:** zWAN Architecture

# zWAN DIRECTOR FEATURES

## zWAN Dashboards & Reports

At the heart of any reasonably sized network, should be a solid strategy around flow collection, querying and visualization. Proper use of flow logs is crucial to SecOps/NetOps from triaging attacks to capacity planning and traffic trending.

zWAN dashboards and reports provide a complete view of the network flows and threats. zWAN displays the flow and log statistics information at two levels, Director level and Edge Controller level.

## Dashboards

### Overview

It serves to display an overview of the servers, clients, services, and protocols of the network.

### Top-N

Whose function is to show the most active services, applications, and accesses on the network. The dashboard consists of 4 additional dashboard, Top Applications, Top Talkers, Top Services and Top Conversations.

### Threats

This dashboard includes a dictionary of public IP addresses that are known to have a poor reputation. This dictionary is built from many OSINT data sources, normalized to a common taxonomy. The Threats dashboard uses this IP reputation information to highlight three threat/risk types.

**IP Reputations** – Number of flows with reputation

**Public Threats** - Public clients with a poor IP reputation that are reaching private addresses.

**At-Risk Servers** - Private Servers that are being reached by clients with a poor IP reputation.

**High-Risk Clients** - Private clients that are accessing public servers which have a poor reputation.

### Geo IP

Geo Location dashboards for Client/Server and Source/Destination perspectives for network flows.

### Traffic Details

Provides more detailed breakdown of various network traffic characteristics. Additionally, it has Servers, Clients, services, and application-based traffic details.

### Flow Records

Provides a peek into the total flows and various types of flows with a list of service logs. This will be client/server based or source/destination-based logs.

### Statistics

Provides network statistics in the form of transmitted/received data, transmitted/received packets, transmitted/received errors for each of the interface in the network. Additionally, events and syslog logs are also listed. Transmitted data rate and received data rate are also displayed in this dashboard.

### Site Availability

SLA – Overall Availability provides SLA percentage uptime for all the edge controllers onboarded with the Director. Edge controller SLA provides uptime duration across a selected time interval.

### Edge Controller Level Charts

In addition to the charts mentioned above there are few more dashboards which are available for edge controller only.

### Overview, System, Interfaces

In addition to the CPU and memory utilization statistics for each edge controller this dashboard also displays link status of the network interfaces transmitted/received bytes and signal quality if GSM/LTE is present. It also displays TWAMP outbound average latency, jitter and packet loss for configured interfaces.

### Flows

Client/server flows which displays network statistics in bytes for each flow between client and server. AS Flow which displays the autonomous system flows between the source and the destination.

### AS Traffic

Provides a view of traffic to and from Autonomous Systems (public IP ranges).

### Flow Exporters

Provides egress and ingress data in bytes for each interface in the edge controller.

### Traffic Details

Provides more detailed breakdown of various network traffic characteristics based on the Traffic Types, Attributes and Locality.

### Global Applications

Provides application-based statistics like top applications and usage in bits per second and packets per second.

### Link Status

Provides the up time and status for each network interface in the edge controller.

## Signal Quality

If the edge controller is equipped with a GSM/LTE module then the RSSI (Received Signal Strength Indicator), SNR (Signal to noise ratio), RSRQ (quality of the received signal) and RSRP (average power received from a single Reference signal) statistics will be provided in this dashboard.

## TWAMP

The Two-Way Active Measurement Protocol (TWAMP) is an open protocol for measuring network performance between any two devices in a network that supports the protocols in the TWAMP framework. This dashboard displays the inbound, outbound and roundtrip data based on latency, jitter and packet loss.

## Logs

System logs, Firewall logs – a list of system logs and firewall logs are provided in this dashboard.

## IPS Alerts

Alerts by GeoIP – a map showing the distribution of alerts by their country/region of origin based on geographic location (determined by IP).

**Top Alerts** – a summary of the most frequent triggered alerts and their description. Clicking an individual alert filters down the dashboard to the information pertaining to that specific alert.

**Number of Alerts** – the total count of alerts triggered by the ruleset.

Top alerts based on Suricata defined signatures, HTTP and protocols.

Top 20 Source/Destination IPs/Ports - pie charts showing the top 20 IPs and ports that alerts were triggered on. You can filter down on specific IPs/ports to see how many and what kind of alerts are being triggered.

Top alerts by TLS certificate issuer distinguish name.
Top multiple unique alerts by destination IP address.
Top multiple unique alerts by source IP address.

Top alerts by TLS Server name indication protocol by which a client indicates which hostname it is attempting to connect to at the start of the handshaking process.

Alert Summary – a table summarizing specific details of each individual alert. You can customize this table to show other parameters of interest for each alert.

## IPS Flow

Provides count of flows for various protocols used by the application. It also displays unique count of source and destination IP addresses, mean flow age and a list of flow events.

## DNS Alert

Displays various statistics for dns alerts generated via “Unbound DNS Resolver” in the edge controller. Stats like overall log count, log count based on return code and event list is provided.

## Reports

Reporting in zWAN is on demand and can be generated at the Director level or edge controller level. Reports can be generated for various intervals with minimum granularity as a minute and maximum as a year.

Reports generated from Kibana have some major issues:

1. Reports cannot be customized.
2. However big report template is it will always generate one page only. (bug)

To fix the issues, we modified the Kibana source to include HTML based reports. These can easily be customized with customer logs and images and the content can also be easily updated.

The Director UI is very simple where in the user must select the type of report and time range after which the report will be loaded on a new tab of the web browser. Once the report is generated the user will be prompted for print it via the print dialog.

**System** – CPU and memory utilization statistics

**Interface** – Transmitted and received data and data-rate based on bytes, packets and errors.

**TWAMP** - The Two-Way Active Measurement Protocol (TWAMP) is an open protocol for measuring network performance between any two devices in a network that supports the protocols in the TWAMP framework. This dashboard displays the inbound, outbound and roundtrip data based on latency, jitter and packet loss.

**Application** – Global application charts to display application statistics as Top applications, usage in packets per second and bits per second. ISP traffic usage (rate) in bytes and packets for each application and for each service

**Firewall Log** – Provides network interface status by link uptime. In addition to that it also displays the overall log count and various events list based on event type like net_balancer, syslog etc.

**Log** – Displays a list of system logs and event list. This can be downloaded as CSV by using the “Export >> Formatted” link provided at the end of the list.

## zWAN PRIMARY FEATURES

| Feature | Description |
|---|---|
| **Centralized Management and Analytics** | zWAN is composed of two main components.<br><br>- A centralized management server(s) that is responsible for the control and management of the SD-WAN functionalities and devices.<br><br>- Distributed edge controller(s) that is responsible for all the data traffic.<br><br>The management server can be hosted on-prem or can be hosted in a cloud. This server(s) is horizontally scalable and is resilient to node failures. |
| **True Zero Touch Provisioning** | zWAN supports a secure true zero-touch provisioning of edge controllers. In order to onboard a device in a remote location the only skill required is the ability to connect the cables and devices are automatically provisioned and configured to operational status. The network administrator can setup rules and policies that will be automatically applied when a matching edge controller is on boarded. |
| **Intuitive Visual Interface** | zWAN provides an intuitive visual interface. This allows for a very little or no learning curve, even for users who are not proficient with networking technologies and concepts. Users should be able to<br><br>- See topology, identify problem areas, alerts in one dashboard<br>- Configure rules, virtual tunnels<br>- Onboard/provision devices.<br>- Setup firewall, add/remove clients etc. |

## ADDITIONAL FEATURES

| Feature | Description |
|---|---|
| **Authentication/Authorization Director** | zWAN can connect to multiple backend authentication/authorization Directors like LDAP and Active Directory to provide admin login and authorization. In addition, zWAN can also add MFA to these logins as an additional security, even if these backend do not support it. |
| **Action Template** | zWAN allows you to use/create action template that can be used to apply configurations for large scale deployment. MSP can create or extract Action template from an existing Tenant. Action Template can contain within themselves various parameters like tunnel configuration, firewall rules etc. and one can create as many actions as one wish. These Actions can be applied to any number of Edge controllers or can applied automatically based on rules when a new Edge controller is on boarded. |
| **Data Collection and Analytics** | zWAN edge controller collects information about the flows that it sees and sends it to the centralized reporting server using IPFIX. This data is analyzed, and various metrics are provided to the user such as<br><br>- Top talkers<br>- Application usage<br>- Top protocols<br>- Geographical usage<br><br>The user can employ cross-filters in these dashboards to drill-down the metrics. zWAN also provides the ability for the user to create their own dashboards based on their need. The user can also configure the server to send out alerts based on the certain thresholds. Various alert mechanisms are supported such as<br><br>- Email<br>- Webhooks |

| | |
|---|---|
| **Syslog** | zWAN edge controllers can be configured to send their syslog output to a user configured syslog server. By default, syslog messages are sent to the reporting server. |
| **Underlay Connectivity** | zWAN supports multiple types of underlay connectivity such as Ethernet, DSL, LTE, fiber or Wi-Fi. The underlay connectivity service could be either public or private and can be un-managed (public broadband) or private (MPLS). zWAN uses the underlay connectivity's characteristics such as cost (flat, usage based etc.), bandwidth, latency, jitter etc. to make decisions on application steering. |
| **Tunnel Virtual Connections** | zWAN supports various tunnel virtual connections between zWAN Edge Controllers. zWAN supports both hub-spoke and mesh topologies. The connections can be encrypted and can be carried over public or private underlay connections. Applications are steered to these tunnels based on their performance/cost/time goals. |
| **Flow Categorization and Automatic Tunneling** | The zWAN Edge Controller categorizes flows and automatically channels the packets to the appropriate tunnel based on the policies and the destination. |
| **Internet Breakout** | There are cases where a set of traffic benefits by directly sending to the internet instead of one of the tunnels. The zWAN edge controller can be configured to classify those packets and steer them directly to the Internet. |
| **Traffic Shaping** | Bandwidth is a limited resource and needs to be used wisely for effective performance of various applications. zWAN allows a network admin to setup limits on bandwidth usage on a per-application basis. The admin can set guaranteed and maximum bandwidth limit on a per-application basis. |
| **Prioritization and QoS** | Certain class of applications like voice and video benefits by traversing a high bandwidth / low latency network. zWAN can classify those packets and can steer those packets to a matching underlay network so that the Quality of Experience is maintained. Optionally zWAN can also the mark the DSCP bits and let the downstream network to perform appropriate prioritization. |
| **Load Balancing and Failover** | zWAN can load balance across multiple WAN Links and recover from link failure within seconds. If a link carrying application traffic fails, the application traffic will be moved from the failed link to a functioning link in seconds without any application timeouts or disconnects. |
| **OSPF Support** | zWAN can create OSPF on virtual networks and create a seamless mesh network topology between branches. The route between branches is auto learnt based on the availability and cost. OSPF provides fast route convergence from link failures. Branch LAN network details can easily be exchanged between each other with OSPF. This enables an entire LAN network to move from one branch to another. |
| **BGP Support** | BGP (Border Gateway Protocol) is a dynamic routing protocol used between two network hosts. BGP is designed to exchange routing information between Autonomous Systems (AS) on the internet. All packet exchanges on the internet go with ASN as the unique identifier. It can be used for the WAN network or exterior routing (eBGP) and the LAN network or interior routing (iBGP). |
| **Multicast** | Multicast provides an efficient method for delivering traffic flows that can be characterized as one-to-many or many-to-many. zWAN supports PIM (Protocol Independent Multicast) to provide multicast support. |
| **Stateful Inspection Firewall** | Stateful firewall services with ACL and/or time-based ACL provides supervision and control. Firewall policy can be applied to one or more edge controllers from the centralized location. |

| | |
|---|---|
| **Flow Classification** | Flow classification applies various filters on the network packets and takes specific actions based on the match. The following actions are covered<br><br>- Load balancing<br>- QoS<br>- Firewall<br><br>The following filters can be applied on the input and output interfaces<br><br>- Source IP (range)<br>- Destination IP (range)<br>- Packet size<br>- DSCP mark<br>- IP protocol type<br>- Port (range)<br>- TCP Flag<br>- Connection state<br>- Deep packet inspection<br>- Time<br>- Connection Limit<br>- Bandwidth usage |
| **SSL Tunnel** | SSL VPN is mutual authentication. Server authenticates Client and vice versa. Server can accept any Client connection as long both use same CA certificate and the x509 Host certificate are generated and signed by the same CA certificate. Additionally, peer connection can be filtered based on Certificate Common Name (CN). |
| **IPSEC Tunnel** | IPSEC Tunnel supports 50+ various encryption types to meet any and all security requirements. |
| **Bridge** | zWAN support software bridge. By combining multiple virtual tunnels and VLAN LAN interface in the bridge, ARP broadcast domain can be extended between branches and subnets can be spanned across remote locations. By enabling STP, path redundancy can be achieved without introducing loop in the network. |
| **Bond** | zWAN support link aggregation both in load balancing and failover mode. By combining multiple virtual tunnels in the BOND, per packet load balancing can be achieved. Failover mode can restrict the packets to a particular path, the second link can be standby. |
| **Multi-homed DHCP server** | A multi-homed DHCP server is useful in creating multiple subnets. zWAN's DHCP server helps to create multiple networks on the same interface by making use of the VLAN functionality, which in-turn helps to classify the traffic based on the domain/subnet and steer traffic through the SDWAN edges controllers. |
| **TWAMP** | Two-Way Active Measurement Protocol otherwise known as TWAMP is an open protocol for measurement of two-way metrics. The minimum and maximum latencies and jitter can be calculated based on the test session. The information collected is analyzed by Orchestrator to tune the network based on the SLA and perform efficient load balancing, QoS and flow classification of the zWAN Edge Controller. The periodicity of running the test sessions can be configured from the Director. The TWAMP scheduler module running in the Edge Controller then run the test sessions based on the parameters configured. |
| **IPS** | zWAN support IPS/IDS for ingress internet traffic. zWAN IPS can quickly identify, stop, and assess the most sophisticated attack. Monitoring can be enabled for Alert or Prevent, based on rule priority and category. It also supports explicit allow list and block list. IPS rules repository can be hosted in Central Controller and the rules will be updated in all Edge Controllers. |
| **IPv6** | IPv6 is supported for WAN interfaces. SSLVPN/IPSEC tunnel can be created over IPv6 and carry IPv4 LAN traffic. |
| **Firmware Management** | Edge Controller Firmware upgrade is managed from Central location. Each Tenant can have its image based on the deployment requirement. Firmware image are tamper proof. Edge controller can boot from known good image. |

## AmZetta zWAN Solution

The AmZetta zWAN SD-WAN solution provides organizations the following components:


**Director** (Cloud or On-Prem)
Central Management Server for ease of management and monitoring.

**EC & vCPE** (Branch Office)
An Edge Controller (EC) is installed at branches, to route local network traffic securely and optimally between branches and destinations. The Edge Controller can be a hardware device or software installed in a VM.

**EC & vEC** (Home Users)
The Virtual Edge Controller (vEC) is software that installs on the EC for security scanning and risk scoring to determine resource access.

**Report Generator**
Real-time reporting of network traffic and application usage as well as other metrics. Track users website and app usage.

**zID** (MFA)
Integrated Multi-Factor Authentication for secure access.

## Conclusion

SD-WAN enhances application performance, user performance, reduces network expenses, unifies network connectivity and enables orchestration of applications are securely delivered across your network while enhancing network security. With the zWAN Director, management is centralized in a single interface that grants control over all underlying networks, users, devices, sessions, edge controllers and data analytics are easily managed.

## How to Get Started?

AmZetta offers free 30-day evaluation with no obligation to purchase. Simply visit https://AmZetta.com/Eval and complete the Evaluation Form. An AmZetta Solutions Engineer will help you get started with your evaluation.

AMZETTA.COM

**AmZetta Technologies**
5555 Oakbrook Parkway, Suite 280
Norcross GA 30093

**Sales & Product Information**
sales@AmZetta.com
1-877.991.1809

**Technical Support**
support@AmZetta.com
1-800.892.6625