Fortinet Secure SD-WAN

airespring®
Cloud, Fully Managed and Connected

FORTINET SECURE SD-WAN

Fortinet's Secure SD-WAN simplifies operations, provides an optimal application user experience and delivers the lowest TCO of any SD-WAN solution.

Many multi-location businesses find that their traditional wide area networks (WANs) are unable to scale to meet the bandwidth requirements of digital transformation and innovations such as cloud on-ramping, Unified Communications (UC), and video conferencing and collaboration tools. These must-have technologies greatly increase traffic demands on the average enterprise's IT architecture, causing performance bottlenecks as well as increased operating expenses (OpEx) since many organizations rely on multi-protocol label switching (MPLS) connectivity. Once the secure cutting edge-connectivity option of choice, MPLS cannot always scale as quickly and affordably as SD-WAN. As a replacement for the traditional WAN, network engineering and operations teams are moving to software-defined wide-area networks (SD-WAN).

But many SD-WAN solutions lack robust security, which leads to greater risk exposure and a higher total cost of ownership (TCO). **Fortinet's Secure SD-WAN** consolidates robust networking, routing, and security capabilities in a single-box SD-WAN solution.

Fortinet Secure SD-WAN enables organizations to solve the secure communications problem for distributed locations quickly and easily. It is easy to manage, agile, reliable, flexible, and ultimately secure. Fortinet offers a custom-designed, Application Specific Integrated Circuit or ASIC for fast application identification and steering, while providing connectivity and advanced security capabilities.

Simplifies Complex Operations in the Enterprise

Fortinet Secure SD-WAN simplifies operations by consolidating various point products in a single solution that boasts a zero-touch installation with automated provisioning. This reduces risk, improves operations, and tightens security. Fortinet SD-Branch also decreases total cost of ownership (TCO) with one console instead of many, eliminating silos, and simplifying management for wired LAN/WLAN, SD-WAN, and security via a single pane of glass.

Fortinet Provides Fully Integrated Security

Fortinet Secure SD-WAN helps Enterprise IT meet the challenges of cloud applications, rapid scaling, higher complexity, rising costs and increasing cybersecurity risks. The solution delivers a consistent and agile network and security infrastructure that keeps up with today's dynamic technology environment across all the diverse clouds commonly used by enterprises today through cloud native integrations. With application-aware traffic steering and high-speed encryption, the solution leverages high bandwidth internet links to optimize spending on expensive direct connections.

Enterprises can get robust security enforcement, ensure compliance, and operate a seamless network with uniform policies while providing end-users a reliable and superior application experience.

Fortinet Secure SD-WAN

airespring®
Cloud, Fully Managed and Connected

Key Features & Functionalities	Benefits	Fortinet
AireSpring White Glove SD-WAN Professional Services	• Includes implementation design and engineering. • We will design (pre-sales), deploy (provisioning) and support (customer service/NOC) your SD-WAN solution at no additional cost. Plus we provide branch deployment support via pre-configuration of SD-WAN edge boxes.	✓
Free Network Monitoring 24/7/365	• 24/7/365 real-time monitoring by the AireSpring Network Operations Center (NOC), using AireNMS. • Proactive ticket initiation, management and resolution by AireSpring NOC in the event of a network alert.	✓
Free 3rd Party Circuit Support	• AireSpring will proactively open repair tickets on behalf of customers for their non-AireSpring, internet-only circuits. Not offered by many vendors. Only available at a premium cost by the few that do.	✓
Free Read and Write Access	• Read and Write Access to Dashboard. Provides customers with configuration level capabilities to their SD-WAN environment.	✓
WAN Failover	• Every Appliance supports multiple WAN uplinks with automatic failover for protection against connection outages. • Optional WAN warm spare failover ensures the integrity of service at the appliance level. In the event an appliance goes offline, a secondary device will automatically take over.	✓
3G/4G Failover	• Traffic is automatically redirected to a 3G/4G interface in the event of a connectivity failure. Requires existing or new 3G/4G circuit (sold separately).	✓
Advanced Firewall and Unified Threat Management (UTM)	• Next-Generation Managed Firewall with UTM features such as Intrusion Prevention System (IPS), Web filtering, Anti-virus, Anti-Spam, Application control. • Advanced Malware Protection (AMP) – provides malware detection for latest emerging threats, eliminates threats by stripping active content from files in real-time, protects against latest botnets, and protects against the latest threats targeting mobile platforms. • SSL deep inspection unlocks encrypted sessions, sees into encrypted packets, finds threats, and blocks them. • Control outbound and inter-network traffic using firewall rules.	✓
Maximum WAN Links	• The maximum number of WAN uplinks supported.	4+ (depending on model)
IPSec Virtual Private Networking (VPN)	• Provides the ability to quickly interconnect locations via an encrypted connection over public networks.	✓
Traffic Shaping	• Provides the ability to prioritize network traffic so that heavy-use applications or those requiring a significant amount of bandwidth to operate do not impact other users on the network.	✓
Per Flow Load Balancing	• Rule-based per flow load balancing. Packets of the same flow go over the same link.	✓
Priority Routing	• Routes calls and other priority real-time application traffic over cleanest WAN connection to eliminate dropped calls, choppy sound quality and echoes.	✓
Border Gateway Protocol (BGP) and Routing Support	• Full routing support: BGP, Open Shortest Path First (OSPF) and multicast.	✓
Bi-directional Priority Routing	• Application link/route decisions are made at the premises and within the AireSpring core network.	✓
Mix & match existing or new MPLS with your SD-WAN	• Mix and match over 20 different vendors with multiple access types to create the optimal solution for your enterprise.	✓
Secure and Private Direct Connection to Most Major Cloud Providers	• Connect privately and securely with full QoS to dozens of cloud providers, hundreds of datacenter providers, and thousands of SaaS providers.	✓
DDoS Mitigation	• Free DDoS Mitigation included with 3-year SD-WAN contract and AireSpring Gateway Access. DDoS Mitigation only provided on in-tunnel internet traffic traversing AireSpring Gateway Access.	✓
Access to AireSpring Gateway	• Able to connect to the AireSpring Gateway.	✓

Ready to find out more? Contact us at 888-389-2899, email sales@airespring.com, or visit our website at www.airespring.com

FORTINET®