Inflnxt

THE NEXT GENERATION SECURE SD WAN

NEXT GENERATION SECURE SD-WAN

is a transformational way to architect, deploy and operate corporate WANs, as it provides a simplified way of deploying and managing remote branch office connectivity in a cost-effective way.

VIRTUAL WAN FABRIC

- Secure overlay fabric
- Transport independence
- Network segmentation

SD-WAN GATEWAY

- Local policy enforcement
- WAN path selection, network QoS, firewall, service chaining
- Telemetry feedback loop to/from SD-WAN controller

SD-WAN CONTROLLER

- Establishes and manages secure virtual overlay to sites
- Defines service chains to enable policy goals
- Manages distribution of interpreted policy to individual elements

MANAGEMENT PORTAL

- Single pane of glass for network configuration and management : cloud-hosted and on-premises
- Zero touch provisioning
- Portal where user defines global policies
- Aggregated visibility on application performance
- User / Group based policies with support for Active Alerts, Logs Directory / LDAP or equivalent
- Centralized single console management of SD-WAN and UTM features

SD-WAN FEATURES

Routing	OSPF, BGP, Static, PBR, PPPOE
User Experience	Application Prioritization over available WAN
GPS (Optional)	Geo-Location tagging for device Geo-Fencing
VPN	IPSEC, L2TP, GRE, Client Access VPN with MFA DMVPN
QOS	Shaping Policy, Rate Limiter, Traffic Policies IPv4/IPv6, Traffic Shaper, DSCP Tagging
NAT	Source NAT, Destination NAT, NATv6, NAT64, NAT Traversal
Network Visibility	Real-Time Streaming Telemetry
Dynamic Multi-path Optimisation	KPI's–Jitter, Packet Loss, Latency, Per packet, Per Flow Load Balancing, FEC
Application Visibility	5000+ Applications, Application Awareness
High Availability	VRRP, Clustering
WAN Overlay over Cloud	Public-AWS, Azure, Private
WAN Policy	WAN Aggregation, LTE and Broadband Intelligent KPI Based Switchover
Advanced LTE	LTE Primary and Bandwidth Aggregation Capability
Troubleshooting	Bandwidth Measure, IPERF, Packet Capture, MTR, Speed Test,Traceroute, Alerts, Logs

LAYER7 SECURITY CAPABILITIES

VISIBILITY

- Near real-time Reporting & Logging
- Drill-down Advanced Network Analytics
- More than 60 pre-defined Reports
- Application Visibility & Reporting
- Web/DNS/TLS Reporting
- Custom Reports
- PDF Reports

SECURITY

- Protects all ports
- Protect all users/devices
- Auto-blocking based on Real-time Threat Intelligence
- IPS/IDS Protection
- Malicious server filtering
- Phishing server filtering
- Protection against new Malware/Virus/ Phishing Outbreaks
- Blocking newly Registered/Recovered/ Dead/DynDNS sites
- Automatic Botnet Filtering
- Blocking DNS/ICMP Tunnels
- Policy based Transparent TLS/SSL Inspection
- Web keyword filtering *

CLOUD CENTRAL MANAGEMENT

- Cloud Management
- Centralized Reporting
- Centralized Policies
- Cloud Scheduled Reports

CLOUD THREAT INTELLIGENCE

- Cloud Web Categorization
- Cloud Threat Intelligence
- Automatic Botnet Detection

FILTERING & COMPLIANCE

- Application Control
- Ad Blocking
- 300+ Million categorized Websites
- Customizable Web Categories/Whitelisting
- DNS based content filtering
- TLS/QUIC SNI based filtering
- Web & URL Filtering
- Customized Landing Pages for Blocked Sessions
- Cloud applications visibility & control *

USER-BASED FILTERING

- User-Based Reporting (Captive Portal)
- User-Based Reporting (AD/LDAP)
- User-Based Filtering policies (Captive Portal)
- User-Based Filtering policies (AD/LDAP)

POLICY-BASED FILTERING

- Filtering policies according to Subnet/IP Addresses
- Filtering policies according to User/Groups
- Time-Based/Scheduled Filtering
- Filtering policies according to Interface/VLAN
- Ability to create filtering exemptions
- Certificate based policy enforcement deep packet inspection *

INTEGRATIONS

- Reports streaming to external Elasticsearch Servers
- Reports streaming to external Syslog Servers
- Central Elasticsearch Reporting for all firewalls
- RESTful API access for configuration and management
- Sandboxing zero day threat protection *

* Features in Roadmap

HARDWARE SPECIFICATION	
Appliance Model	iEdge-1000M
Deployment Mode	Branch/Hub
Core/s	8/16/24
Chipset	Intel Xeon D-2876NT
CPU Architecture	X86
Memory(GB)	128 - 256
Storage	256 - 1024 GB SSD
Network Interfaces	Universal 8 X 1G, 4 X 10G SFP+ slots, 2 X NIM slots for expansion
USB(Supports 3G/4G Dongle for WAN)	2 X 3.0
V.35 Serial Port	Supported through external convertor
SIM Slot(3G/4G/LTE)	Optional
Console	RJ-45
WiFi	NA
Power Supply	1+1 redundant SMPS, hot-plug as optional
Power Input(AC)	230 V
Power Rating(W)	300
Operating Temperature	0°C to 40°C
Humidity	5%-95% relative humidity, non-condensing
Physical Dimensions(LxWxH)mm	438 x 420 x 44
Weight(kg)	8.23
Form Factor	Rackmount 1 RU
AGGREGATED PERFORMANCE	
Aggregated Application Visibility Throughput(Gbps)	120
Aggregated IPSEC/Secure Tunnel VPN throughput(Gbps)	30
Aggregated NGFW L7 Throughput(Gbps)	10
Packets Per Second(Mpps)	180
SESSIONS	
New Connections Per Second	Up to 900K
Max Sessions (IPv4 or IPv6)	Up to 16M
POLICIES	
NAT Rules	10000
ROUTING	
IPv4 Forwarding Table Size	Up to 10M
IPv6 Forwarding Table Size	Up to 1.56M
QOS	
Number of QoS Policies	7650
DSCP Marking by Policy	Yes
IPSEC/Secure Tunnel VPN	
Site-to-Site	10000
INFINXT REMOTE ACCESS VPN	
Max tunnels (Client based tunnel)	5000
HIGH AVAILABILITY	
Device Count	2

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