Infinxt

THE NEXT GENERATION SD WAN

INFINXT SDWAN

DATASHEET

TRUE SDWAN - DATA AND CONTROL PLANE SEPARATION

The concept of SDN (software defined networking) emphasizes on separation of user and control plane traffic. SD-WAN being based on the concepts of SDN should also ensure user and control plane traffic separation. Infinxt provides this separation by using two separate tunnels from the device for management and user traffic individually. These two tunnels are described in detail as below:

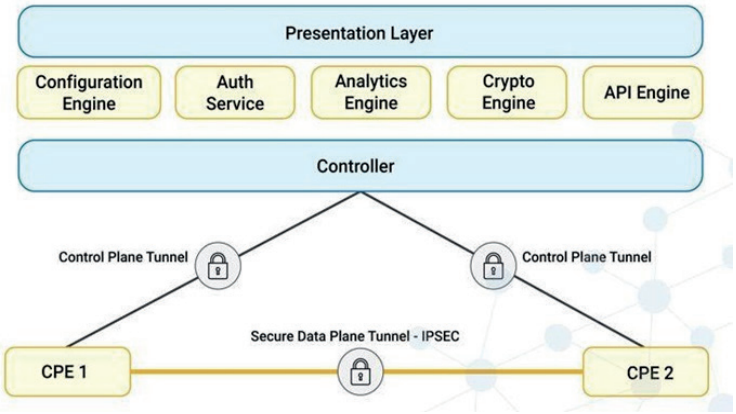
I.CONTROL PLANE TUNNEL

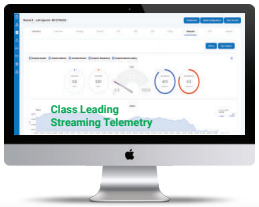
This is the secured management tunnel established from the controller to the CPE units. In Infinxt this tunnel use TLS v1.2 for data security. The main traffic which goes through this tunnel is the configuration commands from controller to the device, network monitoring traffic, KPI monitoring, API communication between the CPE and controller etc. This control plane tunnel is created automatically when a session is initiated by the CPE device on it being switches on and plugged to the network.

II. USER PLANE TUNNEL

This tunnel is formed between the two CPE devices. IPSec/Wire guard is the protocol which is used for this secured tunnel creation. Infinxt VPN is an indigenously developed VPN over wire guard technology. The traffic that traverses through this tunnel is primarily the user traffic. Since this is established only between the user CPE devices, there is no business information or user data that goes up to the controller, rather it is exchanged only between the user locations. Some SDWAN solutions do take all the user traffic till the controller which defies the overall SDN and SDWAN concept and poses data security risk as well. This tunnel can be established by either Auto VPN feature or the generic IPSec configuration through GUI or through Infinxt VPN that has pre-defined security parameters.

INFINXT NEXT GENERATION SD-WAN ARCHITECTURE





SOLUTION FUNCTIONAL CAPABILITIES

GENERAL FUNCTIONS

a) Infinxt is a true SDWAN solution complying with SDN principles where the data plane is separated from the control plane. When the CPE devices constitute the data plane, the control plane is maintained in the cloud or customer Datacentre in both physical or virtual form factor. The CPE devices are configured through the WebUI that is available in the controller. The CPE devices to get registered on to the fabric needs to first authenticate itself with the controller and download the policies and routing information.

b) Infinxt supports applying Global Policy Templates for the remote configuration of multiple appliances together.

c) The solution supports RBAC (Role Based Access Control) whereby the user access rights are defined as the role and job profile of the IT administrator. The user gets access to only relevant information based on their roles and privileges. User authentication function is handled by the authentication engine microservice in the Infinxt controller.

d) Infinxt supports definition of custom roles in addition to pre-defined roles with privilege level of users like Read , Write,

e) Execute etc.

f) Infinxt support abstraction of the underlay heterogenous transports and creates an overly transport that help in application SLA based performance management.

g) In Infinxt, when the CPE devices are registered for the first time through ZTP, the IT administrator has the option to define the topology of the new CPE device. The VPN tunnel options available are Gateway-to-gateway, VPN termination in transparent mode, Hub-spoke, partial mesh, and full mesh topology.

h) The solution is flexible to add the CPE device at the gateway not necessarily having to terminate the WAN links directly on to the device for its monitoring and other SD-WAN functions. The WAN links could be routed through any other gateway device like WAN switch, router, firewall etc.

I) The data plane can be hosted as an NVF in any device, or it is available in the appliance form factor. If there are any workloads in the cloud service providers like Azure, AWS, etc, Infinxt edge image can be deployed from the marketplace.

J) Infinxt supports VRRP (Virtual Router Redundancy Protocol) for high Availability of the solution components

k) Infinxt can do address translation between private and public IP address spaces and support source-based NAT and destination-based NAT

l) It can also be integrated with the existing third-party system like NMS, payment gateway, SMS gateway, SIEM tool etc using REST API where data can be XML or JSON coded.

m) Infinxt CPE devices supports application-level performance monitoring, and traffic control to improve business-critical application performance, facilitate capacity management and planning, and reduce network operating costs. It exports this real time telemetry to the controller for the analytic engine to provide various statistics.

n) Infinxt CPE device needs to register itself to get added on to the SDWAN fabric. For this the device needs to get the IP address and do the DNS resolution to reach the controller. By default, it acts as DHCP relay and tries to get the address from the available DHCP server. But if the situation demands it can also to configured as a DHCP server to facilitate device authentication and registration.

o) Infinxt SDWAN solution supports IPv4 and IPv6 from day one.

p) Infinxt supports hybrid deployment where Non SDWAN sites and SDWAN enabled sites would interoperate in the SDWAN topology.

q) The solution is by default a layer 4 firewall where the ACLs can be created to control the traffic through the gateway

r) Infinxt can perform time synchronization with NTP server.

s) URL filtering helps in restricting access to unnecessary websites and blocks access to domains and websites with low reputation.

t) Infinxt supports virtual interface (IEEE 802.1Q) and all the networking ports are universal/configurable.

u) Path MTU can be detected automatically

v) The solution supports VoIP traffic

w) Infinxt has R&D center & support center in India.

x) Infinxt supports built-in DNS Server and DNS proxy services

ADVANCED ROUTING FUNCTION

a) The solution should be capable of selecting path per traffic type

b) It supports all the major IEEE standard routing protocols like OSPF, BGP, Static, RIP, PBR and Pfr to have the capability to forward traffic via specific WAN paths depending on predefined application policies and performance needs.

c) Infinxt can send packets on same path (symmetric routing) based on the need (User configurable).

d) Infinxt supports BFD for faster convergence to ensure that a session doesn't break during a failover and failback.

e) Infinxt supports end-to-end network segmentation with separate routing and forwarding tables to securely isolate, Intranet departments, non-critical business traffic within a single appliance. It also supports application aware routing by which based on the application type each application can be routed through different path.

f) Applications are identified using SNI and the routing decision is based on the L7 visibility

g) Infinxt has in-built intelligence to support split-tunnels locally at branch site to handoff internet traffic to the ISP and at the same time create secured tunnels with the DC/DR sites for business-critical hosted application access. In fact, the architecture allows for internet break out at the local branch, centralized location, remote location, cloud etc based on the application and the policy defined in the software defined network controller.

h) Infinxt can monitor the remote IP address and change the traffic path according to availability of the remote IP address.

i) Infinxt can integrate transparently into the existing routing infrastructure and be completely transparent to existing routing protocols (eg:- OSPF, BGP etc.). All routing functions, including "dynamic path selection" or any other network routing decisions.

MULTITENANCY SUPPORT

a) Infinxt supports the multitenancy feature that enables ISP or MSP in providing SDWAN services to various customers and manage them through a single dashboard.

b) End customer can be provided with a separate dashboard for their organization to manage their own WAN Infrastructure. The logical separation and multi-tenancy capability are facilitated by the authentication engine of the controller as it enables identification using authentication and passing on the required permissions using authorization.

c) The solution supports VRF that allow for building multiple virtual networks that separate traffic, can carry overlapping IP address ranges, allow the application of distinct security and QoS policies for a subset of data such as guest Wi-Fi provide overall application security.

APPLICATION PERFORMANCE BENCHMARKING AND ENHANCEMENT

a) Infinxt can "pass through" certain applications/traffic without applying any Quality-of-service parameters which is of no interest to the administrator

b) The configured end device DSCP tagging will be preserved by without tampering for Quality of Service.

c) Infinxt can send duplicate data over both links for guaranteed delivery of all applications like data, video, etc. Real-time traffic duplication across multiple links mitigates against latency and packet drops.

d) Infinxt supports allocation of maximum bandwidth usage cap to each class of traffic with capability to burst above the maximum bandwidth usage cap if no other traffic classes attempt to utilize the available bandwidth.

e) It also supports guaranteed bandwidth base on different criteria such as application, Destination TCP/UDP port Number, Destination
IP address and Source IP address

f) Infinxt can define the traffic priority level (critical level) base on different criteria such as application, Destination TCP/UDP port Number, Destination IP address and Source IP address.

g) QOS over the encrypted channel between the edge appliances is also supported in Infinxt.

h) Infinxt can apply QOS policies to all the traffic seen in network, including both optimized and non-optimized traffic flows, including TCP, UDP and other non-TCP traffic types.

l) Infinxt monitors link SLA parameters and supports kink failover due to packet loss, Latency, Jitter, link flap & etc. without session drop.

j) Infinxt monitors the network performance parameters—jitter, packet loss, latency and hop count—and make decisions to forward critical applications over the best performing path based on the defined application policy.

k) Infinxt can leverage multiple links simultaneously for a single application session such that traffic can move across all the links. In case of any one link failing or poorly performing, the link session will not break but continue on the alternate link.

l) During the failure on one link, the critical traffic gets automatically migrated to the other available Service Provider Link without any manual intervention and without session disconnect. QOS will also be maintained during the failure of the WAN link.

m Infinxt does not add any latency for the current traffic path but provides a better performance of the encrypted traffic in comparison to IPSec due to the use of lightweight Wire Guard technology

n) Infinxt continuously checks the link flaps and link quality parameters and traverse the traffic accordingly. i.e. if the link is not stable it would be put in monitor state until it stabilizes to resume the service. In such cases of link flaps or link up/down will not affect the traffic as long as other link is available.

o) Infinxt supports priority queuing to prioritize packet flows for each traffic class defined through QoS.

p) If a failure of one or more network links occur and there isn't enough remaining bandwidth to serve all current sessions, current sessions will be adjusted to confirm with the QOS policies.

TRANSPORT AGNOSTIC FEATURE AND LOAD BALANCING

a) Infinxt is ISP transport agnostic that is not only compatible with MPLS, ILL, Broadband, PPPoE, LTE, Satellite, WiMax etc. but also can share the traffic load across these with application performance SLA

b) Infinxt supports Multiple WAN Links utilization and detects blackouts & brownouts by supporting active / active load balancing & Fast session failover. In terms of load balancing, it supports both
i. Per session load balancing
ii. Per packet load balancing

c) Infinxt supports LTE primary and LTE aggregation where wired WAN links may not be a feasible option and a wired connectivity shouldn't be a pre-requisite to adding a new device to the
controller.

d) The WAN path selection can be based on the near real time analytics of the WAN Links Capacity & Quality (Latency, Jitter, Volume, Packet Loss, hop count etc.).

e) Infinxt supports dynamic WAN path selection based on the policy set from the Infinxt SDWAN controller.

f) Infinxt supports load balancing to bind and balance branch traffic across multiple ISP links of any type like MPLS, Broadband, PPPoE, RT, LTE, ILL etc using different means like weight based, flow based, SLA based etc.

g) Infinxt supports bandwidth spill over where if the bandwidth of a single session exceeds the availability on any link, it uses multiple links simultaneously for the excess bandwidth requirement.

h) Infinxt builds connections dynamically between two data plane devices leveraging multiple links and apply logic for best path selection, traffic switching, QOS and dynamic link bonding.

VPN SECURITY

a) Infinxt maintains an industry standard secure virtual private network that connects the branch locations, and data centres on one single managed network.

b) Infinxt supports encryptions for end-to-end communication using standard encryption technology, such as AES256 or above over any type of WAN link. Rekeying functionality is also available in the solution for encryptions.

c) Infinxt provides data security through the choice of using Poly1305 and Chacha20 as encryption algorithms for the creation of encryption policies. It allows an encryption policy to be attached per virtual private network

d) Virtual private network configuration and policy is performed in the centralised controller

e) The addition of one or more branch devices into the network does not require any changes in the virtual private network configuration in Infinxt controller.

f) Infinxt provides the flexibility of having alternate hub destinations created for application specific traffic using a policy defined for it.

g) Infinxt automatically picks the tunnel encapsulation type based on the application and based on the policy specified in the Infinxt controller.

h) Changes in physical connectivity or physical connectivity type do not require any change in virtual private network configuration in the controller or CPE device at sites

i) The secured tunnel creation between the CPE devices is automated through ZTP/ZTD with any human intervention. The solution also supports DMVPN for a lightweight mesh topology.

j) Infinxt VPN tunnels are created dynamically without any static overlays between branch and the hub.

k) Infinxt supports IPSec VPN creation through configuration wizard to create secured VPN tunnels with third party gateway devices.

CENTRALIZED MANAGEMENT, MONITORING AND CONFIGURATION

a) Infinxt provides real-time streaming analytics on the path utilization, application specific bandwidth utilization and WAN link performance and device health. Though the solution supports SNMP version 2/3, the analytics data collection is done by better efficient and lightweight protocols than SNMP, eg: gRPC etc.

b) Infinxt facilitates pre-emption of failures and vulnerabilities through trend analysis of historical traffic and performance information which assist in trouble analysis, traffic forecasting and SLA compliance.

c) Infinxt dynamically controls data packet forwarding decisions by looking at application type, performance, policies, and WAN path status.

d) Infinxt controller could either be deployed in Public Cloud Service providers like AWS, Azure, GCP or any other IaaS service provider. It can also be deployed at customer Datacentre. It would have the WAN control and analytics capabilities.

e) Infinxt controller provides an intuitive single pane GUI dashboard that makes the solution user friendly and easy to manage.

f) Infinxt controller provides a single, unified platform for network service provisioning, monitoring and assurance, change and compliance management.

g) The feature ZTP (Zero Touch Provision) authenticates all CPE devices with the ZTP server using the authentication engine through PKI or whitelisting of the device serial number/UID.

h) Infinxt supports bandwidth testing on WAN links to check the available bandwidth.

i) Infinxt provides remote diagnostics tools to validate reachability of both WAN and LAN side, Packet Capture, Packet flow, traceroute, ping test etc.

j) As the corporate data never goes to the controller, there would not be any impact on SDWAN data forwarding capability in case of complete disconnection of controllers

k) When the controller is not reachable, Infinxt supports configurational changes to made at the individual CPE devices locally through the management / console port of the device which would be replicated to the controller on re-establishing the connection.

l) On detection of change of WAN IP/ISP of the device, Infinxt supports an alarm functionality to lock the device & and later OTP based SMS to activate the device.

m) Infinxt support Mobile app based ZTP/ZTD for plug and play installation.

n) Through templatised configuration capability, Infinxt supports bulk upload for activation and first-time configuration of edge devices.

o) Upgrade of SD-WAN CPE devices could be centrally done using the Controller/ Management/ Orchestrator platform.

p) Infinxt controller supports configuration in HA mode to avoid single point of failure

q) Infinxt centralised controller supports integration with third party ITSM tool for the workflow management for audit and compliance to review, approve and audit policy changes from the controller

r) Infinxt controller is flexible and scalable to manage the growth of SD-WAN edge devices due to its non-ASIC architecture.

s) Infinxt supports one way latency and traffic loss monitoring.

t) Infinxt dashboard provides guided workflows for deployment and management of SD-WAN infrastructure.

u) All network wide configurations and application forwarding policies are deployed from the controller.

v) The in-built NMS capabilities of Infinxt controller supports network wide device and network visibility for all the devices in the scope of the

REPORTING AND ANALYTICS

a) Infinxt supports granular Real-Time Monitoring and Historical Reporting like
   i. Statistic bandwidth usage of all available links.
   ii. Network Statistics including continuous performance monitoring of loss, latency, and jitter for all network paths
   iii. Link utilization
   iv. Tunnel Utilization
   v. Flow of each application.

b) Infinxt can generate report for
   i. Traffic statistics of all the included path
   ii. Specific application utilization
   iii. Path performance

c) Infinxt supports GUI (Graphical User Interface) for report generation.

d) Infinxt has the option for scheduling reports

e) Infinxt can provide reports of Individual link quality/ Virtual link quality on daily, weekly, monthly, yearly etc.
   i. Packet loss in the links
   ii. Jitter on the links
   iii. Latency of links

f) Infinxt can generate system events/logs for events that have taken place in the system such as login, changes to configuration and system related errors or warnings.

g) Infinxt supports syslog and email/SMS based real time alarm to notify the administrators when any device/link fault or network performance degradation happens.

h) Infinxt can export/customize reports as CSV format / PDF format.

i) Infinxt provides filtering and search capabilities for faster access to desired reports.

j) Infinxt records and maintains the history of all configuration changes made over time and generate trend reports.

k) Infinxt facilitates to go back in time and check for things like average throughput of the link, latency, jitter, etc.

l) Infinxt provides granular filtering and search capabilities

OPERATIONS AND SUPPORT SERVICES

a) Infinxt provides 24 X 7 facilities to raise trouble tickets and customer support on Remote.

b) Advanced replacement of faulty appliances for RMA is supported

c) Infinxt supports customization in case of any unique requirements with the availability of the OEM engineering/-support team in India

d) Infinxt supports controller based summarized view of device and link status along with notification.

PRODUCT PORTFOLIO OF DATA PLANE DEVICES

PARTICULARS	IEDGE-50	IEDGE100	IEDGE-1K
PRODUCT SKU	iEdge50-SDWAN	iEdge100-SDWAN	iEdge1K-SDWAN
Make in India Category	Class -1 local supplier	Class -1 local supplier	Class -1 local supplier
Deployment Mode	Small Branch	Large Branches	Datacentre
Fan less architecture	Yes	Yes	No
Native heatsink	Yes	Yes	No
Form factor	Desk mount	Desk mount	1RU
Appliance Architecture	x86	x86	x86
Interfaces	Universal 2 X 1GbE RJ45, 2 X USB, 1 X HDMI	Universal 4 X 1GbE RJ45, 2 X USB, 1 X HDMI	Universal 6 X 1GbE RJ45, 4 X 10G SFP+, 2 X USB, 1 X
Processor	Intel dual core	Intel dual core	Intel dual core
Power rating	230V, 1.5A(50-60Hz) to 12V, 5A AC/DC adapter	230V, 1.5A(50-60Hz) to 12V, 5A AC/DC adapter	230V, 120W(50-60Hz) AC Power Supply
Dual Power Supply	NA	NA	1+1 redundant, hot plug
Aggregated SD-WAN throughput	1.2 Gbps	2.8 Gbps	30 Gbps
Aggregated IPSec VPN throughput	200 Mbps	600 Mbps	12 Gbps
SD-WAN throughput	350 Mbps	700 Mbps	8 Gbps
IPSec VPN throughput	100 Mbps	150 Mbps	4 Gbps

ON-PREM CONTROLLER

On -prem controller can either be appliance based or VM based. In case of VM based controller the following would be the hardware specs and software requirements to support 1500 edge routers. Infinxt would be able to support more edge appliance through clustering for multiple controller instance.

DESCRIPTION	COMPONENTS
PROCESSOR(S)	Intel® Xeon® Silver 4216 (16-Core, 2.4GHz, 100W) with dual socket scalability option
RAM	128GB DDR4-2666 ECC UDIMM (Max 768GB, 6 DIMMs)
SSD/HDD(s)	4 x 2 TB SAS HDD (Datacenter grade, 1 DWPD)
RAID	2G SAS Modular RAID Controller
NIC	2 x 10Gigabit(10GBase-T) Ethernet on-board
Graphics	On-board graphics using A speed AST2500
Management	On-board IPMI 2.0 with dedicated LAN and KVM over LAN support
Exp. Slots	1 x PCI-Express slot
Ports	4 USB, 2 Network, 1 Management, 1 VGA
Chassis	1U rack-mountable with sliding rails
Power Supply	2 x 500W, 1+1 redundant, hot-plug power supplies (80PLUS Platinum)
OS	Ubuntu 20.04 or higher
Hypervisor	VMware
Database	Mongo DB

Infinity labs

Registered Office :
Teerth-Technospace, C-609,
Bangalore-Mumbai Highway, Baner,Pune, IN – 411045
Website : www.infinitylabs.inEmail: sales@infinitylabs.in

- Founded in 2014, Infinity Labs is one of the fastest growing Technology Consulting & Software Solutions.
- Serving customers across the Globe (India, US, UK & Middle East)
- Solutions customised for Telecom, Banking, Media, Retail, Education & Government verticals